CRS-1 및 IOS XR 운영 모범 사례

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[Cisco IOS XR 개요](#)
[프로세스 및 스레드](#)
[프로세스 및 스레드 상태](#)
[동기 메시지 전달](#)
[차단된 프로세스 및 프로세스 상태](#)
[중요한 프로세스 및 기능](#)
[네티오](#)
[GSP(그룹 서비스 프로세스)](#)
[BCDL 대량 콘텐츠 다운로더](#)
[경량 메시징(LWM)](#)
[엔브먼](#)
[CRS-1 패브릭 소개](#)
[패브릭 플레인](#)
[패브릭 모니터링](#)
[컨트롤 플레인 개요](#)
[Catalyst 6500 구성](#)
[멀티 섀시 제어 평면 관리](#)
[ROMMON 및 Monlib](#)
[업그레이드 지침](#)
[PLIM 및 MSC 개요](#)
[PLIM 초과 서브스크립션](#)
[컨피그레이션 관리](#)
[보안](#)
[LPTS](#)
[내부 패킷은 어떻게 전달됩니까?](#)
[대역 외](#)
[관련 정보](#)

소개

이 문서에서는 다음 내용을 이해할 수 있습니다.

- 프로세스 및 스레드
- CRS-1 패브릭
- 컨트롤 플레인
- Rommon 및 Monlib
- PLIM(Physical Layer Interface Module) 및 MSC(Modular Service Card)
- 컨피그레이션 관리
- 보안
- 대역 외
- SNMP(Simple Network Management Protocol)

사전 요구 사항

요구 사항

Cisco는 Cisco IOS® XR에 대한 지식을 보유하고 있는 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS XR 소프트웨어
- CRS-1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

Cisco IOS XR 개요

Cisco IOS XR은 확장이 가능하도록 설계되었습니다.커널은 마이크로커널 아키텍처이므로 프로세스 관리, 스케줄링, 신호 및 타이머와 같은 필수 서비스만 제공합니다.파일 시스템, 드라이버, 프로토콜 스택 및 애플리케이션과 같은 다른 모든 서비스는 리소스 관리자로 간주되어 메모리 보호 사용자 공간에서 실행됩니다.이러한 기타 서비스는 프로그램 설계에 따라 런타임에 추가 또는 제거할 수 있습니다.마이크로커널의 크기는 12KB입니다.마이크로커널과 기본 운영 체제는 QNX Software Systems의 것이며 Neutrino라고 합니다.QNX는 실시간 운영 체제 설계를 전문으로 합니다.마이크로커널은 선점형이며 스케줄러는 우선 순위를 기준으로 합니다.이렇게 하면 프로세스 간의 컨텍스트 전환이 매우 빠르며, 가장 우선 순위가 높은 스레드에서 항상 필요한 경우 CPU에 액세스할 수 있습니다.Cisco IOS XR에서 활용할 수 있는 몇 가지 이점은 다음과 같습니다.그러나 가장 큰 이점은 운영 체제 코어 내에서 프로세스 간 커뮤니케이션의 상속 설계입니다.

Neutrino는 전송 운영 체제를 나타내는 메시지이며, 메시지는 모든 스레드에서 프로세스 간 통신의 기본 수단입니다.특정 서버가 서비스를 제공하려는 경우 메시지 교환용 채널을 만듭니다.클라이언트는 서비스를 활용하기 위해 관련 파일 설명자에 직접 매핑하여 서버 채널에 연결됩니다.클라이언트와 서버 간의 모든 통신은 동일한 메커니즘에 의해 이루어집니다.이것은 CRS-1이 있는 슈퍼 컴퓨터에 큰 이점입니다.표준 UNIX 커널에서 로컬 읽기 작업을 수행할 때 다음 사항을 고려하십시오.

- 소프트웨어가 커널에 인터럽트합니다.
- 커널이 파일 시스템에 디스패치됩니다.
- 데이터가 수신됩니다.

원격 사례에서는 다음 사항을 고려하십시오.

- 소프트웨어가 커널에 인터럽트합니다.
- 커널 NFS 디스패치
- NFS는 네트워킹 구성 요소를 호출합니다.
- 원격에서 네트워킹 구성 요소를 디스패치합니다.
- NFS가 호출됩니다.
- 커널은 파일 시스템을 디스패치합니다.

로컬 읽기와 원격 읽기의 의미 체계가 동일하지 않습니다.파일 잠금 및 권한 설정에 대한 인수 및 매개 변수가 다릅니다.

QNX 로컬 사례를 고려하십시오.

- 소프트웨어가 커널에 인터럽트합니다.
- 커널은 파일 시스템으로 메시지를 전달합니다.

로컬이 아닌 경우를 고려하십시오.

- 소프트웨어가 커널에 인터럽트합니다.
- 커널은 IPC 전송 메커니즘인 QNET로 이동합니다.
- QNET은 커널로 이동합니다.
- 커널은 파일 시스템을 디스패치합니다.

인수 전달 및 파일 시스템 매개 변수와 관련된 모든 의미 체계는 동일합니다.모든 것이 IPC 인터페이스에서 분리되어 클라이언트와 서버를 완전히 분리할 수 있습니다.즉, 어떤 프로세스도 어느 시점에서든 언제든지 실행할 수 있습니다.특정 Route Processor가 서비스 요청을 처리하는 데 너무 많은 경우, 해당 서비스를 DRP에서 실행되는 다른 CPU로 쉽게 마이그레이션할 수 있습니다.다른 CPU에서 서로 다른 서비스를 실행하는 수퍼 컴퓨터는 여러 노드에 분산되어 다른 노드와 쉽게 통신할 수 있습니다.확장 기회를 제공하기 위해 인프라가 갖춰져 있습니다.Cisco는 이러한 장점을 활용하고 CRS 라우터가 수천 개의 노드로 확장될 수 있도록 하는 메시지 전달 커널의 기본 작업에 연결하는 추가 소프트웨어를 작성했습니다. 이 경우 CPU는 RP(Route Process), DRP(Distributed Route Processor), MSC(Modular Services Card) 또는 SP(Switch Processor)와 같은 OS 인스턴스를 실행합니다.

프로세스 및 스레드

Cisco IOS XR의 범위 내에서 프로세스는 하나 이상의 스레드를 포함하는 메모리의 보호 영역입니다.프로그래머의 관점에서 스레드는 작업을 수행하며 각 스레드는 특정 작업을 수행하기 위해 논리적 실행 경로를 완료합니다.실행 중에 스레드에서 필요로 하는 메모리는 다른 프로세스 스레드에서 보호되어 실행 중인 프로세스에 속합니다.스레드는 실행 단위로서 스택과 레지스터를 포함하는 실행 컨텍스트가 있습니다.프로세스는 가상 주소 공간을 공유하는 스레드 그룹입니다. 단, 프로세스는 단일 스레드를 포함할 수 있지만 더 많은 스레드를 포함할 수 있습니다.다른 프로세스의 다른 스레드가 프로세스의 메모리에 쓰려고 하면 문제가 되는 프로세스가 종료됩니다.프로세스 내에서 작동하는 스레드가 두 개 이상 있는 경우 해당 스레드는 프로세스 내의 동일한 메모리에 액세스할 수 있으므로 다른 스레드의 데이터를 덮어쓸 수 있습니다.동일한 프로세스 내에서 이 스레드를 방지하려면 리소스에 대한 동기화를 유지하려면 절차의 단계를 완료하십시오.

스레드는 상호 제외(MUTEX)라는 개체를 사용하여 서비스에 대한 상호 제외를 보장합니다.MUTEX가 있는 스레드는 예로서 메모리의 특정 영역에 쓸 수 있는 스레드입니다.MUTEX가 없는

다른 스레드는 사용할 수 없습니다.리소스 동기화를 보장하기 위한 다른 메커니즘도 있으며 Semaphores, Conditional Variables 또는 Condvars, Bargers 및 Sleepons도 있습니다.여기서는 논의되지 않지만, 동기화 서비스를 업무의 일부로 제공합니다.여기에서 설명한 원칙을 Cisco IOS와 같게 하면 Cisco IOS는 동일한 메모리 공간에 액세스할 수 있는 모든 스레드와 함께 여러 스레드를 작동하는 단일 프로세스입니다.그러나 Cisco IOS는 이러한 스레드 프로세스를 호출합니다.

프로세스 및 스레드 상태

Cisco IOS XR에는 서비스를 제공하는 서버와 서비스를 사용하는 클라이언트가 있습니다.특정 프로세스에는 동일한 서비스를 제공하는 여러 스레드가 있을 수 있습니다.다른 프로세스에는 특정 시점에 특정 서비스가 필요할 수 있는 클라이언트가 여러 개 있을 수 있습니다.서버에 대한 액세스를 항상 사용할 수 있는 것은 아니며, 클라이언트가 서비스에 대한 액세스를 요청하면 해당 서버에 상주하면서 서버가 사용 가능해질 때까지 기다립니다.이 경우 클라이언트가 차단되었다고 합니다.이를 차단 클라이언트 서버 모델이라고 합니다.클라이언트가 MUTEX와 같은 리소스를 기다리거나 서버가 아직 응답하지 않았기 때문에 차단될 수 있습니다.

ospf **프로세스**에서 스레드의 상태를 확인하려면 show process ospf 명령을 실행합니다.

```
RP/0/RP1/CPU0:CWDCRS#show process ospf
                  Job Id: 250
                     PID: 110795
          Executable path: /disk0/hfr-rout-3.2.3/bin/ospf
               Instance #: 1
               Version ID: 00.00.0000
                  Respawn: ON
            Respawn count: 1
  Max. spawns per minute: 12
             Last started: Tue Jul 18 13:10:06 2006
            Process state: Run
            Package state: Normal
       Started on config: cfg/gl/ipv4-ospf/proc/101/ord_a/routerid
                    core: TEXT SHAREDMEM MAINMEM
                Max. core: 0
                Placement: ON
             startup_path: /pkg/startup/ospf.startup
                   Ready: 1.591s
                Available: 5.595s
         Process cpu time: 89.051 user, 0.254 kernel, 89.305 total
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
250    1      40K  10 Receive       0:00:11:0509 ospf
250    2      40K  10 Receive       0:01:08:0937 ospf
250    3      40K  10 Receive       0:00:03:0380 ospf
250    4      40K  10 Condvar       0:00:00:0003 ospf
250    5      40K  10 Receive       0:00:05:0222 ospf
```

ospf 프로세스에는 250인 JID(작업 ID)가 지정됩니다. 이는 실행 중인 라우터와 일반적으로 특정 버전의 Cisco IOS XR에서 변경되지 않습니다.ospf 프로세스에는 각각 고유한 TID(Thread ID)를 가진 5개의 스레드가 있습니다. 나열되는 것은 각 스레드의 스택 공간, 각 스레드의 우선 순위 및 상태입니다.

동기 메시지 전달

앞서 QNX는 메시지 전달 운영 체제라고 언급되었습니다.운영 체제를 전달하는 동기식 메시지입니다.많은 운영 체제 문제가 동기식 메시징에 반영됩니다.동기식 메시지가 문제를 일으킨다고 하지 않지만 문제가 발생한 현상은 동기식 메시지 전달에 반영됩니다.동기식, 라이프 사이클 또는 상태 정보를 CRS-1 운영자가 쉽게 액세스할 수 있으므로 문제 해결 프로세스에 도움이 됩니다.라이프

사이클을 전달하는 메시지는 다음과 유사합니다.

- 서버가 메시지 채널을 생성합니다.
- 클라이언트는 서버의 채널에 연결됩니다(posix open과 유사).
- 클라이언트는 메시지를 서버(MsgSend)로 보내고 응답 및 블록을 기다립니다.
- 서버는 클라이언트에서 메시지를 수신하고 메시지를 처리하고 클라이언트에 회신합니다.
- 클라이언트는 서버의 응답을 차단 해제하고 처리합니다.

이 차단 클라이언트-서버 모델은 동기화 메시지를 전달하는 것입니다.즉, 클라이언트가 메시지와 블록을 전송합니다.서버는 메시지를 수신하고, 처리하고, 클라이언트에 다시 응답한 다음, 클라이언트가 차단 해제를 취소합니다.구체적인 세부 사항은 다음과 같습니다.

- 서버가 수신 상태에서 대기합니다.
- 클라이언트가 서버에 메시지를 전송하고 차단됩니다.
- 수신 상태에서 대기하는 경우 서버는 메시지를 수신하고 차단 해제를 수행합니다.
- 클라이언트가 회신 상태로 이동합니다.
- 서버가 RUNNING 상태로 이동합니다.
- 서버에서 메시지를 처리합니다.
- 서버가 클라이언트에 응답합니다.
- 클라이언트 차단 해제

클라이언트 및 서버 상태를 확인하려면 **show process** 명령을 실행합니다.

```
RP/0/RP1/CPU0:CWDCRS#show processes
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
1      1       0K  0  Ready       320:04:04:0649 procnto-600-smp-cisco-instr
1      3       0K  10 Nanosleep     0:00:00:0043 procnto-600-smp-cisco-instr
1      5       0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      7       0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      8       0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      11      0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      12      0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      13      0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      14      0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      15      0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      16      0K  10 Receive       0:02:01:0207 procnto-600-smp-cisco-instr
1      17      0K  10 Receive       0:00:00:0015 procnto-600-smp-cisco-instr
1      21      0K  10 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      23      0K  10 Running       0:07:34:0799 procnto-600-smp-cisco-instr
1      26      0K  10 Receive       0:00:00:0001 procnto-600-smp-cisco-instr
1      31      0K  10 Receive       0:00:00:0001 procnto-600-smp-cisco-instr
1      33      0K  10 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      39      0K  10 Receive       0:13:36:0166 procnto-600-smp-cisco-instr
1      46      0K  10 Receive       0:06:32:0015 procnto-600-smp-cisco-instr
1      47      0K  56 Receive       0:00:00:0029 procnto-600-smp-cisco-instr
1      48      0K  10 Receive       0:00:00:0001 procnto-600-smp-cisco-instr
1      72      0K  10 Receive       0:00:00:0691 procnto-600-smp-cisco-instr
1      73      0K  10 Receive       0:00:00:0016 procnto-600-smp-cisco-instr
1      78      0K  10 Receive       0:09:18:0334 procnto-600-smp-cisco-instr
1      91      0K  10 Receive       0:09:42:0972 procnto-600-smp-cisco-instr
1      95      0K  10 Receive       0:00:00:0011 procnto-600-smp-cisco-instr
1      103     0K  10 Receive       0:00:00:0008 procnto-600-smp-cisco-instr
74     1       8K  63 Nanosleep     0:00:00:0001 wd-mbi
53     1      28K  10 Receive       0:00:08:0904 dllmgr
53     2      28K  10 Nanosleep     0:00:00:0155 dllmgr
53     3      28K  10 Receive       0:00:03:0026 dllmgr
53     4      28K  10 Receive       0:00:09:0066 dllmgr
53     5      28K  10 Receive       0:00:01:0199 dllmgr
```

```
270    1      36K  10 Receive       0:00:36:0091 qsm
270    2      36K  10 Receive       0:00:13:0533 qsm
270    5      36K  10 Receive       0:01:01:0619 qsm
270    7      36K  10 Nanosleep     0:00:22:0439 qsm
270    8      36K  10 Receive       0:00:32:0577 qsm
67     1      52K  19 Receive       0:00:35:0047 pkgfs
67     2      52K  10 Sigwaitinfo   0:00:00:0000 pkgfs
67     3      52K  19 Receive       0:00:30:0526 pkgfs
67     4      52K  10 Receive       0:00:30:0161 pkgfs
67     5      52K  10 Receive       0:00:25:0976 pkgfs
68     1       8K  10 Receive       0:00:00:0003 devc-pty
52     1      40K  16 Receive       0:00:00:0844 devc-conaux
52     2      40K  16 Sigwaitinfo   0:00:00:0000 devc-conaux
52     3      40K  16 Receive       0:00:02:0981 devc-conaux
52     4      40K  16 Sigwaitinfo   0:00:00:0000 devc-conaux
52     5      40K  21 Receive       0:00:03:0159 devc-conaux
65545  2      24K  10 Receive       0:00:00:0487 pkgfs
65546  1      12K  16 Reply         0:00:00:0008 ksh
66     1       8K  10 Sigwaitinfo   0:00:00:0005 pipe
66     3       8K  10 Receive       0:00:00:0000 pipe
66     4       8K  16 Receive       0:00:00:0059 pipe
66     5       8K  10 Receive       0:00:00:0149 pipe
66     6       8K  10 Receive       0:00:00:0136 pipe
71     1      16K  10 Receive       0:00:09:0250 shmwin_svr
71     2      16K  10 Receive       0:00:09:0940 shmwin_svr
61     1       8K  10 Receive       0:00:00:0006 mqueue
```

차단된 프로세스 및 프로세스 상태

차단된 상태의 프로세스를 보려면 show process blocked 명령을 실행합니다.

```
RP/0/RP1/CPU0:CWDCRS#show processes blocked
  Jid       Pid Tid                 Name State  Blocked-on
65546      4106   1                  ksh Reply    4104  devc-conaux
  105     61495   2              attachd Reply   24597  eth_server
  105     61495   3              attachd Reply    8205  mqueue
  316     65606   1           tftp_server Reply    8205  mqueue
  233     90269   2               lpts_fm Reply   90223  lpts_pa
  325    110790   1             udp_snmpd Reply   90257  udp
  253    110797   4                ospfv3 Reply   90254  raw_ip
  337    245977   2                fdiagd Reply   24597  eth_server
  337    245977   3                fdiagd Reply    8205  mqueue
65762   5996770   1                  exec Reply       1  kernel
65774   6029550   1                  more Reply    8203  pipe
65778   6029554   1       show_processes Reply       1  kernel
RP/0/RP1/CPU0:CWDCRS#
```

동기화된 메시지 전달을 사용하면 서로 다른 스레드 간의 프로세스 간 통신의 수명 주기를 쉽게 추적할 수 있습니다.스레드는 언제든지 특정 상태에 있을 수 있습니다.차단된 상태는 문제의 징후일 수 있습니다.이는 스레드가 차단됨 상태인 경우 문제가 있음을 의미하지는 않으므로 **show process blocked** 명령을 실행하고 Cisco Technical Support에서 케이스를 열지 마십시오.차단된 스레드도 매우 정상적입니다.

이전 출력을 확인합니다.목록의 첫 번째 스레드를 보면 ksh가 되며 그 회신은 devc-conaux에서 차단됩니다.이 경우 클라이언트인 ksh는 devc-conaux 프로세스로 메시지를 전송했으며, devc-conaux인 서버는 회신할 때까지 ksh 회신이 차단되었습니다.Ksh는 누군가가 콘솔 또는 AUX 포트에서 사용하는 UNIX 셸입니다.Ksh는 콘솔에서 입력을 기다리고, 오퍼레이터가 입력하지 않아 아무것도 없으면 일부 입력을 처리할 때까지 차단된 상태로 유지됩니다.처리 후 ksh는 devc-conaux에서 차단된 응답으로 돌아갑니다.

이는 정상이며 문제를 나타내지 않습니다.차단된 스레드는 정상이며, XR 버전, 사용 중인 시스템 유형, 구성 항목 및 **show process blocked** 명령의 출력을 변경하는 작업에 따라 달라집니다.**show process blocked** 명령을 사용하면 OS 유형 문제를 해결할 수 있습니다.문제가 있는 경우(예: CPU가 높은 경우) 이전 명령을 사용하여 정상 이외의 것으로 보이는 것이 있는지 확인합니다.

작동 중인 라우터의 정상 상태를 파악합니다.그러면 프로세스 라이프 사이클의 문제를 해결할 때 비교로 사용할 수 있는 베이스라인이 제공됩니다.

스레드는 언제든지 특정 상태에 있을 수 있습니다.이 테이블에서는 상태 목록을 제공합니다.

상태가 다음과 같은 경우:	**스레드:**
데드	죽었어커널이 스레드 리소스를 해제하기 위해 대기 중입니다.
실행 중	CPU에서 능동적으로 실행
준비 완료	CPU에서 실행되고 있지 않지만 실행할 준비가 되었습니다.
중지됨	일시 중단(SIGSTOP 신호)
전송	서버가 메시지를 받을 때까지 대기 중
수신	클라이언트가 메시지를 보낼 때까지 대기 중
회신	서버가 메시지에 응답할 때까지 대기 중
스택	추가 스택이 할당되기를 기다리는 중
대기 페이지	프로세스 관리자가 페이지 오류를 해결할 때까지 기다리는 중
SIGSUSPEND	신호 대기 중
SIGWAITINFO	신호 대기 중
난소수면	일정 시간 동안 자는 것
뮤텍스	MUTEX 구입 대기 중
콘드바	조건부 변수가 신호를 받을 때까지 기다리는 중
가입	다른 스레드가 완료될 때까지 기다리는 중
INTR	인터럽트 대기 중
SEM	세마포를 얻기 위해 기다리는 중

중요한 프로세스 및 기능

Cisco IOS XR에는 많은 프로세스가 있습니다.이것들은 그들의 기능을 설명한 몇 가지 중요한 것입니다.

WatchDog 시스템 모니터(WDSysmon)

프로세스 중단 및 메모리 부족 상태를 탐지하기 위해 제공되는 서비스입니다.메모리 누수 또는 기타 외부 환경의 결과로 메모리가 부족할 수 있습니다.중단은 프로세스 교착 상태, 무한 루프, 커널 잠금 또는 예약 오류와 같은 여러 조건의 결과일 수 있습니다.다중 스레드 환경에서는 시스템이 교

착 상태 조건이나 단순한 교착 상태 상태로 나타날 수 있습니다.하나 이상의 스레드가 리소스 경합 때문에 계속할 수 없는 경우 교착 상태가 발생할 수 있습니다.예를 들어 스레드 A는 스레드 B로 메시지를 보낼 수 있고 동시에 스레드 B는 스레드 A로 메시지를 보낼 수 있습니다. 두 스레드 모두 서로 대기하며 송신 차단 상태일 수 있으며 두 스레드 모두 계속 대기합니다.두 개의 스레드가 포함된 간단한 경우이지만 여러 스레드에서 사용하는 리소스를 서버에서 담당하는 경우 해당 리소스에 대한 액세스를 요청하는 많은 스레드는 서버에서 대기 중인 차단된 스레드로 보낼 수 있습니다.

교착 상태는 몇 개의 스레드 간에 발생할 수 있지만 결과적으로 다른 스레드에 영향을 줄 수 있습니다.데드록은 좋은 프로그램 설계로 회피되지만, 프로그램이 얼마나 훌륭하게 설계되고 작성되었는지와 관계없이 가능합니다.특정 타이밍에 종속된 데이터인 특정 이벤트 시퀀스로 인해 교착 상태가 발생할 수 있습니다.교착 상태가 항상 결정적이지는 않으며 일반적으로 재생하기가 매우 어렵습니다.WDSysmon에는 Neutrino에서 지원하는 가장 높은 우선 순위의 63을 실행하는 스레드가 여러 개 있습니다. 우선 순위 63에서 실행되면 우선 순위 기반 선점형 스케줄링 환경에서 스레드가 CPU 시간을 가져오게 됩니다.WDSysmon은 하드웨어 워치독 기능과 함께 작동하며 중단 조건을 찾는 소프트웨어 프로세스를 점검합니다.이러한 조건이 탐지되면 WDSysmon은 해당 조건에 대한 추가 정보를 수집하고 프로세스 또는 커널을 코어드하고, syslog에 쓰기를, 스크립트를 실행하고, 교착 상태에 있는 프로세스를 종료할 수 있습니다.문제의 심각도에 따라 시스템 작동을 유지하기 위해 Route Processor 스위치를 시작할 수 있습니다.

```
RP/0/RP1/CPU0:CWDCRS#show processes wdsysmon
                  Job Id: 331
                     PID: 36908
         Executable path: /disk0/hfr-base-3.2.3/sbin/wdsysmon
              Instance #: 1
              Version ID: 00.00.0000
                 Respawn: ON
           Respawn count: 1
  Max. spawns per minute: 12
            Last started: Tue Jul 18 13:07:36 2006
           Process state: Run
           Package state: Normal
                    core: SPARSE
                Max. core: 0
                   Level: 40
                Mandatory: ON
             startup_path: /pkg/startup/wdsysmon.startup
             memory limit: 10240
                   Ready: 0.705s
        Process cpu time: 4988.295 user, 991.503 kernel, 5979.798 total

JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
331    1      84K  19 Receive       0:00:00:0029 wdsysmon
331    2      84K  10 Receive       0:17:34:0212 wdsysmon
331    3      84K  10 Receive       0:00:00:0110 wdsysmon
331    4      84K  10 Receive       1:05:26:0803 wdsysmon
331    5      84K  19 Receive       0:00:06:0722 wdsysmon
331    6      84K  10 Receive       0:00:00:0110 wdsysmon
331    7      84K  63 Receive       0:00:00:0002 wdsysmon
331    8      84K  11 Receive       0:00:00:0305 wdsysmon
331    9      84K  20 Sem           0:00:00:0000 wdsysmon
```

WDSysmon 프로세스에는 9개의 스레드가 있습니다.우선 순위 10에서 4번, 나머지 4개는 11, 19, 20, 63에 있습니다. 프로세스가 설계되면 프로그래머는 프로세스 내의 각 스레드에 대해 우선순위를 신중하게 고려합니다.앞서 설명한 대로 스케줄러는 우선 순위를 기반으로 하므로 우선 순위가 높은 스레드는 항상 낮은 우선 순위 중 하나를 선점합니다.Priority 63은 스레드에서 실행할 수 있는 가장 높은 우선 순위이며 이 경우 스레드 7입니다.스레드 7은 CPU 돼지를 추적하는 스레드인 감시자 스레드입니다.다른 스레드보다 우선 순위가 더 높은 스레드로 실행해야 합니다. 그렇지 않으면 실행할 기회가 전혀 없을 수 있습니다. 이렇게 하면 스레드에서 수행하도록 설계된 단계에서 실행

되지 않습니다.

네티오

Cisco IOS에는 고속 스위칭 및 프로세스 스위칭의 개념이 있습니다.고속 스위칭은 CEF 코드를 사용하며 인터럽트 시간에 발생합니다.프로세스 스위칭은 IP 스위칭 코드인 ip_input을 사용하며 예약된 프로세스입니다.상위 엔드 플랫폼에서 CEF 스위칭은 하드웨어에서 수행되며 ip_input은 CPU에서 예약됩니다.Cisco IOS XR의 ip_input에 해당하는 값은 Netio입니다.

```
P/0/RP1/CPU0:CWDCRS#show processes netio
                  Job Id: 241
                     PID: 65602
          Executable path: /disk0/hfr-base-3.2.3/sbin/netio
               Instance #: 1
                     Args: d
               Version ID: 00.00.0000
                  Respawn: ON
            Respawn count: 1
  Max. spawns per minute: 12
             Last started: Tue Jul 18 13:07:53 2006
            Process state: Run
            Package state: Normal
                     core: DUMPFALLBACK COPY SPARSE
                Max. core: 0
                    Level: 56
                Mandatory: ON
             startup_path: /pkg/startup/netio.startup
                    Ready: 17.094s
         Process cpu time: 188.659 user, 5.436 kernel, 194.095 total
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
241    1     152K  10 Receive       0:00:13:0757 netio
241    2     152K  10 Receive       0:00:10:0756 netio
241    3     152K  10 Condvar       0:00:08:0094 netio
241    4     152K  10 Receive       0:00:22:0016 netio
241    5     152K  10 Receive       0:00:00:0001 netio
241    6     152K  10 Receive       0:00:04:0920 netio
241    7     152K  10 Receive       0:00:03:0507 netio
241    8     152K  10 Receive       0:00:02:0139 netio
241    9     152K  10 Receive       0:01:44:0654 netio
241    10    152K  10 Receive       0:00:00:0310 netio
241    11    152K  10 Receive       0:00:13:0241 netio
241    12    152K  10 Receive       0:00:05:0258 netio
```

GSP(그룹 서비스 프로세스)

각각 고유한 커널 인스턴스를 실행하는 수 천 개의 노드가 있는 슈퍼컴퓨터에서는 통신이 필요합니다.인터넷에서는 멀티캐스팅 프로토콜을 통해 일대다 통신이 효율적으로 수행됩니다.GSP는 CRS-1 내의 IPC에 사용되는 내부 멀티캐스트 프로토콜입니다. GSP는 비동기 의미와 연결되지 않는 하나 이상의 신뢰할 수 있는 그룹 통신을 제공합니다.이를 통해 GSP는 수천 개의 노드로 확장할 수 있습니다.

```
RP/0/RP1/CPU0:CWDCRS#show processes gsp
                  Job Id: 171
                     PID: 65604
          Executable path: /disk0/hfr-base-3.2.3/bin/gsp
               Instance #: 1
               Version ID: 00.00.0000
                  Respawn: ON
```

```
          Respawn count: 1
  Max. spawns per minute: 12
           Last started: Tue Jul 18 13:07:53 2006
          Process state: Run
          Package state: Normal
                   core: TEXT SHAREDMEM MAINMEM
              Max. core: 0
                  Level: 80
              Mandatory: ON
           startup_path: /pkg/startup/gsp-rp.startup
                  Ready: 5.259s
              Available: 16.613s
        Process cpu time: 988.265 user, 0.792 kernel, 989.057 total
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
171    1     152K  30 Receive       0:00:51:0815 gsp
171    3     152K  10 Condvar       0:00:00:0025 gsp
171    4     152K  10 Receive       0:00:08:0594 gsp
171    5     152K  10 Condvar       0:01:33:0274 gsp
171    6     152K  10 Condvar       0:00:55:0051 gsp
171    7     152K  10 Receive       0:02:24:0894 gsp
171    8     152K  10 Receive       0:00:09:0561 gsp
171    9     152K  10 Condvar       0:02:33:0815 gsp
171    10    152K  10 Condvar       0:02:20:0794 gsp
171    11    152K  10 Condvar       0:02:27:0880 gsp
171    12    152K  30 Receive       0:00:46:0276 gsp
171    13    152K  30 Receive       0:00:45:0727 gsp
171    14    152K  30 Receive       0:00:49:0596 gsp
171    15    152K  30 Receive       0:00:38:0276 gsp
171    16    152K  10 Receive       0:00:02:0774 gsp
```

BCDL 대량 콘텐츠 다운로더

BCDL은 RP 및 MSC와 같은 다양한 노드로 데이터를 안정적으로 멀티캐스트 처리하는 데 사용됩니다.GSP를 기본 전송으로 사용합니다.BCDL은 메시지를 **순서대로** 배달합니다.BCDL에는 에이전트, 프로듀서 및 소비자가 있습니다.에이전트는 데이터를 소비자에게 멀티캐스트에 도달하기 전에 검색하고 버퍼링하기 위해 프로듀서와 통신하는 프로세스입니다.프로듀서는 모든 사람이 원하는 데이터를 생성하는 프로세스이며, 소비자는 프로듀서가 제공한 데이터를 수신하고자 하는 프로세스입니다.BCDL은 Cisco IOS XR 소프트웨어 업그레이드 중에 사용됩니다.

경량 메시징(LWM)

LWM은 Cisco에서 만든 메시징 형식으로서 프로세스 간 통신이 상호 작용하는 애플리케이션과 Neutrino 간에 추상화 계층을 생성하도록 설계되었으며 운영 체제와 전송 레이어의 독립성을 목표로 합니다.Cisco가 OS 공급업체를 QNX에서 다른 것으로 전환하려는 경우, 기본 운영 체제의 기본적인 기능 간의 추상화 레이어는 운영 체제에 대한 의존성을 제거하고 다른 운영 체제로 이식하는 데 도움이 됩니다.LWM은 네이티브 Neutrino 메시지 전달 등의 동기식 보장된 메시지 전달을 제공하며, 수신자가 응답할 때까지 발신자가 차단됩니다.

LWM은 40비트 펄스를 통해 비동기 메시지 전달도 제공합니다.비동기 메시지는 비동기적으로 전송됩니다. 즉, 메시지는 대기열에 있고 발신자는 차단하지 않지만 서버에서 비동기적으로 수신되지 않고 서버가 다음 사용 가능한 메시지를 폴링할 때 전송됩니다.LWM은 클라이언트/서버로 구성됩니다.서버는 메시지를 수신 대기할 **귀**를 주는 채널을 만들고, 루프가 방금 만든 채널에서 수신 메시지를 수신하는 동안 잠시 동안 상주합니다.메시지가 수신되면 차단 해제 및 클라이언트 식별자가 수신됩니다. 이는 수신한 메시지에서 수신 ID와 사실상 동일합니다.그런 다음 서버는 일부 처리를 수행하고 나중에 클라이언트 식별자에 대한 메시지 응답을 수행합니다.

클라이언트 측에서 메시지를 연결합니다.연결된 식별자를 전달한 다음 메시지를 보내고 차단합니다.서버가 처리를 완료하면 응답하고 클라이언트가 차단 해제됩니다.이것은 Neutrinos 네이티브 메

시지가 전달하는 것과 사실상 동일하므로 추상화 레이어는 매우 얇습니다.

LWM은 고성능을 위해 최소 개수의 시스템 통화 및 컨텍스트 스위치로 설계되었으며 Cisco IOS XR 환경에서 IPC를 사용하는 것이 좋습니다.

엔브먼

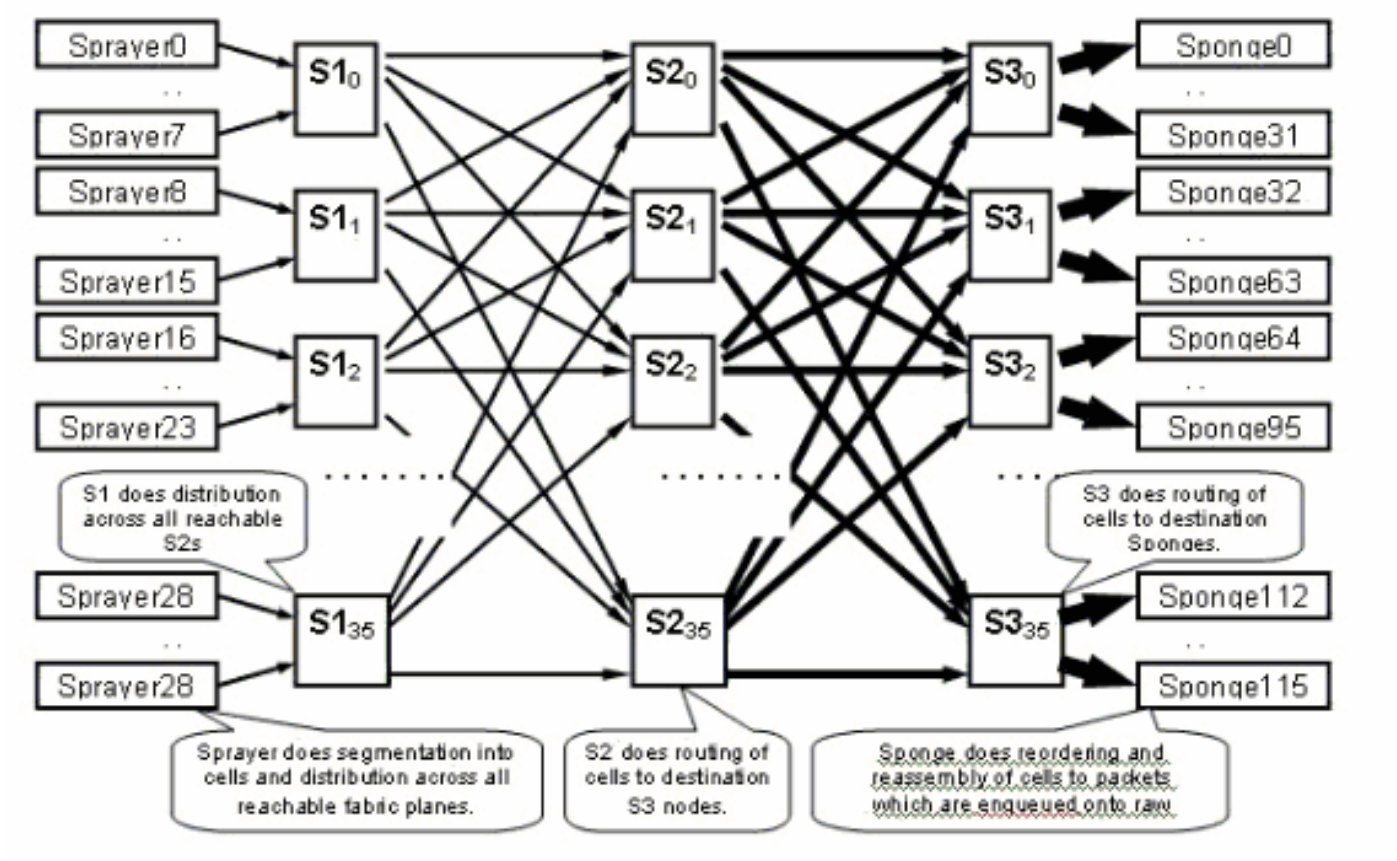
가장 기본적인 수준에서 환경 모니터 시스템은 물리적 매개변수(예: 온도, 전압, 팬 속도 등)가 작동 범위를 벗어나서 하드웨어가 손상될 수 있는 중요한 수준에 도달하는 하드웨어를 종료하는 경고 작업을 수행합니다.또한 사용 가능한 각 하드웨어 센서를 정기적으로 모니터링하고, 측정된 값을 카드별 임계값과 비교하며, 필요한 경우 경보를 발생시켜 이 작업을 수행합니다.시스템 초기화 시 시작된 영구 프로세스로, 섀시의 모든 하드웨어 센서(예: 전압, 온도, 팬 속도)를 정기적으로 폴링하고 이 데이터를 외부 관리 클라이언트에 제공합니다.또한 주기적인 프로세스는 센서 측정값을 경보 임계값과 비교하고, Fault Manager의 후속 조치를 위해 시스템 데이터베이스에 환경 경고를 게시합니다.센서 판독값이 범위를 벗어나면 환경 모니터링 프로세스에서 카드를 종료할 수 있습니다.

CRS-1 패브릭 소개

- 멀티스테이지 패브릭—3단계 벤스 토폴로지
- 혼잡을 최소화하기 위한 패브릭 내 동적 라우팅
- 셀 기반:136바이트 셀, 120바이트 데이터 페이로드
- 트래픽 격리를 개선하고 패브릭에서 버퍼링 요구 사항을 최소화하는 플로우 제어
- 스테이지에서 스테이지까지의 속도 향상
- 2개의 트래픽 캐스트 지원(유니캐스트 및 멀티캐스트)
- 캐스트당 지원되는 트래픽의 2가지 우선 순위(높음 및 낮음)
- 1M 패브릭 멀티캐스트 그룹(FGID) 지원
- 비용 효율적인 내결함성:패브릭 플레인을 사용하는 N+1 또는 N+k 리던던시(1+1과 대조적으로 비용 대폭 증가)

단일 섀시 모드에서 실행할 경우 S1, S2 및 S3 어시스코는 동일한 패브릭 카드에 있습니다.이 카드는 일반적으로 **S123 카드라고도 합니다**.멀티 섀시 컨피그레이션에서 S2는 분리되며 FCC(Fabric Card Chassis)에 있습니다. 이 컨피그레이션에서는 평면, S2 카드 및 S13 카드를 구성하기 위해 패브릭 카드 2개가 필요합니다.각 MSC는 리던던시를 제공하기 위해 8개의 패브릭 플레인에 연결되므로 하나 이상의 플레인을 느슨하게 할 경우 패브릭을 통과할 수 있는 총 트래픽은 더 낮지만 패브릭은 여전히 트래픽을 전달합니다.CRS는 7개의 평면만 있는 대부분의 패킷 크기에 대해 라인레이트로 계속 작동할 수 있습니다.배압은 홀수 평면으로 패브릭을 통해 전송됩니다.두 개 미만의 평면이 있는 시스템은 홀수 평면에서 실행하는 것이 좋습니다.두 개 미만의 평면은 지원되는 구성이 아닙니다.

패브릭 플레인



이전 다이어그램은 하나의 평면을 나타냅니다.그 도표를 8로 곱해야 한다.즉, LC의 스프라이어(ingressq) 어시가 8S1에 연결됩니다(평면당 1S1). 각 패브릭 평면의 S1은 8 분기와 연결됩니다.

- 섀시의 8개 상위 LC
- 하위 LC 8개

16슬롯 LC 섀시당 16개의 S1이 있습니다.상위 LC의 경우 8(평면당 1) + 아래쪽 LC의 경우 8.

단일 16슬롯 섀시에서 S123 패브릭 카드에는 S1s 2개, S2 2개, S3S 4개가 있습니다.그것은 패브릭 속도 계산의 일부입니다.트래픽이 들어갈 수 있는 만큼 패브릭을 종료할 수 있는 트래픽이 2배 많습니다.현재 LC당 2개의 스펀지(fabricq)와 1개의 스프라이어에도 비교됩니다.이렇게 하면 둘 이상의 인그레스 LC가 이그레스 LC에 오버로드될 때 이그레스 LC에서 버퍼링을 수행할 수 있습니다.이그레스 LC는 패브릭에서 추가 대역폭을 흡수할 수 있습니다.

패브릭 모니터링

평면 가용성 및 연결:

```
admin show controller fabric plane all
admin show controller fabric connectivity all detail
```

평면이 셀을 수신/전송하고 있으며 일부 오류가 증가하고 있는지 확인합니다.

```
admin show controllers fabric plane all statistics
```

이전 명령의 약어:

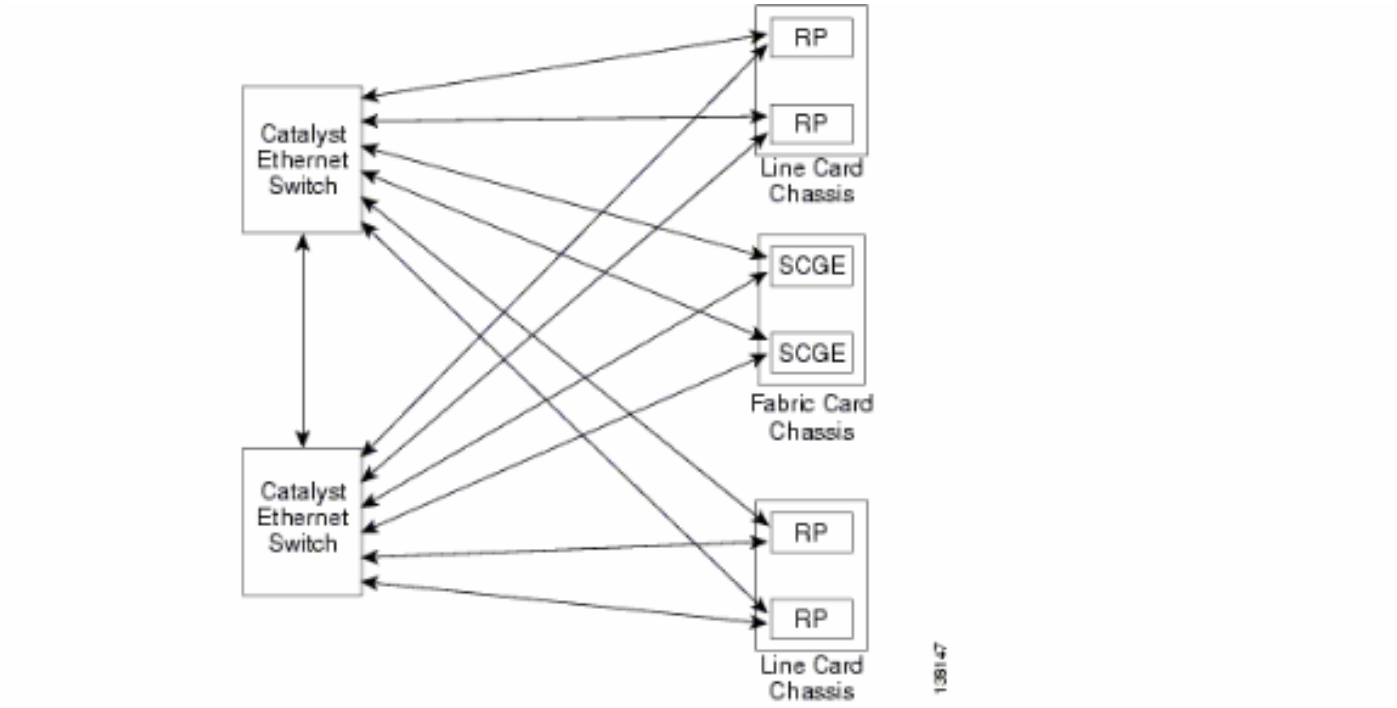
- CE - 수정 가능한 오류
- UCE - 수정 불가능한 오류
- PE - 패리티 오류

부팅 시 발생할 수 있으므로 고객이 몇 가지 오류를 발견하면 걱정하지 마십시오.필드는 런타임에 증가해서는 안 됩니다.패브릭에 문제가 있음을 나타내는 것일 수 있습니다.패브릭 플레인별 오류를 분석하려면 다음 명령을 실행합니다.

```
admin show controllers fabric plane <0-7> statistics detail
```

컨트롤 플레인 개요

라인 카드 섀시와 패브릭 섀시 간의 컨트롤 플레인 연결은 현재 RP(LCC)와 SCGE(FCC)의 기가비트 이더넷 포트를 통해 이루어집니다. 포트 간 상호 연결은 두 개 이상의 기가비트 이더넷 포트를 통해 연결할 수 있는 Catalyst 6500 스위치 쌍을 통해 제공됩니다.



Catalyst 6500 구성

이는 멀티 섀시 컨트롤 플레인에 사용되는 Catalyst 스위치에 대해 권장되는 컨피그레이션입니다.

- 모든 포트에서 단일 VLAN이 사용됩니다.
- 모든 포트는 액세스 모드(트렁킹 없음)에서 실행됩니다.
- 스패닝 트리 802.1w/s는 루프 방지에 사용됩니다.
- 두 스위치를 교차 연결하기 위해 두 개 이상의 링크가 사용되고 STP는 루프 방지에 사용됩니다.채널링은 권장되지 않습니다.
- IOS-XR에서는 표준 기반 802.1s를 지원하지 않으므로 CRS-1 RP 및 SCGE에 연결하는 포트는 사전 표준 모드를 사용합니다.
- 스위치 간, 스위치와 RP/SCGE 간에 연결하는 포트에서 UDLD를 활성화해야 합니다.
- UDLD는 CRS-1에서 기본적으로 활성화되어 있습니다.

Multishelf 시스템에서 Catalyst 6500을 구성하는 방법에 대한 자세한 내용은 Bring Up the Cisco IOS XR Software on a Multishelf System을 참조하십시오.

멀티 섀시 제어 평면 관리

멀티 섀시 시스템의 컨트롤 플레인 연결을 제공하는 Catalyst 6504-E 섀시는 다음 관리 서비스에 대해 구성됩니다.

- 각 PoP에서 LAN 스위치에 연결되는 포트 기가비트 1/2를 통한 대역 내 관리작은 범위의 서브넷 및 프로토콜에 대해서만 액세스가 허용됩니다.
- NTP는 시스템 시간을 설정하는 데 사용됩니다.
- syslog는 표준 호스트에 수행됩니다.
- SNMP 폴링 및 트랩은 중요한 기능에 대해 활성화할 수 있습니다.

참고: Catalyst는 변경되지 않습니다.사전 테스트는 계획된 변경 사항에 대해 수행되어야 하며, 유지 보수 기간 동안 수행하는 것이 좋습니다.

다음은 관리 구성의 예입니다.

```
#In-band management connectivity
interface GigabitEthernet2/1
 description *CRS Multi-chassis Management Ethernet - DO NOT TOUCH*
 ip address [ip address] [netmask]
 ip access-group control_only in
!
!
ip access-list extended control_only
 permit udp [ip address] [netmask] any eq snmp
 permit udp [ip address] [netmask] eq ntp any
 permit tcp [ip address] [netmask] any eq telnet

#NTP

ntp update-calendar
ntp server [ip address]

#Syslog
logging source-interface Loopback0
logging [ip address]
logging buffered 4096000 debugging
no logging console

#RADIUS
aaa new-model
aaa authentication login default radius enable
enable password {password}
radius-server host [ip address] auth-port 1645 acct-port 1646
radius-server key {key}

#Telnet and console access
!
access-list 3 permit [ip address]
!
line con 0
 exec-timeout 30 0
 password {password}
line vty 0 4
 access-class 3 in
 exec-timeout 0 0
password {password}
```

ROMMON 및 Monlib

Cisco monlib는 디바이스에 저장되고 ROMMON에서 실행하기 위해 RAM에 로드되는 실행 프로그램입니다.ROMMON은 디바이스의 파일에 액세스하기 위해 monlib를 사용합니다.ROMMON 버전은 Cisco 기술 지원의 권장 사항에 따라 업그레이드할 수 있으며 이를 수행해야 합니다.최신 ROMMON 버전은 1.40입니다.

업그레이드 지침

다음 단계를 완료하십시오.

1. Cisco CRS-1 ROMMON에서 ROMMON 바이너리를 다운로드합니다(등록된 고객만 해당).
2. TAR 파일의 압축을 풀고 6개의 BIN 파일을 Disk0의 CRS 루트 디렉토리에 복사합니다.
```
RP/0/RP0/Router#dir disk0:/*.bin

Directory of disk0:

65920       -rwx  360464      Fri Oct 28 12:58:02 2005  rommon-hfr-ppc7450-sc-dsmp-A.bin
66112       -rwx  360464      Fri Oct 28 12:58:03 2005  rommon-hfr-ppc7450-sc-dsmp-B.bin
66240       -rwx  376848      Fri Oct 28 12:58:05 2005  rommon-hfr-ppc7455-asmp-A.bin
66368       -rwx  376848      Fri Oct 28 12:58:06 2005  rommon-hfr-ppc7455-asmp-B.bin
66976       -rwx  253904      Fri Oct 28 12:58:08 2005  rommon-hfr-ppc8255-sp-A.bin
67104       -rwx  253492      Fri Oct 28 12:58:08 2005  rommon-hfr-ppc8255-sp-B.bin
```
3. **show diag** 사용 현재 rommon 버전을 보려면 **| inc ROM|NODE|PLIM** 명령을 사용합니다.
```
RP/0/RP0/CPU0:ROUTER(admin)#show diag | inc ROM|NODE|PLIM
NODE 0/0/SP : MSC(SP)
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
PLIM 0/0/CPU0 : 4OC192-POS/DPT
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/2/SP : MSC(SP)
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
PLIM 0/2/CPU0 : 8-10GbE
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/4/SP : Unknown Card Type
NODE 0/6/SP : MSC(SP)
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
PLIM 0/6/CPU0 : 16OC48-POS/DPT
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/RP0/CPU0 : RP
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/RP1/CPU0 : RP
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/SM0/SP : FC/S
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
NODE 0/SM1/SP : FC/S
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
NODE 0/SM2/SP : FC/S
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
NODE 0/SM3/SP : FC/S
ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
```
4. ROMMON을 업그레이드하려면 ADMIN 모드**로 이동하고** upgrade rommon **a all disk0** 명령을 사용합니다.
```
RP/0/RP0/CPU0:ROUTER#admin
RP/0/RP0/CPU0:ROUTER(admin)#upgrade rommon a all disk0
Please do not power cycle, reload the router or reset any nodes until
 all upgrades are completed.
Please check the syslog to make sure that all nodes are upgraded successfully.
If you need to perform multiple upgrades, please wait for current upgrade
 to be completed before proceeding to another upgrade.
Failure to do so may render the cards under upgrade to be unusable.
```
5. ADMIN Mode를 종료하고 show **log를 입력합니다. | inc "OK, ROMMON A"**를 입력하고 모든

노드가 성공적으로 업그레이드되었는지 확인합니다.노드가 하나라도 실패하면 4단계로 돌아가 다시 프로그래밍합니다.

```
RP/0/RP0/CPU0:ROUTER#show logging | inc "OK, ROMMON A"
RP/0/RP0/CPU0:Oct 28 14:40:57.223 PST8: upgrade_daemon[380][360]: OK, ROMMON A is
programmed successfully. SP/0/0/SP:Oct 28 14:40:58.249 PST8: upgrade_daemon[125][121]: OK,
ROMMON A is programmed successfully. SP/0/2/SP:Oct 28 14:40:58.251 PST8:
upgrade_daemon[125][121]: OK, ROMMON A is programmed successfully. LC/0/6/CPU0:Oct 28
14:40:58.336 PST8: upgrade_daemon[244][233]: OK, ROMMON A is programmed successfully.
LC/0/2/CPU0:Oct 28 14:40:58.365 PST8: upgrade_daemon[244][233]: OK, ROMMON A is programmed
successfully. SP/0/SM0/SP:Oct 28 14:40:58.439 PST8: upgrade_daemon[125][121]: OK, ROMMON A
is programmed successfully. SP/0/SM1/SP:Oct 28 14:40:58.524 PST8: upgrade_daemon[125][121]:
OK, ROMMON A is programmed successfully. LC/0/0/CPU0:Oct 28 14:40:58.530 PST8:
upgrade_daemon[244][233]: OK, ROMMON A is programmed successfully. RP/0/RP1/CPU0:Oct 28
14:40:58.593 PST8: upgrade_daemon[380][360]: OK, ROMMON A is programmed successfully.
SP/0/6/SP:Oct 28 14:40:58.822 PST8: upgrade_daemon[125][121]: OK, ROMMON A is programmed
successfully. SP/0/SM2/SP:Oct 28 14:40:58.890 PST8: upgrade_daemon[125][121]: OK, ROMMON A
is programmed successfully. SP/0/SM3/SP:Oct 28 14:40:59.519 PST8: upgrade_daemon[125][121]:
OK, ROMMON A is programmed successfully.
```

6. ROMMON을 업그레이드하려면 ADMIN 모드로 이동하여 **upgrade rommon b all disk0** 명령을 사용합니다.

```
RP/0/RP0/CPU0:ROUTER#admin
RP/0/RP0/CPU0:ROUTER(admin)#upgrade rommon b all disk0
Please do not power cycle, reload the router or reset any nodes until
 all upgrades are completed.
Please check the syslog to make sure that all nodes are upgraded successfully.
If you need to perform multiple upgrades, please wait for current upgrade
 to be completed before proceeding to another upgrade.
Failure to do so may render the cards under upgrade to be unusable.
```

7. ADMIN Mode를 종료하고 show **log를 입력합니다. | inc "OK, ROMMON B"**를 입력하고 모든 노드가 성공적으로 업그레이드되었는지 확인합니다.노드가 하나라도 실패하면 4단계로 돌아가 다시 프로그래밍합니다.

```
RP/0/RP0/CPU0:Router#show logging | inc "OK, ROMMON B"
RP/0/RP0/CPU0:Oct 28 13:27:00.783 PST8: upgrade_daemon[380][360]: OK,
ROMMON B is programmed successfully.
LC/0/6/CPU0:Oct 28 13:27:01.720 PST8: upgrade_daemon[244][233]: OK,
ROMMON B is programmed successfully.
SP/0/2/SP:Oct 28 13:27:01.755 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
LC/0/2/CPU0:Oct 28 13:27:01.775 PST8: upgrade_daemon[244][233]: OK,
ROMMON B is programmed successfully.
SP/0/0/SP:Oct 28 13:27:01.792 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
SP/0/SM0/SP:Oct 28 13:27:01.955 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
LC/0/0/CPU0:Oct 28 13:27:01.975 PST8: upgrade_daemon[244][233]: OK,
ROMMON B is programmed successfully.
SP/0/6/SP:Oct 28 13:27:01.989 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
SP/0/SM1/SP:Oct 28 13:27:02.087 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
RP/0/RP1/CPU0:Oct 28 13:27:02.106 PST8: upgrade_daemon[380][360]: OK,
ROMMON B is programmed successfully.
SP/0/SM3/SP:Oct 28 13:27:02.695 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
SP/0/SM2/SP:Oct 28 13:27:02.821 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
```

8. upgrade 명령은 새로운 ROMMON을 사용하여 bootflash의 특별한 예약 섹션을 사용합니다.그러나 새 ROMMON은 카드를 다시 로드할 때까지 비활성 상태로 유지됩니다.따라서 카드를 다시 로드하면 새 ROMMON이 활성화됩니다.각 노드를 한 번에 하나씩 재설정하거나 전체 라우터를 재설정하면 됩니다.

```
Reload Router:
RP/0/RP0/CPU0:ROUTER#hw-module node 0/RP0/CPU0 or 0/RP1/CPU0 reload (depends on which on is
in Standby Mode.
RP/0/RP0/CPU0:ROUTER#reload
!--- Issue right after the first command. Updating Commit Database. Please wait...[OK]
Proceed with reload? [confirm] !--- Reload each Node. For Fan Controllers (FCx), !--- Alarm
Modules (AMx), Fabric Cards (SMx), and RPs (RPx), !--- you must wait until the reloaded
node is fully reloaded !--- before you reset the next node of the pair. But non-pairs !---
can be reloaded without waiting. RP/0/RP0/CPU0:ROUTER#hw-module node 0/RP0/CPU0 or
0/RP1/CPU0 reload
!--- This depends on which on is in Standby Mode. RP/0/RP0/CPU0:ROUTER#hw-module node
0/FC0/SP
RP/0/RP0/CPU0:ROUTER#hw-module node 0/AM0/SP
RP/0/RP0/CPU0:ROUTER#hw-module node 0/SM0/SP
!--- Do not reset the MSC and Fabric Cards at the same time. RP/0/RP0/CPU0:ROUTER#hw-module
node 0/0/CPU
```

9. **show diag** 사용 현재 ROMMON 버전을 확인하려면 **| inc ROM|NODE|PLIM** 명령을 사용합니다.

```
RP/0/RP1/CPU0:CRS-B(admin)#show diag | inc ROM|NODE|PLIM
NODE 0/0/SP : MSC(SP)
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
PLIM 0/0/CPU0 : 4OC192-POS/DPT
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]
NODE 0/2/SP : MSC(SP)
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
PLIM 0/2/CPU0 : 8-10GbE
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]
NODE 0/6/SP : MSC(SP)
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
PLIM 0/6/CPU0 : 16OC48-POS/DPT
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]
NODE 0/RP0/CPU0 : RP
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]
NODE 0/RP1/CPU0 : RP
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]]
NODE 0/SM0/SP : FC/S
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
NODE 0/SM1/SP : FC/S
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
NODE 0/SM2/SP : FC/S
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
NODE 0/SM3/SP : FC/S
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
```

참고: CRS-8 및 패브릭 섀시에서 ROMMON은 팬 속도를 기본 속도 4000RPM으로 설정합니다.

PLIM 및 MSC 개요

이는 CRS-1 라우터의 패킷 흐름을 나타내며, 이러한 용어는 교환적으로 사용됩니다.

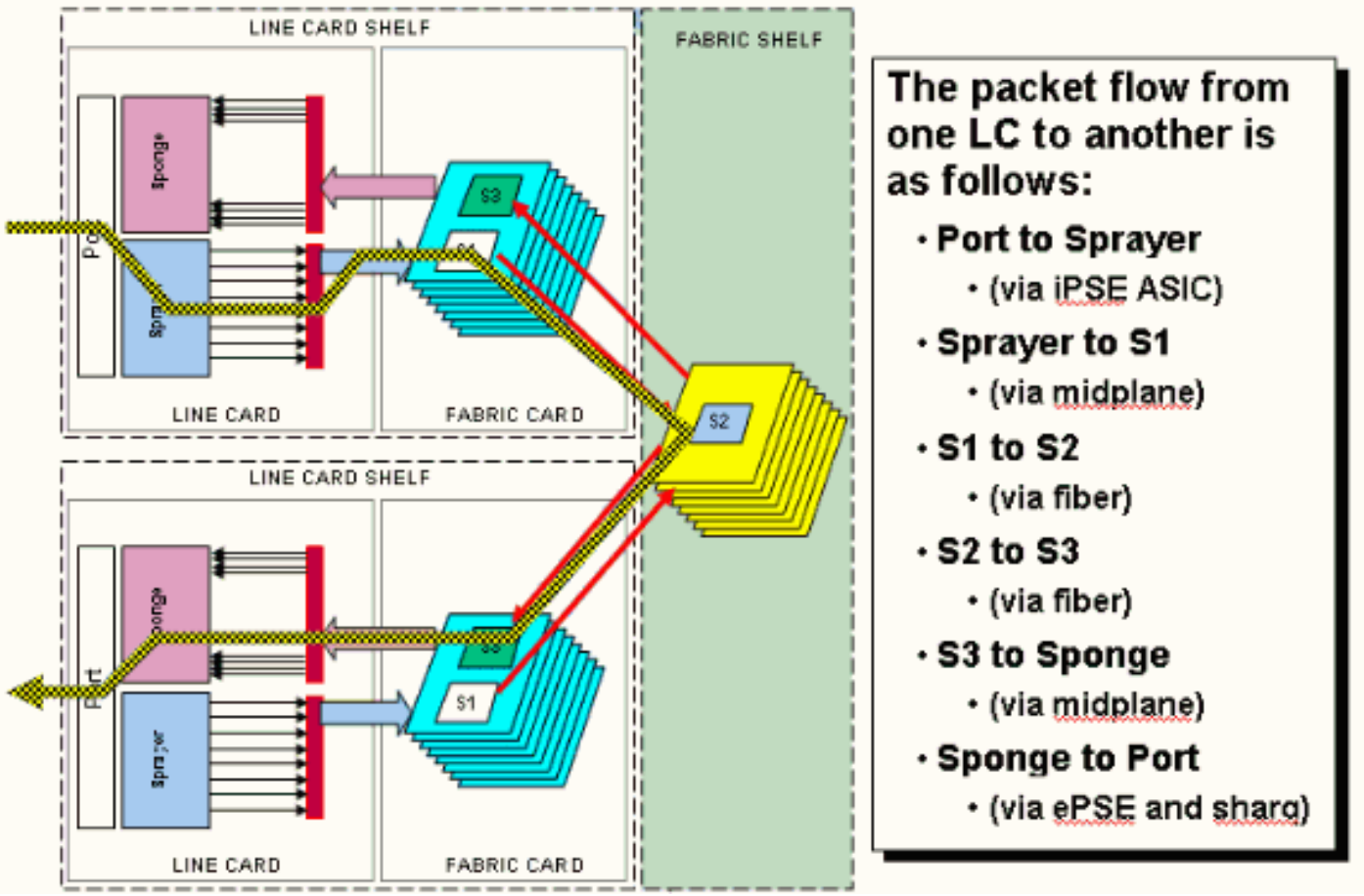
IngressQ ASIC은 Sprlayer ASIC라고도 합니다.

FabricQ ASIC은 스폰지 ASIC라고도 합니다.

EgressQ ASIC는 Sharq ASIC라고도 합니다.

SPP는 PSE(Packet Switch Engine) ASIC라고도 합니다.

Rx PLIM > Rx SPP > Ingress Q > Fabric(패브릭) > Fabric Q > Tx SPP > Egress Q > Tx PLIM (Sprayer) (Sponge) (Sharq)

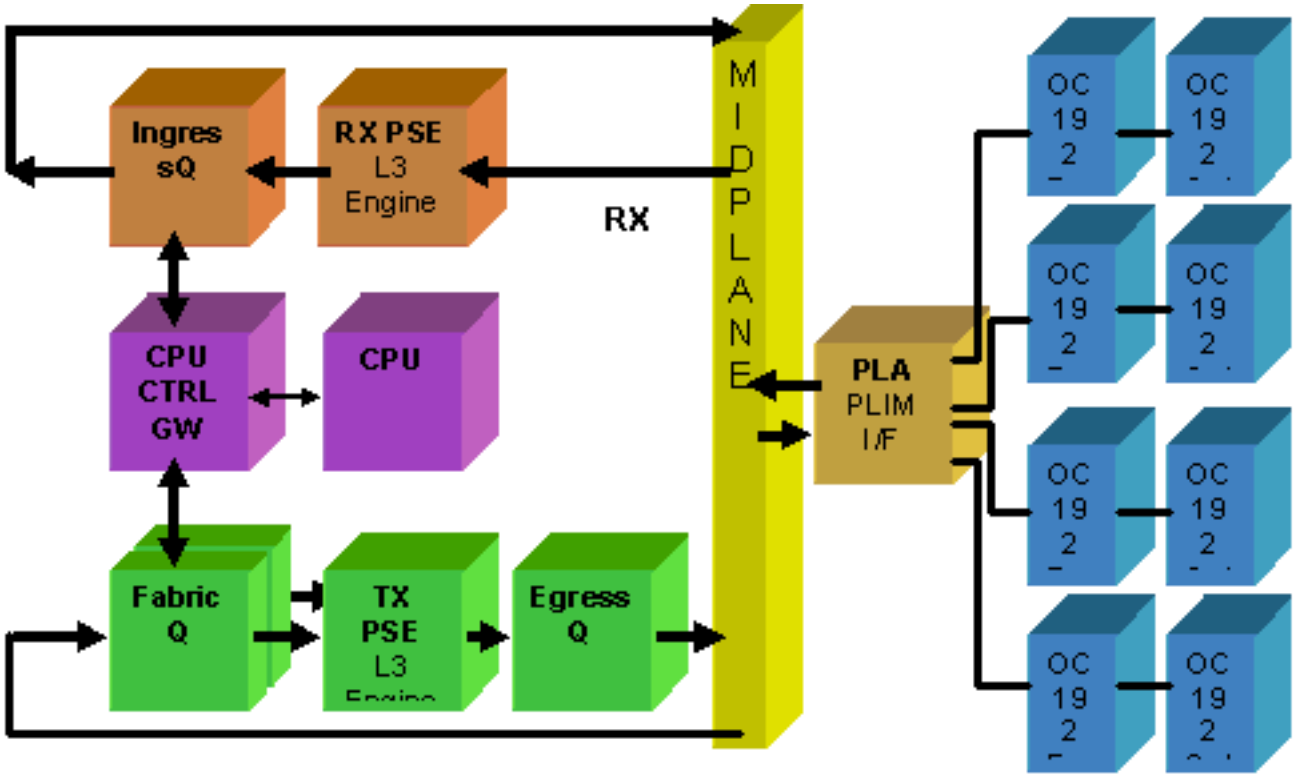


패킷은 PLIM(Physical Layer Interface Module)에서 수신됩니다.

PLIM에는 연결된 MSC에 대한 물리적 인터페이스가 포함되어 있습니다.PLIM 및 MSC는 섀시 백플레인을 통해 연결된 별도의 카드입니다.따라서 특정 MSC에 대한 인터페이스 유형은 해당 MSC가 면맞춤한 PLIM의 유형에 의해 정의됩니다.PLIM 유형에 따라 카드에는 인터페이스에 대한 물리적 미디어 및 프레이밍을 제공하는 다양한 ASIC가 포함되어 있습니다.PLIM ASIC의 목적은 MSC와 물리적 연결 간의 인터페이스를 제공하는 것입니다.광섬유를 종료하고, 광원을 전기 변환으로 전환하며, 미디어 프레이밍을 SDH/Sonet/Ethernet/HDLC/PPP로 종료하고, CRC를 확인하고, 버퍼 헤더라는 일부 제어 정보를 추가하고, MSC에 남아 있는 비트를 전달합니다.PLIM은 HDLC 또는 PPP keepalive를 소스/싱크하지 않습니다.이는 MSC의 CPU에 의해 처리됩니다.

PLIM은 다음과 같은 기능도 제공합니다.

- 1/10 기가비트 이더넷을 위한 MAC 필터링
- 1/10 기가비트 이더넷을 위한 인그레스/이그레스 MAC 어카운팅
- 1/10 기가비트 이더넷을 위한 VLAN 필터링
- 1/10 기가비트 이더넷을 위한 VLAN 어카운팅
- 인그레스 버퍼링 및 혼잡 알림



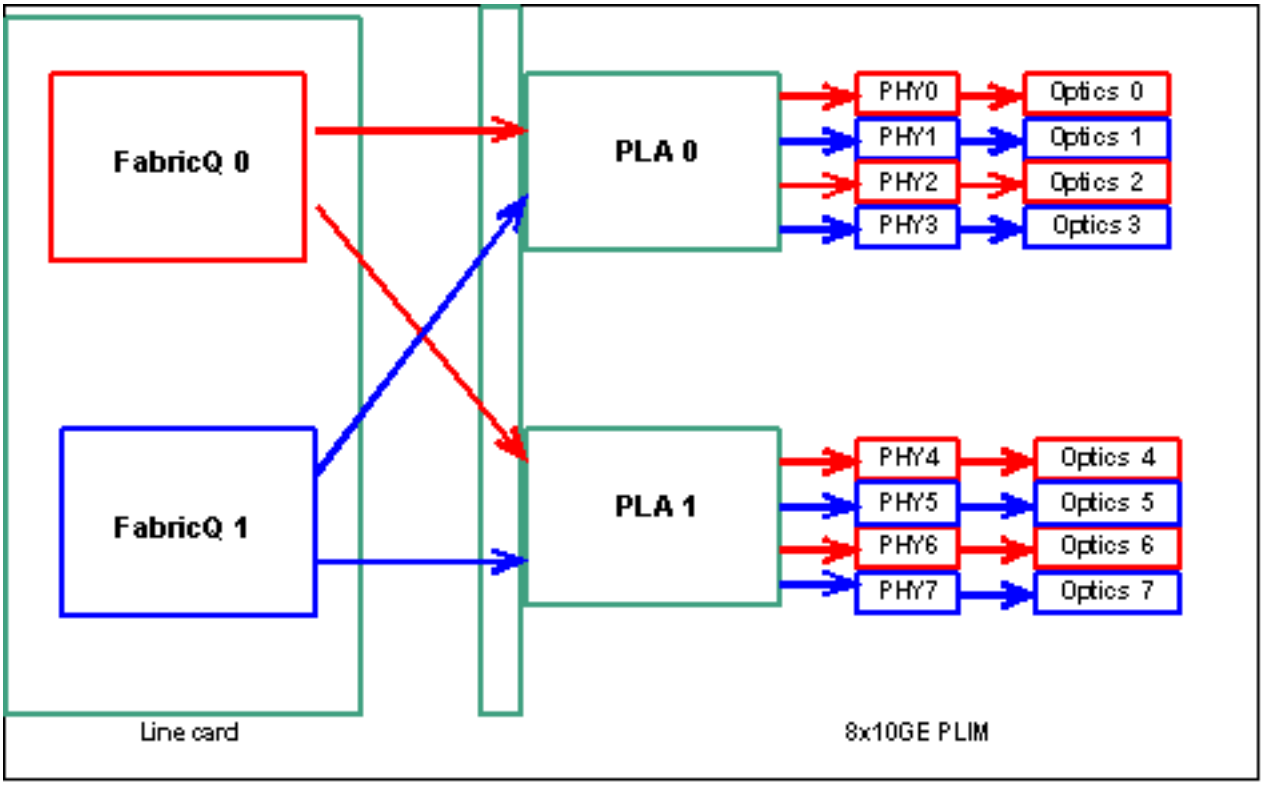
PLIM 초과 서브스크립션

10GE PLIM

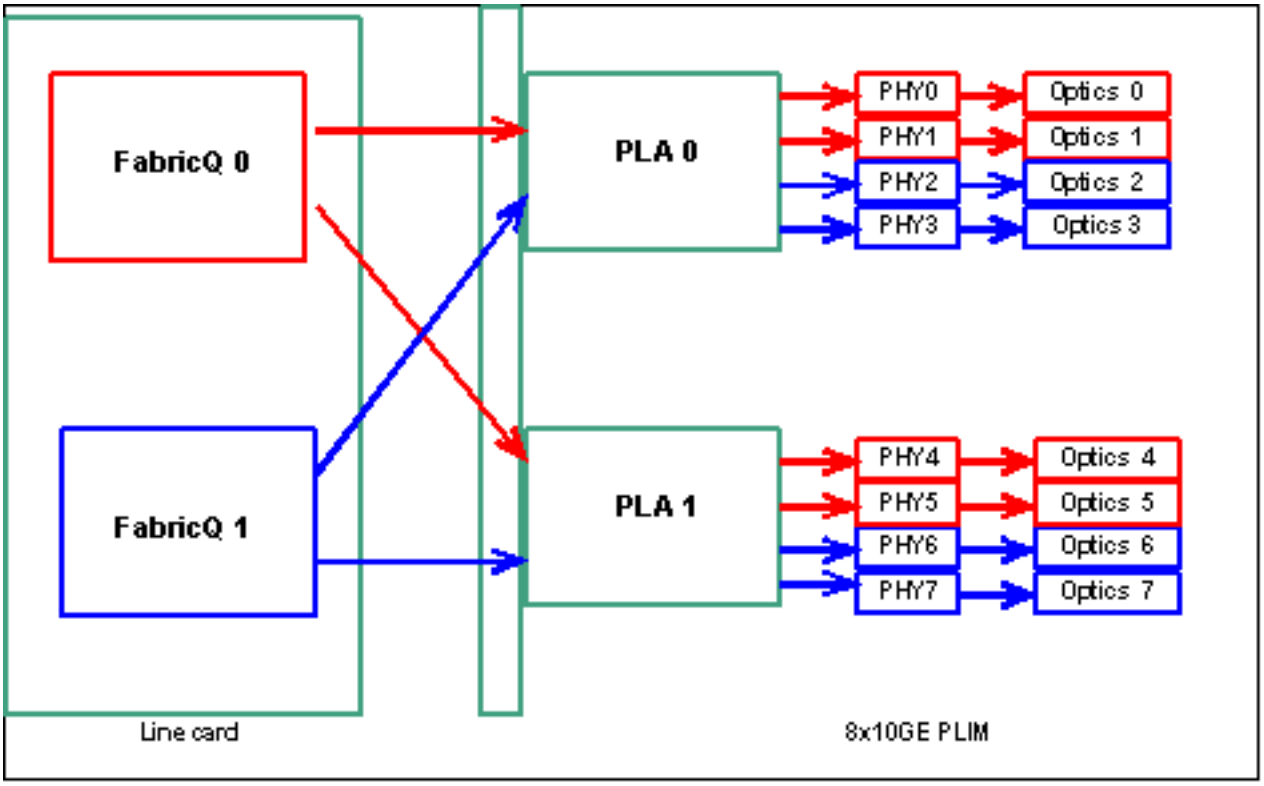
8 X 10G PLIM은 약 80Gbps의 트래픽을 종료할 수 있는 기능을 제공하지만 MSC의 포워딩 용량은 최대 40Gbps입니다.PLIM에서 사용 가능한 모든 포트가 채워지면 초과 서브스크립션이 발생하고 프리미엄 트래픽이 실수로 삭제되지 않도록 QoS 모델링이 매우 중요해집니다.일부 경우 초과 가입은 옵션이 아니므로 방지해야 합니다.이 작업을 수행하려면 8개 포트 중 4개만 사용해야 합니다.또한 MSC 및 PLIM 내의 최적의 대역폭을 4개 포트 각각에 사용할 수 있도록 주의해야 합니다.

참고: 포트 매핑은 릴리스 3.2.2에서 계속 변경됩니다.이 다이어그램을 참조하십시오.

릴리스 3.2.1까지 포트 매핑



릴리스 3.2.2에서 포트 매핑



앞서 언급한 대로 물리적 포트는 2개의 FabricQ ASIC 중 하나를 통해 서비스됩니다.ASIC에 포트 할당은 정적으로 정의되며 변경할 수 없습니다.또한 8 X 10G PLIM에는 2개의 PLA ASIC가 있습니다.첫 번째 PLA 서비스 포트 0~3, 두 번째 서비스 4~7. 8개의 10G PLIM에서 단일 PLA의 대역폭 용량은 약 24Gbps입니다.단일 FabricQ ASIC의 스위칭 용량은 약 62Mpps입니다.

포트 0~3을 채우거나 포트 4~7을 채우면 PLA의 대역폭 용량(24Gbps)이 전체 처리량을 제한하는 4개의 포트 모두에서 공유됩니다.이러한 모든 포트가 하나의 FabricQ ASIC에 의해 서비스되므로 포트 0,2,4 및 6(최대 3.2.1) 또는 0,1,4 및 5(3.2.2 이상)를 채울 경우, 스위칭 용량이 62Mpps인 FabricQ ASIC가 다시 처리량을 제한합니다.

최적의 성능을 얻으려면 PLA와 FabricQ ASIC의 최고 효율성을 얻을 수 있는 방식으로 포트를 활용하는 것이 가장 좋습니다.

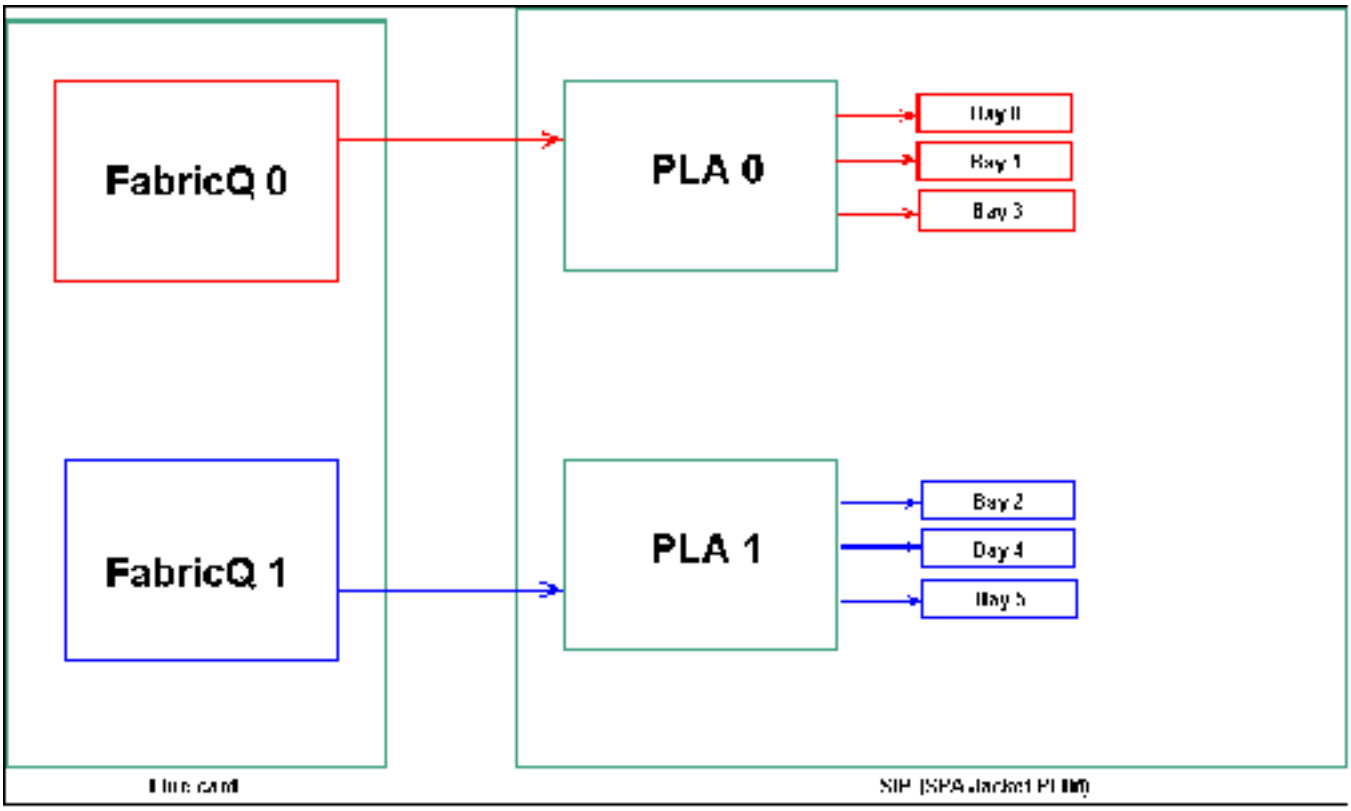
SIP-800/SPA

SIP-800 PLIM은 SPA(Service Port Adapters)라고 하는 모듈형 인터페이스 카드로 작동할 수 있는 기능을 제공합니다. SIP-800은 이론적인 인터페이스 용량이 60Gbps인 6개의 SPA 베이를 제공합니다.MSC의 포워딩 용량은 최대 40Gbps입니다.SIP-800의 모든 베이를 채워야 하는 경우 SPA 유형에 따라 초과 서브스크립션이 발생할 수 있으며 QoS 모델링이 매우 중요하여 프리미엄 트래픽이 실수로 삭제되지 않도록 해야 합니다.

참고: 오버서브스크립션은 POS 인터페이스에서 지원되지 않습니다.그러나 올바른 처리량 용량을 제공하려면 10Gb POS SPA를 배치하는 것이 적절해야 합니다.10Gb 이더넷 SPA는 IOS-XR 릴리스 3.4에서만 지원됩니다. 이 SPA는 초과 서브스크립션 기능을 제공합니다.

일부 경우 초과 가입은 옵션이 아니므로 방지해야 합니다.이를 위해서는 6개의 베이 중 4개만 사용해야 합니다.또한 MSC 및 PLIM 내의 최적의 대역폭을 4개 포트 각각에 사용할 수 있도록 해야 합니다.

SPA 베이 매핑



앞에서 언급한 대로 물리적 포트는 2개의 FabricQ ASIC 중 하나를 통해 서비스됩니다.ASIC에 포트 할당은 정적으로 정의되며 변경할 수 없습니다.또한 SIP-800 PLIM에는 2개의 PLA ASIC가 있습니다.첫 번째 PLA 서비스 포트 0,1 및 3, 두 번째 서비스 2, 4 및 5.

SIP-800 PLIM의 단일 PLA의 대역폭 용량은 약 24Gbps입니다.단일 FabricQ ASIC의 스위칭 용량은 약 62Mpps입니다.

포트 0, 1 및 3 또는 포트 2, 4 및 5를 채울 경우 PLA의 대역폭 용량(24Gbps)은 전체 처리량을 제한하는 세 포트 모두에서 공유됩니다.각 FabricQ가 해당 포트 그룹을 서비스하므로 포트 그룹의 최대 패킷 속도는 62Mpps입니다.최적의 대역폭을 얻기 위해 PLA의 최고 효율성을 얻는 방식으로 포트를 활용하는 것이 가장 좋습니다.

제안된 배치:

	SPA 베이 번호	SPA 베이 번호	SPA 베이 번호	SPA 베이 번호
옵션 1	0	1	4	5
옵션 2	1	2	3	4

카드를 4개 이상의 SPA로 채우려면 이전에 나열된 옵션 중 하나를 완료하여 두 포트 그룹(0,1 & 3 & 2,4 & 5) 간에 인터페이스를 분산하는 것이 좋습니다. 그런 다음 0, 1 및 3, 2, 4 및 5 포트 그룹의 열린 포트 중 하나에 다음 SPA 모듈을 배치해야 합니다.

DWDM XENPACK

릴리스 3.2.2 부터는 DWDM XENPACK을 설치하고 **조정 가능한** 옵틱 모듈을 제공할 수 있습니다 .이러한 XENPACK 모듈의 냉각 요구 사항을 충족하려면 설치된 모듈 사이에 빈 슬롯이 있어야 합니다.또한 단일 DWDM XENPACK 모듈이 설치된 경우 XENPACK 모듈이 DWDM 디바이스가 아닌 경우에도 최대 4개의 포트를 사용할 수 있습니다.따라서 FabricQ에서 PLA로 포트 매핑에 직접적인 영향을 미칩니다.이 요구 사항에 주의를 기울여야 하며 이 표에 나와 있습니다.

제안된 배치:

	옵틱 포트 번호	**옵틱 포트 번호**	**옵틱 포트 번호**	**옵틱 포트 번호**
옵션 1 또는 DWDM XENPACK	0	2	5	7
옵션 2	1	3	4	6

3.2.2 이상 또는 3.3 설치 시 FabricQ 매핑 변경을 방지합니다.따라서 일반 모듈과 DWDM XENPACK 모듈 모두에 더 간단한 배치 패턴을 사용할 수 있습니다.

	옵틱 포트 번호	**옵틱 포트 번호**	**옵틱 포트 번호**	**옵틱 포트 번호**
옵션 1	0	2	4	6
옵션 2	1	3	5	7

4개 이상의 비 DWDM XENPACK 포트로 카드를 채우려면 나열된 옵션 중 하나를 완료하여 두 포트 그룹(0-3 및 4-7) 간에 옵티컬 인터페이스 모듈을 확장하는 것이 좋습니다. 그런 다음 0-3 또는 4-7 포트 그룹의 열린 포트 중 하나에 다음 Optical 인터페이스 모듈을 배치해야 합니다.Optical 인터페이스 모듈 #5에 0-3 포트 그룹을 사용하는 경우 Optical 인터페이스 모듈 #6을 4-7 포트 그룹에 배치해야 합니다.

자세한 내용은 DWDM XENPAK 모듈을 참조하십시오.

컨피그레이션 관리

IOS-XR의 컨피그레이션은 2단계 컨피그레이션을 통해 수행되며, 첫 번째 단계에서 사용자가 컨피그레이션을 입력합니다.이 단계에서는 CLI에서 컨피그레이션 구문만 확인합니다.이 단계에서 입력한 컨피그레이션은 컨피그레이션 에이전트 프로세스에만 알려져 있습니다(예: CLI/XML).컨피그레이션은 sysdb 서버에 기록되지 않으므로 확인되지 않습니다.백엔드 응용 프로그램에 알림이 전송되지 않으며 이 단계의 구성에 액세스하거나 해당 구성에 대한 정보를 얻을 수 없습니다.

두 번째 단계에서는 사용자가 컨피그레이션을 명시적으로 커밋합니다.이 단계에서는 컨피그레이션이 sysdb 서버에 기록되고 백엔드 애플리케이션은 컨피그레이션 및 알림이 sysdb에 의해 생성되는지 확인합니다.첫 번째 단계에서 입력한 컨피그레이션을 커밋하기 전에 컨피그레이션 세션을 중단할 수 있습니다.따라서 1단계에서 입력한 모든 컨피그레이션이 항상 2단계에서 커밋된다고 가정하는 것은 안전하지 않습니다.

또한 1단계와 2단계 동안 여러 사용자가 라우터의 작업 및/또는 실행 중인 컨피그레이션을 수정할 수 있습니다.따라서 1단계에서 컨피그레이션 및/또는 운영 상태를 실행하는 라우터의 테스트는 컨피그레이션이 실제로 커밋되는 2단계에서 유효하지 않을 수 있습니다.

구성 파일 시스템

CFS(Configuration File System)는 라우터의 컨피그레이션을 저장하는 데 사용되는 파일 및 디렉토리 집합입니다.CFS는 RP에서 사용되는 기본 미디어인 disk0:/config/ 디렉토리에 저장됩니다 .CFS의 파일 및 디렉토리는 라우터의 내부 파일이며 사용자가 수정하거나 제거할 수 없습니다.이로 인해 컨피그레이션이 손실되거나 손상되어 서비스에 영향을 미칠 수 있습니다.

CFS는 모든 커밋 후 standby-RP를 확인합니다.이렇게 하면 장애 조치 후 라우터의 컨피그레이션 파일을 보존할 수 있습니다.

라우터 부팅 중에 마지막 활성 컨피그레이션은 CFS에 저장된 컨피그레이션 커밋 데이터베이스에서 적용됩니다.사용자가 각 컨피그레이션 커밋 후 활성 컨피그레이션을 수동으로 저장할 필요는 없습니다. 라우터에서 자동으로 이 작업을 수행하기 때문입니다.

부팅 중에 컨피그레이션을 적용하는 동안에는 컨피그레이션을 변경하는 것이 좋습니다.컨피그레이션 애플리케이션이 완료되지 않은 경우 라우터에 로그온할 때 다음 메시지가 표시됩니다.

시스템 구성 프로세스

이 장치에 대한 시작 컨피그레이션이 현재 로드되고 있습니다.몇 분 정도 걸릴 수 있습니다.완료 시 공지됩니다.이 프로세스가 완료될 때까지 디바이스를 다시 구성하지 마십시오.드문 경우이지만 CFS에서 마지막 활성 컨피그레이션을 복원하는 대신 사용자가 제공한 ASCII 컨피그레이션 파일에서 라우터 컨피그레이션을 복원하는 것이 좋습니다.

다음과 같은 방법으로 구성 파일을 강제로 적용할 수 있습니다.

```
using the “-a” option with the boot command. This option forces
    the use of the specified file only for this boot.

    rommon>boot <image> –a <config-file-path>

    setting the value of “IOX_CONFIG_FILE” boot variable to the
    path of configuration file. This forces the use of the specified file
    for all boots while this variable is set.

    rommon>IOX_CONFIG_FILE=




    rommon>boot <image>
```

라우터 컨피그레이션을 복원하는 동안 하나 이상의 컨피그레이션 항목이 적용되지 않을 수 있습니다.실패한 모든 컨피그레이션은 CFS에 저장되며 다음 다시 로드할 때까지 유지됩니다.

실패한 컨피그레이션을 찾아보고 오류를 해결하고 컨피그레이션을 다시 적용할 수 있습니다.

다음은 라우터를 시작하는 동안 실패한 컨피그레이션을 해결하기 위한 몇 가지 팁입니다.

IOX에서는 다음과 같은 세 가지 이유로 컨피그레이션을 실패한 컨피그레이션으로 분류할 수 있습니다.

1. 구문 오류 - 파서는 구문 오류를 생성합니다. 구문 오류는 일반적으로 CLI 명령과 호환되지 않음을 나타냅니다.구문 오류를 수정하고 컨피그레이션을 다시 적용해야 합니다.
2. 의미 오류 - 구성 관리자가 라우터를 시작하는 동안 컨피그레이션을 복원할 때 백엔드 구성 요소에서 의미 오류를 생성합니다.cfgmgr은 실행 중인 컨피그레이션의 일부로서 컨피그레이션이 수락되도록 보장할 책임이 없습니다.cfgmgr은 단지 **중인일** 뿐이며 백엔드 구성 요소가 생성하는 의미론적 오류만 보고합니다.각 백엔드 구성 요소 소유자는 장애 사유를 분석하고 실패 원인을 파악해야 합니다.사용자는 백 엔드 구성 요소 확인자**의** 소유자를 쉽게 찾기 위해 구성 모드에서 **describe <CLI commands>**를 실행할 수 있습니다.예를 들어, **라우터 bgp 217이** 실패한 컨피그레이션으로 표시되는 경우 **describe** 명령은 구성 요소 검증자가 ipv4-bgp 구성 요소임을 표시합니다.

```
RP/0/0/CPU0:router#configure terminal
RP/0/0/CPU0:router(config)#describe router bgp 217
The command is defined in bgpv4_cmds.parser

Node 0/0/CPU0 has file bgpv4_cmds.parser for boot package /gsr-os-mbi-3.3.87/mbi12000-rp.vm
from gsr-rout
Package:
    gsr-rout
        gsr-rout V3.3.87[Default]  Routing Package
        Vendor : Cisco Systems
        Desc   : Routing Package
        Build  : Built on Mon Apr  3 16:17:28 UTC 2006
        Source : By ena-view3 in /vws/vpr/mletchwo/cfgmgr_33_bugfix for c2.95.3-p8
        Card(s): RP, DRP, DRPSC
        Restart information:
          Default:
            parallel impacted processes restart
Component:
    ipv4-bgp V[fwd-33/66]  IPv4 Border Gateway Protocol (BGP)

File: bgpv4_cmds.parser


User needs ALL of the following taskids:

        bgp (READ WRITE)

It will take the following actions:
  Create/Set the configuration item:
         Path: gl/ip-bgp/0xd9/gbl/edm/ord_a/running
        Value: 0x1
Enter the submode:
        bgp
RP/0/0/CPU0:router(config)#
```

3. Apply errors(오류 적용) - 컨피그레이션이 실행 중인 컨피그레이션의 일부로 확인 및 승인되었지만 백엔드 구성 요소가 어떤 이유로 작동 상태를 업데이트할 수 없습니다.구성이 올바르게 확인되었으므로 실행 중인 컨피그레이션과 백엔드 운영 오류로 인해 실패한 컨피그레이션으로 표시됩니다.구성 요소 적용 소유자를 찾기 위해 적용하지 못한 CLI에서 describe 명령을 다시 실행할 수 있습니다.시작 운영자 중에 실패한 컨피그레이션을 찾아 다시 적용하려면 다음 단계를 완료하십시오.R3.2 운영자의 경우 이 절차를 사용하여 실패한 컨피그레이션을 다시 적용할 수 있습니다.운영자는 **show configuration failed startup** 명령을 사용하여 라우터 시작 중에 저장된 실패한 컨피그레이션을 찾아볼 수 있습니다.운영자는 show configuration failed startup noerror를 실행해야 합니다. **| 파일 myfailed.cfg** 명령을 사용하여 시작 실패 구성을 파

일에 저장합니다.운영자는 **컨피그레이션** 모드로 이동하여 **load/commit** 명령을 사용하여 이 실패한 컨피그레이션을 다시 적용해야 합니다.

```
RP/0/0/CPU0:router(config)#load myfailed.cfg
Loading.
197 bytes parsed in 1 sec (191)bytes/sec
RP/0/0/CPU0:router(config)#commit
```

R3.3 이미지 연산자는 다음 업데이트된 절차를 사용할 수 있습니다.운영자는 **show configuration failed startup** 명령 및 **load configuration failed startup** 명령을 사용하여 실패한 컨피그레이션을 찾아 다시 적용해야 합니다.

```
RP/0/0/CPU0:router#show configuration failed startup
!! CONFIGURATION FAILED DUE TO SYNTAX/AUTHORIZATION ERRORS
telnet vrf default ipv4
server max-servers 5 interface POS0/7/0/3 router static
address-family ipv4 unicast
 0.0.0.0/0 172.18.189.1

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
router bgp 217 !!%
Process did not respond to sysmgr !
RP/0/0/CPU0:router#

RP/0/0/CPU0:router(config)#load configuration failed startup noerror
Loading.
263 bytes parsed in 1 sec (259)bytes/sec
RP/0/0/CPU0:mike3(config-bgp)#show configuration
Building configuration...
telnet vrf default ipv4 server max-servers 5 router static
address-family ipv4 unicast
  0.0.0.0/0 172.18.189.1
 !
!
router bgp 217
!
end

RP/0/0/CPU0:router(config-bgp)#commit
```

커널 덤퍼

기본적으로 IOS-XR는 프로세스 충돌이 발생할 경우 하드 디스크에 코어 덤프를 쓰지만 커널 자체가 충돌하면 쓰이지 않습니다.다중 섀시 시스템의 경우 이 기능은 현재 라인 카드 섀시 0에서만 지원됩니다. 다른 섀시는 향후 소프트웨어 릴리스에서 지원됩니다.

RP 및 MSC에 대한 커널 덤프는 표준 및 관리 모드 컨피그레이션 모두에서 이러한 컨피그레이션을 사용하여 활성화하는 것이 좋습니다.

```
exception kernel memory kernel filepath harddisk:
exception dump-tftp-route port 0 host-address 10.0.2.1/16 destination 10.0.2.1 next-hop 10.0.2.1
tftp-srvr-addr 10.0.2.1
```

커널 덤프 컨피그레이션

이로 인해 커널 충돌이 발생합니다.

1. RP가 충돌하고 덤프는 디스크의 루트 디렉토리에 있는 해당 RP의 하드 디스크에 기록됩니다.

2. MSC가 충돌하면 덤프는 디스크의 루트 디렉토리에 있는 RP0의 하드 디스크에 기록됩니다. 이는 라우팅 프로토콜에 대해 NSF(Non-stop Forwarding)가 구성되어 있으므로 RP 장애 조치 시간에 영향을 주지 않습니다.crash RP 또는 라인 카드가 코어를 쓰는 동안 충돌 후 다시 사용할 수 있게 되기까지 몇 분 정도 더 걸릴 수 있습니다.

표준 및 관리 모드 컨피그레이션에 이 컨피그레이션을 추가하는 예는 여기에 나와 있습니다.관리 모드 컨피그레이션에서는 DRP를 사용해야 합니다.

이 출력은 커널 덤프 컨피그레이션 예를 보여줍니다.

```
RP/0/RP0/CPU0:crs1#configure
RP/0/RP0/CPU0:crs1(config)#exception kernel memory kernel filepat$
RP/0/RP0/CPU0:crs1(config)#exception dump-tftp-route port 0 host-$
RP/0/RP0/CPU0:crs1(config)#commit
RP/0/RP0/CPU0:crs1(config)#
RP/0/RP0/CPU0:crs1#admin
RP/0/RP0/CPU0:crs1(admin)#configure
Session                   Line        User      Date                      Lock
00000201-000bb0db-00000000  snmp        hfr-owne  Wed Apr  5 10:14:44 2006
RP/0/RP0/CPU0:crs1(admin-config)#exception kernel memory kernel f$
RP/0/RP0/CPU0:crs1(admin-config)#exception dump-tftp-route port 0$
RP/0/RP0/CPU0:crs1(admin-config)#commit
RP/0/RP0/CPU0:crs1(admin-config)#
RP/0/RP0/CPU0:crs1(admin)#
```

보안

LPTS

LPTS(Local Packet Transport Services)는 로컬로 전송되는 패킷을 처리합니다.LPTS는 다양한 구성 요소로 이루어져 있습니다.

1. 주요 프로세스를 포트 중재자 프로세스라고 합니다.BGP, IS-IS와 같이 서로 다른 프로토콜 프로세스에서 소켓 요청을 수신하고 해당 프로세스에 대한 모든 바인딩 정보를 추적합니다.예를 들어 BGP 프로세스가 소켓 번호 179에서 수신 대기하면 PA는 BGP 프로세스에서 해당 정보를 가져온 다음 IFIB에서 해당 프로세스에 바인딩을 할당합니다.
2. IFIB는 LPTS 프로세스의 또 다른 구성 요소입니다.특정 포트 바인딩을 수신하는 프로세스가 있는 디렉토리를 유지하는 데 도움이 됩니다.IFIB는 포트 중재자 프로세스에 의해 생성되며 포트 중재자와 함께 보관됩니다.그런 다음 이 정보의 여러 서브세트를 생성합니다.첫 번째 하위 집합은 IFIB의 한 조각입니다.이 슬라이스는 IPv4 프로토콜 등에 연결할 수 있습니다.그런 다음 적절한 플로우 관리자에게 슬라이스가 전송되며, 그런 다음 패킷을 적절한 프로세스로 전달하기 위해 IFIB 슬라이스를 사용합니다.두 번째 하위 집합은 IFIB 전이며, LC는 하나의 프로세스만 있거나 적절한 흐름 관리자에게 패킷을 전달할 수 있습니다.
3. 플로우 관리자는 조회(예: BGP에 대한 여러 프로세스)가 중요하지 않은 경우 패킷을 추가로 배포할 수 있습니다.각 플로우 관리자는 IFIB의 슬라이스 또는 여러 슬라이스를 가지고 있으며 IFIB의 슬라이스와 연관된 적절한 프로세스로 패킷을 적절하게 전달합니다.
4. 목적지 포트에 대해 항목이 정의되지 않은 경우 항목을 삭제하거나 흐름 관리자에게 전달할 수 있습니다.포트에 연결된 정책이 있는 경우 패킷이 연결된 포트 없이 전달됩니다.그런 다음 플로우 관리자가 새 세션 항목을 생성하는 데 도움이 됩니다.

내부 패킷은 어떻게 전달됩니까?

Layer 2(HDLC, PPP) 흐름과 Layer 4 ICMP/PING 흐름 및 라우팅 흐름의 두 가지 유형의 플로우가 있습니다.

1. Layer 2 HDLC/PPP - 이러한 패킷은 프로토콜 식별자로 식별되며 Sprlayer의 CPU 큐로 직접 전송됩니다.레이어 2 프로토콜 패킷은 높은 우선 순위를 얻은 다음 CPU(Squid를 통해)에서 선택하여 처리됩니다.따라서 레이어 2의 keepalive는 CPU를 통해 LC에 직접 응답합니다.따라서 응답을 위해 RP로 이동하지 않아도 되며 분산 인터페이스 관리의 테마를 사용하여 재생됩니다.
2. ICMP(Layer 4) 패킷은 LC에서 수신되며 IFBI를 통해 스프라이어의 CPU 대기열에 조회하여 전송됩니다.그런 다음 이러한 패킷은 CPU로 전송되고(Squid를 통해) 처리됩니다.그런 다음 패브릭을 통해 전달되도록 Sprlayer 이그레스 대기열을 통해 응답이 전송됩니다.이 경우 다른 애플리케이션에서 정보를 필요로 합니다(패브릭을 통해 복제). 패브릭을 통과하면 패킷은 적절한 이그레스 LC와 적절한 스폰지 및 제어 대기열을 통해 전달됩니다.
3. 라우팅 플로우는 IFIB에서 조회한 다음 출력 셰이핑 큐(8000개의 큐)로 전송되며, 그 중 하나는 제어 패킷용으로 예약됩니다.이것은 모양이 없는 대기열이며 가득 찰 때마다 서비스됩니다.- 높은 우선 순위그런 다음 패킷은 우선 순위가 높은 대기열의 패브릭을 통해 스펀지의 CPU 대기열 집합(스프라이어의 Squid 대기열과 유사)으로 전송된 다음 적절한 프로세스, 플로우 관리자 또는 실제 프로세스에 의해 처리됩니다.응답은 이그레스 라인 카드 스폰지를 통해 다시 전송된 다음 라인 카드를 내립니다.이그레스 LC 스폰지는 제어 패킷을 처리하기 위해 특수 대기열을 따로 둡니다.스폰지의 대기열은 이그레스 포트별로 높은 우선순위, 제어 및 낮은 우선순위 패킷으로 분할됩니다.
4. PSE에는 레이어 4, 레이어 2 및 라우팅 패킷의 속도 제한을 위해 구성된 폴리서 집합이 있습니다.이는 사전 설정되며 나중에 사용자가 구성할 수 있도록 변경됩니다.

LPTS의 가장 일반적인 문제 중 하나는 라우터에 ping을 시도할 때 삭제된 패킷입니다.LPTS 폴리서는 일반적으로 이러한 패킷을 제한하는 속도를 제공합니다.이 경우 다음을 확인합니다.

```
RP/0/RP0/CPU0:ss01-crs-1_P1#ping 192.168.3.14 size 8000 count 100
Type escape sequence to abort.
Sending 100, 8000-byte ICMP Echos to 192.168.3.14, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!
!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!
Success rate is 97 percent (97/100), round-trip min/avg/max = 1/2/5 ms
RP/0/RP0/CPU0:ss01-crs-1_P1#show lpts pifib hardware entry statistics location 0/5/CPU0 | excl
0/0

* - Vital; L4 - Layer4 Protocol; Intf - Interface;
DestAddr - Destination Fabric Address;
na - Not Applicable or Not Available

Local, Remote Address.Port          L4    Intf         DestAddr     Pkts/Drops
---------------------------------- ----- ------------ ------------ --- any
any   any          Punt       100/3
224.0.0.5 any                        any   PO0/5/1/0    0x3e         4/0
224.0.0.5 any                        any   PO0/5/1/1    0x3e         4/0
<further output elided>
```

IPsec

IP 패킷은 기본적으로 안전하지 않습니다.IPsec은 IP 패킷을 보호하는 데 사용되는 방법입니다.CRS-1 IPsec은 소프트웨어 전달 경로에 구현되므로 IPsec 세션이 RP/DRP에서 종료됩니다.CRS-1당 총 500개의 IPsec 세션이 지원됩니다.숫자는 CPU 속도 및 할당된 리소스에 따라 달라집니다.이에 대한 소프트웨어 제한은 없으며, RP의 로컬 소스 및 로컬에서 종료된 트래픽만 IPsec 처리에 적합합니다.IPsec 처리 시 오버헤드가 적기 때문에 IPsec 전송 모드 또는 터널 모드를 트래픽 유형

에 사용할 수 있습니다.

R3.3.0은 IPsec을 통한 BGP 및 OSPFv3의 암호화를 지원합니다.

IPsec 구현 방법에 대한 자세한 내용은 Cisco IOS XR System Security Configuration Guide를 참조하십시오.

참고: IPsec에는 crypto pie(예: hfr-k9sec-p.pie-3.3.1)이 필요합니다.

대역 외

콘솔 및 AUX 액세스

CRS-1 RP/SC에는 대역 외 관리를 위해 사용할 수 있는 콘솔 및 AUX 포트와 IP를 통한 대역 외(out-of-band) 관리를 위한 관리 이더넷 포트가 모두 있습니다.

각 RP/SCGE의 콘솔 및 AUX 포트(섀시당 2개)를 콘솔 서버에 연결할 수 있습니다.즉, 단일 섀시 시스템에는 4개의 콘솔 포트가 필요하고, 멀티 섀시 시스템에는 12개의 포트와 Catalyst 6504-E의 Supervisor Engine용 2개의 추가 포트가 필요합니다.

AUX 포트 연결은 IOS-XR 커널에 대한 액세스를 제공하고 콘솔 포트를 통해 이 작업을 수행할 수 없는 경우 시스템 복구를 허용할 수 있으므로 중요합니다.AUX 포트를 통한 액세스는 시스템에 로컬로 정의된 사용자에게만, 사용자가 루트 시스템 또는 cisco 지원 레벨 액세스 권한을 가지고 있는 경우에만 사용할 수 있습니다.또한 사용자에게 **암호**가 정의되어 있어야 합니다.

가상 터미널 액세스

텔넷 및 보안 셸(SSH)을 사용하여 vty 포트를 통해 CRS-1에 연결할 수 있습니다.기본적으로 둘 다 비활성화되어 있으며 사용자가 명시적으로 활성화해야 합니다.

참고: IPsec에는 crypto pie(예: hfr-k9sec-p.pie-3.3.1)이 필요합니다.

먼저 SSH를 활성화하기 위해 이 예와 같이 RSA 및 DSA 키를 생성합니다.

```
RP/0/RP1/CPU0:Crs-1#crypto key zeroize dsa
% Found no keys in configuration.
RP/0/RP1/CPU0:Crs-1#crypto key zeroize rsa
% Found no keys in configuration.

RP/0/RP1/CPU0:Crs-1#crypto key generate rsa general-keys
The name for the keys will be: the_default
  Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keypair.
  Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [1024]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]

RP/0/RP1/CPU0:Crs-1#crypto key generate dsa
The name for the keys will be: the_default
  Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024 bits. Choosing
```

```
a key modulus
How many bits in the modulus [1024]:
Generating DSA keys ...
Done w/ crypto generate keypair
[OK]

!--- VTY access via SSH & telnet can be configured as shown here. vty-pool default 0 4 ssh
server ! line default secret cisco users group root-system users group cisco-support exec-
timeout 30 0 transport input telnet ssh ! ! telnet ipv4 server
```

관련 정보

- 라우터 지원
- 기술 지원 및 문서 – Cisco Systems