Mensajes de Error Comunes de CatOS en los Catalyst 4500/4000 Series Switches

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Mensajes de error en switches de Catalyst serie 4500/4000
%C4K_HWPORTMAN-4-BLOCKEDTXQUEUE:Cola de transmisión bloqueada HwTxQId[dec]en [char], count=[dec]
%CDP-4-NVLANMISMATCH: Discrepancia de vlan nativa detectada en el puerto [DEC]/[DEC]
DTP-1-ILGLCFG: Illegal config (on, isl--on,dot1q) on port [mod/port]
%IP-3-UDP_SOCKOVFL: desbordamiento de zócalo UDP
%IP-3-UDP_BADCKSUM: suma de comprobación UDP defectuosa
%KERNEL-5-UNALIGNACCESS: Corrección del alineamiento realizada
%MCAST-4-RX_JNRANGE:IGMP: Se recibió informe dentro de los parámetros
MGMT-5-LOGIN_FAIL: El usuario no se registró desde la consola
%PAGP-5-PORTFROMSTP / %PAGP-5-PORTTOSTP
%SPANTREE-3-PORTDEL_FAILNOTFOUND
%SYS-3-P2_ERROR: Módulo 1/Desconocido
%SYS-3-P2_ERROR: 1/Se ha agotado el vbufs (búfers internos)
%SYS-3-P2_ERROR: El host xx:xx:xx:xx:xx:xx está inestable entre los puertos
%SYS-4-P2_WARN: Cola 1/bloqueada (tx) en el puerto [char]
%SYS-4-P2_WARN: 1/Filtro de dirección Ethernet MAC de valor cero
%SYS-4-P2_WARN: 1/Invalid crc, dropped packet, count = xx
%SYS-4-P2_WARN: 1/Tráfico no válido de la dirección de origen de multidifusión
%SYS-4-P2_WARN: 1/Astro(mod/puerto)
%SYS-4-P2_WARN: 1/Tag 0
convert_post_SAC_CiscoMIB:Nvram m block [#] unconvertible
Error de checksum global
Información Relacionada

Introducción

Este documento proporciona una breve explicación del registro del sistema común (syslog) y los mensajes de error que ve en los switches Cisco Catalyst 4500/4000 Series que ejecutan el software Catalyst OS (CatOS).

Si no encuentra los detalles de un mensaje de error específico en este documento, utilice la herramienta Error Message Decoder (sólo clientes registrados). Esta herramienta proporciona el significado de los mensajes de error que generan el software Cisco IOS® y el software CatOS.

Nota: El formato exacto del syslog y los mensajes de error que describe este documento puede variar. La variación depende de la versión de software que se ejecuta en el Supervisor Engine del switch.

Nota: Esta es la configuración de registro mínima recomendada en los Catalyst 4500/4000 Series Switches:

- Configure la fecha y la hora en el switch o configure el switch para que utilice el protocolo de tiempo de red (NTP) para obtener la fecha y la hora de un servidor NTP.**Nota:** Ejecute el comando **set time** para establecer la fecha y la hora en el switch.
- Asegúrese de que el registro y sellos de fecha/hora del registro estén habilitados, que es el valor predeterminado.
- Configure el switch para registrar un servidor de syslog, si es posible.

Los mensajes de error en este documento pueden ocurrir en los switches Catalyst 4500/4000 Series y en los derivados de estos switches, como los switches Catalyst 2948G, 2980G y 4912G.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no se limita a una versión específica de software o de hardware.

Convenciones

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

Mensajes de error en switches de Catalyst serie 4500/4000

%C4K_HWPORTMAN-4-BLOCKEDTXQUEUE:Cola de transmisión bloqueada HwTxQId[dec]en [char], count=[dec]

Problema

El switch genera `%C4K_HWPORTMAN-4-BLOCKEDTXQUEUE:cola de transmisión bloqueada HwTxQId[dec]on[char], count=[dec]` errores.

Descripción

Este mensaje de velocidad limitada indica que una cola de transmisión en un puerto está bloqueada por razones distintas a "en pausa". En otras palabras, el tráfico en ese puerto está siendo limitado y bloqueado. Verá los mensajes de la cola de transmisión bloqueada si Supervisor Engine no puede enviar paquetes a la tarjeta de línea debido a la recepción de un bit ocupado desde la tarjeta de línea. Un hardware defectuoso o una discordancia dúplex/velocidad pueden causar este problema. La solución alternativa es configurar ambos lados del link para la negociación automática para velocidad y dúplex. Ejecute el comando **shut/no shut** para recuperar el puerto. Si el problema persiste, mueva el dispositivo conectado a otro puerto y vea si el problema ocurre allí. Como medida final para desbloquear la cola de transmisión (Tx), ejecute el comando **hw-module reset** para reiniciar el switch o restablecer la tarjeta de línea.

%CDP-4-NVLANMISMATCH: Discrepancia de vlan nativa detectada en el puerto [DEC]/[DEC]

Problema

El switch genera frecuentes mensajes syslog `%CDP-4-NVLANMISMATCH`.

Descripción

Este ejemplo muestra el resultado de la consola que se ve cuando se produce este mensaje de error en el switch:

```
%CDP-4-NVLANMISMATCH:Native vlan mismatch detected on port 4/1
```

El switch genera este mensaje cada vez que el puerto del switch está conectado físicamente a otro switch o router. El switch genera este mensaje porque la VLAN nativa configurada en el puerto es diferente de la VLAN nativa configurada en el switch de conexión o en el puerto del router.

Un puerto trunk que configure con el etiquetado IEEE 802.1Q puede recibir tanto tráfico etiquetado como no etiquetado. De forma predeterminada, el switch reenvía el tráfico sin etiqueta con la VLAN nativa configurada para el puerto. Si un paquete tiene el mismo ID de VLAN que el ID de VLAN nativa del puerto de salida, el paquete se transmite sin etiqueta. Si los ID de VLAN no son iguales, el switch transmite el paquete con una etiqueta.

Asegúrese de que la VLAN nativa para un trunk 802.1Q sea la misma en ambos extremos del link trunk. Si la VLAN nativa en un extremo del trunk es diferente a la VLAN nativa del otro extremo, el tráfico de las VLAN nativas en ambos lados no se podrá transmitir correctamente en el trunk. Esta falla de transmisión correcta puede implicar algunos problemas de conectividad en su red.

Para verificar la VLAN nativa configurada en su switch, ejecute el comando **show trunk** *mod*/*port*. En este comando, *mod*/*port* es el puerto trunk. A continuación se muestra un ejemplo de salida del comando:

```
Console> (enable) show trunk 5/24

Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 5/24     desirable    dot1q          not-trunking  1

Port      Vlans allowed on trunk
```

```
--------  --------------------------------------------------------------------
 5/24     1-1005

Port      Vlans allowed and active in management domain
--------  --------------------------------------------------------------------
 5/24     1

Port      Vlans in spanning tree forwarding state and not pruned
--------  --------------------------------------------------------------------
 5/24

Console> (enable)
```

Para cambiar la VLAN nativa configurada en el puerto trunk, ejecute el comando **set vlan** ***vlan-id mod****/port* . En este comando, *mod*/*port* es el puerto trunk.

DTP-1-ILGLCFG: Illegal config (on, isl--on,dot1q) on port [mod/port]

Problema

El switch genera `DTP-1-ILGLCFG: Configuración ilegal (on, isl—on,dot1q) en los` errores de `puerto [mod/port].`

Descripción

Este mensaje puede surgir si ambos lados del tronco están activados, pero los tipos de encapsulación (isl, dot1q) no coinciden. Si los modos troncales se configuran en `deseable`, el tronco no se activa debido a esta configuración incorrecta. Para resolver problemas, verifique el resultado del comando **show trunk** en ambos extremos. Asegúrese de que los tipos de encapsulación sean idénticos.

%IP-3-UDP_SOCKOVFL: desbordamiento de zócalo UDP

Problema

El switch genera `%IP-3-UDP_SOCKOVFL:` mensajes syslog `de desbordamiento de socket UDP.`

Descripción

Este ejemplo muestra el resultado de la consola que se ve cuando ocurre este error:

Nota: El número de socket del protocolo de datagramas de usuario (UDP) que se muestra puede variar o ser siempre el mismo.

```
%IP-3-UDP_SOCKOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKOVFL:UDP socket 2353 overflow
```

El switch genera este mensaje syslog cuando el búfer que se asigna para los paquetes entrantes en el socket especificado (puerto de destino UDP) está lleno. El búfer está lleno porque la velocidad del tráfico destinado a ese socket es demasiado alta. Por ejemplo, esta condición puede ocurrir cuando una estación de administración de red envía un gran número de consultas

SNMP (del inglés Simple Network Management Protocol, protocolo simple de administración de red). Cuando se produce un desbordamiento UDP, intente reducir el número de consultas SNMP. Realice una de estas acciones:

- Aumente el intervalo de sondeo en la estación de administración de red.
- Reduzca el número de objetos MIB sondeados.

En el ejemplo de esta sección, el switch recibió un número excesivo de paquetes destinados a la dirección IP del switch (o la dirección de broadcast) con el socket UDP de destino 2353. Debido a que el búfer de entrada para este socket en el switch está lleno, el switch genera un mensaje syslog. Ejecute el comando **show netstat udp** para ver la cantidad de veces que el switch alcanzó la condición de desbordamiento.

Estos mensajes de syslog indican que una o más estaciones envían una gran cantidad de tráfico UDP en los puertos UDP de destino especificados al switch. Si el switch genera un número excesivo de estos mensajes, utilice un analizador de red para identificar el origen del tráfico y reducir la velocidad del tráfico. Consulte Ejemplo de Configuración de Catalyst Switched Port Analyzer (SPAN) para obtener más información.

Nota: No se preocupe por el contador `de puerto`. Este contador muestra el número de paquetes UDP que el switch recibió y que fueron destinados a puertos inexistentes.

%IP-3-UDP_BADCKSUM: suma de comprobación UDP defectuosa

Problema

El switch genera `%IP-3-UDP_SOCKOVFL:` mensajes syslog `de desbordamiento de socket UDP.`

Descripción

Este ejemplo muestra el resultado de la consola que se ve cuando ocurre este error:

Nota: El número de socket UDP que se muestra puede variar o ser consistentemente el mismo.

```
%IP-3-UDP_BADCKSUM:UDP bad checksum
```

El switch genera este mensaje de syslog cuando el switch detecta una suma de comprobación incorrecta en un datagrama UDP, como paquetes SNMP. El encabezado del datagrama UDP lleva una suma de comprobación que el dispositivo de red receptor verifica para determinar si el datagrama se dañó durante el tránsito. Si la suma de comprobación recibida no coincide con el valor de la suma de comprobación en el encabezado, el datagrama se descarta y se registra un mensaje de error. Ejecute el comando **show netstat udp** para ver la cantidad de veces que el switch detectó un datagrama de checksum erróneo.

```
6500-b (enable) show netstat udp

udp:
0 incomplete headers
0 bad data length fields
0 bad checksums
0 socket overflows
110483 no such ports
```

Este mensaje es sólo informativo. Un dispositivo de red que envía paquetes defectuosos al switch causa este mensaje. Utilice un analizador de red para identificar el origen del tráfico. Consulte Ejemplo de Configuración de Catalyst Switched Port Analyzer (SPAN) para obtener más información.

Nota: No se preocupe por el contador `de puerto`. Este contador muestra el número de paquetes UDP que el switch recibió y que fueron destinados a puertos inexistentes.

%KERNEL-5-UNALIGNACCESS: Corrección del alineamiento realizada

Problema

El switch genera `%KERNEL-5-UNALIGNACCESS:corrección de alineación realizada` mensajes syslog.

Descripción

Este ejemplo muestra el resultado de syslog que se ve cuando ocurre este error:

```
%KERNEL-5-UNALIGNACCESS:Alignment correction made at 0x80056B3C reading 0x81B82F36
```

Estos mensajes de syslog indican que la CPU del switch detectó y corrigió un error de alineación cuando el switch intentó acceder a los datos en la DRAM. Estos mensajes son sólo informativos. Los mensajes no indican un problema con el switch y no afectan el rendimiento del sistema.

En algunos casos, observa un número excesivo de estos mensajes. Por ejemplo, estos mensajes pueden inundar el archivo de registro del servidor syslog o la consola del switch. Si recibe un exceso de mensajes, considere actualizar el software del switch a la última versión de mantenimiento para su tren de versión de software. O ejecute el comando **set logging level kernel 4 default** para modificar el nivel de registro para la `función Kernel` a 4 o menos.

Si actualiza a la versión de mantenimiento más reciente pero aún recibe estos mensajes de syslog, cree una solicitud de servicio (sólo clientes registrados) con Soporte Técnico de Cisco.

%MCAST-4-RX_JNRANGE:IGMP: Se recibió informe dentro de los parámetros

Problema

Un switch que tiene activada la función de snooping del protocolo de administración de grupos de Internet (IGMP) muestra el mensaje `%MCAST-4-RX_JNRANGE:IGMP: Informe Rcvd en el` mensaje de error `01-00-5e-00-00-xx`.

Descripción

Este ejemplo muestra el resultado de syslog que se ve cuando ocurre este error:

```
%MCAST-4-RX_JNRANGE:IGMP: Rcvd Report in the range 01-00-5e-00-00-xx
```

El `Informe Rcvd en el` mensaje `de` syslog `de rango` es sólo informativo. El switch genera este mensaje cuando el switch recibe paquetes de informe IGMP con una dirección MAC multicast que comienza con 01-00-5e-00-00-*xx*. Este rango de direcciones de capa 2 (L2) es equivalente al

rango de direcciones de multidifusión de capa 3 (L3) entre 224.0.0.0 y 224.0.0.255. Estas direcciones están reservadas para el uso de protocolos de ruteo y otros protocolos de detección o mantenimiento de topología de bajo nivel. Algunos ejemplos de estos protocolos incluyen la detección de gateway y los informes de pertenencia a grupos.

Utilice una herramienta de captura de paquetes, como un rastreador, y filtre los mensajes IGMP para resolver este problema. Además, puede utilizar la función Catalyst SPAN para copiar paquetes de un puerto que sospeche recibe estos mensajes de un dispositivo de red. Para suprimir estos mensajes, ejecute el **comando set logging level mcast 2 default**. Este comando cambia el nivel de registro de los mensajes multicast a 2.

Utilice los puertos que muestra el comando **show multicast router** y cualquier enlace ascendente al núcleo de la red como los puertos de origen SPAN. Si estos puertos son puertos trunk, también configure el puerto de destino SPAN como puerto trunk. Ejecute el comando **show trunk** para verificar que los puertos sean puertos trunk.

MGMT-5-LOGIN_FAIL: El usuario no se registró desde la consola

Problema

El switch genera `MGMT-5-LOGIN_FAIL:El usuario no pudo iniciar sesión desde` los errores `de la consola`.

Descripción

Este mensaje puede indicar un problema con el servidor terminal que está conectado al puerto de consola del switch. Cuando la consola del switch está conectada a una línea asíncrona de un servidor terminal y usted realiza un reinicio suave en el switch, la basura (texto aleatorio) se transmite a través de la pantalla durante varios minutos. Si TACACS está habilitado en el switch, varios minutos pueden convertirse en varios días porque TACACS almacena y procesa la basura pieza por pieza. La solución temporal es ejecutar el comando **no exec** en la línea asíncrona a la que se conecta el switch.

Nota: Incluso después de ejecutar el comando **no exec**, los mensajes continúan hasta que el búfer está despejado.

Nota: Si recibe el mensaje de error `%MGMT-5-LOGIN_FAIL:El usuario no pudo iniciar sesión a través de Telnet - se ha alcanzado el intento máximo`, intente limitar el número de usuarios a los que se permite Telnet al switch.

%PAGP-5-PORTFROMSTP / %PAGP-5-PORTTOSTP

Problema

El switch genera frecuentes `%PAGP-5-PORTFROMSTP` y `%PAGP-5-PORTTOSTP` mensajes syslog.

Descripción

Este ejemplo muestra el resultado de la consola que se ve cuando el switch genera estos mensajes syslog:

```
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%PAGP-5-PORTTOSTP:Port 3/3 joined bridge port 3/3
```

La función de registro del protocolo de agregación de puertos (PAgP) informa de eventos que involucran a PAgP. Usted utiliza PAgP para negociar los links EtherChannel entre los switches. El switch genera el mensaje syslog `%PAGP-5-PORTFROMSTP` a la pérdida de un link en un puerto del switch. El switch genera el mensaje syslog `%PAGP-5-PORTTOSTP` cuando se detecta un link en un puerto del switch. Estos mensajes syslog son mensajes informativos normales que indican la adición o extracción de un puerto del árbol de expansión.

Nota: No es necesario habilitar la canalización para que aparezcan estos mensajes.

En el ejemplo de esta sección, el switch primero perdió el link en el puerto 3/3, que quitó el puerto del árbol de expansión. Luego, el switch nuevamente detectó el link en el puerto, que agregó el puerto nuevamente al árbol de expansión.

Si ve estos mensajes con frecuencia para un puerto determinado, el link está inestable, lo que significa que el link se pierde y se recupera constantemente. Investigue la causa. Las causas comunes de la inestabilidad de los links en un puerto del switch incluyen:

- Discordancia dúplex/velocidad
- Cable defectuoso
- Tarjeta de interfaz de la red (NIC) defectuosa u otro problema de estación extremo.
- Puerto de switch defectuoso
- Otro error de configuración

Si desea suprimir estos mensajes de syslog, ejecute el comando **set logging level pagp 4 default** para modificar el nivel de registro para el recurso PAgP a 4 o menos. El nivel de registro predeterminado para PAgP es 5.

%SPANTREE-3-PORTDEL_FAILNOTFOUND

Problema

El switch genera `%SPANTREE-3-PORTDEL_FAILNOTFOUND` periódicos mensajes de syslog.

Descripción

Este ejemplo muestra el resultado de syslog que se ve cuando ocurre este error:

```
%SPANTREE-3-PORTDEL_FAILNOTFOUND:9/5 in vlan 10 not found (PAgP_Group_Rx)
```

Estos mensajes del registro del sistema indican que el PAgP intentó eliminar un puerto del árbol de expansión de la VLAN especificada, pero el puerto no estaba en la estructura de datos del árbol de expansión de esa VLAN. Normalmente, otro proceso, como el protocolo de enlace troncal dinámico (DTP), ya ha eliminado el puerto del árbol de extensión.

Estos mensajes normalmente acompañan a los mensajes %PAGP-5-PORTFROMSTP. Los mensajes son para fines de depuración. Los mensajes no indican un problema con el switch y no afectan el rendimiento del switching. Además, estos mensajes no se registran a menos que haya cambiado la configuración de registro de la función `SPANTREE` predeterminada. El nivel de registro predeterminado para `SPANTREE` es 2.

En algunos casos, observa un número excesivo de estos mensajes. Por ejemplo, estos mensajes pueden inundar la consola del switch. Si recibe un exceso de mensajes, considere actualizar el software del switch a la última versión de mantenimiento para su tren de versión de software. Las versiones de software posteriores eliminan estos mensajes en la mayoría de los casos.

%SYS-3-P2_ERROR: Módulo 1/Desconocido

Problema

`%SYS-3-P2_ERROR:` Se muestra el mensaje de error `1/Unknown module` cuando se instala un nuevo módulo de conmutación en un Catalyst 4500/4000 Series Switch.

Descripción

Este ejemplo muestra el resultado de la consola que se ve cuando ocurre este error:

```
%SYS-3-P2_ERROR: 1/Unknown module (fru minor type 304) in slot 3
```

`%SYS-3-P2_ERROR: 1/El` error de `módulo desconocido` se produce cuando la versión de imagen de software que se ejecuta actualmente en Supervisor Engine no admite el componente de hardware que ha insertado.

En el ejemplo, se inserta un módulo de switching de servidor 1000BASE-X de 18 puertos (WS-X4418) en un switch Catalyst 4500/4000 que ejecuta la versión 4.4(1) del software CatOS. El módulo WS-X4418 requiere una versión de software mínima de 4.5(1).

La medida elusiva consiste en actualizar la versión de software Supervisor Engine con un release de software compatible con el hardware. Consulte Release Notes for Catalyst 4500 Series Switches para obtener una lista de las versiones mínimas de software para cada módulo.

%SYS-3-P2_ERROR: 1/Se ha agotado el vbufs (búfers internos)

Problema

El switch genera `%SYS-3-P2_ERROR: 1/Se han agotado los` mensajes `vbufs` cuando se encienden varios hosts a la vez o alrededor de ella.

Descripción

Este ejemplo muestra el resultado de la consola que se ve cuando se produce el error:

```
%SYS-3-P2_ERROR: 1/Have run out of vbufs(internal buffers)
```

`%SYS-3-P2_ERROR: 1/Se han agotado los` errores `de vbufs(buffers internos)` cuando se encienden varios hosts simultáneamente. Después de encender los hosts, los errores ya no aparecen.

Estos errores no causan ninguna interrupción en la capacidad de Catalyst para conmutar el tráfico. Los mensajes son sólo de carácter informativo.

%SYS-3-P2_ERROR: El host xx:xx:xx:xx:xx:xx está inestable entre los puertos

Problema

El switch genera `%SYS-3-P2_ERROR: El host xx:xx:xx:xx:xx:xx está parpadeando entre los puertos...` mensajes, donde *xx:xx:xx:xx:xx:xx* es una dirección MAC.

Descripción

Este ejemplo muestra el resultado de la consola que se ve cuando ocurre este error:

```
%SYS-4-P2_WARN: 1/Host 00:50:0f:20:08:00 is flapping between port 1/2 and port 4/39
```

Utilice los pasos y pautas de esta sección para comprender y resolver problemas de la causa de este mensaje de error.

El mensaje indica que su switch Catalyst 4500/4000 ha aprendido una dirección MAC que ya existe en la tabla de memoria direccionable por contenido (CAM), en un puerto distinto del original. Este comportamiento ocurre repetidamente durante periodos cortos de tiempo, lo que significa que hay inestabilidad de dirección entre los puertos.

Si el mensaje aparece para varias direcciones MAC, el comportamiento no es normal. Este comportamiento indica un posible problema de red porque las direcciones MAC se mueven rápidamente de un puerto a otro antes del tiempo de envejecimiento predeterminado. El problema puede ser el tráfico en bucle en la red. Los síntomas típicos incluyen:

- Utilización alta de la CPU
- Tráfico lento en toda la red
- Uso elevado de la placa de interconexiones en el switch

Para obtener información sobre cómo identificar y resolver problemas con el árbol de expansión, refiérase a Problemas del Spanning Tree Protocol y Consideraciones de Diseño Relacionadas.

Si el mensaje de error aparece para una o dos direcciones MAC, localice estas direcciones MAC para determinar la causa. Ejecute el comando **show cam *mac_addr*** para identificar de dónde se han aprendido estas direcciones MAC. En este comando, *mac_addr* es la dirección MAC que informa el error como inestable.

Después de determinar entre qué puertos está inestable esta dirección MAC, realice un seguimiento de la dirección MAC. Conéctese a los dispositivos intermedios entre su Catalyst 4500/4000 y el dispositivo que tiene la dirección MAC problemática. Realice esto hasta que pueda identificar el origen y cómo se conecta este dispositivo a la red.

Nota: Debido a que la dirección MAC está inestable entre dos puertos, realice un seguimiento de ambas trayectorias.

Este ejemplo muestra cómo realizar un seguimiento de las dos trayectorias desde las que se ha aprendido esta dirección MAC:

Nota: Suponga que ha recibido este mensaje y que ha comenzado a investigarlo.

```
%SYS-4-P2_WARN: 1/Host 00:50:0f:20:08:00 is flapping between port 1/2 and port 4/39
```

Para rastrear cómo se aprendió esta dirección MAC de ambos puertos, complete estos pasos:

1. Considere primero el puerto 1/2 y ejecute el comando **show cam dynamic 1/2**.Si ve la dirección MAC 00:50:0f:20:08:00 en la lista de direcciones MAC aprendidas en este puerto, determine si es un solo host que está conectado o si hay varios hosts registrados en ese puerto.
2. En base a si hay uno o varios hosts, investigue el dispositivo:Si hay un solo host (00:50:0f:20:08:00) conectado, verifique el otro puerto registrado y vea si el host está conectado de forma dual al switch.En este ejemplo, el otro puerto es el puerto 4/39.Si el host tiene conexiones con otros dispositivos que eventualmente pueden conducir a este switch, intente rastrear los dispositivos intermedios.Con los dispositivos Cisco, ejecute el comando **show cdp neighbors *mod/port* detail**. El resultado proporciona información sobre los dispositivos intermedios.A continuación se muestra un ejemplo de salida:

```
Cat4K> (enable) show cdp neighbors 1/2 detail

Port (Our Port): 1/2
Device-ID: brigitte
Device Addresses:
IP Address: 172.16.1.1
Novell address: aa.0
Holdtime: 171 sec
Capabilities: ROUTER
Version:
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 06-DEC-99 17:10 by phanguye
Platform: cisco 2500
Port-ID (Port on Neighbors's Device): Ethernet0
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: half
System Name: unknown
System Object ID: unknown
Management Addresses: unknown
Physical Location: unknown

Cat4K> (enable)
```

3. Establezca una sesión Telnet con el dispositivo y siga la trayectoria de la dirección MAC.En este ejemplo, la dirección IP es 172.16.1.1.Repita el procedimiento para todas las direcciones MAC que informa el mensaje de error como inestable.
4. Cree un diagrama simple del dispositivo de origen con esa dirección MAC y de las conexiones físicas (los puertos Catalyst 4500/4000) desde las que y a las que esta dirección MAC está inestable.El diagrama permite determinar si se trata de un puerto y una ruta válidos para el diseño de la red.Si verifica que ambos puertos en los que la dirección MAC está inestable proporcionan una trayectoria hacia ese nodo de red, existe la posibilidad de que tenga un problema de falla del árbol de expansión. Consulte Problemas del Spanning Tree Protocol y Consideraciones de Diseño Relacionadas para aislar y resolver este loop.En las redes grandes en las que varios hosts de varios proveedores están interconectados, surge la dificultad al intentar rastrear el host con sólo el uso de la dirección MAC. Utilice la utilidad de búsqueda para las asignaciones IEEE OUI y Company_id para rastrear estas direcciones MAC. Esta lista es la parte frontal de la base de datos donde IEEE ha registrado todas las direcciones MAC que se han asignado a todos los proveedores. Ingrese los primeros tres octetos de la dirección MAC en la **Búsqueda de:** para encontrar el proveedor asociado a este dispositivo. Los primeros tres octetos del ejemplo son 00:50:0f.

Estos son otros problemas que pueden hacer que aparezca este mensaje:

- **Problema de redundancia de NIC del servidor**: hay un servidor con una NIC de doble conexión que se comporta mal y no cumple con los estándares. El servidor utiliza la misma dirección MAC para ambos puertos que se conectan al mismo switch.
- **Desactivación del protocolo de router en espera en caliente (HSRP)**: si se desactiva HSRP, estos mensajes pueden aparecer en la consola de Supervisor Engine. Si observa que la implementación de HSRP en su red es inestable, consulte Comprensión y Troubleshooting de Problemas de HSRP en Redes de Switch Catalyst para resolver el problema.
- **Error de configuración de EtherChannel**: una conexión EtherChannel mal configurada también puede causar estos síntomas. Si los puertos que los informes de mensajes inestables son miembros del mismo grupo de canales, verifique su configuración de EtherChannel y consulte Comprensión del Balanceo de Carga y Redundancia de EtherChannel en Switches Catalyst para resolver problemas de configuración.
- **El host refleja los paquetes nuevamente en la red**: el reflejo de los paquetes nuevamente en la red por un host también puede causar inestabilidad. Normalmente, la causa raíz de esta reflexión de paquetes es una NIC dañada o cualquier falla de la interfaz física del host que está conectado al puerto.Si la reflexión de los paquetes por parte del host es su causa raíz, obtenga un rastro del rastreador y examine el tráfico que va hacia y desde los puertos en los que han aparecido los mensajes. Si un host refleja los paquetes, normalmente ve paquetes duplicados en el seguimiento. Los paquetes duplicados son un posible síntoma de esta inestabilidad de la dirección MAC.Consulte Configuración de SPAN y RSPAN para obtener detalles sobre cómo configurar un puerto para su uso con un sniffer.
- **Defecto de software o hardware**: si ha intentado solucionar el problema del mensaje inestable con las instrucciones de esta sección pero aún así ha notado el problema, solicite más asistencia del Soporte Técnico de Cisco. Asegúrese de mencionar y proporcionar la documentación de la información recopilada mientras sigue los pasos. Esta información hace que la resolución de problemas sea más rápida y eficaz.

%SYS-4-P2_WARN: Cola 1/bloqueada (tx) en el puerto [char]

Problema

El switch genera `cola bloqueada (tx) en los` mensajes del `puerto [char].`

Descripción

Este ejemplo muestra el resultado de syslog que se ve cuando ocurre el error:

```
%SYS-4-P2_WARN: 1/Blocked queue (tx) on port 3/3
%SYS-4-P2_WARN: 1/Blocked queue on gigaport 3, ( 8671 : 0)
```

Estos errores indican un problema de hardware o uno de estos problemas:

- Discordancia dúplex
- Cable defectuoso
- Cableado tipo 1
- Puertos defectuosos

- Problema de hardware de un dispositivo conectado externo

La causa más común de estos errores es un problema de capa física. El problema hace que una cantidad considerable de tráfico se respalde en los gigaports internos K1. Los circuitos integrados para aplicaciones específicas (ASIC) K1 son los chips principales que controlan el switch. Generalmente, el recuento de colas de transmisión bloqueadas aumenta debido a un problema de configuración o al cableado dañado.

En un entorno normal, la cola Tx sólo se puede bloquear durante aproximadamente 20 segundos. Un bloqueo más largo indica un problema significativo. Como resultado, el conteo de colas Tx bloqueadas aumenta si la cola Tx no se ha drenado para el gigaport en 35 segundos.

Si es necesario, comuníquese con Soporte Técnico de Cisco para determinar si el módulo necesita ser reemplazado. Pero primero, vuelva a colocar el módulo y vea si el mensaje de error aún existe.

Estos son los pasos para asignar la cola bloqueada Catalyst 4000/2948G/2980G en Gigaport <gigaport_number> a los puertos del switch del panel frontal, que deben reconstruirse.

Ejemplos de Mensajes de Error:

```
2000 Aug 25 12:22:48 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (331 : 0 )
2000 Aug 25 12:23:41 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (332 : 0 )
2000 Aug 25 12:25:42 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (333 : 0 )
2000 Aug 25 12:46:42 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (334 : 0 )
2000 Aug 25 12:48:41 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (335 : 0 )
2000 Aug 25 12:57:42 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (336 : 0 )
```

Este mensaje de error indica que hay un error de configuración que muy probablemente se deba a un problema de capa física o a una discordancia dúplex relacionada con el gigaport 29. Para encontrar qué puerto(s) se relacionan con el gigaport 29, vea estas tablas. Las tablas varían y dependen del Supervisor Engine.

Asignación de puertos WS-X4013 Gigabit Kirky

K1-A (puertos gigantes 0-11)

Gigaport 0	Uplink 0 (Puerto 1/1) o Interconexión interna K1-C
Gigaport 1	Ranura 6 - Interconexión Gigabit 5
Gigaport 2	Ranura 5 - Interconexión Gigabit 5
Gigaport 3	Ranura 2 - Interconexión Gigabit 5
Gigaport 4	Ranura 3 - Interconexión Gigabit 5
Gigaport 5	Ranura 4 - Interconexión Gigabit 5
Gigaport 6	Ranura 4 - Interconexión Gigabit 4
Gigaport 7	Ranura 3 - Interconexión Gigabit 4
Gigaport 8	Ranura 2 - Interconexión Gigabit 4
Gigaport 9	Ranura 5 - Interconexión Gigabit 4
Gigaport 10	Ranura 6 - Interconexión Gigabit 4
Gigaport 11	Interconexión interna K1-B

K1-B (puertos gigantes 12-23)

Gigaport 12	Interconexión interna K1-A
Gigaport 13	Ranura 6 - Interconexión Gigabit 3
Gigaport 14	Ranura 5 - Interconexión Gigabit 3
Gigaport 15	Ranura 2 - Interconexión Gigabit 3
Gigaport 16	Ranura 3 - Interconexión Gigabit 3
Gigaport 17	Ranura 4 - Interconexión Gigabit 3
Gigaport 18	Ranura 4 - Interconexión Gigabit 2
Gigaport 19	Ranura 3 - Interconexión Gigabit 2
Gigaport 20	Ranura 2 - Interconexión Gigabit 2
Gigaport 21	Ranura 5 - Interconexión Gigabit 2
Gigaport 22	Ranura 6 - Interconexión Gigabit 2
Gigaport 23	Interconexión interna K1-C

K1-C (puertos gigantes 24-35)

Gigaport 24	Interconexión interna a K1-B
Gigaport 25	Ranura 6 - Interconexión Gigabit 1
Gigaport 26	Ranura 5 - Interconexión Gigabit 1
Gigaport 27	Ranura 2 - Interconexión Gigabit 1
Gigaport 28	Ranura 3 - Interconexión Gigabit 1
Gigaport 29	Ranura 4 - Interconexión Gigabit 1
Gigaport 30	Ranura 4 - Interconexión Gigabit 0
Gigaport 31	Ranura 3 - Interconexión Gigabit 0
Gigaport 32	Ranura 2 - Interconexión Gigabit 0
Gigaport 33	Ranura 5 - Interconexión Gigabit 0
Gigaport 34	Ranura 6 - Interconexión Gigabit 0
Gigaport 35	Enlace ascendente 1 (puerto 1/2) o interconexión interna a K1-A

Cada ASIC K1 tiene interconexiones de 12 gigabits. Estas interconexiones gigabit se utilizan entre las tarjetas de línea y el Supervisor Engine como links seriales punto a punto. Cada tarjeta de línea del Catalyst 4000 se conecta a 6 de las interconexiones de 12 gigabits. Se hace referencia a las interconexiones gigabit de 0 a 5 y se conectan en orden inverso. Por ejemplo, en una tarjeta de línea 4148, la interconexión gigabit 5 se conecta a los puertos 1-8, la interconexión gigabit 4 se

conecta a los puertos 9-16.

Asignación de puerto de interconexión de módulo de línea

WS-X4148-RJ, WS-X4148-RJ45V, WS-X4148-RJ21

Puertos	Interconexión Gigabit
1-8	5
9-16	4
17-24	3
25-32	2
33-40	1
41-48	0

WS-X4232-RJ-32, WS-X4232-L3

Puertos	Interconexión Gigabit
1	5
2	4
3-10	3
11-18	2
19-26	1
27-34	0

WS-X4418-GB

Puertos	Interconexión Gigabit
1	5
2	4
3-6	3
7-10	2
11-14	1
15-18	0

WS-X4124-FX-MT

Puertos	Interconexión Gigabit
1-4	5
5-8	4
9-12	3
13-16	2
17-20	1
21-24	0

WS-X4306-GB

Puertos	Interconexión Gigabit
1	5
2	4
3	3
4	2
5	1
6	0

WS: X4412-2GB-TX

Puertos	Interconexión Gigabit
1-2	5
3-4	4
5-6	3
7-8	2
9-10	1
11-12	0

Ejemplo de búsqueda de puertos sospechosos

```
4006-2b1> en

Enter password:

4006-2b1> (enable) sh mod
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X4013            no  ok
2   2    48    10/100BaseTx Ethernet     WS-X4148            no  ok
3   3    34    Router Switch Card        WS-X4232-L3         no  ok
6   6    24    100BaseFX Ethernet        WS-X4124-FX-MT      no  ok

Mod Module-Name         Serial-Num
--- ------------------- --------------------
1                       JAB0438020C
2                       JAB0234036Q
3                       JAB041705GE
6                       JAB0410096R

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
1   00-01-96-62-cc-00 to 00-01-96-62-cf-ff 2.0    5.4(1)      5.5(6)
2   00-50-73-0a-30-e0 to 00-50-73-0a-31-0f 1.0
3   00-01-42-06-72-98 to 00-01-42-06-72-b9 1.0    12.0(7)W5( 12.0(7)W5(15d)
6   00-d0-06-01-68-30 to 00-d0-06-01-68-47 1.0

4006-2b1> (enable)

2000 Aug 25 12:48:41 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 16, (335 : 0 )
2000 Aug 25 12:57:42 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 16, (336 : 0 )
```

Gigaport 16 hace referencia a la ranura 3, gigabit interconnect 3. Dado que la ranura 3 es WS-X4232-L3, la interconexión gigabit 3 se refiere a los puertos 3-10. Cuando resuelva estos problemas de puertos, verifique si hay errores y/o discordancias dúplex que utilicen los comandos

show port, **show mac** y **show counters**. También puede ser útil obtener un **vaciado 1** y ver si hay errores de hardware asociados con los puertos. Una referencia notable en la salida dump 1 es el cscTimeout asociado con el ASIC del módulo de línea para la interconexión correspondiente. El valor de **cscTimeout** debe ser **0**

%SYS-4-P2_WARN: 1/Filtro de dirección Ethernet MAC de valor cero

Problema

El switch genera mensajes `de filtrado de dirección MAC Ethernet de valor cero.`

Descripción

Este ejemplo muestra el resultado de syslog que se ve cuando ocurre este error:

```
%SYS-4-P2_WARN: 1/Filtering Ethernet MAC address of value zero
                from agent host table interface
%SYS-4-P2_WARN: 1/Filtering Ethernet MAC address of value zero
                from agent host table interface
```

El switch genera el mensaje syslog `Filtering Ethernet MAC address of value zero` cuando el switch recibe paquetes con una dirección MAC de origen de 00-00-00-00-00-00. Esta dirección MAC es un MAC de origen no válido.

El mensaje de syslog indica que el switch se niega a aprender la dirección no válida. Sin embargo, el switch reenvía el tráfico que proviene de una dirección MAC de ceros.

La solución alternativa es intentar identificar la estación final que genera tramas con una dirección MAC de origen de ceros. Típicamente, uno de estos dispositivos transmite tales tramas:

- Un generador de tráfico, tal como Spirent SmartBits
- Tipos determinados de servidores, tales como servidores IBM WebSphere de balanceo de carga
- Un router mal configurado o una estación final, como un dispositivo que transmite broadcasts con todos ceros
- Un NIC defectuoso

%SYS-4-P2_WARN: 1/Invalid crc, dropped packet, count = xx

Problema

El switch con Supervisor Engine II (WS-X4013=) genera el mensaje que muestra esta sección y experimenta una pérdida parcial o total de conectividad de red. La pérdida de conectividad puede afectar únicamente a una parte de los puertos de conmutación y puede incluir los puertos de link ascendente.

```
%SYS-4-P2_WARN: 1/Invalid crc, dropped packet, count = xx
```

Descripción

Este ejemplo muestra el resultado de syslog o de la consola que se ve cuando ocurre este error:

```
%SYS-4-P2_WARN: 1/Invalid crc, dropped packet, count = 590073
%SYS-4-P2_WARN: 1/Invalid crc, dropped packet, count = 594688
```

A veces, también ve este mensaje:

```
%SYS-4-P2_WARN: 1/Astro(3/4) - management request timed out
```

Nota: Si sólo obtiene el `%SYS-4-P2_WARN: 1/Astro(3/4) - el` mensaje `de solicitud de administración ha agotado el tiempo de espera`, consulte el %SYS-4-P2_WARN: 1/Astro(mod/port) de este documento.

Nota: Puede experimentar problemas de conectividad de red cuando aparezcan estos mensajes.

Siga estos pasos de troubleshooting y capture el resultado de los comandos durante cada paso:

Nota: Póngase en contacto con el Soporte Técnico de Cisco para obtener asistencia en la resolución de problemas.

1. Ejecute estos comandos:**show logging buffer -1023show tech-supportshow health 1dump 1**
2. Ejecute uno de estos comandos cinco veces, a intervalos aleatorios, y observe el contador `InvalidPacketBufferCrcs`:**show nvramenv 1**—Software CatOS versión 6.1(1) o posterior

   ```
   Cat4k> (enable) show nvramenv 1

   PS1="rommon ! >"
   ?="0"
   DiagBootMode="post"
   MemorySize="64"
   ResetCause="20"
   AutobootStatus="success"
   InvalidPacketBufferCrcs="82325"
   ```

   show env 1: versión de software CatOS 5.5(19) o anteriorCuando repita el comando, observe si el contador `InvalidPacketBufferCrcs` aumenta rápidamente por valores altos.

   ```
   cat4k> (enable) show nvramenv 1

   PS1="rommon ! >"
   ?="0"
   DiagBootMode="post"
   MemorySize="64"
   ResetCause="20"
   AutobootStatus="success"
   InvalidPacketBufferCrcs="82763"
   ```

   Nota: Si ve un pequeño número de `InvalidPacketBufferCrcs` en la salida y ejecuta una versión de software CatOS anterior a 5.5.10, 6.2.3 o 6.3.1, actualice a una versión posterior. Existe la posibilidad de que haya encontrado el ID de bug de Cisco CSCdu48749 (sólo clientes registrados) y CSCdt80707 (sólo clientes registrados) . Consulte Notificación: Los Puertos Catalyst 4000 pierden el estado de VLAN activa, lo que produce pérdida de paquetes para obtener más información.
3. Si encuentra que el contador `InvalidPacketBufferCrcs` aumenta a una velocidad alta, ejecute el comando **reset** para restablecer por software el switch.**Nota:** La captura de la salida en este paso es fundamental.

   ```
   cat4k> (enable) reset
   ```

```
This command will reset the system.
Do you want to continue (y/n) [n]? y

nodcsw0nm1> (enable)
WS-X4013 bootrom version 5.4(1), built on 2000.02.17 18:28:09
H/W Revisions:    Crumb: 5    Rancor: 8    Board: 2
Supervisor MAC addresses: 00:0a:8a:6d:92:00 through 00:0a:8a:6d:95:ff
(1024 addresses)
Installed memory: 64 MB
Testing LEDs.... done!
The system will autoboot in 5 seconds.
Type control-C to prevent autobooting.

rommon 1 >
The system will now begin autobooting.
Autobooting image: "bootflash:cat4000-k9.6-3-9.bin"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC################################
Starting Off-line Diagnostics
Mapping in TempFs
Board type is WS-X4013
DiagBootMode value is "post"
Loading diagnostics...

Power-on-self-test for Module 1:  WS-X4013
Status: (. = Pass, F = Fail)
uplink port 1: .        uplink port 2: F        eobc port: .
processor: .            cpu sdram: .            eprom: .
nvram: .                flash: .                enet console port: .
switch 0 port 0: .      switch 0 port 1: .      switch 0 port 2: .
switch 0 port 3: .      switch 0 port 4: .      switch 0 port 5: .
switch 0 port 6: .      switch 0 port 7: .      switch 0 port 8: .
switch 0 port 9: .      switch 0 port 10: .     switch 0 port 11: .
switch 0 registers: .   switch 0 sram: .        switch 1 port 0: .
switch 1 port 1: .      switch 1 port 2: .      switch 1 port 3: .
switch 1 port 4: .      switch 1 port 5: .      switch 1 port 6: .
switch 1 port 7: .      switch 1 port 8: .      switch 1 port 9: .
switch 1 port 10: .     switch 1 port 11: .     switch 1 registers: .
switch 1 sram: .        switch 2 port 0: F      switch 2 port 1: F
switch 2 port 2: F      switch 2 port 3: F      switch 2 port 4: F
switch 2 port 5: F      switch 2 port 6: F      switch 2 port 7: F
switch 2 port 8: F      switch 2 port 9: F      switch 2 port 10: F
switch 2 port 11: F     switch 2 registers: .   switch 2 sram: F
Module 1 Failed

Exiting Off-line Diagnostics
Failed Module Bringup Process
Use 'show test 1' to see results of tests.
!--- Output suppressed.
```

4. Después de que el switch vuelva a estar en línea, ejecute el comando **show test 1**.
5. Si el resultado del comando muestra fallas de diagnóstico, apague y vuelva a encender el switch.
6. Después de que el switch vuelva a estar en línea, ejecute el comando **show test 1** nuevamente y observe si el switch ha fallado en las pruebas de diagnóstico.
7. Póngase en contacto con el Soporte Técnico de Cisco en base a su observación:Si el switch ha fallado nuevamente las pruebas de diagnóstico, es muy probable que el Supervisor Engine haya fallado. Póngase en contacto con el Soporte Técnico de Cisco para obtener más instrucciones.Si el switch no falla en los diagnósticos al reiniciar el hardware, comuníquese con Soporte Técnico de Cisco con la información que recopiló en los otros

pasos de este procedimiento.**Nota:** Si el Soporte Técnico de Cisco no estuvo involucrado durante la resolución de problemas, debe proporcionar la información en el orden en que se documentó.

Después de realizar el reinicio de hardware, se debe restaurar la conectividad de red.

%SYS-4-P2_WARN: 1/Tráfico no válido de la dirección de origen de multidifusión

Problema

El switch genera `tráfico no válido de` mensajes de `dirección de origen multicast`.

Descripción

Este ejemplo muestra el resultado de syslog que se ve cuando ocurre este error:

```
SYS-4-P2_WARN: 1/Invalid traffic from multicast source address
               81:00:01:00:00:00 on port 2/1
%SYS-4-P2_WARN: 1/Invalid traffic from multicast source address
                81:00:01:01:00:00 on port 2/1
```

El switch genera el mensaje syslog de `tráfico no válido de la dirección de origen multicast` cuando el switch recibe paquetes con una dirección MAC multicast como MAC de origen. El uso de una dirección MAC de difusión o multidifusión como MAC de origen para una trama no cumple con los estándares. Sin embargo, el switch todavía reenvía el tráfico que se origina en una dirección MAC multicast.

El mensaje syslog indica la dirección MAC multicast en el campo MAC de origen de la trama, así como el puerto en el que se recibió el tráfico.

La solución alternativa es tratar de identificar la estación final que genera tramas con una dirección MAC de origen multicast. Típicamente, uno de estos dispositivos transmite tales tramas:

- Un generador de tráfico, como SmartBits
- Dispositivos de terceros que comparten una dirección MAC de multidifusión, como firewall de equilibrio de carga o productos de servidor

%SYS-4-P2_WARN: 1/Astro(mod/puerto)

Problema

El switch genera `%SYS-4-P2_WARN: 1/Astro(6/6)...` mensajes.

Descripción

Este mensaje de error indica que Supervisor Engine ha perdido la comunicación con un componente en una tarjeta de línea. El Supervisor Engine realiza un seguimiento de los tiempos de espera asociados a esta comunicación. Hay muchas causas posibles de esta condición. Para obtener más información sobre este mensaje de error y sus posibles causas, consulte Introducción y resolución de problemas de tiempos de espera Astro/Lemans/NiceR en los switches Catalyst 4000/4500 Series

%SYS-4-P2_WARN: 1/Tag 0

El switch genera `%SYS-4-P2_WARN: 1/Etiqueta 0...` mensajes.

Este ejemplo muestra el resultado de syslog que se ve cuando ocurre este error:

```
%SYS-4-P2_WARN: 1/Tag [dec] on packet from [ether] port [chars],
                but port's native vlan is [dec]
```

Este mensaje indica que se recibió un paquete etiquetado 802.1Q en un puerto no troncal. La VLAN que se deriva de la etiqueta de paquete es diferente de la VLAN nativa del puerto. En el mensaje de error:

- `Tag [dec]` es el identificador de VLAN del paquete.
- El `[éter]` es la dirección MAC del host.
- El `puerto [chars]` es el identificador del puerto.
- El segundo `[dec]` es el número de VLAN nativo.

Existe la posibilidad de que el puerto local esté configurado incorrectamente como puerto de acceso en lugar de como puerto troncal. Como alternativa, el lado remoto puede haberse configurado como puerto troncal en lugar de como puerto de acceso.

Verifique que el puerto local no esté configurado incorrectamente como puerto de acceso en lugar de como puerto troncal. Además, verifique que el lado remoto no esté configurado como puerto troncal en lugar de como puerto de acceso.

convert_post_SAC_CiscoMIB:Nvram m block [#] unconvertible

Problema

El switch genera periódicamente `Convert_post_SAC_CiscoMIB:` mensajes de syslog.

Descripción

Este ejemplo muestra el resultado de la consola que se ve cuando se produce este mensaje:

```
convert_post_SAC_CiscoMIB:Nvram block 0 unconvertible: )
convert_post_SAC_CiscoMIB:Nvram block 1 unconvertible: )
convert_post_SAC_CiscoMIB:Nvram block 2 unconvertible: )
```

El switch a menudo genera estos mensajes de consola cuando actualiza o rebaja las versiones de código CatOS. El error también puede ocurrir cuando carga una configuración de switch que otro switch genera o cuando usa una configuración de switch de otra versión de código. Un failover al Supervisor Engine en espera también puede generar estos mensajes.

Las diferentes versiones del código contienen variables almacenadas en la NVRAM. Cuando el switch se inicia inicialmente en una versión posterior o anterior de CatOS, el switch convierte la configuración anterior en una versión que se puede utilizar en la imagen de inicio actual. Durante este proceso, se desasigna un bloque de memoria particular que no es necesario o no se puede utilizar en el formulario actual, en lugar de convertirse. Esta función interna genera el mensaje de error.

Este mensaje generalmente es sólo informativo. Compare la configuración anterior con la configuración actual para verificar que toda la información de configuración se haya convertido correctamente.

Si estos mensajes aparecen cuando no se han producido actualizaciones de código, cambios de configuración o fallas en Supervisor Engine, cree una solicitud de servicio (sólo clientes registrados) con Soporte Técnico de Cisco.

Error de checksum global

Problema

Este mensaje de error puede aparecer en los Catalyst 4000/4500 y 6000/6500 Series Switches que ejecutan el software del sistema Catalyst OS.

El mensaje de error `Global checksum failed` puede aparecer en la salida del comando **show version**.

```
4000-Switch> (enable) show version
WS-C4006 Software, Version NmpSW: 7.6(2)
Copyright (c) 1995-2003 by Cisco Systems, Inc.
NMP S/W compiled on Jun 25 2003, 23:00:25
GSP S/W compiled on Jun 25 2003, 17:11:56

System Bootstrap Version: 5.4(1)

Hardware Version: 3.2  Model: WS-C4006  Serial #: FOX053701JY

Mod Port Model              Serial #              Versions
--- ---- ------------------ --------------------- --------------------------------
--
1   2    WS-X4013           JAB054207A0           Hw : 3.2
                                                  Gsp: 7.6(2.0)
                                                  Nmp: 7.6(2)
2   48   WS-X4148-RJ45V     JAB05410EQF           Hw : 1.6
3   48   WS-X4148-RJ45V     JAB05410ES5           Hw : 1.6
4   48   WS-X4148-RJ45V     JAB0541070L           Hw : 1.6
5   48   WS-X4148-RJ45V     JAB05410ESC           Hw : 1.6

       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
1       65536K  40935K  24601K  16384K  10543K   5841K  480K  198K  282K

Global checksum failed.

Uptime is 306 days, 8 hours, 0 minute
```

Un mensaje relacionado, `NVRAM: F`, puede aparecer en la salida del comando **show test**.

```
6000-Switch> show test 1

Diagnostic mode: complete   (mode at next reset: complete)


Module 1 : 2-port 1000BaseX Supervisor
Network Management Processor (NMP) Status: (. = Pass, F = Fail, U = Unknown)
```

```
  ROM:  .   Flash-EEPROM: .   Ser-EEPROM: .   NVRAM: F   EOBC Comm: .

Line Card Status for Module 1 : PASS

Port Status :
  Ports 1  2
  -----------
        .  .
!--- Output is suppressed.
```

Descripción

El error de suma de comprobación significa que la próxima vez que se recargue la casilla, es muy probable que NVRAM se pierda debido a una falla en la suma de comprobación CRC mientras leía la configuración. En general, no es un error de hardware, sino que el switch se corrige por sí solo. Esto no tiene efecto en el switch operativo a menos que se realicen cambios en la configuración mientras el switch se encuentra en esta condición. Pero, en la mayoría de los casos, un reinicio resuelve el problema de la suma de comprobación ya que ésta se vuelve a calcular. Este problema se documenta con el ID de bug de Cisco CSCdx87646 (sólo clientes registrados) .

Solución

Complete estos pasos para recuperar el switch de este estado de error:

1. Haga una copia de seguridad de la configuración del switch. Consulte Carga de Archivos de Configuración a un Servidor TFTP para obtener más información sobre cómo realizar una copia de seguridad de la configuración.
2. Reinicie el módulo Supervisor ejecutando el comando **reset** ***supervisor_module_#***.
3. Una vez que se inicie el switch, ejecute los comandos **show version** y **show test** para verificar si la salida es normal.
4. Verifique la configuración existente del switch y restaure desde la copia de seguridad si es necesario.

Información Relacionada

- Guía de mensajes del sistema Switches de la familia Catalyst, 7.4
- Configuración del registro de mensajes de sistema
- Mensajes de Error Comunes de CatOS en Catalyst 5000/5500 Series Switches
- Mensajes de Error Comunes de CatOS en los Catalyst 6500/6000 Series Switches
- Decodificador de Mensajes de Error (solo para clientes registrados)
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems