

# Catalyst 4500/4000 Series 스위치의 일반적인 CatOS 오류 메시지

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[Catalyst 4500/4000 Series 스위치의 오류 메시지](#)

[%C4K\\_HWPORTMAN-4-BLOCKEDTXQUEUE:차단된 전송 큐 HwTxQId\[dec\]on \[char\], count=\[dec\]](#)

[%CDP-4-NVLANMISMATCH:포트 \[dec\]/\[dec\]에서 네이티브 VLAN 불일치 발견](#)

[DTP-1-ILGLCFG:포트 \[mod/port\]의 잘못된 구성\(on, isl—on.dot1q\)](#)

[%IP-3-UDP SOCKOVFL:UDP 소켓 오버플로](#)

[%IP-3-UDP BADCKSUM:UDP 잘못된 체크섬](#)

[%KERNEL-5-UNALIGNACCESS:맞춤 수정](#)

[%MCAST-4-RX\\_JNRANGE:IGMP:범위의 수신 보고서](#)

[MGMT-5-LOGIN\\_FAIL:사용자가 콘솔에서 로그인하지 못했습니다.](#)

[%PAGP-5-PORTFROMSTP / %PAGP-5-PORTTOSTP](#)

[%SPANTREE-3-PORTDEL\\_FAILNOTFOUND](#)

[%SYS-3-P2 ERROR:1/알 수 없는 모듈](#)

[%SYS-3-P2 ERROR:1/vbufs가 부족함\(내부 버퍼\)](#)

[%SYS-3-P2 ERROR:호스트 xx:xx:xx:xx:xx:xx:xx는 포트 간에 플래핑됩니다.](#)

[%SYS-4-P2 WARN:포트 \[char\]의 1/차단된 대기열\(tx\)](#)

[%SYS-4-P2 WARN:값 0의 1/필터링 이더넷 MAC 주소](#)

[%SYS-4-P2 WARN:1/잘못된 crc, 삭제된 패킷, 개수 = xx](#)

[%SYS-4-P2 WARN:멀티캐스트 소스 주소에서 보낸 1/유효하지 않은 트래픽](#)

[%SYS-4-P2 WARN:1/Astro\(mod/port\)](#)

[%SYS-4-P2 WARN:1/태그 0](#)

[convert\\_post SAC CiscoMIB:NVRAM 블록 \[#\]을\(를\) 변환할 수 없습니다.](#)

[글로벌 체크섬 실패 오류](#)

[관련 정보](#)

## 소개

이 문서에서는 Catalyst OS(CatOS) 소프트웨어를 실행하는 Cisco Catalyst 4500/4000 Series 스위치에 표시되는 공통 시스템 로그(syslog) 및 오류 메시지에 대해 간략하게 설명합니다.

이 문서에서 특정 오류 메시지에 대한 세부 정보를 찾을 수 없으면 [오류 메시지 디코더](#) ([등록된](#) 고객

만) 도구를 사용합니다. 이 도구는 Cisco IOS® 소프트웨어 및 CatOS 소프트웨어가 생성하는 오류 메시지의 의미를 제공합니다.

**참고:** 이 문서에서 설명하는 syslog 및 오류 메시지의 정확한 형식은 다를 수 있습니다. 변형은 스위치 Supervisor Engine에서 실행되는 소프트웨어 릴리스에 따라 달라집니다.

**참고:** Catalyst 4500/4000 시리즈 스위치의 권장 최소 로깅 컨피그레이션입니다.

- 스위치의 날짜 및 시간을 설정하거나 NTP 서버에서 날짜 및 시간을 가져오기 위해 NTP(Network Time Protocol)를 사용하도록 스위치를 구성합니다. **참고:** 스위치의 날짜 및 시간을 설정하려면 `set time` 명령을 실행합니다.
- 로깅 및 로깅 시간 스탬프가 활성화되어 있는지 확인합니다(기본값).
- 가능한 경우 syslog 서버에 로깅하도록 스위치를 구성합니다.

이 문서의 오류 메시지는 Catalyst 4500/4000 Series 스위치 및 이러한 스위치의 파생 제품(예: Catalyst 2948G, 2980G 및 4912G 스위치)에서 발생할 수 있습니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 또는 하드웨어 버전으로 제한되지 않습니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

## Catalyst 4500/4000 Series 스위치의 오류 메시지

### %C4K\_HWPORTMAN-4-BLOCKEDTXQUEUE: 차단된 전송 큐 HwTxQId[dec]on [char], count=[dec]

#### 문제

스위치에서 %C4K\_HWPORTMAN-4-BLOCKEDTXQUEUE: HwTxQId[dec]on[char], count=[dec] 오류를 생성합니다.

#### 설명

이 속도 제한 메시지는 포트의 전송 큐가 "일시 중지"가 아닌 이유로 차단되었음을 나타냅니다. 즉, 해당 포트의 트래픽이 제한되고 차단됩니다. 라인 카드에서 사용 중인 비트가 수신되어 Supervisor Engine에서 라인 카드로 패킷을 전송할 수 없는 경우 차단된 전송 큐 메시지가 표시됩니다. 잘못된 하드웨어 또는 속도/이중 불일치가 이 문제를 일으킬 수 있습니다. 해결 방법은 링크의 양쪽을 자동 협상을 구성하여 속도와 양방향을 지정하는 것입니다. 포트를 복구하려면 `shut/no shut` 명령을 실행

합니다. 문제가 계속되면 연결된 디바이스를 다른 포트로 이동하여 문제가 발생하는지 확인합니다. 전송(Tx) 큐의 차단을 해제하기 위한 최종 조치로 스위치를 재부팅하거나 라인 카드를 재설정하려면 `hw-module reset` 명령을 실행합니다.

## [%CDP-4-NVLANMISMATCH:포트 \[dec\]/\[dec\]에서 네이티브 VLAN 불일치 발견](#)

### 문제

스위치는 자주 `%CDP-4-NVLANMISMATCH syslog` 메시지를 생성합니다.

### 설명

다음 예에서는 스위치에서 이 오류 메시지가 발생할 때 표시되는 콘솔 출력을 보여 줍니다.

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

스위치 포트가 다른 스위치 또는 라우터에 물리적으로 연결될 때마다 스위치에서 이 메시지를 생성합니다. 포트의 구성된 네이티브 VLAN이 연결 스위치 또는 라우터 포트에 설정된 네이티브 VLAN과 다르기 때문에 스위치에서 이 메시지를 생성합니다.

IEEE 802.1Q 태깅을 사용하여 구성하는 트렁크 포트는 태그가 지정된 트래픽과 태그가 지정되지 않은 트래픽을 모두 수신할 수 있습니다. 기본적으로 스위치는 해당 포트에 대해 구성된 네이티브 VLAN으로 태그 없는 트래픽을 전달합니다. 패킷의 VLAN ID가 발신 포트 네이티브 VLAN ID와 동일한 경우 패킷은 태그가 지정되지 않은 상태로 전송됩니다. VLAN ID가 동일하지 않으면 스위치는 태그로 패킷을 전송합니다.

802.1Q 트렁크의 네이티브 VLAN이 트렁크 링크의 양쪽 끝에서 동일하지 확인합니다. 트렁크의 한 쪽 끝에 있는 네이티브 VLAN이 다른 쪽 끝에 있는 네이티브 VLAN과 다른 경우 양쪽 모두에 있는 네이티브 VLAN의 트래픽은 트렁크에서 올바르게 전송할 수 없습니다. 이 오류가 올바르게 전송되지 않을 경우 네트워크의 일부 연결 문제가 발생할 수 있습니다.

스위치에 구성된 네이티브 VLAN을 확인하려면 `show trunk mod/port` 명령을 실행합니다. 이 명령에서 `mod/port`는 트렁크 포트입니다. 다음은 명령의 샘플 출력입니다.

```
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)
```

트렁크 포트에 구성된 네이티브 VLAN을 변경하려면 `set vlan vlan-id mod/port` 명령을 실행합니다

.이 명령에서 *mod/port*는 트렁크 포트입니다.

## DTP-1-ILGLCFG:포트 [mod/port]의 잘못된 구성(on, isl—on,dot1q)

### 문제

스위치는 DTP-1-ILGLCFG . [mod/port] 오류 (on, isl—on,dot1q).

### 설명

이 메시지는 트렁크의 양쪽이 모두 on 설정되어 있지만 캡슐화 유형(isl, dot1q)이 일치하지 않을 경우 발생할 수 있습니다.트렁크 모드가 는 경우 컨피그레이션이 잘못되어 트렁크가 나타나지 않습니다.문제를 해결하려면 양쪽 끝에서 **show trunk** 명령의 출력을 확인합니다.캡슐화 유형이 동일한지 확인합니다.

## %IP-3-UDP SOCKOVFL:UDP 소켓 오버플로

### 문제

스위치가 주기적인 %IP-3-UDP SOCKOVFL:UDP syslog 메시지를 생성합니다.

### 설명

다음 예에서는 이 오류가 발생할 때 표시되는 콘솔 출력을 보여 줍니다.

**참고:** 표시되는 UDP(User Datagram Protocol) 소켓 번호는 다양하거나 일관되게 같을 수 있습니다.

```
%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
```

지정된 소켓(UDP 목적지 포트)의 수신 패킷에 할당된 버퍼가 꽉 찬 경우 스위치는 이 syslog 메시지를 생성합니다.해당 소켓으로 향하는 트래픽 비율이 너무 높기 때문에 버퍼가 꽉 찼습니다.예를 들어, 네트워크 관리 스테이션에서 많은 수의 SNMP(Simple Network Management Protocol) 쿼리를 보낼 때 이 상황이 발생할 수 있습니다.UDP 오버플로가 발생하면 SNMP 쿼리 수를 줄이십시오.다음 작업 중 하나를 수행합니다.

- 네트워크 관리 스테이션에서 폴링 간격을 늘립니다.
- 폴링되는 MIB 개체 수를 줄입니다.

이 섹션의 예에서 스위치는 목적지 UDP 소켓 2353을 사용하여 스위치 IP 주소(또는 브로드캐스트 주소)로 지정된 과도한 수의 패킷을 수신했습니다.스위치의 이 소켓에 대한 입력 버퍼가 꽉 찼기 때문에 스위치에서 syslog 메시지를 생성합니다.스위치가 오버플로 조건에 도달한 횟수를 확인하려면 **show netstat udp** 명령을 실행합니다.

이러한 syslog 메시지는 하나 이상의 스테이션이 지정된 대상 UDP 포트에서 스위치로 많은 양의 UDP 트래픽을 전송함을 나타냅니다.스위치에서 이러한 메시지 수가 너무 많으면 네트워크 분석기를 사용하여 트래픽의 소스를 식별하고 트래픽 속도를 줄입니다.자세한 내용은 [Catalyst SPAN\(Switched Port Analyzer\) 컨피그레이션 예](#)를 참조하십시오.

**참고:** 카운터가 대해서는 걱정하지 마십시오.이 카운터는 스위치가 수신한 UDP 패킷 중 존재하지 않는 포트로 향하는 패킷의 수를 표시합니다.

## [%IP-3-UDP\\_BADCKSUM:UDP 잘못된 체크섬](#)

### 문제

스위치가 주기적인 `%IP-3-UDP SOCKOVFL:UDP syslog` 메시지를 생성합니다.

### 설명

다음 예에서는 이 오류가 발생할 때 표시되는 콘솔 출력을 보여 줍니다.

**참고:** 표시되는 UDP 소켓 번호는 서로 다르거나 일관되게 같을 수 있습니다.

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

스위치가 SNMP 패킷과 같은 UDP 데이터그램에서 잘못된 체크섬을 탐지할 경우 이 syslog 메시지를 생성합니다.UDP 데이터그램 헤더는 전송 중에 데이터그램이 손상되었는지 확인하기 위해 수신 네트워크 디바이스가 검사하는 체크섬을 전달합니다.수신된 체크섬이 헤더의 체크섬 값과 일치하지 않으면 데이터그램이 삭제되고 오류 메시지가 기록됩니다.스위치가 잘못된 체크섬 데이터그램을 탐지한 횟수를 확인하려면 **show netstat udp** 명령을 실행합니다.

```
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
```

이 메시지는 정보 제공용입니다.잘못된 패킷을 스위치에 전송하는 네트워크 장치로 인해 이 메시지가 발생합니다.트래픽의 소스를 식별하려면 네트워크 분석기를 사용합니다.자세한 내용은 [Catalyst SPAN\(Switched Port Analyzer\) 컨피그레이션 예](#)를 참조하십시오.

**참고:** 카운터가 대해서는 걱정하지 마십시오.이 카운터는 스위치가 수신한 UDP 패킷 중 존재하지 않는 포트로 향하는 패킷의 수를 표시합니다.

## [%KERNEL-5-UNALIGNACCESS:맞춤 수정](#)

### 문제

스위치가 주기적으로 `%KERNEL-5-UNALIGNACCESS:Alignment correction syslog` 메시지를 생성합니다.

### 설명

다음 예에서는 이 오류가 발생할 때 표시되는 syslog 출력을 보여 줍니다.

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

이러한 syslog 메시지는 스위치가 DRAM의 데이터에 액세스하려고 할 때 스위치 CPU가 정렬 오류를 탐지하고 수정했음을 나타냅니다. 이러한 메시지는 정보 제공용으로만 제공됩니다. 메시지는 스위치에 문제가 있음을 나타내지 않으며 시스템 성능에 영향을 미치지 않습니다.

경우에 따라 이러한 메시지의 수가 너무 많습니다. 예를 들어, 이러한 메시지는 syslog 서버 로그 파일 또는 스위치 콘솔을 플러딩할 수 있습니다. 메시지가 너무 많을 경우 소프트웨어 릴리스 트레인의 최신 유지 보수 릴리스로 스위치 소프트웨어를 업그레이드하는 것이 좋습니다. 또는 **set logging level kernel 4 default** 명령을 실행하여 kernel facility의 로깅 레벨을 4 이하로 수정합니다.

최신 유지 보수 릴리스로 업그레이드하지만 이러한 syslog 메시지가 계속 수신되는 경우 [Cisco 기술 지원](#)을 통해 [서비스 요청](#)(등록된 고객만 해당)을 생성합니다.

## [%MCAST-4-RX\\_JNRANGE:IGMP:범위의 수신 보고서](#)

### 문제

IGMP(Internet Group Management Protocol) 스누핑이 활성화된 스위치에는 %MCAST-4-RX\_JNRANGE:IGMP:01-00-5e-00-00-xx 오류 메시지 Rcvd Report.

### 설명

다음 예에서는 이 오류가 발생할 때 표시되는 syslog 출력을 보여 줍니다.

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

syslog 메시지 Rcvd Report는 정보 제공용입니다. 스위치에서 01-00-5e-00-00-xx로 시작하는 멀티캐스트 MAC 주소가 포함된 IGMP 보고서 패킷을 수신할 때 이 메시지가 생성됩니다. 이 L2(Layer 2) 주소 범위는 224.0.0.0~224.0.0.255 사이의 L3(Layer 3) 멀티캐스트 주소 범위와 같습니다. 이러한 주소는 라우팅 프로토콜 및 기타 낮은 수준의 토폴로지 검색 또는 유지 관리 프로토콜을 사용하기 위해 예약됩니다. 이러한 프로토콜의 예로는 게이트웨이 검색 및 그룹 멤버십 보고 등이 있습니다.

패킷 캡처 툴(예: 스니퍼)을 사용하고 IGMP 메시지를 필터링하여 이 문제를 해결합니다. 또한 Catalyst SPAN 기능을 사용하여 네트워크 디바이스에서 이러한 메시지를 수신하는 것으로 의심되는 포트에서 패킷을 복사할 수 있습니다. 이러한 메시지를 억제하려면 set logging level **멀티캐스트 2 default** 명령을 실행합니다. 이 명령은 멀티캐스트 메시지의 로깅 레벨을 2로 변경합니다.

show multicast router 명령에서 표시하는 포트 및 네트워크의 코어에 대한 업링크를 SPAN 소스 포트에 사용합니다. 이러한 포트가 트렁크 포트인 경우 SPAN 목적지 포트도 트렁크 포트에 구성합니다. 포트가 **트렁크** 포트인지 확인하려면 show trunk 명령을 실행합니다.

## [MGMT-5-LOGIN\\_FAIL:사용자가 콘솔에서 로그인하지 못했습니다.](#)

### 문제

스위치에서 MGMT-5-LOGIN\_FAIL: 오류 .

### 설명

이 메시지는 스위치의 콘솔 포트에 연결된 터미널 서버에 문제가 있음을 나타낼 수 있습니다. 스위

치 콘솔이 터미널 서버의 비동기 회선에 연결되고 스위치에서 소프트 리셋을 수행하면 가비지(임의의 텍스트)가 몇 분 동안 화면을 스트리밍합니다.스위치에서 TACACS가 활성화된 경우, TACACS는 버퍼를 버퍼링하고 가비지 조각을 하나씩 처리하므로 몇 분이 며칠이 될 수 있습니다. 해결 방법은 스위치가 연결되는 비동기 회선에서 no exec 명령을 실행하는 것입니다.

**참고:** no exec 명령을 실행한 후에도 버퍼가 지워질 때까지 메시지가 계속됩니다.

**참고:** 오류 메시지 %MGMT-5-LOGIN\_FAIL:User . . . 스위치에 텔넷할 수 있는 사용자 수를 제한해 보십시오.

## [%PAGP-5-PORTFROMSTP / %PAGP-5-PORTTOSTP](#)

### 문제

스위치는 자주 %PAGP-5-PORTFROMSTP 및 %PAGP-5-PORTTOSTP syslog 메시지를 생성합니다.

### 설명

다음 예에서는 스위치가 다음 syslog 메시지를 생성할 때 표시되는 콘솔 출력을 보여 줍니다.

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

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

PAGP(Port Aggregation Protocol) 로깅 기능은 PAGP와 관련된 이벤트를 보고합니다.PAGP를 사용하여 스위치 간 EtherChannel 링크를 협상합니다.스위치 포트의 링크가 손실되면 스위치 %PAGP-5-PORTFROMSTP syslog 메시지가 생성됩니다.스위치는 스위치 포트에서 링크 탐지할 때 %PAGP-5-PORTTOSTP syslog 메시지를 생성합니다.이러한 syslog 메시지는 스페닝 트리에서 포트를 추가 또는 제거했음을 나타내는 일반 정보 메시지입니다.

**참고:** 이러한 메시지를 표시하려면 채널링을 활성화할 필요가 없습니다.

이 섹션의 예에서 스위치는 먼저 포트 3/3의 링크를 손실했으며, 이는 스페닝 트리에서 포트를 제거했습니다.그런 다음 스위치에서 포트 링크를 다시 감지하여 스페닝 트리에 포트를 다시 추가했습니다.

특정 포트에 대해 이러한 메시지가 자주 표시되면 링크가 플래핑됩니다. 즉 링크가 계속 손실되고 다시 복구됩니다.원인을 조사합니다.스위치 포트에서 링크 플랩의 일반적인 원인은 다음과 같습니다.

- 속도/이중 불일치
- 케이블 오류
- NIC(Network Interface Card) 오류 또는 기타 엔드 스테이션 문제
- 스위치 포트 오류
- 기타 컨피그레이션 오류

이러한 syslog 메시지를 억제하려면 set logging level pagp 4 default 명령을 실행하여 PAGP 기능에 대한 로깅 레벨을 4 이하로 수정합니다.PAGP의 기본 로깅 레벨은 5입니다.

## [%SPANTREE-3-PORTDEL\\_FAILNOTFOUND](#)

### 문제

스위치가 주기적인 %SPANTREE-3-PORTDEL\_FAILNOTFOUND syslog 메시지를 생성합니다.

## 설명

다음 예에서는 이 오류가 발생할 때 표시되는 syslog 출력을 보여 줍니다.

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

이러한 syslog 메시지는 PAgP가 지정된 VLAN에 대한 스페닝 트리에서 포트를 제거하려고 했지만 포트가 해당 VLAN에 대한 스페닝 트리 데이터 구조에 있지 않았음을 나타냅니다.일반적으로 DTP(Dynamic Trunking Protocol)와 같은 다른 프로세스는 스페닝 트리에서 포트를 이미 제거했습니다.

이러한 메시지는 일반적으로 %PAGP-5-PORTFROMSTP 메시지 제공됩니다.이 메시지는 디버깅용입니다.메시지는 스위치에 문제가 있음을 나타내지 않으며 스위칭 성능에 영향을 미치지 않습니다.또한 기본 SPANTREE 기능 로깅 컨피그레이션을 변경하지 않는 한 이러한 메시지 기록되지 않습니다.SPANTREE의 기본 로깅 레벨 2입니다.

경우에 따라 이러한 메시지의 수가 너무 많습니다.예를 들어 이러한 메시지는 스위치 콘솔을 풀러딩할 수 있습니다.메시지가 너무 많을 경우 소프트웨어 릴리스 트레인의 최신 유지 보수 릴리스로 스위치 소프트웨어를 업그레이드하는 것이 좋습니다.이후 소프트웨어 릴리스는 대부분의 경우 이러한 메시지를 표시하지 않습니다.

## [%SYS-3-P2\\_ERROR:1/알 수 없는 모듈](#)

### 문제

%SYS-3-P2\_ERROR:1/Unknown module 오류 메시지는 Catalyst 4500/4000 series 스위치에 새 스위칭 모듈을 설치할 때 표시됩니다.

### 설명

다음 예에서는 이 오류가 발생할 때 표시되는 콘솔 출력을 보여 줍니다.

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

%SYS-3-P2\_ERROR:1/ 오류는 현재 Supervisor Engine에서 실행되는 소프트웨어 이미지 버전이 삽입한 하드웨어 구성 요소를 지원하지 않을 때 발생합니다.

이 예에서는 CatOS 소프트웨어 릴리스 4.4(1)를 실행하는 Catalyst 4500/4000 스위치에 18포트 1000BASE-X 서버 스위칭 모듈(WS-X4418)을 삽입합니다. WS-X4418 모듈에는 최소 4.5(1)의 소프트웨어 릴리스가 필요합니다.

해결 방법은 Supervisor Engine 소프트웨어 버전을 하드웨어를 지원하는 소프트웨어 릴리스로 업그레이드하는 것입니다.각 모듈의 최소 소프트웨어 버전 목록은 [Catalyst 4500 Series 스위치](#)의 릴리스 정보를 참조하십시오.

## [%SYS-3-P2\\_ERROR:1/vbufs가 부족함\(내부 버퍼\)](#)

### 문제



스위치에서 %SYS-3-P2\_ERROR .1/여러 호스트 동시에 또는 동시에 켜지는 경우 vbufs 메시지가 을 나타냅니다.

## 설명

다음 예에서는 오류가 발생할 때 표시되는 콘솔 출력을 보여 줍니다.

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

%SYS-3-P2\_ERROR:1/vbufs( )가 여러 호스트 전원을 동시에 켜면 오류가 발생할 수 있습니다.호스트의 전원이 켜지면 더 이상 오류가 나타나지 않습니다.

이러한 오류는 Catalyst 기능으로 트래픽을 전환하도록 중단시키지 않습니다.메시지는 정보 제공용으로만 제공됩니다.

## [%SYS-3-P2\\_ERROR:호스트 xx:xx:xx:xx:xx:xx는 포트 간에 플래핑됩니다.](#)

## 문제

스위치에서 %SYS-3-P2\_ERROR . xx:xx:xx:xx:xx:xx ... 메시지에서 xx:xx:xx:xx:xx:xx는 MAC 주소입니다.

## 설명

다음 예에서는 이 오류가 발생할 때 표시되는 콘솔 출력을 보여 줍니다.

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

이 오류 메시지의 원인을 파악하고 문제를 해결하려면 이 섹션의 단계와 지침을 사용하십시오.

이 메시지는 Catalyst 4500/4000 스위치가 원래 주소가 아닌 다른 포트에서 CAM(content-addressable memory) 테이블에 이미 있는 MAC 주소를 학습했음을 나타냅니다.이러한 동작은 짧은 시간 동안 반복적으로 발생하며, 이는 포트 간에 주소 플래핑이 있음을 의미합니다.

여러 MAC 주소에 대해 메시지가 나타나면 정상적인 동작이 아닙니다.이 동작은 MAC 주소가 기본 에이징 시간 전에 한 포트에서 다른 포트로 빠르게 이동하므로 가능한 네트워크 문제를 나타냅니다.이 문제는 네트워크에서 트래픽을 루핑하는 것일 수 있습니다.다음과 같은 일반적인 증상이 있습니다.

- 높은 CPU 사용률
- 네트워크 전체에서 느린 트래픽
- 스위치의 높은 백플레인 사용률

스패닝 트리의 문제를 식별하고 해결하는 방법에 대한 자세한 내용은 스패닝 트리 [프로토콜 문제 및 관련 설계 고려 사항을 참조하십시오.](#)

하나 또는 두 개의 MAC 주소에 대한 오류 메시지가 나타나면 원인을 확인하기 위해 이러한 MAC 주소를 찾습니다.`show cam mac_addr` 명령을 실행하여 이러한 MAC 주소가 학습된 위치를 식별합니다.이 명령에서 `mac_addr`은 오류가 플래핑으로 보고하는 MAC 주소입니다.

이 MAC 주소가 플래핑하는 포트 사이를 확인한 후 MAC 주소를 추적합니다.Catalyst 4500/4000과

문제가 있는 MAC 주소가 있는 디바이스 간의 중간 디바이스에 연결합니다. 소스 및 이 디바이스가 네트워크에 연결되는 방법을 식별할 수 있을 때까지 이 작업을 수행합니다.

**참고:** MAC 주소가 두 포트 간에 플래핑되므로 두 경로를 모두 추적합니다.

다음 예에서는 이 MAC 주소가 학습된 두 경로를 모두 추적하는 방법을 보여 줍니다.

**참고:** 이 메시지를 수신했으며 조사를 시작했다고 가정합니다.

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

이 MAC 주소가 두 포트에서 학습된 방법을 추적하려면 다음 단계를 완료하십시오.

1. 포트 1/2를 먼저 고려하고 **show cam dynamic 1/2** 명령을 실행합니다. 이 포트에서 학습된 MAC 주소 목록에 MAC 주소 00:50:0f:20:08:00이 표시되면, 이 호스트가 연결된 단일 호스트 인지 또는 해당 포트에 등록된 여러 호스트가 있는지 확인합니다.
2. 단일 또는 다중 호스트가 있는지 여부에 따라 디바이스를 조사합니다. 연결된 단일 호스트 (00:50:0f:20:08:00)가 있는 경우 등록된 다른 포트를 확인하고 호스트가 스위치에 이중으로 연결되어 있는지 확인합니다. 이 예에서 다른 포트는 포트 4/39입니다. 호스트에 이 스위치로 다시 연결될 수 있는 다른 디바이스에 대한 연결이 있는 경우 중간 디바이스를 추적하십시오. Cisco 디바이스에서 **show cdp neighbors mod/port detail** 명령을 실행합니다. 출력에서는 중간 장치에 대한 정보를 제공합니다. 다음은 샘플 출력입니다.

```
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. 디바이스와 텔넷 세션을 설정하고 MAC 주소의 경로를 따릅니다. 이 예에서는 IP 주소가 172.16.1.1입니다. 오류 메시지가 플래핑으로 보고하는 모든 MAC 주소에 대해 절차를 반복합니다.
4. 해당 MAC 주소와 이 MAC 주소가 플래핑되는 물리적 연결(Catalyst 4500/4000 포트)을 사용하여 소스 디바이스의 간단한 다이어그램을 만듭니다. 다이어그램에서는 이 포트가 네트워크 레이아웃의 유효한 포트와 경로인지 확인할 수 있습니다. MAC 주소가 플래핑되는 두 포트가 모두 해당 네트워크 노드를 향하는 경로를 제공하는지 확인하면 스페닝 트리 오류 문제가 발

생할 가능성이 있습니다. 이 루프를 [격리하고](#) 트러블슈팅하려면 스페닝 트리 프로토콜 [문제 및 관련 설계 고려 사항](#)을 참조하십시오. 여러 벤더의 여러 호스트가 상호 연결되는 대규모 네트워크에서는 MAC 주소만 사용하여 호스트를 추적하려고 할 때 어려움이 발생합니다. [IEEE OUI 및 Company id 할당](#)에 대한 검색 유틸리티를 사용하여 이러한 MAC 주소를 추적할 수 있습니다. 이 목록은 IEEE가 모든 공급업체에 할당된 모든 MAC 주소를 등록한 데이터베이스의 프런트 엔드입니다. Search for(검색 대상)에 MAC 주소의 처음 세 8진수를 **입력합니다**. 이 장치와 연결된 판매업체를 찾기 위한 이 페이지의 필드입니다. 이 예에서 처음 세 8진수는 00:50:0f입니다.

다음은 이 메시지를 표시할 수 있는 기타 문제입니다.

- **Server NIC redundancy problem(서버 NIC 이중화 문제)** - 동작하지 않고 표준을 따르지 않는 이중 연결 NIC가 있는 서버가 있습니다. 서버는 동일한 스위치에 연결하는 두 포트에 동일한 MAC 주소를 사용합니다.
- **HSRP(Hot Standby Router Protocol) 플랩** - HSRP를 플랩하면 이러한 메시지가 Supervisor Engine 콘솔에 나타날 수 있습니다. 네트워크에서 HSRP 구현이 불안정하다는 것을 알게 되면 Catalyst 스위치 네트워크 [의 HSRP 문제 이해 및 문제 해결](#)을 참조하여 문제를 해결하십시오.
- **EtherChannel 컨피그레이션 오류** - EtherChannel 연결이 잘못 구성되면 이러한 증상이 발생할 수 있습니다. 플래핑 메시지가 보고하는 포트가 동일한 채널 그룹의 멤버인 경우 EtherChannel 컨피그레이션을 확인하고 컨피그레이션 트러블슈팅을 위해 EtherChannel [Load Balancing and Redundancy on Catalyst Switches](#)를 참조하십시오.
- **호스트는 패킷을 다시 네트워크로 반영** - 호스트에 의해 네트워크로 다시 리플렉션하면 플래핑도 발생할 수 있습니다. 일반적으로 이 패킷 리플렉션의 근본 원인은 손상된 NIC 또는 포트에 연결된 호스트의 물리적 인터페이스 장애입니다. 호스트에 의한 패킷 리플렉션이 근본 원인 경우 스니퍼 추적을 얻어 메시지가 나타나는 포트를 오가는 트래픽을 검사합니다. 호스트가 패킷을 반영하는 경우 일반적으로 추적에서 중복 패킷을 볼 수 있습니다. 중복 패킷은 이 MAC 주소 플래핑의 증상일 수 있습니다. 스니퍼와 함께 사용할 포트를 구성하는 방법에 대한 자세한 내용은 [SPAN 및 RSPAN](#) 구성을 참조하십시오.
- **소프트웨어 또는 하드웨어 결함**—이 섹션의 지침에 따라 플래핑 메시지를 해결하려고 했지만 여전히 문제가 발생한 경우 [Cisco 기술 지원](#)에서 추가 지원을 [받으십시오](#). 이 단계를 수행하는 동안 수집한 정보에 대한 문서를 반드시 언급하고 제공해야 합니다. 이 정보를 통해 더 신속하게 문제를 해결하고 더 효율적으로 문제를 해결할 수 있습니다.

## [%SYS-4-P2\\_WARN:포트 \[char\]의 1/차단된 대기열\(tx\)](#)

### 문제

스위치는 [char] 메시지 Blocked queue(tx) 생성합니다.

### 설명

다음 예에서는 오류가 발생할 때 표시되는 syslog 출력을 보여 줍니다.

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

이러한 오류는 하드웨어 문제 또는 다음 문제 중 하나를 나타냅니다.

- 듀플렉스 불일치

- 케이블 오류
- 유형 1 케이블 연결
- 결함이 있는 포트
- 외부 연결 장치의 하드웨어 문제

이러한 오류의 가장 일반적인 원인은 물리적 레이어 문제입니다. 이 문제로 인해 내부 K1 기가비트 포트에서 상당한 양의 트래픽이 백업됩니다. K1 ASIC(application-specific integrated circuit)는 스위치를 제어하는 주 칩입니다. 일반적으로 컨피그레이션 문제 또는 케이블 손상으로 인해 차단된 Tx 큐 카운트가 증가합니다.

일반 환경에서는 Tx 큐를 약 20초 동안만 차단할 수 있습니다. 차단 시간이 길어지면 심각한 문제가 발생합니다. 따라서 Tx 큐가 35초 내에 기가포트 동안 드레이트되지 않은 경우 차단된 Tx 큐 카운트가 증가합니다.

필요한 경우 [Cisco Technical Support](#)에 문의하여 모듈을 교체해야 하는지 확인하십시오. 그러나 먼저 모듈을 다시 장착하고 오류 메시지가 여전히 있는지 확인합니다.

다음은 Gigabit <gigaport\_number>의 Catalyst 4000/2948G/2980G Blocked Queue를 Front Panel Switch Ports(전면 패널 스위치 포트)에 매핑하는 단계이며, 다시 연결해야 합니다.

**샘플 오류 메시지:**

```
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 )
```

이 오류 메시지는 물리적 레이어 문제 또는 gigaport 29와 관련된 이중 불일치로 인해 발생하는 구성 오류가 있음을 나타냅니다. gigaport 29와 관련된 포트를 찾으려면 다음 표를 참조하십시오. 테이블은 Supervisor Engine에 따라 다르며 달라집니다.

**WS-X4013 Gigabit Kirky 포트 매핑**

K1-A(기가비트 0-11)

기가포트 0	업링크 0(포트 1/1) 또는 내부 인터커넥트 K1-C
기가포트 1	슬롯 6 - 기가비트 인터커넥트 5
기가포트 2	슬롯 5 - Gigabit Interconnect 5
기가포트 3	슬롯 2 - 기가비트 인터커넥트 5
기가포트 4	슬롯 3 - Gigabit Interconnect 5
기가포트 5	슬롯 4 - 기가비트 인터커넥트 5
기가포트 6	슬롯 4 - 기가비트 인터커넥트 4
기가포트 7	슬롯 3 - Gigabit Interconnect 4
기가포트 8	슬롯 2 - 기가비트 인터커넥트 4
기가포트 9	슬롯 5 - 기가비트 인터커넥트 4
기가포트 10	슬롯 6 - 기가비트 인터커넥트 4
기가포트 11	내부 상호 연결 K1-B

K1-B(기가비트 12-23)

기가포트 12	내부 상호 연결 K1-A
기가포트 13	슬롯 6 - 기가비트 인터커넥트 3
기가포트 14	슬롯 5 - Gigabit Interconnect 3
기가포트 15	슬롯 2 - Gigabit Interconnect 3
기가포트 16	슬롯 3 - Gigabit Interconnect 3
기가포트 17	슬롯 4 - 기가비트 인터커넥트 3
기가포트 18	슬롯 4 - 기가비트 인터커넥트 2
기가포트 19	슬롯 3 - 기가비트 인터커넥트 2
기가포트 20	슬롯 2 - 기가비트 인터커넥트 2
기가포트 21	슬롯 5 - 기가비트 인터커넥트 2
기가포트 22	슬롯 6 - 기가비트 인터커넥트 2
기가포트 23	내부 상호 연결 K1-C

K1-C(기가비트 24-35)

기가포트 24	K1-B에 대한 내부 상호 연결
기가포트 25	슬롯 6 - 기가비트 인터커넥트 1
기가포트 26	슬롯 5 - 기가비트 인터커넥트 1
기가포트 27	슬롯 2 - 기가비트 인터커넥트 1
기가포트 28	슬롯 3 - 기가비트 인터커넥트 1
기가포트 29	슬롯 4 - 기가비트 인터커넥트 1
기가포트 30	슬롯 4 - 기가비트 인터커넥트 0
기가포트 31	슬롯 3 - Gigabit Interconnect 0
기가포트 32	슬롯 2 - 기가비트 인터커넥트 0
기가포트 33	슬롯 5 - Gigabit Interconnect 0
기가포트 34	슬롯 6 - 기가비트 인터커넥트 0
기가포트 35	K1-A에 대한 업링크 1(포트 1/2) 또는 내부 인터커넥트

각 K1 ASIC에는 12기가비트 인터커넥트가 있습니다. 이러한 기가비트 인터커넥트는 라인 카드와 수퍼바이저 엔진 사이에 직렬 포인트-투-포인트 링크로 사용됩니다. Catalyst 4000의 각 라인 카드는 12기가비트 인터커넥트 중 6개에 연결됩니다. 기가비트 인터커넥트는 0에서 5로 참조되며 역순으로 연결됩니다. 예를 들어, 4148 라인 카드의 기가비트 상호 연결 5는 포트 1-8에 연결되고 기가비트 상호 연결 4는 포트 9-16에 연결됩니다.

**Line Module Interconnect 포트 매핑**

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

포트	기가비트 인터커넥트
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

포트	기가비트 인터커넥트
1	5
2	4
3-10	3
11-18	2
19-26	1
27-34	0

WS-X4418-GB

포트	기가비트 인터커넥트
1	5
2	4
3-6	3
7-10	2
11-14	1
15-18	0

WS-X4124-FX-MT

포트	기가비트 인터커넥트
1-4	5
5-8	4
9-12	3
13-16	2
17-20	1
21-24	0

WS-X4306-GB

포트	기가비트 인터커넥트
1	5
2	4
3	3
4	2
5	1
6	0

WS—X4412-2GB-TX

포트	기가비트 인터커넥트
1-2	5
3-4	4
5-6	3
7-8	2
9-10	1
11-12	0

## 의심스러운 포트 찾기 예

```
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 )
```

Gigabit 16은 슬롯 3, 기가비트 인터커넥트 3을 나타냅니다. 슬롯 3은 WS-X4232-L3이므로 기가비트 인터커넥트 3은 포트 3-10을 참조합니다. 이러한 포트를 트러블슈팅할 때 **show port**, **show mac** 및 **show counters** 명령을 사용하는 오류 및/또는 듀플렉스 불일치를 확인합니다. 또한 **덤프 1**을 가져와서 포트와 관련된 하드웨어 오류가 있는지 확인하는 것도 유용합니다. 덤프 1 출력의 한 가지 주목할 만한 참조는 해당 상호 연결을 위해 라인 모듈 ASIC와 연결된 cscTimeout입니다 .cscTimeout의 값은 0이어야 합니다.

## [%SYS-4-P2 WARN:값 0의 1/필터링 이더넷 MAC 주소](#)

### 문제

스위치는 0 메시지 MAC 생성합니다.

### 설명

다음 예에서는 이 오류가 발생할 때 표시되는 syslog 출력을 보여 줍니다.

```
%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
```

소스 MAC 주소 00-00-00-00-00-00-00의 패킷을 스위치가 수신할 경우 스위치는 0 syslog 메시지의 MAC 생성합니다. 이 MAC 주소는 잘못된 소스 MAC입니다.

syslog 메시지는 스위치가 잘못된 주소를 배우기를 거부함을 나타냅니다. 그러나 스위치는 all-zero MAC 주소에서 오는 트래픽을 전달합니다.

해결 방법은 모두 0인 소스 MAC 주소가 있는 프레임을 생성하는 엔드 스테이션을 식별하는 것입니다. 일반적으로 다음 디바이스 중 하나가 이러한 프레임을 전송합니다.

- 트래픽 생성기(예: Spient SmartBits)
- IBM WebSphere 서버 로드 밸런싱 등 특정 유형의 서버
- all-zeros 브로드캐스트를 전송하는 디바이스와 같이 잘못 구성된 라우터 또는 엔드 스테이션
- 결함이 있는 NIC

## [%SYS-4-P2\\_WARN:1/잘못된 crc, 삭제된 패킷, 개수 = xx](#)

### 문제

Supervisor Engine II(WS-X4013=)를 사용하는 스위치는 이 섹션에 표시되는 메시지를 생성하며 네트워크 연결의 일부 또는 전체 손실이 발생합니다. 연결이 끊기면 스위치 포트의 일부에만 영향을 줄 수 있으며 업링크 포트가 포함될 수 있습니다.

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

### 설명

다음 예에서는 이 오류가 발생할 때 표시되는 syslog 또는 콘솔 출력을 보여 줍니다.

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

때때로 다음과 같은 메시지가 표시됩니다.

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

**참고:** %SYS-4-P2\_WARN :1/Astro(3/4) - . [%SYS-4-P2\\_WARN:0](#) 문서의 [1/Astro\(mod/port\)](#) 섹션

**참고:** 이러한 메시지가 나타나면 네트워크 연결 문제가 발생할 수 있습니다.

다음 문제 해결 단계를 따라 각 단계에서 명령 출력을 캡처합니다.

**참고:** [문제 해결에](#) 대한 도움이 필요하면 [Cisco 기술 지원](#)에 문의하십시오.

1. 다음 명령을 실행합니다. `show logging buffer -1023` 기술 지원 표시상태 1 표시덤프 1



## 2. 이러한 명령 중 하나를 무작위로 다섯 번 실행하고 InvalidPacketBufferCrcs 카운터를 `.show nvramenv 1`—CatOS 소프트웨어 릴리스 6.1(1) 이상

```
Cat4k> (enable) show nvramenv 1
```

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

## `show env 1`—CatOS 소프트웨어 릴리스 5.5(19) 이전 명령을 반복할 때 InvalidPacketBufferCrcs 카운터가 높은 값에 의해 빠르게 증가하는지 확인합니다.

```
cat4k> (enable) show nvramenv 1
```

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

**참고:** 출력에 InvalidPacketBufferCrcs가 적은 의 경우 5.5.10, 6.2.3 또는 6.3.1 이전 버전의 CatOS 소프트웨어 버전을 실행하면 최신 릴리스로 업그레이드합니다. Cisco 버그 ID CSCdu48749 ([등록된 고객만 해당](#)) 및 CSCdt80707 ([등록된 고객만 해당](#)) 이 발생할 수 있습니다. [필드 알림](#)을 참조하십시오. [Catalyst 4000 포트에서 활성 VLAN 상태가 손실되어](#) 추가 정보를 위해 [패킷 손실이](#) 발생합니다.

## 3. InvalidPacketBufferCrcs 카운터 높은 속도로 증가하면 `reset` 명령을 실행하여 스위치를 소프트웨어 리셋합니다. **참고:** 이 단계에서 출력 캡처가 중요합니다.

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

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

```
nodcswnml> (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"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
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. 스위치가 다시 온라인 상태가 되면 **show test 1** 명령을 실행합니다.
5. 명령 출력에 진단 오류가 표시되면 스위치를 전원 껐다가 다시 켜십시오.
6. 스위치가 다시 온라인 상태가 되면 **show test 1** 명령을 다시 실행하여 스위치가 진단 테스트에 실패했는지 확인합니다.
7. [Cisco 기술 지원](#)에 문의하시기 바랍니다. 스위치가 진단 테스트를 다시 통과하지 못하면 수퍼 바이저 엔진이 실패할 가능성이 높습니다. 자세한 내용은 [Cisco 기술 지원](#)에 문의하십시오. 스위치가 하드 리셋에 대한 진단 유틸리티에 실패하지 않을 경우 [Cisco 기술 지원](#)에 이 절차의 다른 단계에서 수집한 정보를 문의하십시오. **참고:** 트러블슈팅 중에 Cisco Technical Support가 참여하지 않은 경우 문서화된 순서대로 정보를 제공해야 합니다.

하드 리셋을 수행한 후 네트워크 연결을 복원해야 합니다.

## [%SYS-4-P2 WARN:멀티캐스트 소스 주소에서 보낸 1/유효하지 않은 트래픽](#)

### 문제

스위치는 멀티캐스트 메시지 `Invalid` 생성합니다.

### 설명

다음 예에서는 이 오류가 발생할 때 표시되는 syslog 출력을 보여 줍니다.

```

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

```

스위치가 멀티캐스트 MAC 주소를 소스 MAC로 패킷을 수신할 때 스위치는 멀티캐스트 소스 syslog 메시지에서 `Invalid traffic from`을 생성합니다. 프레임에 대한 소스 MAC로 브로드캐스트 또는 멀티캐스트 MAC 주소를 사용하는 것은 표준 준수 동작이 아닙니다. 그러나 스위치는 멀티캐스트 MAC 주소에서 소싱된 트래픽을 여전히 전달합니다.

syslog 메시지는 프레임의 소스 MAC 필드에 있는 멀티캐스트 MAC 주소와 트래픽을 수신한 포트

를 나타냅니다.

해결 방법은 멀티캐스트 소스 MAC 주소로 프레임을 생성하는 엔드 스테이션을 식별하는 것입니다. 일반적으로 다음 디바이스 중 하나가 이러한 프레임을 전송합니다.

- SmartBits와 같은 트래픽 생성기
- 로드 밸런싱 방화벽 또는 서버 제품과 같은 멀티캐스트 MAC 주소를 공유하는 서드파티 디바이스

## [%SYS-4-P2\\_WARN:1/Astro\(mod/port\)](#)

### 문제

스위치에서 %SYS-4-P2\_WARN .1/Astro(6/6).. 메시지

### 설명

이 오류 메시지는 Supervisor Engine에서 라인 카드의 구성 요소에 대한 통신이 끊겼음을 나타냅니다. Supervisor Engine은 이 통신과 연결된 시간 제한을 추적합니다. 이 상태의 가능한 원인은 많습니다. 이 오류 메시지 및 가능한 원인에 대한 자세한 내용은 [Catalyst 4000/4500 Series 스위치의 Astro/Lemans/NiceR 시간 초과 이해 및 문제 해결을 참조하십시오.](#)

## [%SYS-4-P2\\_WARN:1/태그 0](#)

스위치에서 %SYS-4-P2\_WARN .1/ 0. 메시지

다음 예에서는 이 오류가 발생할 때 표시되는 syslog 출력을 보여 줍니다.

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

이 메시지는 802.1Q 태그 패킷이 트렁크 포트가 아닌 포트에서 수신되었음을 나타냅니다. 패킷 태그에서 파생된 VLAN은 포트 네이티브 VLAN과 다릅니다. 오류 메시지에서:

- Tag [dec]는 패킷의 VLAN 식별자입니다.
- [ether]는 호스트 MAC 주소입니다.
- [chars] 포트는 포트 식별자입니다.
- 두 번째 [dec]는 네이티브 VLAN 번호입니다.

로컬 포트가 트렁크 포트 대신 액세스 포트에 잘못 구성되었을 가능성이 있습니다. 또는 원격 측은 액세스 포트 대신 트렁크 포트에 구성할 수 있습니다.

로컬 포트가 트렁크 포트 대신 액세스 포트에 잘못 구성되지 않았는지 확인합니다. 또한 원격 쪽이 액세스 포트 대신 트렁크 포트에 구성되지 않았는지 확인합니다.

## [convert\\_post\\_SAC CiscoMIB:NVRAM 블록 \[#\]을\(를\) 변환할 수 없습니다.](#)

### 문제

이 스위치는 periodic convert\_post\_SAC\_CiscoMIB .syslog 메시지.

## 설명

다음 예에서는 이 메시지가 발생할 때 표시되는 콘솔 출력을 보여 줍니다.

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

CatOS 코드 버전을 업그레이드하거나 다운그레이드할 때 스위치는 이러한 콘솔 메시지를 자주 생성합니다. 다른 스위치에서 생성하는 스위치 컨피그레이션을 로드하거나 다른 버전의 코드에서 스위치 컨피그레이션을 사용하는 경우에도 오류가 발생할 수 있습니다. 스탠바이 슈퍼바이저 엔진에 대한 장애 조치에서는 이러한 메시지를 생성할 수도 있습니다.

다양한 버전의 코드에는 NVRAM에 저장된 변수가 포함되어 있습니다. 스위치가 처음 CatOS의 이후 또는 이전 버전으로 부팅될 때 스위치는 이전 컨피그레이션을 현재 부트 이미지에서 사용할 수 있는 버전으로 변환합니다. 이 프로세스 중에 필요하지 않거나 현재 형식에서 사용할 수 없는 특정 메모리 블록이 변환되지 않고 할당 해제됩니다. 이 내부 함수는 오류 메시지를 생성합니다.

이 메시지는 일반적으로 정보 제공용입니다. 모든 컨피그레이션 정보가 올바르게 변환되었는지 확인하려면 이전 컨피그레이션을 현재 컨피그레이션과 비교합니다.

코드 업그레이드, 컨피그레이션 변경 또는 Supervisor Engine 장애 조치가 발생하지 않은 경우 이러한 메시지가 나타나면 [Cisco Technical Support를 통해 서비스 요청\(등록된 고객만 해당\)](#)을 [생성합니다](#).

## [글로벌 체크섬 실패 오류](#)

### 문제

이 오류 메시지는 Catalyst OS 시스템 소프트웨어를 실행하는 Catalyst 4000/4500 및 6000/6500 시리즈 스위치에 표시될 수 있습니다.

오류 메시지 `Global checksum failed( )`가 `show version` 명령의 출력에 나타날 수 있습니다.

```
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

Module	DRAM			FLASH			NVRAM		
	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

관련 메시지, NVRAM:F는 show test 명령의 출력에 표시할 수 있습니다.

```
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.

## 설명

전역 체크섬 오류는 다음에 상자가 다시 로드될 때 컨피그레이션을 읽는 동안 실패한 CRC 체크섬 때문에 NVRAM이 손실될 가능성이 높습니다. 이는 일반적으로 하드웨어 오류가 아니지만 스위치가 자체적으로 수정합니다. 스위치가 이 상태에서는 컨피그레이션을 변경하지 않는 한 운영 스위치에 영향을 미치지 않습니다. 그러나 대부분의 경우 재설정 시 체크섬 오류가 다시 계산될 때 해결됩니다. 이 문제는 Cisco 버그 ID CSCdx87646에 설명되어 있습니다([등록된](#) 고객만 해당).

## 솔루션

이 오류 상태에서 스위치를 복구하려면 다음 단계를 완료하십시오.

1. 스위치 구성을 백업합니다. 컨피그레이션 [백업에 대한 자세한 내용은 TFTP 서버](#)에 컨피그레이션 파일 업로드를 참조하십시오.
2. reset supervisor\_# 명령을 실행하여 Supervisor 모듈을 재설정합니다.
3. 스위치가 부팅되면 show version 및 show test 명령을 실행하여 출력이 정상인지 확인합니다.
4. 스위치에 있는 컨피그레이션을 확인하고 필요한 경우 백업에서 복원합니다.

## 관련 정보

- [시스템 메시지 가이드 Catalyst 제품군 스위치, 7.4](#)
- [시스템 메시지 로깅 구성](#)
- [Catalyst 5000/5500 Series 스위치의 일반적인 CatOS 오류 메시지](#)
- [Catalyst 6500/6000 Series 스위치의 일반적인 CatOS 오류 메시지](#)
- [오류 메시지 디코더 \(등록된 고객만 해당\)](#)
- [LAN 제품 지원 페이지](#)

- [LAN 스위칭 지원 페이지](#)
- [기술 지원 및 문서 - Cisco Systems](#)