Solución de problemas del puerto del switch y de la interfaz

Contenido

Introducción

Este documento está diseñado para determinar porqué un puerto o una interfaz tiene problemas. Este documento se aplica a los switches de Catalyst que se ejecutan en el software CatOS en el software del sistema del supervisor o de Cisco IOS® en el supervisor.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

Convenciones

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

Troubleshooting de la Capa Física

Uso del LED para Resolver Problemas

Si tiene acceso físico al switch, puede ahorrar tiempo para mirar los LED de puertos que le dan el estado de link o puede indicar una condición de error (si es rojo o anaranjado). La tabla describe los indicadores del estado LED para los módulos Ethernet o los switches de configuración fija:

Plataforma	URL
Catalyst 6000 Series Switches	LED del Módulo Ethernet
Catalyst 5000 Series Switches	LED del Módulo Ethernet
Catalyst 4000 Series Switches	LED del Módulo Ethernet
Catalyst 3750 Series Switches	LED del Panel Frontal
Catalyst 3550 Series Switches	LED del Panel Frontal
Catalyst 2950/2955 Series Switches	LED del Panel Frontal
Catalyst 2900/3500XL Series Switches	LED del Panel Frontal
Catalyst 1900 Series Switch y 2820 Series Switch	LED del Panel Frontal
Catalyst G-L3 Series Switches	LED del Panel Frontal

Asegúrese de que ambos lados tengan un link. Un solo cable dañado o un puerto apagado pueden provocar el problema en el que un lado tiene una luz de link, pero el otro no.

Una luz de link no garantiza que el cable funcione correctamente. El cable puede haber recibido tensión física, lo que lo hace ser funcional en un nivel marginal. Normalmente, puede identificar esta situación si el puerto tiene muchos errores de paquete, o el puerto se conecta y desconecta constantemente (pierde y recupera el link).

Cómo Verificar el Cable y Ambos Lados de la Conexión

Si no aparece la luz del link para el puerto, puede considerar estas posibilidades:

Posible Causa	Acción Correctiva
No hay cables conectados	Conecte el cable del switch a un dispositivo conocido adecuado.
Puerto Incorrecto	Asegúrese de que los ambos extremos del cable estén conectados en los puertos correctos.

El dispositivo no tiene energía	Asegúrese de que ambos dispositivos tengan energía.
Tipo de cable incorrecto	Verifique la selección del cable. Consulte la Guía del Cable del Switch de Catalyst.
Cable en malas condiciones	Cambie el cable que supuestamente está en malas condiciones por un cable en buenas condiciones. Busque los conectores o pins quebrados o faltantes.
Conexiones débiles	Verifique conexiones débiles. A veces, un cable parece estar asentado en el conector, pero no lo está. Desenchufe el cable y vuelva a insertarlo.
Patch Panels	Elimine las conexiones del patch panel con fallas. Si es posible, desvíe el patch panel para descartarlo.
Convertidores de medios	Elimine los convertidores de medios con fallas: fibra-a-cobre, etc. Si es posible, desvíe el convertidor de medios para descartarlo.
Convertidor de interfaz Gigabit (GBIC) en malas condiciones o incorrecto	Cambie el GBIC que supuestamente está en malas condiciones por un GBIC conocido en buenas condiciones. Verifique el soporte Hw y Sw para este tipo de GBIC. Consulte la sección Troubleshooting de Gigabit Ethernet de este documento.
Puerto, Puerto del Módulo o Interfa	Mover el cable a un puerto conocido en buenas condiciones para resolver problemas con un puerto o un módulo que supuestamente está en malas condiciones. Utilizar el **comando show port** para CatOS o el **comando show interface** para que Cisco IOS busque el estado errdisable, disable o shutdown. **El comando show module**

z en Malas Condiciones o Módulo No Habilitado	puede indicar ser defectuoso, que puede indicar un problema de hardware. Consulte la sección Problemas Comunes de Puertos e Interfaces de este documento para obtener más información.

Cables de Fibra y Cobre Ethernet

Asegúrese de que tiene el cable correcto para el tipo de conexión que desea realizar. El cable de cobre de categoría 3 se puede utilizar para las conexiones del par trenzado sin blindaje de 10 Mbps (UTP), pero nunca se debe utilizar para conexiones UP de 10/100 o 10/100/1000Mbps. Siempre use la categoría 5, la categoría 5e, o la categoría 6 UTP para 10/100 o las conexiones 10/100/1000Mbps.

Advertencia: Los cables de la categoría 5e y de la categoría 6 pueden almacenar niveles elevados de electricidad estática debido a las propiedades dieléctricas de los materiales usados en su construcción. Siempre conecte los cables (especialmente en las nuevas extensiones de cable) a tierra física adecuada y segura antes de conectarlos al módulo.

Para la fibra, asegúrese de tener el cable correcto para las distancias involucradas y el tipo de puertos de fibra que se usen. Las dos opciones son la fibra de modo simple (SMF) o la fibra de modo múltiple (MMF). Asegúrese de que ambos puertos de los dispositivos que están conectados sean SMF, o que ambos sean MMF.

Nota: Para las conexiones de fibra, asegúrese de que el extremo de transmisión de un puerto esté conectado con el extremo de recepción del otro puerto. Las conexiones transmisión a transmisión y recepción a recepción no funcionan.

Distancias de Transmisión Máximas Ethernet y Fast Ethernet

Velocidad del Transmisor y Receptor	Tipo de Cable	Modo Dúplex	Distancia Máxima entre Estaciones
10 Mbps	Categoría 3 UTP	Total y semi	328 pies (100 m)
10 Mbps	MMF	Total y semi	1,2 mi (2 km)
100 Mbps	Categoría 5 UTP Categoría 5e UTP	Total y semi	328 pies (100 m)
100 Mbps	Categoría 6 UTP	Total y semi	328 pies (100 m)
100 Mbps	MMF	Semi	1312 pies (400

			m)
		Total	1,2 mi (2 km)
100 Mbps	S F	Semi	1312 pies (400 m)
		Total	6,2 mi (10 km)

Para obtener más detalles sobre los diferentes tipos de cables/conectores, los requisitos de cableado, los requisitos ópticos (distancia, tipo, cables de patch, etc.), cómo conectar los diferentes cables, y qué cables son utilizados por la mayoría de los switches y módulos Cisco, consulte la Guía sobre Cables para Switches de Catalyst.

Troubleshooting de Gigabit Ethernet

Si conecta el dispositivo A con el dispositivo B sobre un link Gigabit, y el link aparece, realice este procedimiento.

Procedimiento Paso a Paso

1. Verifique que el dispositivo A y B usen el mismo GBIC, longitud de onda corta (SX), longitud de onda larga (LX), trayecto largo (LH), longitud de onda extendida (ZX), o cobre UTP (TX). Ambos dispositivos deben utilizar el mismo tipo de GBIC para establecer el link. Un SX GBIC necesita conectarse con un SX GBIC. Un SX GBIC no se conecta con un LX GBIC. Consulte Nota de Instalación del Cable Patch Acondicionador de Modo para obtener más información.
2. Verifique la distancia y el cable usados por el GBIC según lo definido en esta tabla.**Especificaciones del Cableado de los Puertos 1000BASE-T y 1000BASE-X**Los números otorgados para el cable de fibra óptica con varios modos se efieren al diámetro del núcleo. Para el cable de fibra óptica de modo simple, 8.3 micrones refieren al diámetro del núcleo. Los valores de 9 micrones y 10 micrones corresponden al diámetro de campo de modo (MFD), que es el diámetro de la parte de la fibra por donde pasa la luz. Esta área consiste en el núcleo de la fibra más una pequeña parte de revestimiento circundante. El MFD es una función del diámetro del núcleo, la longitud de onda del láser, y la diferencia del índice refractivo entre el núcleo y el revestimiento.Las distancias están basadas en la pérdida de fibra. Los diversos empalmes y el cable de fibra óptica subestándar reducen las distancias del cableado.Use con MMF solamente.Cuando utiliza un LX/LH GBIC con 62,5 micrones de diámetro MMF, debe instalar un cable de patch acondicionador de modo (CAB-GELX-625 o equivalente) entre el GBIC y el cable MMF en los extremos de transmisión y recepción del link. El cable de patch acondicionador de modo se requiere para las distancias inferiores a 328 pies (100 m) o superiores a 984 pies (300 m). El cable de patch acondicionador de modo evita invalidar el receptor para los tramos cortos de MMF y reduce la demora del modo diferencial para los tramos largos de MMF. Consulte Nota de Instalación del Cable Patch Acondicionador de Modo para obtener más información.Use con SF solamente.Cable de fibra óptica de modo simple y dispersión desplazada.La distancia del link mínima para ZX GBIC es 6,2 millas (10 km) con un atenuador 8-dB instalado en cada extremo del link. Sin los atenuadores, la distancia del link mínima es 24,9 millas (40 km).
3. Si cualquier dispositivo tiene puertos Gigabit múltiples, conecte los puertos entre sí. Lo anterior prueba cada dispositivo y verifica que la interfaz Gigabit funciona correctamente. Por ejemplo, tiene un switch con dos puertos Gigabit. Conecte el puerto Gigabit uno al puerto Gigabit dos. ¿El link aparece? Si es así, el puerto está en buenas condiciones. STP bloquea

el puerto y evita cualquier loop (el puerto uno de recepción (RX) se dirige al puerto dos de transmisión (TX), y el TX del puerto uno se dirige al RX del puerto dos).
4. Si la conexión simple o el Paso 3 falla con los conectores SC, coloque el puerto con loop nuevamente como estaba (el RX del puerto uno se dirige al TX del puerto uno). ¿El puerto aparece? Si no, comuníquese con el TAC, ya que puede ser un puerto defectuoso.
5. Si los pasos 3 y 4 son exitosos, pero no puede establecerse una conexión entre el dispositivo A y B, coloque los puertos con loop con el cable que une los dos dispositivos. Verificar que no haya un cable defectuoso.
6. Verifique que cada dispositivo soporte la especificación 802.3z para la negociación automática Gigabit. El Gigabit Ethernet tiene un procedimiento de negociación automática que es más extenso que el que se usa para 10/100 Ethernet (espec. de la negociación automática Gigabit: IEEE Std 802.3z-1998). Cuando habilita la negociación de link, el sistema negocia automáticamente el control de flujo, el modo dúplex, y la información de falla remota. Debe habilitar o deshabilitar la negociación de link en ambos extremos del link. Ambos extremos del link se deben configurar en el mismo valor o el link no puede conectarse. Se observaron problemas cuando al conectar los dispositivos fabricados antes de que el estándar IEEE 802.3Z fuera ratificado. Si ningún dispositivo soporta la negociación automática Gigabit, se inhabilita la negociación automática Gigabit, y se fuerza la aparición del link. It takes 300msec for the card firmware to notify the software that a 10/100/1000BASE-TX link/port is down. El temporizador del debounce (eliminación de rebote) predeterminado de 300 mseg. viene del temporizador de consultas del firmware a las tarjetas de líneas, que se produce cada 300 milisegundos. Si este link se ejecuta con en el modo 1G (1000BASE-TX), la sincronización del gigabit, que se produce cada 10 mseg., debe poder detectar el link inactivo más rápidamente. Hay una diferencia en el tiempo de detección de la falla de link cuando ejecuta GigabitEthenet en el cobre en comparación con el GigabitEthernet sobre la fibra. Esta diferencia en el tiempo de detección está basada en los estándares IEEE.**Advertencia:** La inhabilitación de la negociación automática oculta los problemas de descartes del link o la capa física. La inhabilitación de la negociación automática se requiere solamente si se usan dispositivos extremos tales como Gigabit NIC anteriores que no pueden soportar el IEEE 802.3Z. No inhabilite la negociación automática entre los switches a menos que se lo requieran absolutamente, ya que los problemas de la capa física pueden no detectarse, lo que resulta en loops de STP. La alternativa es comunicarse con el proveedor y solicitarle una actualización de software o hardware para obtener el soporte de negociación automática para IEEE 802.3z Gigabit.

Para solucionar el mensaje de error: %SYS-4-PORT_GBICBADEEPROM: / %SYS-4-PORT_GBICNOTSUPP, consulte Mensajes de Error Comunes de CatOS en Catalyst 6000/6500 Series Switches.

Para conocer los requisitos del sistema GigabitEthernet y los conversores de interfaz de Gigabite (GBIC), los multiplexores por división de longitud de onda aproximada (CWDM), y los pequeños requisitos del sistema de pequeño factor de forma extraíble, consulte lo siguiente:

- Requisitos del Sistema para Implementar Gigabit Ethernet en Catalyst Switches
- Matriz de Compatibilidad del Switch del Conversor de Interfaz Catalyst Gigabit GigaStack
- Matriz de Compatibilidad de los Módulos de Transmisor y Receptor Gigabit Ethernet de Cisco
- Matriz de Compatibilidad de los Módulos de Transmisor y Receptor Cisco Ethernet de 10 gigabits
- Documentación GBIC, SFP, y CWDM

Para la configuración general y la información de troubleshooting, consulte Configuración y Troubleshooting de la a negociación automática del dúplex completo y del semidúplex de 10/100/1000 MB Ethernet.

Conectado frente a No Conectado

La mayoría de switches Cisco tienen de forma predeterminada un puerto en estado “notconnect”. Esto significa que en ese momento no está conectado pero está dispuesto a conectarse si dispone de una buena conexión con otro dispositivo operativo. Si conecta un cable en buen estado con dos puertos del switch en el estado "notconnect", la luz de link debe ser verde para ambos puertos, y el estado del puerto debe indicar "connected". Esto significa que el puerto está activo en lo que respecta a la capa 1 (L1)

Para CatOS, puede utilizar el comando show port para verificar si el puerto tiene el estado "connected" o "notconnect", o si es otro estado que hace fallar la conectividad, como **disabled** o **errdisable**.

```
Switch> (enable) sh port status 3/1 Port Name Status Vlan Duplex Speed Type ----- --------------
------ ---------- ---------- ------ ----- ------------ 3/1 disabled 1 auto auto 10/100BaseTX !--
- The show port status {mod/port} command show the port is disabled. !--- Use the set port
enable {mod/port}command to try and re-enable it.
```

Para Cisco IOS, puede utilizar el comando show interfaces para verificar si la interfaz muestra el estado "up" o "line protocol up (connected)". El primer “up” se refiere al estado de la capa física de la interfaz. El mensaje "line protocol up" muestra el estado de capa de link de datos de la interfaz e indica que la interfaz puede enviar y recibir keepalives.

```
Router#show interfaces fastEthernet 6/1 FastEthernet6/1 is down, line protocol is down
(notconnect) !--- The interface is down and line protocol is down. !--- Reasons: In this case,
!--- 1) A cable is not properly connected or not connected at all to this port. !--- 2) The
connected cable is faulty. !--- 3) Other end of the cable is not connected to an active port or
device. !--- Note: For gigabit connections, GBICs need to be matched on each !--- side of the
connection. !--- There are different types of GBICs, depending on the cable and !--- distances
involved: short wavelength (SX), !--- long-wavelength/long-haul (LX/LH) and extended distance
(ZX). !--- An SX GBIC needs to connect with an SX GBIC; !--- an SX GBIC does not link with an LX
GBIC. Also, some gigabit !--- connections require conditioning cables, !--- depending on the
lengths involved. Router#show interfaces fastEthernet 6/1 FastEthernet6/1 is up, line protocol
is down (notconnect) !--- The interface is up (or not in a shutdown state), but line protocol
down. !--- Reason: In this case, the device on the other side of the wire is a !--- CatOS switch
with its port disabled. Router#sh interfaces fas 6/1 status Port Name Status Vlan Duplex Speed
Type Fa6/1 notconnect 1 auto auto 10/100BaseTX !--- The show interfaces card-type [slot/port]
status command is the equivalent !--- of show port status for CatOS.
```

Si **show port** muestra connected o **show interfaces** muestra up/ line protocol up (connected) pero aumentan los errores emitidos por este comando, consulte las secciones Información de Salida Específica de los Contadores de Puertos e Interfaces para CatOS o Cisco IOS o Problemas Comunes de Puertos e Interfaces de este documento para obtener asesoramiento sobre troubleshooting.

Comandos Más Comunes para Resolver Problemas con Puertos e Interfaces de CatOS and Cisco IOS

Esta tabla muestra los comandos mas comunes usados para resolver problemas con puertos o interfaces en los switches que se ejecutan con el software CatOS en el supervisor o el software del sistema IOS de Cisco en el software.

Nota: Elija un comando en la columna de la izquierda para dirigirse a la documentación para ese comando. La columna derecha da una breve descripción de lo que hace el comando y menciona cualquier excepción a su uso por plataforma.

Estos comandos son soportados por la herramienta Output Interpreter para CatOS y se pueden utilizar para resolver problemas con el puerto del switch: **show version**, **show module**, **show port**, **show counters** , o **show mac** .

Si tiene el resultado de los comandos admitidos de su dispositivo de Cisco, puede utilizarlo para visualizar los problemas potenciales y sus soluciones. Para utilizar el Output Interpreter, debe ser usuario registrado, iniciar sesión, y habilitar Javascript.

Comandos CatOS	Comandos de Cisco IOS	Descripción
show version	show version	Para los switches que ejecutan CatOS, este comando muestra información de versión de software y hardware por módulo y los tamaños de la memoria del sistema. For switches that run Cisco IOS, this command displays output similar to a Cisco router, like software image name and version information and system memory sizes. Útil para buscar incompatibilidades de software y hardware (con Notas de Versión o Software Advisor) y los bugs (con los Herramientas para Bugs de Software). Para obtener más información sobre el **comando show version**, consulte la sección de este problema Problemas con el Software
show module	show module	Para Catalyst 6000, 5000, 4000 y otros switches modulares que ejecutan CatOS o Cisco IOS, este comando muestra las tarjetas presentes en el switch, la versión de software que ejecutan, y en qué estado se encuentran los módulos: ok, faulty, etc. Útil para diagnosticar problemas de hardware en módulos o puertos. Para obtener más información sobre cómo solucionar problemas de hardware con el **comando show module**, consulte las secciones Estado disabled o shutdown de los puertos y las interfaces Problemas de Hardware de este documento.
show confi	show that run-	Para CatOS, este comando visualiza la configuración no predeterminada del

g	config	switch (todos los cambios realizados a la configuración predeterminada). Todos los cambios a los config. en CatOS se guardan automáticamente. Para Cisco IOS, este comando visualiza el archivo de la configuración actual del switch. Los cambios se guardan a la config. en Cisco IOS con el **comando write memory**. Útil en determinar si el error de configuración del módulo o el puerto o la interfaz puede causar un problema.
show port	show interfaces	Para CatOS, el **comando show port** visualiza si el puerto está conectado, qué VLAN está activa, en qué velocidad/duplex se ejecuta, información sobre el canal, errores, etc. Para Cisco IOS, el **comando show interfaces** visualiza al estado operativo y administrativo de un puerto de switching, un paquete de entrada y de salida, fallas buffer, errores, de un etc. El resultado de estos dos comandos se analiza más detalladamente en la sección Información sobre la Salida Específica de los Contadores de Puertos e Interfaces de este documento.
clear counters	clear counters	Para CatOS y Cisco IOS, use el **comando clear counters** para restablecer los contadores de tráfico y de errores para ver si el problema sólo es temporal o si los contadores siguen aumentando. **Nota:** Los Catalyst 6500/6000 Series Switches no elimina los contadores de bit de una interfaz con el **comando clear counters**. La única manera de eliminar los contadores de bit en estos switches es a través de una recarga.
show port counters	show interfaces counters	Para CatOS, el **comando show port <mod/port>** visualiza los contadores de error de puertos como el FCS, las alineaciones, las colisiones, el etc. Para Cisco IOS en los switches series Catalyst 6000, 4000, 3550, 2950 y 3750, el comando equivalente es **show interfaces** *card-type x/y* **counters errors**. El resultado de estos dos comandos se analiza más detalladamente en la sección Información sobre la Salida Específica de los Contadores de

		Puertos e Interfaces de este documento.
show counters	show counters interface show controllers ethernet-controller	Para CatOS, el **comando show counters** visualiza los contadores de hardware de 64 bits y de 32 bits para un módulo/puerto o interfaz determinados. Los contadores varían al según el tipo de módulo y la plataforma. Para Cisco IOS, el **comando show counters interface** se introdujo en la versión de software 12.1(13)E solo para Catalyst 6000 series solamente y es el equivalente del **comando show counters** para CatOS que muestra contadores de error de 32 bits y 64 bits. Para Cisco IOS en los switches series 2900/3500XL, 2950/2955, 3550, 2970 y 3750, el **comando show controllers ethernet-controller** es similar al **comando show counters** en las plataformas de CatOS. Visualiza las tramas descartadas, las tramas diferidas, los errores de alineación, las colisiones, etc.
show mac	show interfaces counters	Para CatOS, el **comando show mac** visualiza los contadores de MAC para el tráfico que pasa por cada puerto, por ejemplo, las tramas recibidas, las tramas transmitidas, out-lost, in-lost, etc. (este comando no enumera las direcciones MAC detectadas en un puerto por el software bridging. Use el comando show cam dynamic para obtener esta información). Para Cisco IOS, el comando **show interfaces card-type x/y counters** es similar a **show mac** para las plataformas CatOS. El resultado de estos dos comandos se analiza más detalladamente en la sección Información sobre la Salida Específica de los Contadores de Puertos e Interfaces de este documento.
show test	show diagnostic show post	Para CatOS, el **comando show test** visualiza cualquier error de hardware encontrado en el inicio. Para Cisco IOS, el comando equivalente es **show diagnostic** que se introdujo en 12.1(11b)E para Catalyst 6000 series y **show diagnostics**(con una **s**) que se introdujo para las Catalyst 4000 Series.

		Ambos comandos muestran resultados de la autoevaluación en el encendido (POST). Para Cisco IOS en los switches series 2900/3500XL, 2950/2955, 3550, 2970 y 3750, el comando equivalente es **show post** que visualiza los resultados del POST del switch. Para obtener más información sobre cómo solucionar los errores relacionados en los switches Catalyst, ver la sección de los Problemas de Hardware de este documento.

Información sobre la Salida Específica de los Contadores de Puertos e Interfaces en CatOS y Cisco IOS

La mayoría de los switches tienen cierta manera de seguir los paquetes y los errores que se producen en un puerto o interfaz. Los comandos comunes usados para encontrar este tipo de información se describen en la sección Comandos más Comunes para la Resolución de Problemas de Puertos e Interfaces de este documento.

Nota: Puede haber diferencias en la implementación de los contadores en las diversas plataformas y versiones. Aunque los valores de los contadores sean en gran medida son exactos, no son muy precisos en cuanto al diseño. Para conocer las estadísticas exactas del tráfico, se sugiere que use un sniffer para monitorear las interfaces de ingreso y egreso necesarias.

Los errores excesivos para ciertos contadores en general indican un problema. Cuando opera con la configuración semidúplex, algunos errores del link de datos que se incrementan en la Secuencia de Verificación de Trama (FCS), la alineación, los fragmentos minúsculos, y los contadores de colisiones son normales. Generalmente, el índice del uno por ciento de errores del tráfico total es aceptable para las conexiones semidúplex. Si el índice de error a los paquetes de entrada es mayor del dos o tres por ciento, puede observarse una degradación del rendimiento.

En los entornos semidúplexes, es posible para que el switch y el dispositivo conectado detecten el cable y lo transmitan en exactamente el mismo tiempo y resultado en una colisión. Las colisiones pueden provocar fragmentos minúsculos, FCS, y errores de alineación debidos a la trama que no está totalmente copiada en el cable, lo que resulta en tramas fragmentadas.

Cuando opera en un dúplex completo, los errores en el FCS, las Verificaciones Cíclicas de Redundancia (CRC), la alineación, y los contadores de fragmentos minúsculos deben ser mínimos. Si el link opera en el dúplex completo, el contador de colisiones no está activo. Si se incrementa el FCS, el CRC, la alineación, o los contadores de fragmentos minúsculos, verifique si hay discordancia dúplex. La discordancia dúplex es una situación donde el switch opera en el dúplex completo y el dispositivo conectado opera en el semidúplex, o viceversa. Los resultados de una discordancia dúplex son un rendimiento extremadamente lento, conectividad intermitente, y pérdida de conexión. Otras posibles causas de errores del link de datos en el dúplex completo son cables en malas condiciones, puertos de switch defectuosos, o problemas con el software/hardware NIC. Consulte la sección Problemas Comunes de Puertos e Interfaces de este documento para obtener más información.

Show Port para CatOS y Show Interfaces para Cisco IOS

El comando **show port** {mod/port} se usa cuando se ejecuta CatOS en el supervisor. Una alternativa a este comando es el **show port counters** {/port Mod} que visualice solamente los contadores de errores en los puertos. Consulte la Tabla 1 para obtener explicaciones del resultado del contador de errores.

```
Switch> (enable) sh port counters 3/1

  Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
 ----- ---------- ---------- ---------- ---------- ---------
  3/1           0          0          0          0         0

  Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
 ----- ---------- ---------- ---------- ---------- --------- --------- ---------
  3/1           0          0          0          0         0         0         0
```

El comando **show interfaces** *card-type {slot/port}* es el comando equivalente para Cisco IOS en el supervisor. Una alternativa a este comando (para switches Catalyst series 6000, 4000, 3550, 2970 2950/2955, y 3750) es el comando **show interfaces** *card-type {slot/port}* **counters errors** que solamente visualiza los contadores de errores de la interfaz.

Nota: Para 2900/3500XL Series switches, use el comando **show interfaces** *card-type {slot/port}* con el **comando show controllers Ethernet-controller**.

```
Router#sh interfaces fastEthernet 6/1 FastEthernet6/1 is up, line protocol is up (connected)
Hardware is C6k 100Mb 802.3, address is 0009.11f3.8848 (bia 0009.11f3.8848) MTU 1500 bytes, BW
100000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA,
loopback not set Full-duplex, 100Mb/s input flow-control is off, output flow-control is off ARP
type: ARPA, ARP Timeout 04:00:00 Last input 00:00:14, output 00:00:36, output hang never Last
clearing of "show interface" counters never Input queue: 0/2000/0/0 (size/max/drops/flushes);
Total output drops: 0 Queueing strategy: fifo Output queue :0/40 (size/max) 5 minute input rate
0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec
```

El resultado del **comando show interfaces** se explica hasta este punto (en orden):

- up, line protocol is up (connected): el primer first "up" hace referencia al estado de conectado de la capa física de la interfaz. El mensaje "line protocol up" muestra el estado de capa de link de datos de la interfaz e indica que la interfaz puede enviar y recibir keepalives.
- MTU - La Unidad máxima de transmisión (MTU) (MTU) es 1500 bytes para Ethernet por abandono (para la porción de datos máxima del bastidor).
- Full-duplex, 100Mb/s: son las configuraciones de velocidad y dúplex actuales en la interfaz. Esto no indica si se ha utilizado autoneg para lograrlo. Use el **comando show interfaces fas 6/1 status** para ver esto:`Router#sh interfaces fas 6/1 status Port Name Status Vlan Duplex Speed Type Fa6/1 connected 1 a-full a-100 10/100BaseTX !--- Autonegotiation was used to achieve full-duplex and 100Mbps.`
- Last input, output: el número de horas, minutos, y segundos desde que el paquete más reciente fue recibido o transmitido correctamente por la interfaz. Esto sirve para saber cuándo ha fallado una interfaz inactiva.
- Last clearing of "show interface" counters - La última vez que se ejecutó el **comando clear counters** desde la última vez que se reinició el switch. El comando **clear counters** se usa para restablecer las estadísticas de la interfaz.**Nota:** Las variables que pueden afectar el ruteo (por ejemplo, carga y confiabilidad) no se eliminan cuando se eliminan los contadores.
- Input queue: el número de paquetes en la cola de entrada. **Size/max/drops**: la cantidad actual de tramas en la cola//el máximo número de tramas que la cola puede tener antes de comenzar a descartar tramas/el número actual de tramas descartadas debido a que se excedió el tamaño máximo de la cola. **La purga** se utiliza para contar descartes del Descarte selectivo de paquetes (SPD) en Catalyst 6000 Series que ejecuta Cisco IOS. (El contador de

purga se puede utilizar pero nunca incrementa en las Catalyst 4000 Series que ejecutan Cisco IOS). El SPD es un mecanismo que descarta rápidamente los paquetes de prioridad bajas cuando el CPU se sobrecarga para guardar una cierta capacidad de procesamiento para los paquetes con prioridad alta. El contador de purga en el resultado de comando show interface se incrementa como parte del descarte de paquetes selectivos (SPD), que implementa una política para descartar paquetes selectivos en la cola del proceso del IP del router. Por lo tanto, se aplica para procesar solamente el tráfico conmutado.El propósito del SPD es asegurarse de que los paquetes de control importantes, como actualizaciones de ruteo y keepalives, no se descarten cuando la cola de entrada del IP esté llena. Cuando el tamaño de la cola de entrada del IP se encuentre entre los umbrales mínimos y máximos, se descartan los paquetes normales del IP en función de cierta probabilidad de descarte. Este descarte al azar se denomina purga SPD.

- Total output drops - La cantidad de paquetes que se descartan porque la capacidad de la cola de salida está completa. Una causa frecuente para esto podría ser que el tráfico de un link de ancho de banda alto sea conmutado hacia un link de ancho de banda inferior o que el tráfico de links entrantes múltiples sea conmutado a un solo link de salida. Por ejemplo, si una gran cantidad de tráfico saturado entra en una interfaz gigabit y se conmuta hacia una interfaz de 100Mbps, esto podría ocasionar que aumenten las pérdidas en la salida en la interfaz de 100Mbps. Esto ocurre porque la cola de salida en esa interfaz está saturada por el exceso de tráfico debido a la discordancia de velocidad entre los anchos de banda entrante y saliente.
- Output queue: el número de paquetes en la cola de salida. Tamaño/máx. significa la cantidad actual de tramas en la cola/el número máximo de tramas que la cola puede retener antes de estar completa y deber eliminar tramas
- Velocidad de entrada y salida en 5 minutos - Velocidad de entrada y salida promedio vista por la interfaz en los últimos cinco minutos. Para obtener una lectura más precisa especificando un período más corto (por ejemplo, para detectar mejor los bursts), ejecute el comando **load-interval <seconds>** .

El resto del **comando show interfaces** visualiza la salida del contador de errores que es similar o equivalente a la salida del contador de errores de CatOS. Ver la Tabla 1 para obtener las explicaciones de la salida del contador de errores.

```
!--- ...show interfaces command output continues. 1117058 packets input, 78283238 bytes, 0 no
buffer Received 1117035 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0
frame, 0 overrun, 0 ignored 0 watchdog, 0 multicast, 0 pause input 0 input packets with dribble
condition detected 285811 packets output, 27449284 bytes, 0 underruns 0 output errors, 0
collisions, 2 interface resets 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no
carrier 0 output buffer failures, 0 output buffers swapped out
```

Nota: Hay una diferencia entre el contador del comando show interface hecho salir para una interfaz física y una interfaz VLAN. Los contadores de paquetes de entrada se incrementan en la salida del comando **show interface** para una interfaz VLAN cuando ese paquete es procesado por el CPU en la Capa 3 (L3). El tráfico que es conmutado en la Capa 2 (L2) nunca lo hace en el CPU y no se cuenta en los **contadores show interface** para la interfaz VLAN. Sería contado en la **salida show interface** para la interfaz física apropiada.

El comando **show interfaces** *card-type {slot/port}* **counters errors** es el comando Cisco IOS equivalente que se sua para mostrar lso contadores de puerto para CatOS. Ver la Tabla 1 para obtener las explicaciones de la salida del contador de errores.

```
Router#sh interfaces fastEthernet 6/1 counters errors Port Align-Err FCS-Err Xmit-Err Rcv-Err
UnderSize OutDiscards Fa6/1 0 0 0 0 0 0 Port Single-Col Multi-Col Late-Col Excess-Col Carri-Sen
```

```
Runts Giants Fa6/1 0 0 0 0 0 0 0
```

Tabla 1:

Salida del contador de errores de CatOS para **show port** o **show port counters** para Catalyst Series 6000, 5000 y 4000. La salida de contador de errores Cisco IOS para **show interfaces** o **show interfaces** *card-type x/y* **counters errors** para Catalyst Series 6000 y 4000.

Contadores (en orden alfabético)	**Descripción y Causas Comunes del Incremento de los Contadores de Error**
Align-Err	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces counters errors**. Los errores de alineación son un conteo del número de tramas recibidas que no terminan con un número par de octetos y que tienen una mala Verificación por Redundancia Cíclica (CRC). **Causas Comunes:** Éstos generalmente son el resultado de una discordancia dúplex o un problema físico (como cableado, puerto defectuoso, o un NIC defectuoso). Cuando el cable primero está conectado con el puerto, pueden presentarse algunos de estos errores. También, si hay un hub conectado con el puerto, las colisiones entre los otros dispositivos en el hub pueden causar estos errores. **Excepciones en la Plataforma:** Los errores de alineación no se cuentan en Catalyst 4000 Series Supervisor I (WS-X4012) o Supervisor II (WS-X4013).
charlas	**Descripción:** Cisco IOS **sh interfaces** counter. Contador de CatOS que indica que el temporizador de transmisión de tramas jabber ha caducado. Un jabber es una trama de más de 1518 octetos (sin contar los bits de entramado, pero sí los octetos FCS) que no termina con un número par de octetos (error de alineación) o tiene un error de FCS inadecuado.
Carri-Sen	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces counters errors**. El contador Carri-Senador (detección de portadora) incrementa cada vez que un controlador Ethernet desea enviar los datos en una conexión semidúplex. El controlador detecta el cable y verifica si no está ocupado antes de realizar la transmisión. **Causas Comunes:** Esto es normal en un segmento Ethernet semidúplex.
colisiones	**Descripciones:** Cisco IOS **sh interfaces** counter. La cantidad de veces que una colisión se presenta antes de que la interfaz transmita una trama a los medios con éxito. **Causas**

	Comunes: Las colisiones son normales en interfaces configuradas como medio dúplex, pero no deberían existir en interfaces dúplex plenas. Si las colisiones aumentan significativamente, hay un enlace que se usa demasiado o posiblemente una discordancia dúplex con el dispositivo adjunto.
CRC	**Descripción:** Cisco IOS **sh interfaces** counter. Esto aumenta cuando la CRC generada por la estación LAN de origen o dispositivo de extremo lejano no coincide con la suma de comprobación calculada en base a los datos recibidos. **Causas Comunes:** Generalmente, esto indica problemas de ruido o de transmisión en la interfaz LAN o en la LAN en sí. Un elevado número de CRC se produce por lo general como resultado de las colisiones pero también pueden indicar un problema físico (como cableado, mala interfaz o tarjeta de interfaz de red [NIC]) o un desajuste bidireccional.
diferido	**Descripción:** Cisco IOS **sh interfaces** counter. La cantidad de tramas transmitidas con éxito luego de esperar debido a que los medios se hallaban ocupados. **Causas Comunes:** Esto suele ocurrir en entornos semidúplex donde la portadora ya está en uso al intentar transmitir una trama.
pause input	**Descripción:** Contador Cisco IOS **show interfaces** . Un incremento del contador pause input significa que el dispositivo conectado está solicitando que se detenga el tráfico cuando su búfer de recepción está casi lleno. **Causas Comunes:** Este contador aumenta a título informativo, ya que el switch acepta la trama. La petición de detener los paquetes se anula cuando el dispositivo conectado está en condiciones de recibir tráfico.
input packets with dribble condition	**Descripción:** Cisco IOS **sh interfaces** counter. Un error de bit de fichero indica que una trama es demasiado larga. **Causas Comunes:** Este contador de errores de trama se incrementa para fines informativos, ya que el switch acepta la trama.
Excess-Col	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces counters errors**. Recuento de tramas cuya transmisión en una interfaz determinada falla debido a un exceso de colisiones. Se produce una colisión excesiva cuando un paquete colisiona 16 veces seguidas. De esta manera, el paquete deja de transmitirse. **Causas Comunes:** Las colisiones excesivas

	suelen indicar que la carga del segmento debe repartirse entre varios segmentos, pero también pueden indicar una discordancia de dúplex con el dispositivo conectado. Las colisiones no se deben considerar en las interfaces configuradas como dúplex completo.
FCS-Err	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces counters errors**. La cantidad de tramas de tamaño válido con errores en la Secuencia de Verificación de Tramas (FCS) pero sin errores de entramado. **Causas Comunes:** Esto suele ser un problema físico (cableado, puerto erróneo o una mala tarjeta de interfaz de red [NIC]), pero también pueden indicar una discordancia dúplex.
trama	**Descripción:** Cisco IOS **sh interfaces** counter. El número de paquetes que se recibió de forma incorrecta con un error CRC y un número no entero de octetos (error de alineación). **Causas Comunes:** Éste suele ser el resultado de colisiones o de un problema físico (como cableado, puerto incorrecto o NIC), aunque también puede indicar una discordancia dúplex.
Gigantes	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces** y sh **interfaces counters errors**. Las tramas recibidas que excedieron el tamaño máximo de trama IEEE 802.3 (1518 bytes para Ethernet no jumbo) y cuentan con una Secuencia de Verificación de Tramas (FCS) mala. **Causas Comunes:** En muchos casos, este es el resultado de un NIC defectuoso. Intente encontrar el dispositivo con problemas y retírelo de la red. **Excepciones en la Plataforma: Catalyst Cat4000 Series que ejecuta Cisco IOS** Antes de la versión de software 12.1(19)EW, el contador de gigantes aumentaba para una trama > 1518 bytes. Después de 12.1(19)EW, un gigante en **show interfaces** aumenta solamente cuando se recibe una trama >1518 bytes con una FCS mala.
ignorado	**Descripción:** Cisco IOS **sh interfaces** counter. La cantidad de paquetes recibidos e ignorados por la interfaz porque el hardware de la interfaz no fue suficiente en los búferes internos. **Causas Comunes:** Las tormentas de difusión y las ráfagas de ruido pueden hacer que aumente el recuento ignorado.
Errores de entrada	**Descripción:** Cisco IOS **sh interfaces** counter. **Causas Comunes:** Estos incluyen los recuentos ignorados, de fragmentos de tramas minúsculos y gigantes, de falta de buffer, de CRC y de exceso. Otros errores relacionados con la

	entrada hacen aumentar el contador de errores de entrada y algunos datagramas pueden tener más de un error. Por lo tanto, esta suma no puede equilibrar con la suma de conteos enumerados de error de entrada. También consulte la sección Errores de Entrada en una Iterfaz Capa 3 Conectada a un Switchport Capa 2.
Tarde-cuesta	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces** y **sh interfaces counters errors.** La cantidad de veces que se detecta tarde una colisión en una interfaz específica en el proceso de transmisión. Para un puerto de 10Mbit/s, este retraso es mayor a 512 bits times en la transmisión de un paquete. 512 veces bits corresponde a 51.2 microsegundos en un sistema de 10 Mbit/s. **Causas Comunes:** Este error puede indicar una discordancia dúplex, entre otras cosas. En el caso de un escenario de discordancia dúplex, la colisión tardía se observa en el lado del semi dúplex. Debido a que el semi dúplex está transmitiendo, el lado del dúplex completo no espera su turno y transmite de manera simultánea causando un choque tardío. Las colisiones tardías también pueden indicar que un cable Ethernet o un segmento es demasiado largo. Las colisiones no se deben considerar en las interfaces configuradas como dúplex completo.
lost carrier	**Descripción:** Cisco IOS **sh interfaces** counter. El número de veces que la portadora se ha perdido durante la transmisión. **Causas Comunes:** Compruebe que no haya ningún cable defectuoso. Compruebe la conexión física en ambos lados.
Multi-cuesta	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces counters errors**. La cantidad de veces que se produjeron colisiones múltiples antes de que la interfaz transmitiera una trama a los medios de manera exitosa. **Causas Comunes:** Las colisiones son normales en interfaces configuradas como medio dúplex, pero no deberían existir en interfaces dúplex plenas. Si las colisiones aumentan significativamente, hay un enlace que se usa demasiado o posiblemente una discordancia dúplex con el dispositivo adjunto.
no buffer	**Descripción:** Cisco IOS **sh interfaces** counter. El número de paquetes recibidos descartados porque no hay espacio de buffer. **Causas Comunes:** Comparar con contador ignorado. Las tormentas de difusión pueden ser

	responsables de esta situación.
ningún portador	**Descripción:** Cisco IOS **sh interfaces** counter. La cantidad de veces que la portadora no estuvo presente durante la transmisión. **Causas Comunes:** Compruebe que no haya ningún cable defectuoso. Compruebe la conexión física en ambos lados.
Hacia fuera-descarte	**Descripción:** Cantidad de paquetes salientes elegidos para ser descartados aunque no se hayan detectado errores de paquetes. **Causas Comunes:** Una razón posible para descartar tal paquete puede ser liberar el espacio del buffer.
output buffer failures output buffers swapped out	**Descripción:** Cisco IOS **sh interfaces** counter. La cantidad de memoria intermedia con errores e intercambiada. **Causas Comunes:** Los puertos almacenan los paquetes en el buffer Tx cuando el tráfico desviado hacia el puerto es intenso y no se puede manejar. Los puertos empiezan a descartar paquetes cuando el búfer Tx está lleno, lo que aumenta los contadores de agotamiento y de errores en el buffer de salida. El aumento de los contadores de errores del buffer de salida podría indicar que los puertos tienen un ajuste inferior de velocidad o dúplex, o que hay demasiado tráfico en el puerto. Como ejemplo, supóngase una situación en que se reenvía un flujo de multicast de 1 gig a 24 puertos de 100 Mbps. Si una interfaz de egreso tiene un exceso de suscriptores, sería normal ver que los errores del búfer de salida aumentan junto con Out-Discards. Para obtener información sobre cómo resolver problemas, consulte la sección Tramas Diferidas (Out-Lost u Out-Discard) de este documento.
errores de salida	**Descripción:** Cisco IOS **sh interfaces** counter. La suma de todos los errores que previnieron la transmisión final de la interfaz de datagramas de la interfaz. **Causa Común:** Este problema se debe al tamaño pequeño de la Cola de Salida.
desbordamiento	**Descripción:** La cantidad de veces que el hardware de recepción no pudo entregar los datos recibidos a un buffer de hardware. **Causa Común:** La velocidad de entrada de tráfico excedió la capacidad del receptor de manejar los datos.
packets input/output	**Descripción:** Cisco IOS **sh interfaces** counter. El total de paquetes sin errores recibidos y transmitidos en la interfaz. El monitoreo de estos contadores para aumentos es útil para determinar si el tráfico está circulando de forma adecuada a través de la interfaz. El contador de

	bytes incluye tanto los datos como la encapsulación MAC de los paquetes libres de errores recibidos y transmitidos por el sistema.
Rcv-Err	**Descripción:** CatOS **show port** o **show port counters** y Cisco IOS sh interfaces counters error (solamente para Catalyst 6000 Series). **Causas Comunes:** Consulte las Excepciones en la Plataforma. **Excepciones en la Plataforma: Catalyst 5000 Series** rcv-err = errores en el buffer de recepción. Por ejemplo, un fragmento minúsculo, un fragmento gigante o un error de no aumentarán el contador rcv-err. El contador rcv-err en un 5K aumenta solamente como resultado de un exceso de tráfico. En **Catalyst 4000 Series** rcv-err = la suma de todos los errores de recepción, lo que significa, contrariamente a Catalyst 5000, que el contador rcv-err aumenta cuando la interfaz recibe un error como un fragmento minúsculo, un fragmento gigante o un error de FCS.
Fragmentos minúsculos	**Descripción:** sh port en CatOS y **sh interfaces** y **sh interfaces counters errors** en Cisco IOS. Las tramas recibidas que son menores al tamaño mínimo de trama de IEEE 802.3 (64 bytes para Ethernet) y tienen una CRC inadecuada. **Causas Comunes:** Esto puede estar causado por una discordancia dúplex y problemas físicos, como un cable, un puerto o una NIC incorrectos en el dispositivo conectado. **Excepciones en la Plataforma: Catalyst 4000 Series que ejecutan Cisco IOS** Antes de la versión de software 12.1(19)EW, un fragmento minúsculo = tamaño inferior al normal. Tamaño inferior al normal = trama < 64 bytes. El contador de fragmentos minúsculos se incrementaba solamente si se recibía una trama inferior a 64 bytes. A partir de la versión 12.1(19)EW, un fragmento minúsculo = un fragmento. Un fragmento es una trama < 64 bytes pero con una CRC errónea. El resultado es que el contador de fragmentos minúsculos ahora se incrementa en **show interfaces**,junto con el contador de fragmentos en**show interfaces counters errors** cuando se recibe una trama < 64 bytes con una CRC mala. **Cisco Catalyst 3750 Series Switches** En las versiones anteriores a Cisco IOS 12.1(19)EA1, cuando se usa dot1q en la interfaz trunk en Catalyst 3750, se pueden ver fragmentos minúsculos en la salida **show interfaces** porque los paquetes dot1q válidos y encapsulados, que son 61 a 64 bytes e incluyen q-tag, son contados por

	Catalyst 3750 como tramas de tamaño inferior, aunque estos paquetes se reenvíen de forma correcta. Además, estos paquetes no se informan en la categoría adecuada (unicast, multicast, o broadcast) en las estadísticas de recepción. Este problema se resuelve en Cisco IOS release 12.1(19)EA1 o 12.2(18)SE o posterior.
Solo-cuesta	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces counters errors**. Número de veces que se ha producido una colisión antes de que la interfaz transmitiera una trama satisfactoriamente al dispositivo. **Causas Comunes:** Las colisiones son normales en interfaces configuradas como medio dúplex, pero no deberían existir en interfaces dúplex plenas. Si las colisiones aumentan significativamente, hay un enlace que se usa demasiado o posiblemente una discordancia dúplex con el dispositivo adjunto.
válvulas reguladoras	**Descripción:** Cisco IOS **show interfaces**. La cantidad de veces que el receptor del puerto ha sido inhabilitado, posiblemente debido a una sobrecarga del buffer o procesador. Si aparece un asterisco (*) después del valor de contador de throttles, significa que la interfaz está throttled en el momento que se ejecuta el comando. **Causas Comunes:** Los paquetes que pueden aumentar la sobrecarga del procesador incluyen los paquetes IP con opciones, TTL vencida, encapsulación no ARPA, fragmentación, tunelling, paquetes ICMP, paquetes con falla de checksum MTU, falla de RPF, errores de longitud y de checksum IP.
underruns	**Descripción:** La cantidad de veces que el transmisor ha operado más rápido de lo que el switch puede aceptar. **Causas Comunes:** Esto puede ocurrir en situaciones de alto rendimiento cuando una interfaz recibe un gran volumen de ráfagas de tráfico de muchas otras interfaces a la vez. Los restablecimientos de la interfaz pueden producirse con desbordamientos.
De tamaño insuficiente	**Descripción:** CatOS sh port and Cisco IOS sh interfaces counters errors . Las tramas recibidas que son más pequeñas que el tamaño mínimo de trama IEEE 802.3 de 64 bytes de longitud (sin contar los bits de tramas, pero con los octetos FCS) que, de otra manera, están bien formadas. **Causas Comunes:** Verifique el dispositivo que envía esas tramas.
Xmit-Err	**Descripción:** CatOS **sh port** y Cisco IOS **sh interfaces counters errors**. Esto indica que el

	buffer de transmisión interno (Tx) está lleno. **Causas Comunes:** Una causa común de Xmit-Err puede ser el tráfico de un enlace de ancho de banda alto siendo conmutado a un enlace de ancho de banda inferior, o el tráfico de múltiples enlaces de entrada siendo conmutado a un único enlace de salida. Por ejemplo, si una gran cantidad de tráfico congestionado ingresa en una interfaz gigabit y se lo conmuta a una interfaz 100Mbps, esto puede hacer que Xmit-Err aumente en la interfaz 100Mbps. Esto ocurre porque el buffer de salida en esa interfaz está saturada por el exceso de tráfico debido a la asimetría de la velocidad entre los anchos de banda entrante y saliente.

Show Mac para CatOS and Show Interfaces Counters para Cisco IO

El comando show mac {mod/port} es útil cuando se ejecuta en CatOS en el supervisor para controlar el tráfico entrante y saliente en el puerto indicado por los contadores de recepción (Rcv) y transmisión (Xmit) del tráfico de unidifusión, multidifusión y difusión. Esta salida proviene de Catalyst 6000 que ejecuta CatOS:

```
Console> (enable) sh mac 3/1

  Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
  -------- -------------------- -------------------- --------------------
   3/1                     177               256272                 3694

  Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
  -------- -------------------- -------------------- --------------------
   3/1                      30               680377                  153

  Port     Rcv-Octet            Xmit-Octet
  -------- -------------------- --------------------
   3/1                22303565             48381168

  MAC      Dely-Exced MTU-Exced In-Discard Out-Discard -------- ---------- ---------- ----------
----------- 3/1 0 0 233043 17 Port Last-Time-Cleared ----- ------------------------- 3/1 Sun
Jun 1 2003, 12:22:47
```

Este comando también tiene los siguientes contadores de error: **Dely-Exced, MTU-Exced, In-Discard** y **Out-Discard**.

- Exceso de retraso - El número de tramas descartadas por este puerto debido a un retraso excesivo de transmisión a través del switch. Este contador no debería aumentar nunca a menos que el puerto esté sujeto a un uso muy intenso.
- MTU Exceed : es un indicador de que uno de los dispositivos en ese puerto o segmento está transmitiendo un tamaño de trama mayor que el permitido (1518 bytes para Ethernet no jumbo).
- In-Discard: el resultado de tramas entrantes válidas que fueron descartadas porque la trama no necesitaba ser conmutada. Esto sería normal si se conectara un hub a un puerto y dos dispositivos en ese hub estuviesen intercambiando datos. El puerto del switch todavía ve los datos pero no tiene que conmutarlos (puesto que la tabla CAM muestra la dirección MAC de ambos dispositivos asociados al mismo puerto), y así se descarta. Este contador también

puede incrementarse en un puerto configurado como trunk si ese trunk se bloquea para algunos VLAN, o en un puerto que sea el único miembro de VLAN.
- Descarte de paquetes salientes - Cantidad de paquetes salientes elegidos para ser descartados aunque no se hayan detectado errores de paquetes. Una razón posible para descartar tal paquete puede ser liberar el espacio del buffer.

Los Catalyst 4000 and 5000 series switches que ejecutan CatOS tienen dos contadores de errores adicionales en el comando **show mac**. Son los contadores In-Lost y Out-Lost.

```
MAC      Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost Out-Lost -------- ---------- ------
---- ---------- ---------- ---------- ---------- 5/1 0 0 0 0 0 0
```

- In Lost: en Catalyst 4000, este contador es la suma de todos los paquetes de errores recibidos en el puerto. El contador In Lost en Catalyst 5000, por otra parte, hace un seguimiento de la suma de todas las fallas de buffer de recepción.
- Out-Lost : en Catalyst 4000 y 5000, estas son tramas de salida que fueron perdidas antes de que fueran enviadas (debido al espacio del buffer escaso). Esto suele ser resultado de un exceso de suscriptores en el puerto.

El comando **show interfaces** card-type {slot/port} **counters** se usa cuando ejecuta Cisco IOS en Supervisor.

Nota: No hay contadores equivalentes a los contadores **show mac error** de CatOS: Dely-Exced, MTU-Exced and In-Discard en este comando. Sin embargo, hay un contador Out-Discard en el comando **show interfaces counters errors** que se explica en la Tabla 1.

```
Router#sh interfaces fas 6/1 counters Port InOctets InUcastPkts InMcastPkts InBcastPkts Fa6/1
47856076 23 673028 149 Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts Fa6/1 22103793 17
255877 3280 Router# !--- Cisco IOS counters used to monitor inbound and outbound unicast,
multicast !--- and broadcast packets on the interface.
```

Show Counters for CatOS y Show Counters Interface para Cisco IOS

El comando **show counters** [mod/port] ofrece estadísticas aún más detalladas para los puertos y las interfaces. Este comando está disponible para CatOS y el comando equivalente **show counters interface** *card-type {slot/port}* se introduce en Cisco IOS software version 12.1(13)E para Catalyst 6000 series solamente. Estos comandos muestran los contadores de errores de 32 bits y 64 bits por puerto o interfaz. Consulte documentación del comando CatOS parashow counters si desea más información.

Nota: Las estadísticas del contador para Catalyst 6000 series switches que ejecutan Cisco IOS se representan en hexidecimal.

```
Console> (enable) sh counters 3/1 64 bit counters 0 rxHCTotalPkts = 260555 1 txHCTotalPkts =
687411 2 rxHCUnicastPkts = 177 3 txHCUnicastPkts = 30 4 rxHCMulticastPkts = 256684 5
txHCMulticastPkts = 687228 6 rxHCBroadcastPkts = 3694 7 txHCBroadcastPkts = 153 8 rxHCOctets =
22386167 9 txHCOctets = 48850817 10 rxTxHCPkts64Octets = 228929 11 rxTxHCPkts65to127Octets =
701493 12 rxTxHCPkts128to255Octets = 285 13 rxTxHCPkts256to511Octets = 17090 14
rxTxHCpkts512to1023Octets = 168 15 rxTxHCpkts1024to1518Octets = 1 16 txHCTrunkFrames = 395217 17
rxHCTrunkFrames = 236459 18 rxHCDropEvents = 0 32 bit counters 0 rxCRCAlignErrors = 0 1
rxUndersizedPkts = 0 2 rxOversizedPkts = 0 3 rxFragmentPkts = 0 4 rxJabbers = 0 5 txCollisions =
0 6 ifInErrors = 0 7 ifOutErrors = 0 8 ifInDiscards = 233043 9 ifInUnknownProtos = 2 10
ifOutDiscards = 17 !--- Output suppressed.
```

Show Controller Ethernet-Controller para Cisco IOS

Para Catalyst 3750, 3550, 2970, 2950/2955, 2940, y 2900/3500XL switches, use el comando command show controller ethernet-controller para mostrar la salida del contador de tráfico y del

contador de errores que es similar a la salida show port, show interface, show mac y show counters para Catalyst 6000, 5000, 4000 series switches.

```
3550-1#sh controller ethernet-controller fastEthernet 0/1 !--- Output from a Catalyst 3550.
Transmit FastEthernet0/1 Receive 0 Bytes 0 Bytes 0 Unicast frames 0 Unicast frames 0 Multicast
frames 0 Multicast frames 0 Broadcast frames 0 Broadcast frames 0 Discarded frames 0 No dest,
unicast 0 Too old frames 0 No dest, multicast 0 Deferred frames 0 No dest, broadcast 0 1
collision frames 0 2 collision frames 0 FCS errors 0 3 collision frames 0 Oversize frames 0 4
collision frames 0 Undersize frames 0 5 collision frames 0 Collision fragments 0 6 collision
frames 0 7 collision frames 0 Minimum size frames 0 8 collision frames 0 65 to 127 byte frames 0
9 collision frames 0 128 to 255 byte frames 0 10 collision frames 0 256 to 511 byte frames 0 11
collision frames 0 512 to 1023 byte frames 0 12 collision frames 0 1024 to 1518 byte frames 0 13
collision frames 0 14 collision frames 0 Flooded frames 0 15 collision frames 0 Overrun frames 0
Excessive collisions 0 VLAN filtered frames 0 Late collisions 0 Source routed frames 0 Good (1
coll) frames 0 Valid oversize frames 0 Good(>1 coll) frames 0 Pause frames 0 Pause frames 0
Symbol error frames 0 VLAN discard frames 0 Invalid frames, too large 0 Excess defer frames 0
Valid frames, too large 0 Too large frames 0 Invalid frames, too small 0 64 byte frames 0 Valid
frames, too small 0 127 byte frames 0 255 byte frames 0 511 byte frames 0 1023 byte frames 0
1518 byte frames 3550-1# !--- See table for additional counter output for 2900/3500XL Series
switches.
```

Contador	Descripción	Posibles Causas
Tramas Transmitidas		
Tramas descartadas	La cantidad total de tramas cuyo intento de transmisión se abandonó debido a una insuficiencia de recursos. Este total incluye tramas de todos los tipos de destinos.	La carga de tráfico en la interfaz es excesiva, por lo que se descartan tramas. Reduzca la carga de tráfico en la interfaz si se observa un aumento del número de paquetes en este campo.
Tramas demasiado antiguas	Número de tramas que tardaron más de dos segundos en pasar a través del switch. Por esta razón, fueron descartados por el switch. Esto solo ocurriría en condiciones extremas de mucha intensidad.	La carga de tráfico para este switch es excesiva y hace que las tramas sean descartadas. Reduzca la carga en el switch si observa un aumento del número de paquetes en este campo. Es posible que sea necesario modificar la topología de la red para reducir la carga de tráfico de este switch.
Tramas diferidas	La cantidad total de tramas cuyo primer intento de transmisión se retrasó debido al tráfico en el dispositivo de red. Este total incluye solo las	La carga de tráfico destinada a este switch es excesiva, por lo que se descartan tramas. Reduzca la carga en

	tramas que se han transmitido posteriormente sin errores ni colisiones.	el switch si observa un aumento del número de paquetes en este campo. Es posible que sea necesario modificar la topología de la red para reducir la carga de tráfico de este switch.
Tramas de colisión	Los contadores de colisiones de tramas indican el número de veces que se ha intentado transmitir un paquete sin éxito, pero con éxito en el siguiente intento. Esto significa que si el contador2 collision frames aumentó, el switch ha intentado enviar el paquete dos veces sin éxito pero lográndolo en el tercer intento.	La carga de tráfico en la interfaz es excesiva, por lo que se descartan tramas. Reducir la carga de tráfico en la interfaz si ve un número creciente de paquetes en estos campos.
Colisiones excesivas	El contador de colisiones excesivas aumenta cuando se han producido 16 colisiones tardías consecutivas. Después de 16 intentos de enviar el paquete, la trama se descartará y aumentará el contador.	El aumento de este contador indica un problema de cableado, una red demasiado cargada o una discordancia de dúplex. Una red demasiado cargada podría ser resultado de un exceso de dispositivos en una Ethernet compartida.
Colisiones tardías	Una colisión tardía se produce cuando dos dispositivos transmiten al mismo tiempo y ningún punto de la conexión detecta una colisión. Esto puede ser debido a que el tiempo necesario para propagar la señal de un extremo de la red a otro es mayor que el tiempo necesario para poner todo el paquete en la red. Los dos dispositivos que causan	Las colisiones tardías son el resultado de un cableado incorrecto o de un número no soportado de hubs en la red. Las NIC defectuosas también pueden provocar colisiones tardías.

	la colisión tardía nunca ven que el otro está enviando hasta después de que éste coloca todo el paquete en la red. Las colisiones tardías no son detectadas por el transmisor hasta después del intervalo correspondiente a los primeros 64 bytes. Esto es debido a que solo se detectan durante las transmisiones de paquetes mayores de 64 bytes.	
Tramas adecuadas (1 colisión)	El número total de tramas que experimentan exactamente una colisión y posteriormente se transmiten satisfactoriamente.	Las colisiones en los entornos semidúplex son normales.
Tramas adecuadas (> 1 colisión)	El número total de tramas que experimentan entre 2 y 15 colisiones, inclusive, y posteriormente se transmiten satisfactoriamente.	Las colisiones en los entornos semidúplex son normales. Las tramas que aumentan el margen superior de este contador corren el riesgo de superar las 15 colisiones y ser contadas como colisiones excesivas.
Tramas descartadas VLAN	El número de tramas descartadas en una interfaz porque el bit CFI está definido.	El bit del Indicador de Formato Canónico (CFI) en el TCI de una trama 802.1q está definido en 0 en el formato de trama canónico de Ethernet. Si el bit CFI está definido en 1, esto indica la presencia de una trama no canónica RIF (Campo de Información de Enrutamiento) o Token Ring que se descarta.
Tramas Recibidas		

No bandwidth frames	*2900/3500XL solamente.* El número de veces que un puerto ha recibido un paquete de la red, pero el switch no tenía los recursos necesarios para recibirlo. Esto sucede solamente en condiciones de tensión, pero puede suceder con ráfagas de tráfico en varios puertos. Por lo tanto, un número pequeño en el campo No bandwidth frames no es motivo de preocupación. (Aún así debería ser mucho menos del uno por ciento de las tramas recibidas).	La carga de tráfico en la interfaz es excesiva, por lo que se descartan tramas. Reduzca la carga de tráfico en la interfaz si se observa un aumento del número de paquetes en este campo.
No buffers frames	*2900/3500XL solamente.* El número de veces que un puerto ha recibido un paquete de la red, pero el switch no tenía los recursos necesarios para recibirlo. Esto sucede solamente en condiciones de tensión, pero puede suceder con ráfagas de tráfico en varios puertos. Por lo tanto, una pequeña cantidad de No buffers frames no es motivo de preocupación. (Aún así debería ser mucho menos del uno por ciento de las tramas recibidas).	La carga de tráfico en la interfaz es excesiva, por lo que se descartan tramas. Reduzca la carga de tráfico en la interfaz si se observa un aumento del número de paquetes en este campo.
No dest, unicast	No destination unicast es el número de paquetes unicast que el puerto no envió a cualquier otro puerto.	Las siguientes son descripciones breves de situaciones en las que los contadores No dest, (unicast, multicast, y broadcast) pueden incrementarse: • Si un puerto es un puerto de acceso, y el puerto está conectado con
No dest, multicast	No destination multicast es la cantidad de paquetes multicast que el puerto no reenvió a cualquier otro puerto.	
No dest, broadc	No destination broadcast es la cantidad de paquetes broadcast que	

ast	el puerto no reenvió a cualquier otro puerto.	un puerto trunk del Inter-Switch Link Protocol (ISL), el contador No dest es muy largo ya que todos los paquetes ISL entrantes no son reenviados. Esta es una configuración inválida. • Si un puerto está bloqueado por el Spanning Tree Protocol (STP), la mayoría de los paquetes no son reenviados, lo que resulta en paquetes No dest. Si un puerto acaba de adquirir un enlace, habrá un período muy breve (menos de un segundo) en el que los paquetes entrantes no son reenviados. • Si el puerto está en un VLAN por sí mismo, y ningún otro puerto en el switch pertenece a ese VLAN, se descartan todos los paquetes de entrada y el contador se incrementa. • El contador

		también aumenta cuando el puerto de recepción del paquete averigua la dirección de destino del paquete. Si un paquete fue recibido en el puerto 0/1, con la dirección MAC de destino X, y el switch ya ha aprendido que la dirección MAC X se encuentra en el puerto 0/1, aumenta el contador y descarta el paquete. Esto puede suceder en las siguientes situaciones: Si un hub está conectado con el puerto 0/1, y una estación de trabajo conectada con el eje transmite los paquetes a otra estación de trabajo conectada con el hub, el puerto 0/1 no reenvía este paquete a cualquier lugar porque la MAC de destino reside en el mismo puerto.Esto también sucede

		si un switch está conectado con el puerto 0/1, y comienza a inundar todos sus puertos con paquetes para aprender las direcciones MAC. • Si se ha configurado a una dirección estática en otro puerto en la misma VLAN, y no se configuró ninguna dirección estática para el puerto de recepción, el paquete se descarta. Por ejemplo, si un mapa estático para la dirección MAC X fue configurado en el puerto 0/2 para reenviar el tráfico al puerto 0/3, el paquete se debe recibir en el puerto 0/2, sino el paquete se descarta. Si un paquete se envía desde cualquier otro puerto, en la misma VLAN que el puerto 0/2, el paquete se descarta. • Si el puerto es un puerto

		seguro, los paquetes con las direcciones MAC de origen no habilitadas no se reenvían y se incrementa el contador.
Errores de alineación	Los errores de alineación son el número de tramas recibidas que no terminan con un número par de octetos y tienen una CRC defectuosa.	Los errores de alineación se presentan porque la trama no se ha copiado totalmente en el cable, por lo que se producen tramas fragmentadas. Estos son el resultado de colisiones en el semidúplex, dúplex de discordancia, problemas de hardware (NIC, cable o puerto), o un dispositivo conectado que genera tramas con FCS erróneo.
Errores de FCS	El error de conteo FCS es el número de tramas que se recibieron con una checksum incorrecta (valor CRC) en la trama Ethernet. Estas tramas se pierden y no se propagan en otros puertos.	Los errores de FCS son el resultado de colisiones en discordancia semidúplex o dúplex, problemas de hardware (NIC, cable o puerto) o la conexión de un dispositivo que genera tramas que no finalizan en un octeto y tienen un FCS erróneo.
Tramas de tamaño inferior al normal	El número total de paquetes recibidos que tienen una longitud menor de 64 octetos (excluidos los bits de entramado, pero incluidos los octetos FCS), y que sin embargo tiene un valor FCS	Esta es una indicación de una trama deficiente generada por el dispositivo conectado. Verifique que el dispositivo conectado funcione correctamente.

	adecuado.	
Tramas de gran tamaño	Número de paquetes recibidos en el puerto desde la red, donde los paquetes tenían más de 1514 bytes.	Es una indicación de hardware defectuoso, dot1q o un problema de configuración ISL.
Fragmentos de la colisión	La cantidad total de tramas cuya longitud sea inferior a 64 octetos (lo que excluye los bits de entramado, pero que incluyen FCS) y tienen un valor FCS defectuoso.	El aumento del contador indica que los puertos están configurados en semidúplex. Cambie la configuración dúplex a dúplex completo.
Tramas de desbordamiento	La cantidad de veces que el hardware de recepción no pudo entregar los datos recibidos a un buffer de hardware.	La velocidad de entrada de tráfico excedió la capacidad del receptor de manejar los datos.
Tramas filtradas VLAN	La cantidad total de tramas filtradas debido al tipo de información VLAN que contiene la trama.	El puerto se puede configurar para filtrar las tramas etiquetadas 802.1Q. Cuando se recibe una trama que contiene una etiqueta 802.1Q, la trama se filtra y aumenta este contador.
Tramas de origen ruteadas	La cantidad total de tramas recibidas descartadas debido a que el bit de la ruta de origen está definido en la dirección de origen de la trama nativa.	Este tipo de enrutamiento de origen solo se define para Token Ring y FDDI. La especificación Ethernet de IEEE prohíbe este bit en las tramas Ethernet. Por lo tanto, el switch desecha tales tramas.
Tramas de gran tamaño válidas	La cantidad total de tramas recibidas cuya longitud supera la MTU del sistema aunque tengan valores de FCS correctos.	Esta estadística cuenta las tramas que exceden el sistema configurado MTU pero que pueden haber aumentado de 1518 los bytes para

		permitir las especulaciones r Q-in-Q o MPLS.
Tramas de error de símbolo	Gigabit Ethernet (1000 Base-X) utiliza la codificación 8B/10B para traducir los datos 8bit de la subcapa MAC (capa 2) a un símbolo de 10 bit para enviar por cable. Cuando un puerto recibe un símbolo, extrae los datos de 8 bits del símbolo (10 bits).	Un error de símbolo significa que la interfaz detecta un símbolo indefinido recibido (inválido). Puede ignorarse una pequeña cantidad de errores de símbolos. Una gran cantidad de errores de símbolo puede indicar un dispositivo, cable, o hardware desfectuoso.
Tramas inválidas, demasiado grandes	Las tramas gigantes o las tramas recibidas que excedieron el tamaño máximo de trama IEEE 802.3 (1518 bytes para Ethernet no jumbo) y cuentan con una Secuencia de Verificación de Tramas (FCS) defectuosa.	En muchos casos, este es el resultado de un NIC defectuoso. Intente encontrar el dispositivo con problemas y retírelo de la red.
Tramas inválidas, demasiado pequeñas	Las tramas minúsculas o las tramas recibieron que son inferiores a 64 bytes (que incluye los bits FCS y excluye el encabezado de trama) y tienen un error FCS o un error de alineación.	Esto puede estar causado por una discordancia dúplex y problemas físicos, como un cable, un puerto o una NIC incorrectos en el dispositivo conectado.

Show Top para CatOS

El comando show top le permite recopilar y analizar los datos para cada puerto físico en un switch. El comando visualiza estos datos para cada puerto físico:

- Utilización de puertos (Uti %)
- Número de bytes entrantes y salientes (bytes)
- Número de paquetes entrantes y salientes (Pkts)
- Número de paquetes de broadcast (Bcst) entrantes y salientes
- Número de paquetes de multicast (Mcst) entrantes y salientes
- Número de errores (Error) entrantes
- Número de errores de sobrecarga en buffer (Overflow)

```
 Console> (enable) sh top Start Time: Mar 28 2007 06:58:41 End Time: Mar 28 2007 06:59:11
PortType: all Metric: util Port Band- Uti Bytes Pkts Bcst Mcst Error Over width % (Tx + Rx) (Tx
+ Rx) (Tx + Rx) (Tx + Rx) (Rx) flow ----- ----- --- -------------------- ---------- ---------- -
--------- ----- ---- 3/11 a-10 0 334187 1561 22 1536 0 0 3/12 a-100 0 333608 1557 22 1532 0 0
3/25 a-100 0 333622 1555 22 1533 0 0 6/2 1000 0 0 0 0 0 0 0 6/1 1000 0 0 0 0 0 0 0 4/8 1000 0 0
0 0 0 0 0 4/7 1000 0 0 0 0 0 0 0 4/6 1000 0 0 0 0 0 0 0 4/5 1000 0 0 0 0 0 0 0 4/4 1000 0 0 0 0
0 0 0 4/3 1000 0 0 0 0 0 0 0 4/2 1000 0 0 0 0 0 0 0 4/1 1000 0 0 0 0 0 0 0 3/48 auto 0 0 0 0 0 0
0 3/47 auto 0 0 0 0 0 0 0 3/46 auto 0 0 0 0 0 0 0
```

Nota: Cuando calcula la utilización del puerto, el comando agrupa las líneas Tx y Rx en el mismo contador y también observa el ancho de banda de dúplex completo cuando calcula el porcentaje de utilización. Por ejemplo, un puerto Gigabit Ethernet de 2000 Mbps en dúplex completo.

En Errores, es la suma de todos los paquetes de errores recibidos en ese puerto.

El desbordamiento de búfer significa que el puerto recibe más tráfico que el que puede almacenar en su buffer. Esto puede causar ráfagas de tráfico, también un desbordamiento de buffers. La acción sugerida es disminuir la transmisión del dispositivo de origen.

También consulte los contadores “In Lost” y “Out-Lost” del **comando show mac**.

Mensajes de Error Comunes del Sistema

Cisco IOS a veces tiene un formato diferente para los mensajes del sistema. Puede examinar los mensajes del sistema de CatOS y los mensajes del sistema de Cisco IOS para realizar una comparación. Puede consultar **Guía de Mensajes y Procedimientos de Recuperación** para la versión del software que ejecuta. Por ejemplo, puede observar los Mensajes y Procedimientos de Recuperación para la versión 7.6 del software CatOS y compararlos con los Mensajes y Procedimientos de Recuperación para las versiones de Cisco IOS 12.1 E.

Mensajes de Error en los Módulos WS-X6348

Observe estos mensajes de error:

- Coil Pinnacle Header Checksum
- Error de Estado de Máquina de Bobina Mdtif
- Coil Mdtif Packet CRC Error
- Coil Pb Rx Underflow Error
- Coil Pb Rx Parity Error

Puede ver los mensajes de syslog con uno de los errores enumerados:

```
%SYS-5-SYS_LCPERR5:Module 9: Coil Pinnacle Header Checksum Error - Port #37
```

Si ve este tipo de mensaje o nota que los grupos de 10/100 de los puertos que fallan en los módulos WS-X6348, consulte estos documentos para obtener consejo adicionales de troubleshooting en función del sistema operativo que utiliza:

- Troubleshooting de Conectividad del Puerto del Módulo WS-X6348 para Catalyst 6000 con CatOS
- Troubleshooting de Conectividad del Puerto del Módulo WS-X6348 para Catalyst 6500/6000 que ejecuta Cisco IOS System Software

%%PAGP-5-PORTTO / FROMSTP and %ETHC-5-PORTTO / FROMSTP

Para CatOS, use el comando show logging buffer para ver los mensajes de registro almacenados. Para Cisco IOS, use el **comando show logging**.

```
Console> (enable) sh logging buffer 2003 Jun 02 20:12:43 %PAGP-5-PORTTOSTP:Port 3/2 joined
bridge port 3/2 2003 Jun 02 20:59:56 %PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1 !--- This
is the command to view the logging buffer on switches that run CatOS.
```

Este mensaje podría preocupar a los clientes pero en general es informativo.

`%PAGP-5-PORTTO / FROMSTP and %ETHC-5-PORTTO / FROMSTP`

El Port Aggregation Protocol (PAgP) negocia los links EtherChannel entre los switches. Cuando un dispositivo se une o abandona un puerto de bridge, aparece un mensaje informativo en la consola. En la mayoría de los casos, este mensaje es totalmente normal, pero si ve estos mensajes en los puertos que no deberían mostrar inestabilidad por cualquier motivo, debe investigar más.

En la versión 7.x y posterior del software CatOS, "PAGP-5" se ha cambiado por "ETHC-5" para que el mensaje pueda comprenderse.

Este mensaje es específico a Catalyst 4000, 5000, 6000 Series Switch que ejecutan CatOS. No hay mensajes de error para switches que ejecutan Cisco IOS que sean equivalentes a este mensaje. Para obtener más información sobre los mensajes de error en los switches que ejecutan CatOS, consulte estos documentos para su plataforma:

- Mensajes de Error Comunes de CatOS en Catalyst 4000 Series Switches
- Mensajes de Error Comunes de CatOS en Catalyst 5000/5500 Series Switches
- Mensajes de Error Comunes de CatOS en Catalyst 6500/6000 Series Switches

%SPANTREE-3-PORTDEL_FAILNOTFOUND

Este mensaje no indica un problema con el switch. Se produce normalmente junto con los mensajes %PAGP-5-PORTFROMSTP.

El Port Aggregation Protocol (PAgP) negocia los links EtherChannel entre los switches. Cuando un dispositivo se une o abandona un puerto de bridge, aparece un mensaje informativo en la consola. En la mayoría de los casos, este mensaje es totalmente normal, pero si ve estos mensajes en los puertos que no deberían mostrar inestabilidad por cualquier motivo, debe investigar más.

Este mensaje es específico a Catalyst 4000, 5000, 6000 Series Switch que ejecutan CatOS. No hay mensajes de error para switches que ejecutan Cisco IOS que sean equivalentes a este mensaje. Para obtener más información sobre los mensajes de error en los switches que ejecutan CatOS, consulte estos documentos para su plataforma:

- Mensajes de Error Comunes de CatOS en Catalyst 4000 Series Switches
- Mensajes de Error Comunes de CatOS en Catalyst 5000/5500 Series Switches
- Mensajes de Error Comunes de CatOS en Catalyst 6500/6000 Series Switches

%SYS-4-PORT_GBICBADEEPROM: //%SYS-4-PORT_GBICNOTSUPP

La causa más común de este mensaje es cuando se introduce un GBIC no homologado de otro fabricante en un módulo Gigabit Ethernet. El GBIC no tiene una SEEPROM de Cisco, por lo que se genera un mensaje de error.

Los módulos GBIC WS-G5484, WS-G5486 y WS-G5487 utilizados con una tarjeta WS-X6408-GBIC también pueden hacer que aparezcan estos mensajes, aunque no hay problemas con la tarjeta o GBIC y puede obtenerse un parche de software para ello.

Consulte Mensajes de Error Comunes para CatOS en Catalyst 6000/6500 Series Switches para obtener más información.

%AMDP2_FE-3-UNDERFLO

Este mensaje de error aparece cuando se transmite una trama, y el buffer local del chip del controlador del buffer local no recibe suficientes datos. Los datos no se pueden transferir al chip lo suficientemente rápido para ajustarse a la velocidad de salida. Normalmente, esa condición es temporal, según las cargas pico transitorias dentro del sistema. El problema ocurre cuando una cantidad excesiva de tráfico es procesada por la interfaz Fast Ethernet. Se recibe el mensaje de error cuando el nivel de tráfico alcanza aproximadamente 2.5 Mb. Esta restricción del nivel de tráfico se debe a la limitación del hardware. Debido a esto, existe la posibilidad de que el dispositivo conectado al switch de catalyst descarte paquetes.

La resolución por lo general es que el sistema se recupera de forma automática. No se requiere ninguna acción. Si el switch sobrecarga la interfaz de Ethernet, verifique las configuraciones de velocidad y dúplex. También use un programa sniffer para analizar los paquetes que entran y salen de la interfaz Fast Ethernet del router. Para evitar los descartes de paquetes en el dispositivo conectado con el switch de Catalyst, ejecute el comando ip cef en la interfaz Fast Ethernet del dispositivo conectado con el switch.

%INTR_MGR-DFC1-3-INTR: Motor de Cola (Blackwater) [1]: Código de Control Inesperado Recibido de Entramado A FIC

La razón de este mensaje de error es la recepción de un paquete del switch fabric, donde el valor de CRC en el encabezado del entramado en ese paquete no se correspondió con el valor de CRC calculado por el subbloque del Controlador de Interfaz de Entramado (FIC) de Blackwater ASIC. Esto indica que una corrupción del paquete se produjo dentro de la transferencia, y Blackwater recibió el paquete corrupto.

Comando Rechazado: [[Interface] not a Switching Port

En los switches que soportan interfaces L3 y L2, aparece el mensaje *Command rejected: [[interface] not a switching port* cuando intenta ingresar un comando relacionado con la Capa 2 en un puerto que está configurado como interfaz de capa 3.

Para convertir la interfaz de modo de capa 3 a modo de capa 2, ejecute el comando de configuración de interfaz **switchport**. Después de que ejecute este comando, configure el puerto para cualquier propiedad de capa 2.

Problemas Comunes del Puerto y de la Interfaz

El Estado del Puerto o de la Interfaz es Disable o Shutdown

Una causa obvia pero que a veces se ignora de la falla en la conectividad del puerto es la configuración incorrecta en el switch. Si un puerto tiene una luz naranja permanente, significa que

el software dentro del switch apaga el puerto, por la interfaz de usuario o por los procesos internos.

Nota: Algunos LED de puertos de la plataforma funcionan de forma diferente con respecto al STP. Por ejemplo, el Catalyst 1900/2820 muestra los puertos de color naranja cuando están en el modo de bloqueo de STP. En este caso, una luz naranja puede indicar las funciones normales del STP. El Catalyst 6000/5000/4000 no muestra el puerto de color naranja cuando bloquea el STP.

Asegúrese de que el puerto o el módulo no se ha inhabilitado ni se ha apagado por alguna razón. Si un puerto o un módulo se apaga manualmente en un lado del link o el otro, el link no se activa hasta que rehabilita el puerto. Revise el estado del puerto en ambos lados.

Para CatOS, verifique **show port** y, si el puerto está**inhabilitado**, vuelva a habilitarlo.

```
Port  Name                 Status     Vlan       Duplex Speed Type
----- -------------------- ---------- ---------- ------ ----- ------------
 3/1                       disabled 1 auto auto 10/100BaseTX !--- Use the set port enable
mod/port command to re-enable this port.
```

Use el **comando show module** para determinar si el módulo está inhabilitado. Si está inhabilitado, vuelva a habilitarlo:

```
Mod Slot Ports Module-Type              Model               Sub Status
--- ---- ----- ------------------------ ------------------- --- --------
2   2    2     1000BaseX Supervisor     WS-X6K-SUP1A-2GE    yes ok
16  2    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
3   3    48    10/100BaseTX Ethernet    WS-X6348-RJ-45      no  disable !--- Use the set module
enable mod/port command to re-enable this port.
```

Para Cisco IOS, use el **comando show run interface** y verifique si la interfaz está en**estado shutdown**:

```
Switch#sh run interface fastEthernet 4/2 ! interface FastEthernet4/2 switchport trunk
encapsulation dot1q switchport mode trunk shutdown duplex full speed 100 end !--- Use the no
shut command in config-if mode to re-enable this interface.
```

Si el puerto entra en el modo shutdown inmediatamente después de reiniciar el switch, la causa probable es la configuración de seguridad del puerto. Si la inundación de unicast está habilitada en ese puerto, puede hacer que el puerto se apague después de un reinicio. Cisco recomienda que inhabilite la inundación de unicast porque también garantiza que no se produzca inundación en el puerto una vez que se alcanza el límite de la dirección MAC

El Estado del Puerto o de la Interfaz es errDisable

De forma predeterminada, los procesos de software dentro del switch pueden apagar o interconectar un puerto si se detectan ciertos errores.

Cuando mira el **comando show port** para CatOS, el estado puede ser **errdisable**:

```
switch>(enable) sh port 4/3 Port Name Status Vlan Duplex Speed Type ----- ------------------- -
--------- ---------- ------ ----- ------------ 4/3 errdisable 150 auto auto 10/100BaseTX !---
The show port command displays a status of errdisable.
```

O use el comando **show interface** *card-type {slot/port}* **status** para Cisco IOS:

```
Router#show int fasteth 2/4 status Port Name Status Vlan Duplex Speed Type Gi2/4 err-disabled 1
full 1000 1000BaseSX !--- The show interfaces card-type {slot/port} status command for Cisco IOS
!--- displays a status of errdisabled. !--- The show interfaces status errdisabled command shows
all the interfaces !--- in this status.
```

El comando show logging buffer para CatOS y el comando show logging para Cisco IOS también muestran mensajes de error (el formato de mensaje exacto varía) que se relacionan con el estado errdisable.

Los puertos o las interfaces apagadas como resultado de errdisable se denominan razones en CatOS y causas en Cisco IOS. Las razones o las causas de esta situación incluyen error de configuración de EtherChannel que provoca inestabilidad PAgP, discordancia dúplex, protección BPDU y portfast configurados al mismo tiempo, UDLD que detecta un enlace unidireccional.

Tiene que volver a habilitar manualmente o interconectar el puerto para sacarlo del estado errdisable a menos que configure una opción de recuperación errdisable. En software CatOS 5.4(1) y posterior, puede volver a habilitar un puerto automáticamente después de un período de tiempo configurable transcurrido en el estado errdisable. El Cisco IOS en la mayoría de los switches también tiene estas funcionalidades. Lo importante es que incluso si configura la interfaz para recuperarse del errdisable, el problema vuelve a aparecer hasta que se determine la causa raíz.

Para más información sobre las causas de y la recuperación del estado errdisable para los switches que ejecutan CatOS, consulte Recuperación del Estado del Puerto errDisable en las Plataformas de CatOS.

Nota: Use este link como referencia para el estado errdisable en los switches que ejecutan Cisco IOS, puesto que las causas raíz no son las mismas independientemente del sistema operativo que se utilice.

Esta tabla muestra una comparación de los comandos usados para configurar, verificar el estado errdisable, y resolver problemas relacionados con este en los switches que ejecutan CatOS y el Cisco IOS. Elija un comando para ir a la documentación correspondiente.

Comandos errdisable de CatOS	Acción	Comandos errdisable de Cisco IOS
set errdisable-timeout {enable | disable} {reason}	establecer o configurar	errdisable detect cause errdisable recovery cause
set errdisable-timeout interval {interval	establecer o configurar	errdisable recovery {interval
show errdisable timeout	verificar y resolver problemas	show errdisable detect show interfaces status err-disabled

El Estado del Puerto o la Interfaz está Inactivo

Una causa común de los puertos inactivos en los switches que ejecutan CatOS es cuando desaparece la VLAN a la que pertenecen. El mismo problema puede producirse en los switches que ejecutan Cisco IOS cuando las interfaces se configuran como puertos de switch de capa 2 que utilizan el comando switchport.

Cada puerto en un switch de Capa 2 pertenece a una VLAN. Cada puerto en un switch de capa 3 configurado para ser un puerto de switch L2 también debe pertenecer a una VLAN. Si se elimina

esa VLAN, el puerto o la interfaz se vuelve inactiva.

Nota: Algunos switches muestran una luz constante de color anaranjado (ámbar) en cada puerto cuando esto sucede.

Para CatOS, use el comando **show port** or **show port status** junto con el comando **show vlan** para verificar:

```
Switch> (enable) sh port status 2/2 Port Name Status Vlan Duplex Speed Type ----- --------------
------ ---------- ---------- ------ ----- ------------ 2/2 inactive 2 full 1000 1000BaseSX !---
Port 2/2 is inactive for VLAN 2. Switch> (enable) sh vlan VLAN Name Status IfIndex Mod/Ports,
Vlans ---- -------------------------------- --------- ------- ------------------------ 1 default
active 5 2/1 !--- VLANs are displayed in order and VLAN 2 is missing.
```

Para Cisco IOS, use el comando **show interfaces** *card-type {slot/port}* **switchport** junto con **show vlan** para verificar.

```
Router#sh interfaces fastEthernet 4/47 switchport Name: Fa4/47Switchport: Enabled Administrative
Mode: static access Operational Mode: static access Administrative Trunking Encapsulation:
negotiate Operational Trunking Encapsulation: native Negotiation of Trunking: Off Access Mode
VLAN: 11 ((Inactive)) !--- FastEth 4/47 is inactive. Router#sh vlan VLAN Name Status Ports ----
-------------------------------- --------- ------------------------------- 1 default active
Gi1/1, Gi2/1, Fa6/6 10 UplinkToGSR's active Gi1/2, Gi2/2 !--- VLANs are displayed in order and
VLAN 11 is missing. 30 SDTsw-1ToSDTsw-2Link active Fa6/45
```

Si el switch que eliminó la VLAN es un servidor VTP para el dominio VTP, se eliminará también la VLAN de todos los switches servidor y cliente del dominio en su tabla VLAN. Cuando agrega la VLAN nuevamente dentro de la tabla de VLAN de un switch del servidor VTP, los puertos de los switches en el dominio que pertenecen a esa VLAN restaurada se activan nuevamente. Un puerto recuerda qué VLAN se asigna, incluso si se elimina la VLAN en sí.

ConsulteComprensión y Configuración del VLAN Trunk Protocol (VTP) para obtener más información sobre el VTP.

Nota: Si la salida del comando **show interface <interface number> switchport** muestra el puerto como puerto trunk incluso después de configurar el puerto como puerto de acceso con el comando **switchport access vlan** *<vlan no: >* , ejecute el comando **switchport mode access** para que el puerto sea un puerto de acceso.

El Estado del Puerto Uplink o de la Interfaz está Inactivo

En un Catalyst 4510R series switch, para habilitar los puertos de uplink SFP 10-Gigabit Ethernet o Gigabit Ethernet, existe una configuración opcional: Para habilitar el uso simultáneo de interfaces 10-Gigabit Ethernet y Gigabit Ethernet SFP, ejecute el comando hw-module uplink select all. Después de ejecutar el comando, reinicie el switch o la salida del comando**show interface status module** *module number* muestra al puerto uplink como inactivo.

El Cisco IOS Software Release 12.2(25)SG soporta el uso simultáneo de las interfaces 10-Gigabit Ethernet y Gigabit Ethernet SFP en los switches Catalyst 4500.

Nota: En los switches Catalyst de las series 4503, 4506, y 4507R, esta capacidad se habilita automáticamente.

El Contador Diferido en la Interfaz del Switch de Catalyst Comienza a Incrementarse

El problema se debe a que la carga de tráfico destinada al switch es excesiva y hace que se descarten tramas. Normalmente, las tramas diferidas son el número de tramas transmitidas con éxito después de esperar que el dispositivo dejara de estar ocupado. Esto suele ocurrir en entornos semidúplex donde la portadora ya está en uso al intentar transmitir una trama. Pero en los entornos de dúplex completo, el problema ocurre cuando la carga excesiva está destinada para el switch.

Esta es la solución temporal:

- Ajustar manualmente ambos extremos del enlace a dúplex completo para evitar la discordancia en la negociación.
- Cambiar el cable y las conexiones del panel para asegurarse de que no sean defectuosos.

Nota: Si el error del Contador Diferido incrementa en un GigabitEthernet de un Supervisor 720, active la negociación de velocidad en la interfaz como solución temporal.

Falla Intermitente al definir el temporizador [valor] de vlan [n.º vlan]

Esto ocurre cuando la Lógica de Reconocimiento de Dirección Codificada (EARL) no está habilitada para definir el tiempo de envejecimiento para la VLAN a la cantidad de segundos requerida. En este caso, el tiempo de envejecimiento de la VLAN ya está ajustado a envejecimiento rápido.

Si la VLAN ya se encuentra en envejecimiento rápido, EARL no puede ajustar la VLAN a envejecimiento rápido y se bloquea el proceso definido de temporizador de envejecimiento. El tiempo de envejecimiento CAM predeterminado es de cinco minutos, lo que significa que el switch restablece la tabla de direcciones MAC aprendidas cada cinco minutos. De esta forma, se garantiza que la tabla de direcciones MAC (la tabla CAM) contenga las últimas entradas.

El envejecimiento rápido ajusta temporalmente el tiempo de envejecimiento CAM al número de segundos especificado por el usuario y se utiliza junto con el proceso de Notificación de Cambios de Topología (TCN). La idea es que cuando se produce un cambio de topología, este valor es necesario para restablecer la tabla CAM más rápidamente y compensar el cambio en la topología.

Ejecute el comando **show cam aging** para verificar el tiempo de envejecimiento CAM en el switch. Los TCN y el envejecimiento rápido son muy poco frecuentes. Como consecuencia, el mensaje tiene un nivel de gravedad de 3. Si las VLAN se encuentran a menudo en envejecimiento rápido, investigue la causa del problema.

La causa más común de las TCN es cuando hay clientes PC conectados directamente a un switch. Al encender o apagar la PC, el puerto del switch cambia de estado y el switch empieza el proceso TCN. Esto es debido a que el switch no sabe que el dispositivo conectado es un PC; el switch sólo sabe que el puerto ha cambiado de estado.

Para solucionar este problema, Cisco ha creado la función PortFast para los puertos de host. La ventaja de PortFast es que esta función elimina las TCN en los puertos de host.

Nota: PortFast también omite los cálculos del spanning-tree en el puerto, por lo que la función sólo es adecuada en los puertos de host.

Para habilitar PortFast en el puerto, configure uno de estos comandos:

set spantree portfast mod/port enable | inhabilitar

o

set port host mod/port Cisco recomienda este comando si el switch ejecuta CatOS5.4 o versiones posteriores.

Discordancía del modo de concentración links

Verifique el modo de trunking en cada lado del link. Asegúrese de que ambos lados estén en el mismo modo (ambos se conectan mediante trunking con el mismo método: ISL o 802.1q, o ninguno se conecta mediante trunking). Si activa el modo trunking (opuesto al modo automático o deseable) para un puerto y el otro puerto tienen el modo de trunking desactivado, no se pueden comunicar. El trunking cambia el formato del paquete. Los puertos tienen que estar de acuerdo sobre el formato que utilizan en el link, ya que de lo contrario no se entenderán.

Para CatOS, use el comando **show trunk** {mod/port} para verificar el estado del trunk y que la VLAN nativa coincide en ambos extremos (para dot1q).

```
Switch> (enable) sh trunk 3/1 * - indicates vtp domain mismatch Port Mode Encapsulation Status
Native vlan -------- ----------- ------------ ------------ ----------- 3/1 desirable dot1q
trunking 1 Port Vlans allowed on trunk -------- -----------------------------------------------
--------------------- 3/1 1-1005,1025-4094 !--- Output truncated.
```

Para Cisco IOS, use el comando **show interfaces** *card-type {mod/port}* **trunk** para verificar la configuración de trunking y la VLAN Nativa.

```
Router#sh interfaces fastEthernet 6/1 trunk Port Mode Encapsulation Status Native vlan Fa6/1
desirable 802.1q trunking 1 Port Vlans allowed on trunk Fa6/1 1-4094 !--- Output truncated.
```

Consulte estos documentos para obtener más información sobre los diversos modos de trunking, pautas y restricciones:

- Requisitos del Sistema para Implementar el Trunking
- Página de Soporte sobre Tecnología de Trunking

Jumbo, Giants, y Baby Giants

De forma predeterminada, la Unidad Máxima de Transmisión (MTU) de la parte de datos de las tramas Ethernet es de 1500 bytes. Si el tráfico de MTU transmitido supera la MTU soportada, el switch no reenviará el paquete. Además, según el hardware y software, algunas plataformas de switch incrementan los contadores de error de puerto e interfaz como resultado.

- Las tramas Jumbo no se definen como parte de la norma IEEE Ethernet y dependen del proveedor. Se podrían definir como las tramas que superan la trama estándar de Ethernet de 1518 bytes (incluido el encabezado de la capa 2 y la Verificación por Redundancia Cclica [CRC]). Los jumbos suelen tener un tamaño de trama mayor, generalmente > 9000 bytes.
- Las tramas recibidas que excedieron el tamaño máximo de trama (1518 bytes para Ethernet no jumbo) y cuentan con una FCS mala.
- Las tramas Baby Giant son ligeramente mayores que el tamaño máximo de una trama Ethernet. Generalmente se trata de tramas de hasta 1600 bytes de tamaño.

La compatibilidad con los jumbos y los baby giants en los switches Catalyst varía según la plataforma del switch, algunas veces según los módulos dentro del switch. La versión de software también es un factor.

Consulte Configuración de Soporte de Tramas Jumbo/Giant en Switches de Catalyst para obtener más información sobre los requisitos del sistema, la configuración y la resolución de problemas con jumbos y baby giant.

No se Detecta mediante Ping el Dispositivo Final

Verifique el dispositivo final al hacer primero un ping desde el switch directamente conectado y, a continuación, retroceda progresivamente por cada puerto, interfaz, trunk hasta encontrar el origen del error de conectividad. Compruebe que todos los switches puedan ver la dirección MAC del dispositivo final en su tabla de Memoria de Contenido Direccional (CAM).

Para CatOS, use el comando show cam dynamic {mod/port}.

```
Switch> (enable) sh cam dynamic 3/1 * = Static Entry. + = Permanent Entry. # = System Entry. R =
Router Entry. X = Port Security Entry $ = Dot1x Security Entry VLAN Dest MAC/Route Des [CoS]
Destination Ports or VCs / [Protocol Type] ---- ------------------ ----- ----------------------
-------------------- 2 00-40-ca-14-0a-b1 3/1 [ALL] !--- A workstation on VLAN 2 with MAC address
00-40-ca-14-0a-b1 is seen in the CAM table !--- on the trunk port of a switch running CatOS.
Total Matching CAM Entries Displayed =1 Console> (enable)
```

Para Cisco IOS, use el comando show mac address-table dynamic, o sustituya la palabra clave **interface** .

```
Router# sh mac-address-table int fas 6/3 Codes: * - primary entry vlan mac address type learn
qos ports ------+----------------+--------+-----+---+------------------------- * 2
0040.ca14.0ab1 dynamic No -- Fa6/3 !--- A workstation on VLAN 2 with MAC address 0040.ca14.0ab1
is directly connected !--- to interface fastEthernet 6/3 on a switch running Cisco IOS.
```

Una vez que sabe que el switch tiene realmente la dirección MAC del dispositivo en su tabla CAM, determine si este dispositivo está en la misma VLAN o una VLAN distinta de aquella en la que hacer el ping,

Si el dispositivo final se encuentra en una VLAN distinta de aquella en la que intenta hacer el ping, debe configurar un switch L3 o router para permitir que los dispositivos se comuniquen. Compruebe que el direccionamiento L3 en el dispositivo final y en el router/switch L3 esté bien configurado. Verifique la dirección IP, el gateway máscara de subred, el gateway predeterminado, la configuración del Dynamic Routing Protocol, rutas estáticas, etc.

Uso de Set Port Host o Switchport Host para Solucionar Retrasos de Inicialización

Si las estaciones no pueden comunicarse con sus servidores primarios al conectarse a través de un switch, el problema pueden implicar demoras en el puerto del switch que se vuelve activo una vez que se activa el link de la capa física. En algunos casos, estas demoras pueden alcanzar los 50 segundos.

Algunas estaciones de trabajo no pueden esperar tanto antes de encontrar su servidor sin abandonar el intento. Estas demoras se deben al STP, las negociaciones de trunking (DTP), y las negociaciones de EtherChannel (PAgP). Todos estos protocolos puede inhabilitarse para los puertos de acceso cuando no son necesarios, de manera que el puerto de switch empezará a reenviar paquetes pocos segundos después de establecer un enlace con el dispositivo vecino.

El comando set port host se introdujo en la versión 5.4 de CatOS. Este comando desactiva los modos de trunking y de canal, y deja el puerto en estado de reenvío STP.

```
Switch> (enable) set port host 3/5-10 Port(s) 3/5-10 channel mode set to off. !--- The set port
host command also automatically turns off etherchannel on the ports. Warning: Spantree port fast
```

```
start should only be enabled on ports connected to a single host. Connecting hubs,
concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree
loops. Use with caution. !--- Notice the switch warns you to only enable port host on access
ports. Spantree ports 3/5-10 fast start enabled.Dot1q tunnel feature disabled on port(s) 3/5-10.
Port(s) 3/5-10 trunk mode set to off. !--- The set port host command also automatically turns
off trunking on the ports.
```

Nota: Para las versiones de CatOS anteriores a 5.4, se usó el comando **set spantree portfast** {mod/port} **enable**. En las versiones actuales de CatOS, aún tiene la opción de usar solo este comando, pero para ello es necesario desactivar el trunking y EtherChannel por separado para ayudar a arreglar las demoras de inicio de la estación de trabajo. Los comandos adicionales para hacer esto son los siguientes: **set port channel** {mod/port} **off** y **set trunk** {mod/port} **off** .

Para Cisco IOS, puede usar el comando **switchport host** para deshabilitar la canalización y para habilitar spanning-tree portfast y el comando **switchport nonegotiate** para desactivar los de paquetes de negociación de DTP. Use el comando **interface-range** para hacer esto en varias interfaces a la vez.

```
Router6k-1(config)#int range fastEthernet 6/13 - 18 Router6k-1(config-if-range)#switchport
Router6k-1(config-if-range)#switchport host switchport mode will be set to access spanning-tree
portfast will be enabled channel group will be disabled !--- Etherchannel is disabled and
portfast is enabled on interfaces 6/13 - 6/18. Router6k-1(config-if-range)#switchport
nonegotiate !--- Trunking negotiation is disabled on interfaces 6/13 - 6/18. Router6k-1(config-
if-range)#end Router6k-1#
```

Cisco IOS tiene la opción de utilizar el **global spanning-tree portfast default** para aplicar de forma automática portfast a cualquier interfaz configurada como switchport de acceso de capa 2. Verifique la Referencia de Comando para su versión de software para determinar la disponibilidad de este comando. También puede usar el comando **spanning-tree portfast** por interfaz, para ello es necesario desactivar el trunking y EtherChannel por separado para ayudar a solucionar las demoras en el inicio de la estación de trabajo.

Consulte Utilización de Portfast y Otros Comandos para Solucionar Demoras de Conectividad en el Inicio de la Estación de Trabajo para obtener más información sobre cómo solucionar las demoras en el inicio.

Problemas de Velocidad y Dúplex, Negociación Automática o con Tarjetas NIC

Una gran cantidad de errores de alineación, errores FCS o colisiones tardías pueden indicar lo siguiente:

- discordancia dúplex
- Cable Dañado o Defectuoso
- Problemas con la Tarjeta NIC

discordancia dúplex

Un problema habitual de velocidad/dúplex es cuando la configuración dúplex no concuerda entre dos switches, entre un switch y un router o entre el switch y una estación de trabajo o servidor. Esto puede suceder al definir manualmente los ajustes de velocidad y dúplex o debido a problemas de autonegociación entre los dos dispositivos.

Si la discordancia se produce entre dos dispositivos de Cisco con el Cisco Discovery Protocol (CDP) habilitado, consulte los mensajes de error del CDP en la consola o en el buffer de registro de ambos dispositivos. El CDP es útil para detectar errores, así como las estadísticas del sistema en los dispositivos de Cisco cercanos. CDP es propiedad de Cisco y funciona al enviar paquetes a una dirección mac conoocida 01-00-0C-CC-CC-CC.

El ejemplo muestra los mensajes de log que resultan de una discordancia de dúplex entre dos Catalyst 6000 series switches: uno que ejecuta CatOS, y el otro ejecuta Cisco IOS. Estos mensajes generalmente le dicen cuál es la discordancia y dónde se produce.

```
2003 Jun 02 11:16:02 %CDP-4-DUPLEXMISMATCH:Full/half duplex mismatch detected on port 3/2
!--- CatOS switch sees duplex mismatch. Jun 2 11:16:45 %CDP-4-DUPLEX_MISMATCH: duplex mismatch
discovered on FastEthernet6/2 (not half duplex), with TBA04251336 3/2 (half duplex). !--- Cisco
IOS switch sees duplex mismatch.
```

Para CatOS, use el comando **show cdp neighbor** *[mod/port]* **detail** para visualizar la información CDP para los dispositivos vecinos de Cisco.

```
Switch> (enable) sh cdp neighbor 3/1 detail Port (Our Port): 3/1 Device-ID: Router Device
Addresses: IP Address: 10.1.1.2 Holdtime: 133 sec Capabilities: ROUTER SWITCH IGMP Version:
Cisco Internetwork Operating System Software IOS (tm) c6sup2_rp Software (c6sup2_rp-PK2S-M),
Version 12.1(13)E6, EARLY DEPL OYMENT RELEASE SOFTWARE (fc1) TAC Support:
http://www.cisco.com/tac Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Fri 18-Apr-03
15:35 by hqluong Platform: cisco Catalyst 6000 Port-ID (Port on Neighbors's Device):
FastEthernet6/1 !--- Neighbor device to port 3/1 is a Cisco Catalyst 6000 Switch on !--- FastEth
6/1 running Cisco IOS. VTP Management Domain: test1Native VLAN: 1 Duplex: full !--- Duplex is
full. System Name: unknown System Object ID: unknown Management Addresses: unknown Physical
Location: unknown Switch> (enable)
```

Para Cisco IOS, use el comando **show cdp neighbors** *card-type {slot/port}* **detail** para visualizar la información CDP para los dispositivos vecinos de Cisco.

```
Router#sh cdp neighbors fastEthernet 6/1 detail ------------------------- Device ID: TBA04251336
Entry address(es): IP address: 10.1.1.1 Platform: WS-C6006, Capabilities: Trans-Bridge Switch
IGMP Interface: FastEthernet6/1, Port ID (outgoing port): 3/1 Holdtime : 152 sec Version : WS-
C6006 Software, Version McpSW: 6.3(3) NmpSW: 6.3(3) Copyright (c) 1995-2001 by Cisco Systems !--
- Neighbor device to FastEth 6/1 is a Cisco Catalyst 6000 Switch !--- on port 3/1 running CatOS.
advertisement version: 2 VTP Management Domain: 'test1' Native VLAN: 1 Duplex: full !--- Duplex
is full. Router#
```

Definir un ajuste de velocidad/dúplex automático en un lado y 100/dúplex completo en el otro también es un error de configuración que puede provocar una discordancia de dúplex. Si el puerto de switch recibe un montón de colisiones tardías, esto indica generalmente un problema de discordancia de dúplex y puede hacer que el puerto se coloque en estado errdisable. El lado semidúplex solo espera paquetes en determinados momentos, no en cualquier momento, por lo que podría contar los paquetes recibidos a destiempo como colisiones. Hay otras causas para las colisiones tardías además de la discordancia de dúplex, pero es una de las razones más comunes. Siempre configure ambos lados de la conexión para que negocien automáticamente los ajustes de velocidad y dúplex, o definir estos ajustes manualmente en ambos lados.

Para CatOS, use el comando **show port status** [mod/port] para visualizar el estado de velocidad y el dúplex además de otra información. Use los comandos **set port speed** y **set port duplex** para ajustar ambos lados a 10 o 100 y semidúplex o dúplex completo, según convenga.

```
Switch> (enable) sh port status 3/1 Port Name Status Vlan Duplex Speed Type ----- --------------
------ ---------- ---------- ------ ----- ------------ 3/1 connected 1 a-full a-100 10/100BaseTX
Switch> (enable)
```

Para Cisco IOS, use el comando **show interfaces** card-type {slot/port} **status** para visualizar las configuraciones de velocidad y dúplex y otra información. Use los comandos **speed and duplex**s del modo de configuración de interfaz para ajustar manualmente ambos lados a 10 o 100 y semidúplex o dúplex completo, según convenga.

```
Router#sh interfaces fas 6/1 status Port Name Status Vlan Duplex Speed Type Fa6/1 connected 1 a-
full a-100 10/100BaseTX
```

Si usa el comando **show interfaces** sin la **opción de estado**, aparecerán los ajustes de velocidad y dúplex, pero no se sabrá si estos valores de velocidad y dúplex se obtuvieron o no por

negociación automática.

```
Router#sh int fas 6/1 FastEthernet6/1 is up, line protocol is up (connected) Hardware is C6k
100Mb 802.3, address is 0009.11f3.8848 (bia 0009.11f3.8848) MTU 1500 bytes, BW 100000 Kbit, DLY
100 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set
Full-duplex, 100Mb/s !--- Full-duplex and 100Mbps does not tell you whether autoneg was used to
achieve this. !--- Use the sh interfaces fas 6/1 status command to display this.
```

Cable dañado o defectuoso

Compruebe siempre que el cable no sufra daños o fallas marginales. El cable puede ser lo suficientemente bueno para conectarse a la capa física, pero corrompe los paquetes como resultado de pequeños daños en el cableado o los conectores. Compruebe o intercambie el cable de cobre o fibra. Intercambie las conexiones de fibra del GBIC (si es extraíble). Descarte las conexiones erróneas del patch panel o los conversores de medios entre el origen y el destino. Intente colocar el cable en otro puerto o interfaz si hay alguno disponible y verifique si el problema continúa.

Problemas de Negociación automática y con la Tarjeta NIC

Los problemas a veces se producen entre los switches de Cisco y ciertas tarjetas NIC de terceros. Los puertos de los switches Catalyst y las interfaces están predeterminados para negociar automáticamente. Es habitual que los dispositivos portátiles u otros dispositivos también estén predeterminados para negociar automáticamente, aunque a veces se producen problemas.

Para resolver problemas de negociación automática, se suele recomendar ajustar manualmente ambos lados. Si ni la negociación automática ni la configuración manual parecen funcionar, podría haber un problema con el firmware o el software de la tarjeta NIC. Actualizar el driver de la tarjeta NIC a la última versión disponible en el sitio web de la fábrica para resolver el problema.

Consulte Configuración y Troubleshooting de Negociación Automática de Semidúplex/Dúplex Completo de Ethernet 10/100/1000Mbn para obtener detalles sobre cómo resolver problemas de velocidad/dúplex y negociación automática.

Consulte Resolución de Problemas de Compatibilidad entre los Switches Catalyst de Cisco y las NIC para obtener información sobre cómo resolver los problemas NIC de terceros.

Loops del Spanning Tree

Los loops del Spanning-Tree Protocol (STP) pueden provocar problemas graves de rendimiento que se disfrazan como problemas de puerto o interfaz. En esta situación, su ancho de banda es utilizado por las mismas tramas una y otra vez, lo que deja poco espacio para el tráfico legítimo.

La función de protección de loop del STP brinda protección adicional contra los loops de reenvío de Capa 2 (loops STP). Un loop de STP se crea cuando un puerto de bloqueo STP en las transiciones erróneas de una topología redundante al estado de reenvío. Esto sucede generalmente porque uno de los puertos de una topología redundante (no no necesariamente el puerto de bloqueo STP) recibe físicamente no más de BPDU de STP. En su operación, el STP está basado en la transmisión o en la recepción continua de las BPDU, según el rol del puerto. El puerto designado transmite los BPDU, y el puerto no designado recibe los BPDU.

Cuando uno de los puertos en una topología físicamente redundante deja de recibir BPDU, el STP considera a la topología como un loop libre. Finalmente, se designa el puerto de bloqueo del puerto de respaldo o alternativo y pasa al estado de reenvío. Esta situación crea un loop.

La función de protección de loop hace verificaciones adicionales. Si ya no se reciben las BPDU en un puerto no designado y el protector de loop está habilitado, ese puerto será desplazado a un estado de bloqueo incoherente con el loop en lugar de desplazarse a un estado de escuchar/aprender/reenviar. Sin la función de protección de loop, el puerto asumiría el rol de puerto designado. El puerto se desplaza al estado de reenvío de STP y crea un loop. Consulte Mejoras del Spanning-Tree Protocol usando las Funciones de Protección de Loop y Detección de Desviación de BPDU para obtener más información sobre la función de protección de loop.

Este documento abarca las razones por las que el STP puede fallar, qué información buscar para identificar el origen del problema, y qué clase de diseño minimiza los riesgos de STP.

Los loops también pueden provocarse por un link unidireccional. Para obtener más información, consulte la sección UDLD: problemas de link unidireccional de este documento.

UDLD: link unidireccional

Un link unidireccional es un link en el que el tráfico sale en un sentido, pero no se recibe tráfico en sentido contrario. El switch no sabe que el link de retorno es defectuoso (el puerto piensa que el link está activo y que funciona).

La rotura de un cable de fibra u otros problemas en los cables o el puerto pueden provocar esta comunicación unidireccional. Estos links parcialmente funcionales pueden producir problemas como los loops de STP cuando los switches involucrados no saben que el link está dañado parcialmente. El UDLD puede poner un puerto en el estado de errdisable cuando detecta un link unidireccional. El comando udld aggressive-mode puede configurarse en los switches que ejecutan CatOS y Cisco IOS (consulte la disponibilidad de comandos en las release notes) para conexiones punto a punto entre switches cuando los links defectuosos no se pueden tolerar. Esta función ayuda a identificar problemas con los links unidireccionales de difícil detección

Consulte Comprensión y Configuración del Unidirectional Link Detection Protocol (UDLD) para obtener información de configuración sobre el UDLD.

Tramas Diferidas (Out-Lost o Out-Discard)

Si tiene un gran número de tramas diferidas, o Out-Discard (también denominadas Out-Lost en algunas plataformas), significa que los buffers de salida del switch se llenaron y el switch tuvo que descartar estos paquetes. Esto podría indicar que este segmento opera con una velocidad o dúplex inferior, o que hay demasiado tráfico en este puerto.

Para CatOS, use el **comando show mac** para el módulo y el puerto o el módulo completo para ver las tramas out-discards:

```
MAC      Dely-Exced MTU-Exced  In-Discard Out-Discard
-------- ---------- ---------- ---------- -----------
2/1              0          -          0    10175888 2/2 0 - 0 9471889 2/3 0 - 0 9095371 2/4 0 -
0 8918785 !--- The show mac command run on mod 2 at different intervals shows !--- the out-
discard counter incrementing.
```

Para Cisco IOS, use el comando show interfaces counters error.

```
Router#sho interfaces counters error Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
OutDiscards Fa7/47 0 0 0 0 0 0 Fa7/48 0 0 0 0 0 2871800 Fa8/1 0 0 0 0 0 2874203 Fa8/2 103 0 0
103 0 2878032 Fa8/3 147 0 0 185 0 0 Fa8/4 100 0 0 141 0 2876405 Fa8/5 0 0 0 0 0 2873671 Fa8/6 0
0 0 0 0 2 Fa8/7 0 0 0 0 0 0 !--- The show interfaces counters errors command shows certain
```

```
interfaces !--- incrementing large amounts of OutDiscards while others run clean.
```

Investigue las siguientes causas comunes de errores en el buffer de salida:

Velocidad o Dúplex Inferior para la Cantidad de Tráfico

Su red puede enviar demasiados paquetes a través de este puerto para que este pueda manejarlos con el ajuste de velocidad o dúplex actual. Esto podría ocurrir cuando varios puertos de alta velocidad desembocan en un solo puerto (generalmente más lento). Puede desplazar el dispositivo que está bloqueado en este puerto a un medio más rápido. Por ejemplo, si el puerto es de 10 Mbps, desplace este dispositivo a un puerto de 100 Mbps o un puerto Gigabit. Puede cambiar la topología para rutear las tramas de forma diferente.

Problemas de Congestión: Segmento Demasiado Ocupado

Si se comparte el segmento, los otros dispositivos en este segmento pueden transmitir tanto que el switch no tiene ninguna oportunidad de transmitir. Evitar los hubs de Daisy Chain siempre que sea posible. La congestión puede provocar la pérdida de paquetes. La pérdida de paquetes causa retransmisiones en la capa de transporte, lo que a su vez hace que los usuarios experimenten el tiempo de espera en el nivel de la aplicación. Puede actualizar los links de 10 Mbps a links de 100Mbps o Gigabit Ethernet cuando sea posible. Puede quitar algunos dispositivos de los segmentos saturados a otros segmentos menos poblados. Haga que la prevención de la congestión sea una prioridad en su red.

Aplicaciones

A veces, las características de transmisión del tráfico de las aplicaciones usadas pueden causar problemas de buffer de salida. Las transferencias de archivo NFS que provienen de un servidor Gigabit conectado que utiliza el user datagram protocol (UDP) con un tamaño de la venta de 32 K son un ejemplo de ajuste de aplicación que podría generar este tipo Si ha verificado o intentado las otras sugerencias de este documento (velocidad/dúplex verificado, sin errores físicos en el link, todo el tráfico es tráfico válido normal, etc.), reducir el tamaño de la unidad enviado por la aplicación puede ayudar a solucionar este problema.

Problemas del Software

Si detecta un comportamiento que solo puede considerarse "extraño", puede aislar el comportamiento a un equipo específico, y ha considerado todo lo sugerido hasta ahora, esto puede indicar problemas de software o hardware. Generalmente es más fácil actualizar el software que actualizar el hardware. Primero, cambie el software.

Para CatOS, use el comando show version para verificar la versión actual de software y la memoria Flash libre para la actualización.

```
Switch> (enable) sh ver WS-C6006 Software, Version NmpSW: 6.3(3) Copyright (c) 1995-2001 by
Cisco Systems NMP S/W compiled on Oct 29 2001, 16:50:33 System Bootstrap Version: 5.3(1)
Hardware Version: 2.0 Model: WS-C6006 Serial #: TBA04251336 PS1 Module: WS-CAC-1300W Serial #:
SON04201377 PS2 Module: WS-CAC-1300W Serial #: SON04201383 Mod Port Model Serial # Versions ---
---- ------------------ ----------- ----------------------------------- 1 2 WS-X6K-SUP1A-2GE
SAD041901PP Hw : 3.6 Fw : 5.3(1) Fw1: 5.4(2) Sw : 6.3(3) Sw1: 6.3(3) WS-F6K-PFC SAD041803S3 Hw :
2.0 !--- Output truncated. DRAM FLASH NVRAM Module Total Used Free Total Used Free Total Used
Free ------ ------- ------- ------- ------- ------- ------- ----- ----- ----- 1 65408K 47274K
18134K 16384K 14009K 2375K 512K 308K 204K !--- Typical CatOS show version output. !--- Verify
free memory before upgrading. Uptime is 32 days, 4 hours, 44 minutes Console> (enable)
```

Para Cisco IOS, use el comando show version para verificar la versión actual de software junto

con **dir flash**: o el comando **dir bootflash**: (según la plataforma) para verificar la memoria Flash disponible para la actualización:

```
Router#sh ver Cisco Internetwork Operating System Software IOS (tm) Catalyst 4000 L3 Switch
Software (cat4000-IS-M), Version 12.1(13)EW, EA RLY DEPLOYMENT RELEASE SOFTWARE (fc1) TAC
Support: http://www.cisco.com/tac Copyright (c) 1986-2002 by cisco Systems, Inc. Compiled Fri
20-Dec-02 13:52 by eaarmas Image text-base: 0x00000000, data-base: 0x00E638AC ROM: 12.1(12r)EW
Dagobah Revision 71, Swamp Revision 24 trunk-4500 uptime is 2 weeks, 2 days, 6 hours, 27 minutes
System returned to ROM by redundancy reset System image file is "bootflash:cat4000-is-mz.121-
13.EW.bin" !--- Typical Cisco IOS show version output. Router#dir bootflash: Directory of
bootflash:/ 1 -rw- 8620144 Mar 22 2002 08:26:21 cat4000-is-mz.121-13.EW.bin 61341696 bytes total
(52721424 bytes free) !--- Verify available flash memory on switch running Cisco IOS. Router
```

Cómo Actualizar el Software

Para obtener información sobre la actualización de software para los switches de Catalyst, elija su plataforma en Switches LAN & ATM y consulte la sección Configuración de Software > Actualización de Software y Trabajar con Archivos de Configuración.

Incompatibilidad de Hardware y Software

En determinadas situaciones, el software no es compatible con el hardware. Esto ocurre cuando sale nuevo hardware que requiere un software especial de apoyo. Para obtener más información sobre la compatibilidad del software, use la herramienta Software Advisor.

Bugs de software

El sistema operativo puede tener un error. Si carga una versión de software más nueva, puede solucionar este error. Puede buscar errores de software conocidos con la Herramienta para Errores de Software.

Imágenes Dañadas

Las imágenes pueden dañarse o perderse. Para obtener información con respecto a la recuperación de las imágenes dañadas, elija su plataforma en Switches LAN y ATM y consulte la sección Troubleshooting > Recuperación de Imagen de Software Perdida o Dañada

Problemas de Hardware

Compruebe los resultados de show module para los switches Catalyst series 6000 y 4000 que ejecutan CatOS o Cisco IOS.

```
Switch> (enable) sh mod Mod Slot Ports Module-Type Model Sub Status --- ---- ----- -------------
------------ ------------------ ----------- 1 1 2 1000BaseX Supervisor WS-X6K-S2U-MSFC2 yes ok
15 1 1 Multilayer Switch Feature WS-F6K-MSFC2 no ok 3 3 8 1000BaseX Ethernet WS-X6408A-GBIC no
faulty 5 5 48 10/100BaseTX Ethernet WS-X6348-RJ-45 no faulty !--- Status of "faulty" indicates a
possible hardware problem. !--- This could be a line card problem, but since two mods are
effected, !--- perhaps there's a problem with the supervisor. !--- Use the reset command (CatOS)
or hw-module{mod}reset command (Cisco IOS), !--- or try physically reseating the modules and the
supervisor. !--- Also, try moving the supervisor to slot 2.
```

Compruebe los resultados de POST del switch para ver si se indicaron fallas para cualquier parte del switch. Las fallas de cualquier prueba de un módulo o puerto muestran una "F" en los resultados de la prueba.

Para CatOS, use el comando show test para ver todos los resultados de la prueba. Para ver los resultados de la prueba por módulo, use el comando **show test** {Mod}:

```
Switch> (enable) sh test 3 Diagnostic mode: complete (mode at next reset: minimal) !--- The
diaglevel is set to complete which is a longer but more thorough test. !--- The command to do
this for CatOS is set test diaglevel complete. Module 3 : 16-port 1000BaseX EthernetLine Card
Status for Module 3 : PASS Port Status : Ports 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ----------
---------------------------------------- . . . . . GBIC Status : Ports
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ---------------------------------------------------- . .
. . . N . . . . . N N Line Card Diag Status for Module 3 (. = Pass, F = Fail, N = N/A)
Loopback Status [Reported by Module 1] : Ports 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ----------
---------------------------------------- F F F F F F F F F F F F F F F F !--- The failed
loopback tests mean the ports are currently unusable. !--- Use the reset {mod} command or, if
necessary, physically reseat the !--- module to try and fix this problem. !--- If these steps
fail, open a case with Cisco Technical Support.
```

Para Cisco IOS, en los switches modulares como Cat6000 y 4000, use el comando show diagnostics. Para ver los resultados POST por módulo, use el comando [show diagnostics module *{mod}*](#) .

```
ecsj-6506-d2#sh diagnostic module 3 Current Online Diagnostic Level = Minimal !--- The
diagnostic level is set to minimal which is a shorter, !--- but also less thorough test result.
!--- You may wish to configure diagnostic level complete to get more test results. Online
Diagnostic Result for Module 3 : MINOR ERROR Online Diagnostic Level when Line Card came up =
Minimal Test Results: (. = Pass, F = Fail, U = Unknown) 1 . TestLoopback : Port 1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 ----------------------------------------------
-------------------------- . . . . . F F F F F F !--- Notice the
MINOR ERROR test result and failed loopback test which means !--- these ports are currently
unusable. !--- Use the hw-module{mod}reset command or, if necessary, physically reseat the !---
module to try and fix this problem. !--- If these steps fail, open a case with Cisco Technical
Support.
```

Nota: Para switches Catalyst Series 3750, 3550, 2970, 2950/2955, y 2900/3500XL use el **comando show post**, que indica simplemente éxito o error simple para el estado hw. Use los LED en estos switches para que pueda comprender los resultados POST. Consulte Comprensión de los Resultados Post.

Para obtener más información sobre cómo resolver problemas de hardware en los switches Catalyst que ejecutan CatOS y Cisco IOS, visite las páginas de soporte Switches LAN y ATM , elija su plataforma y consulte la sección **Troubleshooting > Hardware** .

Para obtener información sobre posibles problemas relacionados con avisos importantes, consulte Avisos Importantes para Switches LAN y ATM.

Errores de Entrada en una Interfaz Capa 3 Conectada con un Switchport Capa 2

De forma predeterminada, todos los puertos capa 2 se encuentran en el modo deseable dinámico, por lo que el puerto capa 2 intenta formar un link de trunk y envía paquetes al dispositivo remoto. Cuando una interfaz de capa 3 está conectada con un switchport de capa 2, no puede interpretar estas tramas, que da lugar a errores de Entrada, errores WrongEncap, y descartes de la cola de Entrada.

Para resolver esto, cambie el modo del puerto del switch a acceso estático o trunk según su requisito.

```
Switch2(config)#int fa1/0/12
Switch2(config-if)#switchport mode access
```

o

```
Switch2(config)#int fa1/0/12
Switch2(config-if)#switchport trunk encapsulation dot1q Switch2(config-if)#switchport mode trunk
```

Incrementar Rápidamente el Contador Rx-No-Pkt-Buff y los Errores de Entrada

El contador Rx-No-Pkt-Buff puede incrementarse en los puertos cuando tiene conectores, como WS-X4448-GB-RJ45, WS-X4548-GB-RJ45, y WS-X4548-GB-RJ45V. También un cierto aumento de descarte de paquetes es normal y es el resultado de la ráfaga de tráfico.

Estos tipos de errores aumentan rápidamente, especialmente cuando el tráfico que pasa a través de ese link es alto o cuando tiene dispositivos tales como servidores conectados con esa interfaz. Esta carga alta de tráfico suscribe puertos en exceso, que agota los buffers de entrada y hace que el contador Rx-No-Pkt-Buff y los errores de entrada aumenten rápidamente.

Si un paquete no puede ser recibido totalmente porque el switch está fuera de los buffers del paquete, este contador se incrementa una vez para cada paquete descartado. Este contador indica el estado interno de los ASIC de Switching en Supervisor y no indica necesariamente una condición de error.

Tramas de Pausa

Cuando la cola Rx FIFO (primero en entrar, primero en salir) de la parte de recepción (Rx) del puerto está llena, la parte de transmisión (Tx) del puerto comienza a generar traumas de pausa con un valor de intervalo mencionado en ella. Se espera que el dispositivo remoto detenga/reduzca la transmisión de paquetes para el intervalo mencionado en la trama de pausa.

Si el Rx puede borrar la cola Rx o alcanzar la marca de agua baja dentro de este intervalo, el Tx envía una trama de pausa especial que menciona el intervalo como cero (0x0). Esto habilita el dispositivo remoto para comenzar a transmitir los paquetes.

Si el Rx todavía funciona en la cola, una vez que expira el intervalo, el Tx envía una nueva trama de pausa otra vez con un nuevo valor del intervalo.

Si Rx-No-Pkt-Buff es cero o no se incrementa y se incrementa el contador TxPauseFrames, indica que nuestro switch genera tramas de pausa y el extremo remoto obedece, por lo tanto, la cola Rx FIFO se agota.

Si Rx-No-Pkt-Buff aumenta y TxPauseFrames también aumenta, significa que el extremo remoto no tiene en cuenta las tramas de pausa (no soporta el control de flujo) y continúa enviando tráfico a pesar de las tramas de pausa. Para solucionar esta situación, configure manualmente la velocidad y dúplex, e inhabilite el control de flujo, si es necesario.

Estos tipos de errores en la interfaz se relacionan con un problema de tráfico con los puertos con un exceso de suscriptores. Los módulos de switching The WS-X4448-GB-RJ45, WS-X4548-GB-RJ45, y WS-X4548-GB-RJ45V tienen 48 puertos con suscriptores en exceso en seis grupos de ocho puertos:

- Puertos 1, 2,3, 4, 5, 6, 7, 8
- Puertos 9, 10, 11, 12, 13, 14, 15, 16
- Puertos 17, 18, 19, 20, 21, 22, 23, 24
- Puertos 25, 26, 27, 28, 29, 30, 31, 32
- Puertos 33, 34, 35, 36, 37, 38, 39, 40
- Puertos 41, 42, 43, 44, 45, 46, 47, 48

Los ocho puertos dentro de cada grupo usan un circuito común que divide de forma eficaz el grupo en una sola conexión Gigabit Ethernet no bloqueadora, de dúplex completo a un entramado

interno de switches. Para cada grupo de ocho puertos, las tramas recibidas son guardadas en buffer y se envían al link común Gigabit Ethernet, al entramado interno de switches. Si la cantidad de datos recibidos para un puerto comienza a exceder la capacidad del buffer, el control de flujo envía las tramas de pausa al puerto remoto para detener el tráfico temporalmente y evitar la pérdida de tramas.

Si las tramas recibidas en cualquier grupo exceden el ancho de banda de 1 Gbps, el dispositivo comienza a descartar las tramas. Estos descartes no son evidentes ya que se producen en el intervalo ASIC y no en las interfaces reales. Esto puede reducir la producción de paquetes a través del dispositivo.

El Rx-No-Pkt-Buff no depende de la velocidad del tráfico total. Depende de la cantidad de paquetes que se almacenan en el buffer Rx FIFO del módulo ASIC. El tamaño de este buffer es solamente 16 KB. Se cuentan con flujos breves de ráfagas de tráfico cuando algunos paquetes llenan este buffer. Así, Rx-No-Pkt-Buff en cada puerto puede contarse cuando la velocidad de tráfico total de este grupo de puerto ASIC excede 1 Gbps, ya que WS-X4548-GB-RJ45 es un módulo con suscriptores en exceso 8:1.

Cuando tiene dispositivos que necesiten trasladar una gran cantidad de tráfico a través de esa interfaz, considere el uso de un puerto de cada grupo para que el circuito común que comparte un solo grupo no se vea afectado por la cantidad de tráfico. Cuando el módulo de switching Gigabit Ethernet no se utiliza completamente, puede conectar las conexiones de puerto de equilibrio en los grupos de puerto para optimizar la banda ancha disponible. Por ejemplo, con el módulo de switching WS-X4448-GB-RJ45 10/100/1000, puede conectar puertos de diferentes grupos, como los puertos 4, 12, 20, o 30 (en cualquier orden), antes de conectar los puertos del mismo grupo, como los puertos 1, 2, 3, 4, 5, 6, 7, y 8.

Si esto no soluciona el problema, debe considerar un módulo sin ninguna suscripción en exceso de los puertos.

Comprender los Descartes de Protocolo Desconocido

Los descartes de protocolo desconocido son un contador en la interfaz. Son causados por protocolos que no comprende el router/switch.

Este ejemplo del comando show running-config interface muestra los descartes del protocolo desconocido en la interfaz Gigabit Ethernet 0/1.

```
Switch#sh run int Gig 0/1 GigabitEthernet0/1 is up, line protocol is up Hardware is BCM1125
Internal MAC, address is 0000.0000.0000 (via 0000.0000) MTU 1500 bytes, BW 1000000 Kbit/sec, DLY
10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation 802.1Q Virtual LAN, Vlan
ID 1., loopback not set Keepalive set (10 sec) Full-duplex, 1000Mb/s, media type is RJ45 output
flow-control is XON, input flow-control is XON ARP type: ARPA, ARP Timeout 04:00:00 Last input
00:00:05, output 00:00:03, output hang never Last clearing of "show interface" counters 16:47:42
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo
Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate
0 bits/sec, 0 packets/sec 3031 packets input, 488320 bytes, 0 no buffer Received 3023
broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 63107 multicast, 0 pause input 0 input packets with dribble condition detected 7062
packets output, 756368 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets 2015
unknown protocol drops 4762 unknown protocol drops 0 babbles, 0 late collision, 0 deferred 0
lost carrier, 0 no carrier, 0 pause output 0 output buffer failures, 0 output buffers swapped
out
```

Los descartes del protocolo desconocido se caen normalmente porque la interfaz donde se reciben estos paquetes no se configura para este tipo de protocolo, o puede ser cualquier

protocolo que el router no reconozca.

Por ejemplo, si conecta hace dos routers e inhabilita el CDP en una interfaz del router, se producen descartes del protocolo desconocido en esa interfaz. Los paquetes CDP ya no se reconocen, y se descartan.

Trunking entre un switch y un router

Los links de trunk entre un switch y un router pueden hacer que el switchport quede desactivado. El trunk puede activarse después de que usted inhabilita y habilita el switchport pero, finalmente, el switchport puede desactivarse nuevamente.

Complete estos pasos para resolver el problema:

1. Asegúrese de que Cisco Discovery Protocol (CDP) se ejecute entre el switch y el router y que ambos pueda verse.
2. Inhabilite **Keepalives** en la interfaz del router.
3. Configure de nuevo la encapsulación en ambos dispositivos.

Cuando se inhabilita keepalives, el CDP habilita el link para que funcione normalmente.

Problemas de Conectividad debido a la Suscripción en Exceso

Cuando utiliza los módulos WS-X6548-GE-TX o WS-X6148-GE-TX, existe la posibilidad de que la utilización del puerto individual genere problemas de conectividad o pérdida de paquetes en las interfaces que los rodean. Consulte Problemas de Conectividad de Módulo/Interfaz para obtener más información sobre la suscripción en exceso.

Subinterfaces en los módulos SPA

En los módulos SPA, después de que cree una subinterface con 802.1Q, la mismo VLAN ya no puede usarse en el switch. Una vez que tiene dot1q de encapsulación en una subinterface, ya no puede utilizar más esa VLAN en el sistema porque las versiones 6500 o 7600 asignan internamente la VLAN y hacen que esa subinterfaz sea el único miembro.

Para resolver este problema, crees puertos trunk en vez de las subinterfaces. De esa manera, la VLAN se puede considerar en todas las interfaces.

Troubleshooting rxTotalDrops

Si todos los otros contadores son cero, y el único contador de error que informa errores es rxTotalDrops, la causa más probable es que el Spanning Tree bloquea una o más VLAN en el puerto uplink, por lo que se descarta la Lógica de Boqueo de Color CBL).

```
6509> (enable) show counters 1/2
64 bit counters
0  rxHCTotalPkts                    =         32513986812
1  txHCTotalPkts                    =         29657802587
2  rxHCUnicastPkts                  =         18033363526
3  txHCUnicastPkts                  =         29498347453
4  rxHCMulticastPkts                =         13469995420
5  txHCMulticastPkts                =            21719352
6  rxHCBroadcastPkts                =           757199011
```

```
7  txHCBroadcastPkts                 =           137735782
8  rxHCOctets                        =       25149393527621
9  txHCOctets                        =       23336028193116
10 rxTxHCPkts64Octets                =              387871
11 rxTxHCPkts65to127Octets           =          13704213656
12 rxTxHCPkts128to255Octets          =          16915931224
13 rxTxHCPkts256to511Octets          =           1068961475
14 rxTxHCpkts512to1023Octets         =           1945427146
15 rxTxHCpkts1024to1518Octets        =          11340361825
16 txHCTrunkFrames                   =          29657506751
17 rxHCTrunkFrames                   =          32513986812
18 rxHCDropEvents                    =                    0

32 bit counters
0  rxCRCAlignErrors                  =          0
1  rxUndersizedPkts                  =          0
2  rxOversizedPkts                   =          0
3  rxFragmentPkts                    =          0
4  rxJabbers                         =          0
5  txCollisions                      =          0
6  ifInErrors                        =          0
7  ifOutErrors                       =          0
8  ifInDiscards                      =          0
9  ifInUnknownProtos                 =          0
10 ifOutDiscards                     =         98
11 txDelayExceededDiscards           =          0
12 txCRC                             =          0
13 linkChange                        =          1
14 wrongEncapFrames                  =          0
0  dot3StatsAlignmentErrors          =          0
1  dot3StatsFCSErrors                =          0
2  dot3StatsSingleColFrames          =          0
3  dot3StatsMultiColFrames           =          0
4  dot3StatsSQETestErrors            =          0
5  dot3StatsDeferredTransmisions     =          0
6  dot3StatsLateCollisions           =          0
7  dot3StatsExcessiveCollisions      =          0
8  dot3StatsInternalMacTransmitErrors =         0
9  dot3StatsCarrierSenseErrors       =          0
10 dot3StatsFrameTooLongs            =          0
11 dot3StatsInternalMacReceiveErrors  =         0
12 dot3StatsSymbolErrors             =          0
0  txPause                           =          0
1  rxPause                           =          0
0 rxTotalDrops = 253428855 1 rxFIFOFull = 0 2 rxBadCode = 0 Last-Time-Cleared ------------------
-------- Sat Oct 27 2007, 08:24:35 6509> (enable)
```

Cuando el puerto bloquea las VLAN en un lado, pero el lado remoto se reenvía a esas VLAN, la interfaz incrementa los contadores rxTotalDrops.

Compare las VLAN permitidas en el trunk en ambos lados del link. También verifique al estado del spanning tree para las VLAN permitidas en ambos lados. Las BPDU todavía se envían en VLAN configuradas activamente, por lo que el switch A envía BPDU en todos los puertos de envío configurados, pero el switch B los descarta porque no tiene esas VLAN configuradas. En otras palabras, el switch B obtiene los paquetes para las VLAN para las que no está configurado, por lo que simplemente los descarta. Estos no son errores reales sino un simple error de configuración.

los ifOutDiscards ocurren generalmente cuando el buffer del transmitir (tx) consigue por completo (quizá debido al oversubscription) y después comienza a caer los paquetes.

Caídas de resultados del Troubleshooting

Típicamente, las caídas de resultados ocurrirán si se configura QoS y no está proporcionando al suficiente ancho de banda a cierta clase de paquetes. También ocurre cuando estamos golpeando el oversubscription.

Por ejemplo, aquí usted ve una gran cantidad de caídas de resultados en el gigabitethernet 8/9 de la interfaz en un Catalyst 6500 Series Switch:

```
Switch#show interface GigabitEthernet8/9 GigabitEthernet8/9 is up, line protocol is up
(connected) Hardware is C6k 1000Mb 802.3, address is 0013.8051.5950 (bia 0013.8051.5950)
Description: Connection To Bedok_Core_R1 Ge0/1 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 18/255, rxload 23/255 Encapsulation ARPA, loopback not set Keepalive
set (10 sec) Full-duplex, 1000Mb/s, media type is SX input flow-control is off, output flow-
control is off Clock mode is auto ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:28,
output 00:00:10, output hang never Last clearing of "show interface" counters never Input queue:
0/2000/3/0 (size/max/drops/flushes); Total output drops: 95523364 Queueing strategy: fifo Output
queue: 0/40 (size/max) 5 minute input rate 94024000 bits/sec, 25386 packets/sec 5 minute output
rate 71532000 bits/sec, 24672 packets/sec 781388046974 packets input, 406568909591669 bytes, 0
no buffer Received 274483017 broadcasts (257355557 multicasts) 0 runts, 0 giants, 0 throttles 3
input errors, 2 CRC, 0 frame, 0 overrun, 0 ignored 0 watchdog, 0 multicast, 0 pause input 0
input packets with dribble condition detected 749074165531 packets output, 324748855514195
bytes, 0 underruns 0 output errors, 0 collisions, 3 interface resets 0 babbles, 0 late
collision, 0 deferred 0 lost carrier, 0 no carrier, 0 PAUSE output 0 output buffer failures, 0
output buffers swapped out
```

Para analizar el problema, recoja la salida de estos comandos:

- muestre el det de la utilización de estructura
- muestre los errores de entramado
- muestre la capacidad del hardware de plataforma
- mostrar el medidor de tráfico de Catalyst6000
- muestre el descenso de la reescritura de motor de la capacidad del hardware de plataforma

Last Input Never de la Salida del Comando Show interface

Este ejemplo del comando show interface muestra el **Last input never** en la interfaz TenGigabitEthernet1/15.

```
Switch#show interface TenGigabitEthernet1/15 TenGigabitEthernet1/15 is up, line protocol is up
(connected) Hardware is C6k 10000Mb 802.3, address is 0025.84f0.ab16 (bia 0025.84f0.ab16)
Description: lsnbuprod1 solaris MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability
255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Full-duplex, 10Gb/s input flow-control is off, output flow-control is off ARP type: ARPA, ARP
Timeout 04:00:00 Last input never, output 00:00:17, output hang never Last clearing of "show
interface" counters 2d22h Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops:
0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0
packets/sec 5 minute output rate 46000 bits/sec, 32 packets/sec 52499121 packets input,
3402971275 bytes, 0 no buffer Received 919 broadcasts (0 multicasts) 0 runts, 0 giants, 0
throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 watchdog, 0 multicast, 0 pause
input 0 input packets with dribble condition detected 118762062 packets output, 172364893339
bytes, 0 underruns 0 output errors, 0 collisions, 3 interface resets 0 babbles, 0 late
collision, 0 deferred 0 lost carrier, 0 no carrier, 0 PAUSE output 0 output buffer failures, 0
output buffers swapped out
```

Esto muestra el número de horas, minutos, y segundos desde que el paquete más reciente fue recibido con éxito por una interfaz y procesado localmente en el router. Esta información es útil cuando una interfaz inactiva ha fallado. Se espera que este contador se actualice solo cuando los paquetes se conmuten por porceso, no cuando los paquetes se conmuten rápidamente.

Last input never significa que no hubo una transferencia de paquetes de interfaz exitosa a otro

punto final o terminal. Esto significa generalmente que no hubo transferencia de paquetes en relación con esa entidad.

Información Relacionada

- Troubleshooting de Problemas de Compatibilidad entre Cisco Catalyst Switches y NIC
- Utilización de Portfast y Otros Comandos para Solucionar Demoras al Iniciar la Conectividad de la Estación de Trabajo
- Configuración y resolución de problemas de negociación automática de half/full duplex para Ethernet 10/100/1000 Mb
- Recuperación del Estado de Puerto errDisable en las Plataformas CatOS
- Actualización de Imágenes de Software y Manejo de Archivos de Configuración en Switches de Catalyst
- Recuperación de Switches Catalyst Ejecutando CatOS a partir de Fallas de Iniciación
- Recuperación de Imagen de Software Perdida o Dañada en Cisco Catalyst 2900XL y 3500XL Series Switches
- Soporte Técnico y Documentación - Cisco Systems