Prácticas recomendadas para los switches Catalyst serie 6500/6000 y Catalyst serie 4500/4000 que ejecutan el software Cisco IOS

Contenido

Introducción
Antes de comenzar
Background
Referencias
Configuración Básica
Protocolos del Plano de Control de Catalyst
VLAN 1
Características estándar
VLAN Trunk Protocol
Negociación automática Fast Ethernet
Negociación automática de Gigabit Ethernet
Dynamic Trunking Protocol
Spanning Tree Protocol
EtherChannel
Detección de Link Unidireccional
Switching multicapa
Tramas gigantes
Funciones de seguridad del software Cisco IOS
Funciones de Seguridad Básicas
Servicios de seguridad AAA
TACACS+
Configuración de la Administración
Diagramas de la Red
Interfaz de administración del switch y VLAN nativa
Administración Fuera de Banda
Registro del Sistema
SNMP (Protocolo de administración de red simple)
Network Time Protocol
Cisco Discovery Protocol
Configuración de Lista de Verificación
Comandos globales
Comandos de interfaz
Información Relacionada

Introducción

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

Los switches Catalyst 6500/6000 y Catalyst 4500/4000 Series soportan uno de estos dos sistemas operativos que se ejecutan en el Supervisor Engine:

- SO Catalyst (CatOS)
- Cisco IOS Software

Con CatOS, existe la opción de ejecutar Cisco IOS Software en tarjetas secundarias del router o módulos como:

- Tarjeta de función de switch multicapa (MSFC) en Catalyst 6500/6000
- El módulo 4232 de capa 3 (L3) en el Catalyst 4500/4000

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

- La línea de comandos de CatOS para el switching
- Línea de comandos del software Cisco IOS para el ruteo

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

Para Cisco IOS Software, hay sólo una línea de comandos para la configuración. En este modo, la funcionalidad de CatOS se ha integrado en Cisco IOS Software. La integración da como resultado una sola línea de comandos para la configuración de switching y routing. En este modo, Cisco IOS Software es el software del sistema y reemplaza a CatOS.

Tanto los sistemas operativos CatOS como Cisco IOS Software se implementan en redes críticas. CatOS, con la opción Cisco IOS Software para tarjetas y módulos secundarios del router, se soporta en esta serie de switches:

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

El software del sistema Cisco IOS se soporta en esta serie de switches:

- Catalyst 6500/6000
- Catalyst 4500/4000

Refiérase al documento Prácticas Recomendadas para los Catalyst 4500/4000, 5500/5000 y 6500/6000 Series Switches que Ejecutan la Configuración y Administración de CatOS para obtener información sobre CatOS porque este documento cubre el software del sistema Cisco IOS.

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

- Una única interfaz de usuario
- Una plataforma de gestión de red unificada
- Funciones de QoS mejoradas
- Compatibilidad con switching distribuido

Este documento proporciona guía de configuración modular. Por lo tanto, puede leer cada sección de forma independiente y realizar cambios en un enfoque por fases. Este documento asume una comprensión básica y familiaridad con la interfaz de usuario de Cisco IOS Software. El documento no cubre el diseño general de la red de campus.

Antes de comenzar

Background

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

- Soluciones que, estadísticamente, tienen la exposición más amplia sobre el terreno y, por lo tanto, el menor riesgo
- Soluciones sencillas que ofrecen cierta flexibilidad para obtener resultados deterministas
- Soluciones fáciles de gestionar y que los equipos de operaciones de red configuran
- Soluciones que promueven la alta disponibilidad y la alta estabilidad

Referencias

Hay muchos sitios de referencia para las líneas de productos Catalyst 6500/6000 y Catalyst 4500/4000 en Cisco.com. Las referencias que se enumeran en esta sección proporcionan una profundidad adicional en los temas que se tratan en este documento.

Refiérase al Soporte de Tecnología de Switching LAN para obtener más información sobre cualquiera de los temas que abarca este documento. La página de soporte proporciona documentación del producto, así como documentos de resolución de problemas y configuración.

Este documento proporciona referencias a material público en línea para que pueda leer más. Pero otras referencias fundamentacionales y educativas buenas son:

- Aspectos esenciales de Cisco ISP
- Comparación de los Sistemas Operativos Cisco Catalyst y Cisco IOS para Cisco Catalyst 6500 Series Switch
- Switching LAN de Cisco (serie de desarrollo profesional de CCIE)
- Creación de redes conmutadas multicapa de Cisco
- Gestión de fallos y rendimiento
- SEGURIDAD: Un Plan General de Seguridad para Redes para Empresas
- Manual de campo de Cisco: Configuración del switch Catalyst

Configuración Básica

Esta sección trata sobre las funciones que se implementan cuando se utiliza 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. Una comprensión básica de los protocolos es útil cuando se aborda cada sección.

Tráfico de Supervisor Engine

La mayoría de las funciones habilitadas en una red Catalyst requieren la cooperación de dos o más switches. Por lo tanto, debe haber un intercambio controlado de mensajes de keepalive, parámetros de configuración y cambios de administración. Tanto si estos protocolos son propiedad de Cisco, como Cisco Discovery Protocol (CDP), o basados en estándares, como IEEE 802.1D (protocolo de árbol de extensión [STP]), todos tienen ciertos elementos en común cuando los protocolos se implementan en la serie Catalyst.

En el reenvío de tramas básico, las tramas de datos del usuario se originan en los sistemas finales. La dirección de origen (SA) y la dirección de destino (DA) de las tramas de datos no se modifican en todos los dominios conmutados por capa 2 (L2). Las tablas de búsqueda de memoria direccionable por contenido (CAM) en cada Supervisor Engine del switch se rellenan mediante un proceso de aprendizaje de SA. Las tablas indican qué puerto de salida reenvía cada trama recibida. Si el destino es desconocido o la trama está destinada a una dirección de difusión o multidifusión, el proceso de aprendizaje de la dirección está incompleto. Cuando el proceso está incompleto, la trama se reenvía (inundada) a todos los puertos de esa VLAN. El switch también debe reconocer qué tramas deben conmutarse a través del sistema y qué tramas deben dirigirse a la CPU del switch. La CPU del switch también se conoce como Procesador de administración de red (NMP).

Se utilizan entradas especiales en la tabla CAM para crear el plano de control de Catalyst. Estas entradas especiales se denominan entradas del sistema. El plano de control recibe y dirige el tráfico al NMP en un puerto de switch interno. Por lo tanto, con el uso de protocolos con direcciones MAC de destino conocidas, el tráfico del plano de control se puede separar del tráfico de datos.

Cisco tiene un rango reservado de direcciones Ethernet MAC y de protocolo, como se muestra en la tabla de esta sección. Este documento cubre cada dirección reservada en detalle, pero esta tabla proporciona un resumen, para mayor comodidad:

Función	Tipo de protocolo SNAP[1] HDLC [2]	MAC de Multicast de Destino
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+, RPVST+[4]	0x010b	01-00-0c-cc-cc-cd
Bridge VLAN	0x010c	01-00-0c-cd-cd-ce
UDLD[5]	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
UplinkFast STP	0x200a	01-00-0c-cd-cd-cd
IEEE Spanning Tree 802.1d	N/A: DSAP [7] 42 SSAP[8] 42	01-80-c2-00-00-00

ISL[9]	N/A	01-00-0c-00-00-00
VTP[10]	0x2003	01-00-0c-cc-cc-cc
Pausa IEEE 802.3x	N/D: DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

[1] SNAP = Protocolo de acceso de subred.

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

[3] PAgP = Protocolo de agregación de puertos.

[4] PVST+ = Por VLAN Spanning Tree+ y RPVST+ = Rapid PVST+.

[5] UDLD = Detección de Link Unidireccional.

[6] DTP = Protocolo de enlace troncal dinámico.

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

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

[9] ISL = Inter-Switch Link.

[10] VTP = VLAN Trunk Protocol.

La mayoría de los protocolos de control de Cisco utilizan una encapsulación SNAP IEEE 802.3, que incluye Logical Link Control (LLC) 0xAAAA03 e Identificador único organizacional (OUI) 0x00000C. Puede ver esto en un seguimiento del analizador de LAN.

Estos protocolos suponen conectividad de punto a punto. Tenga en cuenta que el uso deliberado de las direcciones de destino multicast permite que dos switches Catalyst se comuniquen de forma transparente a través de switches que no son de Cisco. Los dispositivos que no entienden ni interceptan las tramas simplemente las inundan. Sin embargo, las conexiones punto a multipunto a través de entornos de varios proveedores pueden dar lugar a comportamientos inconsistentes. En general, evite las conexiones punto a multipunto a través de entornos de varios proveedores. Estos protocolos terminan en los routers de Capa 3 y funcionan solamente dentro de un dominio de switch. Estos protocolos reciben prioridad sobre los datos del usuario mediante el procesamiento y la programación del Circuito Integrado para Aplicaciones Específicas (ASIC) de entrada.

Ahora la discusión gira hacia el SA. Los protocolos de switch utilizan una dirección MAC tomada de un banco de direcciones disponibles. Un EPROM en el chasis proporciona el banco de direcciones disponibles. Ejecute el comando **show module** para mostrar los rangos de direcciones disponibles para cada módulo para el suministro del tráfico como las unidades de datos del protocolo de puente STP (BPDU) o las tramas ISL. Este es un ejemplo de resultado del comando:

```
>show module
…

Mod MAC-Address(es)                         Hw      Fw          Sw
```

```
--- ------------------------------------ ------ ---------- -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)     6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- These are the MACs for sourcing traffic.
```

VLAN 1

VLAN 1 tiene un significado especial en las redes Catalyst.

Cuando se realiza el trunking, Catalyst Supervisor Engine siempre utiliza la VLAN predeterminada, VLAN 1, para etiquetar una cantidad de protocolos de control y administración. Estos protocolos incluyen CDP, VTP y PAgP. Todos los puertos del switch, que incluye la interfaz sc0 interna, se configuran de forma predeterminada para que sean miembros de VLAN 1. Todos los troncales llevan VLAN 1 de forma predeterminada.

Estas definiciones son necesarias para ayudar a aclarar algunos términos bien utilizados en las redes Catalyst:

- La VLAN de administración es donde reside sc0 para CatOS y switches de menor capacidad. Puede cambiar esta VLAN. Tenga esto en cuenta cuando esté interactuando con los switches CatOS y Cisco IOS.
- La VLAN nativa es la VLAN a la que regresa un puerto cuando no se conecta mediante trunking. Además, la VLAN nativa es la VLAN sin etiqueta en un troncal IEEE 802.1Q.

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

- Cuando el diámetro de VLAN 1, como cualquier otra VLAN, se hace lo suficientemente grande como para representar un riesgo para la estabilidad, particularmente desde una perspectiva STP, debe eliminar la VLAN. Consulte la sección Interfaz de administración de switches y VLAN nativa para obtener más detalles.
- Debe mantener los datos del plano de control en la VLAN 1 separados de los datos del usuario para simplificar la resolución de problemas y maximizar los ciclos de CPU disponibles. Evite los loops de Capa 2 en VLAN 1 cuando diseñe redes de campus multicapa sin STP. Para evitar los loops de Capa 2, borre manualmente la VLAN 1 de los puertos 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 ocurre incluso si se eliminó la VLAN1 de los troncos y no es la VLAN nativa. Si borra la VLAN 1 para los datos de usuario, la acción no tendrá impacto en el tráfico del plano de control que todavía se envía con el uso de VLAN 1.
- En un trunk ISL, los paquetes DTP se envían a través de VLAN1. Este es el caso incluso si la VLAN 1 se ha borrado 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. Este es el caso incluso si la VLAN nativa se ha borrado del trunk.
- En PVST+, las BPDU IEEE 802.1Q se reenvían sin etiqueta en la VLAN 1 del árbol de expansión común para la interoperabilidad con otros proveedores, a menos que la VLAN 1 se haya borrado del tronco. Este sucede independientemente de la configuración de la VLAN nativa. Las BPDU de PVST+ de Cisco se envían y etiquetan para el resto de las VLAN. Vea la sección Spanning Tree Protocol para obtener 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 ha borrado de los troncales.
- No borre ni inhabilite VLAN 1 en los trunks entre los bridges MST y los bridges PVST+. Pero, en el caso de que la VLAN 1 esté inhabilitada, el puente MST debe convertirse en root para que todas las VLAN eviten la ubicación del puente MST de sus puertos de frontera en el estado root-inconsistent. Consulte Comprensión de Multiple Spanning Tree Protocol (802.1s)para conocer los detalles.

Características estándar

Esta sección del documento se centra en las funciones básicas de switching que son comunes a cualquier entorno. Configure estas funciones en todos los dispositivos de switching Catalyst del software Cisco IOS en la red del cliente.

VLAN Trunk Protocol

Propósito

Un dominio VTP, que también se denomina dominio de administración de VLAN, se compone de uno o más switches interconectados a través de un trunk que comparte el mismo nombre de dominio VTP. VTP está diseñado para permitir a los usuarios realizar cambios de configuración de VLAN centralmente en uno o más switches. VTP comunica automáticamente los cambios a todos los demás switches del dominio VTP (red). Puede configurar un switch para que esté en un solo dominio VTP. Antes de crear VLAN, determine el modo VTP que se utilizará en la red.

Información Operativa General

VTP es un protocolo de mensajería de Capa 2. VTP administra la adición, eliminación y cambio de nombre de VLAN en toda la red para mantener la consistencia de la configuración de VLAN. VTP minimiza los errores de configuración y las inconsistencias de configuración que pueden dar lugar a varios problemas. Los problemas incluyen nombres de VLAN duplicados, especificaciones de tipo VLAN incorrectas y violaciones de seguridad.

De forma predeterminada, el switch está en modo de servidor VTP y está en estado de dominio sin administración. Estos parámetros predeterminados cambian cuando el switch recibe un anuncio de un dominio sobre un link troncal o cuando se configura un dominio de administración.

El protocolo VTP se comunica entre los switches mediante el uso de un conocido tipo de protocolo SNAP HDLC 0x2003 de multidifusión de destino Ethernet (01-00-0c-cc-cc-cc) y multidifusión de destino SNAP. Al igual que otros protocolos intrínsecos, VTP también utiliza una encapsulación SNAP IEEE 802.3, que incluye LLC 0xAAAA03 y OUI 0x0000C. Puede ver esto en un seguimiento del analizador de LAN. VTP no funciona sobre los puertos no troncales. Por lo tanto, los mensajes no se pueden enviar hasta que DTP haya activado el tronco. En otras palabras, VTP es una carga útil de ISL o 802.1Q.

Los tipos de mensajes incluyen:

- Anuncios de resumen cada 300 segundos (s)
- Subconjunto de anuncios y solicitud de anuncios cuando haya cambios

- Se une cuando el recorte VTP está activado

El número de revisión de la configuración VTP se incrementa en uno con cada cambio en un servidor, y esa tabla se propaga a través del dominio.

Al eliminar una VLAN, los puertos que alguna vez fueron miembros de la VLAN ingresan un estado `inactivo`. De manera similar, si un switch en modo cliente no puede recibir la tabla de VLAN VTP en el inicio, ya sea desde un servidor VTP o desde otro cliente VTP, todos los puertos en VLAN que no sean la VLAN 1 predeterminada se desactivan.

Puede configurar la mayoría de los switches Catalyst para que funcionen en cualquiera de estos modos VTP:

- Servidor: en el modo de servidor VTP, puede:Crear VLANModificar VLANEliminación de VLANEspecifique otros parámetros de configuración, como la versión VTP y el recorte VTP, para todo el dominio VTPLos servidores VTP anuncian su configuración de VLAN a otros switches en el mismo dominio VTP. Los servidores VTP también sincronizan su configuración de VLAN con otros switches en base a los anuncios que se reciben a través de links troncales. El servidor VTP es el modo predeterminado.
- Cliente: los clientes VTP se comportan de la misma manera que los servidores VTP. Pero no puede crear, cambiar ni eliminar VLAN en un cliente VTP. Además, el cliente no recuerda la VLAN después de un reinicio porque no se escribe información de VLAN en la NVRAM.
- Transparente: los switches VTP transparente no participan en VTP. Un switch transparente VTP no anuncia su configuración de VLAN y no sincroniza su configuración de VLAN en base a los anuncios recibidos. Sin embargo, en la versión 2 de VTP, los switches transparentes reenvían anuncios VTP que los switches reciben sus interfaces troncales.

Función	Servidor	Cliente	Transparente	Off [1]
Mensajes VTP de la Fuente	Yes	Yes	No	—
Escuchar mensajes VTP	Yes	Yes	No	—
Crear VLAN	Yes	No	Sí (solo de importancia local)	—
Recordar VLAN	Yes	No	Sí (solo de importancia local)	—

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

Esta tabla es un resumen de la configuración inicial:

Función	Valor Predeterminado
Nombre de Dominio de VTP	Nulo
Modo VTP	Servidor
VTP Version	Se habilita la versión 1
Recorte VTP	Inhabilitado

En el modo transparente VTP, las actualizaciones VTP simplemente se ignoran. La conocida dirección MAC de multidifusión VTP se elimina del CAM del sistema que se utiliza normalmente para capturar tramas de control y dirigirlas al Supervisor Engine. Debido a que el protocolo utiliza una dirección multicast, el switch en modo transparente u otro switch proveedor simplemente inunda la trama a otros switches de Cisco en el dominio.

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

- Soporte Token Ring
- Compatibilidad con información VTP no reconocida: los switches ahora propagan valores que no pueden analizar.
- Modo transparente dependiente 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 VTPv2 es posible en todos los switches, todos los switches se pueden habilitar con la configuración de un único switch.

Para obtener más información, consulte Introducción al protocolo de enlace troncal de VLAN (VTP).

Funcionamiento de VTP en Cisco IOS Software

En CatOS, los cambios de configuración se escriben en la memoria RAM no volátil (NVRAM) inmediatamente después de que se realiza un cambio. Por el contrario, Cisco IOS Software no guarda los cambios de configuración en NVRAM a menos que ejecute el comando **copy run start**. Los sistemas de servidores y clientes VTP requieren que las actualizaciones de VTP de otros servidores VTP se guarden inmediatamente en la NVRAM, sin intervención del usuario. Los requisitos de actualización de VTP se cumplen por la operación predeterminada de CatOS, pero el modelo de actualización de Cisco IOS Software requiere una operación de actualización alternativa.

Para esta modificación, se introdujo una base de datos de VLAN en el Cisco IOS Software para el Catalyst 6500 como método para guardar inmediatamente las actualizaciones de VTP para los clientes y servidores VTP. En algunas versiones de software, esta base de datos de VLAN se presenta como un archivo independiente en la NVRAM, denominado archivo vlan.dat. Verifique su versión de software para determinar si se requiere una copia de seguridad de la base de datos de VLAN. Se puede ver la información de VTP/VLAN almacenada en el archivo vlan.dat para el cliente VTP o el servidor VTP si se emite el comando show vtp status.

La configuración VTP/VLAN completa no se guarda en el archivo de configuración de inicio en NVRAM cuando se ejecuta el comando **copy run start** en estos sistemas. Esto no se aplica a los sistemas que se ejecutan como VTP transparente. Los sistemas transparentes VTP guardan la configuración VTP/VLAN completa en el archivo de configuración de inicio en NVRAM cuando ejecuta el comando **copy run start**.

En las versiones del software Cisco IOS anteriores a la versión 12.1(11b)E del software Cisco IOS, sólo puede configurar VTP y VLAN a través del modo de base de datos VLAN. El modo de base de datos de VLAN es un modo independiente del modo de configuración global. El motivo de este requisito de configuración es que, cuando configura el dispositivo en el servidor de modo VTP o en el cliente de modo VTP, los vecinos VTP pueden actualizar la base de datos VLAN dinámicamente a través de los anuncios VTP. No desea que estas actualizaciones se propaguen

automáticamente a la configuración. Por lo tanto, la base de datos de VLAN y la información de VTP no se almacenan en la configuración principal, sino en la NVRAM en un archivo con el nombre vlan.dat.

Este ejemplo muestra cómo crear una VLAN Ethernet en el modo de base de datos VLAN:

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

En Cisco IOS Software Release 12.1(11b)E y posteriores, puede configurar VTP y VLAN a través del modo de base de datos VLAN o a través del modo de configuración global. En el modo VTP server o VTP mode transparent, la configuración de las VLAN aún actualiza el archivo vlan.dat en la NVRAM. Sin embargo, estos comandos no se guardan en la configuración. Por lo tanto, los comandos no se muestran en la configuración en ejecución.

Consulte la sección *Configuración de VLAN en el Modo de Configuración Global del documento* Configuración de VLAN para obtener más información.

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

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

Nota: La configuración de VLAN se almacena en el archivo vlan.dat, que se almacena en la memoria no volátil. Para realizar una copia de seguridad completa de su configuración, incluya el archivo vlan.dat en la copia de seguridad junto con la configuración. A continuación, si el switch completo o el módulo Supervisor Engine requieren reemplazo, el administrador de red debe cargar ambos archivos para restaurar la configuración completa:

- El archivo vlan.dat
- El archivo de configuración

VTP y VLAN extendidas

La función Extended System ID se utiliza para habilitar la identificación de VLAN de rango extendido. Cuando se habilita el ID de sistema extendido, inhabilita el conjunto de direcciones MAC utilizado para el árbol de expansión de VLAN y deja una única dirección MAC que identifica

el switch. Las versiones 12.1(11b)EX y 12.1(13)E del software Catalyst IOS introducen el soporte de ID de sistema extendido para Catalyst 6000/6500 para soportar las VLAN 4096 de conformidad con el estándar IEEE 802.1Q. Esta función se introduce en Cisco IOS Software Release12.1(12c)EW para los switches Catalyst 4000/4500. Estas VLAN se organizan en varios rangos, cada uno de los cuales se puede utilizar de forma diferente. Algunas de estas VLAN se propagan a otros switches en la red cuando utiliza el VTP. Las VLAN de rango extendido no se propagan, por lo que debe configurar las VLAN de rango extendido manualmente en cada dispositivo de red. Esta función Extended System ID es equivalente a la función de reducción de direcciones MAC en Catalyst OS.

Esta tabla describe los rangos de VLAN:

VLAN	Rango	Uso	¿Propagados por VTP?
0, 4095	Reservado	Sólo para uso del sistema. No puede ver ni utilizar estas VLAN.	—
1	Normal	Cisco predeterminado. Puede utilizar esta VLAN, pero no puede eliminarla.	Yes
2–1001	Normal	Para VLAN Ethernet. Puede crear, utilizar y eliminar estas VLAN.	Yes
1002–1005	Normal	Los valores predeterminados de Cisco para FDDI y Token Ring. No puede eliminar las VLAN 1002-1005.	Yes
1006–4094	Reservado	Sólo para VLAN Ethernet.	No

Los protocolos de switch utilizan una dirección MAC tomada de un banco de direcciones disponibles que proporciona un EPROM en el chasis como parte de los identificadores de puente para las VLAN que se ejecutan bajo PVST+ y RPVST+. Los switches Catalyst 6000/6500 y Catalyst 4000/4500 admiten direcciones MAC 1024 o 64 que dependen del tipo de chasis.

Los switches Catalyst con direcciones MAC 1024 no habilitan el ID de sistema extendido de forma predeterminada. Las direcciones MAC se asignan secuencialmente, con la primera dirección MAC en el rango asignada a VLAN 1, la segunda dirección MAC en el rango asignado a VLAN 2, etc. Esto permite que los switches soporten 1024 VLAN y cada VLAN utiliza un identificador de puente único.

Tipo de Chasis	Dirección de chasis
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	641
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	641

[1] El chasis con 64 direcciones MAC habilita el ID de sistema extendido de forma predeterminada y la función no se puede inhabilitar.

Refiérase a la sección *Comprensión del ID de puente* de Configuración de STP e IEEE 802.1s MST para obtener más información.

Para los switches de la serie Catalyst con direcciones MAC 1024, habilitar la ID de sistema extendido permite el soporte de 4096 VLAN que se ejecutan en PVST+ o 16 instancias MISTP para tener identificadores únicos sin el aumento del número de direcciones MAC que se requieren en el switch. Extended System ID reduce el número de direcciones MAC que requiere el STP de una por cada instancia de VLAN o MISTP a una por switch.

Esta figura muestra el identificador de puente cuando el ID de sistema extendido no está habilitado. El identificador de bridge consiste en una prioridad de bridge de 2 bytes y una dirección MAC de 6 bytes.

El ID de sistema extendido modifica la parte del identificador de puente del protocolo de árbol de extensión (STP) de las unidades de datos del protocolo de puente (BPDU). El campo de prioridad original de 2 bytes se divide en 2 campos; Un campo de prioridad de puente de 4 bits y una extensión de ID de sistema de 12 bits que permite la numeración de VLAN de 0-4095.

Cuando se habilita el ID de sistema extendido en los switches Catalyst para aprovechar VLAN de rango extendido, debe habilitarse en todos los switches dentro del mismo dominio STP. Esto es necesario para mantener los cálculos de raíz STP en todos los switches consistentes. Una vez que se habilita el ID de sistema extendido, la prioridad de puente raíz se convierte en un múltiplo de 4096 más el ID de VLAN. Los switches sin ID de sistema extendido pueden reclamar root inadvertidamente ya que tienen una granularidad más fina en la selección de su ID de puente.

Aunque se recomienda mantener una configuración uniforme de ID de sistema extendido dentro del mismo dominio STP, no es práctico aplicar ID de sistema extendido en todos los dispositivos de red cuando se introduce un nuevo chasis con 64 direcciones MAC en el dominio STP. Sin embargo, es importante comprender cuándo se configuran dos sistemas con la misma prioridad de árbol de expansión, el sistema sin ID de sistema extendido tiene una mejor prioridad de árbol de expansión. Ejecute este comando para habilitar la configuración de ID de sistema extendido:

spanning-tree extend system-id

Las VLAN internas se asignan en orden ascendente, a partir de VLAN 1006. Se recomienda asignar las VLAN de usuario lo más cerca posible de VLAN 4094 para evitar conflictos entre las VLAN de usuario y las VLAN internas. Ejecute el comando **show vlan internal usage** en un switch

para visualizar las VLAN asignadas internamente.

```
Switch#show vlan internal usage

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

En el IOS nativo, la **política de asignación interna de vlan descendente** se puede configurar para que las VLAN internas se asignen en orden descendente. El equivalente CLI para el software CatOS no se soporta oficialmente.

política de asignación interna de VLAN descendente

Recomendación de configuración de Cisco

Las VLAN se pueden crear cuando un Catalyst 6500/6000 está en modo de servidor VTP, incluso sin nombre de dominio VTP. Configure primero el nombre de dominio VTP antes de configurar las VLAN en los switches Catalyst 6500/6000 que ejecutan el software del sistema Cisco IOS. La configuración en este orden mantiene la consistencia con otros switches Catalyst que ejecutan CatOS.

No hay una recomendación específica acerca de si se debe utilizar los modos cliente/servidor de VTP o el modo transparente de VTP. Algunos clientes prefieren la facilidad de administración del modo cliente/servidor VTP, a pesar de algunas consideraciones que se señalan en esta sección. Se recomienda tener dos switches en modo de servidor en cada dominio para redundancia, normalmente los dos switches de capa de distribución. Establezca el resto de los switches en el dominio en el modo cliente. Cuando implementa el modo cliente/servidor con el uso de VTPv2, recuerde que siempre se acepta un número de revisión mayor en el mismo dominio VTP. Si un switch que se configura en el modo de cliente o servidor VTP se introduce en el dominio VTP y tiene un número de revisión mayor que los servidores VTP existentes, esto sobrescribe la base de datos VLAN dentro del dominio VTP. Si el cambio de configuración es involuntario y se eliminan las VLAN, esta sobreescritura puede causar una interrupción importante en la red. Para asegurarse de que los switches cliente o servidor siempre tengan un número de revisión de la configuración que sea inferior al del servidor, cambie el nombre de dominio VTP del cliente a otro nombre que no sea el nombre estándar y, a continuación, vuelva al estándar. Esta acción configura la revisión de la configuración en el cliente en 0.

La capacidad de VTP de realizar los cambios fácilmente en una red tiene ventajas y desventajas. Muchas empresas prefieren un enfoque prudente y utilizan el modo `transparente` VTP por estas razones:

- Esta práctica fomenta un buen control de cambios porque el requisito de modificar una VLAN en un switch o puerto trunk debe considerarse un switch a la vez.
- El modo transparente VTP limita el riesgo de un error del administrador, como la eliminación accidental de una VLAN. Estos errores pueden afectar a todo el dominio.
- Las VLAN se pueden recortar de los troncales a los switches que no tienen puertos en la VLAN. Esto hace que la inundación de tramas sea más eficiente en términos de ancho de banda. La poda manual también tiene un diámetro reducido del árbol de expansión. Vea la sección Dynamic Trunking Protocol para obtener más información. Una configuración de VLAN por switch también fomenta esta práctica.
- No hay riesgo de la introducción en la red de un nuevo switch con un número de revisión de VTP más alto que sobrescriba toda la configuración de VLAN de dominio.
- El modo transparente VTP del software Cisco IOS se soporta en Campus Manager 3.2, que es parte de CiscoWorks2000. Se ha eliminado la restricción anterior que requiere que tenga al menos un servidor en un dominio VTP.

Comandos VTP	**Comentarios**
nombre de dominio de vtp	CDP verifica el nombre para ayudar a evitar el cableado entre los dominios. Los nombres de dominio distinguen entre mayúsculas y minúsculas.
vtp mode {server | cliente | transparent}	VTP funciona en uno de los tres modos.
vlan *vlan_number*	Esto crea una VLAN con el ID proporcionado.
switchport trunk allowed *vlan_range*	Este es un comando de interfaz que permite a los troncales transportar VLAN donde sea necesario. El valor predeterminado son todas las VLAN.
switchport trunk pruning *vlan_r*	Este es un comando de interfaz que limita el diámetro STP mediante el recorte manual, como en los troncales de la capa de distribución a la capa de acceso, donde la VLAN no existe. De forma predeterminada, todas las VLAN son elegibles para podar.

ange	

Otras Opciones

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

La sección Recomendación de configuración de Cisco de este documento aboga por las ventajas de recortar las VLAN para reducir la inundación innecesaria de tramas. El comando **vtp pruning** borra las VLAN automáticamente, lo que detiene la inundación ineficiente de tramas donde no se necesitan.

Nota: A diferencia del recorte manual de VLAN, el recorte automático no limita el diámetro del árbol de expansión.

El IEEE ha producido una arquitectura basada en estándares para lograr resultados VTP similares. Como miembro del protocolo de registro de atributos genéricos (GARP) 802.1Q, el protocolo de registro de VLAN genérico (GVRP) permite la interoperabilidad de la gestión de VLAN entre proveedores. Sin embargo, GVRP está fuera del alcance de este documento.

Nota: El software Cisco IOS no tiene capacidad de modo apagado VTP y sólo admite VTPv1 y VTPv2 con recorte.

Negociación automática Fast Ethernet

Propósito

La negociación automática es una función opcional del estándar IEEE 802.3u Fast Ethernet (FE). La negociación automática permite a los dispositivos intercambiar automáticamente información sobre las capacidades dúplex y de velocidad a través de un enlace. La negociación automática funciona en la capa 1 (L1). La función está dirigida a los puertos que están asignados a áreas donde los usuarios o dispositivos transitorios se conectan a una red. Entre los ejemplos se incluyen los hubs y switches de capa de acceso.

Información Operativa General

La negociación automática utiliza una versión modificada de la prueba de integridad del link para los dispositivos 10BASE-T para negociar la velocidad e intercambiar otros parámetros de negociación automática. La prueba de integridad del link 10BASE-T original se conoce como impulso de link normal (NLP). La versión modificada de la prueba de integridad del enlace para la negociación automática de 10/100 Mbps se denomina Fast Link Pulse (FLP). Los dispositivos 10BASE-T esperan un pulso de ráfaga cada 16 (+/-8) milisegundos (ms) como parte de la prueba de integridad del link. FLP para negociación automática de 10/100 Mbps envía estas ráfagas cada 16 (+/-8) ms con los pulsos adicionales cada 62,5 (+/-7) microsegundos. Los pulsos dentro de la secuencia de ráfagas generan palabras de código que se utilizan para los intercambios de compatibilidad entre socios de link.

En 10BASE-T, se envía un pulso de link cada vez que aparece una estación. Este es un pulso único que se envía cada 16 ms. Los dispositivos 10BASE-T también envían un pulso de link cada 16 ms cuando el link está inactivo. Estos pulsos de link también se denominan latidos o NLP.

Un dispositivo 100BASE-T envía FLP. Este pulso se envía como una ráfaga en lugar de un pulso. La ráfaga se completa en 2 ms y se repite cada 16 ms. Tras la inicialización, el dispositivo transmite un mensaje FLP de 16 bits al socio de link para la negociación de velocidad, dúplex y control de flujo. Este mensaje de 16 bits se envía repetidamente hasta que el partner reconoce el mensaje.

Nota: Según la especificación IEEE 802.3u, no puede configurar manualmente un socio de link para dúplex completo de 100 Mbps y aún así negociar automáticamente al dúplex completo con el otro socio de link. Un intento de configurar un socio de link para dúplex completo de 100-Mbps y el otro socio de link para negociación automática da como resultado una discordancia dúplex. La discordancia dúplex resulta porque un partner de link negocia automáticamente y no ve ningún parámetro de negociación automática del otro socio de link. A continuación, el primer partner de link adopta de forma predeterminada el semidúplex.

Todos los módulos de switching Ethernet Catalyst 6500 admiten 10/100 Mbps y dúplex medio o dúplex completo. Ejecute el comando **show interface capabilities** para verificar esta funcionalidad en otros switches Catalyst.

Una de las causas más comunes de los problemas de rendimiento en los links Ethernet de 10/100 Mbps ocurre cuando un puerto en el link funciona en semidúplex mientras que el otro puerto funciona en dúplex completo. Esta situación ocurre ocasionalmente cuando se reinicia uno o ambos puertos en un link y el proceso de negociación automática no da como resultado la misma configuración para ambos socios de link. La situación también ocurre cuando se vuelve a configurar un lado de un link y se olvida de reconfigurar el otro lado. Puede evitar la necesidad de realizar llamadas de asistencia relacionadas con el rendimiento si:

- Cree una política que requiera la configuración de puertos para el comportamiento necesario para todos los dispositivos no transitorios
- Aplicar la política con medidas adecuadas de control de cambios

Los síntomas típicos del problema de rendimiento aumentan la secuencia de verificación de tramas (FCS), la comprobación de redundancia cíclica (CRC), la alineación o los contadores de fragmentos en el switch.

En el modo semidúplex, tiene un par de cables de recepción y un par de cables de transmisión. Ambos cables no se pueden utilizar al mismo tiempo. El dispositivo no puede transmitir cuando hay un paquete en el lado de recepción.

En el modo dúplex completo, tiene el mismo par de cables de recepción y transmisión. Sin embargo, ambos se pueden utilizar al mismo tiempo porque las funciones Detección de colisión y Sentido de la portadora se han inhabilitado. El dispositivo puede transmitir y recibir al mismo tiempo.

Por lo tanto, funciona una conexión semidúplex a dúplex completo, pero hay un gran número de colisiones en el lado semidúplex que resultan en un rendimiento deficiente. Las colisiones ocurren porque el dispositivo configurado como dúplex completo puede transmitir al mismo tiempo que el dispositivo recibe datos.

En los documentos de esta lista se analiza detalladamente la negociación automática. Estos documentos explican cómo funciona la negociación automática y analizan diversas opciones de configuración:

- Configuración y resolución de problemas de negociación automática de half/full duplex para

Ethernet 10/100/1000 Mb
- Troubleshooting de Problemas de Compatibilidad entre Cisco Catalyst Switches y NIC

Un concepto erróneo común sobre la negociación automática es que es posible configurar manualmente un socio de link para 100-Mbps dúplex completo y negociar automáticamente con el otro socio de link para dúplex completo. De hecho, si se intenta hacer esto, se obtienen modos dúplex desiguales. Esto es una consecuencia porque un partner de link negocia automáticamente, no ve ningún parámetro de negociación automática del otro socio de link y de forma predeterminada es semidúplex.

La mayoría de los módulos Ethernet Catalyst admiten 10/100 Mbps y dúplex medio/completo. Sin embargo, puede confirmar esto si ejecuta el comando **show interface *mod/port* capabilities**.

FEFI

La indicación de fallos de extremo lejano (FEFI) protege las interfaces 100BASE-FX (fibra) y Gigabit, mientras que la negociación automática protege 100BASE-TX (cobre) frente a fallos físicos relacionados con la capa/señalización.

Un error de extremo lejano es un error en el link que una estación puede detectar mientras que la otra estación no puede. Un cable de transmisión desconectado es un ejemplo. En este ejemplo, la estación de envío todavía recibe datos válidos y detecta que el link es bueno a través del monitor de integridad del link. Sin embargo, la estación de envío no puede detectar que la otra estación no recibe la transmisión. Una estación 100BASE-FX que detecta un error remoto puede modificar su flujo `IDLE` transmitido para enviar un patrón de bit especial para informar al vecino de la falla remota. El patrón de bits especial se conoce como el patrón `FEFI-IDLE`. el patrón FEFI-IDLE apaga posteriormente el puerto remoto (errdisable). Consulte la sección Detección de Link Unidireccional de este documento para obtener más información sobre la protección contra fallas.

Estos módulos/hardware admiten FEFI:

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

Recomendación de puerto de infraestructura de Cisco

La configuración de la negociación automática en links de 10/100 Mbps o de la velocidad del código duro y dúplex depende en última instancia del tipo de socio de link o dispositivo final que se ha conectado a un puerto de switch Catalyst. La negociación automática entre los dispositivos extremos y los switches Catalyst generalmente funciona sin inconvenientes, y los switches Catalyst cumplen con la especificación IEEE 802.3u. Sin embargo, cuando las tarjetas de interfaz de red (NIC) o los switches del proveedor no cumplen exactamente, pueden producirse problemas. Además, las funciones avanzadas específicas del proveedor que no se describen en la especificación IEEE 802.3u para la negociación automática de 10/100 Mbps pueden causar incompatibilidad de hardware y otros problemas. Estos tipos de funciones avanzadas incluyen la autopolaridad y la integridad del cableado. Este documento proporciona un ejemplo:

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

En algunas situaciones, debe establecer host, velocidad de puerto y dúplex. En general, complete estos pasos básicos de solución de problemas:

- Asegúrese de que la negociación automática está configurada en ambos lados del link o que la codificación dura está configurada en ambos lados.

- Verifique las notas de la versión para ver las advertencias comunes.
- Verifique la versión del controlador NIC o el sistema operativo que ejecuta. A menudo se necesita el último driver o parche.

Como regla general, primero utilice la negociación automática para cualquier tipo de partner de link. La configuración de la negociación automática de dispositivos transitorios, como los portátiles, aporta ventajas evidentes. La negociación automática también funciona bien con otros dispositivos, por ejemplo:

- Con dispositivos no transitorios como servidores y estaciones de trabajo fijas
- De switch a switch
- De switch a router

Pero, por algunas de las razones que se mencionan en esta sección, pueden surgir problemas de negociación. Refiérase a Configuración y Troubleshooting de Negociación Automática de Semidúplex/Dúplex Completo de Ethernet 10/100/1000Mb para ver los pasos básicos de troubleshooting en estos casos.

Desactivar negociación automática para:

- Puertos compatibles con dispositivos de infraestructura de red, como switches y routers
- Otros sistemas finales no transitorios, como servidores e impresoras

Siempre configure los parámetros de velocidad y dúplex para estos puertos.

Configure manualmente estas configuraciones de link de 10/100 Mbps para velocidad y dúplex, que normalmente son dúplex completo de 100 Mbps:

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

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

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

Ejecute estos comandos de interfaz para configurar la velocidad y el dúplex:

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

Recomendaciones de los puertos de acceso de Cisco

Los usuarios finales, los trabajadores móviles y los hosts transitorios necesitan negociación automática para minimizar la administración de estos hosts. También puede hacer que la negociación automática funcione con los switches Catalyst. A menudo se necesitan los controladores NIC más recientes.

Ejecute estos comandos globales para habilitar la negociación automática de velocidad para el

puerto:

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

Nota: Si configura la velocidad del puerto en auto en un puerto Ethernet de 10/100 Mbps, tanto la velocidad como el dúplex se negocian automáticamente. No puede cambiar el modo dúplex de los puertos de negociación automática.

Cuando las NIC o los switches de proveedor no cumplen exactamente con la especificación IEEE 802.3u, pueden producirse problemas. Además, las funciones avanzadas específicas del proveedor que no se describen en la especificación IEEE 802.3u para la negociación automática de 10/100 Mbps pueden causar incompatibilidad de hardware y otros problemas. Estas características avanzadas incluyen la autopolaridad y la integridad del cableado.

Otras Opciones

Cuando se inhabilita la negociación automática entre los switches, la indicación de falla de la Capa 1 también puede perderse para ciertos problemas. Utilice los protocolos de Capa 2 para aumentar la detección de fallas, como UDLD agresivo.

La negociación automática no detecta estas situaciones, incluso cuando la negociación automática está habilitada:

- Los puertos se atascan y no reciben ni transmiten
- Un lado de la línea está arriba pero el otro lado ha caído
- Los cables de fibra están mal cableados

La negociación automática no detecta estos problemas porque no se encuentran en la capa física. Los problemas pueden conducir a loops STP o agujeros negros de tráfico.

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

Negociación automática de Gigabit Ethernet

Propósito

Gigabit Ethernet (GE) tiene un procedimiento de negociación automática más extenso que el que se utiliza para Ethernet de 10/100 Mbps (IEEE 802.3z). Con los puertos GE, la negociación automática se utiliza para intercambiar:

- Parámetros de control de flujo
- Información de falla remota
- Información dúplex**Nota:** Los puertos GE de la serie Catalyst sólo admiten el modo dúplex completo.

IEEE 802.3z ha sido sustituido por las especificaciones IEEE 802.3:2000. Consulte la Suscripción de Estándares Redes de Área Local y Metropolitana + Borradores (LAN/MAN 802) para obtener más información.

Información Operativa General

A diferencia de la negociación automática con FE de 10/100 Mbps, la negociación automática GE no implica la negociación de la velocidad del puerto. Además, no puede ejecutar el comando **set port speed** para inhabilitar la negociación automática. La negociación de puerto GE se habilita de forma predeterminada, y los puertos en ambos extremos de un link GE deben tener la misma configuración. El link no aparece si los puertos en cada extremo del link están configurados de manera inconsistente, lo que significa que los parámetros intercambiados son diferentes.

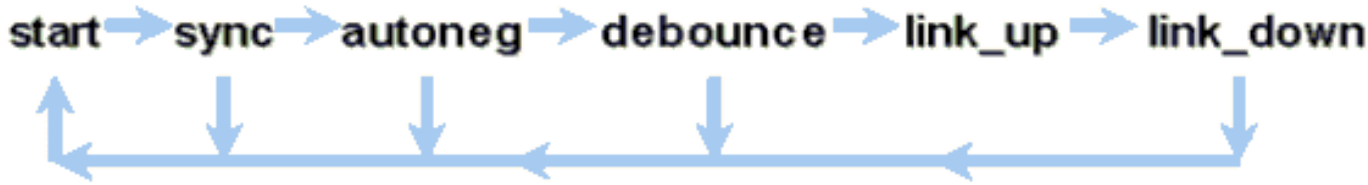
Por ejemplo, suponga que hay dos dispositivos, A y B. Cada dispositivo puede tener la función de negociación automática habilitada o inhabilitada. Esta es una tabla que tiene configuraciones posibles y sus respectivos estados de link:

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

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

Nota: Hay un diccionario de 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 afirma una condición de falla de sincronización y el link se cambia 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 la negociación automática se inhabilita en un puerto, la fase de autenticación ya no es una opción.

La especificación 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: Sin embargo, la especificación de fibra GE sólo contiene 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 **sync-restart-delay** sólo tiene un efecto cuando la negociación automática está configurada en enable.

Recomendación de puerto de infraestructura de Cisco

La configuración de la negociación automática es mucho más importante en un entorno GE que en un entorno de 10/100 Mbps. Sólo inhabilite la negociación automática en estas situaciones:

- En los puertos del switch que se conectan a dispositivos que no son capaces de soportar la negociación
- Cuando surgen problemas de conectividad debido a problemas de interoperabilidad

Habilite la negociación Gigabit en todos los links de switch a switch y, en general, en todos los dispositivos GE. El valor predeterminado en las interfaces Gigabit es la negociación automática. Aún así, ejecute este comando para asegurarse de que la negociación automática esté habilitada:

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

Una excepción conocida es cuando se conecta a un router de switch Gigabit (GSR) que ejecuta el software Cisco IOS anterior a la versión 12.0(10)S del software Cisco IOS, la versión que agregó control de flujo y negociación automática. En este caso, desactive esas dos funciones. Si no apaga esas funciones, el puerto del switch informa que no está conectado y el GSR informa errores. Ésta es una secuencia de comandos de interfaz de ejemplo:

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

Recomendaciones de los puertos de acceso de Cisco

Dado que los FLP pueden variar entre proveedores, debe analizar las conexiones de switch a servidor caso por caso. Los clientes de Cisco han encontrado algunos problemas con la negociación Gigabit en servidores Sun, HP e IBM. Que todos los dispositivos utilicen la negociación automática Gigabit a menos que el proveedor de NIC indique específicamente lo contrario.

Otras Opciones

El control de flujo es una parte opcional de la especificación 802.3x. El control de flujo debe negociarse si se utiliza. Los dispositivos pueden o no pueden enviar y/o responder a una trama PAUSE (MAC 01-80-C2-00-00-00 0F conocido). Y posiblemente los dispositivos no puedan aceptar la solicitud de control de flujo del vecino de extremo lejano. Un puerto con un búfer de

entrada que comienza a llenarse envía una trama PAUSE al socio de link. El partner de link detiene la transmisión y mantiene cualquier trama adicional en las memorias intermedias de salida del partner de link. Esta función no resuelve ningún problema de sobresuscripción en estado estacionario. Sin embargo, la función hace que el búfer de entrada sea más grande por una fracción del búfer de salida del partner a lo largo de las ráfagas.

La función PAUSE está diseñada para evitar el descarte innecesario de tramas recibidas por los dispositivos (switches, routers o estaciones finales) debido a las condiciones de desbordamiento de búfer que causa la sobrecarga de tráfico transitorio a corto plazo. Un dispositivo bajo sobrecarga de tráfico previene el desbordamiento de búfer interno cuando el dispositivo envía una trama PAUSE. La trama PAUSE contiene un parámetro que indica el tiempo que el partner dúplex completo debe esperar antes de que el partner envíe más tramas de datos. El partner que recibe la trama PAUSE deja de enviar datos durante el período especificado. Cuando este temporizador caduca, la estación comienza a enviar tramas de datos de nuevo, desde donde la estación dejó de funcionar.

Una estación que emite una PAUSE puede emitir otra trama PAUSE que contiene un parámetro de tiempo cero. Esta acción cancela el resto del período de pausa. Por lo tanto, una trama PAUSE recién recibida invalida cualquier operación PAUSE que esté actualmente en curso. Además, la estación que emite la trama PAUSE puede extender el período PAUSE. La estación emite otra trama PAUSE que contiene un parámetro de tiempo distinto de cero antes del vencimiento del primer período PAUSE.

Esta operación PAUSE no es un control de flujo basado en velocidad. La operación es un simple mecanismo de inicio-parada que permite al dispositivo bajo el tráfico, el que envió la trama PAUSE, una posibilidad de reducir su congestión del búfer.

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

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

```
flowcontrol {receive | send} {off | on | desired}
```

```
>show port flowcontrol

 Port  Send FlowControl    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 6/1   off      off        on       on           0       0
 6/2   off      off        on       on           0       0
 6/3   off      off        on       on           0       0
```

Nota: Todos los módulos Catalyst responden a una trama PAUSE si se negocia. Algunos módulos (por ejemplo, WS-X5410 y WS-X4306) nunca envían tramas de pausa, incluso si negocian para hacerlo, porque no tienen bloqueo.

Dynamic Trunking Protocol

Propósito

Para ampliar las VLAN entre los dispositivos, los troncales identifican y marcan temporalmente (link local) las tramas Ethernet originales. Esta acción permite que las tramas se multiplexen en un único link. La acción también asegura que los dominios de seguridad y broadcast VLAN separados se mantengan entre los switches. Las tablas CAM mantienen la trama a la asignación de VLAN dentro de los switches.

Información Operativa General

DTP es la segunda generación de ISL dinámico (DISL). DISL sólo admite ISL. DTP admite ISL y 802.1Q. Este soporte asegura que los switches en cualquiera de los extremos de un tronco coincidan en los diferentes parámetros de las tramas troncales. Estos parámetros incluyen:

- Tipo de encapsulación configurado
- VLAN nativa
- Capacidad de hardware

El soporte de DTP también ayuda a proteger frente a la inundación de tramas etiquetadas por los puertos no troncales, lo que supone un riesgo de seguridad potencialmente grave. DTP protege contra tales inundaciones porque asegura que los puertos y sus vecinos estén en estados consistentes.

Modo Trunking

DTP es un protocolo de Capa 2 que negocia los parámetros de configuración entre un puerto del switch y su vecino. DTP utiliza otra dirección MAC multicast conocida de 01-00-0c-cc-cc-cc y un tipo de protocolo SNAP de 0x2004. Esta tabla describe la función en cada uno de los posibles modos de negociación DTP:

Modo	Función	Tramas DTP Transmitidas ?	Etapa Final (Puerto Local)
`Auto dinámico` (equivalente al modo `Auto` en CatOS)	Hace que el puerto sea capaz de convertir el link en un trunk. El puerto se convierte en un puerto troncal si el puerto vecino está configurado en modo encendido o deseable.	Sí, periódicamente	`Trunking`
`Troncal` (equivalente al modo `ON` en CatOS)	Pone el puerto en modo trunking permanente y negocia para convertir el link en un trunk. El puerto se convierte en puerto trunk aunque el puerto de vecindad no acepte el cambio.	Sí, periódicamente	`Trunking, sin condiciones`
`Nonego`			`Trunking`

tiate	Pone el puerto en modo trunking permanente pero no permite que el puerto genere tramas DTP. Debe configurar manualmente el puerto vecino como puerto troncal para establecer un link troncal. Esto es útil para dispositivos que no soportan DTP.	No	, sin condiciones
Valor deseable dinámico (el comando comparable de CatOS es 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.
Acceso	Pone el puerto en modo permanente no troncal y negocia para convertir el link en un link no troncal. El puerto se convierte en un puerto no troncal incluso si el puerto vecino no acepta el cambio.	No, en estado estable, pero transmite informes para acelerar la detección de extremo remoto después de un cambio desde el encendido.	Sin conexión troncal

Nota: El tipo de encapsulación ISL y 802.1Q se puede establecer o negociar.

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

- Las conexiones punto a punto y los dispositivos de Cisco admiten puertos troncales 802.1Q que solo son punto a punto.
- A lo largo de la negociación DTP, los puertos no participan en STP. El puerto se agrega al STP solamente después de que el tipo de puerto se convierta en uno de estos tres tipos:AccesoISL802.1QPAgP es el siguiente proceso a ejecutar antes de que el puerto participe en STP. PAgP se utiliza para la negociación automática de EtherChannel.
- La VLAN 1 siempre está presente en el puerto troncal. Si el puerto se conecta mediante

trunking en el modo ISL, los paquetes DTP se envían en la VLAN 1. Si el puerto no se conecta mediante trunking en el modo ISL, los paquetes DTP se envían en la VLAN nativa (para los puertos troncales 802.1Q o no troncales).

- Los paquetes DTP transfieren el nombre de dominio VTP, además de la configuración del tronco y el estado de administración. El nombre de dominio VTP debe coincidir para que aparezca un tronco negociado. Estos paquetes se envían cada segundo durante la negociación y cada 30 segundos después de la negociación. Si un puerto en el modo `automático` o `deseable` no detecta un paquete DTP en el plazo de 5 minutos (min), el puerto se configura como no troncal.

Precaución: Debe entender que los modos `trunk`, `nonegotiate` y `access` **especifican explícitamente en qué estado termina el puerto.** Una configuración incorrecta puede conducir a un estado peligroso/incoherente en el que un lado se conecta mediante trunking y el otro no se conecta mediante trunking.

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

Tipo de Encapsulación

Descripción General sobre el Funcionamiento de ISL

ISL es un protocolo de enlace troncal propietario de Cisco (esquema de etiquetado de VLAN). ISL lleva muchos años en uso. Por el contrario, 802.1Q es mucho más reciente, pero 802.1Q es el estándar IEEE.

ISL encapsula completamente la trama original en un esquema de etiquetado de dos niveles. De esta manera, ISL es efectivamente un protocolo de tunelización y, como beneficio adicional, transporta tramas que no son Ethernet. ISL agrega un encabezado de 26 bytes y un FCS de 4 bytes a la trama Ethernet estándar. Los puertos configurados para ser troncales esperan y manejan las tramas Ethernet más grandes. ISL admite 1024 VLAN.

Formato de trama: la etiqueta ISL está sombreada

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

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

Descripción General sobre el Funcionamiento de 802.1Q

Aunque el estándar IEEE 802.1Q sólo pertenece a Ethernet, el estándar especifica mucho más que los tipos de encapsulación. 802.1Q incluye, entre otros protocolos de registro de atributos genéricos (GARP), mejoras del árbol de extensión y etiquetado de QoS 802.1p. Consulte Estándares IEEE Online para obtener más información

El formato de trama 802.1Q conserva la SA y DA Ethernet original. Sin embargo, los switches ahora deben esperar recibir tramas baby-gigante, incluso en los puertos de acceso donde los hosts pueden utilizar el etiquetado para expresar la prioridad de usuario 802.1p para la señalización de QoS. La etiqueta es de 4 bytes. Las tramas Ethernet v2 802.1Q son de 1522 bytes, lo que constituye un logro del grupo de trabajo IEEE 802.3ac. Además, 802.1Q admite espacio de numeración para 4096 VLAN.

Todas las tramas de datos que se transmiten y reciben son etiquetadas 802.1Q, excepto aquellas tramas de datos que están en la VLAN nativa. En este caso, hay una etiqueta implícita que se basa 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, estas tramas también se pueden recibir etiquetadas.

Si desea más información, consulte estos documentos:

- Interoperabilidad de VLAN
- Conexión troncal entre los switches de las series Catalyst 4500/4000, 5500/5000 y 6500/6000 que usan encapsulación 802.1Q con el software del sistema CatOS de Cisco

Formato de trama 802.1Q/802.1p

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

Recomendación de configuración de Cisco

Uno de los principales objetivos de diseño de Cisco es esforzarse por lograr la uniformidad en la red cuando sea posible. Todos los productos Catalyst más nuevos admiten 802.1Q y algunos sólo admiten 802.1Q, como los módulos anteriores de las series Catalyst 4500/4000 y Catalyst 6500. Por lo tanto, todas las nuevas implementaciones deben seguir este estándar IEEE 802.1Q y las redes más antiguas deben migrar gradualmente desde ISL.

Ejecute estos comandos de interfaz para habilitar el trunking 802.1Q en un puerto particular:

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

El estándar IEEE permite la interoperabilidad entre proveedores. La interoperabilidad del proveedor es ventajosa en todos los entornos de Cisco, ya que se encuentran disponibles nuevos dispositivos y NIC compatibles con 802.1p. Aunque las implementaciones de ISL y 802.1Q son sólidas, el estándar IEEE en última instancia tiene una mayor exposición de campo y mayor soporte de terceros, lo que incluye soporte para analizadores de red. Además, una consideración menor es que el estándar 802.1Q también tiene una sobrecarga de encapsulación menor que ISL.

Para que esté completa, el etiquetado implícito en las VLAN nativas crea una consideración de seguridad. La transmisión de tramas de una VLAN, VLAN X, a otra VLAN, VLAN Y, sin un router es posible. La transmisión puede producirse sin un router si el puerto de origen (VLAN X) se encuentra en la misma VLAN que la VLAN nativa de un troncal 802.1Q en el mismo switch. La solución alternativa es utilizar una VLAN ficticia para la VLAN nativa del tronco.

Ejecute estos comandos de interfaz para establecer una VLAN como nativa (el valor predeterminado) para el enlace troncal 802.1Q en un puerto determinado:

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

Dado que todos los nuevos hardware admiten 802.1Q, todas las nuevas implementaciones siguen el estándar IEEE 802.1Q y migran gradualmente las redes anteriores desde ISL. Hasta hace poco, muchos módulos Catalyst 4500/4000 no admitían ISL. Por lo tanto, 802.1Q es la única opción para la conexión troncal Ethernet. Consulte la salida del comando **show interface capabilities** , o el comando **show port capabilities** para CatOS. Debido a que la compatibilidad con enlaces troncales requiere el hardware adecuado, un módulo que no admite 802.1Q nunca puede admitir 802.1Q. Una actualización de software no confiere soporte para 802.1Q. La mayoría del hardware nuevo para los switches Catalyst 6500/6000 y Catalyst 4500/4000 es compatible con ISL y 802.1Q.

Si la VLAN 1 se borra de un tronco, como se describe en la sección Interfaz de administración del switch y VLAN nativa, aunque no se transmiten ni reciben datos del usuario, el NMP continúa pasando los protocolos de control en la VLAN 1. Algunos ejemplos de protocolos de control son CDP y VTP.

Además, como se describe en la sección VLAN 1, los paquetes CDP, VTP y PAgP siempre se envían en la VLAN 1 cuando se realiza el trunking. Con el uso de la encapsulación dot1q (802.1Q), estas tramas de control se etiquetan con VLAN 1 si se cambia la VLAN nativa del switch. Si se cambia el trunking dot1q a un router y la VLAN nativa en el switch, se necesita una subinterfaz en VLAN 1 para recibir las tramas CDP etiquetadas y proporcionar la visibilidad de vecino CDP en el router.

Nota: Hay una consideración potencial de seguridad con dot1q que causa el etiquetado implícito de la VLAN nativa. La transmisión de tramas de una VLAN a otra sin un router puede ser posible. Refiérase a las Preguntas Frecuentes sobre la Detección de Intrusiones para obtener más detalles. La solución alternativa es utilizar un ID de VLAN para la VLAN nativa del tronco que no se utiliza para el acceso del usuario final. Para lograrlo, la mayoría de los clientes de Cisco simplemente dejan VLAN 1 como VLAN nativa en un trunk y asignan puertos de acceso a VLAN distintas de VLAN 1.

Cisco recomienda una configuración explícita del modo troncal de `deseable dinámico` en ambos extremos. Este modo es el modo predeterminado. En este modo, los operadores de red pueden confiar en los mensajes de estado syslog y de línea de comandos que un puerto está `activo` y trunking. Este modo es diferente del modo `encendido`, que puede hacer que un puerto aparezca aunque el vecino esté mal configurado. Además, los troncales de modo `deseable` proporcionan estabilidad en situaciones en las que un lado del link no puede convertirse en trunk o deja caer el `estado trunk`.

Si el tipo de encapsulación se negocia entre switches con el uso de DTP, y se elige ISL como ganador de forma predeterminada si ambos extremos lo soportan, debe ejecutar este comando de interfaz para especificar dot1q[1]:

```
switchport trunk encapsulation dot1q
```

[1] Ciertos módulos que incluyen WS-X6548-GE-TX y WS-X6148-GE-TX no admiten enlaces troncales ISL. Estos módulos no aceptan el comando **switchport trunk encapsulation *dot1q*** .

Nota: Ejecute el comando **switchport mode access** para inhabilitar los trunks en un puerto. Esta inhabilitación ayuda a eliminar el tiempo de negociación perdido cuando se activan los puertos host.

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

Otras Opciones

Otra configuración común del cliente utiliza el modo `deseable dinámico` en la capa de distribución y la configuración predeterminada más simple (`modo automático dinámico`) en la capa de acceso. Algunos switches, como el Catalyst 2900XL, los routers Cisco IOS u otros dispositivos de proveedor, no soportan actualmente la negociación troncal a través de DTP. Puede utilizar el modo `no negociación` para establecer un puerto en trunk incondicionalmente con estos dispositivos. Este modo puede ayudar a estandarizar en una configuración común en el campus.

Cisco recomienda `nonegotiate` cuando se conecta a un router Cisco IOS. A lo largo de la conexión en puente, algunas tramas DTP que se reciben de un puerto configurado con **switchport mode trunk** pueden regresar al puerto trunk. Tras la recepción de la trama DTP, el puerto del switch intenta renegociar innecesariamente. Para renegociar, el puerto del switch hace que el tronco `caiga` y luego se `active`. Si se habilita el modo de no negociación , el switch no envía tramas DTP.

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

Spanning Tree Protocol

Propósito

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

En algunos aspectos, STP es un protocolo temprano que se desarrolló inicialmente para especificaciones de puente basadas en software lentas (IEEE 802.1D). Sin embargo, el STP puede ser complicado para implementarlo exitosamente en redes conmutadas grandes que tienen:

- Muchas VLAN
- Muchos switches en un dominio
- Compatibilidad con varios proveedores
- Mejoras IEEE más recientes

El software del sistema Cisco IOS ha adoptado nuevos desarrollos de STP. Los nuevos estándares IEEE que incluyen el STP rápido 802.1w y los protocolos de árbol de extensión múltiple 802.1s proporcionan convergencia rápida, distribución de carga y escalado del plano de control. Además, las funciones de mejora de STP como RootGuard, el filtrado de BPDU, la protección Portfast BPDU y Loopguard proporcionan protección adicional contra los loops de reenvío de Capa 2.

Descripción general del funcionamiento de PVST+

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

Inicialmente, las BPDU se envían desde todos los switches y contienen la BID de cada switch y el costo de trayectoria para alcanzar ese switch. Esto habilita la determinación del puente raíz y la trayectoria de menor costo a la raíz. Los parámetros de configuración adicionales que se transportan en BPDU desde la raíz reemplazan los parámetros que se configuran localmente de modo que toda la red utilice temporizadores consistentes. Por cada BPDU que un switch recibe de la raíz, el NMP central de Catalyst procesa una nueva BPDU y la envía con la información de la raíz.

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 (que se encuentra frente al puente raíz) en cada puente que no sea raíz.
3. Se elige un puerto designado para el reenvío de BPDU en cada segmento.
4. Los puertos no designados se bloquean.

Si desea más información, consulte estos documentos:

- Configuración de STP e IEEE 802.1s MST
- Introducción al Rapid Spanning Tree Protocol [protocolo de árbol de expansión rápida] (802.1w)

Temporizadores básicos predeterminados	Nombre	Función
2 seg.	Saludo	Controla la salida de las BPDU.
15 seg.	Demora de Reenvío (Fwd delay)	Controla el tiempo que un puerto pasa en el estado `de escucha` y en el `estado de aprendizaje` e influye en el proceso de cambio de topología.
20 seg.	maxage	Controla el tiempo que el switch mantiene la topología actual antes de que el switch busque una trayectoria

		alternativa. Después del tiempo máximo de envejecimiento (maxage), una BPDU se considera obsoleta y el switch busca un nuevo puerto raíz del conjunto de puertos de bloqueo. Si no hay ningún puerto bloqueado disponible, el switch afirma ser la raíz en sí en los puertos designados.

Cisco recomienda que no cambie los temporizadores porque esto puede afectar negativamente a la estabilidad. La mayoría de las redes implementadas no están ajustadas. Los temporizadores STP simples a los que se puede acceder a través de la línea de comandos (como hello-interval, maxage, etc.) están compuestos por un conjunto complejo de otros temporizadores intrínsecos y supuestos. Por lo tanto, es difícil ajustar los temporizadores y considerar todas las ramificaciones. Además, puede socavar la protección UDLD. Consulte la sección Detección de Link Unidireccional para obtener más detalles.

Nota sobre los Temporizadores STP:

Los valores predeterminados del temporizador STP se basan en un cálculo que considera un diámetro de red de siete switches (siete saltos de switch de la raíz al borde de la red), y el tiempo necesario para que una BPDU viaje del puente raíz a los switches de borde en la red, que están a siete saltos de distancia. Esta suposición calcula los valores del temporizador que son aceptables para la mayoría de las redes. Sin embargo, puede cambiar estos temporizadores a valores más óptimos para acelerar los tiempos de convergencia a través de los cambios de topología de red.

Puede configurar el puente raíz con el diámetro de la red para una VLAN específica, y los valores del temporizador se calculan en consecuencia. Cisco recomienda que, si debe hacer cambios, sólo configure los parámetros de diámetro y de tiempo hello opcional en el bridge root para la VLAN.

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

Esta macro hace la raíz del switch para la VLAN especificada, computa nuevos valores del temporizador en base al diámetro y el tiempo hello especificado, y propaga esta información en las BPDU de configuración a todos los otros switches en la topología.

La sección Nuevos Estados de Puerto y Funciones de Puerto describe el STP 802.1D y compara y contrasta el STP 802.1D con el STP rápido (RSTP). Consulte Introducción al protocolo de árbol de extensión rápido (802.1w) para obtener más información sobre RSTP.

Nuevos Estados y Funciones de Puerto

802.1D se define en cuatro estados de puerto diferentes:

- Escucha
- Learning
- Bloqueo
- Reenvío

Consulte la tabla de la sección Estados de Puerto para obtener más información. El estado del puerto es mixto (ya sea que bloquea o reenvía el tráfico), al igual que la función que desempeña el puerto en la topología activa (puerto raíz, puerto designado, etc.). Por ejemplo, desde un punto de vista operativo, no hay diferencia entre un puerto en estado de bloqueo y un puerto en estado de escucha. Ambos descartan tramas y no aprenden direcciones MAC. La diferencia real radica en la función que el árbol de expansión asigna al puerto. Usted puede asumir de manera segura que un puerto de escucha es designado o root y está en camino al estado de reenvío. Desafortunadamente, una vez que el puerto está en estado de reenvío, no hay manera de inferir del estado del puerto si el puerto es root o designado. Esto demuestra el fracaso de esta terminología basada en el estado. RSTP resuelve esta falla porque RSTP desvincula la función y el estado de un puerto.

Estados de Puertos

Estados de puerto en STP 802.1D

Estados de puertos	Medios	Tiempos predeterminados para el siguiente estado
`Inhabilitado`	Sin funcionamiento desde el punto de vista administrativo.	
`Bloqueo`	Recibe BPDU y detiene los datos del usuario.	Monitorea la recepción de BPDU. 20 segundos de espera para el vencimiento máximo o cambio inmediato si se detecta una falla de link directo/local.
`Escucha`	Envía o recibe BPDU para verificar si es necesario volver al bloqueo.	Espere 15 segundos Fwddelay.
`Learning`	Genera una tabla de topología/CAM.	Espere 15 segundos Fwddelay.
`Reenvío`	Envía/recibe datos.	

El cambio de topología básico total es:

- 20 + 2 (15) = 50 s, si espera a que caduque el máximo
- 30 segundos para falla de link directo

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

Estado de	Estado de	¿El puerto está	¿El puerto

Puerto de STP (802.1D)	Puerto RSTP (802.1w)	incluido en la topología activa?	detecta direcciones MAC?
Inhabilitado	Descarte	No	No
Bloqueo	Descarte	No	No
Escucha	Descarte	Yes	No
Learning	Learning	Yes	Yes
Reenvío	Reenvío	Yes	Yes

Funciones de Puerto

El rol es ahora una variable que se asigna a un puerto dado. Los roles de puerto raíz y de puerto designado permanecen, pero el rol de puerto de bloqueo ahora se divide en los roles de puerto alternativo y de respaldo. El algoritmo de árbol de extensión (STA) determina la función de un puerto en función de las BPDU. Recuerde esto sobre las BPDU para mantener las cosas simples: siempre hay una manera de comparar dos BPDU cualesquiera y decidir si una es más útil que la otra. La base de la decisión es el valor que se almacena en la BPDU y, ocasionalmente, el puerto en el que se recibe la BPDU. El resto de esta sección explica enfoques muy prácticos para las funciones de los puertos.

Función de puerto raíz

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

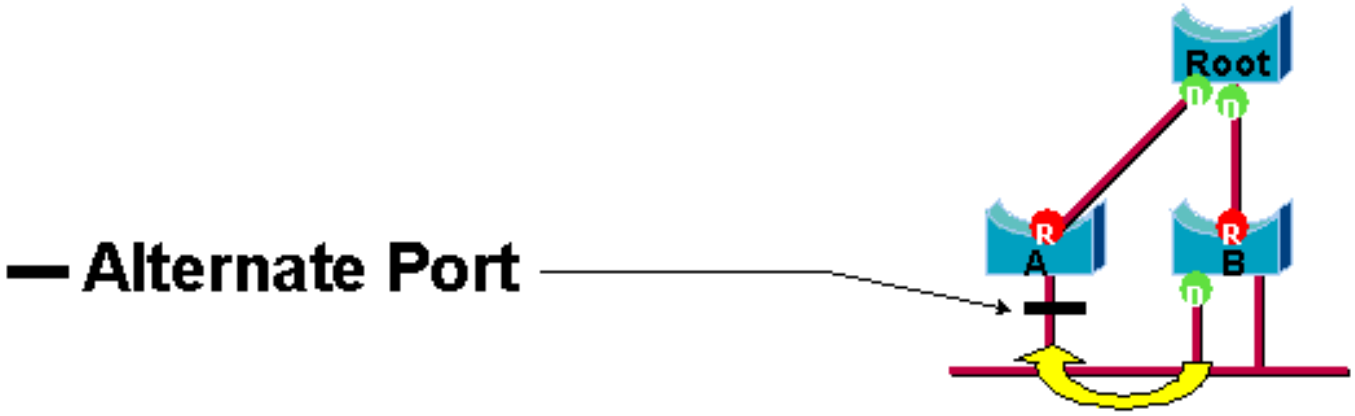
Función de Puerto Designado

Se designa un puerto si puede enviar la mejor BPDU en el segmento al que está conectado el puerto. Los puentes 802.1D se conectan entre segmentos diferentes (por ejemplo, segmentos Ethernet) para crear un dominio puenteado. En un segmento dado, sólo puede haber un trayecto hacia el bridge raíz. Si hay dos trayectorias, hay un loop de conexión en puente en la red. Todos los puentes que están conectados a un segmento dado escuchan las BPDU de los otros y acuerdan en el puente que envía la mejor BPDU como el puente designado para el segmento. El puerto correspondiente en ese puente está designado.

Funciones de Puerto Alternativo y de Respaldo

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

Un puerto alternativo es un puerto que se bloquea al recibir BPDU más útiles de otro puente. Este diagrama ilustra:



Un puerto de respaldo es un puerto que se bloquea al recibir BPDU más útiles del mismo puente en el que se encuentra el puerto. Este diagrama ilustra:

Esta diferenciación ya se realizó internamente en 802.1d. Esto es esencialmente cómo funciona UplinkFast de Cisco. La razón detrás de esto es que un puerto alternativo proporciona una trayectoria alternativa al bridge raíz. Por lo tanto, este puerto puede reemplazar el puerto raíz si

falla. Por supuesto, un puerto de respaldo proporciona conectividad redundante al mismo segmento y no puede garantizar una conectividad alternativa al bridge root. Por lo tanto, el puerto de respaldo fue excluido del grupo de link ascendente.

Como resultado, RSTP calcula la topología final para el spanning tree con el uso de exactamente los mismos criterios que 802.1D. No hay ningún cambio en la forma en que se utilizan las diferentes prioridades de puerto y puente. El nombre blocking (bloqueo) se utiliza para el estado de descarte en la implementación de Cisco. Las versiones 7.1 y posteriores de CatOS aún muestran los estados de escucha y aprendizaje, lo que proporciona aún más información sobre un puerto de la que requiere el estándar IEEE. Pero la nueva característica es que ahora hay una diferencia entre el rol que el protocolo ha determinado para un puerto y su estado actual. Por ejemplo, ahora es perfectamente válido que un puerto sea designado y de bloqueo al mismo tiempo. Aunque esto suele suceder durante periodos muy cortos de tiempo, significa simplemente que este puerto está en estado transitorio hacia el reenvío designado.

Interacciones STP con VLAN

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

- Un único árbol de extensión para todas las VLAN o protocolo de árbol de extensión común (CST), como IEEE 802.1D
- Un Spanning Tree por VLAN, o Spanning Tree compartido, como Cisco PVST
- Un árbol de extensión por conjunto de VLAN o árbol de extensión múltiple (MST), como IEEE 802.1s

Desde el punto de vista de la configuración, estos tres tipos de modos de árbol de expansión relacionados con la interacción con las VLAN se pueden configurar en uno de los tres tipos de modos siguientes:

- **pvst**: Spanning Tree por VLAN. Esto en realidad implementa PVST+, pero en Cisco IOS Software se indica simplemente como PVST.
- **fast-pvst**: la evolución del estándar 802.1D mejora los tiempos de convergencia e incorpora las propiedades basadas en estándares (802.1w) de UplinkFast y BackboneFast.
- **mst**: es el estándar 802.1s para un árbol de expansión por conjunto de VLAN o MST. Esto también incorpora el componente rápido 802.1w dentro del estándar.

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

Un Spanning Tree por VLAN o PVST+ permite el balanceo de carga pero requiere más procesamiento de CPU BPDU a medida que aumenta el número de VLAN.

El nuevo estándar 802.1s (MST) permite la definición de hasta 16 instancias/topologías STP activas y la asignación de todas las VLAN a estas instancias. En un entorno de campus típico, solo es necesario definir dos instancias. Esta técnica permite que el STP se amplíe a muchos miles de VLAN mientras habilita el balanceo de carga.

El soporte para Rapid-PVST y MST pre-estándar se introduce en Cisco IOS Software Release 12.1(11b)EX y 12.1(13)E para Catalyst 6500. Catalyst 4500con Cisco IOS Software Release 12.1(12c)EW y versiones posteriores soportan MST pre-estándar. El soporte PVST rápido se agrega en la plataforma Cisco IOS Software Release12.1(19)EW para Catalyst 4500. El MST estándar es compatible con Cisco IOS Software Release 12.2(18)SXF para Catalyst 6500 y Cisco

IOS Software Release12.2(25)SG para Catalyst 4500 Series Switches.

Para obtener más información, consulte Comprensión del protocolo de árbol de extensión rápido (802.1w) y Comprensión del protocolo de árbol de extensión múltiple (802.1s).

Puertos lógicos de árbol de expansión

Las notas de la versión de Catalyst 4500 y 6500 proporcionan orientación sobre el número de puertos lógicos en el árbol de expansión por switch. La suma de todos los puertos lógicos equivale al número de troncales en el switch por el número de VLAN activas en los troncales, más el número de interfaces que no son troncales en el switch. El software Cisco IOS genera un mensaje de registro del sistema si el número máximo de interfaces lógicas excede la limitación. Se recomienda no exceder las directrices recomendadas.

Esta tabla compara el número de puertos lógicos soportados con varios modos STP y tipo de supervisor:

Supervisor	PVST+	RPVST+	MST
Catalyst 6500 Supervisor 1	6000[1] en total 1200 por módulo de conmutación	6000 en total 1200 por módulo de switching	25 000 en total 3 000 [2] por módulo de conmutación
Catalyst 6500 Supervisor 2	13 000 [1] en total 1 800 [2] por módulo de conmutación	10 000 en total 1 800 [2] por módulo de conmutación	50 000 en total 6 000 [2] por módulo de conmutación
Catalyst 6500 Supervisor 720	13 000 en total 1 800 [2] por módulo de conmutación	10 000 en total 1 800 [2] por módulo de conmutación	50 003 en total 6 000 [2] por módulo de conmutación
Catalyst 4500 Supervisor II más	1500 en total	1500 en total	25 000 en total
Catalyst 4500 Supervisor II más 10GE	1500 en total	1500 en total	25 000 en total
Catalyst 4500 Supervisor IV	3000 en total	3000 en total	50 000 en total
Catalyst 4500 Supervisor	3000 en total	3000 en total	50 000 en total

r V			
Catalyst 4500 Supervisor V 10GE	3000 en total	3000 en total	80 000 en total

[1] El número máximo de puertos lógicos totales soportados en PVST+ antes de la versión 12.1(13)E del software del IOS de Cisco es de 4500.

[2] módulos de switching de 10 Mbps, 10/100 Mbps y 100 Mbps admiten un máximo de 1200 interfaces lógicas por módulo.

[3] El número máximo de puertos lógicos totales soportados en MST antes de Cisco IOS Software Release 12.2(17b)SXA es de 30.000.

Recomendación

Es difícil proporcionar una recomendación de modo de árbol de expansión sin información detallada como hardware, software, número de dispositivos y número de VLAN. En general, si el número de puertos lógicos no excede la directriz recomendada, se recomienda el modo PVST rápido para la nueva implementación de red. El modo PVST rápido proporciona convergencia de red rápida sin necesidad de configuración adicional, como Backbone Fast y Uplink Fast. Ejecute el siguiente comando para establecer el spanning-tree en el modo Rapid-PVST:

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

Otras Opciones

En una red con una mezcla de hardware antiguo y software antiguo, se recomienda el modo PVST+. Ejecute este comando para establecer el spanning-tree en el modo PVST+:

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

Se recomienda el modo MST para el diseño de red de VLAN en cualquier lugar con un gran número de VLAN. Para esta red, la suma de los puertos lógicos puede exceder la directriz para PVST y Rapid-PVST. Ejecute este comando para establecer el spanning-tree en el modo MST:

```
spanning-tree mode mst
```

Formatos BPDU

Para soportar el estándar IEEE 802.1Q, Cisco amplió el protocolo PVST que existe para proporcionar el protocolo PVST+. PVST+ agrega soporte para links en la región del árbol de expansión mono IEEE 802.1Q. PVST+ es compatible tanto con el árbol de extensión único IEEE 802.1Q como con los protocolos PVST de Cisco que existen. Además, PVST+ agrega mecanismos de verificación para asegurarse de que no haya inconsistencia de configuración de troncal de puerto e ID de VLAN entre los switches. PVST+ es compatible con Plug and Play con

PVST, sin necesidad de un nuevo comando o configuración de interfaz de línea de comandos (CLI).

A continuación se presentan algunos aspectos destacados de la teoría operativa del protocolo PVST+:

- PVST+ interactúa con el árbol de expansión mono 802.1Q. PVST+ interactúa con los switches compatibles con 802.1Q en el STP común a través de la conexión troncal 802.1Q. El árbol de expansión común se encuentra en la VLAN 1, la VLAN nativa, de forma predeterminada. Una BPDU de árbol de expansión común se transmite o recibe con la dirección MAC de grupo de puente estándar IEEE (01-80-c2-00-00-00, tipo de protocolo 0x010c) a través de enlaces 802.1Q. El spanning tree común se puede arraigar en la región del PVST o del spanning tree mono.
- PVST+ tuneliza las BPDU PVST a través de la región VLAN 802.1Q como datos de multidifusión. Para cada VLAN en un trunk, las BPDU con la dirección MAC de Cisco Shared STP (SSTP) (01-00-0c-cc-cd) se transmiten o reciben. Para las VLAN iguales al identificador de VLAN de puerto (PVID), la BPDU no está etiquetada. Para todas las demás VLAN, las BPDU se etiquetan.
- PVST+ es compatible con versiones anteriores del switch de Cisco existente en PVST a través de la conexión troncal ISL. Las BPDU encapsuladas por ISL se transmiten o reciben a través de los troncales ISL, que es el mismo que con los PVST anteriores de Cisco.
- PVST+ verifica si hay inconsistencias de puerto y VLAN. PVST+ bloquea los puertos que reciben BPDU inconsistentes para evitar que ocurran loops de reenvío. PVST+ también notifica a los usuarios a través de mensajes de syslog cualquier inconsistencia.

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

Recomendaciones de configuración de Cisco

Todos los switches Catalyst tienen el STP habilitado de forma predeterminada. Incluso si elige un diseño que no incluye loops de Capa 2 y el STP no está habilitado para mantener activamente un puerto bloqueado, deje la función habilitada por estas razones:

- Si hay un loop, STP evita los problemas que pueden empeorar con los datos de multidifusión y difusión. A menudo, el mal parcheado, un cable defectuoso u otra causa induce un loop.
- STP protege frente a una falla de EtherChannel.
- La mayoría de las redes se configuran con STP y, por lo tanto, obtienen la máxima exposición al campo. Por lo general, una mayor exposición equivale a un código más estable.
- El STP protege contra el mal comportamiento de las NIC conectadas duales (o la conexión en puente habilitada en los servidores).
- Muchos protocolos están estrechamente relacionados con el STP en el código. Algunos ejemplos son:PAgPSnooping del protocolo de mensajes de grupo de Internet (IGMP)TrunkingSi se ejecuta sin STP, puede obtener resultados no deseados.
- Durante una interrupción de la red informada, los ingenieros de Cisco suelen sugerir que el no uso del STP está en el centro de la falla, si es que es posible.

Para habilitar el spanning tree en todas las VLAN, ejecute estos comandos globales:

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

```
!--- Set spanning-tree parameters to default values.
```

No cambie los temporizadores, que pueden afectar negativamente a la estabilidad. La mayoría de las redes implementadas no están ajustadas. Los temporizadores STP simples a los que se puede acceder a través de la línea de comandos, como hello-interval y maxage, tienen un conjunto complejo de otros temporizadores intrínsecos y supuestos. Por lo tanto, puede tener dificultades si intenta ajustar los temporizadores y considerar todas las ramificaciones. Además, puede socavar la protección UDLD.

Lo ideal es que mantenga el trafico de los usuarios fuera de la VLAN de administración. Esto no se aplica en el switch Catalyst 6500/6000 Cisco IOS. Aun así, debe respetar esta recomendación en los switches Cisco IOS de menor tamaño y en los switches CatOS que pueden tener una interfaz de administración independiente y deben integrarse con los switches Cisco IOS. Especialmente con los procesadores de switch Catalyst más antiguos, mantenga la VLAN de administración separada de los datos de usuario para evitar problemas con STP. Una estación final con mal comportamiento puede potencialmente mantener al procesador Supervisor Engine tan ocupado con los paquetes de broadcast que el procesador puede perder una o más BPDU. Sin embargo, los switches más nuevos con CPU y controles de regulación más potentes reducen esta consideración. Consulte la sección Interfaz de administración de switches y VLAN nativa de este documento para obtener más detalles.

No sobrescriba la redundancia. Esto puede llevar a demasiados puertos de bloqueo y puede afectar negativamente a la estabilidad a largo plazo. Mantenga el diámetro STP total por debajo de siete saltos. Intente diseñar al modelo multicapa de Cisco siempre que sea posible este diseño. El modelo incluye:

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

Influya y sepa dónde residen la funcionalidad raíz y los puertos bloqueados. Documentar esta información en el diagrama de topología. Conozca su topología de árbol de expansión, que es esencial para resolver problemas. Los puertos bloqueados son donde comienza la resolución de problemas STP. La causa del cambio del bloqueo al reenvío es a menudo la parte clave del análisis de la causa raíz. Elija las capas de distribución y de núcleo como la ubicación de la raíz/raíz secundaria porque estas capas se consideran las partes más estables de la red. Compruebe la existencia de una superposición óptima de protocolo de router en espera en caliente (HSRP) y capa 3 con rutas de reenvío de datos de capa 2.

Este comando es una macro que configura la prioridad de bridge. La raíz establece que la prioridad es mucho menor que la predeterminada (32.768), y la prioridad secundaria establece que es razonablemente menor que la predeterminada:

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

Nota: Esta macro establece que la prioridad raíz sea:

- 8192 de forma predeterminada
- La prioridad raíz actual menos 1, si se conoce otro bridge raíz
- La prioridad raíz actual, si su dirección MAC es menor que la raíz actual

Quite las VLAN innecesarias de los puertos troncales, lo que es un ejercicio bidireccional. La acción limita el diámetro de la sobrecarga de procesamiento de STP y NMP en partes de la red

donde ciertas VLAN no son necesarias. El recorte automático de VTP no quita el STP de un trunk. También puede quitar la VLAN 1 predeterminada de los troncales.

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

Otras Opciones

Cisco tiene otro protocolo STP, llamado **VLAN-bridge**, que funciona con el uso de una dirección MAC de destino conocida de **01-00-0c-cd-cd-ce** y tipo de protocolo de 0x010c.

Este protocolo es más útil si existe la necesidad de conectar protocolos no ruteables o heredados entre VLAN sin interferencia con las instancias del árbol de expansión IEEE que se ejecutan en esas VLAN. Si las interfaces VLAN para el tráfico no puenteado se bloquean para el tráfico de Capa 2, la superposición del tráfico de Capa 3 también se elimina involuntariamente, lo que es un efecto secundario no deseado. Este bloqueo de Capa 2 puede ocurrir fácilmente si las interfaces VLAN para el tráfico no puenteado participan en el mismo STP que las VLAN IP. VLAN-bridge es una instancia separada de STP para los protocolos puenteados. El protocolo proporciona una topología independiente que puede manipularse sin afectar el tráfico IP.

Ejecute el protocolo VLAN-bridge si se requiere bridging entre VLAN en routers Cisco como MSFC.

Función STP PortFast

Puede utilizar PortFast para eludir el funcionamiento normal del árbol de expansión en los puertos de acceso. PortFast acelera la conectividad entre las estaciones finales y los servicios a los que las estaciones finales necesitan conectarse después de la inicialización del link. La implementación de DHCP de Microsoft necesita ver el puerto de acceso en el modo de `reenvío` inmediatamente después de que el estado del link `se` activa para solicitar y recibir una dirección IP. Algunos protocolos, como Intercambio de Paquetes entre Redes (IPX)/Intercambio de Paquetes Secuenciados (SPX), necesitan ver el puerto de acceso en el modo de `reenvío inmediatamente después de que el estado del link sube` para evitar los problemas de Get Nearest Server (GNS).

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

Descripción General de PortFast Operations

PortFast omite los estados de `escucha` normal, `aprendizaje` y `reenvío` de STP. La función mueve un puerto directamente del `bloqueo` al `modo de reenvío` después de que el link se vea como `activo`. Si esta función no está habilitada, el STP desecha todos los datos del usuario hasta que decide que el puerto está listo para pasar al modo de reenvío. Este proceso puede tardar (2 x RetrasoReenvío), que es de 30 segundos de forma predeterminada.

El modo `Portfast` evita la generación de una Notificación de cambio de topología (TCN) STP cada vez que un estado de puerto cambia de `aprendizaje` a `reenvío`. Los TCN son normales. Sin embargo, una oleada de TCN que llega al puente raíz puede prolongar el tiempo de convergencia innecesariamente. Una ola de TCN ocurre a menudo por la mañana, cuando las personas encienden sus PC.

Recomendación de configuración del puerto de acceso de Cisco

Establezca STP PortFast en `on` para todos los puertos host habilitados. Además, establezca explícitamente STP PortFast en `off` para links de switch y puertos que no están en uso.

Ejecute el comando **switchport host** macro en el modo de configuración de la interfaz para implementar la configuración recomendada para los puertos de acceso. La configuración también ayuda significativamente a la negociación automática y al rendimiento de la conexión:

```
switch(config)#interface type slot#/port#

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

Nota: PortFast no significa que el spanning tree no se ejecute en absoluto en los puertos. Aún se envían, se reciben y se procesan BDPU. El árbol de extensión es esencial para una LAN totalmente funcional. Sin la detección y el bloqueo del loop, un loop puede desactivar la LAN por completo de forma involuntaria y rápida.

Además, inhabilite el trunking y la canalización para todos los puertos 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 deja estos protocolos para negociar, el retraso subsiguiente en la activación del puerto puede conducir a situaciones indeseables. Los paquetes iniciales de las estaciones de trabajo, como las solicitudes DHCP e IPX, no se reenvían.

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

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

Luego, en cualquier puerto de acceso que tenga un hub o un switch en una sola VLAN, inhabilite la función PortFast en cada interfaz con el comando **interface**:

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

Otras Opciones

La protección PortFast BPDU proporciona un método para evitar loops. La protección BPDU mueve un puerto que no es de enlace troncal a un estado `errDisable` en la recepción de una BPDU en ese puerto.

En condiciones normales, nunca reciba ningún paquete BPDU en un puerto de acceso configurado para PortFast. Una BPDU entrante indica una configuración no válida. La mejor acción es apagar el puerto de acceso.

El software del sistema Cisco IOS ofrece un útil comando global que habilita automáticamente

`BPDU-ROOT-GUARD` en cualquier puerto que esté habilitado para UplinkFast. *Utilice siempre* este comando. El comando funciona por switch y no por puerto.

Ejecute este comando global para habilitar `BPDU-ROOT-GUARD`:

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

Un mensaje de trampa o syslog del protocolo simple de administración de red (SNMP) notifica al administrador de red si el puerto deja de funcionar. También puede configurar un tiempo de recuperación automático para los puertos `errDisabled`. Consulte la sección Detección de Link Unidireccional de este documento para obtener más detalles.

Refiérase a Mejora de la Protección PortFast BPDU del Spanning Tree para obtener más detalles.

Nota: PortFast para puertos troncales se introdujo en la versión 12.1(11b)E del software del IOS de Cisco. PortFast para puertos troncales está diseñado para aumentar los tiempos de convergencia de las redes de Capa 3. Cuando utilice esta función, asegúrese de inhabilitar la protección BPDU y el filtro BPDU sobre una base de interfaz.

UplinkFast

Propósito

UplinkFast provee una rápida convergencia STP luego de una falla de enlace directo en la capa de acceso de la red. UplinkFast funciona sin modificar el STP. El objetivo es acelerar el tiempo de convergencia en una circunstancia específica a menos de tres segundos, en lugar del retraso típico de 30 segundos. Refiérase a Comprensión y Configuración de la Función Cisco UplinkFast.

Información Operativa General

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

Un grupo de link ascendente es un conjunto de puertos por VLAN que puede considerar como un puerto raíz y un puerto raíz de respaldo. En condiciones normales, los puertos raíz aseguran la conectividad desde el acceso hacia la raíz. Si esta conexión raíz primaria falla por cualquier razón, el link raíz de respaldo se inicia inmediatamente, sin la necesidad de pasar por los típicos 30 segundos de demora de convergencia.

Debido a que UplinkFast omite efectivamente el proceso normal de manejo de cambios en la topología STP (`escucha` y `aprendizaje`), se necesita un mecanismo alternativo de corrección de topología. El mecanismo necesita actualizar los switches en el dominio con la información de que las estaciones finales locales son accesibles a través de una trayectoria alternativa. Por lo tanto, el switch de capa de acceso que ejecuta UplinkFast también genera tramas para cada dirección MAC en su tabla CAM a una dirección MAC multicast conocida (01-00-0c-cd-cd HDLC protocol 0x200a). Este proceso actualiza la tabla CAM en todos los switches del dominio con la nueva topología.

Recomendación de Cisco

Cisco recomienda que habilite UplinkFast para switches de acceso con puertos bloqueados si ejecuta un árbol de expansión 802.1D. No utilice UplinkFast en los switches sin el conocimiento implícito de topología de un link raíz de respaldo, normalmente switches de distribución y de núcleo en el diseño multicapa de Cisco. En términos generales, no habilite UplinkFast en un switch con más de dos formas de salir de una red. Si el switch se encuentra en un entorno de acceso complejo y tiene más de un bloqueo de link y un reenvío de link, evite el uso de esta función en el switch o consulte a su ingeniero de servicios avanzados.

Ejecute este comando global para habilitar UplinkFast:

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

Este comando en Cisco IOS Software no ajusta automáticamente todos los valores de prioridad de bridge a un valor alto. Más bien, el comando sólo cambia esas VLAN con una prioridad de bridge que no se ha cambiado manualmente a otro valor. Además, a diferencia de CatOS, cuando restaura un switch que tenía UplinkFast habilitado, la forma no de este comando (**no spanning-tree uplinkfast**) devuelve todos los valores modificados a sus valores predeterminados. Por lo tanto, cuando utiliza este comando, *debe* verificar el estado actual de las prioridades del puente antes y después para asegurar que se alcance el resultado deseado.

Nota: Necesita la palabra clave **all protocols** para el comando UplinkFast cuando se habilita la función de filtrado de protocolo. Debido a que el CAM registra el tipo de protocolo así como 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 es necesario configurar UplinkFast con RSTP porque el mecanismo se incluye de forma nativa y se habilita automáticamente en RSTP.

BackboneFast

Propósito

BackboneFast proporciona una convergencia rápida después de que se produce una falla de link indirecto. BackboneFast reduce los tiempos de convergencia del valor predeterminado de 50 segundos a, normalmente, 30 segundos y, de esta manera, agrega funcionalidad al STP. De nuevo, esta función sólo se aplica cuando se ejecuta 802.1D. No configure la función cuando ejecute Rapid PVST o MST (que incluye el componente rápido).

Información Operativa General

BackboneFast se inicia cuando un puerto raíz o un puerto bloqueado en un switch recibe BPDU inferiores del bridge designado. El puerto normalmente recibe BPDU inferiores cuando un switch descendente pierde la conexión con la raíz y comienza a enviar BPDU para elegir una nueva raíz. Una BPDU inferior identifica a un switch como el root bridge y el bridge designado a la vez.

Bajo las reglas normales del spanning tree, el switch receptor ignora las BPDU inferiores durante el tiempo máximo configurado. De forma predeterminada, el máximo es 20 segundos. Pero, con BackboneFast, el switch ve la BPDU inferior como una señal de un posible cambio en la topología. El switch utiliza BPDU de consultas de enlaces raíz (RLQ) para determinar si tiene una ruta alternativa al puente raíz. Esta adición del protocolo RLQ permite que un switch verifique si la raíz aún está disponible. RLQ mueve un puerto bloqueado al `reenvío` antes y notifica al switch

aislado que envió la BPDU inferior que la raíz aún está allí.

A continuación se muestran algunos aspectos destacados de la operación del protocolo:

- Un switch transmite el paquete RLQ solamente fuera del puerto raíz (lo que significa que el paquete va hacia la raíz).
- Un switch que recibe un RLQ puede responder si es el switch raíz, o si ese switch sabe que ha perdido la conexión con la raíz. Si el switch no conoce estos hechos, debe reenviar la consulta fuera de su puerto raíz.
- Si un switch ha perdido la conexión con la raíz, el switch debe responder en negativo a esta consulta.
- La respuesta debe enviarse sólo fuera del puerto desde el que se originó la consulta.
- El switch raíz debe responder siempre a esta consulta con una respuesta positiva.
- Si la respuesta se recibe en un puerto no raíz, descarte la respuesta.

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

Recomendación de Cisco

Habilite BackboneFast en todos los switches que ejecutan STP solamente si todo el dominio de árbol de expansión puede soportar esta función. Puede agregar la función sin interrumpir una red de producción.

Ejecute este comando global para habilitar BackboneFast:

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

Nota: Debe configurar este comando global en todos los switches de un dominio. El comando agrega funcionalidad al STP que todos los switches necesitan entender.

Otras Opciones

BackboneFast no se soporta en los switches Catalyst 2900XL y 3500XL. En general, debe habilitar BackboneFast si el dominio del switch contiene estos switches además de los switches Catalyst 4500/4000, 5500/5000 y 6500/6000. Cuando implementa BackboneFast en entornos con switches XL, bajo topologías estrictas, puede habilitar la función donde el switch XL es el último switch en línea y sólo está conectado al núcleo en dos lugares. No implemente esta función si la arquitectura de los switches XL está en modo de cadena de margarita.

No es necesario configurar BackboneFast con RSTP o 802.1w porque el mecanismo se incluye de forma nativa y se habilita automáticamente en RSTP.

Función de Protección contra Loops de Spanning Tree Protocol

La función de protección contra loops es una optimización propiedad de Cisco para el protocolo STP. La protección contra loops protege las redes de Capa 2 de los loops que se producen debido a un mal funcionamiento de la interfaz de red, CPU ocupada o cualquier cosa que impida el reenvío normal de BPDU. Se crea un loop STP cuando un puerto de bloqueo en una topología redundante pasa erróneamente al estado de reenvío. Esto suele suceder porque uno de los

puertos en una topología físicamente redundante (no necesariamente el puerto de bloqueo) dejó de recibir BPDU.

La protección contra loops solo es útil en redes conmutadas donde los switches se conectan mediante enlaces punto a punto, como ocurre en la mayoría de las redes de campus y Data Centers modernas. La idea es que, en un link punto a punto, un bridge designado no puede desaparecer sin enviar una BPDU inferior o apagar el link. La función de protección contra loops STP se introdujo en Cisco IOS Software Release 12.1(13)E del Catalyst Cisco IOS Software para Catalyst 6500 y Cisco IOS Software Release 12.1(9)EA1 para los switches Catalyst 4500.

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

La protección contra loops verifica si un puerto raíz o un puerto raíz alternativo/de respaldo recibe BPDU. Si el puerto no recibe BPDU, la protección contra loops coloca al puerto en un estado inconsistente (bloqueo) hasta que comienza a recibir BPDU nuevamente. Un puerto en el estado inconsistente no transmite BPDU. Si dicho puerto recibe BPDU nuevamente, el puerto y el link se vuelven a considerar viables. La condición loop-inconsistent se quita del puerto y el STP determina el estado del puerto. De esta manera, la recuperación es automática.

La función de protección contra loops aísla la falla y deja que el spanning tree converja en una topología estable sin el link o el bridge de la falla. La protección contra loops evita loops STP con la velocidad de la versión STP que está en uso. No hay dependencia del propio STP (802.1D o 802.1w) o al ajustar los temporizadores STP. Por estas razones, Cisco recomienda implementar la protección contra loops junto con el UDLD en topologías que dependen del STP y donde el software soporta las funciones.

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

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

Después de que la BPDU se recibe en un puerto en un estado STP loop-inconsistent, el puerto pasa a otro estado STP. Según la BPDU recibida, esto significa que la recuperación es automática y no es necesaria ninguna intervención. Después de la recuperación, se registra este mensaje:

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

Interacción con Otras Funciones de STP

Protección de raíz

La protección de raíz hace que un puerto siempre sea puerto designado. La protección contra loops sólo es efectiva si el puerto es un puerto raíz o un puerto alternativo, lo que significa que sus funciones son mutuamente excluyentes. Por lo tanto, la protección contra loops y la 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 un puerto raíz en estado de bloqueo, UplinkFast coloca en estado de reenvío un nuevo puerto raíz. Además, UplinkFast no selecciona un puerto es estado loop-inconsistent como puerto raíz.

BackboneFast

La protección contra loops es compatible con BackboneFast. BackboneFast se activa mediante la recepción de una BPDU inferior que proviene de un puente designado. Debido a que las BPDU se reciben de este link, la protección contra loops no se inicia. Por lo tanto, 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. Debido a que un puerto habilitado para PortFast no es un puerto raíz/alternativo, la protección contra loops y PortFast son mutuamente excluyentes.

PAgP

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

- STP siempre elige 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 un conjunto de puertos que ya están bloqueados por la protección contra loops se agrupan para formar un canal, el STP pierde toda la información de estado para esos puertos, y el nuevo puerto de canal posiblemente pueda alcanzar el estado de reenvío con una función designada.
- 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 alcanzar el estado de reenvío con una función designada, incluso si uno o más de los links que formaron el canal son unidireccionales.

En estos últimos dos casos, existe la posibilidad de un loop hasta que UDLD detecte la falla. Pero la protección contra loops no puede detectarla.

Comparación de Protección contra Loops y UDLD

La protección contra loops y la funcionalidad UDLD se superponen parcialmente, en el sentido de que ambas protegen contra las fallas STP que causan los links unidireccionales. Estas dos funciones son diferentes en el enfoque del problema y también en la funcionalidad. Específicamente, hay fallas unidireccionales específicas que el UDLD no puede detectar, como fallas causadas 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 o en situaciones donde el link ha sido

unidireccional desde el link. En el caso de un link que ha sido unidireccional desde el link, el puerto nunca recibe BPDU y se convierte en designado. Esto puede ser un comportamiento normal, por lo que la protección contra loops no cubre este caso en particular. UDLD brinda protección contra tal escenario.

La habilitación de UDLD y la protección contra loops proporciona el nivel más alto de protección. Para obtener más información sobre una comparación de funciones entre el protector de loop y el UDLD, consulte:

- Sección *Protección contra Loops vs. Detección de Link Unidireccional* de Mejoras del Spanning-Tree Protocol usando las Funciones de Detección de Desviación de Bucle Guard y BPDU
- sección UDLD de este documento

Recomendación de Cisco

Cisco recomienda la habilitación global de la protección contra loops en una red de switch con loops físicos. Puede activar la protección contra loops globalmente 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.

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

Otras Opciones

Para los switches que no soportan una configuración global de protección contra loops, la recomendación es habilitar la función en todos los puertos individuales, que incluye los puertos de canal de puerto. Aunque no hay beneficios si habilita la protección contra loops en un puerto designado, no considere la habilitación un problema. Además, la reconvergencia de un spanning tree válido puede en realidad transformar un puerto designado en un puerto raíz, y esto hace que la función se vuelva útil en este puerto.

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

Las redes con topologías sin loops pueden, aún así, obtener beneficios con esta función en caso de que los loops se introduzcan accidentalmente. Sin embargo, la habilitación de la protección contra loops en este tipo de topología puede conducir a problemas de aislamiento de la red. Si crea una topología sin loops y desea evitar problemas de aislamiento de red, puede inhabilitar la protección contra loops de forma global o individual. No habilite la protección contra loops en links compartidos.

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

or

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

Función de Protección de Raíz de Spanning Tree

La función de protección de raíz proporciona una manera de asegurar la posición de root bridge en la red. La protección raíz se asegura de que el puerto que habilita esta función sea el puerto designado. Normalmente, los puertos root bridge son todos puertos designados, a menos que dos o más puertos del root bridge estén conectados. Si el bridge recibe BPDU STP superiores en un puerto con la función de protección de raíz habilitada, el bridge hace que este puerto ingrese a un estado STP root-inconsistent. Este estado root-inconsistent es con eficacia igual a un estado de escucha. No se reenvía tráfico a través de este puerto. De esta manera, la protección de raíz hace cumplir la posición del puente de raíz. La protección de raíz está disponible en la versión 12.1E y posterior del software del IOS de Cisco.

Información Operativa General

La protección de raíz es un mecanismo incorporado de STP. La protección de raíz no tiene un temporizador propio y depende de la recepción de BPDU solamente. Cuando la protección de raíz se aplica a un puerto, niega a este puerto la posibilidad de convertirse en un puerto raíz. Si la recepción de una BPDU desencadena una convergencia de árbol de expansión que hace que un puerto designado se convierta en un puerto raíz, el puerto se pone luego en un estado root inconsistente. Este mensaje de syslog ilustra:

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

Después de que el puerto deja de enviar BPDU superiores, vuelve a desbloquearse. A través de STP, el puerto pasa del estado de escucha al estado de aprendizaje y, finalmente, pasa al estado de reenvío. Este mensaje de syslog muestra la transición:

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

La recuperación es automática. No es necesaria ninguna intervención humana.

Debido a que la protección de raíz obliga a que se designe un puerto y la protección contra loops sólo es efectiva si el puerto es un puerto raíz o un puerto alternativo, las funciones son mutuamente excluyentes. Por lo tanto, no puede habilitar la protección contra loops y la protección de raíz en un puerto al mismo tiempo.

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

Recomendación de Cisco

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

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

EtherChannel

Propósito

EtherChannel abarca un algoritmo de distribución de tramas que multiplica eficientemente las tramas a través de los links de 10/100 Mbps o Gigabit del componente. El algoritmo de distribución de tramas permite la multiplexación inversa de varios canales en un único link lógico. Aunque cada plataforma difiere de la siguiente en implementación, debe comprender estas propiedades comunes:

- Debe haber un algoritmo para multiplicar estadísticamente las tramas a través de múltiples canales. En los switches Catalyst, esto está relacionado con el hardware. Aquí están los ejemplos:Catalyst 5500/5000: la presencia o ausencia de un Ethernet Bundling Chip (EBC) en el móduloCatalyst 6500/6000: algoritmo que puede leer más en la trama y multiplex por dirección IP
- Existe la creación de un canal lógico para que se pueda ejecutar una única instancia de STP o se pueda utilizar un único peering de ruteo, que depende de si es un EtherChannel de Capa 2 o Capa 3.
- Existe un protocolo de administración para verificar la consistencia de los parámetros en cualquiera de los extremos del link y para ayudar a administrar la recuperación de agrupamiento de la falla o adición del link. Este protocolo puede ser PAgP o protocolo de control de agregación de enlaces (LACP).

Información Operativa General

EtherChannel abarca un algoritmo de distribución de tramas que multiplica eficientemente las tramas a través de los links de 10/100 Mbps, Gigabit o 10-Gigabit del 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 asegura que, cuando se reciben las tramas, el algoritmo no causa el orden incorrecto de las tramas que forman parte de una conversación o duplicación de tramas determinadas.

Esta tabla ilustra el algoritmo de distribución de tramas en detalle para cada plataforma enumerada:

Platform	Algoritmo de Balanceo de Carga del Canal
Catalyst serie 3750	Catalyst 3750 que ejecuta el algoritmo de balanceo de carga del software Cisco IOS que utiliza direcciones MAC o direcciones IP, y el origen del mensaje o el destino del mensaje, o ambos.
Catalyst 4500 Series	Catalyst 4500 que ejecuta el algoritmo de balanceo de carga del software del IOS de Cisco que utiliza direcciones MAC, direcciones IP o números de puerto de Capa 4 (L4), y el origen del mensaje o el destino del mensaje, o ambos.
Serie Cata	Hay dos algoritmos de hash que se pueden utilizar, que dependen del hardware de Supervisor Engine. El hash es un polinomio de 17 grados que

lyst 6500 /600 0	se implementa en hardware. En todos los casos, el hash toma el número de puerto MAC, IP address o IP TCP/UDP y aplica el algoritmo para generar un valor de 3 bits. Este proceso se produce por separado tanto para las SA como para los DA. A continuación, se utiliza la operación XOR con los resultados para generar otro valor de 3 bits. El valor determina qué puerto del canal se utiliza para reenviar el paquete. Los canales en el Catalyst 6500/6000 se pueden formar entre puertos en cualquier módulo y pueden tener hasta ocho puertos.

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

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

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

Nota: Consulte estos documentos para obtener más detalles sobre el soporte de EtherChannel en otras plataformas y cómo configurar y resolver problemas de EtherChannel:

- Introducción a la Redundancia y el Balanceo de Carga de Etherchannel en Switches Catalyst
- Configuración de EtherChannel de Capa 3 y Capa 2 (Guía de Configuración de Cisco IOS Software Catalyst 6500 Series, 12.2SX)
- Configuración de EtherChannel de Capa 3 y Capa 2 (Guía de Configuración de Cisco IOS Software Catalyst 6500 Series, 12.1E)

- Configuración de EtherChannel (Guía de Configuración de Cisco IOS Software del Switch Catalyst 4500 Series, 12.2(31)SG)
- Configuración de EtherChannels (Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE)
- Configuración de EtherChannel en Switches Catalyst 4500/4000, 5500/5000 y 6500/6000 que funcionan con el software del sistema CatOS

Recomendación de Cisco

Los switches Catalyst de las series 3750, 4500 y 6500/6000 realizan el balanceo de carga mediante el hashing de las direcciones IP de origen y de destino de forma predeterminada. Esto se recomienda, suponiendo que IP es el protocolo dominante. Ejecute este comando para configurar el balanceo de carga:

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

Otras Opciones

Dependiendo de los flujos de tráfico, puede utilizar la distribución de Capa 4 para mejorar el balanceo de carga si la mayoría del tráfico se encuentra entre la misma dirección IP de origen y de destino. Debe comprender que, cuando se configura la distribución de Capa 4, el hash sólo incluye los puertos de origen y destino de Capa 4. No combina las direcciones IP de Capa 3 en el algoritmo de hash. Ejecute este comando para configurar el balanceo de carga:

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

Nota: La distribución de Capa 4 no se puede configurar en los Catalyst 3750 Series Switches.

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

Dependiendo de las plataformas de hardware, puede utilizar los comandos CLI para determinar qué interfaz en el EtherChannel reenvía el flujo de tráfico específico, con la política de distribución de tramas como base.

Para los switches Catalyst 6500, ejecute el comando **remote login switch** para iniciar sesión de forma remota en la consola Switch Processor (SP). Luego, ejecute el comando **test etherchannel load-balance interface port-channel number {ip | l4port | mac} [*source_ip_add* | *source_mac_add* | *source_l4_port*] [***dest_ip_add** | *dest_mac_add* | *dest_l4_port*]**.

Para los switches Catalyst 3750, ejecute el comando **test etherchannel load-balance interface *port-channel number* {ip | mac} [*source_ip_add* | *source_mac_add*] [*dest_ip_add* | *dest_mac_add*]**.

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

Pautas y Restricciones para la Configuración de EtherChannel

EtherChannel verifica las propiedades de todos los puertos físicos antes de agregar puertos compatibles en un solo puerto lógico. Las pautas y las restricciones de configuración varían para diversas plataformas de switch. Complete estas pautas y restricciones para evitar problemas de

agrupamiento. Por ejemplo, si se habilita QoS, los EtherChannels no se forman cuando se agrupan los módulos de switching de las series Catalyst 6500/6000 con diferentes capacidades de QoS. Para los switches Catalyst 6500 que ejecutan el Cisco IOS Software, puede inhabilitar la verificación del atributo de puerto QoS en el agrupamiento EtherChannel con el comando de interfaz de canal de puerto **no mls qos channel-consistency**. El comando **show interface capability** ***mod/port*** muestra la capacidad del puerto QoS y determina si los puertos son compatibles.

Consulte estas pautas para diferentes plataformas para evitar problemas de configuración:

- Configuración de EtherChannel de Capa 3 y Capa 2 (Guía de Configuración de Cisco IOS Software Catalyst 6500 Series, 12.2SX)
- Configuración de EtherChannel de Capa 3 y Capa 2 (Guía de Configuración de Cisco IOS Software Catalyst 6500 Series, 12.1E)
- Configuración de EtherChannel (Guía de Configuración de Cisco IOS Software del Switch Catalyst 4500 Series, 12.2(31)SG)
- Configuración de EtherChannels (Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE)

El número máximo de EtherChannels soportados también depende de la plataforma de hardware y de las versiones de software. Los switches Catalyst 6500 que ejecutan Cisco IOS Software Release 12.2(18)SXE y posteriores soportan un máximo de 128 interfaces de canal de puerto. Las versiones de software anteriores a Cisco IOS Software Release 12.2(18)SXE admiten un máximo de 64 interfaces de canal de puerto. El número de grupo configurable puede ser del 1 al 256, independientemente de la versión de software. Los switches Catalyst serie 4500 admiten un máximo de 64 EtherChannels. Para los switches Catalyst 3750, se recomienda no configurar más de 48 EtherChannels en la pila de switches.

Cálculo del Costo del Puerto del Spanning Tree

Debe comprender el cálculo del costo del puerto del árbol de expansión para EtherChannels. Puede calcular el costo del puerto del árbol de expansión para EtherChannels con el método corto o largo. De forma predeterminada, el costo del puerto se calcula en modo corto.

Esta tabla ilustra el costo del puerto del árbol de expansión para un EtherChannel de Capa 2 en base al ancho de banda:

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

Nota: En CatOS, el costo del puerto del árbol de expansión para un EtherChannel permanece igual después de la falla del link del miembro del canal de puerto. En Cisco IOS Software, el costo del puerto para EtherChannel se actualiza inmediatamente para reflejar el nuevo ancho de banda disponible. Si el comportamiento deseado es evitar cambios innecesarios en la topología del árbol

de expansión, puede configurar estáticamente el costo del puerto del árbol de expansión con el uso del comando **spanning-tree cost** *cost*.

Port Aggregation Protocol (PAgP)

Propósito

PAgP es un protocolo de administración que verifica la consistencia de los parámetros en cualquiera de los extremos del link. PAgP también ayuda al canal con la adaptación a la falla o adición del link. Estas son las características de PAgP:

- PAgp requiere que todos los puertos del canal pertenezcan a la misma VLAN o estén configurados como puertos trunk. Debido a que las VLAN dinámicas pueden forzar el cambio de un puerto a una VLAN diferente, las VLAN dinámicas no se incluyen en la participación de EtherChannel.
- Cuando ya existe un agrupamiento y se modifica la configuración de un puerto, todos los puertos del agrupamiento se modifican para que coincidan con esa configuración. Un ejemplo de tal cambio es un cambio en la VLAN o un cambio en el modo `troncal`.
- 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 físico (o lógico) individual que se va a agrupar. La misma dirección MAC de grupo multicast que se utiliza para los paquetes CDP se utiliza para enviar paquetes PAgP. La dirección MAC es 01-00-0c-cc-cc-cc. Pero el valor del protocolo es 0x0104. Este es un resumen del funcionamiento del protocolo:

- Mientras el puerto físico esté activo, los paquetes PAgP se transmiten cada segundo durante la detección y cada 30 segundos en estado estable.
- Si se reciben paquetes de datos pero no se reciben paquetes PAgP, se asume que el puerto está conectado a un dispositivo que no es apto para PAgP.
- Escuche los paquetes PAgP que prueban que el puerto físico tiene una conexión bidireccional a otro dispositivo compatible con PAgP.
- Tan pronto como se reciban dos de estos paquetes en un grupo de puertos físicos, intente formar un puerto agregado.
- Si los paquetes PAgP se detienen durante un período, el estado de PAgP se derriba.

Procesamiento Normal

Estos conceptos ayudan a demostrar el comportamiento del protocolo:

- Puerto agregado: puerto lógico que se compone de todos los puertos físicos en la misma agregación y se puede identificar por su propio ifIndex SNMP. Un puerto agregado no contiene puertos no operativos.
- Canal: una agregación que cumple los criterios de formación. Un canal puede contener puertos no operativos y es un superconjunto de puerto agregado. Los protocolos, que incluyen STP y VTP pero excluyen CDP y DTP, se ejecutan sobre PAgP sobre los puertos agregados. Ninguno de estos protocolos puede enviar o recibir paquetes hasta que PAgP conecte los puertos agregados a uno o más puertos físicos.

- Capacidad de grupo: cada puerto físico y puerto agregado posee un parámetro de configuración que se denomina `capacidad de grupo`. Un puerto físico se puede agregar con cualquier otro puerto físico que tenga la misma `capacidad de grupo`, y solamente con tal puerto físico.
- Procedimiento de agregación: cuando un puerto físico alcanza el estado `UpData` o `UpPAgP`, el puerto se conecta a un puerto agregado apropiado. Cuando el puerto deja cualquiera de esos estados para otro estado, el puerto se desconecta del puerto agregado.

Esta tabla proporciona más detalles sobre los estados:

Estado	Significado
`UpData`	No se han recibido paquetes PAgP. Se envían paquetes PAgP. El puerto físico es el único puerto conectado al puerto agregado. Los paquetes que no son de PAgP se transmiten 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 que no son de PAgP se transmiten entre el puerto físico y el puerto agregado.

Ambos extremos de ambas conexiones deben coincidir en la agrupación. La agrupación se define como el grupo más grande de puertos en el puerto agregado que ambos extremos de la conexión permiten.

Cuando un puerto físico alcanza el estado `UpPAgP`, el puerto se asigna al puerto agregado que tiene puertos físicos miembro que coinciden con la `capacidad de grupo` del nuevo puerto físico y que están en el estado `BiDir` o el estado `UpPAgP`. Dichos puertos `BiDir` se mueven al estado `UpPAgP` al mismo tiempo. Si no hay ningún puerto agregado que tenga parámetros de puerto físico constituyentes que sean compatibles con el puerto físico recién preparado, el puerto se asigna a un puerto agregado con parámetros adecuados que no tienen puertos físicos asociados.

Un tiempo de espera PAgP puede ocurrir en el último vecino conocido en el puerto físico. El puerto que agota el tiempo de espera se elimina del puerto agregado. Al mismo tiempo, se quitan todos los puertos físicos del mismo puerto agregado que tienen temporizadores que también han 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 falla un link en un canal que existe, el puerto agregado se actualiza y el tráfico se desvía por los links que permanecen sin pérdidas. Entre los ejemplos de tal falla se incluyen:

- El puerto está desconectado
- Se elimina el convertidor de interfaz Gigabit (GBIC)
- La fibra está rota

Nota: Cuando falla un link en un canal con una apagado o eliminación de un módulo, el comportamiento puede ser diferente. Por definición, un canal requiere dos puertos físicos. Si se pierde un puerto del sistema en un canal de dos puertos, el puerto agregado lógico se desconecta y el puerto físico original se reinicializa con respecto al árbol de expansión. El tráfico se puede descartar hasta que el STP permita que el puerto vuelva a estar disponible para los datos.

Esta diferencia en los dos modos de falla es importante cuando planifica el mantenimiento de una red. Puede haber un cambio en la topología STP del cual debe tener en cuenta al realizar una extracción o inserción en línea de un módulo. Debe administrar cada link físico del canal con el sistema de administración de red (NMS) porque el puerto agregado puede permanecer inalterado a causa de una falla.

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

- Si se utiliza un solo puerto por módulo para formar un canal, utilice tres o más módulos (tres en total).
- Si el canal abarca dos módulos, utilice dos puertos en cada módulo (cuatro en total).
- Si se necesita un canal de dos puertos entre dos tarjetas, utilice solamente los puertos de Supervisor Engine.

Opciones de Configuración

Puede configurar EtherChannels de diferentes modos, como se resume en esta tabla:

Modo	Opciones Configurables
`Encendido`	El PAgP no está en funcionamiento. El puerto canaliza, independientemente de cómo se configure el puerto vecino. Si el puerto del vecino está encendido se forma un canal.
`Auto`	La agregación está bajo el control de PAgP. Un puerto se coloca en un estado de negociación pasivo. No se envían paquetes PAgP en la interfaz hasta que se recibe al menos un paquete PAgP que indica que el remitente funciona en el modo `deseable`.
`Deseable`	La agregación está bajo el control de PAgP. Un puerto se coloca en un estado de negociación activo, en el que el puerto inicia negociaciones con otros puertos a través de la transmisión de paquetes PAgP. Un canal está formado con otro grupo de puertos, ya sea en modo deseable o automático.
`No silencioso` Éste es el valor predeter	Un modo de palabra clave automático o deseable. Si no se recibe ningún paquete de datos en la interfaz, la interfaz nunca se conecta a un puerto agregado y no se puede utilizar para datos. Esta verificación de bidireccionalidad se proporcionó para el

minado en los puertos de fibra FE y GE de Catalyst 5500/5000.	hardware específico de Catalyst 5500/5000 porque algunos fallos de link provocan una ruptura del canal. Cuando habilita el modo `no silencioso`, nunca se permite que un puerto vecino que se recupera vuelva y divida el canal innecesariamente. El agrupamiento más flexible y las comprobaciones de bidireccionalidad mejoradas están presentes de forma predeterminada en el hardware de las series Catalyst 4500/4000 y 6500/6000.
`Silent` Esta es la opción predeterminada en todos los puertos Catalyst 6500/6000 y 4500/4000, así como en los puertos de cobre 5500/5000.	Un modo de palabra clave automático o deseable. Si no se recibe ningún paquete de datos en la interfaz, después de un período de tiempo de espera de 15 segundos, la interfaz se conecta sola a un puerto agregado. Por lo tanto, la interfaz se puede utilizar para la transmisión de datos. `El modo silencioso además permite la operación del canal en el caso de un socio que puede ser un analizador o un servidor que nunca envía PAgP.`

La configuración `silenciosa/no silenciosa` afecta la forma en que los puertos reaccionan a las situaciones que causan tráfico unidireccional. Cuando un puerto no puede transmitir debido a una interfaz física fallida o a una fibra o cable rotos, el puerto vecino todavía puede permanecer en estado operativo. El partner continúa transmitiendo datos. Sin embargo, los datos se pierden porque no se puede recibir tráfico de retorno. Los loops de árbol de expansión también pueden formarse debido a la naturaleza unidireccional del link.

Algunos puertos de fibra tienen la capacidad deseada para llevar el puerto a un estado no operativo cuando el puerto pierde su señal de recepción (FEFI). Esta acción hace que el puerto del partner no funcione y hace que los puertos en ambos extremos del link se desactiven de forma efectiva.

Cuando utiliza dispositivos que transmiten datos (BPDU) y no puede detectar condiciones unidireccionales, utilice el modo `no silencioso` para permitir que los puertos permanezcan inoperativos hasta que estén presentes los datos de recepción y se verifique que el enlace sea bidireccional. El tiempo que el PAgP tarda en detectar un link unidireccional es de aproximadamente 3,5 * 30 segundos = 105 s. Treinta segundos es el tiempo entre dos mensajes PAgP sucesivos. Use el UDLD, que es el detector más rápido de enlaces unidireccionales.

Cuando utiliza dispositivos que no transmiten datos, utilice el modo `silencioso`. El uso del modo `silencioso` fuerza al puerto a conectarse y funcionar, independientemente de si los datos recibidos están presentes o no. Además, para los puertos que pueden detectar la presencia de una

condición unidireccional, el modo `silencioso` se utiliza de forma predeterminada. Ejemplos de estos puertos son las plataformas más recientes que utilizan FEFI y UDLD de Capa 1.

Para desactivar la canalización en una interfaz, ejecute el comando **no channel-group** *number* :

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

Verificación

La tabla de esta sección proporciona un resumen de todos los posibles escenarios de modo de canalización PAgP entre dos switches conectados directamente, el Switch A y el Switch B. Algunas de estas combinaciones pueden hacer que el STP coloque los puertos en el lado de canalización en el estado `errDisable`, lo que significa que esas combinaciones apagan los puertos en el lado de canalización. La función EtherChannel misconfiguration guard está habilitada de forma predeterminada.

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 PAgP)	Canal (no PAgP)
Encendido	No configurado	Sin Canal (puerto errDisable)	Sin Canal
Encendido	Auto	Sin Canal (puerto errDisable)	Sin Canal
Encendido	Deseable	Sin Canal (puerto errDisable)	Sin Canal
No configurado	Encendido	Sin Canal	Sin Canal (puerto errDisable)
No configurado	No configurado	Sin Canal	Sin Canal
No configurado	Auto	Sin Canal	Sin Canal
No configurado	Deseable	Sin Canal	Sin Canal
Auto	Encendido	Sin Canal	Sin Canal (puerto errDisable)
Auto	No configurado	Sin Canal	Sin Canal
Auto	Auto	Sin Canal	Sin Canal
Auto	Deseable	Canal PAgP	Canal PAgP
Deseable	Encendido	Sin Canal	Sin Canal
Deseable	No	Sin Canal	Sin Canal

	configurado		
Deseable	Auto	Canal PAgP	Canal PAgP
Deseable	Deseable	Canal PAgP	Canal PAgP

Recomendación de configuración de Cisco para canales L2

Habilite PAgP y use un ajuste de `desirable-desirable` en todos los links EtherChannel. Consulte este resultado para obtener más información:

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

Verifique la configuración de esta manera:

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

Evitar errores de configuraciones de EtherChannel

Puede configurar mal un EtherChannel y crear un loop de árbol de expansión. Este error de configuración puede saturar el proceso del switch. El software del sistema Cisco IOS incluye la **función de configuración incorrecta de la protección EtherChannel del árbol de expansión** para evitar este problema.

Ejecute este comando de configuración en todos los switches Catalyst que ejecutan Cisco IOS Software como software del sistema:

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

Otras Opciones

Al canalizar dos dispositivos que no soportan PAgP pero que soportan LACP, la recomendación es habilitar LACP con la configuración de LACP activo en ambos extremos de los dispositivos. Consulte la sección Protocolo de control de agregación de enlaces (LACP) de este documento para obtener más información.

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

- Servidores
- Director local
- Switches de contenido
- Routers
- Switches con software anterior
- Switches Catalyst 2900XL/3500XL

- Catalyst 8540

Ejecute estos comandos:

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

Protocolo de control de agregación de enlaces (LACP)

El LACP es un protocolo que permite a los puertos con características similares formar un canal a través de la negociación dinámica con switches contiguos. PAgP es un protocolo propiedad de Cisco que sólo puede ejecutarse en los switches de Cisco y en los switches que liberan los proveedores con licencia. 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.

LACP es compatible con estas plataformas y versiones:

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

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

- Velocidad
- Dúplex
- VLAN nativa y tipo de enlace troncal

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

- El protocolo LACP sólo puede ejecutarse en puertos dúplex completo y no admite puertos semidúplex.
- El protocolo LACP admite puertos en espera activos. 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 agregar todos los puertos compatibles (por ejemplo, si el sistema remoto tiene limitaciones de hardware más restrictivas), todos los puertos que no se pueden incluir activamente en el canal se ponen en estado de espera activo y se utilizan sólo si uno de los puertos usados falla.

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

Información Operativa General

El LACP controla cada puerto físico (o lógico) individual que se va a agrupar. Los paquetes LACP se envían con el uso de la dirección MAC del grupo 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 periódicamente en cada enlace agregable.
- 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 agregable escuchan la información que se envía dentro del protocolo y deciden qué acciones o acciones tomar.
- Los puertos compatibles se configuran en un canal, hasta el 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 (por ejemplo, debido a una falla de link), los partners del protocolo agotan el tiempo de espera y toman las medidas adecuadas en función del nuevo estado del sistema.
- Además de las transmisiones periódicas de la unidad de datos LACP (LACPDU), si se produce un cambio en la información de estado, el protocolo transmite una LACPDU impulsada por eventos a los partners. Los partners del protocolo toman las medidas apropiadas en función del nuevo estado del sistema.

Parámetros LACP

Para que el LACP pueda determinar si un conjunto de links se conecta al mismo sistema y si esos links son compatibles desde el punto de vista de la agregación, es necesario poder establecer:

- Un identificador global único para cada sistema que participa en la agregación del link.A cada sistema que ejecuta LACP se le debe asignar una prioridad que puede elegir automáticamente (con la prioridad predeterminada 32768) o por el administrador. La prioridad del sistema se utiliza principalmente en conjunto con una dirección MAC del sistema para formar el identificador de sistema.
- Un medio para identificar el conjunto de capacidades asociadas con cada puerto y con cada agregador, tal como lo entiende un sistema dado.A cada puerto del sistema se le debe asignar una prioridad automáticamente (con la prioridad predeterminada de 128) o por el administrador. La prioridad se utiliza en conjunto con el número de puerto para formar el identificador del puerto.
- Un medio para identificar un grupo de agregación de enlaces y su agregador asociado.La capacidad de un puerto para agregarse con otro se resume en un simple parámetro entero de 16 bits estrictamente mayor que cero al que se denomina clave. Cada clave se determina sobre la base de diferentes factores, tales como:Las características físicas del puerto, que incluyen la velocidad de datos, la duplexidad y el medio punto a punto o compartidoRestricciones de configuración establecidas por el administrador de redDos claves se asocian a cada puerto:Una clave administrativaUna clave operativaLa clave administrativa permite que la administración manipule los valores clave y, por lo tanto, el usuario puede elegir esta clave. El sistema utiliza la clave operativa para formar agregaciones. El usuario no puede elegir ni cambiar directamente esta clave. Se dice que el conjunto de puertos en un sistema determinado que comparten el mismo valor de clave operativa son miembros del mismo grupo de claves.

Por lo tanto, dados dos sistemas y un conjunto de puertos con la misma clave administrativa, cada sistema intenta agregar los puertos, comenzando desde el puerto con la prioridad más alta en el sistema de mayor prioridad. Este comportamiento es posible porque cada sistema conoce estas prioridades:

- Su propia prioridad, que el usuario o el software asignaron
- Su prioridad de partner, que se descubrió a través de paquetes LACP

Comportamiento en caso de Fallas

El comportamiento de falla para el LACP es el mismo que el comportamiento de falla para el PAgP. Si falla un link en un canal existente (por ejemplo, si se desconecta un puerto, se elimina un GBIC o se rompe una fibra), se actualiza el puerto agregado y el tráfico se divide en los links restantes en un segundo. Cualquier tráfico que no requiera un redireccionamiento después de la falla (que es el tráfico que continúa enviándose en el mismo link) no sufre ninguna pérdida. El restablecimiento del link fallido activa otra actualización en el puerto agregado y el tráfico se bloquea de nuevo.

Opciones de Configuración

Puede configurar los EtherChannels de LACP en diferentes modos, como se resume 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.
Apagado (o no configurado)	El puerto no está canalizando, independientemente de cómo se configura el vecino.
Pasivo (valor predeterminado)	Esto es similar al modo automático en PagP. El switch no inicia el canal, pero entiende los paquetes LACP entrantes. El par (en estado activo) inicia la negociación (enviando un paquete LACP) que el switch recibe y a la que responde el switch, formando finalmente el canal de agregación con el par.
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.

El LACP utiliza un temporizador de intervalo de 30 segundos (Slow_Periodic_Time) después de establecer los EtherChannels de LACP. El número de segundos antes de la invalidación de la información LACPDU recibida cuando se utilizan tiempos de espera largos (3 veces el tiempo_periódico_lento) es 90. Se recomienda el UDLD como un detector más rápido de links unidireccionales. No puede ajustar los temporizadores LACP y, en este punto, no puede configurar los switches para que utilicen la transmisión de unidad de datos de protocolo rápido (PDU) (cada segundo) para mantener el canal después de que se forme el canal.

Verificación

La tabla de esta sección proporciona un resumen de todos los posibles escenarios de modo de

canalización de LACP entre dos switches conectados directamente (los switches A y B). Algunas de estas combinaciones pueden hacer que la protección EtherChannel coloque los puertos en el lado de canalización en el estado errdisable. La función EtherChannel misconfiguration guard está habilitada de forma predeterminada.

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	Sin Canal (puerto errDisable)	Sin Canal
Encendido	Pasivo	Sin Canal (puerto errDisable)	Sin Canal
Encendido	Activo	Sin Canal (puerto 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

Recomendaciones de Cisco

Cisco recomienda habilitar PAgP en las conexiones de canales entre los switches de Cisco. Al canalizar dos dispositivos que no soportan PAgP pero que soportan LACP, la recomendación es habilitar LACP con la configuración de LACP activo en ambos extremos de los dispositivos.

En los switches que ejecutan CatOS, todos los puertos en un Catalyst 4500/4000 y un Catalyst 6500/6000 utilizan el protocolo de canal PAgP de forma predeterminada. Para configurar los puertos para utilizar el LACP, debe configurar el protocolo de canal en los módulos en el LACP. El LACP y el PAgP no pueden ejecutarse en el mismo módulo de los switches que ejecutan CatOS. Esta limitación no se aplica a los switches que ejecutan Cisco IOS Software. Los switches que ejecutan Cisco IOS Software pueden soportar PAgP y LACP en el mismo módulo. Ejecute estos comandos para configurar el modo de canal LACP en activo y asignar un número de clave administrativa:

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

El comando **show etherchannel summary** muestra un resumen de una línea por grupo de canales que incluye esta información:

- Números de grupo
- Números de canal de puerto

- Estado de los puertos
- Los puertos que forman parte del canal

El comando **show etherchannel port-channel** muestra información detallada del canal de puerto para todos los grupos de canales. El resultado incluye esta información:

- Estado del canal
- Protocolo que se utiliza
- El tiempo transcurrido desde que se empaquetaron los puertos

Para mostrar información detallada para un grupo de canales específico, con los detalles de cada puerto mostrados por separado, utilice el comando **show etherchannel** *channel_number* **detail**. El resultado del comando incluye los detalles del partner y los detalles del canal del puerto. Consulte Configuración de LACP (802.3ad) entre un Catalyst 6500/6000 y un Catalyst 4500/4000 para obtener más información.

Otras Opciones

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

- Servidores
- Director local
- Switches de contenido
- Routers
- Switches con software antiguo
- Switches Catalyst 2900XL/3500XL
- Catalyst 8540

Ejecute estos comandos:

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

Detección de Link Unidireccional

Propósito

UDLD es propiedad de Cisco, protocolo liviano desarrollado para detectar instancias de comunicaciones unidireccionales entre los dispositivos. Existen otros métodos para detectar el estado bidireccional de los medios de transmisión, como FEFI. Sin embargo, hay casos en los que los mecanismos de detección de Capa 1 no son suficientes. Estos escenarios pueden dar como resultado:

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

La función UDLD aborda estas condiciones de falla en las interfaces Ethernet de fibra y cobre:

- Monitorea las configuraciones físicas de cableado: se apaga como `errDisabled` cualquier puerto con cables incorrectos.

- Protege contra links unidireccionales: cuando se detecta un link unidireccional que ocurre debido a un mal funcionamiento de medios o de puertos/interfaces, el puerto afectado se apaga como `errDisabled`. Se genera un mensaje syslog correspondiente.
- Además, el modo agresivo UDLD verifica que un link bidireccional previamente considerado no pierda conectividad en el caso de que el link se vuelva inutilizable debido a la congestión. El modo agresivo UDLD realiza pruebas de conectividad continuas a través del link. El propósito principal del modo agresivo UDLD es evitar la retención en negro del tráfico en ciertas condiciones fallidas que no son tratadas por el UDLD del modo normal.

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

El árbol de expansión tiene un flujo de BPDU unidireccional de estado estable y puede tener las fallas que se enumeran en esta sección. Un puerto puede fallar repentinamente en transmitir BPDU, lo que causa un cambio de estado STP desde el `bloqueo` al `reenvío` en el vecino. Sin embargo, todavía existe un loop porque el puerto aún puede recibir.

Información Operativa General

UDLD es un protocolo de Capa 2 que funciona sobre la capa LLC (destino MAC 01-00-0c-cc-cc-cc, SNAP HDLC tipo de protocolo 0x0111). Cuando ejecuta UDLD en combinación con FEFI y los mecanismos de la Capa 1 de negociación automática, puede validar la integridad física (L1) y lógica (L2) de un link.

UDLD tiene disposiciones para las características y protección que FEFI y la negociación automática no pueden realizar. Estas funciones incluyen:

- La detección y la caché de la información del vecino
- El cierre de cualquier puerto mal conectado
- Detección de fallas o mal funcionamiento de interfaz lógica/puerto en links que no son punto a punto**Nota:** Cuando los links no son punto a punto, atraviesan los conversores de medios o los concentradores.

El UDLD emplea estos dos mecanismos básicos.

1. UDLD aprende los vecinos y mantiene la información actualizada en una memoria caché local.
2. El UDLD envía un tren de sondas/mensajes de eco (hello) UDLD a la detección de un nuevo vecino o cuando un vecino solicita una resincronización de la memoria caché.

El UDLD envía constantemente sondas/mensajes de eco en todos los puertos. Al recibir un mensaje UDLD correspondiente en un puerto, se activa una fase de detección y un proceso de validación. El puerto se habilita si se cumplen todas las condiciones válidas. Las condiciones se cumplen si el puerto es bidireccional y está correctamente cableado. Si no se cumplen las condiciones, el puerto es `errDisabled`, lo que activa este mensaje de syslog:

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
```

```
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

Para obtener una lista completa de mensajes del sistema por función, que incluye eventos UDLD, refiérase a Mensajes UDLD (Mensajes del Sistema Cisco IOS, Volumen 2 de 2).

Después del establecimiento de un link y su clasificación como bidireccional, el UDLD continúa anunciando sondas/mensajes de eco en un intervalo predeterminado de 15 s.

Esta tabla proporciona información sobre los estados del puerto:

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

Mantenimiento de caché de vecino

El UDLD envía periódicamente paquetes hello de sonda/eco en cada interfaz activa para mantener la integridad de la memoria caché del vecino UDLD. En la recepción de un mensaje hello, el mensaje se almacena en memoria caché durante un período máximo, que se define como el tiempo de espera. Cuando caduca el tiempo de espera, la entrada de caché respectiva se desactualiza. Si se recibe un nuevo mensaje hello dentro del período de espera, el nuevo mensaje reemplaza la entrada anterior y se restablece el temporizador de tiempo de vida correspondiente.

Siempre que se inhabilita una interfaz habilitada para UDLD o cuando se reinicia un dispositivo, se borran todas las entradas de caché existentes para las interfaces a las que afecta el cambio de configuración. Esta limpieza mantiene la integridad de la memoria caché UDLD. El UDLD transmite al menos un mensaje para informar a los vecinos respectivos de la necesidad de vaciar las entradas de caché correspondientes.

Mecanismo de detección de eco

El mecanismo de eco forma la base del algoritmo de detección. Siempre que un dispositivo UDLD se entera de un nuevo vecino o recibe una solicitud de resincronización de un vecino fuera de sincronización, el dispositivo inicia o reinicia la ventana de detección en su lado de la conexión y envía una ráfaga de mensajes de eco en respuesta. Debido a que este comportamiento debe ser el mismo en todos los vecinos, el remitente de eco espera recibir ecos en respuesta. Si la ventana de detección finaliza sin recibir ningún mensaje de respuesta válido, el link se considera unidireccional. A partir de este punto, se puede activar un proceso de restablecimiento de link o cierre de puerto. Otras condiciones anómalas poco comunes para las que el dispositivo verifica son:

- Fibras de transmisión con bucle invertido (Tx) al conector Rx del mismo puerto
- Fallos de cableado en el caso de una interconexión de medios compartida (por ejemplo, un concentrador o un dispositivo similar)

Tiempo de Convergencia

Para evitar loops STP, Cisco IOS Software Release 12.1 y posteriores han reducido el intervalo de mensajes predeterminado UDLD de 60 segundos a 15 segundos. Este intervalo se modificó para cerrar un link unidireccional antes de que un puerto anteriormente bloqueado en el árbol de expansión 802.1D pueda pasar a un estado de reenvío. El valor del intervalo de mensajes determina la velocidad en la que un vecino envía las sondas UDLD después de la fase de conexión o de detección. El intervalo de mensaje no necesita coincidir con ambos extremos de un link, aunque la configuración coherente sea deseable, en lo posible. Cuando se establecen los vecinos UDLD, el intervalo de mensaje configurado se envía al vecino y el intervalo de tiempo de espera para ese par se calcula como:

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

Como tal, una relación de peer se agota el tiempo de espera después de que se pierdan tres saludos (o sondas) consecutivos. Debido a que los intervalos de mensajes son diferentes en cada lado, este valor de tiempo de espera es simplemente diferente en cada lado, y un lado reconoce una falla más rápidamente.

El tiempo aproximado necesario para que el UDLD detecte una falla unidireccional de un link previamente estable es aproximadamente:

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

Esto es aproximadamente 41 segundos con el intervalo de mensajes predeterminado de 15 segundos. Esta cantidad de tiempo es mucho más corta que los 50 segundos que generalmente son necesarios para que el STP vuelva a converger. Si la CPU de NMP tiene algunos ciclos de repuesto y si el usuario monitorea cuidadosamente su nivel de utilización (una buena práctica), es aceptable una reducción del intervalo de mensajes (par) al mínimo de 7 segundos. Además, esta reducción del intervalo de mensajes ayuda a acelerar la detección por un factor significativo.

Nota: El mínimo es 1 segundo en la versión 12.2(25)SEC del software del IOS de Cisco.

Por lo tanto, el UDLD tiene una dependencia asumida de los temporizadores del spanning tree predeterminado. Si el STP está configurado para converger más rápidamente que el UDLD, considere un mecanismo alternativo, como la función de protección contra loops STP. Considere un mecanismo alternativo en este caso cuando implemente RSTP (802.1w) también, porque RSTP tiene características de convergencia en ms, dependiendo de la topología. Para estas instancias, utilice la protección contra loops junto con el UDLD para proporcionar la mayor protección posible. La protección contra loops evita loops STP con la velocidad de la versión STP que está en uso. Y UDLD se encarga de la detección de conexiones unidireccionales en links EtherChannel individuales o en casos en los que las BPDU no fluyen a lo largo de la dirección rota.

Nota: El UDLD es independiente del STP. El UDLD no detecta todas las situaciones de falla de STP, como aquellas fallas causadas por una CPU que no envía BPDU por un tiempo mayor que (2 * Fwddelay + maxage). Por esta razón, Cisco recomienda implementar UDLD junto con la protección contra loops en topologías que dependen del STP.

Precaución: Tenga cuidado con las versiones anteriores del UDLD en los switches 2900XL/3500XL que utilizan un intervalo de mensajes predeterminado no configurable de 60 segundos. Son susceptibles a las condiciones del loop del árbol de expansión.

Modo Agresivo UDLD

Se creó un UDLD agresivo para abordar específicamente aquellos pocos casos en los que se necesita una prueba continua de conectividad bidireccional. Como tal, la característica del modo agresivo proporciona protección mejorada contra las condiciones peligrosas de link unidireccional en estas situaciones:

- Cuando la pérdida de PDU UDLD es simétrica y ambos extremos agotan el tiempo de espera. En este caso, ninguno de los puertos está inhabilitado.
- Un lado de un link tiene un puerto atascado (tanto Tx como Rx).
- Un lado del link permanece arriba mientras que el otro lado desciende.
- La negociación automática u otro mecanismo de detección de fallas de Capa 1 está inhabilitado.
- Es deseable reducir la dependencia de los mecanismos FEFI de Capa 1.
- Necesita la máxima protección contra fallas de link unidireccional en links FE/GE punto a punto. Específicamente, cuando no se admite falla entre dos vecinos, las sondas UDLD agresivas pueden considerarse como latidos del corazón, cuya presencia garantiza la salud del link.

El caso más común para una implementación de UDLD agresiva es realizar la verificación de conectividad en un miembro de un paquete cuando la negociación automática u otro mecanismo de detección de fallas de Capa 1 está inhabilitado o inutilizable. Es particularmente útil con las conexiones EtherChannel porque PAgP y LACP, aunque estén activados, no utilizan temporizadores hello muy bajos en estado estable. En este caso, el UDLD agresivo tiene la ventaja añadida de prevenir posibles loops de árbol de expansión.

Es importante comprender que el modo normal UDLD verifica si hay una condición de link unidireccional, incluso después de que un link alcanza el estado bidireccional. El UDLD tiene la intención de detectar problemas de Capa 2 que causan loops STP, y esos problemas son generalmente unidireccionales (porque las BPDU fluyen solamente en una dirección en estado estable). Por lo tanto, el uso de UDLD normal junto con la negociación automática y la protección contra loops (para redes que dependen de STP) es casi siempre suficiente. Con el modo UDLD agresivo habilitado, después de que todos los vecinos de un puerto hayan caducado, ya sea en el anuncio o en la fase de detección, el modo UDLD agresivo reinicia la secuencia de link en un esfuerzo por resincronizarse con cualquier vecino potencialmente fuera de sincronización. Si después de un tren rápido de mensajes (ocho reintentos fallidos) el link todavía se considera indeterminado, el puerto se pone en el estado errdisable.

Nota: Algunos switches no son aptos para UDLD agresivos. Actualmente, Catalyst 2900XL y Catalyst 3500XL tienen intervalos de mensajes codificados de 60 segundos. Esto no se considera lo suficientemente rápido como para protegerse frente a loops STP potenciales (con los parámetros STP predeterminados asumidos).

Recuperación Automática de Links UDLD

La recuperación errdisable global se inhabilita de forma predeterminada. Después de habilitarlo globalmente, si un puerto entra en el estado errdisable, 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. Dependiendo de la versión de software, puede prevenir manualmente una habilitación de puerto si configura el tiempo de espera errdisable para ese puerto para inhabilitar con el uso del mecanismo de recuperación de tiempo de espera errdisable para el UDLD:

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

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

Consulte errdisable recovery (Referencia de Comandos de Catalyst 6500 Series Cisco IOS, 12.1 E) para obtener más detalles sobre cómo configurar un período de tiempo de espera para los puertos en estado errdisable.

La recuperación de Errdisable puede ser especialmente importante para el UDLD en la capa de acceso cuando los switches de acceso se distribuyen a través de un entorno de campus y la visita manual de cada switch para volver a habilitar ambos links ascendentes lleva un tiempo considerable.

Cisco no recomienda errdisable recovery en el núcleo de la red porque normalmente hay varios puntos de entrada en un núcleo y la recuperación automática en el núcleo puede provocar problemas recurrentes. Por lo tanto, debe volver a habilitar manualmente un puerto en el núcleo si UDLD inhabilita el puerto.

UDLD en los Links Ruteados

Para el propósito de esta discusión, un link enrutado es uno de estos dos tipos de conexión:

- Punto a punto entre dos nodos de router (configurados con una máscara de subred de 30 bits)
- Una VLAN con varios puertos pero que soporta solamente las conexiones ruteadas, como en una topología de núcleo de Capa 2 dividida

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

Nota: Una falla de Capa 1 o Capa 2 en cualquier red enrutada punto a punto da como resultado la eliminación casi inmediata de la conexión de Capa 3. Debido a que el único puerto del switch en esa VLAN pasa a un estado no conectado en caso de falla de Capa 1/Capa 2, la función de estado automático de la interfaz sincroniza los estados del puerto de Capa 2 y Capa 3 en aproximadamente dos segundos y coloca la interfaz VLAN de Capa 3 en un estado activo/inactivo (el protocolo de línea está inoperativo).

Si asume los valores predeterminados del temporizador, OSPF envía mensajes hello cada 10 segundos y tiene un intervalo muerto de 40 segundos (4 * hello). Estos temporizadores son constantes para el OSPF de punto a punto y las redes de broadcast. Debido a que OSPF requiere comunicación bidireccional para formar una adyacencia, el tiempo de conmutación por fallas en peor situación es de 40 segundos. Esto es cierto incluso si la falla de la Capa 1/Capa 2 no es pura en una conexión punto a punto y deja un escenario a medio cocer con el cual el protocolo de Capa 3 debe tratar. Debido a que el tiempo de detección del UDLD es muy similar al tiempo de detección de un temporizador OSPF muerto que caduca (aproximadamente 40 segundos), las ventajas de la configuración del modo normal UDLD en un link punto a punto de Capa 3 OSPF

son limitadas.

En muchos casos, EIGRP converge más rápido que OSPF. Pero es importante tener en cuenta que la comunicación bidireccional no es un requisito para que los vecinos intercambien información de ruteo. En escenarios de fallas semirelaborados muy específicos, EIGRP es vulnerable a la retención en negro del tráfico que dura hasta que algún otro evento traiga las rutas a través de ese vecino activo. El modo normal UDLD puede aliviar estas circunstancias porque detecta la falla del link unidireccional y el error inhabilita el puerto.

Para las conexiones enrutadas de Capa 3 que utilizan cualquier protocolo de ruteo, el UDLD normal todavía proporciona protección contra problemas que están presentes en la activación inicial del link, como cableado incorrecto o hardware defectuoso. Además, el modo agresivo UDLD proporciona estas ventajas en las conexiones enrutadas de capa 3:

- Evita la retención en negro innecesaria del tráfico (se requieren temporizadores mínimos en algunos casos)
- Coloca un link inestable en el estado errdisable
- Protege contra loops que se derivan de configuraciones EtherChannel de Capa 3

Comportamiento predeterminado del UDLD

El UDLD está globalmente desactivado y preparado para la habilitación en puertos de fibra de manera predeterminada. Debido a que el UDLD es un protocolo de infraestructura que se necesita solamente entre los switches, el UDLD se inhabilita de forma predeterminada en los puertos de cobre, que tienden a utilizarse para el acceso del host. Tenga en cuenta que debe habilitar el UDLD globalmente y en el nivel de interfaz antes de que los vecinos puedan alcanzar el estado bidireccional. El intervalo de mensajes predeterminado es de 15 segundos. Sin embargo, el intervalo de mensajes predeterminado puede mostrarse como siete segundos en algunos casos. Consulte Cisco bug ID CSCea70679 (sólo clientes registrados) para obtener más información. El intervalo de mensajes predeterminado se puede configurar entre 7 y 90 segundos, y el modo agresivo UDLD se inhabilita. Cisco IOS Software Release 12.2(25)SEC reduce aún más este temporizador mínimo a un segundo.

Recomendación de configuración de Cisco

En la gran mayoría de los casos, Cisco recomienda que habilite el modo normal UDLD en todos los links FE/GE punto a punto entre los switches de Cisco, y establezca el intervalo de mensajes UDLD en 15 segundos cuando utilice temporizadores de árbol de expansión 802.1D predeterminados. Además, cuando las redes dependen del STP para la redundancia y la convergencia (lo que significa que hay uno o más puertos en el estado de bloqueo de STP en la topología), utilice el UDLD junto con las características y protocolos apropiados. Estas funciones incluyen FEFI, negociación automática, protección contra loops, etc. Normalmente, si se habilita la negociación automática, el modo agresivo no es necesario porque la negociación automática compensa la detección de fallas en la Capa 1.

Ejecute una de estas dos opciones de comando para habilitar el UDLD:

Nota: La sintaxis ha cambiado en varias plataformas/versiones.

-

```
udld enable
!--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.
```

```
udld port
```

or

-

```
udld enable
!--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled
by individual port command.
```

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

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

Los comandos de configuración global **errdisable recovery cause udld** y **errdisable recovery interval** *se pueden utilizar para recuperarse automáticamente del estado UDLD error-disabled.*

Cisco recomienda que sólo utilice el mecanismo de recuperación errdisable en la capa de acceso de la red, con temporizadores de recuperación de 20 minutos o más, si el acceso físico al switch es difícil. La mejor situación es permitir tiempo para la estabilización y solución de problemas de la red, antes de que el puerto vuelva a estar en línea y cause inestabilidad en la red.

Cisco recomienda que *no* utilice los mecanismos de recuperación en el núcleo de la red porque esto puede causar inestabilidad relacionada con los eventos de convergencia cada vez que se vuelve a activar un link defectuoso. El diseño redundante de una red de núcleo proporciona una trayectoria de respaldo para un link fallido y permite tiempo para una investigación de los motivos de falla del UDLD.

Utilizar UDLD sin protección de loop STP

En el caso de los links de capa 3 punto a punto o de capa 2 donde existe una topología STP sin loops (sin bloqueo de puertos), Cisco recomienda que habilite el UDLD agresivo en los links FE/GE punto a punto entre los switches de Cisco. En este caso, el intervalo del mensaje se establece en siete segundos y 802.1D STP utiliza temporizadores predeterminados.

UDLD en EtherChannels

Tanto si la protección contra loops STP está implementada o no, se recomienda el modo agresivo UDLD para cualquier configuración EtherChannel, junto con el modo de canal deseable. En las configuraciones de EtherChannel, una falla en el link del canal que transporta las BPDU del árbol de expansión y el tráfico de control PAgP puede causar loops inmediatos entre los partners del canal si los links del canal se desagrupan. El modo agresivo UDLD apaga un puerto fallido. El PAgP (modo de canal automático/deseable) puede negociar un nuevo enlace de control y eliminar eficazmente un link fallido del canal.

UDLD con árbol de extensión 802.1w

Para evitar loops cuando utiliza versiones más recientes del spanning tree, utilice el modo normal UDLD y la protección de loop STP con RSTP como 802.1w. El UDLD puede proporcionar protección de links unidireccionales durante una fase de link, y la protección de loop STP puede prevenir loops STP en el caso de que los links se vuelvan unidireccionales *después de que* el

UDLD haya establecido los links como bidireccionales. Debido a que no puede configurar el UDLD para que sea menor que los temporizadores 802.1w predeterminados, la protección contra loops STP es necesaria para prevenir completamente los loops en topologías redundantes.

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

Probar y Monitorear el UDLD

No es fácil probar UDLD sin un componente genuinamente defectuoso/unidireccional en el laboratorio, como GBIC defectuoso. El protocolo fue diseñado para detectar los escenarios de falla menos comunes que los escenarios que se emplean generalmente en un laboratorio. Por ejemplo, si realiza una prueba sencilla como desconectar una cadena de una fibra para ver el estado `errdisable` deseado, primero debe desactivar la negociación automática de la Capa 1. De lo contrario, el puerto físico se desactiva, lo que reajusta la comunicación de mensaje UDLD. El extremo remoto se mueve al estado `indeterminado` en el modo normal UDLD, y se mueve al estado errdisable solamente con el uso del modo UDLD agresivo.

Un método de prueba adicional simula la pérdida de PDU vecina para el UDLD. El método es utilizar filtros de capa MAC para bloquear la dirección de hardware UDLD/CDP mientras se permite que pasen otras direcciones. Algunos switches no envían tramas UDLD cuando el puerto está configurado para ser un destino del analizador de puerto conmutado (SPAN), lo que simula un vecino UDLD que no responde.

Para monitorear el UDLD, utilice este comando:

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

Además, desde el modo de habilitación en Cisco IOS Software Release 12.2(18)SXD o los switches posteriores, puede ejecutar el comando oculto **show udld neighbor** para verificar el contenido de la memoria caché UDLD (de la manera en que CDP lo hace). A menudo es muy útil comparar la memoria caché UDLD con la memoria caché CDP para verificar si hay una anomalía específica del protocolo. Siempre que CDP también se ve afectado, significa generalmente que todas las BPDU/PDU se ven afectadas. Por lo tanto, también verifique STP. Por ejemplo, verifique las modificaciones recientes de identidad o cambios en la ubicación de los puertos raíz o designados.

Puede monitorear el estado UDLD y la consistencia de la configuración con el uso de las variables UDLD SNMP MIB de Cisco.

Switching multicapa

Overview

En el software del sistema Cisco IOS, el switching multicapa (MLS) es compatible con Catalyst serie 6500/6000 y sólo internamente. Esto significa que el router debe estar instalado en el switch. Los motores supervisores Catalyst 6500/6000 más nuevos admiten MLS CEF, en el cual la tabla de ruteo se descarga a cada tarjeta. Esto requiere hardware adicional, que incluye la presencia de una tarjeta de reenvío distribuido (DFC). Los DFC no se soportan en el software CatOS, incluso si opta por utilizar Cisco IOS Software en la tarjeta del router. Los DFC sólo se soportan en el software del sistema Cisco IOS.

La memoria caché MLS que se utiliza para habilitar las estadísticas de NetFlow en los switches Catalyst es la memoria caché basada en flujo que utilizan la tarjeta Supervisor Engine I y los switches Catalyst heredados para habilitar el switching de Capa 3. MLS se habilita de forma predeterminada en Supervisor Engine 1 (o Supervisor Engine 1A) con MSFC o MSFC2. No es necesaria ninguna configuración MLS adicional para la funcionalidad MLS predeterminada. Puede configurar la memoria caché MLS en uno de los tres modos siguientes:

- destino
- source-destination
- puerto de destino de origen

La máscara de flujo se utiliza para determinar el modo MLS del switch. Estos datos se utilizan posteriormente para habilitar los flujos de Capa 3 en los switches Catalyst aprovisionados por IA de Supervisor Engine. Los blades Supervisor Engine II no utilizan la memoria caché MLS para conmutar paquetes porque esta tarjeta está habilitada para CEF de hardware, lo que es una tecnología mucho más escalable. La memoria caché de MLS se mantiene en la tarjeta Supervisor Engine II para habilitar la exportación estadística de NetFlow solamente. Por lo tanto, el Supervisor Engine II se puede habilitar para el flujo completo si es necesario, sin impacto negativo en el switch.

Configuración

El tiempo de envejecimiento de MLS se aplica a todas las entradas de caché de MLS. El valor aging-time se aplica directamente al envejecimiento del modo de destino. El valor de tiempo de envejecimiento de MLS se divide en dos para derivar el tiempo de envejecimiento del modo de origen a destino. Divida el valor de tiempo de envejecimiento de MLS en ocho para encontrar el tiempo de envejecimiento de flujo completo. El valor predeterminado de tiempo de envejecimiento de MLS es 256 s.

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

Otros eventos pueden provocar la depuración de entradas MLS. Estos eventos incluyen:

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

Para mantener el tamaño de la memoria caché MLS por debajo de 32,000 entradas, habilite estos parámetros después de ejecutar el comando **mls aging**:

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

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

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

Configuración

Una entrada de caché típica que se quita es la entrada para los flujos hacia y desde un servidor de nombres de dominio (DNS) o un servidor TFTP que posiblemente no se puedan volver a utilizar después de crear la entrada. La detección y el agotamiento de estas entradas ahorra espacio en la memoria caché de MLS para otro tráfico de datos.

Si necesita habilitar el tiempo de envejecimiento rápido de MLS, establezca el valor inicial en 128 segundos. Si el tamaño de la memoria caché de MLS continúa creciendo más de 32.000 entradas, disminuya la configuración hasta que el tamaño de la memoria caché se mantenga por debajo de 32.000. Si la memoria caché continúa creciendo más de 32.000 entradas, disminuya el tiempo de envejecimiento normal de MLS.

Configuración de MLS recomendada por Cisco

Deje MLS en el valor predeterminado, sólo destino, a menos que se requiera la exportación de NetFlow. Si se requiere NetFlow, habilite MLS full flow solamente en los sistemas Supervisor Engine II.

Ejecute este comando para habilitar el destino de flujo MLS:

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

Tramas gigantes

Unidad máxima de transmisión

La unidad de transmisión máxima (MTU) es el datagrama o tamaño de paquete más grande en bytes que una interfaz puede enviar o recibir sin fragmentar el paquete.

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

- **1518 bytes** para tramas normales (1500 bytes más 18 bytes adicionales de encabezado Ethernet y cola CRC)
- **1522 bytes** para tramas encapsuladas en 802.1Q (1518 más 4 bytes de etiquetado)

Baby Giants: La función Baby Giants permite al switch pasar/reenviar paquetes que son ligeramente más grandes que la MTU Ethernet IEEE, en lugar de declarar las tramas de tamaño excesivo y descartarlas.

Jumbo: La definición del tamaño de trama depende del proveedor, ya que los tamaños de tramas no forman parte del estándar IEEE. Las tramas gigantes son tramas que son más grandes que el tamaño de trama Ethernet estándar (que es de 1518 bytes, que incluye el encabezado de Capa 2

y la secuencia de verificación de tramas [FCS]).

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

Cuándo Esperar Paquetes Que Sean Mayores De 1518 Bytes

Para transportar el tráfico a través de las redes conmutadas, asegúrese de que la MTU de tráfico transmitido no exceda de la que se soporta en las plataformas del switch. Hay varias razones por las que el tamaño de MTU de ciertas tramas puede ser truncado:

- **Requisitos específicos del proveedor**: las aplicaciones y ciertas NIC pueden especificar un tamaño de MTU que está fuera de los 1500 bytes estándar. Este cambio se ha producido debido a estudios que demuestran que un aumento en el tamaño de una trama Ethernet puede aumentar el rendimiento promedio.
- **Enlace: para transportar información VLAN-ID entre switches u otros dispositivos de red, se usó trunking para incrementar la trama Ethernet estándar.** Actualmente, las dos formas más comunes de conexión troncal son:encapsulación ISL propietaria de Cisco802.1Q
- **Switching de etiquetas multiprotocolo (MPLS)**: después de habilitar MPLS en una interfaz, MPLS tiene el potencial de aumentar el tamaño de trama de un paquete, que depende del número de etiquetas en la pila de etiquetas para un paquete con etiquetas MPLS. El tamaño total de la etiqueta es 4 bytes. El tamaño total de una pila de etiquetas es:
  ```
  n * 4 bytes
  ```
  Si se forma una pila de etiquetas, es posible que las tramas excedan la MTU.
- **Tunelización 802.1Q**: los paquetes de tunelización 802.1Q contienen dos etiquetas 802.1Q, de las cuales sólo una a la vez suele ser visible para el hardware. Por lo tanto, la etiqueta interna agrega 4 bytes al valor MTU (tamaño del contenido).
- **Universal Transport Interface (UTI)/Layer 2 Tunneling Protocol Version 3 (Layer 2TPv3)**: UTI/Layer 2TPv3 encapsula los datos de Capa 2 que se reenviarán a través de la red IP. UTI/Capa 2TPv3 puede aumentar el tamaño de trama original en hasta 50 bytes. La nueva trama incluye un nuevo encabezado IP (20 bytes), un encabezado de capa 2TPv3 (12 bytes) y un nuevo encabezado de capa 2. La carga útil de Capa 2TPv3 consiste en la trama de Capa 2 completa, que incluye el encabezado de Capa 2.

Propósito

El switching basado en hardware de alta velocidad (1 Gbps y 10 Gbps) ha convertido a las tramas gigantes en una solución muy concreta para problemas de rendimiento inferior al óptimo. Aunque no existe un estándar oficial para el tamaño de trama Jumbo, un valor bastante común que se suele adoptar en el campo es de 9216 bytes (9 KB).

Consideración de la eficiencia de la red

Puede calcular la eficiencia de la red para un reenvío de paquetes si divide su tamaño de carga útil por la suma del valor de tara y el tamaño de carga útil.

Incluso si el aumento de la eficiencia de la red con tramas gigantes es modesto y va del 94,9% (1500 bytes) al 99,1% (9216 bytes), la sobrecarga de procesamiento (utilización de la CPU) de los dispositivos de red y los hosts finales disminuye proporcionalmente al tamaño del paquete. Esta es la razón por la que las tecnologías de red LAN y WAN de alto rendimiento tienden a preferir un

tamaño máximo de trama bastante grande.

La mejora del rendimiento sólo es posible cuando se realizan transferencias de datos largas. Entre las aplicaciones de ejemplo se incluyen:

- Comunicación adosada del servidor (por ejemplo, transacciones de Network File System [NFS])
- Agrupación en clústeres de servidores
- Copias de seguridad de datos de alta velocidad
- Interconexión supercomputadora de alta velocidad
- Transferencias gráficas de datos de aplicaciones

Consideración del Rendimiento de la Red

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

- 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

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

Según esta fórmula, el rendimiento máximo de TCP alcanzable es directamente proporcional al MSS. Esto significa que, con RTT constante y pérdida de paquetes, puede duplicar el rendimiento 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.

Información Operativa General

La especificación estándar IEEE 802.3 define un tamaño máximo de trama Ethernet de **1518**. Las tramas encapsuladas 802.1Q, con una longitud de entre 1519 y 1522 bytes, se agregaron a la especificación 802.3 en una etapa posterior a través de la adición IEEE Std 802.3ac-1998. A veces se les menciona en la literatura como **bebés gigantes**.

En general, los paquetes se clasifican como **tramas gigantes** cuando exceden la longitud máxima Ethernet especificada para una conexión Ethernet específica. Los paquetes Baby giant también se conocen como tramas Jumbo.

El principal punto de confusión sobre las tramas jumbo es la configuración: diferentes interfaces admiten diferentes tamaños máximos de paquetes y, a veces, tratan los paquetes grandes de maneras ligeramente diferentes.

Catalyst 6500 Series

Esta tabla intenta resumir los tamaños de MTU soportados actualmente por diferentes tarjetas en la plataforma Catalyst 6500:

Tarjeta de línea	Talla de la MTU

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

Consulte Configuración de Ethernet, Fast Ethernet, Gigabit Ethernet y Conmutación 10-Gigabit Ethernet para obtener más información.

Soporte Jumbo de Capa 2 y Capa 3 en Catalyst 6500/6000 Cisco IOS Software

Hay soporte Jumbo de Capa 2 y Capa 3 con PFC/MSFC1, PFC/MSFC2 y PFC2/MSFC2 en todos los puertos GE configurados como interfaces físicas de Capa 2 y Capa 3. El soporte existe independientemente de si estos puertos son trunking o canalización. Esta función está disponible en Cisco IOS Software Release 12.1.1E y posteriores.

- Los tamaños de MTU de todos los puertos físicos con capacidad Jumbo están unidos. Un cambio en uno de ellos cambia todo. Siempre mantienen el mismo tamaño de MTU de trama Jumbo después de que se habiliten.
- Durante la configuración, active todos los puertos en la misma VLAN que jumbo-enabled o no habilite ninguno de ellos jumbo-enabled.
- El tamaño de MTU de la interfaz virtual conmutada (SVI) (interfaz VLAN) se establece por separado de la MTU de los puertos físicos. Un cambio en la MTU de los puertos físicos no cambia el tamaño de la MTU de SVI. Además, un cambio en la MTU de SVI no afecta a la MTU de los puertos físicos.
- El soporte de tramas gigantes de Capa 2 y Capa 3 en interfaces FE comenzó en Cisco IOS Software Release 12.1(8a) EX01. El comando **mtu 1500** inhabilita jumbo en FE, y el comando

mtu 9216 habilita jumbo en FE. Consulte Cisco bug ID CSCdv90450 (sólo clientes registrados) .

- Las tramas jumbo de Capa 3 en las interfaces VLAN se soportan solamente en:PFC/MSFC2 (Cisco IOS Software Release 12.1(7a)E y posteriores)PFC2/MSFC2 (Cisco IOS Software Release 12.1(8a)E4 y posteriores)
- No se recomienda utilizar tramas gigantes con PFC/MSFC1 para las interfaces VLAN (SVI) porque es posible que MSFC1 no pueda manejar la fragmentación como desee.
- No se admite fragmentación para los paquetes dentro de la misma VLAN (Jumbo de capa 2).
- Los paquetes que necesitan fragmentación en las VLAN/subredes (Jumbo de capa 3) se envían al software para su fragmentación.

Comprensión del Soporte de Tramas Jumbo en Catalyst 6500/6000 Cisco IOS Software

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

Comprobación del tamaño del tráfico en puente y enrutado en el software Cisco IOS

Tarjeta de línea	Acceso	Egress
Puertos de 10, 10/100 y 100 Mbps	La verificación del tamaño de la MTU se ha realizado. El soporte de tramas gigantes compara el tamaño del tráfico de ingreso con el tamaño de MTU del puerto LAN global en puertos Ethernet de 10, 10/100 y 100 Mbps y LAN de 10 GE que tienen configurado un tamaño de MTU no predeterminado. El puerto descarta el tráfico que está sobredimensionado.	La verificación del tamaño de la MTU no se ha realizado. Los puertos configurados con un tamaño de MTU no predeterminado transmiten tramas que contienen paquetes de cualquier tamaño mayores a 64 bytes. Con un tamaño de MTU no predeterminado configurado, los puertos LAN Ethernet de 10, 10/100 y 100 Mbps no comprueban si hay tramas de salida de tamaño excesivo.
Puertos GE	La verificación del tamaño de la MTU no se ha realizado. Los puertos configurados con un tamaño de MTU no predeterminado aceptan tramas que contienen paquetes de cualquier tamaño mayores a 64	La verificación del tamaño de la MTU se ha realizado. El soporte de tramas gigantes compara el tamaño del tráfico de salida con el tamaño de MTU del puerto LAN de salida global en puertos GE de

	bytes y no verifican tramas de ingreso de tamaño excesivo.	salida y 10-GE LAN que tienen configurado un tamaño de MTU no predeterminado. El puerto descarta el tráfico que está sobredimensionado.
Puertos 10-GE	La verificación del tamaño de la MTU se ha realizado. El puerto descarta el tráfico que está sobredimensionado.	La verificación del tamaño de la MTU se ha realizado. El puerto descarta el tráfico que está sobredimensionado.
SVI	La verificación del tamaño de la MTU no se ha realizado. El SVI no verifica el tamaño de trama en el lado de ingreso.	La verificación del tamaño de la MTU se ha realizado. El tamaño de MTU se verifica en el lado de salida de la SVI.
	PFC	
Todo el tráfico ruteado	Para el tráfico que se debe rutear, el soporte de tramas gigantes en la PFC compara los tamaños de tráfico con los tamaños de MTU configurados y proporciona conmutación de Capa 3 para el tráfico gigantesco entre las interfaces que se configuran con tamaños de MTU lo suficientemente grandes como para alojar el tráfico. Entre interfaces que no están configuradas con tamaños de MTU suficientemente grandes: • Si el bit Don't Fragment (DF) no está configurado, la PFC envía el tráfico a la MSFC para fragmentarse y enrutarse en el software. • Si el bit DF está configurado, el PFC descarta el tráfico.	

Recomendaciones de Cisco

Si se implementa correctamente, las tramas jumbo pueden proporcionar una mejora potencial de seis veces en el rendimiento de TCP de una conexión Ethernet, con una sobrecarga de fragmentación reducida (más una sobrecarga de CPU más baja en los dispositivos finales).

Debe asegurarse de que no haya ningún dispositivo entre el que no pueda manejar el tamaño de MTU especificado. Si este dispositivo fragmenta y reenvía los paquetes, anula todo el proceso. Esto puede resultar en una sobrecarga agregada en este dispositivo para la fragmentación y reensamblado de paquetes.

En estos casos, la detección de MTU de trayectoria IP ayuda a los remitentes a encontrar la longitud mínima común de paquetes que es adecuada para transmitir tráfico a lo largo de cada trayectoria. Alternativamente, puede configurar dispositivos host jumbo con reconocimiento de tramas con un tamaño de MTU que sea el mínimo de todos los que se soportan en la red.

Debe comprobar cuidadosamente cada dispositivo para asegurarse de que admita el tamaño de MTU. Vea la tabla de soporte de tamaño de MTU en esta sección.

El soporte de tramas gigantes se puede habilitar en estos tipos de interfaces:

- Interfaz de canal de puerto
- SVI
- Interfaz física (capa 2/capa 3)

Puede habilitar tramas jumbo en el canal de puerto o en las interfaces físicas que participan en el canal de puerto. Es muy importante asegurarse de que la MTU en todas las interfaces físicas sea la misma. De lo contrario, puede producirse una interfaz suspendida. Debe cambiar la MTU de una interfaz de canal de puerto porque cambia la MTU de todos los puertos miembro.

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

Asegúrese siempre de que todas las interfaces físicas en una VLAN estén configuradas para tramas jumbo antes de configurar el soporte de tramas jumbo en una SVI. La MTU de un paquete no se verifica en el lado de ingreso de una SVI. Pero se verifica en el lado de salida de una SVI. Si la MTU del paquete es mayor que la MTU SVI de salida, el paquete se fragmenta por software (si el bit DF no está configurado), lo que da como resultado un rendimiento deficiente. La fragmentación de software solo se produce para el switching de Capa 3. Cuando un paquete se reenvía a un puerto de Capa 3 o a una SVI con una MTU más pequeña, ocurre la fragmentación del software.

La MTU de una SVI debe ser siempre más pequeña que la MTU más pequeña entre todos los puertos del switch en la VLAN.

Catalyst 4500 Series

Las tramas Jumbo se soportan principalmente en los puertos sin bloqueo de las tarjetas de línea Catalyst 4500. Estos puertos GE sin bloqueo tienen conexiones directas al entramado de conmutación de Supervisor Engine y admiten tramas jumbo:

- Motores supervisoresWS-X4515, WS-X4516: dos puertos GBIC de enlace ascendente en Supervisor Engine IV o VWS-X4516-10GE: dos enlaces ascendentes de 10 GE y los cuatro enlaces ascendentes SFP de 1 GE.WS-X4013+: dos enlaces ascendentes 1 GEWS-X4013+10GE: dos enlaces ascendentes 10-GE y los cuatro enlaces ascendentes SFP 1-GEWS-X4013+TS: 20 puertos 1-GE
- Tarjetas de líneaWS-X4306-GB: módulo GE 1000BASE-X (GBIC) de seis puertosWS-X4506-GB-T: SFP de 6 puertos 10/100/1000 Mbps y 6 puertosWS-X4302-GB: módulo GE 1000BASE-X (GBIC) de dos puertosLos dos primeros puertos GBIC de un módulo GE de switching de servidor de 18 puertos (WS-X4418-GB) y puertos GBIC del módulo WS-X4232-GB-RJ
- Switches de configuración fijaWS-C4948: los 48 puertos 1-GEWS-C4948-10GE: los 48 puertos 1-GE y dos puertos 10-GE

Puede utilizar estos puertos GE sin bloqueo para soportar tramas gigantes de 9 KB o la supresión de transmisión de hardware (sólo Supervisor Engine IV). El resto de las tarjetas de línea admiten marcos de Baby Giant. Puede utilizar baby giants para el puente de MPLS o para el paso a través de Q en Q con una carga útil máxima de 1552 bytes.

Nota: El tamaño de la trama aumenta con las etiquetas ISL/802.1Q.

Los Baby Giants y las tramas jumbo son transparentes para otras funciones de Cisco IOS con Supervisor Engines IV y V.

Funciones de seguridad del software Cisco IOS

Funciones de Seguridad Básicas

En un momento dado, la seguridad a menudo se pasaba por alto en los diseños de las instalaciones. Sin embargo, la seguridad es ahora una parte esencial de todas las redes empresariales. Normalmente, el cliente ya ha establecido una política de seguridad para ayudar a definir qué herramientas y tecnologías de Cisco son aplicables.

Protección básica de contraseñas

La mayoría de los dispositivos del software Cisco IOS se configuran con dos niveles de contraseñas. El primer nivel es para el acceso Telnet al dispositivo, también conocido como acceso vty. Una vez concedido el acceso vty, debe obtener acceso para habilitar el modo o el modo exec privilegiado.

Proteja el modo de activación del switch

La contraseña de activación permite al usuario obtener acceso completo a un dispositivo. Proporcione la contraseña de activación sólo a personas de confianza.

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

Asegúrese de que la contraseña obedece a estas reglas:

- La contraseña debe contener entre uno y 25 caracteres alfanuméricos en mayúscula y minúscula.
- La contraseña no debe tener un número como el primer carácter.
- Puede utilizar los espacios iniciales, pero se ignoran. Se reconocen los espacios intermedios y finales.
- La verificación de contraseña distingue entre mayúsculas y minúsculas. Por ejemplo, la contraseña secreta es diferente a la contraseña secreta.

Nota: El comando **enable secret** utiliza una función de hash de Message Digest 5 (MD5) criptográfica unidireccional. Si ejecuta el comando **show running-config**, puede ver esta contraseña cifrada. El uso del comando **enable password** es otra manera de establecer la contraseña de habilitación. Sin embargo, el algoritmo de cifrado que se utiliza con el comando **enable password** es débil y se puede revertir fácilmente para obtener la contraseña. Por lo tanto, no utilice el comando **enable password**. Utilice el comando enable secret para mayor seguridad: Consulte Hechos de Cifrado de Contraseña de Cisco IOS para obtener más información.

Acceso Telnet/VTY seguro al switch

De forma predeterminada, el software Cisco IOS admite cinco sesiones Telnet activas. Estas

sesiones se denominan vty 0 a 4. Puede habilitar estas líneas para el acceso. Pero para habilitar el login, también necesita el set password para estas líneas.

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

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

- El primer carácter no puede ser un número.
- La cadena puede contener cualquier carácter alfanumérico, hasta 80 caracteres. Los caracteres incluyen espacios.
- No puede especificar la contraseña con el formato number-space-character. El espacio después del número causa problemas. Por ejemplo, hello 21 es una contraseña legal, pero 21 hello no es una contraseña legal.
- La verificación de contraseña distingue entre mayúsculas y minúsculas. Por ejemplo, la contraseña secreta es diferente a la contraseña secreta.

Nota: Con esta configuración de línea vty, el switch almacena la contraseña en texto sin formato. Si alguien ejecuta el comando **show running-config**, esta contraseña es visible. Para evitar esta situación, utilice el comando **service password-encryption**. El comando cifra la contraseña de forma laxa. El comando sólo cifra la contraseña de la línea vty y la contraseña de habilitación que se configura con el comando **enable password**. La contraseña de habilitación configurada con el comando **enable secret** utiliza un cifrado más fiable. La configuración con el comando **enable secret** es el método recomendado.

Nota: Para tener más flexibilidad en la administración de seguridad, asegúrese de que todos los dispositivos del software Cisco IOS implementen el modelo de seguridad de autenticación, autorización y contabilidad (AAA). AAA puede emplear bases de datos locales, RADIUS y TACACS+. Consulte la sección Configuración de Autenticación TACACS+ para obtener más información.

Servicios de seguridad AAA

Descripción General de las Operaciones de AAA

El control de acceso controla quién tiene permiso para acceder al switch y qué servicios pueden utilizar estos usuarios. Los servicios de seguridad de red AAA proporcionan el marco principal para configurar el control de acceso en su switch.

Esta sección describe en detalle los diversos aspectos de AAA:

- Autenticación: este proceso valida la identidad reclamada de un usuario final o un dispositivo. En primer lugar, se especifican los diversos métodos que se pueden utilizar para autenticar al usuario. Estos métodos definen el tipo de autenticación que se debe realizar (por ejemplo, TACACS+ o RADIUS). También se define la secuencia en la que se intentan estos métodos de autenticación. Los métodos se aplican luego a las interfaces apropiadas, que activan la autenticación.
- Autorización: este proceso otorga derechos de acceso a un usuario, grupos de usuarios,

sistemas o procesos. El proceso AAA puede realizar una autorización o autorización única por tarea. El proceso define los atributos (en el servidor AAA) en lo que el usuario tiene permiso para realizar. Siempre que el usuario intenta iniciar un servicio, el switch consulta el servidor AAA y solicita permiso para autorizar al usuario. Si el servidor AAA lo aprueba, se autoriza al usuario. Si el servidor AAA no lo aprueba, el usuario no obtiene permiso para ejecutar ese servicio. Puede utilizar este proceso para especificar que algunos usuarios sólo pueden ejecutar ciertos comandos.
- Contabilidad: este proceso permite realizar un seguimiento de los servicios a los que acceden los usuarios y de la cantidad de recursos de red que consumen. Cuando se habilita la contabilización, el switch informa la actividad del usuario al servidor AAA en forma de registros contables. Entre los ejemplos de actividad de usuario de los que se informa se incluyen la hora de la sesión y la hora de inicio y parada. A continuación, el análisis de esta actividad se puede llevar a cabo con fines de gestión o facturación.

Aunque AAA es el método principal y recomendado para el control de acceso, Cisco IOS Software proporciona funciones adicionales para el control de acceso simple que están fuera del alcance de AAA. Estas funciones adicionales incluyen:

- Autenticación de nombre de usuario local
- Autenticación de contraseña de línea
- Habilitar autenticación de contraseña

Pero estas funciones no proporcionan el mismo grado de control de acceso que es posible con AAA.

Para entender mejor AAA, consulte estos documentos:

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

Estos documentos no mencionan necesariamente los switches. Pero los conceptos de AAA que describen los documentos son aplicables a los switches.

TACACS+

Propósito

De forma predeterminada, las contraseñas de modo privilegiado y no privilegiado son globales. Estas contraseñas se aplican a todos los usuarios que acceden al switch o al router, ya sea desde el puerto de la consola o a través de una sesión Telnet a través de la red. La implementación de estas contraseñas en los dispositivos de red lleva mucho tiempo y no está centralizada. Además, puede tener dificultades con la implementación de restricciones de acceso con el uso de listas de control de acceso (ACL) que pueden ser propensas a errores de configuración. Para superar estos problemas, adopte un enfoque centralizado cuando configure nombres de usuario, contraseñas y políticas de acceso en un servidor central. Este servidor puede ser Cisco Secure Access Control Server (ACS) o cualquier servidor de terceros. Los dispositivos se configuran para utilizar estas bases de datos centralizadas para las funciones de AAA. En este caso, los dispositivos son switches de software Cisco IOS. El protocolo que se utiliza entre los dispositivos y el servidor central puede ser:

- TACACS+

- RADIUS
- Kerberos

TACACS+ es una implementación común en las redes de Cisco y es el objetivo de esta sección. TACACS+ proporciona estas funciones:

- Autenticación: proceso que identifica y verifica a un usuario. Se pueden utilizar varios métodos para autenticar a un usuario. Pero el método más común incluye una combinación de nombre de usuario y contraseña.
- Autorización: cuando el usuario intenta ejecutar un comando, el switch puede verificar con el servidor TACACS+ para determinar si se le concede permiso al usuario para utilizar ese comando en particular.
- Contabilización: este proceso registra lo que un usuario hace o ha hecho en el dispositivo.

Consulte Comparación de TACACS+ y RADIUS para ver una comparación entre TACACS+ y RADIUS.

Información Operativa General

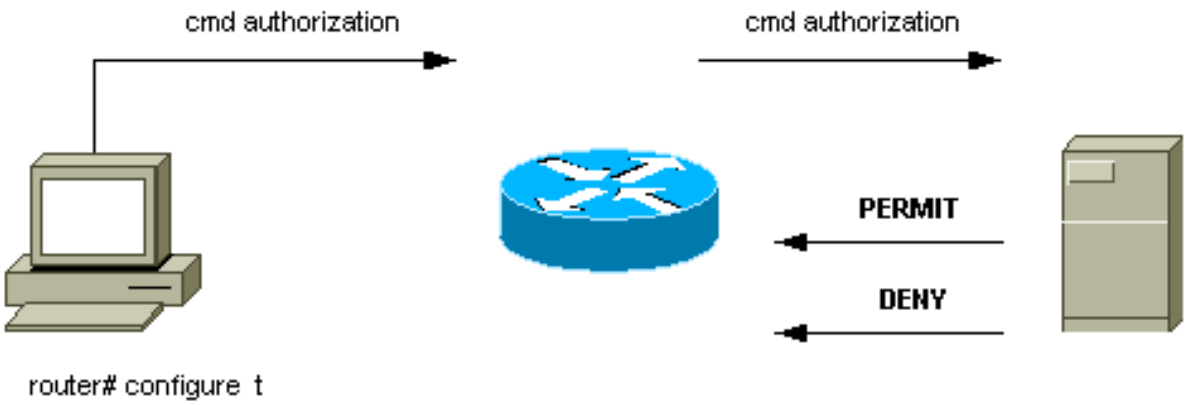
El protocolo TACACS+ reenvía los nombres de usuario y las contraseñas al servidor centralizado. La información se cifra a través de la red con hash unidireccional MD5. Consulte RFC 1321 para obtener más información. TACACS+ utiliza el puerto TCP 49 como protocolo de transporte, lo que ofrece estas ventajas sobre UDP:

Nota: RADIUS utiliza UDP.

- Transporte orientado a la conexión
- Reconocimiento separado de que se ha recibido una solicitud (reconocimiento de TCP [ACK]), independientemente de la carga del mecanismo de autenticación de back-end
- Indicación inmediata de un desperfecto del servidor (reinicio [RST] de paquetes)

Durante una sesión, si es necesaria una verificación de autorización adicional, el switch verifica con TACACS+ para determinar si al usuario se le concede permiso para utilizar un comando determinado. Este paso proporciona un mayor control sobre los comandos que se pueden ejecutar en el switch y proporciona el desacoplamiento del mecanismo de autenticación. Con el uso de la contabilidad de comandos, puede auditar los comandos que un usuario determinado ha ejecutado mientras el usuario está conectado a un dispositivo de red determinado.

Este diagrama muestra el proceso de autorización involucrado:



Cuando un usuario se autentica en un dispositivo de red con el uso de TACACS+ en un intento de inicio de sesión ASCII simple, este proceso ocurre típicamente:

- Cuando se establece la conexión, el switch se pone en contacto con el daemon TACACS+ para obtener un mensaje de nombre de usuario. A continuación, el switch muestra el mensaje del 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 muestra el mensaje de contraseña para el usuario, que ingresa una contraseña que también se envía al daemon 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.` Al usuario se le niega el acceso adicional o se le solicita que vuelva a intentar la secuencia de inicio de sesión. El resultado depende del daemon TACACS+.`ERROR: se produjo un error en algún momento durante la autenticación.` El error puede estar en el demonio o en la conexión de red entre el demonio y el switch. Si se recibe `una` respuesta `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 requiere autorización TACACS+, se vuelve a contactar con el daemon TACACS+. El daemon TACACS+ devuelve una respuesta de autorización `ACCEPT` o `REJECT`. Si se devuelve una respuesta `ACCEPT`, la respuesta contiene datos en forma de atributos que se utilizan para dirigir la `sesión EXEC` o `NETWORK` para ese usuario. Esto determina a qué comandos puede acceder el usuario.

Pasos básicos de configuración de AAA

La configuración de AAA es relativamente sencilla después de comprender el proceso básico. Para configurar la seguridad en un router Cisco o servidor de acceso con el uso de AAA, realice estos pasos:

1. Para habilitar AAA, ejecute el comando **aaa new-model** global configuration.
   `Switch(config)#aaa new-model`

Sugerencia: Guarde la configuración antes de configurar los comandos AAA. Guarde la configuración de nuevo sólo después de haber completado todas sus configuraciones AAA y estén satisfechos de que la configuración funciona correctamente. Luego, puede recargar el switch para recuperarse de bloqueos imprevistos (antes de guardar la configuración), si es necesario.

2. Si decide utilizar un servidor de seguridad independiente, configure los parámetros del protocolo de seguridad como RADIUS, TACACS+ o Kerberos.
3. Utilice el comando **aaa authentication** para definir las listas de métodos para la autenticación.
4. Utilice el comando **login authentication** para aplicar las listas de métodos a una interfaz o línea determinada.
5. Ejecute el comando opcional **aaa authorization** para configurar la autorización.
6. Ejecute el comando opcional **aaa accounting** para configurar la contabilidad.
7. Configure el servidor externo AAA para procesar las solicitudes de autenticación y autorización del switch.**Nota:** Consulte la documentación del servidor AAA para obtener más información.

Configuración de autenticación TACACS+

Realice estos pasos para configurar la autenticación TACACS+:

1. Ejecute el comando **aaa new-model** en el modo de configuración global para habilitar AAA en el switch.
2. Defina el servidor TACACS+ y la clave asociada.Esta clave se utiliza para cifrar el tráfico entre el servidor TACACS+ y el switch. En el comando **tacacs-server host 1.1.1.1 key mysecretkey**, el servidor TACACS+ está en la dirección IP 1.1.1.1 y la clave de cifrado es mysecretkey. Para verificar que el switch pueda alcanzar el servidor TACACS+, inicie un ping ICMP (Internet Control Message Protocol) desde el switch.
3. Defina una lista de métodos.Una lista de métodos define la secuencia de mecanismos de autenticación para intentar varios servicios. Los diversos servicios pueden ser, por ejemplo:HabilitarInicio de sesión (para acceso vty/Telnet)**Nota:** Consulte la sección Funciones básicas de seguridad de este documento para obtener información sobre el acceso vty/Telnet.ConsolaEste ejemplo considera **login** solamente. Debe aplicar la lista de métodos a las interfaces/líneas:

```
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
Switch(config)#line vty 0 4
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

En esta configuración, el comando **aaa authentication login** utiliza el nombre de lista inventado METHOD-LIST-LOGIN y utiliza el método tacacs+ antes de utilizar la línea de método. Los usuarios se autentican con el uso del servidor TACACS+ como el primer método. Si el servidor TACACS+ no responde o envía un mensaje de ERROR, la contraseña configurada en la línea se utiliza como segundo método. Pero si el servidor TACACS+ niega al usuario y responde con un mensaje REJECT, AAA considera la transacción exitosa y no utiliza el segundo método.**Nota:** La configuración no está completa hasta que se aplique la lista (METHOD-LIST-LOGIN) a la línea vty. Ejecute el comando **login authentication METHOD-LIST-LOGIN** en el modo de configuración de línea, como se

muestra en el ejemplo.**Nota:** El ejemplo crea una puerta trasera para cuando el servidor TACACS+ no está disponible. Los administradores de seguridad pueden o no pueden aceptar la implementación de una puerta trasera. Asegúrese de que la decisión de implementar tales puertas traseras cumpla con las políticas de seguridad del sitio.

Configuración de autenticación RADIUS

La configuración RADIUS es casi idéntica a la configuración TACACS+. Basta con sustituir la palabra RADIUS por TACACS en la configuración. Esta es una configuración RADIUS de ejemplo para el acceso al puerto COM:

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

Banners de Login

Cree los banners de dispositivo adecuados que indiquen específicamente las acciones que se realizan con acceso no autorizado. No anuncie el nombre del sitio ni la información de red a usuarios no autorizados. Los carteles ofrecen recursos en caso de que un dispositivo se vea comprometido y el autor sea capturado. Ejecute este comando para crear banners de inicio de sesión:

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

Seguridad Física

Asegúrese de que se necesita una autorización adecuada para acceder físicamente a los dispositivos. Mantenga el equipo en un espacio controlado (bloqueado). Para garantizar que la red permanezca operativa y no se vea afectada por manipulaciones maliciosas o factores ambientales, asegúrese de que todos los equipos tengan:

- Una fuente de alimentación ininterrumpible (UPS) adecuada, con fuentes redundantes siempre que sea posible
- Control de temperatura (aire acondicionado)

Recuerde que, si una persona con intención maliciosa viola el acceso físico, es mucho más probable que se produzca una interrupción por recuperación de contraseña u otros medios.

Configuración de la Administración

Diagramas de la Red

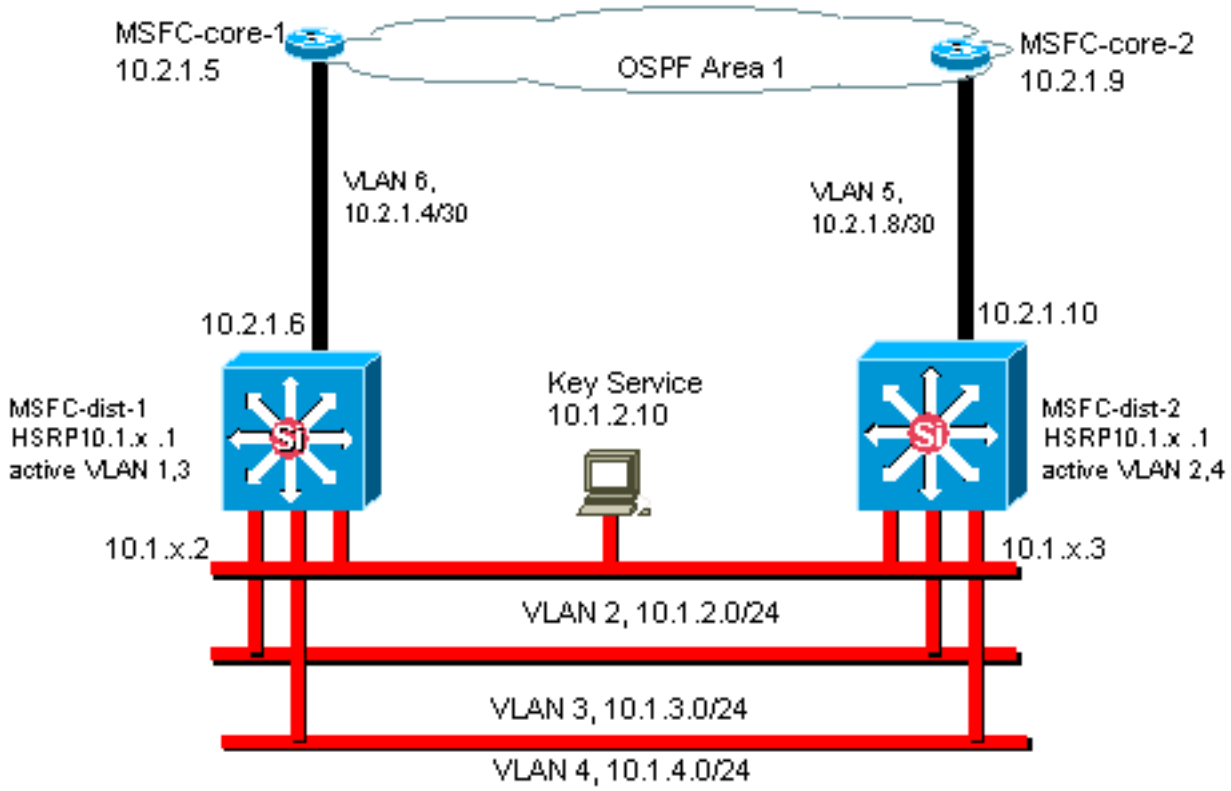
Propósito

Los diagramas de redes limpios son fundamentales en el funcionamiento de las redes. Los diagramas se convierten en fundamentales durante la resolución de problemas y son el vehículo más importante para la comunicación de información durante la derivación a proveedores y partners durante una interrupción. No subestime la preparación, preparación y accesibilidad que proporcionan los diagramas de red.

Recomendación

Estos tres tipos de diagramas son necesarios:

- **Diagrama general**: incluso para las redes más grandes, un diagrama que muestra la conectividad física o lógica de extremo a extremo es importante. A menudo, las empresas que han implementado un diseño jerárquico documentan cada capa por separado. Cuando planifica y resuelve problemas, lo que importa es saber bien cómo se unen los dominios.
- **Diagrama físico**: este diagrama muestra todo el hardware y cableado de switch y router. Asegúrese de que el diagrama etiqueta cada uno de estos aspectos:TrunksEnlacesVelocidadesGrupos de canalesNúmeros de puertoRanurasTipos de chasisSoftwaredominios VTPRoot BridgePrioridad del puente raíz de respaldoDirección MACPuertos bloqueados por VLANPara una mayor claridad, represente los dispositivos internos como el router MSFC Catalyst 6500/6000 como un router en una porra que está conectada a través de un tronco.
- **Diagrama lógico**: este diagrama muestra solamente la funcionalidad de Capa 3, lo que significa que muestra los routers como objetos y VLAN como segmentos Ethernet. Asegúrese de que el diagrama identifica estos aspectos:Direcciones IPSubnetsDireccionamiento secundarioHSRP activo y en esperaAcceder a las capas de distribución del núcleoInformación de ruteo



Interfaz de administración del switch y VLAN nativa

Propósito

Esta sección describe la importancia y los problemas potenciales del uso de la VLAN 1 predeterminada. Esta sección también cubre los problemas potenciales cuando se ejecuta el tráfico de administración al switch en la misma VLAN que el tráfico de usuario en los switches de la serie 6500/6000.

Los procesadores en Supervisor Engines y MSFC para Catalyst 6500/6000 Series utilizan VLAN 1 para una serie de protocolos de control y administración. Algunos ejemplos son:

- Protocolos de control de switch:BPDU STPVTPDTPCDP
- Protocolos de administración:SNMP (Protocolo de administración de red simple)TELNETProtocolo Secure Shell (SSH)Syslog

Cuando la VLAN se utiliza de esta manera, se denomina VLAN nativa. La configuración predeterminada del switch establece VLAN 1 como la VLAN nativa predeterminada en los puertos troncales Catalyst. Puede dejar la VLAN 1 como la VLAN nativa. Pero tenga en cuenta que cualquier switch que ejecute el software del sistema Cisco IOS en su red establece todas las interfaces que se configuran como puertos de switch de Capa 2 para acceder a los puertos en VLAN 1 de forma predeterminada. Lo más probable es que un switch en algún lugar de la red utilice VLAN 1 como VLAN para el tráfico de usuarios.

La principal preocupación con el uso de VLAN 1 es que, en general, el NMP de Supervisor Engine no necesita ser interrumpido por gran parte del tráfico de broadcast y multidifusión que generan las estaciones finales. Las aplicaciones de multidifusión en particular tienden a enviar muchos datos entre servidores y clientes. El Supervisor Engine no necesita ver estos datos. Si los recursos o los búfers del Supervisor Engine están completamente ocupados mientras el Supervisor Engine escucha tráfico innecesario, el Supervisor Engine no puede ver los paquetes de administración que pueden causar un loop de árbol de expansión o una falla de EtherChannel (en el peor de los casos).

El comando **show interfaces** *interface_type slot/port* counters y el comando **show ip traffic** pueden darle alguna indicación de:

- La proporción de tráfico de difusión a unidifusión
- Proporción de tráfico IP a tráfico no IP (que no se ve normalmente en las VLAN de administración)

VLAN 1 etiqueta y maneja la mayor parte del tráfico del plano de control. La VLAN1 se habilita en todos los trunks de forma predeterminada. Con redes de campus más grandes, debe tener cuidado con el diámetro del dominio STP VLAN 1. La inestabilidad en una parte de la red puede afectar la VLAN 1 y puede influir en la estabilidad del plano de control y la estabilidad del STP para todas las demás VLAN. Puede limitar la transmisión VLAN 1 de los datos de usuario y el funcionamiento del STP en una interfaz. Simplemente no configure la VLAN en la interfaz troncal.

Esta configuración no detiene la transmisión de paquetes de control de switch a switch en VLAN 1, como con un analizador de red. Pero no se reenvían datos y el STP no se ejecuta sobre este link. Por lo tanto, puede utilizar esta técnica para dividir VLAN 1 en dominios de falla más pequeños.

Nota: No puede borrar la VLAN 1 de los troncales a los Catalyst 2900XL/3500XL.

Incluso si se cuida de restringir las VLAN de usuario a dominios de switch relativamente pequeños y, en consecuencia, a límites de falla/Capa 3 pequeños, algunos clientes todavía sienten la tentación de tratar la VLAN de administración de manera diferente. Estos clientes intentan cubrir toda la red con una única subred de administración. No existe ninguna razón técnica por la que una aplicación NMS central deba estar adyacente a la capa 2 de los dispositivos que administra la aplicación, ni tampoco se trata de un argumento de seguridad calificado. Limite el diámetro de las VLAN de administración a la misma estructura de dominio ruteada que la de las VLAN de usuario. Considere la administración fuera de banda y/o la compatibilidad con SSH como una forma de aumentar la seguridad de la administración de red.

Otras Opciones

Hay consideraciones de 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. De esta manera, el diseño requiere la restricción de cada subred/VLAN IP a un único switch de capa de acceso (o clúster de switches). En estos diseños, no se puede configurar ningún enlace troncal hasta la capa de acceso.

¿Crea una VLAN de administración independiente y habilita el trunking para transportarlo entre las capas de acceso de Capa 2 y de distribución de Capa 3? No hay una respuesta fácil a esta pregunta. Considere estas dos opciones para la revisión del diseño con su ingeniero de Cisco:

- **Opción 1**: enlace troncal de dos o tres VLAN únicas desde la capa de distribución hasta cada switch de capa de acceso. Esta configuración permite una VLAN de datos, una VLAN de voz y una VLAN de administración, y todavía tiene la ventaja de que el STP está inactivo. Se necesita un paso de configuración adicional para borrar la VLAN 1 de los troncales. En esta solución, también hay que tener en cuenta los puntos de diseño para evitar que el tráfico ruteado en espera sea temporalmente negro durante la recuperación de fallos. Utilice STP PortFast para trunks (en el futuro) o sincronización VLAN autostate con reenvío STP.
- **Opción 2**: una sola VLAN para datos y administración puede ser aceptable. Si desea mantener la interfaz sc0 separada de los datos del usuario, el hardware de switch más reciente hace que este escenario sea menos problemático que antes. El hardware más reciente proporciona:CPU más potentes y controles de limitación de velocidad del plano de controlUn diseño con dominios de broadcast relativamente pequeños, como se recomienda en el diseño multicapaPara tomar una decisión final, examine el perfil de tráfico de broadcast para la VLAN y hable con su ingeniero de Cisco sobre las capacidades del hardware del switch. Si la VLAN de administración contiene todos los usuarios en ese switch de capa de acceso, utilice filtros de entrada IP para asegurar el switch de los usuarios, según la sección Funciones de Seguridad del Software Cisco IOS.

Cisco Management Interface y recomendación de VLAN nativa

Interfaz de administración

El software del sistema Cisco IOS le ofrece la opción de configurar las interfaces como interfaces de Capa 3 o como puertos de switch de Capa 2 en una VLAN. Cuando utiliza el comando **switchport** en Cisco IOS Software, todos los puertos del switch son puertos de acceso en VLAN 1 de forma predeterminada. Por lo tanto, a menos que configure lo contrario, los datos del usuario también pueden existir de forma predeterminada en la VLAN 1.

Haga que la VLAN de administración sea una VLAN distinta de la VLAN 1. Mantenga todos los datos de usuario fuera de la VLAN de administración. En su lugar, configure una interfaz loopback0 como la interfaz de administración en cada switch.

Nota: Si utiliza el protocolo OSPF, esto también se convierte en el ID del router OSPF.

Asegúrese de que la interfaz de loopback tenga una máscara de subred de 32 bits y configure la interfaz de loopback como una interfaz de Capa 3 pura en el switch. Aquí tiene un ejemplo:

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

VLAN nativa

Configure la VLAN nativa para que sea una VLAN ficticia obvia que nunca se habilita en el router. Cisco recomendó VLAN 999 en el pasado, pero la elección es puramente arbitraria.

Ejecute estos comandos de interfaz para establecer una VLAN como la nativa (predeterminada) para el enlace troncal 802.1Q en un puerto determinado:

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

Para ver recomendaciones adicionales de configuración de trunking, vea la sección Dynamic Trunking Protocol de este documento.

Administración Fuera de Banda

Propósito

Puede aumentar la disponibilidad de la gestión de redes si crea una infraestructura de gestión independiente en torno a la red de producción. Esta configuración permite que los dispositivos sean accesibles de forma remota, a pesar del tráfico que se controla o de los eventos del plano de control que se producen. Estos dos enfoques son típicos:

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

Información Operativa General

Puede proporcionar a cada router y switch de la red una interfaz de administración Ethernet fuera de banda en una VLAN de administración. Configure un puerto Ethernet en cada dispositivo de la VLAN de administración y cablearlo fuera de la red de producción a una red de administración conmutada independiente.

Nota: Los switches Catalyst 4500/4000 tienen una interfaz me1 especial en el Supervisor Engine que se utilizará sólo para la administración fuera de banda y no como puerto de switch.

Además, puede lograr la conectividad del servidor terminal si configura un router Cisco 2600 o

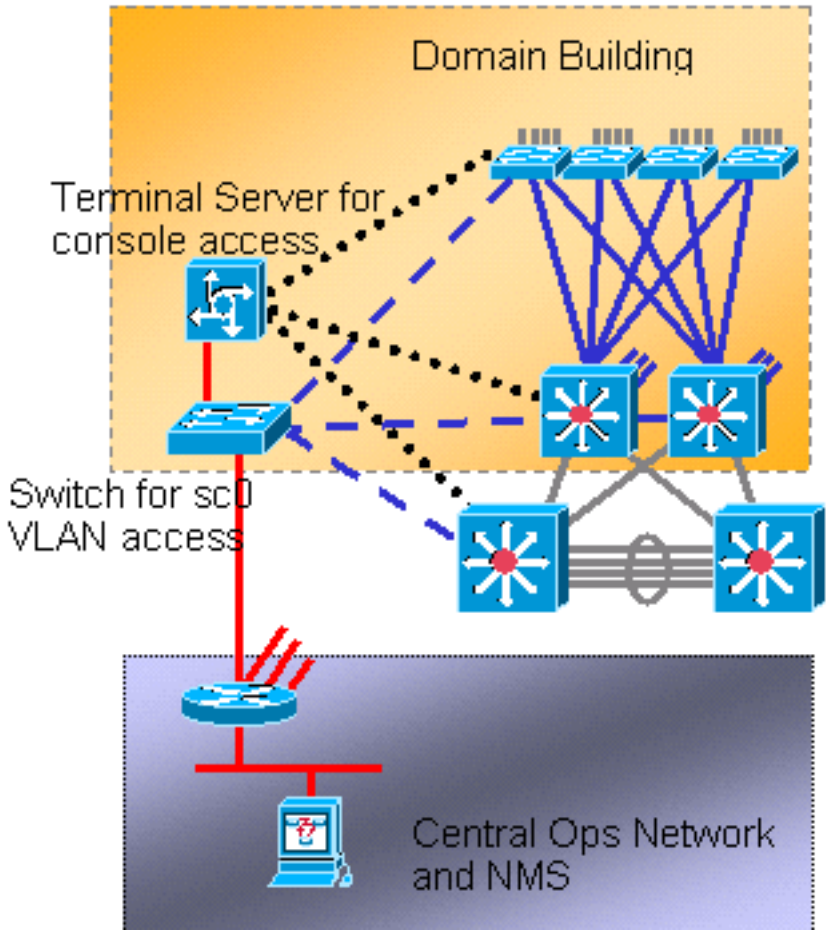
3600 con cables seriales RJ-45 para acceder al puerto de consola de cada router y switch en el diseño. El uso de un servidor terminal también evita la necesidad de configurar escenarios de respaldo, como módems en puertos auxiliares para cada dispositivo. Puede configurar un solo módem en el puerto auxiliar del servidor terminal. Esta configuración proporciona servicio de acceso telefónico a los otros dispositivos durante una falla de conectividad de red. Refiérase a Conexión de un Módem al Puerto de la Consola en Switches Catalyst para obtener más información.

Recomendación

Con esta disposición, son posibles dos trayectos fuera de banda a cada switch y router, además de numerosas trayectorias dentro de banda. Este arreglo permite una administración de red de alta disponibilidad. Las ventajas son:

- El arreglo separa el tráfico de administración de los datos de usuario.
- La dirección IP de administración se encuentra en una subred independiente, VLAN y switch para la seguridad.
- Existe una mayor seguridad para el suministro de datos de administración durante los fallos de la red.
- No hay un spanning tree activo en la VLAN de administración. La redundancia aquí no es crítica.

Este diagrama muestra la administración fuera de banda:



Registro del Sistema

Propósito

Los mensajes de Syslog son específicos de Cisco y pueden ofrecer información más precisa y con mayor capacidad de respuesta que el SNMP estandarizado. Por ejemplo, las plataformas de gestión como Cisco Resource Manager Essentials (RME) y Network Analysis Toolkit (NATKit) hacen un uso intensivo de la información de syslog para recopilar los cambios de inventario y configuración.

Recomendación de configuración de Cisco Syslog

El registro del sistema es una práctica operativa común y aceptada. Un syslog UNIX puede capturar y analizar información/eventos en el router como:

- Estado de la interfaz
- Alertas de seguridad
- Condiciones del entorno
- Bloqueo de proceso de CPU
- Otros eventos

El software Cisco IOS puede realizar el registro UNIX a un servidor UNIX syslog. El formato syslog de Cisco UNIX es compatible con 4.3 Berkeley Standard Distribution (BSD) UNIX. Utilice estas configuraciones de registro de Cisco IOS Software:

- **no logging console**: de forma predeterminada, todos los mensajes del sistema se envían a la consola del sistema. El registro de la consola es una tarea de alta prioridad en Cisco IOS Software. Esta función se diseñó principalmente para proporcionar mensajes de error al operador del sistema antes de una falla del sistema. Inhabilite el registro de la consola en todas las configuraciones del dispositivo para evitar una situación en la que el router/switch pueda colgarse mientras el dispositivo espera una respuesta de un terminal. Pero los mensajes de la consola pueden ser útiles durante el aislamiento de problemas. En estos casos, habilite el registro de la consola. Ejecute el comando **logging console level** para obtener el nivel deseado de registro de mensajes. Los niveles de registro son de 0 a 7.
- **no logging monitor**: este comando inhabilita el registro de líneas de terminal distintas de la consola del sistema. Se puede requerir el registro del monitor (con el uso de **logging monitor debugging** u otra opción de comando). En este caso, habilite el registro del monitor en el nivel de registro específico necesario para la actividad. Vea el elemento **no logging console** en esta lista para obtener más información sobre los niveles de registro.
- **logging buffered 16384**: el comando **logging buffered** debe agregarse para registrar los mensajes del sistema en el buffer de registro interno. El búfer de registro es circular. Una vez que se llena el búfer de registro, las entradas más antiguas se sobrescriben con entradas más recientes. El tamaño del búfer de registro es configurable por el usuario y se especifica en bytes. El tamaño del búfer del sistema varía según la plataforma. 16384 es un buen valor predeterminado que proporciona un registro adecuado en la mayoría de los casos.
- **logging trap notification**: Este comando proporciona mensajes de nivel de notificación (5) al servidor syslog especificado. El nivel de registro predeterminado para todos los dispositivos (consola, monitor, búfer y trampas) es debugging (nivel 7). Si deja el nivel de registro de trampas en 7, se producen muchos mensajes extraños que tienen poca o ninguna preocupación por el estado de la red. Establezca el nivel de registro predeterminado para las trampas en 5.
- **logging facility local7**: Este comando establece el nivel/recurso de registro predeterminado para el syslogging de UNIX. Configure el servidor syslog que recibe estos mensajes para el

mismo recurso/nivel.
- **logging host**: Este comando establece la dirección IP del servidor de registro UNIX.
- **logging source-interface loopback 0**: Este comando configura la IP SA predeterminada para los mensajes syslog. Codifique el SA de registro para facilitar la identificación del host que envió el mensaje.
- **service timestamps debug datetime localtime show-timezone msec**: de forma predeterminada, los mensajes de registro no se marcan el tiempo. Puede utilizar este comando para habilitar la marca de hora de los mensajes de registro y configurar la marca de hora de los mensajes de depuración del sistema. Timestamping proporciona la sincronización relativa de los eventos registrados y mejora la depuración en tiempo real. Esta información es especialmente útil cuando los clientes envían resultados de depuración al personal de soporte técnico para obtener asistencia. Para habilitar la marca de tiempo de los mensajes de depuración del sistema, utilice el comando en el modo de configuración global. El comando sólo tiene un efecto cuando la depuración está habilitada.

Nota: Además, habilite el registro para el estado del link y el estado del paquete en todas las interfaces Gigabit de infraestructura.

El software Cisco IOS proporciona un mecanismo único para establecer la función y el nivel de registro para todos los mensajes del sistema que están destinados a un servidor syslog. Establezca el nivel de trampa de registro en notificación (nivel 5). Si configura el nivel de mensaje de trampa en notificación, puede minimizar el número de mensajes de información que se reenvían al servidor syslog. Esta configuración puede reducir significativamente la cantidad de tráfico syslog en la red y puede disminuir el impacto en los recursos del servidor syslog.

Agregue estos comandos a cada router y switch que ejecute Cisco IOS Software para habilitar la mensajería syslog:

- Comandos de configuración de syslog globales:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- Comandos de configuración de syslog de interfaz:

```
logging event link-status
logging event bundle-status
```

SNMP (Protocolo de administración de red simple)

Propósito

Puede utilizar SNMP para recuperar estadísticas, contadores y tablas que se almacenan en MIB de dispositivo de red. Los NMS como HP OpenView pueden utilizar la información para:

- Generar alertas en tiempo real
- Disponibilidad de la medida
- Producir información de planificación de capacidad
- Ayuda para realizar comprobaciones de configuración y resolución de problemas

Operación de la Interfaz de Administración SNMP

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

El marco SNMP consta de estas tres partes:

- Un administrador SNMP
- Un agente SNMP
- MIB

El administrador SNMP es el sistema que utiliza SNMP para controlar y monitorear las actividades de los hosts de red. El sistema de gestión más común se denomina NMS. Puede aplicar el término NMS a un dispositivo dedicado que se utiliza para la administración de la red o a las aplicaciones que se utilizan en dicho dispositivo. Hay una variedad de aplicaciones de administración de red disponibles para su uso con SNMP. Estas aplicaciones van desde simples aplicaciones CLI hasta interfaces gráficas de usuario completas, como la línea de productos CiscoWorks.

El agente SNMP es el componente de software dentro del dispositivo administrado que mantiene los datos del dispositivo y los informa, según sea necesario, a los sistemas de administración. El agente y MIB residen en el dispositivo de ruteo (el router, el servidor de acceso o el switch). Para habilitar el agente SNMP en un dispositivo de ruteo de Cisco, debe definir la relación entre el administrador y el agente.

La MIB es un área de almacenamiento de información virtual para la información de administración de red. La MIB consta de colecciones de objetos administrados. Dentro de la MIB, hay colecciones de objetos relacionados que se definen en los módulos MIB. Los módulos MIB se escriben en el lenguaje del módulo SNMP MIB, como lo definen STD 58, RFC 2578 , RFC 2579 y RFC 2580 .

Nota: Los módulos MIB individuales también se conocen como MIB. por ejemplo, MIB de Grupo de Interfaces (IF-MIB) es un módulo MIB dentro de la MIB de su sistema.

El agente SNMP contiene variables MIB, cuyos valores puede solicitar o cambiar el administrador SNMP mediante operaciones get o set. Un administrador puede obtener un valor de un agente o almacenarlo en ese agente. El agente recopila datos de la MIB, que es el repositorio para la información sobre los parámetros del dispositivo y los datos de red. El agente también puede responder a las solicitudes del jefe para obtener o establecer datos.

Un administrador puede enviar las solicitudes de agente para obtener y establecer valores MIB. El agente puede responder a estas solicitudes. Independientemente de esta interacción, el agente puede enviar notificaciones no solicitadas (trampas o informes) al administrador para notificar al administrador las condiciones de la red. Con algunos mecanismos de seguridad, un NMS puede recuperar información en los MIB con las solicitudes `get` y `get next`, y puede ejecutar el comando

set para cambiar los parámetros. Además, puede configurar un dispositivo de red para generar un mensaje de trampa al NMS para las alertas en tiempo real. Los puertos IP UDP 161 y 162 se utilizan para trampas.

Descripción General de las Operaciones de Notificaciones SNMP

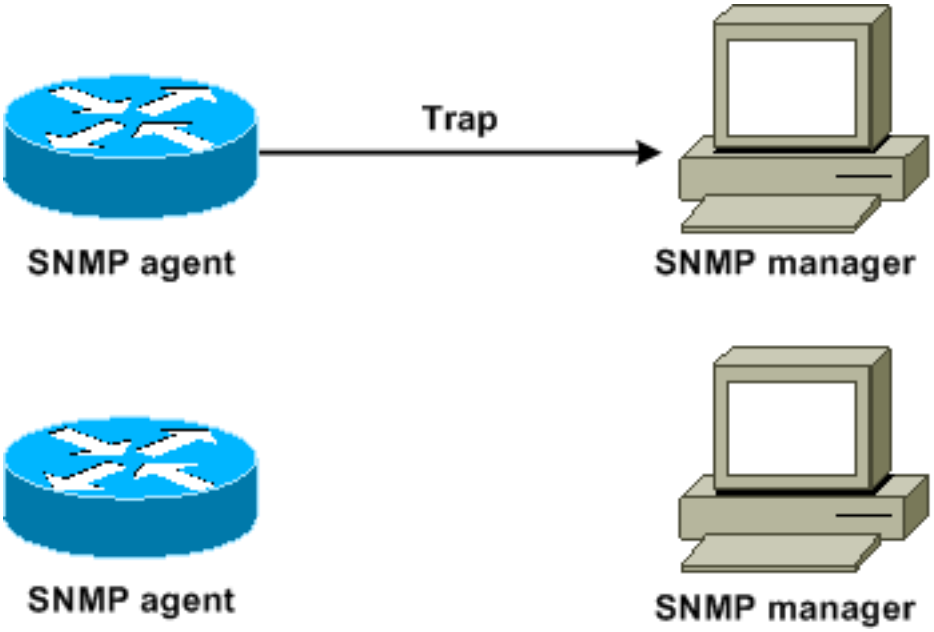
Una característica clave de SNMP es la capacidad de generar notificaciones de un agente SNMP. Estas notificaciones no requieren que se envíen solicitudes del administrador SNMP. Las notificaciones no solicitadas (asincrónicas) se pueden generar como trampas o solicitudes de información. Las trampas son mensajes que alertan al administrador SNMP a una condición en la red. Las solicitudes de información (informes) son trampas que incluyen una solicitud de confirmación de recepción del administrador SNMP. Las notificaciones pueden indicar eventos significativos como:

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

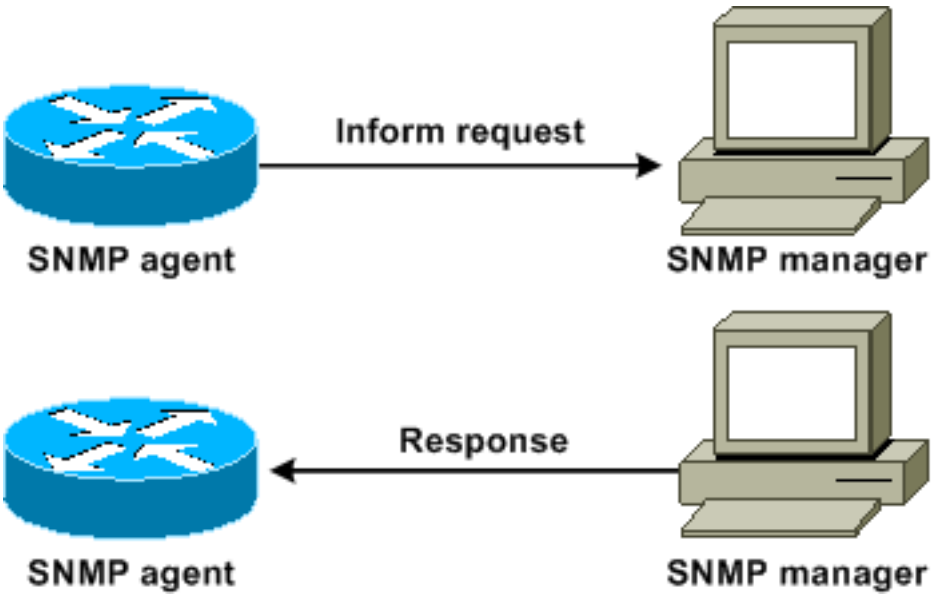
Las trampas son menos confiables que los informes porque el receptor no envía ningún reconocimiento cuando el receptor recibe una trampa. El remitente no puede determinar si se recibió la trampa. Un administrador SNMP que recibe una solicitud de informe reconoce el mensaje con una unidad de datos (PDU) del protocolo de respuesta SNMP. Si el administrador no recibe una solicitud de informe, no envía una respuesta. Si el remitente nunca recibe una respuesta, puede enviar la solicitud de informe de nuevo. Es más probable que los informes lleguen al destino deseado.

Sin embargo, a menudo se prefieren las trampas porque los informes consumen más recursos en el router y en la red. Una trampa se descarta en cuanto se envía. Sin embargo, una solicitud de informe debe mantenerse en la memoria hasta que se reciba una respuesta o se agote el tiempo de espera de la solicitud. Además, las trampas se envían sólo una vez, mientras que un informe se puede volver a intentar varias veces. Los reintentos incrementan el tráfico y contribuyen a una sobrecarga mayor en la red. Por lo tanto, las trampas y las solicitudes de información proporcionan un equilibrio entre la fiabilidad y los recursos. Si necesita que el administrador SNMP reciba cada notificación, utilice las solicitudes de información. Pero si le preocupa el tráfico en la red o la memoria del router y no necesita recibir cada notificación, utilice trampas.

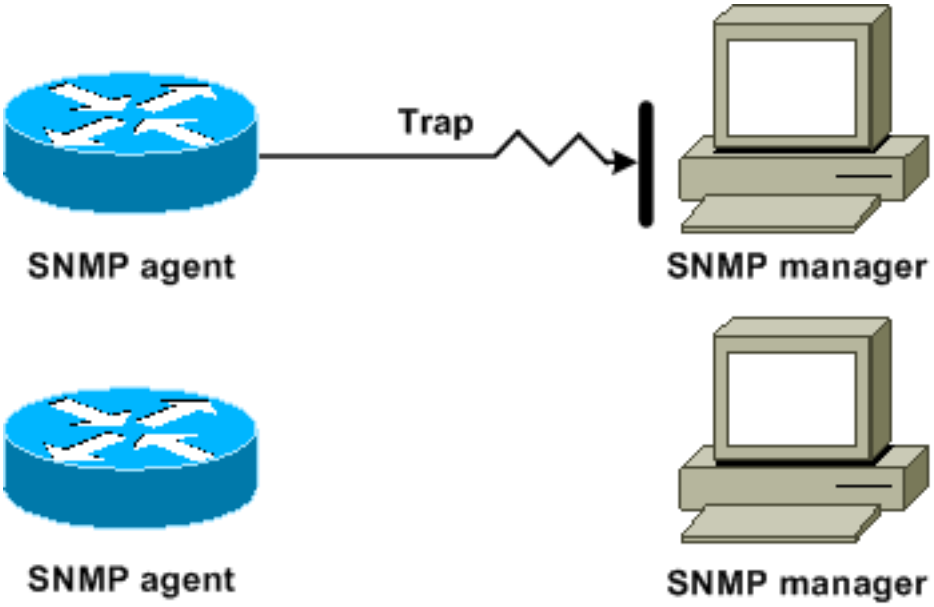
Estos diagramas ilustran las diferencias entre las trampas y las solicitudes de información:



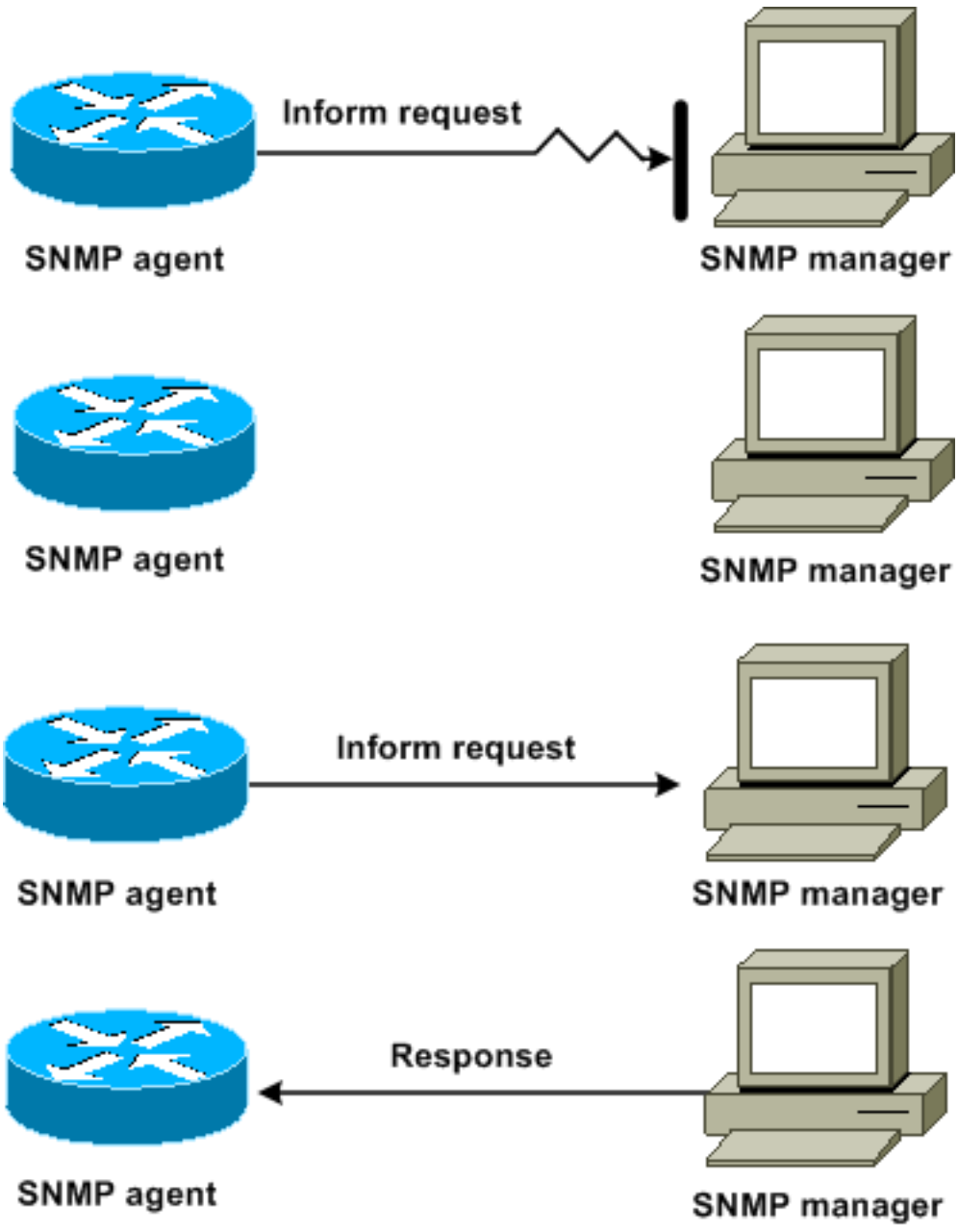
Este diagrama ilustra cómo el router del agente envía con éxito una trampa al administrador SNMP. Aunque el administrador recibe la trampa, el administrador no envía ninguna confirmación al agente. El agente no tiene forma de saber que la trampa llegó al destino.



Este diagrama ilustra cómo el router agente envía con éxito una solicitud de informe al administrador. Cuando el administrador recibe la solicitud de informe, envía una respuesta al agente. De esta manera, el agente sabe que la solicitud de informe llegó al destino. Observe que, en este ejemplo, hay el doble de tráfico. Pero el agente sabe que el administrador recibió la notificación.



En este diagrama, el agente envía una trampa al administrador, pero la trampa no llega al administrador. El agente no tiene forma de saber que la trampa no llegó al destino, por lo que la trampa no se envía de nuevo. El administrador nunca recibe la trampa.



En este diagrama, el agente envía una solicitud de informe al administrador, pero la solicitud de informe no llega al administrador. Como el administrador no recibió la solicitud de informe, no hay respuesta. Después de un período de tiempo, el agente reenvía la solicitud de informe. La segunda vez, el administrador recibe la solicitud de informe y responde con una respuesta. En este ejemplo, hay más tráfico. Pero la notificación llega al administrador SNMP.

Referencia de MIB y RFC de Cisco

Los documentos RFC suelen definir módulos MIB. Los documentos RFC se envían al Grupo de Trabajo de Ingeniería de Internet (IETF), un organismo internacional de estándares. Las personas o los grupos escriben RFC para su consideración por la Sociedad de Internet (ISOC) y la comunidad de Internet en su conjunto. Consulte la página de inicio de Internet Society para obtener información sobre el proceso de normas y las actividades del IETF. Consulte la página de inicio de IETF para leer el texto completo de todos los RFC, borradores de Internet (I-Ds) y STD a los que hacen referencia los documentos de Cisco.

La implementación de Cisco de SNMP utiliza:

- Las definiciones de las variables MIB II que RFC 1213 describe
- Las definiciones de trampas SNMP que RFC 1215 describe

Cisco proporciona sus propias extensiones MIB privadas con cada sistema. Los MIB de Cisco Enterprise cumplen con las pautas que los RFCs relevantes describen, a menos que la documentación indique lo contrario. Puede encontrar los archivos de definición del módulo MIB y una lista de los MIBs soportados en cada plataforma de Cisco en la página de inicio de Cisco MIB.

Versiones SNMP

Cisco IOS Software soporta estas versiones de SNMP:

- SNMPv1: estándar de Internet completo que define RFC 1157 . RFC 1157 reemplaza las versiones anteriores que se publicaron como RFC 1067 y RFC 1098 . La seguridad se basa en las cadenas de comunidad.
- SNMPv2c: SNMPv2c es el marco administrativo basado en cadena de comunidad para SNMPv2. SNMPv2c (la c representa la comunidad) es un protocolo experimental de Internet que RFC 1901 , RFC 1905 y RFC 1906 definen . SNMPv2c es una actualización de las operaciones de protocolo y los tipos de datos de SNMPv2p (SNMPv2 Classic). SNMPv2c utiliza el modelo de seguridad basado en la comunidad de SNMPv1.
- SNMPv3—SNMPv3 es un protocolo interoperable basado en estándares que RFC 2273 , RFC 2274 y RFC 2275 definen . SNMPv3 proporciona acceso seguro a los dispositivos con una combinación de autenticación y cifrado de paquetes a través de la red.Las funciones de seguridad que proporciona SNMPv3 son:Integridad del mensaje: garantiza que un paquete no se ha alterado en tránsito.Autenticación: determina que el mensaje proviene de un origen válido.Cifrado: muestra el contenido de un paquete, lo que impide que un origen no autorizado lo detecte.

Tanto SNMPv1 como SNMPv2c utilizan una forma de seguridad basada en la comunidad. Una ACL de dirección IP y una contraseña definen la comunidad de administradores que pueden acceder a la MIB de agente.

El soporte de SNMPv2c incluye un mecanismo de recuperación masiva e informes de mensajes

de error más detallados a las estaciones de administración. El mecanismo de recuperación masiva permite recuperar tablas y grandes cantidades de información, lo que minimiza el número de viajes de ida y vuelta necesarios. El soporte mejorado de manejo de errores SNMPv2c incluye códigos de error expandidos que distinguen diferentes tipos de condiciones de error. estas condiciones se notifican por medio de un único código de error en SNMPv1. Los códigos de retorno de error informan ahora del tipo de error.

SNMPv3 proporciona tanto modelos de seguridad como niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación que se configura para un usuario y para el grupo en el que el usuario reside. Un nivel de seguridad es el nivel de seguridad permitido dentro de un modelo de seguridad. La combinación de un modelo de seguridad y un nivel de seguridad determina qué mecanismo de seguridad utilizar cuando se maneja un paquete SNMP.

Configuración general de SNMP

Ejecute estos comandos en todos los switches del cliente para habilitar la administración SNMP:

- Comando para ACL SNMP:
  ```
  Switch(config)#access-list 98 permit ip_address
  !--- This is the SNMP device ACL.
  ```
- Comandos SNMP globales:

```
!--- These are sample SNMP community strings. Switch(config)#snmp-server community RO-
community ro 98
snmp-server community RW-community rw 98
snmp-server contact Glen Rahn (Home Number)
snmp-server location text
```

Recomendación de Notificaciones de Trampa de SNMP

SNMP es la base para la administración de la red, y se habilita y utiliza en todas las redes.

Un agente SNMP puede comunicarse con varios administradores. Por esta razón, puede configurar el software para soportar las comunicaciones con una estación de administración con el uso de SNMPv1 y otra estación de administración con el uso de SNMPv2. La mayoría de los clientes y NMS todavía utilizan SNMPv1 y SNMPv2c porque el soporte de dispositivos de red SNMPv3 en las plataformas NMS es un poco lento.

Habilite las trampas SNMP para todas las funciones que están en uso. Si lo desea, puede desactivar otras funciones. Después de habilitar una trampa, puede ejecutar el comando **test snmp** y configurar el manejo apropiado en el NMS para el error. Algunos ejemplos de este manejo incluyen una alerta de localizador o una ventana emergente.

Todas las trampas están desactivadas de forma predeterminada. Habilite todas las trampas en los switches de núcleo, como muestra este ejemplo:

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

También, habilite las trampas de puerto para los puertos clave, como los links de infraestructura a routers y switches, y los puertos de servidor clave. La habilitación no es necesaria para otros

puertos, como los puertos host. Ejecute este comando para configurar el puerto y habilitar la notificación de link activo/inactivo:

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

A continuación, especifique los dispositivos para recibir las trampas y actuar en las trampas de manera apropiada. Ahora puede configurar cada destino de trampa como un destinatario SNMPv1, SNMPv2 o SNMPv3. Para los dispositivos SNMPv3, se pueden enviar informes confiables en lugar de trampas UDP. Esta es la configuración:

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

Recomendaciones de sondeo SNMP

Asegúrese de que estas MIB son las MIB clave que se sondean o monitorean en las redes de campus:

Nota: Esta recomendación proviene del grupo Cisco Network Management Consulting.

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

Network Time Protocol

Propósito

El protocolo de tiempo de red (NTP), RFC 1305 , sincroniza el horario entre un conjunto de servidores de tiempo y clientes distribuidos. NTP permite la correlación de eventos en la creación de registros del sistema y cuando se producen otros eventos específicos de tiempo.

Información Operativa General

RFC 958 documentó primero NTP. Pero NTP ha evolucionado a través de RFC 1119 (NTP versión 2). RFC 1305 ahora define NTP, que está en su tercera versión.

NTP sincroniza la hora de un cliente o servidor de la computadora con otro servidor o fuente de tiempo de referencia, como una radio, receptor satelital o módem. NTP proporciona una precisión del cliente que normalmente se encuentra dentro de un ms en las LAN y hasta unas pocas decenas de ms en las WAN, en relación con un servidor primario sincronizado. Por ejemplo, puede utilizar NTP para coordinar el tiempo universal coordinado (UTC) a través de un receptor de servicio de posicionamiento global (GPS).

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

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

Actualmente, están disponibles las implementaciones de la versión 3 de NTP (NTPv3) y la versión 4 de NTP (NTPv4). La última versión de software en la que se está trabajando es NTPv4, pero el

estándar oficial de Internet sigue siendo NTPv3. Además, algunos proveedores de sistemas operativos personalizan la implementación del protocolo.

Salvaguardias de NTP

La implementación de NTP también intenta evitar la sincronización con una máquina en la que el tiempo no puede ser preciso. NTP lo hace de dos maneras:

- NTP no se sincroniza con una máquina que no está sincronizada.
- NTP siempre compara el tiempo informado por varias máquinas y no se sincroniza con una máquina en la que el tiempo es significativamente diferente de los demás, incluso si esa máquina tiene un estrato más bajo.

Asociaciones

Las comunicaciones entre las máquinas que ejecutan NTP, conocidas como asociaciones, generalmente se configuran estáticamente. Cada máquina recibe las direcciones IP de todas las máquinas con las que necesita formar asociaciones. Es posible realizar un mantenimiento de tiempo preciso mediante el intercambio de mensajes NTP entre cada par de máquinas con una asociación. Pero en un entorno LAN, puede configurar NTP para utilizar los mensajes de difusión IP. Con esta alternativa, puede configurar la máquina para enviar o recibir mensajes de difusión, pero la precisión del tiempo de espera se reduce marginalmente porque el flujo de información es unidireccional.

Si la red está aislada de Internet, la implementación de Cisco NTP le permite configurar una máquina para que actúe como si estuviera sincronizada con el uso de NTP, cuando realmente ha determinado el tiempo con el uso de otros métodos. Otras máquinas se sincronizan con esa máquina con el uso de NTP.

Una asociación NTP puede ser:

- Una asociación de peersEsto significa que este sistema puede sincronizarse con el otro o permitir que el otro sistema se sincronice con él.
- Una asociación de servidorEsto significa que sólo este sistema se sincroniza con el otro sistema. El otro sistema no se sincroniza con este sistema.

Si desea formar una asociación NTP con otro sistema, utilice uno de estos comandos en el modo de configuración global:

Comando	Propósito
ntp peer *ip-address* [normal-sync] [version *number*] [key *key-id*] [source *interface*] [prefer]	Crea una asociación de peers con otro sistema
ntp server *ip-address* [version *number*] [key *key-id*] [source *interface*] [prefer]	Crea una asociación de servidor con otro sistema

Nota: Sólo es necesario configurar un extremo de una asociación. El otro sistema establece automáticamente la asociación.

Acceder a los servidores de hora pública

La subred NTP incluye actualmente más de 50 servidores públicos primarios que se sincronizan directamente con UTC mediante 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. Hay unos 100 servidores públicos secundarios que están sincronizados con los servidores principales. Estos servidores proporcionan sincronización a un total de más de 100 000 clientes y servidores en Internet. La página Public NTP Servers mantiene las listas actuales y se actualiza con frecuencia.

Además, hay numerosos servidores privados primarios y secundarios que normalmente no están disponibles para el público. Consulte Proyecto de protocolo de tiempo de red (Universidad de Delaware) para ver una lista de servidores NTP públicos e información sobre cómo utilizarlos. No hay garantía de que estos servidores NTP públicos de Internet estén disponibles y produzcan la hora correcta. Por lo tanto, debe considerar otras opciones. Por ejemplo, utilice varios dispositivos GPS independientes que están conectados directamente a varios routers.

Otra opción es el uso de varios routers, establecidos como maestro de Estrato 1. Pero no se recomienda el uso de tal router.

Estrato

NTP utiliza un estrato para describir el número de saltos NTP que una máquina está lejos de una fuente de tiempo autorizada. Un servidor de hora de estrato 1 tiene un reloj atómico o de radio conectado directamente. Un servidor de hora de estrato 2 recibe su tiempo de un servidor de hora de estrato 1, etc. Una máquina que ejecuta NTP elige automáticamente como su origen de tiempo la máquina con el número de estrato más bajo con el que se configura para comunicarse a través de NTP. Esta estrategia construye efectivamente un árbol auto-organizado de altavoces NTP.

NTP evita la sincronización con un dispositivo en el que es posible que la hora no sea exacta. Consulte la sección *NTP Safeguards* de Network Time Protocol para obtener detalles.

Relación Peer del Servidor

- Un servidor responde a las solicitudes del cliente pero no intenta incorporar ninguna información de fecha de un origen de hora del cliente.
- Un par responde a las solicitudes de los clientes e intenta utilizar la solicitud del cliente como candidato potencial para obtener una mejor fuente de tiempo y ayudar a estabilizar su frecuencia de reloj.
- Para ser peers verdaderos, ambos lados de la conexión deben entrar en una relación de peers, en lugar de una situación en la que un usuario funciona como peer y el otro usuario como servidor. Que los pares intercambien claves para que sólo los hosts confiables puedan hablar con otros como pares.
- En una solicitud de cliente a un servidor, el servidor responde al cliente y olvida que el cliente hizo una pregunta.
- En una solicitud de cliente a un par, el servidor responde al cliente. El servidor mantiene la información de estado sobre el cliente para realizar un seguimiento de lo bien que el cliente realiza en el mantenimiento de la hora y qué servidor de estrato ejecuta el cliente.

Un servidor NTP puede manejar muchos miles de clientes sin problemas. Pero cuando un servidor NTP gestiona más de unos pocos clientes (hasta unos pocos cientos), la capacidad del servidor para conservar la información de estado tiene un impacto en la memoria. Cuando un servidor NTP maneja más de la cantidad recomendada, se consumen más recursos de CPU y ancho de banda en la caja.

Modos de comunicación con el servidor NTP

Estos son dos modos separados para comunicarse con el servidor:

- Modo de difusión
- Modo cliente/servidor

En el modo de difusión, los clientes escuchan. En el modo cliente/servidor, los clientes sondean el servidor. Puede utilizar la difusión NTP si no hay ningún enlace WAN debido a su velocidad. Para atravesar un link WAN, utilice el modo cliente/servidor (mediante sondeo). El modo de difusión está diseñado para una LAN, en la que muchos clientes pueden necesitar sondear el servidor. Sin el modo de broadcast, este sondeo puede generar un gran número de paquetes en la red. La multidifusión NTP todavía no está disponible en NTPv3, pero está disponible en NTPv4.

De forma predeterminada, Cisco IOS Software se comunica con el uso de NTPv3. Pero el software es compatible con versiones anteriores de NTP.

Sondeo

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

Al configurar por primera vez NTP en un cuadro de Cisco, NTP envía ocho consultas en sucesión rápida en intervalos `NTP_MINPOLL` (2^4=16 s). `NTP_MAXPOLL` es de 2^14 segundos (16.384 s o 4 horas, 33 min, 4 s). Este período de tiempo es el período más largo antes de que el NTP vuelva a sondear para obtener una respuesta. Actualmente, Cisco no dispone de un método que permita al usuario forzar manualmente el tiempo `POLL`.

El contador de sondeo de NTP comienza a los 2^6 (64) s, o 1 min, 4 s. Esta vez se incrementa con poderes de 2, a medida que los dos servidores se sincronizan entre sí, a 2^10. Puede esperar que los mensajes de sincronización se envíen en un intervalo de uno de 64, 128, 256, 512 o 1024 s, según la configuración del servidor o del par. Cuanto más tiempo transcurre entre los sondeos, más estable es el reloj actual debido a los loops de fase bloqueada. Los loops de bloqueo de fase recortan el cristal del reloj local, hasta 1024 segundos (17 min).

El tiempo varía entre 64 segundos y 1024 segundos como una potencia de 2 (que equivale a una vez cada 64, 128, 256, 512 o 1024 segundos). El tiempo se basa en el loop de fase bloqueada que envía y recibe paquetes. Si hay mucha fluctuación en el tiempo, el sondeo se produce con más frecuencia. Si el reloj de referencia es preciso y la conectividad de red es uniforme, los tiempos de sondeo convergen en 1024 segundos entre cada sondeo.

El intervalo de sondeo NTP cambia a medida que cambia la conexión entre el cliente y el servidor. Con una mejor conexión, el intervalo de sondeo es más largo. En este caso, una mejor conexión significa que el cliente NTP ha recibido ocho respuestas para las últimas ocho solicitudes. El intervalo de sondeo se duplica. Una única respuesta perdida hace que el intervalo de sondeo se reduzca a la mitad. El intervalo de sondeo comienza a los 64 segundos y alcanza un máximo de 1024 segundos. En las mejores circunstancias, el tiempo requerido para que el intervalo de sondeo pase de 64 segundos a 1024 segundos es poco más de 2 horas.

Difusiones

Las broadcasts NTP nunca se reenvían. Si ejecuta el comando **ntp broadcast**, el router comienza a originar broadcasts NTP en la interfaz en la que está configurado.

Normalmente, usted ejecuta el comando **ntp broadcast** para enviar broadcasts NTP a una LAN para atender las estaciones finales del cliente y los servidores.

Sincronización horaria

La sincronización de un cliente con un servidor consiste en varios intercambios de paquetes. Cada intercambio es un par de solicitud/respuesta. Cuando un cliente envía una solicitud, el cliente almacena su hora local en el paquete enviado. Cuando un servidor recibe el paquete, almacena su propia estimación de la hora actual en el paquete y se devuelve el paquete. Cuando se recibe la respuesta, el receptor registra una vez más su propio tiempo de recepción para estimar el tiempo de viaje del paquete.

Estas diferencias de tiempo se pueden utilizar para estimar el tiempo necesario para que el paquete transmita del servidor al solicitante. Ese tiempo de ida y vuelta se tiene en cuenta para una estimación de la hora actual. Cuanto más corto sea el tiempo de ida y vuelta, más precisa será la estimación del tiempo actual.

El tiempo no se acepta hasta que se hayan realizado varios intercambios de paquetes de acuerdo. Algunos valores esenciales se colocan en filtros multietapas para estimar la calidad de las muestras. Por lo general, son necesarios unos 5 minutos para que un cliente NTP se sincronice con un servidor. Curiosamente, esto también se aplica a los relojes de referencia locales que no tienen ningún retraso por definición.

Además, la calidad de la conexión de red también influye en la precisión final. Las redes lentas e impredecibles con retrasos variables tienen un efecto negativo en la sincronización horaria.

Se requiere una diferencia de tiempo inferior a 128 ms para que NTP se sincronice. La precisión típica en Internet varía entre unos 5 ms y 100 ms, lo que puede variar con los retrasos en la red.

Niveles de Tráfico de NTP

El ancho de banda que utiliza el NTP es mínimo. El intervalo entre los mensajes de sondeo que los pares intercambian generalmente vuelve a tener no más de un mensaje cada 17 min (1024 s). Con una planificación cuidadosa, puede mantener esto dentro de las redes de router a través de los links WAN. Haga que los clientes NTP se conecten a los servidores NTP locales y no en toda la WAN a los routers de núcleo de sitio central, que son los servidores de nivel 2.

Un cliente NTP convergente utiliza promedios de 0,6 bits por segundo (bps) por servidor.

Recomendación de Cisco NTP

- Cisco recomienda que tenga varios servidores de tiempo y diversas rutas de red para lograr una alta precisión y fiabilidad. Algunas configuraciones incluyen la autenticación criptográfica para prevenir los ataques maliciosos o accidentales al protocolo.
- Según el RFC, NTP está diseñado realmente para permitirle sondear varios servidores de tiempo diferentes y utilizar análisis estadísticos complicados para obtener un tiempo válido, incluso si no está seguro de que todos los servidores que sondea son autoritarios. NTP calcula los errores de todos los relojes. Por lo tanto, todos los servidores NTP devuelven el tiempo junto con una estimación del error actual. Cuando utiliza varios servidores de tiempo, NTP también desea que estos servidores coincidan en algún momento.
- La implementación de Cisco de NTP no admite el servicio del estrato 1. No puede conectarse

a un radio o reloj atómico. Cisco recomienda que el servicio de hora de su red se derive de los servidores NTP públicos disponibles en Internet IP.

- Habilite todos los switches cliente para enviar regularmente solicitudes de hora del día a un servidor NTP. Puede configurar hasta 10 direcciones de servidor/par por cliente para que pueda lograr una sincronización rápida.
- Para reducir la sobrecarga del protocolo, los servidores secundarios distribuyen el tiempo a través de NTP a los hosts de red local restantes. En aras de la fiabilidad, puede equipar a los hosts seleccionados con relojes menos precisos pero menos costosos para utilizarlos en el caso de una falla de los servidores primario y/o secundario o de las trayectorias de comunicación entre ellos.
- **ntp update-calendar**: NTP generalmente cambia solamente el reloj del sistema. Este comando permite que NTP actualice la información de fecha y hora en el calendario. La actualización se realiza solamente si la hora NTP está sincronizada. De lo contrario, el calendario mantiene su propia hora y no se ve afectado por la hora NTP o el reloj del sistema. Utilice siempre esto en los routers de gama alta.
- **clock calendar-valid**: este comando declara que la información del calendario es válida y sincronizada. Utilice esta opción en el maestro NTP. Si esto no se configura, el router de gama alta que tiene el calendario todavía piensa que su hora es no autoritativa, incluso si tiene la línea maestra NTP.
- Cualquier número de estrato superior a 15 se considera no sincronizado. Esta es la razón por la que ve el estrato 16 en el resultado del comando **show ntp status** en los routers para los cuales los relojes no están sincronizados. Si el maestro está sincronizado con un servidor NTP público, asegúrese de que el número de estrato de la línea principal NTP sea uno o dos más alto que el número de estrato más alto de los servidores públicos que sondee.
- Muchos clientes tienen NTP configurado en modo de servidor en sus plataformas de Cisco IOS Software, sincronizados desde varias fuentes fiables de Internet o desde un reloj de radio. Internamente, una alternativa más simple al modo de servidor cuando usted opera un gran número de switches es habilitar NTP en el modo broadcast en la VLAN de administración en un dominio conmutado. Este mecanismo permite al Catalyst recibir un reloj de mensajes de broadcast únicos. Sin embargo, la precisión en el tiempo se reduce marginalmente porque el flujo de información es unidireccional.
- El uso de direcciones de loopback como fuente de actualizaciones también puede ayudar con la consistencia. Puede abordar los problemas de seguridad de dos maneras:Con el control de las actualizaciones del servidor, que Cisco recomiendaPor autenticación

Comandos de Configuración Global NTP

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1

!--- For the server: clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ntp source loopback0
ntp update-calendar
```

```
!--- This is optional: interface vlan_id ntp broadcast
!--- This sends NTP broadcast packets. ntp broadcast client
!--- This receives NTP broadcast packets. ntp authenticate
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
!--- This provides further security, if needed.
```

Comando de estado NTP

```
show ntp status

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

Esta es la dirección del reloj de referencia para el router Cisco cuando el router actúa como maestro NTP. Si el router no se ha sincronizado con ningún servidor NTP, el router utiliza esta dirección como ID de referencia. Para obtener detalles sobre la configuración y los comandos, consulte la sección *Configuración de NTP* de Administración Básica del Sistema.

Cisco Discovery Protocol

Propósito

CDP se ejecuta en la capa 2 (capa de enlace de datos) en todos los routers, puentes, servidores de acceso y switches de Cisco. CDP permite a las aplicaciones de administración de red detectar dispositivos de Cisco que son vecinos de dispositivos ya conocidos. En particular, las aplicaciones de administración de red pueden detectar vecinos que ejecutan protocolos transparentes de capa inferior. Con CDP, las aplicaciones de administración de red pueden aprender el tipo de dispositivo y la dirección de agente SNMP de los dispositivos vecinos. Esta función permite que las aplicaciones envíen consultas SNMP a los dispositivos vecinos.

Los comandos **show** asociados a la función CDP permiten al ingeniero de red determinar esta información:

- Número de módulo/puerto de otros dispositivos CDP adyacentes
- Estas direcciones del dispositivo adyacente:Dirección MACDirección IPDirección de canal de puerto
- La versión de software del dispositivo adyacente
- Esta información sobre el dispositivo adyacente:VelocidadDúplexDominio de VTPConfiguración de VLAN nativa

La sección Descripción General Operativa resalta algunas de las mejoras de CDP versión 2 (CDPv2) sobre CDP versión 1 (CDPv1).

Información Operativa General

CDP se ejecuta en todos los medios LAN y WAN que admiten SNAP.

Cada dispositivo configurado en CDP envía mensajes periódicos a una dirección multicast. Cada dispositivo anuncia al menos una dirección en la que el dispositivo puede recibir mensajes SNMP.

Los anuncios también contienen información sobre el tiempo de vida o de espera. Esta información indica el tiempo que un dispositivo receptor debe mantener la información CDP antes del descarte.

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

Los mensajes CDP contienen uno o más mensajes que permiten al dispositivo de destino recopilar y almacenar información sobre cada dispositivo vecino.

Esta tabla proporciona los parámetros que soporta CDPv1:

Parámetro	Tipo	Descripción
1	ID del dispositivo	Nombre de host del dispositivo o número de serie del hardware en ASCII
2	Dirección	La dirección de Capa 3 de la interfaz que envía la actualización
3	Identificación del puerto	El puerto en el que se envía la actualización CDP
4	Capacidades	Describe las funciones del dispositivo de esta manera: • Router: 0x01 • Bridge SR[1]: 0x04 • Switch: 0x08 (proporciona switching de capa 2 o capa 3) • Host: 0x10 • Filtrado condicional IGMP: 0x20 • El puente o el switch no reenvía los paquetes de informes IGMP en los puertos que no son del router.
5	Versión	Cadena de caracteres que contiene la versión de software **Nota:** El resultado del comando **show version** muestra la misma información.
6	Platform	La plataforma de hardware, por ejemplo, WS-C5000, WS-C6009 y Cisco RSP[2]

[1] SR = ruta de origen.

[2] RSP = Procesador de switch de ruta.

En CDPv2, se han introducido tipos, longitud y valores adicionales (TLV). CDPv2 admite cualquier TLV. Pero esta tabla proporciona los parámetros que pueden ser particularmente útiles en entornos conmutados y que el software Catalyst utiliza.

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

Parámetro	Tipo	Descripción
9	Dominio de VTP	El dominio VTP, si está configurado en el dispositivo
10	VLAN nativa	En dot1q, las tramas para la VLAN, en la que se encuentra el puerto si el puerto no se conecta mediante trunking, permanecen sin etiquetar. Esto se denomina generalmente VLAN nativa.
11	Dúplex Medio/ Total	Este TLV contiene la configuración dúplex del puerto de envío.
14	ID de VLAN del dispositivo	Permite que el tráfico VoIP se diferencie de otro tráfico mediante un ID de VLAN independiente (VLAN auxiliar).
16	Consumo de Energía	Cantidad máxima de energía que se espera que el dispositivo conectado consuma, en mW.
17	MTU (unidad de transmisión básica)	La MTU de la interfaz por la cual se transmite la trama CDP.
18	Confianza ampliada	Indica que el puerto está en el modo de confianza extendida.
19	COS para puertos no confiables	Valor de clase de servicio (CoS) que se utilizará para marcar todos los paquetes recibidos en el puerto no confiable de un dispositivo de switching conectado.
20	SysName	Nombre de dominio completo del dispositivo (0, si se desconoce).
25	Energía solicitada	Transmitido por un dispositivo con alimentación para negociar un nivel de energía adecuado.
26	Alimentación disponi	Transmitido por un switch. Permite a un dispositivo con alimentación negociar y seleccionar una configuración de

	ble	alimentación adecuada.

CDPv2/Power over Ethernet

Algunos switches, como los Catalyst 6500/6000 y 4500/4000, tienen la capacidad de suministrar energía a los dispositivos con alimentación a través de cables de par trenzado (UTP) no blindados. La información que se recibe a través de CDP (Parámetros 16, 25, 26) ayuda en la optimización de la administración de energía del switch.

Interacción entre teléfonos IP CDPv2/Cisco

Los teléfonos IP de Cisco proporcionan conectividad para un dispositivo Ethernet de 10/100 Mbps conectado externamente. Esta conectividad se consigue mediante la integración de un switch interno de capa 2 de tres puertos en el teléfono IP. Los puertos de switch internos se denominan:

- P0 (dispositivo telefónico IP interno)
- P1 (puerto externo de 10/100 Mbps)
- P2 (puerto externo de 10/100 Mbps que se conecta al switch)

Puede transferir tráfico de voz en una VLAN independiente en el puerto del switch si configura los puertos trunk de acceso dot1q. Esta VLAN adicional se conoce como VLAN auxiliar (CatOS) o de voz (Cisco IOS Software). En consecuencia, el tráfico etiquetado dot1q del teléfono IP se puede enviar en la VLAN auxiliar/de voz, y el tráfico sin etiqueta se puede enviar a través del puerto externo 10/100-Mbps del teléfono a través de la VLAN de acceso.

Los switches Catalyst pueden informar a un teléfono IP del ID de VLAN de voz a través de CDP (Parámetro 14: Dispositivo VLAN-ID TLV). Como resultado, el teléfono IP etiqueta todos los paquetes relacionados con VoIP con el ID de VLAN apropiado y la prioridad 802.1p. Este TLV CDP también se utiliza para identificar si un teléfono IP está conectado a través del parámetro ID del dispositivo.

Este concepto se puede aprovechar al desarrollar una política de QoS. Puede configurar el switch Catalyst para interactuar con el teléfono IP de tres maneras:

- Teléfono IP de Cisco con dispositivo de confianzaConfiar condicionalmente en CoS sólo cuando se detecta un teléfono IP a través de CDP. Siempre que se detecta un teléfono IP a través del parámetro CDP-14, el estado de confianza del puerto se establece en COS de confianza. Si no se detecta ningún teléfono IP, el puerto no es de confianza.
- Confianza ampliadaEl switch puede informar al teléfono IP a través de CDP (Parámetro 18) para que confíe en todas las tramas recibidas en su puerto de dispositivo externo de 10/100 Mbps.
- Reescritura de COS para puertos no confiablesEl switch puede informar al teléfono IP a través de CDP (Parámetro 19) para reescribir los valores 802.1p CoS recibidos en su puerto de dispositivo externo de 10/100 Mbps.**Nota:** De forma predeterminada, todo el tráfico que se recibe en los puertos externos de 10/100 Mbps del teléfono IP no es de confianza.

Nota: Este es un ejemplo de configuración para conectar el teléfono IP que no es de Cisco a un switch.

Nota: Por ejemplo,

```
Switch(config)#interface gigabitEthernet 2/1
```

```
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk

!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Recomendación de configuración de Cisco

La información que CDP proporciona puede ser extremadamente útil cuando se resuelven problemas de conectividad de Capa 2. Habilite CDP en todos los dispositivos que soportan su funcionamiento. Ejecute estos comandos:

- Para habilitar el CDP globalmente en el switch:
  ```
  Switch(config)#cdp run
  ```

- Para habilitar CDP por puerto:
  ```
  Switch(config)#interface type slot#/port#
  Switch(config-if)#cdp enable
  ```

Configuración de Lista de Verificación

Comandos globales

Inicie sesión, habilite e ingrese en el modo de configuración global para comenzar el proceso de configuración del switch.

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

Comandos globales genéricos (para toda la empresa)

Esta sección Comandos globales enumera los comandos globales que se aplican a todos los switches en la red empresarial del cliente.

Esta configuración contiene los comandos globales recomendados para agregar a la configuración inicial. Debe cambiar los valores del resultado antes de copiar y pegar el texto en la CLI. Ejecute estos comandos para aplicar la configuración global:

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
```

```
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

Comandos globales específicos de cada chasis de switch

Los comandos globales de esta sección son específicos de cada chasis de switch que se instala en la red.

Variables de configuración específicas del chasis

Para establecer la fecha y la hora, ejecute este comando:

```
Switch#clock set hh:mm:ss day month year
```

Para configurar el nombre de host del dispositivo, ejecute estos comandos:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat6500
```

Para configurar la interfaz de loopback para la administración, ejecute estos comandos:

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

Para mostrar la revisión del Supervisor Engine Cisco IOS Software, ejecute estos comandos:

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

Para mostrar la revisión del archivo de arranque MSFC, ejecute este comando:

```
Cat6500#dir bootflash:
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

Para especificar la información de contacto y la ubicación del servidor SNMP, ejecute estos comandos:

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

Para copiar la configuración de inicio de un Supervisor Engine existente a un nuevo Supervisor Engine, podría haber alguna pérdida de configuración, por ejemplo, la configuración en las interfaces del supervisor existente. Cisco recomienda copiar la configuración en un archivo de texto y pegarla en segmentos en la consola para ver si se producen problemas de configuración.

Comandos de interfaz

Tipos de puertos funcionales de Cisco

Los puertos del switch en el software Cisco IOS se denominan interfaces. Hay dos tipos de modos de interfaz en Cisco IOS Software:

- Interfaz enrutada de capa 3
- Interfaz de switch de capa 2

La función de interfaz se refiere a cómo se ha configurado el puerto. La configuración del puerto puede ser:

- Interfaz enrutada
- Interfaz virtual conmutada (SVI)
- Puerto de acceso
- Tronco
- EtherChannel
- Una combinación de estos

El tipo de interfaz se refiere a un tipo de puerto. El tipo de puerto puede ser:

- FE
- GE
- Canal de puerto

Esta lista describe brevemente las diferentes funciones de la interfaz de Cisco IOS Software:

- Interfaz física enrutada (predeterminada): cada interfaz del switch es una interfaz de capa 3 enrutada de forma predeterminada, similar a cualquier router de Cisco. La interfaz enrutada debe estar en una subred IP única.
- Interfaz de puerto del switch de acceso: esta función se utiliza para colocar interfaces en la misma VLAN. Los puertos se deben convertir de una interfaz ruteada a una interfaz conmutada.
- SVI: una SVI se puede asociar a una VLAN que contiene puertos de switch de acceso para el ruteo entre VLAN. Configure el SVI para asociarlo a una VLAN cuando desee una ruta o un puente entre los puertos del switch de acceso en diferentes VLAN.
- Interfaz de puerto del switch troncal: esta función se utiliza para transportar varias VLAN a otro dispositivo. Los puertos se deben convertir de una interfaz ruteada a un puerto de switch troncal.
- EtherChannel: se utiliza un EtherChannel para agrupar puertos individuales en un único puerto lógico para obtener redundancia y equilibrio de carga.

Recomendaciones sobre el tipo de puerto funcional de Cisco

Utilice la información de esta sección para ayudar a determinar los parámetros que se aplicarán a las interfaces.

Nota: Algunos comandos específicos de la interfaz se incorporan siempre que es posible.

Negociación automática

No utilice negociación automática en ninguna de estas situaciones:

- Para puertos que admiten dispositivos de infraestructura de red como switches y routers

- Para otros sistemas finales no transitorios, como servidores e impresoras

Configure manualmente para velocidad y dúplex estas configuraciones de link de 10/100 Mbps. Las configuraciones suelen ser 100-Mbps full-duplex:

- Switch a switch de enlace de 100 MB
- Enlace de 100 MB de switch a servidor
- Enlace de 100 MB de switch a router

Puede configurar estos parámetros de esta manera:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

Cisco recomienda configuraciones de enlace de 10/100 Mbps para los usuarios finales. Los trabajadores móviles y los hosts transitorios necesitan negociación automática, como muestra este ejemplo:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

El valor predeterminado en las interfaces Gigabit es `negociación automática`. Pero ejecute estos comandos para asegurarse de que la negociación automática esté habilitada. Cisco recomienda habilitar la negociación Gigabit:

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

Raíz del Spanning Tree

Teniendo en cuenta el diseño de la red, identifique el switch que mejor se adapte para ser la raíz de cada VLAN. Por lo general, elija un switch potente en medio de la red. Coloque el puente raíz en el centro de la red y conecte directamente el puente raíz a los servidores y routers. Esta configuración generalmente reduce la distancia promedio de los clientes a los servidores y routers. Consulte la sección Spanning Tree Protocol Problems and Related Design Considerations (Problemas en el protocolo de árbol de expansión y consideraciones de diseño) para obtener más información.

Para obligar a un switch a ser la raíz de una VLAN designada, ejecute este comando:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

Spanning Tree PortFast

PortFast omite el funcionamiento normal del spanning tree en los puertos de acceso para acelerar los retrasos iniciales de conectividad que ocurren cuando las estaciones finales están conectadas a un switch. Refiérase a Uso de PortFast y Otros Comandos para Solucionar Demoras de Conectividad de Inicio de la Estación de Trabajo para obtener más información sobre PortFast.

Establezca STP PortFast en on para todos los puertos de acceso habilitados que están conectados a un solo host. Aquí tiene un ejemplo:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

Habilite el UDLD solamente en los puertos de infraestructura conectados por fibra o en los cables Ethernet de cobre para monitorear la configuración física de los cables. Ejecute estos comandos para habilitar el UDLD:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

Información de Configuración de VLAN

Configure las VLAN con estos comandos:

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

Repita los comandos para cada VLAN y luego salga. Ejecutar este comando:

```
Cat6500(config)#exit
```

Ejecute este comando para verificar todas las VLAN:

```
Cat6500#show vlan
```

SVI enrutadas

Configure los SVI para el ruteo entre VLAN. Ejecute estos comandos:

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

Repita estos comandos para cada función de interfaz que contenga una SVI ruteada y luego salga. Ejecutar este comando:

```
Cat6500(config-if)#^Z
```

Interfaz física única enrutada

Ejecute estos comandos para configurar la interfaz de Capa 3 ruteada predeterminada:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

Repita estos comandos para cada función de interfaz que contenga una interfaz física ruteada y, a continuación, salga. Ejecutar este comando:

```
Cat6500(config-if)#^Z
```

EtherChannel enrutado (L3)

Para configurar EtherChannel en las interfaces de Capa 3, ejecute los comandos en esta sección.

Configure una interfaz lógica de canal de puerto de esta manera:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

Realice los pasos de esta sección para los puertos que forman ese canal en particular. Aplique la información restante al canal de puerto, como muestra este ejemplo:

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

Nota: Después de configurar un EtherChannel, la configuración que aplica a la interfaz de canal de puerto afecta al EtherChannel. La configuración que se aplica a los puertos LAN afecta solamente al puerto LAN donde se aplica la configuración.

EtherChannel (L2) con enlace troncal

Configure el EtherChannel de Capa 2 para el trunking de esta manera:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Realice los pasos de esta sección solamente para los puertos que forman ese canal en particular.

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Nota: Después de configurar un EtherChannel, la configuración que aplica a la interfaz de canal de puerto afecta al EtherChannel. La configuración que se aplica a los puertos LAN afecta solamente al puerto LAN donde se aplica la configuración.

Verifique la creación de todos los EtherChannels y trunks. Aquí tiene un ejemplo:

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

Puertos de acceso

Si la función de interfaz es un puerto de acceso configurado como una sola interfaz, ejecute estos comandos:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

Repita estos comandos para cada interfaz que deba configurarse como puerto de switch de Capa 2.

Si el puerto del switch se va a conectar a las estaciones finales, ejecute este comando:

```
Cat6500(config-if)#spanning-tree portfast
```

Puerto troncal (interfaz física única)

Si la función de interfaz es un puerto trunk que se configura como una sola interfaz, ejecute estos comandos:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Repita estos comandos para cada función de interfaz que deba configurarse como puerto troncal.

Información de contraseña

Ejecute estos comandos para obtener información de contraseña:

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password

CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

Guarde la configuración

Ejecute este comando para guardar la configuración:

```
Cat6500#copy running-config startup-config
```

Nuevas Funciones de Software de Cisco IOS Software Release 12.1(13)E

Consulte Configuración del Soporte del Teléfono IP de Cisco para obtener más información sobre el soporte del teléfono IP.

Consulte Reconocimiento de aplicaciones basadas en la red y Reconocimiento de aplicaciones basadas en la red distribuida para obtener más información sobre el Reconocimiento de aplicaciones basadas en la red (NBAR) para los puertos LAN.

Notas:

- NBAR para puertos LAN se soporta en el software en el MSFC2.
- El PFC2 proporciona soporte de hardware para las ACL de entrada en los puertos LAN donde se configura NBAR.
- Cuando se habilita la QoS de PFC, el tráfico a través de los puertos LAN donde se configura NBAR pasa a través de las colas de ingreso y egreso y los umbrales de descarte.
- Cuando se habilita la QoS de PFC, la MSFC2 establece la clase de servicio de salida (CoS) igual a la precedencia IP de salida.
- Después de que el tráfico pasa a través de una cola de ingreso, todo el tráfico se procesa en el software en el MSFC2 en los puertos LAN donde se configura NBAR.
- La NBAR distribuida está disponible en las interfaces FlexWAN con la versión 12.1(6)E y posteriores del software del IOS de Cisco.

Las mejoras de NetFlow Data Export (NDE) incluyen:

- Máscara de flujo de interfaz de origen de destino y de interfaz completa
- NDE versión 5 de PFC2
- NetFlow de muestra
- Opción para rellenar estos campos adicionales en los registros NDE:Dirección IP del router de salto siguienteInterfaz de entrada SNMP ifIndexInterfaz de salida SNMP ifIndexNúmero de

sistema autónomo de origen

Consulte Configuración de NDE para obtener más información sobre estas mejoras.

Otras mejoras de las funciones incluyen:

- Configuración de UDLD
- Configuración de VTP
- Configuración de Servicios de Caché Web Usando WCCP

Estos comandos son nuevos comandos:

- **standby delay minimum reload**
- **link debounce**
- **política de asignación interna de VLAN {ascendente | descendente}**
- **system jumbomtu**
- **clear catalyst6000 traffic-meter**

Estos comandos son comandos mejorados:

- **show vlan internal usage**: este comando se mejoró para incluir las VLAN que utilizan las interfaces WAN.
- **show vlan id**: este comando se mejoró para soportar la entrada de un rango de VLAN.
- **show l2protocol-tunnel**: este comando se mejoró para soportar la entrada de un ID de VLAN.

La versión 12.1(13)E del software del IOS de Cisco admite estas funciones de software, que anteriormente se admitían en las versiones 12.1 EX del software del IOS de Cisco:

- Configuración de EtherChannels de Capa 2 que incluyen interfaces en diferentes módulos de conmutación equipados con DFCConsulte la sección Advertencias generales resueltas en la versión 12.1(13)E del Id. de bug Cisco CSCdt27074 (sólo clientes registrados) .
- Redundancia de Route Processor Redundancy Plus (RPR+)Consulte Configuración de la Redundancia de RPR o RPR+ Supervisor Engine.**Nota:** En Cisco IOS Software Release 12.1(13)E y posteriores, las funciones de redundancia RPR y RPR+ reemplazan la redundancia mejorada de alta disponibilidad del sistema (EHSA).
- 4096 VLAN de capa 2Consulte Configuración de VLAN.**Nota:** Cisco IOS Software Release 12.1(13)E y versiones posteriores soportan la configuración de 4096 interfaces VLAN de Capa 3. Configure un total combinado de no más de 2000 interfaces VLAN de Capa 3 y puertos de Capa 3 en una MSFC2 con un Supervisor Engine II o un Supervisor Engine I. Configure un total combinado de no más de 1000 interfaces VLAN de capa 3 y puertos de capa 3 en una MSFC.
- Tunelización IEEE 802.1QConsulte Configuración de Tunelización IEEE 802.1Q y Tunelización de Protocolo de Capa 2.
- Tunelización del protocolo IEEE 802.1QConsulte Configuración de Tunelización IEEE 802.1Q y Tunelización de Protocolo de Capa 2.
- Árbol de extensión múltiple (MST) IEEE 802.1sConsulte Configuración de STP e IEEE 802.1s MST.
- STP rápido (RSTP) IEEE 802.1wConsulte Configuración de STP e IEEE 802.1s MST.
- LACP IEEE 802.3adConsulte Configuración de EtherChannel de Capa 3 y Capa 2.
- Filtrado de PortFast BPDUConsulte Configuración de las Funciones STP.
- Creación automática de interfaces VLAN de capa 3 para admitir VLAN ACL (VACL)Consulte Configuración de la Seguridad de la Red.

- VACL captura puertos que pueden ser cualquier puerto Ethernet de Capa 2 en cualquier VLANConsulte Configuración de la Seguridad de la Red.
- Tamaño de MTU configurable en puertos físicos individuales de capa 3Consulte Descripción General de la Configuración de la Interfaz.
- Configuración de los puertos de destino SPAN como troncales de modo que todo el tráfico SPAN esté etiquetadoConsulte Configuración de SPAN Local y Remoto.

Información Relacionada

- Herramientas y recursos - Cisco Systems
- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems