Messaggi di errore comuni di CatOS sugli switch Catalyst serie 4500/4000

Sommario

Introduzione

In questo documento viene fornita una breve spiegazione dei log di sistema comuni (syslog) e dei messaggi di errore visualizzati sugli switch Cisco Catalyst serie 4500/4000 con software Catalyst OS (CatOS).

Se non si trovano i dettagli di un messaggio di errore specifico in questo documento, usare lo strumento Error Message Decoder (solo utenti registrati). Questo strumento fornisce il significato dei messaggi di errore generati dal software Cisco IOS® e dal software CatOS.

Nota: il formato esatto del syslog e dei messaggi di errore descritti in questo documento può variare. La variazione dipende dalla versione software in esecuzione sul Supervisor Engine dello switch.

Nota: questa è la configurazione minima consigliata per la registrazione sugli switch Catalyst serie 4500/4000:

- Impostare la data e l'ora sullo switch o configurare lo switch in modo che utilizzi il protocollo NTP (Network Time Protocol) per ottenere la data e l'ora da un server NTP.**Nota:** usare il comando **set time** per impostare la data e l'ora sullo switch.
- Verificare che i timestamp di registrazione e registrazione siano abilitati (impostazione predefinita).
- Se possibile, configurare lo switch in modo che acceda a un server syslog.

I messaggi di errore riportati in questo documento possono essere visualizzati sugli switch Catalyst serie 4500/4000 e sui relativi derivati, ad esempio sugli switch Catalyst 2948G, 2980G e 4912G.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Messaggi di errore sugli switch Catalyst serie 4500/4000

%C4K_HWPORTMAN-4-BLOCKEDTXQUEUE:Coda di trasmissione bloccata HwTxQId[dec]on [char], count=[dec]

Problema

Lo switch genera errori `%C4K_HWPORTMAN-4-BLOCKEDTXQUEUE:Blocked transmission queue HwTxQId[dec]on[char], count=[dec].`

Descrizione

Questo messaggio con limiti di velocità indica che una coda di trasmissione su una porta è bloccata per motivi diversi dalla "pausa". In altre parole, il traffico su quella porta è stato limitato e bloccato. I messaggi della coda di trasmissione bloccata vengono visualizzati se il Supervisor Engine non è in grado di inviare i pacchetti alla scheda di linea a causa della ricezione di un bit occupato dalla scheda di linea. Il problema può essere causato da hardware non valido o da una mancata corrispondenza velocità/duplex. Per risolvere il problema, configurare entrambi i lati del collegamento in modo che eseguano la negoziazione automatica per la velocità e il duplex. Usare il comando shut/**no shut** per ripristinare la porta. Se il problema persiste, spostare il dispositivo connesso su un'altra porta e verificare se il problema si verifica. Come ultima misura per sbloccare la coda di trasmissione (Tx), usare il comando **hw-module reset** per riavviare lo switch o ripristinare la scheda di linea.

%CDP-4-NVLANMISMATCH: Mancata corrispondenza della vlan nativa rilevata sulla porta [dec]/[dec]

Problema

Lo switch genera frequenti messaggi syslog di `%CDP-4-NVLANMISMATCH`.

Descrizione

In questo esempio viene mostrato l'output della console visualizzato quando sullo switch viene visualizzato questo messaggio di errore:

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

Lo switch genera questo messaggio ogni volta che la porta dello switch è connessa fisicamente a un altro switch o router. Lo switch genera questo messaggio perché la VLAN nativa configurata sulla porta è diversa dalla VLAN nativa impostata sulla porta dello switch o del router di connessione.

Una porta trunk configurata con tag IEEE 802.1Q può ricevere sia traffico con tag che traffico senza tag. Per impostazione predefinita, lo switch inoltra il traffico senza tag alla VLAN nativa configurata per la porta. Se un pacchetto ha lo stesso ID VLAN dell'ID VLAN nativo della porta in uscita, il pacchetto viene trasmesso senza tag. Se gli ID delle VLAN non sono gli stessi, lo switch trasmette il pacchetto con un tag.

Verificare che la VLAN nativa per un trunk 802.1Q sia la stessa su entrambe le estremità del collegamento trunk. Se la VLAN nativa su un'estremità del trunk è diversa dalla VLAN nativa sull'altra estremità, il traffico delle VLAN native su entrambi i lati non può essere trasmesso correttamente sul trunk. La mancata trasmissione corretta può causare problemi di connettività nella rete.

Per verificare la VLAN nativa configurata sullo switch, usare il comando **show trunk** *mod*/*porta*. In questo comando, *mod*/*porta* è la porta trunk. Di seguito viene riportato un esempio dell'output 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)
```

Per modificare la VLAN nativa configurata sulla porta trunk, usare il *comando* ***set vlan*** *vlan-id mod/porta*. In questo comando, *mod/porta* è la porta trunk.

DTP-1-ILGLCFG: Configurazione non valida (on, isl—on,dot1q) sulla porta [mod/porta]

Problema

Lo switch genera il comando `DTP-1-ILGLCFG: Errori di configurazione non validi (on, isl—on,dot1q) sulla porta [mod/porta].`

Descrizione

Questo messaggio può apparire se entrambi i lati del trunk sono impostati su `on`, ma i tipi di incapsulamento (`isl, dot1q`) non corrispondono. Se le modalità del trunk sono impostate su `desiderabile`, il trunk non viene visualizzato a causa di questa configurazione errata. Per risolvere il problema, controllare l'output del comando **show trunk** su entrambe le estremità. Verificare che i tipi di incapsulamento siano identici.

%IP-3-UDP_SOCKOVFL:overflow del socket UDP

Problema

Lo switch genera messaggi syslog di `%IP-3-UDP_SOCKOVFL:UDP socket overflow`.

Descrizione

In questo esempio viene mostrato l'output della console visualizzato quando si verifica questo errore:

Nota: il numero di socket UDP (User Datagram Protocol) visualizzato può variare o essere sempre lo stesso.

```
%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
```

Lo switch genera questo messaggio syslog quando il buffer allocato per i pacchetti in arrivo sul socket specificato (porta di destinazione UDP) è pieno. Il buffer è pieno perché la velocità del traffico destinato a quel socket è troppo alta. Questa condizione può verificarsi, ad esempio, quando una stazione di gestione di rete invia un numero elevato di query SNMP (Simple Network Management Protocol). Quando si verifica un overflow UDP, provare a ridurre il numero di query SNMP. Eseguire una delle azioni seguenti:

- Aumentare l'intervallo di polling sulla stazione di gestione di rete.
- Ridurre il numero di oggetti MIB sottoposti a polling.

Nell'esempio di questa sezione, lo switch ha ricevuto un numero eccessivo di pacchetti destinati all'indirizzo IP dello switch (o all'indirizzo di broadcast) con socket UDP 2353 di destinazione. Poiché il buffer di input per questo socket sullo switch è pieno, lo switch genera un messaggio syslog. Utilizzare il comando **show netstat udp** per verificare il numero di volte in cui lo switch ha raggiunto la condizione di overflow.

Questi messaggi syslog indicano che una o più stazioni inviano una grande quantità di traffico UDP alle porte UDP di destinazione specificate allo switch. Se lo switch genera un numero eccessivo di messaggi, utilizzare un analizzatore di rete per identificare l'origine del traffico e ridurre la velocità del traffico. Per ulteriori informazioni, fare riferimento all'esempio di configurazione di Catalyst Switched Port Analyzer (SPAN).

Nota: il contatore della `porta non è presente`. Questo contatore indica il numero di pacchetti UDP ricevuti dallo switch e destinati a porte inesistenti.

%IP-3-UDP_BADCKSUM:checksum UDP non valido

Problema

Lo switch genera messaggi syslog di `%IP-3-UDP_SOCKOVFL:UDP socket overflow`.

Descrizione

In questo esempio viene mostrato l'output della console visualizzato quando si verifica questo errore:

Nota: il numero di socket UDP visualizzato può variare o essere sempre lo stesso.

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

Lo switch genera questo messaggio syslog quando rileva un checksum errato su un datagramma UDP, ad esempio i pacchetti SNMP. L'intestazione del datagramma UDP contiene un checksum che il dispositivo di rete ricevente controlla per determinare se il datagramma è stato danneggiato durante la trasmissione. Se il checksum ricevuto non corrisponde al valore di checksum nell'intestazione, il datagramma viene eliminato e viene registrato un messaggio di errore. Utilizzare il comando **show netstat udp** per verificare il numero di volte in cui lo switch ha rilevato un datagramma di checksum errato.

```
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
```
Questo messaggio è puramente informativo. Questo messaggio viene generato da un dispositivo di rete che invia pacchetti errati allo switch. Usare un analizzatore di rete per identificare l'origine del traffico. Per ulteriori informazioni, fare riferimento all'esempio di configurazione di Catalyst Switched Port Analyzer (SPAN).

Nota: il contatore della `porta non è presente`. Questo contatore indica il numero di pacchetti UDP ricevuti dallo switch e destinati a porte inesistenti.

%KERNEL-5-UNALIGNACCESS:Correzione allineamento eseguita

Problema

Lo switch genera messaggi syslog con `%KERNEL-5-UNALIGNACCESS:Alignment correction` periodici.

Descrizione

Nell'esempio viene mostrato l'output syslog visualizzato quando si verifica questo errore:

```
%KERNEL-5-UNALIGNACCESS:Alignment correction made at 0x80056B3C reading 0x81B82F36
```
Questi messaggi syslog indicano che la CPU dello switch ha rilevato e corretto un errore di allineamento quando lo switch ha tentato di accedere ai dati nella DRAM. Questi messaggi sono puramente informativi. I messaggi non indicano problemi con lo switch e non influiscono sulle prestazioni del sistema.

In alcuni casi viene visualizzato un numero eccessivo di messaggi. Ad esempio, questi messaggi possono sovraccaricare il file di log del server syslog o la console dello switch. Se si riceve un numero eccessivo di messaggi, valutare l'opportunità di aggiornare il software dello switch all'ultima release di manutenzione per il software release train. In alternativa, usare il comando **set logging level kernel 4 default** per modificare il livello di log per la funzionalità `Kernel` a 4 o inferiore.

Se si esegue l'aggiornamento all'ultima release di manutenzione ma si ricevono comunque questi messaggi syslog, creare una richiesta di servizio (solo utenti registrati) con il supporto tecnico Cisco.

%MCAST-4-RX_JNRANGE:IGMP: Rapporto ricezione nell'intervallo

Problema

Se lo snooping IGMP (Internet Group Management Protocol) è abilitato, sullo switch verrà visualizzato il messaggio `%MCAST-4-RX_JNRANGE:IGMP: Report ricevuto nell'intervallo 01-00-5e-00-00-xx`. Messaggio di errore.

Descrizione

Nell'esempio viene mostrato l'output syslog visualizzato quando si verifica questo errore:

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

Il `rapporto RCV nel` messaggio syslog `range` è puramente informativo. Lo switch genera questo messaggio quando riceve pacchetti di report IGMP con un indirizzo MAC multicast che inizia con 01-00-5e-00-00-*xx*. Questo intervallo di indirizzi di layer 2 (L2) equivale a un intervallo di indirizzi multicast di layer 3 (L3) compreso tra 224.0.0.0 e 224.0.0.255. Questi indirizzi sono riservati all'utilizzo dei protocolli di routing e di altri protocolli di individuazione o manutenzione della topologia di basso livello. Esempi di tali protocolli includono l'individuazione dei gateway e la creazione di rapporti sull'appartenenza ai gruppi.

Per risolvere il problema, usare uno strumento di acquisizione dei pacchetti, ad esempio uno sniffer, e filtrare i messaggi IGMP. Inoltre, è possibile usare la funzione Catalyst SPAN per copiare i pacchetti da una porta che si sospetta riceva questi messaggi da un dispositivo di rete. Per eliminare questi messaggi, eseguire il comando **set logging level mcast 2 default**. Con questo comando il livello di registrazione dei messaggi multicast viene impostato su 2.

Usare le porte mostrate dal comando **show multicast router** e gli eventuali uplink al core della rete come porte di origine SPAN. Se queste porte sono porte trunk, configurare anche la porta di destinazione SPAN come porta trunk. Usare il comando **show trunk** per verificare che le porte siano porte trunk.

MGMT-5-LOGIN_FAIL:Accesso dell'utente dalla console non riuscito

Problema

Lo switch genera `MGMT-5-LOGIN_FAIL:Accesso dell'utente non riuscito a causa di` errori `della console`.

Descrizione

Questo messaggio può indicare un problema con il Terminal Server collegato alla porta console dello switch. Quando la console dello switch è collegata a una linea asincrona di un Terminal Server e si esegue un reset a caldo sullo switch, il garbage (testo casuale) viene trasmesso attraverso lo schermo per alcuni minuti. Se TACACS è abilitato sullo switch, alcuni minuti possono trasformarsi in diversi giorni perché TACACS memorizza ed elabora il Garbage Pezzo per Pezzo. Per risolvere il problema, usare il comando **no exec** sulla riga asincrona a cui si connette lo switch.

Nota: anche dopo aver eseguito il comando **no exec**, i messaggi continuano finché il buffer non viene cancellato.

Nota: se viene visualizzato il messaggio di errore `%MGMT-5-LOGIN_FAIL:L'utente non è riuscito a eseguire la registrazione tramite Telnet - è stato raggiunto il numero massimo di tentativi`, provare a limitare il numero di utenti autorizzati a connettersi allo switch in modalità Telnet.

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

Problema

Lo switch genera frequenti messaggi syslog `%PAGP-5-PORTFROMSTP` e `%PAGP-5-PORTTOSTP`.

Descrizione

Nell'esempio viene mostrato l'output della console visualizzato quando lo switch genera questi messaggi syslog:

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

La funzione di registrazione PAgP (Port Aggregation Protocol) segnala gli eventi che coinvolgono PAgP. Il protocollo PAgP viene utilizzato per negoziare i collegamenti EtherChannel tra gli switch. Lo switch genera il messaggio syslog `%PAGP-5-PORTFROMSTP` alla perdita di un collegamento su una porta dello switch. Lo switch genera il messaggio syslog `%PAGP-5-PORTTOSTP` al rilevamento di un collegamento su una porta dello switch. Questi messaggi syslog sono normali messaggi informativi che indicano l'aggiunta o la rimozione di una porta dallo spanning tree.

Nota: per visualizzare questi messaggi non è necessario abilitare il channeling.

Nell'esempio di questa sezione, lo switch ha prima perso il collegamento sulla porta 3/3, che ha rimosso la porta dallo Spanning Tree. Quindi, lo switch ha nuovamente rilevato il collegamento sulla porta, che ha riaggiunto la porta allo spanning tree.

Se questi messaggi vengono visualizzati di frequente per una porta specifica, il collegamento lampeggia, ovvero viene perso e riacquisito costantemente. Indaghi la causa. Le cause tipiche dello sfarfallio dei collegamenti su una porta dello switch sono:

- Mancata corrispondenza velocità/duplex
- Cavo difettoso
- Guasto della scheda di interfaccia di rete (NIC) o un altro problema della stazione terminale
- Porta dello switch guasta
- Altre configurazioni errate

Per eliminare questi messaggi syslog, usare il comando **set logging level pagp 4 default** per impostare il livello di log per la funzione PAgP su un valore pari o inferiore a 4. Il livello di registrazione predefinito per PAgP è 5.

%SPANTREE-3-PORTDEL_FAILNOTFOUND

Problema

Lo switch genera messaggi syslog `%SPANTREE-3-PORTDEL_FAILNOTFOUND` periodici.

Descrizione

Nell'esempio viene mostrato l'output syslog visualizzato quando si verifica questo errore:

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

Questi messaggi syslog indicano che il gruppo PAgP ha tentato di rimuovere una porta dallo spanning tree per la VLAN specificata, ma la porta non si trovava nella struttura di dati dello spanning tree per tale VLAN. In genere, un altro processo, ad esempio il DTP (Dynamic Trunking Protocol), ha già rimosso la porta dallo Spanning Tree.

Questi messaggi in genere accompagnano i messaggi `%PAGP-5-PORTFROMSTP`. I messaggi sono destinati a scopi di debug. I messaggi non indicano problemi con lo switch e non influiscono sulle prestazioni dello switch. Inoltre, questi messaggi non vengono registrati a meno che non sia stata modificata la configurazione di registrazione predefinita della funzione `SPANTREE`. Il livello di registrazione predefinito per `SPANTREE` è 2.

In alcuni casi viene visualizzato un numero eccessivo di messaggi. Ad esempio, questi messaggi possono inondare la console dello switch. Se si riceve un numero eccessivo di messaggi, valutare l'opportunità di aggiornare il software dello switch all'ultima release di manutenzione per il software release train. Nella maggior parte dei casi, le versioni software più recenti eliminano questi messaggi.

%SYS-3-P2_ERROR: 1/Modulo sconosciuto

Problema

Il `%SYS-3-P2_ERROR:` Quando si installa un nuovo modulo di switching in uno switch Catalyst serie 4500/4000, viene visualizzato il messaggio di errore `1/Unknown module`.

Descrizione

In questo esempio viene mostrato l'output della console visualizzato quando si verifica questo errore:

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

Il `%SYS-3-P2_ERROR: 1/L'`errore del `modulo sconosciuto` si verifica quando la versione dell'immagine software attualmente in esecuzione sul Supervisor Engine non supporta il componente hardware inserito.

Nell'esempio, un modulo di switching per server 1000BASE-X (WS-X4418) a 18 porte è inserito in uno switch Catalyst 4500/4000 con software CatOS versione 4.4(1). Il modulo WS-X4418 richiede una versione software minima di 4.5(1).

Per ovviare al problema, aggiornare la versione software del Supervisor Engine a una versione software che supporti l'hardware. Per un elenco delle versioni software minime per ciascun modulo, fare riferimento alle note sulla versione degli switch Catalyst serie 4500.

%SYS-3-P2_ERROR: 1/I buffer interni hanno esaurito i vbufs

Problema

Lo switch genera `%SYS-3-P2_ERROR: 1/Esaurire i` messaggi `vbufs` quando più host sono accesi nello stesso momento o quasi contemporaneamente.

Descrizione

In questo esempio viene mostrato l'output della console visualizzato quando si verifica l'errore:

`%SYS-3-P2_ERROR: 1/Have run out of vbufs(internal buffers)`
Il `%SYS-3-P2_ERROR: Gli` errori `1/Have run out of vbufs (internal buffer)` possono verificarsi quando più host vengono accesi contemporaneamente. Dopo l'accensione degli host, gli errori non vengono più visualizzati.

Questi errori non causano interruzioni alla capacità del sistema Catalyst di commutare il traffico. I messaggi sono di natura puramente informativa.

%SYS-3-P2_ERROR: Host xx:xx:xx:xx:xx:xx sta flapping tra le porte

Problema

Lo switch genera `%SYS-3-P2_ERROR: Host xx:xx:xx:xx:xx:xx sta flapping tra porte...` messaggi, dove *xx:xx:xx:xx:xx:xx* è un indirizzo MAC.

Descrizione

In questo esempio viene mostrato l'output della console visualizzato quando si verifica questo errore:

`%SYS-4-P2_WARN: 1/Host 00:50:0f:20:08:00 is flapping between port 1/2 and port 4/39`
Per individuare e risolvere le cause di questo messaggio di errore, attenersi alla procedura e alle linee guida descritte in questa sezione.

Il messaggio indica che lo switch Catalyst 4500/4000 ha appreso un indirizzo MAC già esistente nella tabella CAM (Content-Addressable Memory) su una porta diversa da quella originale. Questo comportamento si verifica ripetutamente in brevi periodi di tempo, il che significa che vi è uno sfarfallio di indirizzi tra le porte.

Se il messaggio viene visualizzato per più indirizzi MAC, il comportamento non è normale. Questo comportamento indica un possibile problema di rete perché gli indirizzi MAC si spostano rapidamente da una porta all'altra prima del tempo di aging predefinito. Il problema può essere il traffico sulla rete che continua a scorrere. I sintomi tipici includono:

- Utilizzo CPU elevato
- Traffico lento in tutta la rete
- Elevato utilizzo del backplane sullo switch

Per informazioni su come identificare e risolvere i problemi relativi allo Spanning Tree, fare riferimento a Problemi del protocollo Spanning Tree e considerazioni correlate sulla progettazione.

Se viene visualizzato il messaggio di errore per uno o due indirizzi MAC, individuare questi indirizzi MAC per determinarne la causa. Usare il comando **show cam** ***mac_addr*** per identificare da dove sono stati appresi questi indirizzi MAC. In questo comando, *mac_addr* è l'indirizzo MAC segnalato dall'errore come flapping.

Dopo aver determinato le porte su cui lampeggia l'indirizzo MAC, individuare l'indirizzo MAC. Collegare i dispositivi intermedi tra lo switch Catalyst 4500/4000 e il dispositivo con il problema all'indirizzo MAC. Eseguire questa operazione finché non si è in grado di identificare l'origine e la modalità di connessione della periferica alla rete.

Nota: poiché l'indirizzo MAC è sfasato tra due porte, individuare entrambi i percorsi.

Nell'esempio viene mostrato come tracciare entrambi i percorsi dai quali è stato appreso questo indirizzo MAC:

Nota: si supponga di aver ricevuto questo messaggio e di aver iniziato a verificarlo.

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

Per verificare come è stato appreso questo indirizzo MAC da entrambe le porte, attenersi alla seguente procedura:

1. Prendere in considerazione prima la porta 1/2 ed eseguire il comando **show cam dynamic 1/2**.Se l'indirizzo MAC 00:50:0f:20:08:00 è presente nell'elenco degli indirizzi MAC appresi su questa porta, determinare se si tratta di un host singolo connesso o se esistono più host registrati su quella porta.
2. A seconda che vi siano uno o più host, esaminare il dispositivo:Se è collegato un solo host (00:50:0f:20:08:00), controllare l'altra porta registrata e verificare che l'host sia collegato due volte allo switch.Nell'esempio, l'altra porta è la porta 4/39.Se l'host dispone di connessioni ad altri dispositivi che possono ricondurre allo switch, provare a individuare i dispositivi intermedi.Sui dispositivi Cisco, eseguire il **comando show cdp neighbors** *mod*/*porta* ***detail***. L'output fornisce informazioni sui dispositivi intermedi.Di seguito è riportato un esempio di output:

```
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. Stabilire una sessione Telnet con il dispositivo e seguire il percorso dell'indirizzo MAC.Nell'esempio, l'indirizzo IP è 172.16.1.1.Ripetere la procedura per tutti gli indirizzi MAC segnalati dal messaggio di errore come flapping.
4. Creare un semplice diagramma del dispositivo di origine con l'indirizzo MAC e delle connessioni fisiche (le porte Catalyst 4500/4000) da cui e verso cui l'indirizzo MAC lampeggia.Il diagramma consente di determinare se si tratta di una porta e di un percorso

validi per il layout di rete.Se si verifica che entrambe le porte su cui l'indirizzo MAC sta flapping forniscano un percorso verso il nodo di rete, è possibile che si sia verificato un errore nello spanning-tree. Per isolare e risolvere questo loop, consultare il documento sui problemi del protocollo Spanning Tree e sulle relative considerazioni di progettazione.Nelle reti di grandi dimensioni in cui più host di fornitori diversi sono interconnessi, si verifica un problema quando si cerca di individuare l'host utilizzando solo l'indirizzo MAC. Usare l'utility di ricerca per le assegnazioni IEEE OUI e Company_id per rintracciare questi indirizzi MAC. Questo elenco è il front-end del database in cui IEEE ha registrato tutti gli indirizzi MAC assegnati a tutti i fornitori. Immettere i primi tre ottetti dell'indirizzo MAC nella casella **Cerca:** per trovare il fornitore associato al dispositivo. I primi tre ottetti dell'esempio sono 00:50:0f.

Di seguito sono riportati altri problemi che possono causare la visualizzazione del messaggio:

- **Problema di ridondanza NIC del server**: esiste un server con una NIC a doppio collegamento che si comporta in modo errato e non rispetta gli standard. Il server utilizza lo stesso indirizzo MAC per entrambe le porte che si connettono allo stesso switch.
- **HSRP (Hot Standby Router Protocol) flapping**: il flapping di HSRP può causare la visualizzazione di questi messaggi nella console Supervisor Engine. Se l'implementazione HSRP sulla rete è instabile, consultare il documento sulla descrizione e la risoluzione dei problemi HSRP sulle reti degli switch Catalyst per risolvere il problema.
- **Configurazione errata di EtherChannel**: anche una connessione EtherChannel non configurata correttamente può causare questi sintomi. Se le porte segnalate dal messaggio di flapping appartengono allo stesso gruppo di canali, controllare la configurazione di EtherChannel e fare riferimento alla sezione Informazioni sul bilanciamento del carico e sulla ridondanza EtherChannel sugli switch Catalyst per risolvere i problemi relativi alla configurazione.
- **L'host riflette i pacchetti sulla rete**: anche il riflesso dei pacchetti sulla rete da parte di un host può causare il flapping. In genere, la causa principale di questo riflesso del pacchetto è una scheda NIC rotta o un qualsiasi errore dell'interfaccia fisica dell'host connesso alla porta.Se la causa principale dei pacchetti è il riflesso dei pacchetti, è possibile ottenere una traccia dello sniffer ed esaminare il traffico che va a e dalle porte su cui sono visualizzati i messaggi. Se un host riflette i pacchetti, in genere nella traccia vengono visualizzati pacchetti duplicati. I pacchetti duplicati sono un possibile sintomo di questo flapping dell'indirizzo MAC.Per ulteriori informazioni su come configurare una porta per l'utilizzo di uno sniffer, consultare il documento sulla configurazione di SPAN e RSPAN.
- **Difetto software o hardware**: se si è tentato di risolvere il problema del flapping usando le istruzioni in questa sezione, ma si nota comunque il problema, richiedere ulteriore assistenza al supporto tecnico Cisco. Accertarsi di menzionare e di fornire la documentazione relativa alle informazioni raccolte durante l'esecuzione dei passaggi. Queste informazioni rendono più rapida ed efficiente la risoluzione dei problemi.

%SYS-4-P2_WARN: 1/Coda bloccata (tx) sulla porta [char]

Problema

Lo switch genera messaggi `Blocked Queue (tx) sulla porta [char]`.

Descrizione

Nell'esempio viene mostrato l'output syslog visualizzato quando si verifica l'errore:

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

Questi errori indicano un problema hardware o uno dei seguenti problemi:

- Mancata corrispondenza del duplex
- Cavo difettoso
- Cablaggio di tipo 1
- Porte guaste
- Problema hardware di una periferica esterna collegata

La causa più comune di questi errori è un problema del livello fisico. Il problema causa un notevole aumento del traffico sui gigapporti K1 interni. I circuiti integrati specifici dell'applicazione K1 (ASIC) sono i chip principali che controllano lo switch. In genere, il numero di code Tx bloccate aumenta a causa di un problema di configurazione o di un cablaggio danneggiato.

In un ambiente normale, la coda Tx può essere bloccata solo per circa 20 secondi. Un blocco più lungo indica un problema significativo. Di conseguenza, il conteggio delle code Tx bloccate aumenta se la coda Tx non viene svuotata per il gigaport in 35 secondi.

Se necessario, contattare il supporto tecnico Cisco per determinare se il modulo deve essere sostituito. Ma prima, riposizionare il modulo e vedere se il messaggio di errore esiste ancora.

Di seguito viene riportata la procedura per mappare la coda bloccata di Catalyst 4000/2948G/2980G su Gigaport <numero_gigaport> alle porte dello switch del pannello anteriore, che devono essere riposizionate.

Messaggi di errore di esempio:

```
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 )
```

Questo messaggio di errore indica che si è verificato un errore di configurazione probabilmente dovuto a un problema del layer fisico o a una mancata corrispondenza duplex relativa a gigaport 29. Per individuare le porte correlate a gigaport 29, fare riferimento a queste tabelle. Le tabelle variano e dipendono dal Supervisor Engine.

Mappatura porta Gigabit WS-X4013

K1-A (gigaporti 0-11)

Gigaport 0	Uplink 0 (porta 1/1) o interconnessione interna K1-C
Gigaport 1	Slot 6 - interconnessione Gigabit 5
Gigaport 2	Slot 5 - Interconnessione Gigabit 5
Gigaport 3	Slot 2 - interconnessione Gigabit 5
Gigaport 4	Slot 3 - Interconnessione Gigabit 5

Gigaport 5	Slot 4 - interconnessione Gigabit 5
Gigaport 6	Slot 4 - Interconnessione Gigabit 4
Gigaport 7	Slot 3 - Interconnessione Gigabit 4
Gigaport 8	Slot 2 - Interconnessione Gigabit 4
Gigaport 9	Slot 5 - Interconnessione Gigabit 4
Gigaport 10	Slot 6 - interconnessione Gigabit 4
Gigaport 11	Interconnessione interna K1-B

K1-B (gigaporti 12-23)

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

K1-C (gigaporti 24-35)

Gigaport 24	Interconnessione interna a K1-B
Gigaport 25	Slot 6 - interconnessione Gigabit 1
Gigaport 26	Slot 5 - Interconnessione Gigabit 1
Gigaport 27	Slot 2 - interconnessione Gigabit 1
Gigaport 28	Slot 3 - Interconnessione Gigabit 1
Gigaport 29	Slot 4 - interconnessione Gigabit 1
Gigaport 30	Slot 4 - interconnessione Gigabit 0
Gigaport 31	Slot 3 - interconnessione Gigabit 0
Gigaport 32	Slot 2 - interconnessione Gigabit 0
Gigaport 33	Slot 5 - interconnessione Gigabit 0
Gigaport 34	Slot 6 - interconnessione Gigabit 0
Gigaport 35	Uplink 1 (porta 1/2) o interconnessione interna a K1-A

Ogni ASIC K1 ha interconnessioni da 12 gigabit. Queste interconnessioni Gigabit vengono utilizzate tra le schede di linea e il Supervisor Engine come collegamenti seriali point-to-point. Ogni scheda di linea di Catalyst 4000 può essere connessa a 6 interconnessioni da 12 gigabit. Alle interconnessioni Gigabit vengono fatto riferimento da 0 a 5 e le connessioni vengono eseguite in ordine inverso. Ad esempio, su una scheda di linea 4148, l'interconnessione gigabit 5 si connette alle porte 1-8, l'interconnessione gigabit 4 si connette alle porte 9-16.

Mappatura porte di interconnessione modulo di linea

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

Porte	Interconnessione 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

Porte	Interconnessione Gigabit
1	5
2	4
3-10	3
11-18	2
19-26	1
27-34	0

WS-X4418-GB

Porte	Interconnessione Gigabit
1	5
2	4
3-6	3
7-10	2
11-14	1
15-18	0

WS-X4124-FX-MT

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

WS-X4306-GB

Porte	Interconnessione Gigabit

1	5
2	4
3	3
4	2
5	1
6	0

WS—X4412-2 GB-TX

Porte	Interconnessione Gigabit
1-2	5
3-4	4
5-6	3
7-8	2
9-10	1
11-12	0

Esempio di ricerca di porte sospette

```
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 fa riferimento allo slot 3, interconnessione Gigabit 3. Poiché lo slot 3 è un WS-X4232-L3, interconnessione Gigabit 3 fa riferimento alle porte 3-10. Quando si risolvono i problemi relativi a queste porte, verificare la presenza di errori e/o mancata corrispondenza duplex che utilizzano i comandi **show port**, **show mac** e **show counters**. Può inoltre essere utile ottenere un **dump 1** e verificare se sono presenti errori hardware associati alle porte. Un riferimento importante

nell'output del dump 1 è il cscTimeout associato al modulo di linea ASIC per l'interconnessione corrispondente. Il valore di **cscTimeout** deve essere **0**

%SYS-4-P2_WARN: 1/Filtraggio dell'indirizzo MAC Ethernet con valore zero

Problema

Lo switch genera messaggi con `indirizzo MAC Ethernet filtro di valore zero`.

Descrizione

Nell'esempio viene mostrato l'output syslog visualizzato quando si verifica questo errore:

```
%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
```

Lo switch genera il messaggio syslog `dell'indirizzo MAC Ethernet del filtro con valore zero` quando riceve i pacchetti con indirizzo MAC di origine 00-00-00-00-00-00. Questo indirizzo MAC è un indirizzo MAC di origine non valido.

Il messaggio syslog indica che lo switch rifiuta di apprendere l'indirizzo non valido. Tuttavia, lo switch inoltra il traffico che ha origine da un indirizzo MAC composto da tutti gli zeri.

Per risolvere il problema, provare a identificare la stazione terminale che genera i frame con un indirizzo MAC di origine composto da tutti gli zeri. In genere, uno di questi dispositivi trasmette tali frame:

- Generatore di traffico, ad esempio SmartBits Spirent
- Alcuni tipi di server, ad esempio i server IBM WebSphere con bilanciamento del carico
- Router o unità terminale non configurati correttamente, ad esempio un dispositivo che trasmette programmi con zeri
- Una scheda NIC difettosa

%SYS-4-P2_WARN: 1/Crc non valido, pacchetto ignorato, conteggio = xx

Problema

Lo switch con Supervisor Engine II (WS-X4013=) genera il messaggio mostrato in questa sezione e rileva la perdita parziale o totale della connettività di rete. La perdita di connettività può influire solo su una parte delle porte dello switch e può includere le porte uplink.

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

Descrizione

Nell'esempio viene mostrato l'output syslog o console visualizzato quando si verifica questo errore:

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

A volte viene visualizzato anche questo messaggio:

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

Nota: se viene visualizzato solo il messaggio di `%SYS-4-P2_WARN: 1/Astro(3/4) -` messaggio di `timeout della richiesta di gestione`, vedere il %SYS-4-P2_WARN: Sezione 1/Astro(mod/porta) di questo documento.

Nota: quando vengono visualizzati questi messaggi, è possibile che si verifichino problemi di connettività di rete.

Attenersi alla seguente procedura di risoluzione dei problemi e acquisire l'output dei comandi durante ogni fase:

Nota: per assistenza nella risoluzione dei problemi, contattare il supporto tecnico Cisco.

1. Utilizzare i seguenti comandi:**show logging buffer -1023show tech-supportmostra integrità 1dump 1**
2. Eseguire uno di questi comandi cinque volte, a intervalli casuali, e osservare il contatore `InvalidPacketBufferCrcs`:**show nvramenv 1**—Software CatOS release 6.1(1) o successive

   ```
   Cat4k> (enable) show nvramenv 1

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

   show env 1—Software CatOS versione 5.5(19) o precedenteMentre si ripete il comando, osservare se il contatore `InvalidPacketBufferCrcs` aumenta rapidamente di valori elevati.

   ```
   cat4k> (enable) show nvramenv 1

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

   Nota: se nell'output viene visualizzato un numero ridotto di `InvalidPacketBufferCrc` e si esegue una versione del software CatOS precedente alla 5.5.10, 6.2.3 o 6.3.1, aggiornare il sistema a una versione successiva. È possibile che si sia verificato un errore Cisco con ID CSCdu48749 (solo utenti registrati) e CSCdt80707 (solo utenti registrati). Per ulteriori informazioni, fare riferimento al documento sulla comunicazione dei prodotti: Per ulteriori informazioni, le porte Catalyst 4000 perdono lo stato VLAN attivo con conseguente perdita di pacchetti.
3. Se il contatore `InvalidPacketBufferCrcs` aumenta molto, usare il comando **reset** per ripristinare a caldo lo switch.**Nota:** l'acquisizione dell'output in questo passo è di importanza

critica.

```
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"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC################################
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. Dopo aver riattivato lo switch, eseguire il comando **show test 1**.
5. Se l'output del comando mostra errori di diagnostica, spegnere e riaccendere lo switch (hard reset).
6. Dopo aver riattivato lo switch, eseguire nuovamente il comando **show test 1** e verificare se lo switch non ha superato i test di diagnostica.
7. Contatta il supporto tecnico Cisco sulla base dei tuoi commenti:Se lo switch non ha superato di nuovo i test diagnostici, è molto probabile che il Supervisor Engine abbia avuto esito negativo. Per ulteriori istruzioni, contattare il supporto tecnico Cisco.Se la diagnostica dello

switch non ha esito negativo dopo un reset a freddo, contattare il supporto tecnico Cisco fornendo le informazioni raccolte nelle altre fasi della procedura.**Nota:** se il supporto tecnico Cisco non è stato coinvolto durante la risoluzione dei problemi, è necessario fornire le informazioni nell'ordine in cui sono state documentate.

Dopo aver eseguito il reset a freddo, è necessario ripristinare la connettività di rete.

%SYS-4-P2_WARN: 1/Traffico non valido da indirizzo di origine multicast

Problema

Lo switch genera `traffico non valido da` messaggi di `indirizzi di origine multicast.`

Descrizione

Nell'esempio viene mostrato l'output syslog visualizzato quando si verifica questo errore:

```
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
```

Lo switch genera il messaggio syslog `Traffico non valido da indirizzo di origine multicast` quando riceve pacchetti con un indirizzo MAC multicast come indirizzo MAC di origine. L'uso di un indirizzo MAC broadcast o multicast come indirizzo MAC di origine per un frame non è conforme agli standard. Tuttavia, lo switch inoltra ancora il traffico che ha origine da un indirizzo MAC multicast.

Il messaggio syslog indica l'indirizzo MAC multicast nel campo MAC di origine del frame e la porta su cui è stato ricevuto il traffico.

Per risolvere il problema, provare a identificare la stazione terminale che genera i frame con un indirizzo MAC di origine multicast. In genere, uno di questi dispositivi trasmette tali frame:

- Generatore di traffico, ad esempio SmartBits
- Dispositivi di terze parti che condividono un indirizzo MAC multicast, ad esempio prodotti firewall o server per il bilanciamento del carico

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

Problema

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

Descrizione

Questo messaggio di errore indica che il Supervisor Engine ha perso la comunicazione con un componente su una scheda di linea. Il Supervisor Engine tiene traccia di tutti i timeout associati alla comunicazione. Le cause possibili sono numerose. Per ulteriori informazioni su questo messaggio di errore e sulle possibili cause, consultare il documento sulla descrizione e la risoluzione dei problemi di timeout di Astro/Lemans/NiceR sugli switch Catalyst serie 4000/4500

%SYS-4-P2_WARN: 1/Tag 0

Lo switch genera `%SYS-4-P2_WARN: 1/Tag 0...` messaggi.

Nell'esempio viene mostrato l'output syslog visualizzato quando si verifica questo errore:

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

Questo messaggio indica che è stato ricevuto un pacchetto con tag 802.1Q su una porta non trunk. La VLAN derivata dal tag del pacchetto è diversa dalla VLAN nativa della porta. Nel messaggio di errore:

- Il `tag [dec]` è l'identificatore VLAN del pacchetto.
- L'`[etere]` è l'indirizzo MAC dell'host.
- La `porta [chars]` è l'identificatore della porta.
- Il secondo `[dec]` è il numero di VLAN nativa.

È possibile che la porta locale non sia configurata correttamente come porta di accesso anziché come porta trunk. In alternativa, il lato remoto può essere configurato come porta trunk anziché come porta di accesso.

Verificare che la porta locale non sia configurata in modo errato come porta di accesso anziché come porta trunk. Verificare inoltre che il lato remoto non sia configurato come porta trunk anziché come porta di accesso.

convert_post_SAC_CiscoMIB:blocco Nvram [#] non convertibile

Problema

Lo switch genera periodicamente `convert_post_SAC_CiscoMIB:` messaggi syslog.

Descrizione

In questo esempio viene mostrato l'output della console visualizzato quando viene visualizzato questo messaggio:

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

Lo switch genera spesso questi messaggi della console quando si aggiornano o si downgrade le versioni del codice CatOS. L'errore può verificarsi anche quando si carica una configurazione di switch generata da un altro switch o quando si utilizza una configurazione di switch di un'altra versione del codice. Anche il failover sul Supervisor Engine di standby può generare questi messaggi.

Versioni diverse del codice contengono variabili archiviate nella NVRAM. Quando lo switch viene avviato con una versione successiva o precedente di CatOS, converte la configurazione precedente in una versione utilizzabile dall'immagine di avvio corrente. Durante questo processo, un particolare blocco di memoria non necessario o non utilizzabile nel modulo corrente viene deallocato anziché convertito. Questa funzione interna genera il messaggio di errore.

In genere questo messaggio è puramente informativo. Confrontare la configurazione precedente con la configurazione corrente per verificare che tutte le informazioni di configurazione siano state convertite correttamente.

Se questi messaggi vengono visualizzati senza aggiornamenti del codice, modifiche della configurazione o failover del Supervisor Engine, creare una richiesta di servizio (solo utenti registrati) con il supporto tecnico Cisco.

Errore checksum globale non riuscito

Problema

Questo messaggio di errore può essere visualizzato sugli switch Catalyst serie 4000/4500 e 6000/6500 con software Catalyst OS.

Il messaggio di errore `Checksum globale non riuscito` può essere visualizzato nell'output 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 messaggio correlato, `NVRAM: F`, può essere visualizzato nell'output 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.
```

Descrizione

L'errore di checksum globale indica che al successivo caricamento della casella, la NVRAM probabilmente verrà persa a causa di un errore di checksum CRC durante la lettura della configurazione. In genere non si tratta di un errore hardware, ma lo switch si corregge da solo. L'operazione non ha alcun impatto sullo switch a meno che non vengano apportate modifiche alla configurazione quando lo switch è in queste condizioni. Ma la maggior parte delle volte, un reset risolve il fallimento del checksum mentre viene ricalcolato. Questo problema è documentato nell'ID bug Cisco CSCdx87646 (solo utenti registrati).

Soluzione

Per ripristinare lo switch dallo stato di errore, completare i seguenti passaggi:

1. Eseguire il backup della configurazione dello switch. Per ulteriori informazioni sul supporto della configurazione, fare riferimento a Caricamento dei file di configurazione su un server TFTP.
2. Ripristinare il modulo Supervisor usando il comando **reset** ***supervisor_module_#***.
3. Una volta avviato lo switch, usare i comandi **show version** e **show test** per verificare se l'output è normale.
4. Verificare la configurazione esistente sullo switch e, se necessario, ripristinarla dal backup.

Informazioni correlate

- Guida ai messaggi di sistema - Switch della famiglia Catalyst, 7.4
- Configurazione di Log messaggi di sistema
- Messaggi di errore comuni di CatOS sugli switch Catalyst serie 5000/5500
- Messaggi di errore comuni di CatOS sugli switch Catalyst serie 6500/6000
- Decodificatore messaggi di errore (solo utenti registrati)
- Pagine di supporto dei prodotti LAN
- Pagina di supporto dello switching LAN
- Documentazione e supporto tecnico – Cisco Systems