

직렬 회선 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[show interfaces serial 명령을 사용한 문제 해결](#)

[일련 행: show interfaces serial status 라인 조건](#)

[일련 행: 직렬 링크에서 출력 삭제 증가](#)

[일련 행: 직렬 링크의 입력 삭제 증가](#)

[일련 행: 총 인터페이스 트래픽의 1%를 초과하여 입력 오류 증가](#)

[일련 행: 직렬 회선 입력 오류 문제 해결](#)

[일련 행: 직렬 링크에서 인터페이스 재설정 증가](#)

[일련 행: 시리얼 링크에서 캐리어 전환 수 증가](#)

[show controllers 명령 사용](#)

[디버그 명령 사용](#)

[확장 ping 테스트 사용](#)

[Ping 테스트 수행](#)

[잠금 문제 해결](#)

[잠금 개요](#)

[잠금 문제 원인](#)

[잠금 문제 탐지](#)

[잠금 문제 격리](#)

[클럭 문제 솔루션](#)

[버퍼 조정](#)

[시스템 버퍼 조정](#)

[보류 대기열 제한 구현](#)

[우선 순위 대기열을 사용하여 병목 현상 감소](#)

[특수 직렬 회선 테스트](#)

[CSU 및 DSU 루프백 테스트](#)

[HDLC 또는 PPP 링크에 대한 CSU 및 DSU 로컬 루프백 테스트](#)

[HDLC 또는 PPP 링크에 대한 CSU 및 DSU 원격 루프백 테스트](#)

[show interfaces serial 명령에 대한 자세한 정보](#)

[show interfaces serial parameters](#)

[T1 문제 해결](#)

[show controller t1 명령을 사용하여 문제 해결](#)

[컨트롤러 t1 조건 표시](#)

[T1 오류 이벤트 트러블슈팅](#)

[ISDN 스위치 유형 및 PRI-그룹이 올바르게 구성되었는지 확인](#)

[신호 채널 확인](#)

[PRI 문제 해결](#)

[하드웨어 루프백 플러그 테스트 수행](#)

[문제 해결 E1](#)

[show controller e1 명령을 사용하여 문제 해결](#)

[E1 오류 이벤트 트러블슈팅](#)

[ISDN 스위치 유형 및 PRI-그룹이 올바르게 구성되었는지 확인](#)

[신호 채널 확인](#)

[PRI 문제 해결](#)

[관련 정보](#)

[소개](#)

이 장에서는 일반적인 문제 해결 정보 및 직렬 연결 문제 해결을 위한 도구 및 기술에 대해 설명합니다. 이 장은 다음 섹션으로 구성됩니다.

- **show interfaces serial** 명령을 사용하여 문제 해결
- **show controllers** 명령 사용
- 디버그 명령 사용
- 확장 ping 테스트 사용
- 잠금 문제 해결
- 버퍼 조정
- 특수 직렬 회선 테스트
- **show interfaces serial** 명령에 대한 자세한 정보
- T1 문제 해결
- E1 문제 해결

[사전 요구 사항](#)

[요구 사항](#)

이 문서의 독자는 다음 정의를 숙지해야 합니다.

- DTE = 데이터 터미널 장비
- CD = 캐리어 탐지
- CSU = 채널 서비스 유닛
- DSU = 디지털 서비스 유닛
- SCTE = 직렬 클럭에서 외부 전송
- DCE = 데이터 회로 종료 장비
- CTS = 보내기 지우기
- DSR = 데이터 세트 준비
- SAP = 서비스 광고 프로토콜
- IPX = 네트워크 간 패킷 교환
- FDDI = 파이버 분산 데이터 인터페이스
- ESF = 확장 수퍼프레임 형식

- B8ZS = 바이너리 8-0 대체
- LBO = 라인 구축

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

show interfaces serial 명령을 사용한 문제 해결

show interfaces serial EXEC 명령의 출력에는 직렬 인터페이스와 관련된 정보가 표시됩니다. 그림 15-1은 HDLC(High-Level Data Link Control) 직렬 인터페이스에 대한 **show interfaces serial EXEC** 명령의 출력을 보여줍니다.

이 섹션에서는 **show interfaces serial** 명령을 사용하여 WAN(Wide Area Network) 환경에서 직렬 회선 연결 문제를 진단하는 방법에 대해 설명합니다. 다음 섹션에서는 명령 출력의 몇 가지 중요한 필드에 대해 설명합니다.

이 장의 뒷부분에 나오는 "**show interfaces serial** 명령에 대한 자세한 정보" 섹션에 자세히 설명되어 있습니다.

일련 행: show interfaces serial status 라인 조건

show interfaces serial display의 인터페이스 상태 행에서 5가지 가능한 문제 상태를 식별할 수 있습니다(그림 15-1 참조).

- Serial x가 다운, 회선 프로토콜이 다운
- Serial x가 작동되고 회선 프로토콜이 다운됨
- Serial x가 작동되고 회선 프로토콜이 작동(반복됨)
- Serial x가 작동되고 회선 프로토콜이 다운됨(비활성화됨)
- Serial x가 관리 목적으로 다운되고 라인 프로토콜이 다운됨

그림 15-1 HDLC show interface serial 명령 출력

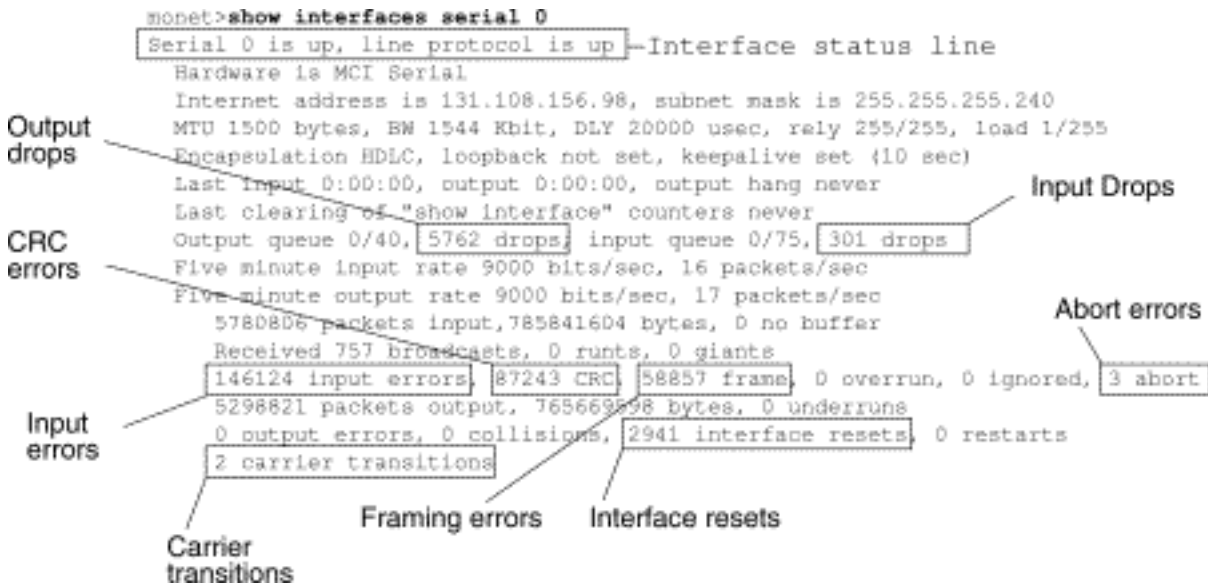


표 15-1: 일련 행: show interfaces serial Status Line Conditions(인터페이스 일련 상태 라인 조건) - 이 표에서는 인터페이스 상태 조건, 조건과 관련된 가능한 문제 및 해당 문제에 대한 해결책을 보여줍니다.

상태 라인 조건	가능한 문제	솔루션
Serial x가 작동되고 회선 프로토콜이 작동함		이것이 적절한 상태 라인 조건입니다. 필요한 조치가 없습니다.
Serial x가 다운, 회선 프로토콜이 다운 (DTE 모드)	<ul style="list-style-type: none"> 일반적으로 라우터가 CD 신호를 감지하지 않음을 나타냅니다(즉, CD가 활성화 상태가 아닙니다). 전화 회사 문제 - 회선이 다운되었거나 회선이 CSU/DSU에 연결되지 않았습 	<ol style="list-style-type: none"> CSU/DSU의 LED를 확인하여 CD가 활성 상태인지 확인하거나 줄에서 브레이크아웃 상자를 삽입하여 CD 신호를 확인합니다. 올바른 케이블 및 인터페이스를 사용하고 있는지 확인합니다(하드웨어 설치 설명서 참조). 분할 상자를 삽입하고 모든 제어 리드를 선택합니다. 문제가 있는지 확인하려면 임대 회선 또는 기타 통신업체 서비스에 문의하십시오. 결함이 있는 부품을 교체합니다. 라우터 하드웨어에 결함이 있다고 의심되는 경우 직렬 회선을 다른 포트로 변경합니다. 연결이 시작되면 이전에 연결된 인터페

	<p>니다.</p> <ul style="list-style-type: none"> • 케이블 연결 오류 또는 부정확 함 • 하드웨어 장애 (CSU/DSU) 	<p>이스에 문제가 발생합니다</p>
<p>Serial x가 작동되고 회선 프로토콜이 다운됨(DTE 모드)</p>	<ul style="list-style-type: none"> • 로컬 또는 원격 라우터가 잘못 구성되었습 니다. • Keepalive를 원 격 라우터에서 전송하 지 않음 • 임대 회선 또는 기타 캐리어 서 비스 문 제 - 잡 음이 있 는 회선 또는 잘 못 구성 되었거 나 오류 가 발생 한 스위 치 • 케이블 타이밍 문제 (CSU/DSU에 SCTE가 설정되 지 않음) 로컬 또 	<ol style="list-style-type: none"> 1. 모뎀, CSU 또는 DSU를 로컬 루프백 모드로 설정하 고 show interfaces serial 명령을 사용하여 회선 프로토콜이 작동하는지 확인 합니다. 회선 프로토콜이 작동하면 전화 회사 문제 또는 실패한 원격 라우터에 문제가 발생할 수 있습니다. 2. 원격 끝에 문제가 있는 경 우 원격 모뎀, CSU 또는 DSU에서 1단계를 반복합 니다. 3. 모든 케이블을 확인합 니다 . 케이블이 올바른 인터페이스, 올바른 CSU/DSU 및 올바른 전화 회사 네트워크 종료 지점에 연결되어 있는지 확인합니다. show controllers EXEC 명령을 사용하여 어떤 케이블이 어떤 인터페이스에 연결되어 있는지 확인합니다. 4. debug serial interface EXEC 명령을 활성화합 니다. 주의: 디버깅 출력은 CPU 프로세스에 높은 우선 순위가 할당되므로 시스템을 사용할 수 없게 만들 수 있습니다. 따라서 debug 명령을 사용하여 특정 문제를 해결하거나 Cisco 기술 지원 담당자와 의 문제 해결 세션 중에만 사용합니다. 또한 네트워크 트래픽이 낮고 사용자

	<p>는 원격 CSU/DSU에 실패했습니다.</p> <ul style="list-style-type: none"> • 실패한 로컬 또는 원격 CSU/DSU • 라우터 하드웨어 오류 (로컬 또는 원격) 	<p>가 적은 기간 동안 debug 명령을 사용하는 것이 가장 좋습니다. 이러한 기간 동안 디버깅하면 디버그 명령 처리 오버헤드가 증가하여 시스템 사용에 영향을 미칠 가능성이 줄어듭니다.</p> <ol style="list-style-type: none"> 5. 회선 프로토콜이 로컬 루프백 모드에서 나타나지 않고 debug serial interface EXEC 명령의 출력에 keepalive 카운터가 증가하지 않는 것으로 표시되면 라우터 하드웨어 문제가 발생할 가능성이 높습니다. 라우터 인터페이스 하드웨어를 바꿉니다. 6. 회선 프로토콜이 작동되고 keepalive 카운터가 증가하면 로컬 라우터에 문제가 없습니다. 이 장의 뒷부분에 나오는 "Troubleshooting Clocking Problems" 및 "CSU and DSU Loopback Tests" 섹션에 설명된 대로 직렬 회선을 트러블슈팅합니다. 7. 라우터 하드웨어에 결함이 있다고 의심되는 경우 시리얼 라인을 미사용 포트 로 변경합니다. 연결이 시작되면 이전에 연결된 인터페이스에 문제가 발생합니다.
<p>Serial x가 작동되고 회선 프로토콜이 다운됨(DCE 모드)</p>	<ul style="list-style-type: none"> • Clockrate interface configuration 명령 누락 • DTE 디바이스가 SCTE 	<ol style="list-style-type: none"> 1. 직렬 인터페이스에 clockrate interface configuration 명령을 추가합니다. 구문: 클럭 속도 bps 구문 설명: bps-원하는 클럭 속도(비트/초): 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 800000, 1000000, 1300000, 2000000, 4000000

	<p>모드를 지원하지 않거나 설정되지 않았습니까.</p> <ul style="list-style-type: none"> • 실패한 원격 CSU 또는 DSU • 실패 또는 잘못된 케이블 • 라우터 하드웨어 오류 	<p>또는 80000000</p> <ol style="list-style-type: none"> 2. 가능한 경우 DTE 디바이스를 SCTE 모드로 설정합니다. CSU/DSU에서 SCTE를 지원하지 않는 경우 Cisco 라우터 인터페이스에서 SCTE를 비활성화해야 할 수 있습니다. 이 장의 뒷부분에 나오는 "전송 시계 반전" 섹션을 참조하십시오. 3. 올바른 케이블이 사용되고 있는지 확인합니다. 4. 라인 프로토콜이 여전히 다운된 경우 하드웨어 장애 또는 케이블 연결 문제가 발생할 수 있습니다. 분할 상자를 삽입하고 리드를 확인합니다. 5. 필요에 따라 결함이 있는 부품을 교체합니다.
<p>Serial x가 작동되고 회선 프로토콜이 작동(반복됨)</p>	<p>회선에 루프가 있습니다. 루프가 처음 탐지되면 keepalive 패킷의 시퀀스 번호가 임의의 숫자로 변경됩니다. 동일한 난수가 링크를 통해 반환되면 루프가 존재합니다.</p>	<ol style="list-style-type: none"> 1. show running-config privileged EXEC 명령을 사용하여 루프백 인터페이스 컨피그레이션 명령 항목을 찾습니다. 2. 루프백 인터페이스 컨피그레이션 명령 엔트리를 찾은 경우 no loopback interface configuration 명령을 사용하여 루프를 제거합니다. 3. 루프백 인터페이스 컨피그레이션 명령을 찾지 못한 경우 CSU/DSU를 검사하여 수동 루프백 모드에서 구성되었는지 확인합니다. 이러한 경우 수동 루프백을 비활성화합니다. 4. CSU 또는 DSU를 재설정하고 라인 상태를 검사합니다. 회선 프로토콜이 작동하면 다른 작업이 필요하지 않습니다. 5. CSU 또는 DSU가 수동 루프백 모드에서 구성되지 않은 경우, 임대 회선 또는 기타 캐리어 서비스에 문

		의하여 회선 문제 해결 지원을 받으십시오.
Serial x가 작동되고 회선 프로토콜이 다운됨(비활성화됨)	<ul style="list-style-type: none"> • 전화 회사 서비스 문제로 인한 높은 오류율 • CSU 또는 DSU 하드웨어 문제 • 불량 라우터 하드웨어 (인터페이스) 	<ol style="list-style-type: none"> 1. 직렬 분석기 및 브레이크아웃 박스로 회선 문제를 해결합니다. CTS 및 DSR 신호를 전환해야 합니다. 2. 루프 CSU/DSU(DTE 루프) 문제가 계속되면 하드웨어 문제가 발생할 수 있습니다. 문제가 계속되면 전화 회사에 문제가 생길 가능성이 크다. 3. 필요한 경우 불량 하드웨어 교체(CSU, DSU, 스위치, 로컬 또는 원격 라우터)
Serial x가 관리 목적으로 다운되고 라인 프로토콜이 다운됨	<ul style="list-style-type: none"> • 라우터 컨피그레이션에 shutdown interface configuration 명령이 포함됩니다. • 중복 IP 주소 	<ol style="list-style-type: none"> 1. shutdown 명령에 대한 라우터 컨피그레이션을 확인합니다. 2. no shutdown interface 컨피그레이션 명령을 사용하여 shutdown 명령을 제거합니다. 3. show running-config privileged EXEC 명령 또는 show interfaces EXEC 명령을 사용하여 동일한 IP 주소가 없는지 확인합니다. 4. 중복 주소가 있는 경우 IP 주소 중 하나를 변경하여 충돌을 해결합니다.

일련 행: 직렬 링크에서 출력 삭제 증가

시스템이 패킷을 전송 버퍼에 전달하려고 하지만 사용할 수 있는 버퍼가 없는 경우 **show interfaces serial** 명령의 출력 삭제는 나타납니다(그림 15-1 참조).

증상: 직렬 링크의 출력 삭제 수가 증가하고 있습니다.

표 15-2 직렬 행: 직렬 링크의 출력 삭제 증가 - 이 표에서는 이러한 증상을 일으킬 수 있는 문제를 요약하고 해결책을 제안합니다.

가능한 문제	솔루션
직렬 인	1. 액세스 목록 또는 기타 방법으로 주기적인

터페이스에 대한 입력 속도가 직렬 링크에서 사용할 수 있는 대역폭을 초과합니다.

브로드캐스트 트래픽(예: 라우팅 및 SAP 업데이트)을 최소화합니다. 예를 들어, SAP 업데이트 간의 지연 시간을 늘리려면 `ipx sap-interval interface configuration` 명령을 사용합니다.

2. **hold-queue out interface** 컨피그레이션 명령을 사용하여 출력 보류 대기열 크기를 작은 증분(예: 25%)으로 늘립니다.
3. 영향을 받는 인터페이스에서 자주 사용되는 프로토콜에 대해 고속 스위칭을 끕니다. 예를 들어, IP 빠른 스위칭을 끄려면 **no ip route-cache interface configuration** 명령을 입력합니다. 다른 프로토콜에 대한 명령 구문은 Cisco IOS 컨피그레이션 가이드 및 명령 참조를 참조하십시오.
4. 우선순위 목록을 구성하여 느린 직렬 링크에 우선 순위 큐잉을 구현합니다. 우선순위 목록 구성에 대한 자세한 내용은 Cisco IOS 컨피그레이션 가이드 및 명령 참조를 참조하십시오.

참고: 특정 조건에서 출력 삭제를 사용할 수 있습니다. 예를 들어, 링크가 과도하게 사용되었다고 알려진 경우(상황을 해결할 방법이 없는 경우), 패킷을 보유하는 것보다 패킷을 삭제하는 것이 더 좋은 경우가 많습니다. 이는 플로우 제어를 지원하고 데이터를 재전송할 수 있는 프로토콜(예: TCP/IP 및 Novell IPX)에 적용됩니다. 그러나 DECnet 및 LAN 전송과 같은 일부 프로토콜은 삭제된 패킷에 민감하며 재전송을 제대로 수용하지 못합니다(있는 경우).

일련 행: 직렬 링크의 입력 삭제 증가

시스템에서 처리 중인 인터페이스 패킷이 너무 많으면 `show interfaces serial EXEC` 명령의 출력에 입력 드롭이 나타납니다(그림 15-1 참조).

증상: 직렬 링크의 입력 삭제 수가 증가하고 있습니다.

표 15-3: 일련 행: 직렬 링크의 입력 삭제 증가 - 이 표에서는 이러한 증상을 일으킬 수 있는 문제를 요약하고 해결책을 제안합니다.

가능한 문제	솔루션
입력 속도가 라우터 용량을 초과하거나 입력 큐가 출력 대기열 크기를	참고: 입력 삭제 문제는 일반적으로 고속 인터페이스(예: 이더넷, 토큰 링, FDDI)와 직렬 인터페이스 간에 트래픽이 라우팅되는 경우에 발생합니다. 트래픽이 적을 때 문제가 없습니다. 트래픽 속도가 증가하면 백업이 시작됩니다. 라우터는 이러한 혼잡한 기간 동안 패킷을 삭제합니다.

초과함	<ol style="list-style-type: none"> 패킷을 삭제하는 인터페이스에 대한 공통 대상 인터페이스의 출력 대기열 크기를 늘립니다. <code>hold-queue out interface</code> 컨피그레이션 명령을 사용합니다. <code>show interfaces</code> 출력에서 더 이상 드롭이 표시되지 않을 때까지 이러한 큐를 조금씩 늘립니다. 기본 출력 보류 대기열 제한은 패킷 100개입니다. 인터페이스 컨피그레이션 명령의 <code>hold-queue</code> 명령을 사용하여 입력 큐 크기를 줄여 입력 삭제를 출력 드롭으로 강제 적용합니다. 출력 삭제는 입력 삭제보다 라우터 성능에 미치는 영향이 적습니다. 기본 입력 보류 대기열은 75개의 패킷입니다.
-----	--

일련 행: 총 인터페이스 트래픽의 1%를 초과하여 입력 오류 증가

`show interfaces` 직렬 출력에 입력 오류가 나타나는 경우(그림 15-1 참조) 이러한 오류의 가능한 소스가 여러 개 있습니다. 가장 가능성이 높은 출처는 표 15-4에 요약되어 있습니다.

참고: CRC(cyclic redundancy check) 오류, 프레임링 오류 또는 총 인터페이스 트래픽의 1% 이상에 대한 입력 오류 값은 격리되고 복구해야 하는 링크 문제의 종류를 나타냅니다.

증상: 총 인터페이스 트래픽의 1%를 초과하는 입력 오류 수가 증가하고 있습니다.

표 15-4: 일련 행: 총 인터페이스 트래픽의 1%를 초과하여 입력 오류 증가

가능한 문제	솔루션
<p>다음 문제로 인해 이 증상이 나타날 수 있습니다.</p> <ul style="list-style-type: none"> 잘못된 전화 회사 장비 시끄러운 직렬 회선 잘못된 잠금 구성 (SCTE가 설정되지 않음) 잘못된 케이블 또는 케이블이 너무 길다 잘못된 케이블 또는 연결 잘못된 CSU 또는 DSU 잘못된 라우터 하드웨어 데이터 변환기 또는 라우터와 DSU 간에 	<p>참고: 라우터를 WAN 또는 직렬 네트워크에 연결할 때는 데이터 변환기를 사용하지 않는 것이 좋습니다.</p> <ol style="list-style-type: none"> 직렬 분석기를 사용하여 입력 오류의 원인을 격리합니다. 오류를 탐지하면 라우터 외부에 있는 디바이스에서 하드웨어 문제가 있거나 클럭 불일치가 발생할 수 있습니다. 루프백 및 ping 테스트를 사용하여 특정 문제 소스를 격리합니다. 자세한 내용은 이 장의 뒷부분에서 "trace 명령 사용" 및 "CSU 및 DSU 루프백 테스트" 섹션을 참조하십시오.

사용되는 기타 장치	3. 패턴을 찾습니다. 예를 들어, 일관된 간격으로 오류가 발생할 경우 라우팅 업데이트 전송과 같은 주기적인 기능과 관련이 있을 수 있습니다.
------------	---

일련 행: 직렬 회선 입력 오류 문제 해결

표 15-5: 이 표에서는 **show interfaces serial** 명령(그림 15-1 참조)에 표시되는 다양한 입력 오류 유형, 오류를 일으킬 수 있는 가능한 문제 및 이러한 문제의 해결 방법에 대해 설명합니다.

입력 오류 유형 (필드 이름)	가능한 문제	솔루션
CRC 오류 (CRC)	<p>CRC 오류는 CRC 계산이 전달되지 않아 데이터가 손상되었음을 나타내는 경우에 발생합니다. 다음 이유 중 하나가 있습니다.</p> <ul style="list-style-type: none"> • 시끄러운 직렬 회선 • 직렬 케이블이 너무 길거나 CSU/DSU에서 라우터로 연결되는 케이블이 차폐되어 있지 않습니다. • DSU에서 SCTE 모드가 활성화되지 않음 • CSU 라인 클럭이 잘못 구성되었습니다. • T1 링크의 밀도 문제(잘못된 프레임링 또는 코딩 사양) 	<ol style="list-style-type: none"> 1. 회선이 전송 요구 사항에 맞게 충분히 깨끗한지 확인합니다. 필요한 경우 케이블을 보호하십시오. 2. 케이블이 권장 길이 (15.24m) 또는 T1 링크의 경우 25피트 (7.62m)를 넘지 않도록 하십시오. 3. 모든 디바이스가 일반 회선 클럭에 대해 올바르게 구성되었는지 확인합니다. 로컬 및 원격 DSU에서 SCTE를 설정합니다. CSU/DSU에서 SCTE를 지원하지 않는 경우 이 장의 뒷부분에 나오는 "전송 시계 반전" 섹션을 참조하십시오. 4. 로컬 및 원격 CSU/DSU가 임대 회선 또는 기타 캐리어 서비스(예: ESF/B8ZS)에서 사용하는 것과 동일한 프레임링 및 코딩 체계에 대해 구성되었는지 확인합니다. 5. 임대 회선 또는 기타 통신사 서비스에 문의하십시오.

		<p>고 회선에서 무결성 테스트를 수행하도록 합니다.</p>
<p>프레이밍 오류 (프레임)</p>	<p>다음 이유 중 하나로 패킷이 8비트 바이트 경계에서 끝나지 않을 때 프레이밍 오류가 발생합니다.</p> <ul style="list-style-type: none"> • 시끄러운 직렬 회선 • 잘못 설계된 케이블; 직렬 케이블이 너무 깁니다. CSU 또는 DSU에서 라우터로 연결되는 케이블은 보호되지 않습니다. • DSU에서 SCTE 모드가 활성화되지 않았습니다. CSU 라인 클럭이 잘못 구성되었습니다. 클럭 중 하나가 로컬 클럭용으로 구성되어 있습니다. • T1 링크의 밀도 문제(잘못된 프레이밍 또는 코딩 사양) 	<ol style="list-style-type: none"> 1. 회선이 전송 요구 사항에 맞게 충분히 깨끗한지 확인합니다. 필요한 경우 케이블을 보호하십시오. 올바른 케이블을 사용하고 있는지 확인합니다. 2. 케이블이 권장 길이 (15.24m) 또는 T1 링크의 경우 25피트 (7.62m)를 넘지 않도록 하십시오. 3. 모든 디바이스가 일반 회선 시계를 사용하도록 올바르게 구성되었는지 확인합니다. 로컬 및 원격 DSU에서 SCTE를 설정합니다. CSU/DSU에서 SCTE를 지원하지 않는 경우 이 장의 뒷부분에 나오는 "전송 시계 반전" 섹션을 참조하십시오. 4. 로컬 및 원격 CSU/DSU가 임대 회선 또는 기타 캐리어 서비스(예: ESF/B8ZS)에서 사용하는 것과 동일한 프레이밍 및 코딩 체계에 대해 구성되었는지 확인합니다. 5. 임대 회선 또는 기타 통신 서비스에 문의하고 회선에서 무결성 테스트를 수행하도록 합니다.
<p>중단 전송 (중단)</p>	<p>중단은 한 개의 비트의 잘못된 시퀀스를 나타냅니다(한 줄에 7개 이상). 다음과 같은 사유가 발생할 수 있습니다.</p> <ul style="list-style-type: none"> • DSU에서 SCTE 모드가 	<ol style="list-style-type: none"> 1. 모든 디바이스가 일반 회선 시계를 사용하도록 올바르게 구성되었는지 확인합니다. 로컬 및 원격 DSU에서 SCTE를 설정합니다. CSU/DSU에서 SCTE를 지원하지 않는

	<p>활성화되지 않음</p> <ul style="list-style-type: none"> • CSU 라인 클럭이 잘못 구성되었습니다. • 직렬 케이블이 너무 길거나 CSU 또는 DSU에서 라우터로 연결되는 케이블이 차폐되지 않았습니다. • T1 링크의 밀도 문제(잘못된 프레이밍 또는 코딩 사양) • 패킷이 전송 중에 종료됨 - 일반적으로 인터페이스 재설정 또는 프레이밍 오류 발생 • 하드웨어 문제 불량 회로, 잘못된 CSU/DSU 또는 원격 라우터의 잘못된 전송 인터페이스 	<p>경우 이 장의 뒷부분에 나오는 "전송 시계 반전" 섹션을 참조하십시오.</p> <ol style="list-style-type: none"> 2. 필요한 경우 케이블을 보호하십시오. 케이블이 권장 길이(15.24m) 또는 T1 링크의 경우 25피트(7.62m)를 넘지 않도록 하십시오. 모든 연결이 정상인지 확인합니다. 3. 링크의 양쪽 끝에서 하드웨어를 확인합니다. 필요한 경우 결함이 있는 장비를 교체합니다. 4. 데이터 전송률을 낮추고 중단이 감소하는지 확인합니다. 5. 로컬 및 원격 루프백 테스트를 사용하여 중단이 발생하는 위치를 확인합니다. 이 장의 뒷부분에 나오는 "특수 직렬 회선 테스트" 섹션을 참조하십시오. 6. 임대 회선 또는 기타 통신사 서비스에 문의하고 회선에서 무결성 테스트를 수행하도록 합니다.
--	--	---

일련 행: 직렬 링크에서 인터페이스 재설정 증가

show interfaces serial EXEC 명령의 출력에 나타나는 인터페이스 재설정은 누락된 keep-alive 패킷의 결과입니다(그림 15-1 참조).

증상: 직렬 링크에서 인터페이스 재설정의 수가 증가하고 있습니다.

표 15-6: 이 표에서는 이 증상의 원인이 될 수 있는 문제를 요약하고 해결책을 제안합니다.

가능한 문제	솔루션
다음 문제로 인해 이 증상이 나타날 수 있습니다.	<p>인터페이스 재설정이 발생하는 경우 show interfaces serial 명령 출력의 다른 필드를 검사하여 문제의 원인을 확인합니다. 인터페이스 재설정의 증가를 기록하고 있다고 가정할 때 다음 필드를 검토합니다.</p> <ol style="list-style-type: none"> 1. show interfaces serial 출력에 출력 드랍이

<ul style="list-style-type: none"> • 링크 혼잡 (일반적으로 출력 삭제와 연관됨) • CD 전환을 일으키는 줄 오류 • CSU, DSU 또는 스위치에서 가능한 하드웨어 문제 	<p>많은 경우 "Serial Lines: Increasing Output Drops on Serial Link," 이 장의 앞부분에서 설명합니다.</p> <ol style="list-style-type: none"> 2. show interfaces serial display의 carrier transitions 필드를 확인합니다. 인터페이스 재설정을 등록하는 동안 캐리어 전환이 높은 경우 문제가 잘못된 링크나 잘못된 CSU 또는 DSU일 가능성이 높습니다. 임대 회선 또는 운송업체 서비스에 문의하고 필요에 따라 결함 장비를 교체하십시오. 3. show interfaces serial display에서 입력 오류 필드를 검토합니다. 인터페이스 재설정이 증가하는 동안 입력 오류가 높으면 문제가 잘못된 링크 또는 잘못된 CSU/DSU일 수 있습니다. 임대 회선 또는 기타 운송업체 서비스에 문의하고 필요에 따라 결함 장비를 교체하십시오.
---	--

일련 행: 시리얼 링크에서 캐리어 전환 수 증가

캐리어 전환은 통신 사업자 신호(예: 링크의 원격 끝에서 인터페이스 재설정)가 중단될 때마다 **show interfaces serial EXEC** 명령의 출력에 나타납니다.

증상: 시리얼 링크에서 캐리어 전환 수가 증가하고 있습니다.

표 15-7은 이 증상의 원인이 될 수 있는 문제를 요약하고 해결책을 제시합니다.

표 15-7: 일련 행: 시리얼 링크에서 캐리어 전환 수 증가

가능한 문제	솔루션
<p>다음 문제로 인해 이 증상이 나타날 수 있습니다.</p> <ul style="list-style-type: none"> • 외부 소스로 인한 회선 중단(케이블 연결, 빨간색 또는 노란색 T1 경보의 물리적 분 	<ol style="list-style-type: none"> 1. 링크의 양쪽 끝에서 하드웨어를 확인합니다. 브레이크아웃 박스 또는 직렬 분석기를 부착하여 문제의 원인을 확인하기 위한 테스트를 실시합니다.

<p>리, 네트워크 어딘가에서 번개 발생 등)</p> <ul style="list-style-type: none"> 스위치, DSU 또는 라우터 하드웨어 오류 	<ol style="list-style-type: none"> 분석기나 브레이크아웃 상자에서 외부 문제를 식별할 수 없는 경우 라우터 하드웨어를 확인합니다. 필요한 경우 결함이 있는 장비를 교체합니다.
---	--

show controllers 명령 사용

show controllers EXEC 명령은 직렬 회선 문제 해결 시 또 다른 중요한 진단 도구입니다. 명령 구문은 플랫폼에 따라 다릅니다.

- Cisco 7000 Series 라우터의 직렬 인터페이스의 경우 **show controllers cbus** EXEC 명령을 사용합니다.
- Cisco 액세스 제품의 경우 **show controllers** EXEC 명령을 사용합니다.
- AGS, CGS 및 MGS의 경우 **show controllers mci** EXEC 명령을 사용합니다.

그림 15-2는 show controllers cbus EXEC 명령의 출력을 보여줍니다. 이 명령은 FSIP(Fast Serial Interface Processor) 카드가 장착된 Cisco 7000 Series 라우터에서 사용됩니다. CSU/DSU(Channel Service Unit/Digital Service Unit)에 연결된 케이블이 올바른 인터페이스에 연결되어 있는지 확인하려면 명령 출력을 확인합니다. 마이크로코드 버전이 최신 버전인지 확인할 수도 있습니다.

그림 15-2: show controllers cbus 명령 출력

```

Harold>show controllers cbus
Switch Processor 5, hardware version 11.1, microcode version 10.7
Microcode loaded from system
512 Kbytes of main memory, 128 Kbytes cache memory
4 256 byte buffers, 4 1024 byte buffers, 312 1520 byte buffers
1024 byte system buffer
Restarts: 0 line down, 0 hung output, 0 controller error
FSIP 0, hardware version 1.0, microcode version 175.0
Microcode loaded from system
Interface 0 - Serial 0/0, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tq 23
Transmitter delay is 0 microseconds
Interface 1 - Serial 0/1, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tq 23
Transmitter delay is 0 microseconds
Interface 2 - Serial 0/2, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tq 23
Transmitter delay is 0 microseconds
Interface 3 - Serial 0/3, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tq 23
Transmitter delay is 0 microseconds

```

Microcode version

Interface and attached cable information

Cisco 2000, Cisco 2500, Cisco 3000, Cisco 4000 Series 액세스 서버 및 라우터와 같은 액세스 제품에 대해서는 **show controllers** EXEC 명령을 사용합니다. 그림 15-3은 Cisco 2503 액세스 서버의 BRI(Basic Rate Interface) 및 직렬 인터페이스의 **show controllers** 명령 출력을 보여줍니다. 일부 출력은 표시되지 않습니다.

show controllers 출력은 인터페이스 채널의 상태와 케이블이 인터페이스에 연결되었는지 여부를 나타냅니다. 그림 15-3에서 직렬 인터페이스 0에는 RS-232 DTE 케이블이 연결되어 있습니다. 직렬 인터페이스 1에는 케이블이 연결되어 있지 않습니다.

그림 15-4는 show controllers mci 명령의 출력을 보여줍니다. 이 명령은 AGS, CGS 및 MGS 라우터에서만 사용됩니다. 전기 인터페이스가 UNKNOWN(V.35, EIA/TIA-449 또는 기타 전기 인터페이스 유형 대신)으로 표시되는 경우 잘못 연결된 케이블이 문제가 될 수 있습니다. 카드 내부 배선에 문제가 있거나 잘못된 어플라이언스가 있을 수도 있습니다. 전기 인터페이스를 알 수 없는 경우 show interfaces serial EXEC 명령에 해당하는 디스플레이에 인터페이스 및 회선 프로토콜이 다운되었음을 표시합니다.

그림 15-3: show controllers 명령 출력

```
Maude>show controllers
BRI unit 0
D Chan Info:
Layer 1 is DEACTIVATED
D channel is deactivated

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

B1 Chan Info:
Layer 1 is DEACTIVATED
B channel 1 is deactivated

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

B2 Chan Info:

[. . .]
LANCE unit 0, idb 0x9515C, ds 0x96F00, regaddr = 0x2130000, reset_mask 0x2
IB at 0x40163F4: mode=0x0000, mcfilter 0000/0000/0000/0000
station address 0000.0c0a.28a7 default station address 0000.0c0a.28a7
buffer size 1524

[. . .]
0 missed datagrams, 0 overruns, 0 late collisions, 0 lost carrier events
0 transmitter underruns, 0 excessive collisions, 0 tdr, 0 babbles
0 memory errors, 0 spurious initialization done interrupts
0 no enp status, 0 buffer errors, 0 overflow errors
0 one_col, 0 more_col, 3 deferred, 0 tx_buff
0 throttled, 0 enabled
Lance csr0 = 0x73

HD unit 0, idb = 0x98D28, driver structure at 0x9AAD0
buffer size 1524 HD unit 0, RS-232 DTE cable
Attached cable on serial interface 0

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

HD unit 1, idb = 0x9C1B8, driver structure at 0x9DF60
buffer size 1524 HD unit 1, No DCE cable
No attached cable on serial interface 1

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
```

그림 15-4: show controllers mci 명령 출력

Electrical interface identified as type UNKNOWN, suggesting a hardware failure or improperly connected cable.

```
MCI 1, controller type 1.1, microcode version 1.0
 128 Kbytes of main memory, 4 Kbytes cache memory
16 system TX buffers, largest buffer size 1520
Restarts: 0 line down, 0 hung output, 0 controller error
Interface 0 is Ethernet1, station address 0000.0c00.3b09
 22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
Transmitter delay is 0 microseconds
Interface 1 is Serial2, electrical interface is UNKNOWN
 22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
Transmitter delay is 0 microseconds
High speed synchronous serial interface
Interface 3 is Serial3, electrical interface is V.35 DTE
 22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
Transmitter delay is 0 microseconds
High speed synchronous serial interface
```

디버그 명령 사용

다양한 **debug** privileged EXEC 명령의 출력은 많은 인터넷워킹 이벤트의 프로토콜 상태 및 네트워크 활동과 관련된 진단 정보를 제공합니다.

주의: 디버깅 출력은 CPU 프로세스에 높은 우선 순위가 할당되므로 시스템을 사용할 수 없게 만들 수 있습니다. 따라서 debug 명령만 사용하여 특정 문제를 해결하거나 Cisco 기술 지원 담당자와의 문제 해결 세션 중에만 사용합니다. 또한 네트워크 트래픽이 낮고 사용자가 적은 기간 동안 debug 명령을 사용하는 것이 가장 좋습니다. 이러한 기간 동안 디버깅하면 디버그 명령 처리 오버헤드가 증가하여 시스템 사용에 영향을 미칠 가능성이 줄어듭니다. debug 명령을 모두 사용하는 경우 특정 no debug 명령 또는 no debug all 명령으로 비활성화해야 합니다.

다음 **debug** 명령은 직렬 및 WAN 문제를 해결할 때 유용합니다. 이러한 각 명령의 기능 및 출력에 대한 자세한 내용은 디버그 명령 참조 발행물에서 확인할 수 있습니다.

- **debug serial interface** - HDLC keepalive 패킷이 증가하는지 확인합니다. 그렇지 않으면 인터페이스 카드 또는 네트워크에 가능한 타이밍 문제가 있습니다.
- **debug x25 events** - SVC(Switched Virtual Circuit)의 열기 및 닫기와 같은 X.25 이벤트를 탐지합니다. 결과 "원인 및 진단" 정보가 이벤트 보고서에 포함됩니다.
- **debug lab**- 출력 링크 액세스 절차, LAB(Balanced) 또는 Level 2 X.25 정보.
- **debug arp** - 라우터가 WAN 클라우드의 반대쪽에 있는 라우터(ARP 패킷 포함)에 대한 정보를 전송할지 또는 학습하는지 여부를 나타냅니다. TCP/IP 네트워크의 일부 노드가 응답하지만 다른 노드는 응답하지 않을 경우 이 명령을 사용합니다.
- **debug frame-relay lmi** - 프레임 릴레이 스위치와 라우터가 LMI 패킷을 보내고 받는지 확인하는데 유용한 LMI(Local Management Interface) 정보를 가져옵니다.
- **debug frame-relay events** - 라우터와 프레임 릴레이 스위치 간에 교환이 발생하는지 확인합니다.
- **debug ppp negotiation** - PPP 시작 중에 전송된 PPP(Point-to-Point Protocol) 패킷을 표시합니다. 여기서 PPP 옵션은 협상됩니다.
- **debug ppp packet** - 보내고 받는 PPP 패킷을 표시합니다. 이 명령은 낮은 수준의 패킷 덤프를 표시합니다.
- **debug ppp errors** - PPP 연결 협상 및 작업과 연결된 PPP 오류(예: 불법 또는 형식이 잘못된 프레임)를 표시합니다.
- **debug ppp chap** - PPP CHAP(Challenge Handshake Authentication Protocol) 및 PAP>Password Authentication Protocol) 패킷 교환을 표시합니다.

- **debug serial packet** - 전송 및 수신되는 SMDS(Switched Multabit Data Service) 패킷을 표시합니다. 이 표시는 패킷이 전송되지 않았거나 잘못 수신된 이유를 나타내는 오류 메시지도 인쇄합니다. SMDS의 경우 SMDS 패킷이 전송되거나 수신될 때 명령은 전체 SMDS 헤더 및 일부 페이로드 데이터를 덤프합니다.

확장 ping 테스트 사용

ping 명령은 여러 호스트 시스템뿐만 아니라 Cisco 인터넷워킹 디바이스에서 사용할 수 있는 유용한 테스트입니다. TCP/IP에서 이 진단 도구를 ICMP(Internet Control Message Protocol) 에코 요청이라고도 합니다.

참고: ping 명령은 **show interfaces** 직렬 표시에 높은 수준의 입력 오류가 등록될 때 특히 유용합니다. 그림 15-1을 참조하십시오.

Cisco 인터넷워킹 디바이스는 여러 ping 패킷을 순서대로 전송하는 것을 자동화하는 메커니즘을 제공합니다. 그림 15-5는 확장 ping 옵션을 지정하는 데 사용되는 메뉴를 보여줍니다. 이 예에서는 20개의 연속 ping을 지정합니다. 그러나 직렬 회선에서 구성 요소를 테스트할 때는 1000ping과 같이 훨씬 더 큰 숫자를 지정해야 합니다.

그림 15-5: 확장 Ping 사양 메뉴

```

Betelgeuse# ping
Protocol [ip]:
Target IP address: 129.44.12.7
Repeat count [5]: 20
Datagram size [100]: 64
Timeout in seconds [2]:
Extended commands [n]: yes
Source address:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]: 0xFFFF
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 20, 64-byte ICMP Echos to 129.44.12.7, timeout is 2 seconds:
Packet has data pattern 0xFFFF
!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
  
```

Ping 테스트 수행

일반적으로 직렬 회선 ping 테스트를 다음과 같이 수행합니다.

1. CSU 또는 DSU를 로컬 루프백 모드로 전환합니다.
2. 다양한 데이터 패턴 및 패킷 크기를 전송하도록 extended ping 명령을 구성합니다. 그림 15-6 및 그림 15-7은 각각 All-Zeros(1500바이트) ping과 All-One(1500바이트) ping이라는 두 가지 유용한 ping 테스트를 보여줍니다.
3. **show interfaces serial** 명령 출력(그림 15-1 참조)을 검사하고 입력 오류가 증가했는지 확인합니다. 입력 오류가 증가하지 않으면 로컬 하드웨어(DSU, 케이블, 라우터 인터페이스 카드)가 양호한 상태일 수 있습니다. 이 테스트 시퀀스가 많은 CRC 및 프레임링 오류가 발생하여 프롬프트가 표시되었다고 가정하면 잠금 문제가 발생할 수 있습니다. CSU 또는 DSU에서 타이밍 문제를 확인합니다. 이 장의 뒷부분에 나오는 "Troubleshooting Clocking Problems" 섹션을 참조하십시오.

4. 잠금 컨피그레이션이 올바르며 제대로 작동하고 있다고 판단하면 CSU 또는 DSU를 원격 루프백 모드로 전환합니다.
5. ping 테스트를 반복하고 입력 오류 통계의 변경 사항을 확인합니다.
6. 입력 오류가 증가하면 직렬 회선이나 CSU/DSU에 문제가 있습니다. WAN 서비스 공급업체에 문의하고 CSU 또는 DSU를 바꿉니다. 문제가 계속되면 기술 지원 담당자에게 문의하십시오.

그림 15-6: ALI-0 1500바이트 ping 테스트

```

yowzers#ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
1500 byte packet size --- Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 192.169.51.14
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
All zeros ping --- Data pattern [0xABCD]: 0x0000
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.169.51.22, timeout is 2 seconds:
Packet has data pattern 0x0000
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/6/8 ms
yowzers#

```

그림 15-7 올인원 1500바이트 ping 테스트

```

zounds#ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
1500 byte packet size --- Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 192.169.51.14
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
All ones ping --- Data pattern [0xABCD]: 0xffff
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.169.51.22, timeout is 2 seconds:
Packet has data pattern 0xFFFF
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/6/8 ms
zounds#

```

잠금 문제 해결

직렬 연결의 클러킹 충돌로 인해 연결 서비스가 만성적인 손실되거나 성능이 저하될 수 있습니다. 이 섹션에서는 잠금 문제의 중요한 측면에 대해 설명합니다. 잠금 문제 원인, 잠금 문제 감지, 잠금 문제 격리, 문제 해결 방법 잠금

잠금 개요

CSU/DSU는 데이터를 통과하는 데이터에서 데이터 시계를 파생시킵니다. 시계를 복구하려면 CSU/DSU 하드웨어가 시계를 통과하는 8비트의 모든 데이터에 대해 1비트 값을 하나 이상 받아야

합니다. 이를 *one density*로 알려져 있습니다. 고밀도 유지 관리를 통해 하드웨어는 데이터 시계를 안정적으로 복구할 수 있습니다.

최신 T1 구현에서는 일반적으로 바이너리 8-0 대체(B8ZS) 코딩을 사용하여 ESF(Extended Superframe Format) 프레임링을 사용합니다. B8ZS는 직렬 링크를 통해 연속된 8개의 0이 전송될 때마다 특수 코드가 대체되는 체계를 제공합니다. 그런 다음 이 코드는 연결의 원격 끝에서 해석됩니다. 이 기술은 데이터 스트림에 관계없이 밀도를 보장합니다.

이전 T1 구현에서는 SF(Superframe Format) 프레임링 및 AMI(Alternate Mark Inversion) 코딩이라고도 하는 D4를 사용합니다. AMI는 B8ZS와 같은 코딩 체계를 사용하지 않습니다. 따라서 데이터 스트림과 별개로 밀도가 유지되지 않으므로 전송할 수 있는 데이터 유형이 제한됩니다.

직렬 통신의 또 다른 중요한 요소는 SCTE(Serial Clock Transmit External) 터미널 타이밍입니다. SCTE는 DTE(데이터 터미널 장비) 디바이스(예: 라우터)에서 DCE(데이터 통신 장비) 디바이스(예: CSU/DSU)로 다시 올리는 클럭입니다.

DCE 디바이스가 내부 클럭 대신 SCTE를 사용하여 DTE의 데이터를 샘플링할 때 CSU/DSU와 라우터 간에 케이블이 위상 변경되는 경우에도 오류 없이 데이터를 샘플링하는 것이 더 좋습니다. 64kbps 이상 빠른 직렬 전송에는 SCTE를 사용하는 것이 좋습니다. CSU/DSU에서 SCTE를 지원하지 않는 경우 이 장의 뒷부분에 나오는 "전송 시계 반전" 섹션을 참조하십시오.

잠금 문제 원인

일반적으로 직렬 WAN 상호 연결의 클럭 문제는 다음 원인 중 하나로 인해 발생할 수 있습니다.

- 잘못된 DSU 컨피그레이션
- 잘못된 CSU 컨피그레이션
- 사양에서 벗어난 케이블 - 15.24m(50피트) 이상 또는 차폐되지 않은 케이블
- 잡음 또는 불량 패치 패널 연결
- 여러 케이블이 한 줄로 연결됨

잠금 문제 탐지

직렬 인터페이스에서 클럭킹 충돌을 탐지하려면 다음과 같이 입력 오류를 찾습니다.

1. 링크 양쪽 끝에 있는 라우터에서 **show interfaces serial EXEC** 명령을 사용합니다.
2. 명령 출력에 CRC, 프레임링 오류 및 중단이 있는지 검사합니다.
3. 이러한 단계 중 하나가 인터페이스에서 트래픽의 약 0.5% 2.0%를 초과하는 오류를 나타낼 경우, WAN에 클럭 문제가 있을 수 있습니다.
4. 다음 섹션인 "Locking Problems(잠금 문제 격리)"에 설명된 대로 잠금 충돌 소스를 격리합니다.
5. 결함이 있는 패치 패널을 우회하거나 복구합니다.

잠금 문제 격리

잠금 충돌이 입력 오류의 가장 가능성 있는 원인임을 확인한 후 다음 절차를 사용하여 이러한 오류의 원인을 격리합니다.

1. 이 장의 앞부분에서 "CSU and DSU Loopback Tests(CSU 및 DSU 루프백 테스트)" 섹션에 설명된 대로 일련의 ping 테스트 및 루프백 테스트(로컬 및 원격 모두)를 수행합니다.

- 문제의 원인이 되는 연결의 끝을 확인하거나 문제가 라인에 있는지 확인합니다. 로컬 루프백 모드에서 ping 테스트에서 다른 패턴과 크기를 실행합니다(예: 1500바이트 데이터그램 사용). 단일 패턴 및 패킷 크기를 사용해도 오류가 발생하지 않을 수 있습니다. 특히 라우터 또는 CSU/DSU에 대한 직렬 케이블에 문제가 있는 경우 더욱 그렇습니다.

- show interfaces serial EXEC** 명령을 사용하고 입력 오류 수가 증가하는지, 누적되는 위치를 확인합니다.

연결 양쪽 끝에서 입력 오류가 누적되는 경우 CSU를 잠그는 것이 가장 큰 문제입니다.

한 쪽 끝에만 입력 오류가 발생하는 경우 DSU 잠금 또는 케이블 연결 문제가 있을 수 있습니다.

한쪽 끝의 중단은 다른 쪽 끝의 정보가 잘못된 정보이거나 회선 문제가 있는 것으로 나타납니다.

참고: 항상 **show interfaces serial** 명령 출력(그림 15-1 참조)을 참조하고 오류 카운트의 변경 사항을 기록하거나 오류 카운트가 변경되지 않으면 주의하십시오.

클럭 문제 솔루션

표 15-8 일련 번호: 문제 및 해결 방법: 이 표에서는 문제의 원인을 기준으로 문제를 해결하기 위한 권장 해결 방법을 설명합니다.

가능한 문제	솔루션
잘못된 CSU 컨피그레이션	<ol style="list-style-type: none"> 양쪽 끝에 있는 CSU가 클럭 소스(로컬 또는 회선)에 일치하는지 확인합니다. CSU가 동의하지 않으면 CSU가 동의하지 않도록 구성합니다. 일반적으로 이 선은 소스입니다. CSU의 LBO 설정을 확인하여 임피던스가 물리적 라인의 임피던스와 일치하는지 확인합니다. CSU 구성에 대한 자세한 내용은 CSU 하드웨어 설명서를 참조하십시오.
잘못된 DSU 컨피그레이션	<ol style="list-style-type: none"> 양쪽 끝에 있는 DSU에 SCTE 모드가 활성화되었는지 확인합니다. 연결의 양쪽 끝에서 SCTE가 활성화되지 않은 경우 활성화하십시오. 1개의 밀도가 유지되어야 합니다. 따라서 DSU는 임대 회선 또는 기타 캐리어 서비스에서 사용하는 것과 동일한 프레임링 및 코딩 체계(예: ESF 및 B8ZS)를 사용해야 합니다. 프레임링 및 코딩 체계에 대한 자세한 내용은 임대 회선 공급업체에 문의하십시오. 캐리어 서비스에서 AMI 코딩을 사용하는 경우 링크의 양쪽에서 전송 시계를 변환하거나 비트-스킬 모드에서 DSU를 실행합니다. DSU 구성에 대한 자세한 내용은 DSU 하드웨어 설명서를 참조하십시오.
케이블-라우터	케이블이 15.24m(50피트)보다 긴 경우 더 짧은 케이블을 사용합니다. 케이블이 차폐되지 않은

사양이 부족합니다.	경우 차폐된 케이블로 교체합니다.
------------	--------------------

전송 시계 반전

SCTE를 지원하지 않는 CSU/DSU를 사용하여 64kbps 이상의 속도로 직렬 연결을 시도하는 경우 라우터에서 전송 시계를 반전해야 할 수 있습니다. 전송 클럭을 반전하면 데이터와 클럭 신호 간의 위상 변화를 보상합니다.

전송 시계를 반전하는 데 사용되는 특정 명령은 플랫폼에 따라 다릅니다. Cisco 7000 Series 라우터에서 **invert-transmit-clock interface configuration** 명령을 입력합니다. Cisco 4000 Series 라우터의 경우 **dte-invert-txc interface configuration** 명령을 사용합니다.

라우터에 올바른 명령 구문을 사용하고 있는지 확인하려면 라우터 또는 액세스 서버의 사용 설명서 및 Cisco IOS 구성 가이드 및 명령 참조를 참조하십시오.

참고: 이전 플랫폼에서 전송 시계를 반전하려면 물리적 접퍼를 이동해야 할 수 있습니다.

버퍼 조정

과도한 대역폭 사용률(70% 이상)으로 인해 전반적인 성능이 저하되고 일시적인 장애가 발생할 수 있습니다. 예를 들어 DECnet 파일 전송은 네트워크의 어느 곳에서 패킷이 삭제되어 실패할 수 있습니다.

상황이 충분히 나쁘면 링크의 대역폭을 늘려야 합니다. 그러나 대역폭을 늘릴 필요가 없거나 즉시 실용적이지 않을 수 있습니다. 한계 직렬 회선 초과 사용 문제를 해결하는 한 가지 방법은 라우터가 데이터 버퍼를 사용하는 방법을 제어하는 것입니다.

주의: 일반적으로 Cisco 기술 지원 담당자와 긴밀하게 작업하지 않는 한 시스템 버퍼를 조정하지 마십시오. 라우터의 시스템 버퍼를 잘못 조정하면 하드웨어 및 네트워크의 성능에 심각한 영향을 줄 수 있습니다.

다음 세 가지 옵션 중 하나를 사용하여 버퍼 사용 방법을 제어합니다.

- 시스템 버퍼와 관련된 매개 변수 조정
- 입력 또는 출력 대기열에 유지되는 패킷 수(보류 대기열) 지정
- 전송을 위해 트래픽이 대기되는 방법의 우선순위 지정(우선 순위 출력 대기열)

이러한 옵션과 연결된 컨피그레이션 명령은 Cisco IOS 컨피그레이션 가이드 및 명령 참조에 설명되어 있습니다.

다음 섹션에서는 이러한 옵션이 적용될 수 있는 상황을 식별하고 이러한 옵션을 사용하여 직렬 /WAN 상호 연결의 연결 및 성능 문제를 해결하는 방법을 정의하는 데 중점을 둡니다.

시스템 버퍼 조정

Cisco 라우터에는 두 가지 일반 버퍼 유형이 있습니다. 하드웨어 버퍼와 시스템 버퍼를 제공합니다. 시스템 버퍼만 시스템 관리자가 직접 구성할 수 있습니다. 하드웨어 버퍼는 각 인터페이스와 연결된 수신 및 전송 버퍼로 특별히 사용되며, 특별한 컨피그레이션이 없는 경우 시스템 소프트웨어 자체에서 동적으로 관리합니다.

시스템 버퍼는 주 시스템 메모리와 연결되고 서로 다른 크기의 메모리 블록에 할당됩니다. 시스템 버퍼의 상태를 확인하는 데 유용한 명령은 **show buffers EXEC** 명령입니다. 그림 15-8은 **show buffers** 명령의 출력을 보여줍니다.

그림 15-8 show buffers 명령 출력

```
Cookie-Monster>show buffers
Buffer elements:
  401 in free list (500 max allowed)
  87777499 hits, 0 misses, 0 created
Small buffers, 104 bytes (total 120, permanent 120):
  114 in free list (20 min, 250 max allowed)
  70005538 hits, 6 misses, 2 trims, 2 created
Middle buffers, 600 bytes (total 90, permanent 90):
  88 in free list (10 min, 200 max allowed)
  25696696 hits, 27 misses, 27 trims, 27 created
Big buffers, 1524 bytes (total 90, permanent 90):
  90 in free list (5 min, 300 max allowed)
  8214530 hits, 15 misses, 366 trims, 366 created
Large buffers, 5024 bytes (total 5, permanent 5):
  5 in free list (0 min, 30 max allowed)
  15017 hits, 12 misses, 16354 trims, 16354 created
Rogue buffers, 18024 bytes (total 3, permanent 0):
  2 in free list (0 min, 4 max allowed)
  297582 hits, 17 misses, 30 trims, 33 created

0 failures (0 no memory) Failures
```

show buffers 출력에서 다음을 수행합니다.

- **total** - 사용된 버퍼와 사용되지 않은 버퍼를 포함하여 풀의 총 버퍼 수를 식별합니다.
- **permanent** - 풀에 할당된 버퍼의 영구 수를 식별합니다. 이러한 버퍼는 항상 풀에 있으며 잘라낼 수 없습니다.
- **in free list** - 현재 풀에 사용 가능한 버퍼 수를 식별합니다.
- **min** - RP(Route Processor)가 사용 가능한 목록에 유지하려는 최소 버퍼 수를 식별합니다.min 매개 변수는 지정된 시간에 풀의 버퍼 수요를 예측하는 데 사용됩니다.사용 가능한 목록의 버퍼 수가 최소 값보다 낮으면 RP는 해당 풀에 대해 더 많은 버퍼를 생성하려고 시도합니다.
- **max allowed** - 사용 가능한 목록에서 허용되는 최대 버퍼 수를 식별합니다.max allowed 매개 변수는 풀이 더 이상 필요하지 않은 버퍼를 독점하지 못하게 하고 나중에 사용하기 위해 이 메모리를 시스템으로 다시 확보합니다.사용 가능한 목록의 버퍼 수가 최대 허용 값보다 큰 경우 RP는 풀에서 버퍼를 트리밍하려고 시도해야 합니다.
- **hits** - 풀에서 요청된 버퍼 수를 식별합니다. 적중 카운터는 버퍼에 대한 최대 수요를 충족해야 하는 풀을 결정하는 메커니즘을 제공합니다.
- **miss** - 버퍼가 요청된 횟수를 식별하고 RP에서 추가 버퍼가 필요하다는 것을 탐지했습니다. 다시 말해, 사용 가능한 목록의 버퍼 수가 최소 아래로 떨어졌습니다. Misses 카운터는 RP에서 추가 버퍼를 강제로 생성한 횟수를 나타냅니다.
- **trms** - 사용 가능한 목록의 버퍼 수가 최대 허용 버퍼 수를 초과할 때 RP가 풀에서 잘린 버퍼 수를 식별합니다.
- **created** - 풀에서 생성된 버퍼 수를 식별합니다. RP는 사용 가능한 목록의 버퍼 수가 최소 버퍼보다 적을 때까지 버퍼에 대한 수요가 증가하면 버퍼를 생성합니다. 또는 사용 가능한 목록의 버퍼가 0이기 때문에 오류가 발생합니다.
- **failures** - 추가 버퍼를 생성하려고 시도한 후에도 요청자에게 버퍼를 부여하지 못한 횟수를 식별합니다. 실패 수는 버퍼 부족으로 인해 삭제된 패킷 수를 나타냅니다.
- **no memory** - 메모리가 부족하여 추가 버퍼를 만들 수 없어 발생한 오류 수를 식별합니다.

그림 15-8의 **show buffers** 명령 출력은 trims의 수가 많음을 나타내고 큰 버퍼의 경우 생성된 필드를 나타냅니다. 이 필드에서 높은 숫자를 수신하는 경우 시스템 버퍼에 대해 구성된 최대 여유 값

을 늘려 시리얼 링크 성능을 높일 수 있습니다. **trims**는 사용 가능한 목록의 버퍼 수가 **최대 허용** 버퍼 수를 초과할 때 RP가 플에서 **잡린** 버퍼 수를 식별합니다.

buffers max free number 전역 컨피그레이션 명령을 사용하여 사용 가능한 시스템 버퍼 수를 늘릴 수 있습니다. 구성하는 값은 **show buffers** 명령 출력의 **total** 필드에 표시된 그림의 약 150%여야 합니다. **show buffers** 출력이 더 이상 **trims** 및 생성된 버퍼를 나타내지 않을 때까지 이 프로세스를 반복합니다.

show buffers 명령 출력에서 (**메모리 없음**) 필드(그림 15-8의 마지막 출력 줄 참조)에 많은 수의 오류가 표시되는 경우 시스템 버퍼 사용량을 줄이거나 라우터의 공유 또는 주 메모리(물리적 RAM)를 늘려야 합니다. 기술 지원 담당자에게 문의하십시오.

보류 대기열 제한 구현

보류 대기열은 각 라우터 인터페이스에서 발신 또는 수신 패킷을 저장하는 데 사용하는 버퍼입니다. 라우터가 패킷을 삭제하기 전에 대기열에 있는 데이터 패킷 수를 늘리려면 **hold-queue interface configuration** 명령을 사용합니다. **show interfaces** 출력에서 더 이상 드롭이 표시되지 않을 때까지 이러한 큐를 조금씩 늘립니다. 기본 출력 보류 대기열 제한은 패킷 100개입니다.

참고: **hold-queue** 명령은 라우터에서 생성된 프로세스 전환 패킷 및 정기 업데이트에 사용됩니다.

다음 조건에서 **hold-queue** 명령을 사용하여 패킷 삭제를 방지하고 직렬 링크 성능을 개선할 수 있습니다.

- 삭제를 허용할 수 없는 애플리케이션이 있으며 프로토콜은 더 긴 지연을 허용할 수 있습니다. DECnet은 두 조건을 모두 충족하는 프로토콜의 예입니다. LAT(Local-Area Transport)는 지연을 허용하지 않기 때문에 그렇지 않습니다.
- 인터페이스가 매우 느립니다. 대역폭이 낮거나 예상 사용률이 가용 대역폭을 산발적으로 초과할 가능성이 있습니다.

참고: 출력 보류 대기열에 지정된 수를 늘리면 시스템 버퍼 수를 늘려야 할 수 있습니다. 사용되는 값은 네트워크에서 예상되는 트래픽과 연결된 패킷의 크기에 따라 달라집니다.

우선 순위 대기열을 사용하여 병목 현상 감소

우선 순위 큐잉은 인터페이스별로 트래픽의 우선 순위를 지정할 수 있는 목록 기반 제어 메커니즘입니다. 우선 순위 큐잉에는 다음 두 단계가 포함됩니다.

1. 프로토콜 유형 및 우선순위 레벨별로 우선순위 목록을 생성합니다.
2. 특정 인터페이스에 우선순위 목록을 할당합니다.

이 두 단계 모두 **priority-list** 전역 컨피그레이션 명령 버전을 사용합니다. 또한 **priority-list** 사양에서 **access-list** 전역 컨피그레이션 명령을 참조하여 추가 트래픽 제어를 적용할 수 있습니다. 우선순위 목록 정의의 예와 우선순위 큐잉과 관련된 명령 구문에 대한 자세한 내용은 Cisco IOS 컨피그레이션 가이드 및 명령 참조를 참조하십시오.

참고: 우선 순위 큐잉은 크기가 다른 네 개의 보류 대기열을 자동으로 생성합니다. 이는 컨피그레이션에 포함된 모든 보류 대기열 사양을 재정의합니다.

다음 조건에서 패킷의 삭제를 방지하고 직렬 링크 성능을 향상하려면 우선 순위 큐잉을 사용합니다

- 인터페이스가 느리면 전송 중인 다양한 트래픽 유형이 있으며 터미널 트래픽 성능을 개선하고

자 합니다.

- 특정 시간에 발생하는 파일 전송과 같은 매우 많은 부하가 간헐적으로 발생하는 직렬 링크가 있는 경우 우선 순위 큐잉은 많은 트래픽 기간에 폐기할 트래픽 유형을 선택하는 데 도움이 됩니다.

일반적으로 우선 순위 큐를 구현할 때 기본 대기열 수로 시작합니다. 우선순위 큐잉을 활성화한 후 `show interfaces serial EXEC` 명령을 사용하여 모니터 출력을 삭제합니다. 지정된 트래픽 대기열에서 출력 삭제가 높은 우선순위로 발생한다는 것을 알게 되면, 큐에 추가할 수 있는 패킷 수를 늘리십시오(`priority-list` 전역 컨피그레이션 명령의 `queue-limit` 키워드 옵션 사용). 기본 `queue-limit` 인수는 높은 우선순위 대기열의 경우 20개, 중간 대기열의 경우 40개, 보통의 경우 60개, 낮은 경우 80개입니다.

참고: DEC(Digital Equipment Corporation) LAT 트래픽을 브리징할 경우 라우터가 매우 적은 패킷을 삭제해야 합니다. 그렇지 않으면 LAT 세션이 예기치 않게 종료될 수 있습니다. 라우터에서 출력 패킷을 삭제하는 경우 우선 순위가 높은 대기열 깊이가 약 100(`queue-limit` 키워드로 지정됨)입니다. 직렬 회선이 약 50%의 대역폭 사용률을 받는 경우 일반적인 작업 값입니다. 라우터가 패킷을 삭제하고 있고 활용률이 100%인 경우 다른 회선이 필요합니다.

DEC LAT를 브리징할 때 혼잡을 완화하는 또 다른 툴은 LAT 압축입니다. `interface configuration` 명령 `bridge-group group lat-compression`을 사용하여 LAT 압축을 구현할 수 있습니다.

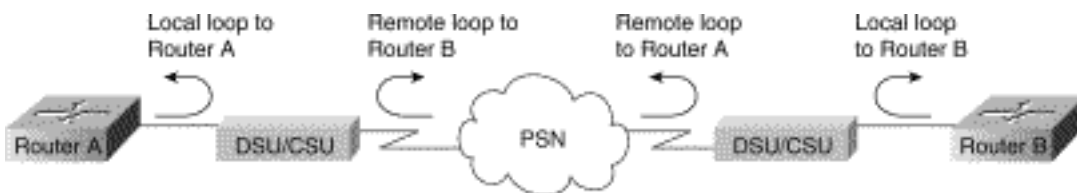
특수 직렬 회선 테스트

라우터에서 사용할 수 있는 기본 진단 기능 외에도 다양한 보조 툴과 기술을 사용하여 케이블, 스위칭 장비, 모뎀, 호스트 및 원격 인터넷워킹 하드웨어의 상태를 확인할 수 있습니다. 자세한 내용은 CSU, DSU, 직렬 분석기 또는 기타 장비에 대한 설명서를 참조하십시오.

CSU 및 DSU 루프백 테스트

`show interfaces serial EXEC` 명령의 출력에 직렬 회선이 작동하지만 회선 프로토콜이 다운되었음을 나타내는 경우 CSU/DSU 루프백 테스트를 사용하여 문제의 원인을 확인합니다. 먼저 로컬 루프백 테스트를 수행한 다음 원격 테스트를 수행합니다. 그림 15-9는 CSU/DSU 로컬 및 원격 루프백 테스트의 기본 토폴로지를 보여줍니다.

그림 15-9: CSU/DSU 로컬 및 원격 루프백 테스트



참고: 이러한 테스트는 기본적으로 일반적이며 CSU 또는 DSU에 인터넷워킹 시스템을 연결하는 것으로 가정합니다. 그러나 기본 제공 CSU/DSU 기능이 있는 멀티플렉서에 연결하는 테스트도 기본적으로 동일합니다. X.25 또는 PSN(Frame Relay packet-switched network) 환경에서는 루프백 개념이 없으므로 루프백 테스트는 X.25 및 Frame Relay 네트워크에 적용되지 않습니다.

HDLC 또는 PPP 링크에 대한 CSU 및 DSU 로컬 루프백 테스트

다음은 기본 제공 시스템 진단 기능과 함께 루프백 테스트를 수행하기 위한 일반적인 절차입니다.

1. CSU/DSU를 로컬 루프 모드로 설정합니다(공급업체 설명서 참조). 로컬 루프 모드에서는 회선

클럭(T1 서비스에서)의 사용이 종료되고 DSU는 로컬 클럭을 사용해야 합니다.

2. **show interfaces serial EXEC** 명령을 사용하여 라인 상태가 "line protocol is down"에서 "line protocol is up(loaded)"로 변경되는지 아니면 작동 중지 상태인지 확인할 수 있습니다.
3. CSU 또는 DSU가 로컬 루프백 모드에 있을 때 회선 프로토콜이 나타나면 직렬 연결의 원격 끝에서 문제가 발생함을 나타냅니다. 상태 라인이 상태를 변경하지 않으면 라우터, 연결 케이블 또는 CSU/DSU에 문제가 발생할 수 있습니다.
4. 문제가 로컬인 것으로 나타나면 **debug serial interface privileged EXEC** 명령을 사용합니다.
5. CSU/DSU를 로컬 루프 모드에서 해제합니다. 회선 프로토콜이 다운되면 **debug serial interface** 명령 출력은 **keepalive** 카운터가 증가하지 않음을 나타냅니다.
6. CSU/DSU를 로컬 루프 모드로 다시 배치합니다. 따라서 **keepalive** 패킷이 증가하기 시작해야 합니다. 특히 **mineseen** 및 표시된 **keepalive**의 값은 10초마다 증가합니다. 이 정보는 **디버그 직렬 인터페이스** 출력에 나타납니다. **keepalive**가 증가하지 않으면 인터페이스 카드 또는 네트워크에 타이밍 문제가 있을 수 있습니다. 타이밍 문제를 수정하는 방법에 대한 자세한 내용은 이 장의 앞부분에 있는 "클럭킹 문제 해결" 절을 참조하십시오. **keepalive**가 증가하지 않으면 인터페이스 카드 또는 네트워크에 타이밍 문제가 있을 수 있습니다. 타이밍 문제를 수정하는 방법에 대한 자세한 내용은 이 장의 앞부분에 있는 "클럭킹 문제 해결" 절을 참조하십시오.
7. 로컬 라우터, CSU/DSU 하드웨어 및 연결된 케이블을 확인합니다. 케이블이 T1 링크의 권장 길이(15.24m) 또는 25피트(7.62m) 내에 있는지 확인합니다. 케이블이 올바른 포트에 연결되었는지 확인합니다. 필요한 경우 결함이 있는 장비를 교체합니다.

그림 15-10은 HDLC 직렬 연결에 대한 **debug serial interface** 명령의 출력(누락된 **keepalive**)을 보여주며, 이로 인해 줄이 다운되고 인터페이스가 재설정됩니다.

그림 15-10: **debug serial interface** 명령 출력

```
router# debug serial interface

Serial1: HDLC nyseq 636119, mineseen 636119, yourseen 515032, line up
Serial1: HDLC nyseq 636120, mineseen 636120, yourseen 515033, line up
Serial1: HDLC nyseq 636121, mineseen 636121, yourseen 515034, line up
Serial1: HDLC nyseq 636122, mineseen 636122, yourseen 515035, line up
Serial1: HDLC nyseq 636123, mineseen 636123, yourseen 515036, line up
Serial1: HDLC nyseq 636124, mineseen 636124, yourseen 515037, line up
Serial1: HDLC nyseq 636125, mineseen 636125, yourseen 515038, line up
Serial1: HDLC nyseq 636126, mineseen 636126, yourseen 515039, line up
Serial1: HDLC nyseq 636127, mineseen 636127, yourseen 515040, line up
Serial1: HDLC nyseq 636128, mineseen 636127, yourseen 515041, line up
Serial1: HDLC nyseq 636129, mineseen 636129, yourseen 515042, line up
Serial1: HDLC nyseq 636130, mineseen 636130, yourseen 515043, line up
Serial1: HDLC nyseq 636131, mineseen 636130, yourseen 515044, line up
Serial1: HDLC nyseq 636132, mineseen 636130, yourseen 515045, line up
Serial1: HDLC nyseq 636133, mineseen 636130, yourseen 515046, line down
```

1 missed keepalive

3 missed keepalives

Line goes down, interface resets

HDLC 또는 PPP 링크에 대한 CSU 및 DSU 원격 루프백 테스트

로컬 하드웨어가 제대로 작동하는지 확인했지만 직렬 링크를 통해 연결을 설정하려고 할 때 여전히 문제가 발생하는 경우 원격 루프백 테스트를 사용하여 문제 원인을 격리하십시오.

참고: 이 원격 루프백 테스트에서는 HDLC 캡슐화가 사용되고 있으며 이전 로컬 루프 테스트가 이 테스트 바로 전에 수행되었다고 가정합니다.

루프백 테스트를 수행하려면 다음 단계가 필요합니다. 루프백 테스트를 수행하려면 다음 단계가 필요합니다.

1. 원격 CSU 또는 DSU를 원격 루프백 모드로 전환합니다(공급업체 설명서 참조).

2. **show interfaces serial EXEC** 명령을 사용하여 라인 프로토콜이 "Serial x is up, line protocol is up (loaded)"이라는 상태 줄로 작동 상태로 유지되는지 아니면 "line protocol is down"이라는 상태 줄로 다운되는지 확인합니다.
3. 회선 프로토콜이 작동(반복되는 상태)된 경우, 직렬 연결의 원격 종료(원격 CSU/DSU와 원격 라우터 간)에 문제가 있을 수 있습니다. 원격 끝에서 로컬 및 원격 테스트를 모두 수행하여 문제 소스를 격리합니다.
4. 원격 루프백 모드가 활성화될 때 회선 상태가 "line protocol is down"으로 변경되면 해당 밀도가 올바르게 유지되는지 확인합니다. CSU/DSU는 임대 회선이나 다른 캐리어 서비스(예: ESF 및 B8ZS)에서 사용하는 것과 동일한 프레임링 및 코딩 체계를 사용하도록 구성해야 합니다.
5. 문제가 계속되면 WAN 네트워크 관리자 또는 WAN 서비스 조직에 문의하십시오.

[show interfaces serial 명령에 대한 자세한 정보](#)

다음 하위 섹션에서는 **show interfaces serial** 명령의 매개변수, 구문 설명, 샘플 출력 표시 및 필드 설명을 다룹니다.

[show interfaces serial parameters](#)

직렬 인터페이스에 대한 정보를 표시하려면 **show interfaces serial** privileged EXEC 명령을 사용합니다.

```
show interfaces serial [number] [accounting]
show interfaces serial [number [:channel-group] [accounting] (Cisco 4000 series)
show interfaces serial [slot | port [:channel-group]] [accounting] (Cisco 7500 series)
show interfaces serial [type slot | port-adapter | port] [serial]
(ports on VIP cards in the Cisco 7500 series)
show interfaces serial [type slot | port-adapter | port] [:t1-channel] [accounting | crb]
(CT3IP in Cisco 7500 series)
```

[구문 설명](#)

- **number**-선택 사항입니다. 포트 번호입니다.
- **accounting**-선택 사항입니다. 인터페이스를 통해 전송된 각 프로토콜 유형의 패킷 수를 표시합니다.
- **:channel-group**-선택 사항입니다. NPM이 있는 Cisco 4000 Series 또는 MIP가 있는 Cisco 7500 Series에서 channel-group controller configuration 명령으로 정의된 0~23 범위의 T1 채널 그룹 번호를 지정합니다.
- **slot** -슬롯 정보에 적합한 하드웨어 설명서를 참조합니다.
- **port** -포트 정보에 적합한 하드웨어 설명서를 참조합니다.
- **port-adapter**-포트 어댑터 호환성에 대한 자세한 내용은 해당 하드웨어 설명서를 참조하십시오.
- **:t1-channel**-선택 사항입니다. CT3IP의 경우 T1 채널은 1에서 28 사이의 숫자입니다.
- CT3IP의 T1 채널은 다른 Cisco 제품과 함께 사용되는 기존의 0 기반 체계(0~27)보다 1~28의 번호가 지정됩니다. 이는 Channelized T3 장비 내에서 T1 채널에 대한 Telco 번호 지정 체계와 일관성을 유지하기 위한 것입니다.
- **crb**-선택 사항입니다. 인터페이스 라우팅 및 브리징 정보를 표시합니다.

[명령 모드](#)

특별 권한 EXEC

사용 지침

이 명령은 Cisco 4000 Series용 Cisco IOS Release 10.0에 처음 나타났습니다. Cisco 7000 Series용 Cisco IOS Release 11.0에 처음 등장했으며 CT3IP를 포함하도록 Cisco IOS Release 11.3에서 수정되었습니다.

샘플 표시

다음은 동기식 직렬 인터페이스에 대한 **show interfaces** 명령의 샘플 출력입니다.

```
Router# show interfaces serial
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 150.136.190.203, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 0:00:07, output 0:00:00, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    16263 packets input, 1347238 bytes, 0 no buffer
    Received 13983 broadcasts, 0 runts, 0 giants
    2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
  1 carrier transitions
    22146 packets output, 2383680 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets, 0 restarts
```

필드 설명

표 15-9: **show interfaces serial** Field Descriptions - 이 표에서는 출력에 표시되는 중요한 필드에 대해 설명합니다.

필드	설명
직렬 ...{up 임 아 래쪽 }...관리 목적으 로 다 운됨	인터페이스 하드웨어가 현재 활성 상태인지(캐리어 탐지가 있는지) 또는 관리자가 해제했는지 여부를 나타냅니다.
회선 프로토 콜은 {up입 니다. 아래쪽 }	라인 프로토콜을 처리하는 소프트웨어 프로세스에서 사용 가능한 라인(즉, keepalives가 성공함)을 고려하는지 또는 관리자가 삭제했는지 여부를 나타냅니다.
회선 프로토 콜은	라인 프로토콜을 처리하는 소프트웨어 프로세스에서 사용 가능한 라인(즉, keepalives가 성공함)을 고려하는지 또는 관리자가 삭제했는지 여부를

{up입 니다. 아래쪽 }	나타냅니다.
하드웨 어는	하드웨어 유형을 지정합니다.
인터넷 주소:	인터넷 주소 및 서브넷 마스크를 지정합니다.
MTU	인터페이스의 최대 전송 단위입니다.
대역폭	인터페이스에 대해 구성된 대역폭 매개 변수의 값 (초당 킬로비트 수)을 나타냅니다. bandwidth 매개 변수는 IGRP 메트릭만 계산하는 데 사용됩니다. 인터페이스가 기본(T1의 경우 1536 또는 1544, 표준 동기 직렬 회선의 경우 56)과 일치하지 않는 회선 속도로 직렬 회선에 연결된 경우 bandwidth 명령을 사용하여 이 직렬 회선의 정확한 라인 속도를 지정합니다.
DLY	인터페이스의 지연(마이크로초)
의존적	인터페이스의 신뢰성은 255(255/255는 100% 안정성)의 극히 일부로서 5분 동안의 지수 평균으로 계산됩니다.
로드	인터페이스의 신뢰성은 255(255/255는 100% 안정성)의 극히 일부로서 5분 동안의 지수 평균으로 계산됩니다.
캡슐화	인터페이스에 할당된 캡슐화 방법입니다.
루프백	루프백이 설정되었는지 여부를 나타냅니다.
keepali ve	keepalive를 설정할지 여부를 나타냅니다.
마지막 입력	인터페이스에서 마지막 패킷을 성공적으로 수신한 이후의 시간, 분 및 초 수입니다. Dead 인터페이스가 실패한 경우를 파악하는 데 유용합니다.
마지막 출력	마지막 패킷이 인터페이스에 의해 성공적으로 전송된 이후 경과한 시간, 분 및 초 수입니다. 마지막 패킷이 인터페이스에 의해 성공적으로 전송된 이후 경과한 시간, 분 및 초 수입니다.
출력 중단	너무 오래 걸린 전송으로 인해 인터페이스가 마지막으로 재설정된 이후의 시간, 분 및 초(또는 전혀 안 함) 수입니다. 마지막 필드의 시간이 24시간을 초과하면 날짜 및 시간이 인쇄됩니다. 해당 필드가 오버플로되면 별표가 인쇄됩니다.
출력 대기열 , 입력 대기열 삭제, 삭제	출력 및 입력 대기열의 패킷 수입니다. 각 숫자 뒤에는 슬래시, 큐의 최대 크기, 큐가 가득 찬 패킷 수가 옵니다.
5분 입 력 속 도 5분	지난 5분 동안 초당 전송된 평균 비트 및 패킷 수입니다. 5분 입력 및 출력 속도는 주어진 5분 기간 동안 초당 트래픽의 근사화로만 사용해야 합니다.

출력 속도	이러한 속도는 5분의 시간 상수로 기하급수적으로 가중 평균입니다. 4개의 시간 상수가 전달되어야 평균이 해당 기간 동안 균일한 트래픽 스트림의 순간 속도의 2% 내에 속합니다.
패킷 입력	시스템에서 받은 오류 없는 총 패킷 수입입니다.
바이트	시스템에서 수신한 오류 없는 패킷에서 데이터 및 MAC 캡슐화를 포함한 총 바이트 수입입니다.
버퍼 없음	기본 시스템에 버퍼 공간이 없어 삭제된 수신된 패킷 수입입니다. 무시된 수와 비교합니다. 이더넷 네트워크의 브로드캐스트 스톱 및 직렬 회선의 노이즈 폭증은 입력 버퍼 이벤트가 없는 경우가 많습니다.
수신... 브로드캐스트	인터페이스에서 받은 총 브로드캐스트 또는 멀티캐스트 패킷 수입입니다.
runts	미디어의 최소 패킷 크기보다 작기 때문에 삭제된 패킷 수입입니다.
giants	미디어의 최대 패킷 크기를 초과하여 삭제된 패킷 수입입니다.
입력 오류	버퍼 없음, 런타임, 대형, CRC, 프레임, 오버런, 무시 및 중단 수의 총 수입입니다. 다른 입력 관련 오류는 카운트를 증가시킬 수도 있으므로 이 합계가 다른 카운트와 일치하지 않을 수 있습니다.
CRC	원본 스테이션 또는 원엔드 디바이스에서 생성된 순환 중복 검사가 수신된 데이터에서 계산된 체크섬과 일치하지 않습니다. 직렬 링크에서 CRC는 일반적으로 데이터 링크의 노이즈, 게인 적중률 또는 기타 전송 문제를 나타냅니다.
프레임	CRC 오류와 정수가 아닌 8진수 수가 잘못 수신된 패킷 수입입니다. 직렬 회선에서는 일반적으로 노이즈 또는 기타 전송 문제의 결과입니다.
오버런	입력 속도가 수신자의 데이터 처리 능력을 초과했기 때문에 직렬 수신기 하드웨어에서 수신된 데이터를 하드웨어 버퍼로 전달할 수 없는 횟수입니다.
무시됨	인터페이스 하드웨어가 내부 버퍼에서 낮게 실행되었기 때문에 인터페이스에서 무시한 수신된 패킷 수입입니다. 브로드캐스트 스톱과 노이즈 폭증으로 인해 무시된 수가 증가할 수 있습니다.
중단	직렬 인터페이스에서 1비트의 잘못된 시퀀스입니다. 이는 일반적으로 직렬 인터페이스와 데이터 링크 장비 간의 잠금 문제를 나타냅니다.
캐리어 전환	캐리어가 직렬 인터페이스의 신호 감지 상태가 변경된 횟수. 예를 들어, DCD(데이터 캐리어 탐지)가 작동 중지되고 작동하면 캐리어 전환 카운터가 두 번 증가합니다. 캐리어 감지 회선의 상태가 자주 변경되는 경우 모뎀 또는 회선 문제를 나타냅니다.

패킷 출력	시스템에서 전송한 총 메시지 수입니다.
바이트 출력	시스템에서 전송한 데이터 및 MAC 캡슐화를 포함한 총 바이트 수입니다.
언더런	전송기가 라우터에서 처리할 수 있는 속도보다 빠르게 실행된 횟수입니다. 일부 인터페이스에서는 이 오류가 보고되지 않을 수 있습니다.
출력 오류	검사 중인 인터페이스에서 데이터그램의 최종 전송을 방해하는 모든 오류의 합계입니다. 일부 데이터그램에는 둘 이상의 오류가 있을 수 있으며, 다른 데이터그램에는 특정 테이블 범주에 속하지 않는 오류가 있을 수 있으므로 이 값이 열거 출력 오류의 합계와 균형을 이루지는 않을 수 있습니다.
충돌	이더넷 충돌로 인해 재전송된 메시지 수입니다. 이는 일반적으로 과도한 LAN(즉, 이더넷 또는 트랜시버 케이블이 너무 길거나, 스테이션 간 리피터 2개 이상 또는 다중 구간(Cascaded) 멀티포트 트랜시버가 너무 많음)의 결과입니다. 일부 충돌은 정상입니다. 그러나 충돌 비율이 약 4% 또는 5%로 증가할 경우 세그먼트에 결함이 있는 장비가 없는지 확인하고 기존 스테이션을 새 세그먼트로 이동하는 것이 좋습니다. 충돌하는 패킷은 출력 패킷에서 한 번만 계산됩니다.
인터페이스 재설정	인터페이스가 완전히 재설정된 횟수입니다. 이는 전송을 위해 대기열에 있는 패킷이 몇 초 내에 전송되지 않은 경우 발생할 수 있습니다. 직렬 회선에서 이 문제는 전송 클럭 신호를 제공하지 않는 모뎀이 고장나거나 케이블 문제로 인해 발생할 수 있습니다. 시스템에서 캐리어가 시리얼 인터페이스의 라인 탐지가 작동 중이지만 라인 프로토콜이 다운된 것을 발견하면 인터페이스를 재시작하기 위해 주기적으로 인터페이스를 재설정합니다. 인터페이스가 루프백 또는 종료된 경우에도 인터페이스 재설정이 발생할 수 있습니다.
재시작	오류로 인해 컨트롤러가 다시 시작된 횟수입니다.
경보 표시, 원격 경보, rx LOF, rx LOS	CSU/DSU 경보 수, 프레임 손실 및 신호 손실 수 신 발생 횟수입니다.
BER 비활성, NELR 비활성, FELR 비활성	BER(Bit Error Rate) 경보, NELR(Near-End Loop Remote) 및 FELR(Far-End Loop Remote)에 대한 G.703-E1 카운터의 상태입니다. NELR 또는 FELR은 설정할 수 없습니다.

T1 문제 해결

이 섹션에서는 다이얼인 고객을 위한 T1 회로의 문제 해결 기법 및 절차에 대해 설명합니다.

show controller t1 명령을 사용하여 문제 해결

이 명령은 컨트롤러 하드웨어와 관련된 컨트롤러 상태를 표시합니다. 표시되는 정보는 일반적으로 기술 지원 담당자가 수행하는 진단 작업에만 유용합니다.

NMP(Network Management Processor) 또는 MIP(MultiChannel Interface Processor)는 포트 어댑터를 쿼리하여 현재 상태를 확인할 수 있습니다. T1 링크에 대한 통계를 표시하려면 **show controller t1** 명령을 실행합니다.

슬롯 및 포트 번호를 지정하면 15분 간격에 대한 통계가 표시됩니다. **show controller t1 EXEC** 명령은 물리적 레이어 및 데이터 링크 레이어 문제를 논리적으로 해결하기 위한 정보를 제공합니다. 이 섹션에서는 **show controller t1** 명령을 사용하여 논리적으로 문제를 해결하는 방법에 대해 설명합니다.

대부분의 T1 오류는 잘못 구성된 행으로 인해 발생합니다. 통신 사업자가 권장하는 내용에 따라 라인 인코딩, 프레이밍 및 클럭 소스가 구성되어 있는지 확인합니다.

컨트롤러 t1 조건 표시

T1 컨트롤러는 다음 세 가지 상태 중 하나일 수 있습니다.

- 관리 기능 저하
- 아래로
- 위로

T1 컨트롤러가 관리적으로 다운되었습니까?

컨트롤러가 수동으로 종료되었을 때 관리상 종료됩니다. 이 오류를 수정하려면 컨트롤러를 다시 시작해야 합니다.

1. 활성화 모드를 입력합니다.

```
maui-nas-03>en
Password:
maui-nas-03#
```

2. 전역 컨피그레이션 모드로 들어갑니다.

```
maui-nas-03#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
maui-nas-03(config)#
```

3. 컨트롤러 컨피그레이션 모드로 들어갑니다.

```
maui-nas-03(config)#controller t1 0
maui-nas-03(config-controlle)#
```

4. 컨트롤러를 다시 시작합니다.

```
maui-nas-03(config-controlle)#shutdown
maui-nas-03(config-controlle)#no shutdown
```

전화가 연결되었습니까?

T1 컨트롤러 및 행이 작동하지 않을 경우 다음 메시지 중 하나가 **show controller t1 EXEC** 출력에 나타나는지 확인합니다.

- 수신기의 프레임 손실
- 수신기에 신호가 손실됨

T1 수신기에 프레임 손실이 있는 경우:

T1 수신기에 프레임 손실이 있는 경우 다음 단계를 수행합니다.

1. 포트에 구성된 프레이밍 형식이 라인의 프레이밍 형식과 일치하는지 확인합니다. 실행 중인 컨피그레이션 또는 **show controller t1** 명령 출력에서 컨트롤러의 프레이밍 형식을 확인할 수 있습니다. 프레이밍 형식을 변경하려면 프레이밍 {SF 아래와 같이 컨트롤러 컨피그레이션 모드에서 | ESF} 명령:

```
maui-nas-03#configure terminal
```

구성 명령을 한 줄에 하나씩 입력합니다. CNTL/Z로 끝냅니다.

```
maui-nas-03 (config)#controller t1 0  
maui-nas-03 (config-controller)#framing esf
```

2. 다른 프레이밍 형식을 사용하여 경보가 지워지는지 확인합니다.
3. 케이블 길이 {long을 사용하여 줄 기본 설정을 **변경합니다.** | short} 명령

LBO(Line Build Out)는 회로의 첫 번째 리피터까지의 거리를 기준으로 데시벨 단위로 손실을 보정합니다. 디바이스에서 리피터까지의 거리가 더 길면 회선의 신호 강도를 높여 해당 거리의 손실을 보완해야 합니다.

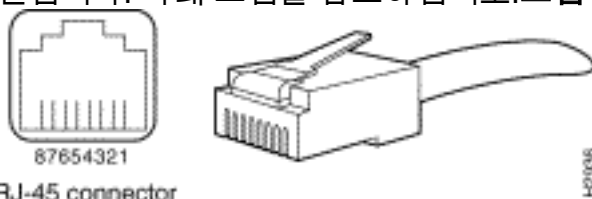
구축 설정에 대한 자세한 내용은 서비스 제공업체 및 Cisco IOSTO 명령 참조를 참조하십시오.

문제가 해결되지 않으면 아래의 "T1 수신기에 신호 손실이 있는 경우" 섹션을 진행합니다.

T1 수신기에 신호 손실이 있는 경우:

T1 수신기에 신호 손실이 있는 경우 다음 단계를 수행합니다.

1. 인터페이스 포트와 T1 서비스 공급자의 장비(또는 T1 터미널 장비) 간의 케이블이 올바르게 연결되어 있는지 확인합니다. 케이블이 올바른 포트에 연결되어 있는지 확인합니다. 필요한 경우 케이블 연결을 수정합니다.
2. 케이블 무결성을 확인합니다. 케이블의 휴식 또는 기타 물리적 이상을 확인합니다. 핀아웃이 올바르게 설정되었는지 확인합니다. 필요한 경우 케이블을 교체합니다.
3. 케이블 커넥터를 확인합니다. 전송 및 수신 쌍 또는 열린 수신 쌍을 취소하면 오류가 발생할 수 있습니다. 수신 쌍을 라인 1 및 2로 설정합니다. 전송 쌍을 라인 4 및 5로 설정합니다. RJ-45 잭의 핀은 1부터 8까지 번호가 매겨집니다. 핀 1은 금속 핀이 있는 잭을 볼 때 가장 왼쪽에 있는 핀입니다. 아래 그림을 참조하십시오. **그림 15-10: RJ-45 케이블**



4. 롤오버 케이블을 사용해 보십시오.

각 단계에서 **show controller t1 EXEC** 명령을 실행하여 컨트롤러가 오류를 발생하는지 확인합니다.

show controller t1 출력에서 줄이 루프백 모드에 있는지 확인합니다. 행은 테스트용으로만 루프백 모드여야 합니다.

루프백을 끄려면 아래와 같이 컨트롤러 컨피그레이션 모드에서 **no loopback** 명령을 사용합니다.

```
maui-nas-03(config-controlle)#no loopback
```

컨트롤러에 경보가 표시되는 경우:

컨트롤러가 알람을 표시하는지 확인하려면 **show controller** 명령 출력을 확인합니다.

이제 다양한 경보와 이를 수정하는 데 필요한 절차에 대해 설명하겠습니다.

수신(RX) AIS(Alarm Indication Signal)(파란색):

수신된 AIS(Alarm Indication Signal)는 포트에 연결된 장비의 라인 업스트림에서 경보가 발생함을 의미합니다.

1. 포트에 구성된 프레임링 형식이 라인의 프레임링 형식과 일치하는지 확인합니다. 그렇지 않은 경우 컨트롤러의 프레임링 형식을 라인의 형식과 일치하도록 변경합니다.
2. 서비스 공급업체에 문의하여 Telco 내에서 잘못된 컨피그레이션을 확인합니다.

수신(Rx) 원격 경보 표시(RAID)(노란색):

수신한 RAID는 원엔드 장비가 업스트림 장비에서 수신하는 신호에 문제가 있음을 의미합니다.

1. 외부 루프백 케이블을 포트에 삽입합니다. 루프백 플러그를 만들려면 장 뒷부분의 "루프백 플러그 생성" 섹션을 참조하십시오.
2. 경보가 있는지 확인합니다. 경보가 표시되지 않으면 로컬 하드웨어가 양호한 상태일 수 있습니다. 이 경우:케이블을 확인합니다. 자세한 내용은 "T1 수신기에 신호 손실이 있는 경우" 절을 참조하십시오.원격 끝의 설정을 확인하고 포트 설정과 일치하는지 확인합니다.문제가 계속되면 서비스 공급업체에 문의하십시오.
3. 루프백 플러그를 제거하고 T1 줄을 다시 연결합니다.
4. 케이블을 확인합니다. 자세한 내용은 "T1 수신기에 신호 손실이 있는 경우" 절을 참조하십시오.
5. 라우터의 전원을 껐다가 켜십시오.
6. T1 회선을 다른 포트에 연결합니다. 회선 설정과 동일한 설정으로 포트를 구성합니다. 문제가 지속되지 않으면 하나의 포트에 결함이 있습니다.T1 회선을 원래 포트에 다시 연결합니다."T1 오류 이벤트 문제 해결" 섹션으로 이동합니다.문제가 계속되면 다음을 수행합니다.
7. "하드웨어 루프백 플러그 테스트 수행" 섹션에 설명된 대로 하드웨어 루프 테스트를 수행합니다.
8. T1 컨트롤러 카드를 교체합니다.
9. "T1 오류 이벤트 문제 해결" 섹션으로 이동합니다.

원격 경보 전송 송신기(빨간색):

CSU가 T1 라인의 프레이밍 패턴과 동기화할 수 없는 경우 빨간색 경보가 선언됩니다.

1. 포트에 구성된 프레이밍 형식이 라인의 프레이밍 형식과 일치하는지 확인합니다. 컨트롤러의 프레이밍 형식을 줄의 형식과 일치하도록 변경하지 않는 경우
2. 원격 끝의 설정을 확인하고 포트 설정과 일치하는지 확인합니다.
3. 서비스 공급업체에 문의하십시오.

Transmit(Tx) RAID(Remote Alarm Indication)(노란색):

인터페이스에서 전송된 RAID는 인터페이스에 원엔드 장비에서 수신하는 신호에 문제가 있음을 나타냅니다.

1. 원격 끝의 설정을 확인하고 포트 설정과 일치하는지 확인합니다.
2. 전송 RAID에는 T1 포트/카드에서 멀리 떨어진 장비에서 오는 신호와 함께 발생하는 문제의 특성을 나타내는 다른 경보와 함께 사용해야 합니다.

해당 문제를 해결하여 전송 RAID를 해결합니다.

전송(Tx) AIS(파란색):

전송(Tx) AIS(파란색)를 수정하려면 아래 단계를 수행하십시오.

1. 포트에 구성된 프레이밍 형식이 라인의 프레이밍 형식과 일치하는지 확인합니다. 그렇지 않으면 불일치를 수정합니다.
2. 라우터의 전원을 껐다가 켜십시오.
3. T1 회선을 다른 포트에 연결합니다. 회선 설정과 동일한 설정으로 포트를 구성합니다.
4. "하드웨어 루프백 플러그 테스트 수행" 섹션에 설명된 대로 하드웨어 루프 테스트를 수행합니다.
5. T1 컨트롤러 카드를 교체합니다.
6. "T1 오류 이벤트 문제 해결" 섹션으로 이동합니다.

T1 오류 이벤트 트러블슈팅

`show controller t1 EXEC` 명령은 문제 해결에 사용할 수 있는 오류 메시지를 제공합니다. 이제 몇 가지 오류 메시지와 오류를 수정하는 방법에 대해 살펴보겠습니다.

오류 카운터가 증가하고 있는지 확인하려면 `show controller t1` 명령을 반복해서 실행합니다. 현재 간격의 카운터 값을 확인합니다.

프레이밍 및 선형코드 설정에 대해서는 서비스 공급업체에 문의하십시오. ESF 프레이밍 및 AMI 라인 에코딩과 SF 프레이밍을 함께 사용하여 B8ZS 라인 에코딩을 사용하는 것이 좋습니다.

Slip Secs 카운터가 증가하고 있습니다.

T1 행에 전표가 있으면 잠금 문제가 있음을 나타냅니다. T1 제공자(Telco)는 CPE(Customer Premises Equipment)를 동기화해야 하는 잠금을 제공합니다.

1. 클럭 소스가 네트워크에서 파생되는지 확인합니다. 클럭 소스가 라인 프라이머리(Line Primary)인지 확인하여 확인할 수 있습니다. **참고:** 액세스 서버에 여러 개의 T1이 있는 경우 하나만 기본 서버가 될 수 있고 다른 T1은 기본 서버에서 시계를 파생합니다. 이 경우 기본 클럭

소스로 지정된 T1 라인이 올바르게 구성되었는지 확인합니다.

2. 컨트롤러 컨피그레이션 모드에서 T1 클럭 소스를 올바르게 설정합니다.

```
maui-nas-03(config-controlle)#clock source line primary
```

프레이밍 손실 초 카운터가 증가하고 있습니다.

프레이밍 손실 초 카운터가 증가할 때 다음 단계를 수행합니다.

1. 포트에 구성된 프레이밍 형식이 라인의 프레이밍 형식과 일치하는지 확인합니다. **show controller t1** 출력에서 프레이밍이 {ESF/SF}인지 확인하여 확인할 수 있습니다.
2. 프레이밍 형식을 변경하려면 프레이밍 {SF}를 사용하십시오. 아래와 같이 컨트롤러 컨피그레이션 모드에서 |ESF} 명령을 실행합니다.

```
maui-nas-03(config-controlle)#framing esf
```

3. 케이블 길이 {long}를 사용하여 줄 빌드를 변경합니다. |short} 명령
구축 설정에 대한 자세한 내용은 서비스 제공업체 및 Cisco IOSTO 명령 참조를 참조하십시오.

라인 코드 위반이 증가하고 있습니다.

라인 코드 위반이 증가하는 경우 다음 단계를 수행합니다.

1. 포트에 구성된 라인 인코딩이 라인의 프레이밍 형식과 일치하는지 확인합니다. **show controller t1** 출력에서 라인 코드가 {B8ZS|AMI}인지 확인하여 확인할 수 있습니다.
2. 선형코드를 변경하려면 선 코드 {ami}를 사용하십시오. 아래와 같이 컨트롤러 컨피그레이션 모드에서 |b8zs} 명령을 실행합니다.

```
maui-nas-03(config-controlle)#linecode b8zs
```

3. 케이블 길이 {long}를 사용하여 줄 빌드를 변경합니다. |short} 명령
기본 설정 설정에 대한 자세한 내용은 서비스 공급자 및 Cisco IOS® 명령 참조를 참조하십시오.

ISDN 스위치 유형 및 PRI-그룹이 올바르게 구성되었는지 확인

show running-config 명령을 사용하여 ISDN 스위치 유형 및 PRI-group timeslot이 올바르게 구성되었는지 확인합니다. 올바른 값은 서비스 공급업체에 문의하십시오.

ISDN 스위치 유형 및 PRI 그룹을 변경하려면

```
maui-nas-03#configure terminal
maui-nas-03(config)#isdn switch-type primary-5ess
maui-nas-03(config)#controller t1 0
maui-nas-03(config-controlle)#pri-group timeslots 1-24
```

신호 채널 확인

오류 카운터가 증가하지 않지만 문제가 지속되면 신호 채널이 작동 및 올바르게 구성되었는지 확인하십시오.

1. **show interface serial x:23** 명령을 실행합니다. 여기서 x는 인터페이스 번호로 교체해야 합니다

다.

2. 인터페이스가 작동 중인지 확인합니다. 인터페이스가 작동되지 않은 경우 **no shutdown** 명령을 사용하여 인터페이스를 활성화합니다.

```
maui-nas-03#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
maui-nas-03 (config)#interface serial 0:23
maui-nas-03 (config-if)#no shutdown
```

3. 캡슐화가 PPP인지 확인합니다. 인터페이스에서 PPP를 사용하지 않는 경우 인터페이스 컨피그레이션 모드에서 **캡슐화 ppp** 명령을 사용하여 수정합니다.

```
maui-nas-03 (config-if)#encapsulation ppp
```

4. 루프백이 설정되어 있는지 확인합니다. 루프백은 테스트 용도로만 설정해야 합니다. 루프백을 제거하려면 **no loopback** 명령을 사용합니다.

```
maui-nas-03 (config-if)#no loopback
```

5. 라우터의 전원을 껐다가 켜십시오.
6. 문제가 계속되면 서비스 공급자 또는 Cisco TAC에 문의하십시오.

PRI 문제 해결

PRI를 트러블슈팅할 때마다 T1이 양쪽 끝에서 완전히 실행 중인지 확인해야 합니다. 위에서 설명한 대로 레이어 1 문제가 해결된 경우 레이어 2 및 레이어 3 문제를 고려하십시오.

show isdn status 명령을 사용한 문제 해결

show isdn status 명령은 모든 ISDN 인터페이스의 스냅샷을 표시하는 데 사용됩니다. 레이어 1, 2 및 3의 상태를 표시합니다.

1. 레이어 1이 활성 상태인지 확인합니다. T1이 중단되지 않은 경우 레이어 1 상태는 항상 ACTIVE로 표시되어야 합니다. **show isdn status**가 레이어 1이 비활성화되었음을 나타내는 경우 T1 회선의 물리적 연결에 문제가 있습니다. "T1 컨트롤러 T1이 다운되었습니까?" 섹션을 참조하십시오. 또한 T1이 관리 목적으로 다운되지 않았는지 확인합니다. T1 컨트롤러를 **가동**하려면 **no shutdown** 명령을 사용합니다.
2. 레이어 2 상태가 MULTIPLE_FRAME_ESTABLISHED인지 확인합니다.

원하는 레이어 2 상태는 Multiple_Frame_Established이며, 이는 레이어 2 프레임을 교환하고 레이어 2 초기화를 완료했음을 나타냅니다.

레이어 2가 Multiple_Frame_Established가 아닌 경우 **show controller t1 EXEC** 명령을 사용하여 문제를 진단합니다. 이 장의 [show controller t1 명령을 사용한 문제 해결](#) 섹션을 참조하십시오.

show isdn status는 현재 상태의 스냅샷이므로 Multiple_Frame_Established를 나타내더라도 레이어 2가 위아래로 바운스될 수 있습니다. **debug isdn q921**을 사용하여 레이어 2가 안정적인지 확인합니다.

debug isdn q921 명령은 D-채널의 라우터에서 발생하는 데이터 링크 레이어(레이어 2) 액세스 절차를 표시합니다.

필요에 따라 **logging console** 또는 **terminal monitor** 명령을 사용하여 디버그 메시지를 표시하도록 구성되어 있는지 확인합니다.

참고: 프로덕션 환경에서 콘솔 로깅이 비활성화되어 있는지 확인합니다. show logging 명령을 입력합니다. 로깅이 활성화된 경우 콘솔 포트가 로그 메시지로 오버로드되는 즉시 액세스 서버가 간헐적으로 중지될 수 있습니다. no logging console 명령을 입력합니다.

참고: 디버그 isdn q921이 켜져 있고 디버그 출력을 받지 못한 경우 디버그 출력을 얻으려면 전화를 걸거나 컨트롤러를 재설정하십시오.

1. 레이어 2가 안정적인지 확인합니다. 서비스가 작동 및 작동 중지되지 않음을 나타내는 메시지에 대한 디버그 출력을 확인해야 합니다. 다음 유형의 디버그 출력이 표시되면 줄이 안정적이지 않습니다.

```
Mar 20 10:06:07.882: %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se0:23, TEI 0
changed to down
Mar 20 10:06:09.882: %LINK-3-UPDOWN: Interface Serial0:23, changed state to down
Mar 20 10:06:21.274: %DSX1-6-CLOCK_CHANGE: Controller 0 clock is now selected
as clock source
Mar 20 10:06:21.702: %ISDN-6-LAYER2UP: Layer 2 for Interface Se0:23, TEI 0 changed
to up
Mar 20 10:06:22.494: %CONTROLLER-5-UPDOWN: Controller T1 0, changed state to up
Mar 20 10:06:24.494: %LINK-3-UPDOWN: Interface Serial0:23, changed state to up
```

레이어 2가 안정적이지 않을 경우 이 장의 앞부분에서 "T1 오류 이벤트 문제 해결"을 참조하십시오.

2. 전송(TX) 및 수신(RX) 측면에서 모두 SAPI 메시지만 표시되는지 확인합니다.

```
Mar 20 10:06:52.505: ISDN Se0:23: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:06:52.505: ISDN Se0:23: RX <- RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.505: ISDN Se0:23: TX -> RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: RX <- RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: RX <- RRf sapi = 0 tei = 0 nr = 0
```

3. 레이어 2가 다시 초기화하려고 함을 나타내는 SABME 메시지가 표시되지 않는지 확인합니다. 이는 일반적으로 RP(Poll Requests)를 전송하고 스위치에서 응답을 받지 않거나 RRf(Poll Request)를 전송할 때 발생합니다. 다음은 SABME 메시지의 예입니다.

```
Mar 20 10:06:21.702: ISDN Se0:23: RX <- SABMEp sapi = 0 tei = 0
Mar 20 10:06:22.494: ISDN Se0:23: TX -> SABMEp sapi = 0 tei = 0
```

SABME 메시지가 표시되는 경우 show running-config 명령을 사용하여 ISDN 스위치 유형 및 PRI-group timeslot이 올바르게 구성되었는지 확인합니다. 올바른 값은 서비스 공급업체에 문의하십시오. ISDN 스위치 유형 및 PRI 그룹을 변경하려면

```
maui-nas-03#configure terminal
maui-nas-03(config)#isdn switch-type primary-5ess
maui-nas-03(config)#controller t1 0
maui-nas-03(config-controller)#pri-group timeslots 1-24
```

4. show interfaces serial x:23 명령을 사용하여 D-channel이 작동 중인지 확인합니다. D-채널이 가동되지 않은 경우 no shutdown 명령을 사용하여 이 명령을 실행합니다.

```
maui-nas-03(config)#interface serial 0:23
maui-nas-03(config-if)#no shutdown
```

5. 캡슐화가 PPP인지 확인합니다. 그렇지 않은 경우 캡슐화 ppp 명령을 사용하여 캡슐화를 설정합니다.

```
maui-nas-03(config-if)#encapsulation ppp
```

6. 인터페이스가 루프백 모드인지 확인합니다. 정상적인 작동을 위해 인터페이스는 루프백 모드에 있지 않아야 합니다.

```
maui-nas-03(config-if)#no loopback
```

7. 라우터의 전원을 껐다가 켜십시오.
8. 문제가 계속되면 서비스 제공업체 또는 Cisco TAC에 문의하십시오.

하드웨어 루프백 플러그 테스트 수행

하드웨어 루프백 플러그 테스트를 사용하여 라우터에 결함이 있는지 테스트할 수 있습니다. 라우터가 하드웨어 루프백 플러그 테스트를 통과하면 해당 문제가 라인의 다른 위치에 존재합니다.

루프백 플러그 생성:

루프백 플러그를 생성하려면 다음 단계를 수행합니다.

1. 와이어 커터를 사용하여 작동 중인 RJ-45 또는 RJ-48 케이블을 잘라 5인치 케이블과 커넥터가 연결되어 있도록 합니다.
2. 전선을 벗겨라.
3. 핀 1과 4의 와이어를 함께 비틀십시오.
4. 핀 2와 5의 와이어를 함께 비틀십시오.

RJ-45/48 잭의 핀은 1부터 8까지 번호가 매겨집니다. 핀 1은 금속 핀이 있는 잭을 볼 때 가장 왼쪽에 있는 핀입니다.

루프백 플러그 테스트 수행

루프백 플러그 테스트를 수행하려면 다음 단계를 수행합니다.

1. 문제의 T1 포트에 플러그를 삽입합니다.
2. **write memory** 명령을 사용하여 라우터 컨피그레이션을 저장합니다.

```
maui-nas-03#write memory
Building configuration...
[OK]
```

3. 캡슐화를 HDLC로 설정

```
maui-nas-03#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
maui-nas-03(config)#interface serial 0
maui-nas-03(config-if)#enc
maui-nas-03(config-if)#encapsulation HDLC
maui-nas-03(config-if)#^Z
```

4. 인터페이스에 IP 주소가 있는지 확인하려면 show running-config 명령을 사용합니다. 인터페이스에 IP 주소가 없는 경우 고유한 주소를 얻어 서브넷 마스크가 255.255.255.0인 인터페이스에 할당합니다.

```
maui-nas-03(config)#ip address 172.22.53.1 255.255.255.0
```

5. clear counters 명령을 사용하여 인터페이스 카운터를 지웁니다.

```
maui-nas-03#clear counters
Clear "show interfaces" counters on all interfaces [confirm]
maui-nas-03#
```

6. 이 장의 앞부분의 "Using Extended Ping Tests" 섹션에 설명된 대로 확장 ping 테스트를 수행합니다.

문제 해결 E1

이 섹션에서는 다이얼인 고객을 위한 E1 회로의 문제 해결 기법 및 절차에 대해 설명합니다.

show controller e1 명령을 사용하여 문제 해결

이 명령은 컨트롤러 하드웨어와 관련된 컨트롤러 상태를 표시합니다. 표시되는 정보는 일반적으로 기술 지원 담당자가 수행하는 진단 작업에만 유용합니다.

NMP 또는 MIP는 포트 어댑터를 쿼리하여 현재 상태를 확인할 수 있습니다. **show controller e1** 명령을 실행하여 E1 링크에 대한 통계를 표시합니다. 슬롯 및 포트 번호를 지정하면 15분 간격에 대한 통계가 표시됩니다.

show controller e1 EXEC 명령은 물리적 레이어 및 데이터 링크 레이어 문제를 논리적으로 해결하기 위한 정보를 제공합니다. 이 섹션에서는 **show controller e1** 명령을 사용하여 논리적으로 문제를 해결하는 방법에 대해 설명합니다.

대부분의 E1 오류는 잘못 구성된 행으로 인해 발생합니다. 서비스 제공자가 권장하는 내용에 따라 라인 인코딩, 프레임링, 클럭 소스 및 라인 종료(균형 또는 비균형)가 구성되었는지 확인합니다.

컨트롤러 e1 조건 표시

E1 컨트롤러는 다음 세 가지 상태 중 하나일 수 있습니다.

- 관리 기능 저하
- 아래로
- 위로

E1 컨트롤러가 관리적으로 다운되었습니까?

컨트롤러가 수동으로 종료되었을 때 관리상 종료됩니다. 이 오류를 수정하려면 컨트롤러를 다시 시작해야 합니다.

1. 활성화 모드를 입력합니다.

```
maui-nas-03>enable  
Password:  
maui-nas-03#
```

2. 전역 컨피그레이션 모드로 들어갑니다.

```
maui-nas-03#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
maui-nas-03(config)#
```

3. 컨트롤러 컨피그레이션 모드로 들어갑니다.

```
maui-nas-03(config)#controller e1 0  
maui-nas-03(config-controlle)#
```

4. 컨트롤러를 다시 시작합니다.

```
maui-nas-03(config-controlle)#shutdown  
maui-nas-03(config-controlle)#no shutdown
```

전화가 연결되었습니까?

E1 회선이 작동하지 않으면 회선 구성이 올바르고 원격 끝의 설정과 일치하는지 확인합니다.

1. 회선 및 원격 끝의 프레임링을 확인합니다. E1 라인의 경우 프레임링은 CRC4 또는 noCRC4입니다.
2. 회선과 원격 끝의 선형값을 확인합니다. Linecoding은 AMI 또는 HDB3입니다.
3. 라인 종료가 균형 또는 비균형(75ohm 또는 120ohm)으로 설정되어 있는지 확인합니다.

올바른 설정에 대한 자세한 내용은 서비스 공급업체에 문의하십시오. 필요에 따라 로컬 또는 원격 엔드디바이스 모두를 변경합니다.

E1 컨트롤러 및 행이 작동하지 않을 경우 다음 메시지 중 하나가 **show controller e1 EXEC** 출력에 나타나는지 확인합니다.

- 수신기의 프레임 손실
- 수신기에 신호가 손실됨

E1 수신기에 프레임 손실이 있는 경우:

E1 수신기에 프레임이 손실된 경우 다음 단계를 수행합니다.

1. 포트에 구성된 프레임링 형식이 라인의 프레임링 형식과 일치하는지 확인합니다. 실행 중인 컨피그레이션 또는 **show controller e1** 명령 출력에서 컨트롤러의 프레임링 형식을 확인할 수 있습니다. 프레임링 형식을 변경하려면 프레임링 {CRC4를 사용하십시오. 아래와 같이 컨트롤러 컨피그레이션 모드에서 | **no CRC4**} 명령:

```
maui-nas-03#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
maui-nas-03(config)#controller E1 0
maui-nas-03(config-controller)#framing CRC4
```

2. 다른 프레임링 형식을 사용하여 경보가 지워지는지 확인합니다. 문제가 해결되지 않으면 아래의 "E1 수신기에 신호 손실이 있는 경우" 섹션을 진행합니다.
3. 원격 끝의 프레임링 형식을 확인합니다.
4. 원격 끝의 연결 코드를 확인합니다.

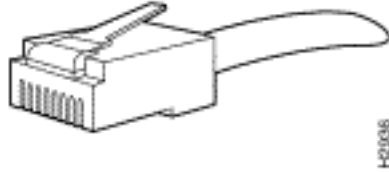
E1 수신기에 신호 손실이 있는 경우:

E1 수신기에 신호가 손실된 경우 다음 단계를 수행합니다.

1. 인터페이스 포트와 E1 서비스 공급자의 장비(또는 E1 터미널 장비) 간의 케이블이 올바르게 연결되어 있는지 확인합니다. 케이블이 올바른 포트에 연결되어 있는지 확인합니다. 필요한 경우 케이블 연결을 수정합니다.
2. 케이블 무결성을 확인합니다. 케이블의 휴식 또는 기타 물리적 이상을 확인합니다. 핀아웃이 올바르게 설정되었는지 확인합니다. 필요한 경우 케이블을 교체합니다.
3. 케이블 커넥터를 확인합니다. 전송 및 수신 쌍 또는 열린 수신 쌍을 취소하면 오류가 발생할 수 있습니다. 수신 쌍을 라인 1 및 2로 설정합니다. 전송 쌍을 라인 4 및 5로 설정합니다. RJ-48 잭의 핀은 1부터 8까지 번호가 매겨집니다. 핀 1은 금속 핀이 있는 잭을 볼 때 가장 왼쪽에 있는 핀입니다. 자세한 내용은 다음 그림을 참조하십시오. **그림 15-11: RJ-45 케이블**



RJ-45 connector



4. 롤오버 케이블을 사용해 보십시오.

5. 원엔드 블록 오류가 있는지 확인합니다. 이 경우 로컬 끝의 수신 리드에 문제가 있습니다. 자세한 내용은 TAC에 문의하십시오.

각 단계에서 **show controller e1 EXEC** 명령을 실행하여 컨트롤러가 오류를 발생하는지 확인합니다

회선이 루프백 모드인 경우

show controller e1 출력에서 줄이 루프백 모드에 있는지 확인합니다. 행은 테스트용으로만 루프백 모드여야 합니다.

루프백을 끄려면 아래와 같이 컨트롤러 컨피그레이션 모드에서 **no loopback** 명령을 사용합니다.

```
maui-nas-03 (config-controller) #no loopback
```

컨트롤러에 경보가 표시되는 경우:

컨트롤러가 알람을 표시하는지 확인하려면 **show controller** 명령 출력을 확인합니다.

이제 다양한 경보와 이를 수정하는 데 필요한 절차에 대해 설명하겠습니다.

수신기(Rx)에 원격 경보 있음:

수신된 원격 경보는 포트에 연결된 장비의 라인 업스트림에서 경보가 발생함을 의미합니다.

1. 포트에 구성된 프레이밍 형식이 라인의 프레이밍 형식과 일치하는지 확인합니다. 그렇지 않은 경우 컨트롤러의 프레이밍 형식을 라인의 형식과 일치하도록 변경합니다.
2. 원격 엔드 장비의 라인 인코딩 설정을 확인합니다. 올바른 설정에 대해서는 서비스 공급업체에 문의하십시오. 필요에 따라 잘못된 컨피그레이션을 수정합니다.
3. 외부 루프백 케이블을 포트에 삽입합니다. 루프백 플러그를 만들려면 장 앞부분의 "하드웨어 루프백 플러그 테스트 수행" 섹션을 참조하십시오.
4. 경보가 있는지 확인합니다. 경보가 표시되지 않으면 로컬 하드웨어가 양호한 상태일 수 있습니다. 이 경우:케이블을 확인합니다. 자세한 내용은 "E1 수신기에 신호 손실이 있는 경우" 절을 참조하십시오.원격 끝의 설정을 확인하고 포트 설정과 일치하는지 확인합니다.문제가 계속되면 서비스 공급업체에 문의하십시오.
5. 루프백 플러그를 제거하고 E1 회선을 다시 연결합니다.
6. 케이블을 확인합니다. 자세한 내용은 "E1 수신기에 신호 손실이 있는 경우" 절을 참조하십시오.
7. 라우터의 전원을 껐다가 켜십시오.
8. E1 회선을 다른 포트에 연결합니다. 회선 설정과 동일한 설정으로 포트를 구성합니다. 문제가 지속되지 않으면 하나의 포트에 결합이 있습니다.E1 회선을 원래 포트에 다시 연결합니다."E1 오류 이벤트 문제 해결" 섹션으로 이동합니다.문제가 계속되면 다음을 수행합니다.
9. "하드웨어 루프백 플러그 테스트 수행" 섹션에 설명된 대로 하드웨어 루프 테스트를 수행합니다

다.

10. E1 컨트롤러 카드를 교체합니다.

11. "E1 오류 이벤트 문제 해결" 섹션으로 이동합니다.

원격 경보 전송 송신기(빨간색):

CSU가 E1 라인의 프레임링 패턴과 동기화할 수 없는 경우 빨간색 경보가 선언됩니다.

1. 포트에 구성된 프레임링 형식이 라인의 프레임링 형식과 일치하는지 확인합니다. 컨트롤러의 프레임링 형식을 줄의 형식과 일치하도록 변경하지 않는 경우
2. 원격 끝의 설정을 확인하고 포트 설정과 일치하는지 확인합니다.
3. 외부 루프백 케이블을 포트에 삽입합니다. 루프백 플러그를 만들려면 장 앞부분의 "하드웨어 루프백 플러그 테스트 수행" 섹션을 참조하십시오.
4. 경보가 있는지 확인합니다. 경보가 표시되지 않으면 로컬 하드웨어가 양호한 상태일 수 있습니다. 이 경우:케이블을 확인합니다. 자세한 내용은 "E1 수신기에 신호 손실이 있는 경우" 절을 참조하십시오.문제가 계속되면 서비스 공급업체에 문의하십시오.
5. E1 회선을 다른 포트에 연결합니다. 회선 설정과 동일한 설정으로 포트를 구성합니다. 문제가 해결되지 않으면 하나의 포트에 결합이 있습니다.E1 회선을 원래 포트에 다시 연결합니다."E1 오류 이벤트 문제 해결" 섹션으로 이동합니다.문제가 계속되면 다음을 수행합니다.
6. "하드웨어 루프백 플러그 테스트 수행" 섹션에 설명된 대로 하드웨어 루프 테스트를 수행합니다.
7. E1 컨트롤러 카드를 교체합니다.
8. "E1 오류 이벤트 문제 해결" 섹션으로 이동합니다.
9. 서비스 공급업체에 문의하십시오.

E1 오류 이벤트 트러블슈팅

show controller e1 EXEC 명령은 문제 해결에 사용할 수 있는 오류 메시지를 제공합니다. 이제 몇 가지 오류 메시지와 오류를 수정하는 방법에 대해 살펴보겠습니다.

오류 카운터가 증가하고 있는지 확인하려면 **show controller e1** 명령을 반복해서 실행합니다. 현재 간격의 카운터 값을 확인합니다. 프레임링 및 선형코드 설정에 대해서는 서비스 공급업체에 문의하십시오.

Slip Secs 카운터가 증가하고 있습니다.

E1 행에 슬립이 있는 경우 잠금 문제가 있음을 나타냅니다. E1 제공자(Telco)는 CPE(Customer Premises Equipment)를 동기화해야 하는 잠금을 제공합니다.

1. 클럭 소스가 네트워크에서 파생되는지 확인합니다. 클럭 소스가 라인 프라이머리(Line Primary)인지 확인하여 확인할 수 있습니다.**참고:** 액세스 서버에 여러 E1이 있는 경우 하나만 기본 서버가 될 수 있고 다른 E1은 기본 서버에서 시계를 파생합니다. 이 경우 기본 클럭 소스로 지정된 E1 회선이 올바르게 구성되었는지 확인합니다.
2. 컨트롤러 컨피그레이션 모드에서 E1 클럭 소스를 올바르게 설정합니다.

```
maui-nas-03(config-controllle)#clock source line primary
```

프레임링 손실 초 카운터가 증가하고 있습니다.

프레이밍 손실 초 카운터가 증가할 때 다음 단계를 수행합니다.

1. 포트에 구성된 프레이밍 형식이 라인의 프레이밍 형식과 일치하는지 확인합니다. 프레이밍이 **show controller e1** 출력에서 {CRC4|no CRC4}인지 확인하여 확인할 수 있습니다.
2. 프레이밍 형식을 변경하려면 프레이밍 {**CRC4**}를 사용하십시오. / 컨트롤러 컨피그레이션 모드에서 다음과 같은 **CRC4** 명령 없음:

```
maui-nas-03 (config-controlle) #framing crc4
```

라인 코드 위반 증가:

라인 코드 위반이 증가하는 경우 다음 단계를 수행합니다.

1. 포트에 구성된 라인 인코딩이 라인의 프레이밍 형식과 일치하는지 확인합니다. **show controller e1** 출력에서 라인 코드가 {AMI/HDB3}인지 확인하여 확인할 수 있습니다.
2. 선형코드를 변경하려면 **회선 코드** {ami}를 사용하십시오. 아래와 같이 컨트롤러 컨피그레이션 모드에서 / **hdb3** 명령을 실행합니다.

```
maui-nas-03 (config-controlle) #linecode ami
```

ISDN 스위치 유형 및 PRI-그룹이 올바르게 구성되었는지 확인

show running-config 명령을 사용하여 ISDN 스위치 유형 및 PRI-group timeslot이 올바르게 구성되었는지 확인합니다. 올바른 값은 서비스 공급업체에 문의하십시오.

ISDN 스위치 유형 및 PRI 그룹을 변경하려면

```
maui-nas-03#configure terminal
maui-nas-03 (config) #isdn switch-type primary-net5
maui-nas-03 (config) #controller e1 0
maui-nas-03 (config-controlle) #pri-group timeslots 1-31
```

신호 채널 확인

오류 카운터가 증가하지 않지만 문제가 지속되면 신호 채널이 작동 및 올바르게 구성되었는지 확인하십시오.

1. **show interface serial x:15** 명령을 실행합니다. 여기서 x는 인터페이스 번호로 교체해야 합니다.
2. 인터페이스가 작동 중인지 확인합니다. 인터페이스가 작동되지 않은 경우 **no shutdown** 명령을 사용하여 인터페이스를 활성화합니다.

```
maui-nas-03#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
maui-nas-03 (config) #interface serial 0:15
maui-nas-03 (config-if) #no shutdown
```

3. 캡슐화가 PPP인지 확인합니다. 인터페이스에서 PPP를 사용하지 않는 경우 인터페이스 컨피그레이션 모드에서 **캡슐화 ppp** 명령을 사용하여 수정합니다.

```
maui-nas-03 (config-if) #encapsulation ppp
```

4. 루프백이 설정되어 있는지 확인합니다. 루프백은 테스트 용도로만 설정해야 합니다. 루프백을 제거하려면 `no loopback` 명령을 사용합니다.

```
maui-nas-03(config-if)#no loopback
```

5. 라우터의 전원을 껐다가 켜십시오.
6. 문제가 계속되면 서비스 제공업체 또는 Cisco TAC에 문의하십시오.

PRI 문제 해결

PRI를 트러블슈팅할 때 E1이 양쪽 끝에서 완전히 실행 중인지 확인해야 합니다. 위에서 설명한 대로 레이어 1 문제가 해결된 경우 레이어 2 및 레이어 3 문제를 고려하십시오.

show isdn status 명령을 사용한 문제 해결

`show isdn status` 명령은 모든 ISDN 인터페이스의 스냅샷을 표시하는 데 사용됩니다. 레이어 1, 2 및 3의 상태를 표시합니다.

1. 레이어 1이 활성 상태인지 확인합니다. E1이 중단되지 않은 경우 레이어 1 상태는 항상 ACTIVE로 표시되어야 합니다. `show isdn status`가 레이어 1이 비활성화되었음을 나타내는 경우 E1 라인의 물리적 연결에 문제가 있습니다. "E1 컨트롤러가 관리적으로 다운되었습니까?" 섹션을 참조하십시오. 또한 E1이 관리 목적으로 다운되지 않았는지 확인합니다. E1 컨트롤러를 가동하려면 `no shutdown` 명령을 사용합니다.

2. 레이어 2 상태가 MULTIPLE_FRAME_ESTABLISHED인지 확인합니다.

원하는 레이어 2 상태는 Multiple_Frame_Established이며, 이는 ISDN 스위치와 엔드 디바이스 간의 시작 프로토콜이 설정되었고 레이어 2 프레임을 교환하고 있음을 나타냅니다.

레이어 2가 Multiple_Frame_Established가 아닌 경우 `show controller e1 EXEC` 명령을 사용하여 문제를 진단합니다. 이 장의 "`show controller e1` 명령을 사용하여 트러블슈팅" 섹션 및 "E1 오류 이벤트 트러블슈팅" 섹션을 참조하십시오.

`show isdn` 상태는 현재 상태의 스냅샷이므로 Multiple_Frame_Established를 나타내더라도 레이어 2가 위아래로 바운스될 수 있습니다. `debug isdn q921` 명령을 사용하여 레이어 2가 안정적인지 확인합니다.

디버그 q921 사용

`debug isdn q921` 명령은 D-채널의 라우터에서 발생하는 데이터 링크 레이어(레이어 2) 액세스 절차를 표시합니다.

`logging console` 또는 `terminal monitor` 명령을 사용하여 디버그 메시지를 보도록 구성되었는지 확인합니다.

참고: 프로덕션 환경에서 콘솔 로깅이 비활성화되어 있는지 확인합니다. `show logging` 명령을 입력합니다. 로깅이 활성화된 경우 콘솔 포트가 로그 메시지로 오버로드되는 즉시 액세스 서버가 간헐적으로 중지될 수 있습니다. `no logging console` 명령을 입력합니다.

참고: 디버그 `isdn q921`이 켜져 있고 디버그 출력을 받지 못한 경우 디버그 출력을 얻으려면 전화를 걸거나 컨트롤러를 재설정하십시오.

1. 레이어 2가 안정적인지 확인합니다. 서비스가 작동 및 작동 중지되지 않음을 나타내는 메시지

에 대한 디버그 출력을 확인해야 합니다. 다음 유형의 디버그 출력이 표시되면 줄이 안정적이지 않습니다.

```
Mar 20 10:06:07.882: %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se0:15, TEI 0
changed to down
Mar 20 10:06:09.882: %LINK-3-UPDOWN: Interface Serial0:15, changed state to down
Mar 20 10:06:21.274: %DSX1-6-CLOCK_CHANGE: Controller 0 clock is now selected
as clock source
Mar 20 10:06:21.702: %ISDN-6-LAYER2UP: Layer 2 for Interface Se0:15, TEI 0
changed to up
Mar 20 10:06:22.494: %CONTROLLER-5-UPDOWN: Controller E1 0, changed state to up
Mar 20 10:06:24.494: %LINK-3-UPDOWN: Interface Serial0:15, changed state to up
```

레이어 2가 안정적이지 않을 경우 이 장의 앞부분에서 "E1 오류 이벤트 문제 해결"을 참조하십시오.

2. 전송(TX) 및 수신(RX) 측면에서 모두 SAPI 메시지만 표시되는지 확인합니다.

```
Mar 20 10:06:52.505: ISDN Se0:15: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:06:52.505: ISDN Se0:15: RX <- RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.505: ISDN Se0:15: TX -> RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: RX <- RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: RX <- RRf sapi = 0 tei = 0 nr = 0
```

3. 레이어 2가 다시 초기화하려고 함을 나타내는 SABME 메시지가 표시되지 않는지 확인합니다.

이는 일반적으로 RP(Poll Requests)를 전송하고 스위치에서 응답을 받지 않거나 RRf(Poll Request)를 전송할 때 발생합니다. 다음은 SABME 메시지의 예입니다. SABME 메시지(UA 프레임 수신)에 대한 ISDN 스위치로부터 응답을 받아야 합니다.

```
Mar 20 10:06:21.702: ISDN Se0:15: RX <- SABMEp sapi = 0 tei = 0
Mar 20 10:06:22.494: ISDN Se0:15: TX -> SABMEp sapi = 0 tei = 0
```

SABME 메시지가 표시되면 **show running-config** 명령을 사용하여 ISDN 스위치 유형 및 PRI-group timeslot이 올바르게 구성되었는지 확인합니다. 올바른 값은 서비스 공급업체에 문의하십시오. ISDN 스위치 유형 및 PRI 그룹을 변경하려면

```
maui-nas-03#configure terminal
maui-nas-03(config)#isdn switch-type primary-net5
maui-nas-03(config)#controller e1 0
maui-nas-03(config-controller)#pri-group timeslots 1-31
```

4. **show interfaces serial x:15** 명령을 사용하여 D-channel이 작동 중인지 확인합니다. D-채널이 가동되지 않은 경우 **no shutdown** 명령을 사용하여 이 명령을 실행합니다.

```
maui-nas-03(config)#interface serial 0:15
maui-nas-03(config-if)#no shutdown
```

5. 캡슐화가 PPP인지 확인합니다. 캡슐화 **ppp** 명령을 사용하여 캡슐화를 설정하지 않는 경우

```
maui-nas-03(config-if)#encapsulation ppp
```

6. 인터페이스가 루프백 모드인지 확인합니다. 정상적인 작동을 위해 인터페이스는 루프백 모드에 있지 않아야 합니다.

```
maui-nas-03(config-if)#no loopback
```

7. 라우터의 전원을 껐다가 켜십시오.

8. 문제가 계속되면 서비스 공급업체 또는 Cisco TAC에 문의하십시오.

관련 정보

- [Technical Support - Cisco Systems](#)