Catalyst 6500/6000 스위치 높은 CPU 사용률

목차

소개

이 문서에서는 Cisco Catalyst 6500/6000 Series 스위치 및 VSS(Virtual Switching System) 1440 기반 시스템에서 CPU 사용률이 높은 원인을 설명합니다.Cisco 라우터와 마찬가지로 스위치는 **show processes cpu** 명령을 사용하여 스위치 수퍼바이저 엔진 프로세서의 CPU 사용률을 표시합니다.그러나 Cisco 라우터와 스위치 간의 아키텍처 및 포워딩 메커니즘의 차이 때문에 **show processes cpu** 명령의 일반적인 출력은 크게 다릅니다.출력의 의미도 다르다.이 문서에서는 이러한 차이점을 명확히 설명하고 스위치의 CPU 사용률 및 **show processes cpu** 명령 출력을 해석하는 방법에 대해 설명합니다.

참고: 이 문서에서 "switch" 및 "switches"는 Catalyst 6500/6000 스위치를 나타냅니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Catalyst 6500/6000 스위치 및 VSS(Virtual Switching System) 1440 기반 시스템의 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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.

참고: VSS(Virtual Switching System) 1440 기반 시스템에 지원되는 소프트웨어는 Cisco IOS® Software 릴리스 12.2(33)SXH1 이상입니다.

표기 규칙

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

CatOS와 Cisco IOS 시스템 소프트웨어의 차이점

Supervisor Engine의 Catalyst OS(CatOS) 및 MSFC(Multilayer Switch Feature Card)의 Cisco IOS® Software(하이브리드):CatOS 이미지를 시스템 소프트웨어로 사용하여 Catalyst 6500/6000 스위치에서 수퍼바이저 엔진을 실행할 수 있습니다.선택 사항인 MSFC가 설치된 경우 별도의 Cisco IOS 소프트웨어 이미지를 사용하여 MSFC를 실행합니다.

Supervisor Engine 및 MSFC 모두에서 Cisco IOS Software(기본):단일 Cisco IOS 소프트웨어 이미지를 시스템 소프트웨어로 사용하여 Catalyst 6500/6000 스위치에서 수퍼바이저 엔진과 MSFC를

모두 실행할 수 있습니다.

참고: 자세한 내용은 Cisco Catalyst 6500 Series 스위치에 대한 Cisco Catalyst 및 Cisco IOS 운영 체제 비교를 참조하십시오.

Catalyst 6500/6000 스위치의 CPU 사용률 이해

Cisco 소프트웨어 기반 라우터는 패킷을 처리하고 라우팅하기 위해 소프트웨어를 사용합니다 .Cisco 라우터의 CPU 사용률은 라우터가 더 많은 패킷 처리 및 라우팅을 수행함에 따라 증가하는 경향이 있습니다.따라서 **show processes cpu** 명령은 라우터의 트래픽 처리 로드를 상당히 정확하게 나타낼 수 있습니다.

Catalyst 6500/6000 스위치는 CPU를 동일한 방식으로 사용하지 않습니다.이러한 스위치는 소프트웨어가 아닌 하드웨어에서 포워딩 결정을 내립니다.따라서 스위치가 스위치를 통과하는 대부분의 프레임에 대해 포워딩 또는 스위칭 결정을 내릴 때 이 프로세스에는 수퍼바이저 엔진 CPU가 포함되지 않습니다.

Catalyst 6500/6000 스위치에는 2개의 CPU가 있습니다.하나의 CPU는 NMP(Network Management Processor) 또는 SP(Switch Processor)라고 하는 수퍼바이저 엔진 CPU입니다. 다른 CPU는 MSFC 또는 RP(Route Processor)라고 하는 레이어 3 라우팅 엔진 CPU입니다.

SP CPU는 다음과 같은 기능을 수행합니다.

- MAC 주소 학습 및 에이징 지원**참고:** MAC 주소 학습은 경로 설정이라고도 합니다.
- 네트워크 제어를 제공하는 프로토콜 및 프로세스 실행예를 들면 STP(Spanning Tree Protocol), CDP(Cisco Discovery Protocol), VTP(VLAN Trunk Protocol), DTP(Dynamic Trunking Protocol), PAgP(Port Aggregation Protocol) 등이 있습니다.
- 스위치의 CPU로 향하는 네트워크 관리 트래픽을 처리합니다.예를 들면 텔넷, HTTP 및 SNMP(Simple Network Management Protocol) 트래픽이 있습니다.

RP CPU는 다음 기능을 수행합니다.

- 레이어 3 라우팅 및 ARP(Address Resolution Protocol) 테이블 구축 및 업데이트
- CEF(Cisco Express Forwarding) FIB(Forwarding Information Base) 및 인접성 테이블을 생성하고 PFC(Policy Feature Card)로 테이블을 다운로드합니다.
- RP로 향하는 네트워크 관리 트래픽을 처리합니다.예를 들면 텔넷, HTTP 및 SNMP 트래픽이 있습니다.

소프트웨어로 이동하는 트래픽 트리거 상황 및 기능

스위치로 향하는 패킷

스위치로 향하는 모든 패킷은 소프트웨어로 이동합니다.이러한 패킷에는 다음이 포함됩니다.

- 패킷 제어제어 패킷은 STP, CDP, VTP, HSRP(Hot Standby Router Protocol), PAgP, LACP(Link Aggregation Control Protocol) 및 UDLD(UniDirectional Link Detection)에 대해 수신됩니다.
- 라우팅 프로토콜 업데이트이러한 프로토콜의 예로는 RIP(Routing Information Protocol), EIGRP(Enhanced Interior Gateway Routing Protocol), BGP(Border Gateway Protocol) 및

OSPF 프로토콜(Open Shortest Path First Protocol)이 있습니다.
- 스위치로 향하는 SNMP 트래픽
- 스위치에 대한 텔넷 및 SSH(Secure Shell Protocol) 트래픽SSH로 인한 높은 CPU 분리는 다음과 같습니다.

```
00:30:50.793 SGT Tue Mar 20 2012

CPU utilization for five seconds: 83%/11%; one minute: 15%; five minutes: 8%

 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process

   3        6468      8568        754 69.30%  7.90%  1.68%   1 SSH Process
```

  CPU가 높게 설정될 때 설정된 SSH 세션 수를 확인하기 위해 EEM 스크립트에 다음 명령을 포함합니다.사용자 표시라인 표시
- ARP 요청에 대한 ARP 응답

특수 처리가 필요한 패킷 및 조건

이 목록은 소프트웨어에서 패킷을 처리하도록 하는 특정 패킷 유형 및 조건을 제공합니다.

- IP 옵션, 만료된 TTL(Time to Live) 또는 비 ARPA(Advanced Research Projects Agency) 캡슐화가 포함된 패킷
- 터널링과 같은 특수 처리가 있는 패킷
- IP 단편화
- RP 또는 SP의 ICMP(Internet Control Message Protocol) 메시지가 필요한 패킷
- MTU(최대 전송 단위) 검사 실패
- IP 체크섬 및 길이 오류가 포함된 IP 오류가 있는 패킷
- 입력 패킷이 비트 오류(예: SBE)를 반환하면 소프트웨어 처리를 위해 패킷이 CPU로 전송되고 수정됩니다.시스템은 버퍼를 할당하고 CPU 리소스를 사용하여 이를 수정합니다.
- PBR 및 재귀 액세스 목록이 트래픽 흐름의 경로에 있으면 패킷이 소프트웨어 스위치로 전환되므로 추가 CPU 주기가 필요합니다.
- 인접성 동일 인터페이스
- RPF(Reverse Path Forwarding) 확인에 실패한 패킷 - **rpf-failure**
- 간략/수신Glean은 ARP 확인이 필요한 패킷을 나타내며, receive는 수신 케이스에 속하는 패킷을 참조합니다.
- Cisco IOS Software 및 CatOS의 Supervisor Engine 720에서 소프트웨어가 스위칭되는 IPX(Internetwork Packet Exchange) 트래픽IPX 트래픽은 Supervisor Engine 2/Cisco IOS Software에서도 소프트웨어 스위치로 설정되지만 Supervisor Engine 2/CatOS에서는 트래픽이 하드웨어 스위치로 전환됩니다.IPX 트래픽은 두 운영 체제 모두에 대해 Supervisor Engine 1A에서 하드웨어 스위칭됩니다.
- AppleTalk 트래픽
- 하드웨어 리소스 전체 조건이러한 리소스에는 FIB, CAM(Content-Addressable Memory) 및 TCAM(Ternary CAM)이 포함됩니다.

ACL 기반 기능

- ICMP 연결 불가 기능이 설정된 ACL(Access Control List) 거부 트래픽**참고:** 이것이 기본값입니다.IP 연결 불가 패킷이 활성화된 경우 일부 ACL 거부 패킷이 MSFC로 유출됩니다.ICMP 연결 불가 패킷이 필요한 패킷은 사용자 구성 가능한 속도로 유출됩니다.기본적으로 속도는 초당

500패킷(pps)입니다.

- 지원되지 않는 매개 변수(예: 소스 호스트)를 기반으로 IPX 필터링Supervisor Engine 720에서는 레이어 3 IPX 트래픽의 프로세스가 항상 소프트웨어에 있습니다.
- **log** 키워드를 사용하여 로깅이 필요한 ACE(Access Control Entries)이는 ACL 로그 및 VACL(VLAN ACL) 로그 기능에 적용됩니다.로깅이 필요하지 않은 동일한 ACL의 ACE는 하드웨어에서 여전히 처리됩니다.PFC3을 사용하는 Supervisor Engine 720은 ACL 및 VACL 로깅을 위해 MSFC로 리디렉션되는 패킷의 속도 제한을 지원합니다.Supervisor Engine 2는 VACL 로깅을 위해 MSFC로 리디렉션되는 패킷의 속도 제한을 지원합니다.Supervisor Engine 2의 ACL 로깅에 대한 지원은 Cisco IOS Software Release 12.2S 지사에 대해 예정되어 있습니다.
- 정책 라우팅 트래픽, **일치 길이**, **IP 우선순위 설정** 또는 기타 지원되지 않는 매개변수set **interface** 매개 변수는 소프트웨어에서 지원됩니다.그러나 **set interface null 0** 매개 변수는 예외입니다.이 트래픽은 PFC2를 사용하는 Supervisor Engine 2의 하드웨어에서 처리되고 PFC3을 사용하는 Supervisor Engine 720에서 처리됩니다.
- 비 IP 및 비 IPX 라우터 ACL(RACL)비 IP RACL은 모든 수퍼바이저 엔진에 적용됩니다.비 IPX RACL은 PFC가 있는 Supervisor Engine 1a 및 PFC2가 있는 Supervisor Engine 2에만 적용됩니다.
- RACL에서 거부된 브로드캐스트 트래픽
- 유니캐스트 RPF(uRPF) 확인, ACL ACE에서 거부된 트래픽이 RPF 검사는 PFC2가 있는 Supervisor Engine 2 및 PFC3이 있는 Supervisor Engine 720에 적용됩니다.
- 인증 프록시인증 프록시가 적용되는 트래픽은 Supervisor Engine 720에서 속도를 제한할 수 있습니다.
- Cisco IOS Software IP Security(IPsec)Supervisor Engine 720에서는 Cisco IOS 암호화의 대상이 되는 트래픽을 속도 제한 할 수 있습니다.

NetFlow 기반 기능

이 섹션에서 설명하는 NetFlow 기반 기능은 Supervisor Engine 2 및 Supervisor Engine 720에만 적용됩니다.

- NetFlow 기반 기능은 항상 소프트웨어 흐름의 첫 번째 패킷을 확인해야 합니다.플로우의 첫 번째 패킷이 소프트웨어에 도달하면 동일한 플로우의 후속 패킷은 하드웨어 스위치입니다.이 흐름 배열은 재귀 ACL, WCCP(Web Cache Communication Protocol) 및 Cisco IOS SLB(Server Load Balancing)에 적용됩니다.**참고:** Supervisor Engine 1에서 재귀 ACL은 동적 TCAM 항목을 사용하여 특정 플로우에 대한 하드웨어 바로가기를 생성합니다.원칙은 똑같다.플로우의 첫 번째 패킷은 소프트웨어로 이동합니다.해당 플로우의 후속 패킷은 하드웨어 스위치입니다.
- TCP 가로채기 기능을 사용하면 3방향 핸드셰이크 및 세션 종료가 소프트웨어에서 처리됩니다.나머지 트래픽은 하드웨어에서 처리됩니다.**참고:** 동기화(SYN), SYN 승인(SYN ACK) 및 ACK 패킷은 3방향 핸드셰이크를 구성합니다.세션 종료는 마침(FIN) 또는 재설정(RST)과 함께 발생합니다.
- NAT(Network Address Translation)를 사용하면 트래픽이 다음과 같이 처리됩니다.Supervisor Engine 720에서 다음을 수행합니다.NAT가 필요한 트래픽은 초기 변환 후 하드웨어에서 처리됩니다.플로우의 첫 번째 패킷의 변환은 소프트웨어에서 발생하며, 그 플로우의 후속 패킷은 하드웨어 스위치드(hardware-switched)입니다.TCP 패킷의 경우 TCP 3방향 핸드셰이크가 완료된 후 NetFlow 테이블에서 하드웨어 바로가기가 생성됩니다.Supervisor Engine 2 및 Supervisor Engine 1에서 다음을 수행합니다.NAT가 필요한 모든 트래픽은 소프트웨어 스위치입니다.
- CBAC(Context-based Access Control)는 NetFlow 바로 가기를 사용하여 검사가 필요한 트래픽을 분류합니다.그런 다음 CBAC는 이 트래픽만 소프트웨어로 전송합니다.CBAC는 소프트웨어

전용 기능입니다.검사를 받는 트래픽은 하드웨어 스위칭이 아닙니다.**참고:** Supervisor Engine 720에서는 검사 대상인 트래픽의 속도를 제한할 수 있습니다.

멀티캐스트 트래픽

- PIM(Protocol Independent Multicast) 스누핑
- IGMP(Internet Group Management Protocol) 스누핑(TTL = 1)이 트래픽은 실제로 라우터로 전송됩니다.
- MLD(Multicast Listener Discovery) 스누핑(TTL = 1)이 트래픽은 실제로 라우터로 전송됩니다.
- FIB 누락
- 멀티캐스트 소스에 직접 연결된 등록을 위한 멀티캐스트 패킷이러한 멀티캐스트 패킷은 랑데부 지점으로 터널링됩니다.
- IP 버전 6(IPv6) 멀티캐스트

기타 기능

- 네트워크 기반 애플리케이션 인식(NBAR)
- ARP 검사(CatOS만 해당)
- 포트 보안, CatOS 전용
- DHCP 스누핑

IPv6 상황

- hop-by-hop 옵션 헤더가 있는 패킷
- 라우터와 동일한 목적지 IPv6 주소를 가진 패킷
- 범위 적용 검사에 실패한 패킷
- 출력 링크의 MTU를 초과하는 패킷
- TTL이 1보다 작거나 같은 패킷
- 출력 VLAN과 동일한 입력 VLAN이 있는 패킷
- IPv6 uRPF소프트웨어는 모든 패킷에 대해 이 uRPF를 수행합니다.
- IPv6 재귀 ACL소프트웨어에서 이러한 재귀 ACL을 처리합니다.
- IPv6 사이트 내 자동 터널 주소 지정 프로토콜(ISATAP) 터널의 6to4 접두사소프트웨어에서 이 터널링을 처리합니다.ISATAP 터널로 들어가는 다른 모든 트래픽은 하드웨어 스위치입니다.

LCP Schedular 및 DFC 모듈

DFC(Distributed Forwarding Card)에서 높은 CPU에서 실행되는 `lcp` 프로세스는 문제가 아니며 작업에 아무런 문제가 되지 않습니다.LCP 스케줄러는 펌웨어 코드의 일부입니다.DFC가 필요하지 않은 모든 모듈에서 펌웨어는 LCP(Line Card Processor)라는 특정 프로세서에서 실행됩니다. 이 프로세서는 ASIC 하드웨어를 프로그래밍하고 중앙 수퍼바이저 모듈과 통신하는 데 사용됩니다.

lcp 이 시작되면 모든 프로세스 시간을 사용할 수 있습니다.그러나 새 프로세스에 프로세서 시간이 필요할 경우 lcp `schedular`를 사용하면 새 프로세스에 대한 프로세스 시간이 늘어납니다.이 높은 CPU 사용률과 관련하여 시스템의 성능에 영향을 미치지 않습니다.우선 순위가 더 높은 프로세스에서 필요로 하지 않는 한 이 프로세스는 사용되지 않는 모든 CPU 사이클을 간단히 사용합니다.

```
DFC#show process cpu
```

```
PID  Runtime(ms)   Invoked  uSecs    5Sec   1Min   5Min TTY Process
  22           0         1      0   0.00%  0.00%  0.00%   0 SCP ChilisLC Lis
  23           0         1      0   0.00%  0.00%  0.00%   0 IPC RTTYC Messag
  24           0         9      0   0.00%  0.00%  0.00%   0 ICC Slave LC Req
  25           0         1      0   0.00%  0.00%  0.00%   0 ICC Async mcast
  26           0         2      0   0.00%  0.00%  0.00%   0 RPC Sync
  27           0         1      0   0.00%  0.00%  0.00%   0 RPC rpc-master
  28           0         1      0   0.00%  0.00%  0.00%   0 Net Input
  29           0         2      0   0.00%  0.00%  0.00%   0 Protocol Filteri
  30           8       105     76   0.00%  0.00%  0.00%   0 Remote Console P
  31          40      1530     26   0.00%  0.00%  0.00%   0 L2 Control Task
  32          72       986     73   0.00%  0.02%  0.00%   0 L2 Aging Task
  33           4        21    190   0.00%  0.00%  0.00%   0 L3 Control Task
  34          12       652     18   0.00%  0.00%  0.00%   0 FIB Control Task
  35        9148       165  55442   1.22%  1.22%  1.15%   0 Statistics Task
  36           4       413      9   0.00%  0.00%  0.00%   0 PFIB Table Manag
  37      655016  64690036     10  75.33% 77.87% 71.10%   0 lcp schedular
  38           0       762      0   0.00%  0.00%  0.00%   0 Constellation SP
```

CPU 사용률 문제 해결을 위한 일반적인 원인 및 솔루션

IP 연결 불가

액세스 그룹이 패킷을 거부하면 MSFC는 ICMP 도달 불가 메시지를 전송합니다.이 작업은 기본적으로 발생합니다.

ip unreachables 명령의 기본 **활성화**를 통해 수퍼바이저 엔진은 하드웨어에서 거부된 대부분의 패킷을 삭제합니다.그런 다음 수퍼바이저 엔진은 드롭을 위해 MSFC에 적은 수의 패킷(최대 10pps)만 전송합니다.이 작업은 ICMP-unreachable 메시지를 생성합니다.

거부된 패킷의 삭제 및 ICMP-unreachable 메시지의 생성은 MSFC CPU에 로드를 부여합니다.로드를 제거하기 위해 no ip unreachables interface **configuration** 명령**을** 실행할 수 있습니다.이 명령은 ICMP-unreachable 메시지를 비활성화합니다. 그러면 가 모든 액세스 그룹 거부 패킷의 하드웨어를 드롭할 수 있습니다.

VACL에서 패킷을 거부하면 ICMP-unreachable 메시지가 전송되지 않습니다.

NAT 변환

NAT는 하드웨어 및 소프트웨어 전달을 모두 사용합니다.NAT 변환의 초기 설정은 소프트웨어에서 수행되어야 하며 추가 포워딩은 하드웨어에서 수행됩니다.NAT는 Netflow 테이블도 사용합니다(최대 128KB). 따라서 Netflow 테이블이 가득 차면 스위치도 소프트웨어를 통해 NAT 전달을 적용하기 시작합니다.이는 일반적으로 트래픽 버스트가 높으면 발생하며 CPU 6500이 증가합니다.

플로우 캐시 테이블에서 CEF FIB 테이블 공간 사용

Supervisor Engine 1에는 128,000개의 항목을 지원하는 플로우 캐시 테이블이 있습니다.그러나 해싱 알고리즘의 효율성을 기준으로 이러한 항목의 범위는 32,000에서 120,000입니다. Supervisor Engine 2에서 FIB 테이블이 생성되어 PFC에 프로그래밍됩니다.테이블에는 최대 256,000개의 항목이 있습니다.PFC3-BXL이 포함된 Supervisor Engine 720은 최대 1,000,000개의 항목을 지원합니다.이 공간을 초과하면 소프트웨어에서 패킷이 전환됩니다.이로 인해 RP의 CPU 사용률이 높을 수 있습니다.CEF FIB 테이블의 경로 수를 확인하려면 다음 명령을 사용합니다.

```
Router#show processes cpu
```

```
CPU utilization for five seconds:  99.26%
                     one minute: 100.00%
                    five minutes: 100.00%

PID Runtime(ms) Invoked    uSecs    5Sec    1Min    5Min    TTY Process
--- ----------- ---------- -------- ------- ------- ------- --- ---------------
1   0           0          0          0.74%   0.00%   0.00% -2  Kernel and Idle
2   2           245        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat
3   0           1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr
4   0           1          0          0.00%   0.00%   0.00% -2  L2L3PatchRev
5   653         11737      1000       0.00%   0.00%   0.00% -2  SynDi
!--- Output is suppressed. 26 10576 615970 1000 0.00% 0.00% 0.00% 0 L3Aging 27 47432 51696 8000
0.02% 0.00% 0.00% 0 NetFlow 28 6758259 1060831 501000 96.62% 96.00% 96.00% 0   Fib
29  0           1          0          0.00%   0.00%   0.00% -2  Fib_bg_task
!--- Output is suppressed. CATOS% show mls cef
Total L3 packets switched:           124893998234
Total L3 octets switched:          53019378962495
Total route entries:                       112579
  IP route entries:                        112578
  IPX route entries:                            1
  IPM route entries:                            0
IP load sharing entries:                      295
IPX load sharing entries:                       0
Forwarding entries:                        112521
Bridge entries:                                56
Drop entries:                                   2


IOS% show ip cef summary
IP Distributed CEF with switching (Table Version 86771423), flags=0x0
  112564 routes, 1 reresolve, 0 unresolved (0 old, 0 new)
  112567 leaves, 6888 nodes, 21156688 bytes, 86771426
inserts, 86658859
invalidations
  295 load sharing elements, 96760 bytes, 112359 references
  universal per-destination load sharing algorithm, id 8ADDA64A
  2 CEF resets, 2306608 revisions of existing leaves
  refcounts:  1981829 leaf, 1763584 node
!--- You see these messages if the TCAM space is exceeded: %MLSCEF-SP-7-FIB_EXCEPTION: FIB TCAM
exception, Some entries will be software switched %MLSCEF-SP-7-END_FIB_EXCEPTION: FIB TCAM
exception cleared, all CEF entries will be hardware switched
```

Supervisor Engine 2에서 인터페이스에 RPF 검사를 구성한 경우 FIB 항목 수가 절반으로 감소합니다.이 컨피그레이션은 더 많은 패킷을 소프트웨어 스위치로 전환하여 결과적으로 CPU 사용률이 높아질 수 있습니다.

높은 CPU 사용률 문제를 해결하려면 경로 요약을 활성화합니다.라우트 요약은 프로세서 워크로드, 메모리 요구 사항 및 대역폭 수요를 줄여 복잡한 네트워크의 레이턴시를 최소화할 수 있습니다.

TCAM 사용률 및 최적화에 대한 자세한 내용은 Catalyst 6500 Series 스위치의 ACL 이해를 참조하십시오.

최적화된 ACL 로깅

최적화된 ACL 로깅(OAL)은 ACL 로깅을 위한 하드웨어 지원을 제공합니다.OAL을 구성하지 않는 한 로깅이 필요한 패킷 프로세스는 MSFC3의 소프트웨어에서 완전히 수행됩니다. OAL은 PFC3의 하드웨어에서 패킷을 허용하거나 삭제합니다. OAL은 로깅 메시지를 생성하기 위해 최적화된 루틴을 사용하여 MSFC3에 정보를 전송합니다.

참고: OAL에 대한 자세한 내용은 Understanding Cisco IOS ACL Support(Cisco IOS ACL 지원 이해

)의 PFC3을 *통한 최적화된 ACL 로깅* 섹션을 참조하십시오.

CPU에 대한 패킷 속도 제한

Supervisor Engine 720에서 속도 리미터는 패킷이 소프트웨어로 이동할 수 있는 속도를 제어할 수 있습니다.이 속도 제어는 서비스 거부 공격을 방지하는 데 도움이 됩니다.Supervisor Engine 2에서 다음 속도 제한 중 일부를 사용할 수도 있습니다.

```
Router#show mls rate-limit
   Rate Limiter Type       Status      Packets/s   Burst
---------------------   ----------   ---------   -----
         MCAST NON RPF   Off                  -       -
        MCAST DFLT ADJ   On              100000     100
      MCAST DIRECT CON   Off                  -       -
        ACL BRIDGED IN   Off                  -       -
       ACL BRIDGED OUT   Off                  -       -
           IP FEATURES   Off                  -       -
          ACL VACL LOG   On                2000       1
           CEF RECEIVE   Off                  -       -
             CEF GLEAN   Off                  -       -
      MCAST PARTIAL SC   On              100000     100
        IP RPF FAILURE   On                 500      10
           TTL FAILURE   Off                  -       -
ICMP UNREAC. NO-ROUTE   On                 500      10
ICMP UNREAC. ACL-DROP   On                 500      10
         ICMP REDIRECT   Off                  -       -
           MTU FAILURE   Off                  -       -
           LAYER_2 PDU   Off                  -       -
            LAYER_2 PT   Off                  -       -
             IP ERRORS   On                 500      10
           CAPTURE PKT   Off                  -       -
            MCAST IGMP   Off                  -       -

Router(config)#mls rate-limit ?
  all        Rate Limiting for both Unicast and Multicast packets
  layer2     layer2 protocol cases
  multicast  Rate limiting for Multicast packets
  unicast    Rate limiting for Unicast packets
```

예를 들면 다음과 같습니다.

```
Router(config)#mls rate-limit layer2 l2pt 3000
```

모든 CEF 펀딩된 패킷을 MSFC로 속도-제한하려면 다음 예에 있는 명령을 실행합니다.

```
Router(config)#mls ip cef rate-limit 50000
```

TTL=1로 인해 CPU에 펀딩된 패킷 수를 줄이려면 다음 명령을 실행합니다.

```
Router(config)#mls rate-limit all ttl-failure 15
!--- where 15 is the number of packets per second with TTL=1. !--- The valid range is from 10 to
1000000 pps.
```

예를 들어, IPv4 TTL이 1인 것을 보여주는 netdr 캡처의 출력입니다.

```
Source mac     00.00.50.02.10.01  3644
Dest mac       AC.A0.16.0A.B0.C0  4092
Protocol       0800               4094
Interface      Gi1/8              3644
Source vlan    0x3FD(1021)        3644
Source index   0x7(7)             3644
Dest index     0x380(896)         3654

L3

ipv4 source    211.204.66.117      762
ipv4 dest      223.175.252.49     3815
ipv4 ttl                  1     3656
ipv6 source               -        0
ipv6 dest                 -        0
ipv6 hoplt                -        0
ipv6 flow                 -        0
ipv6 nexthdr              -        0
```

또한 CPU에 유출되는 TTL=1의 패킷 때문에 CPU가 높을 수 있습니다.CPU로 유출되는 패킷 수를 제한하려면 하드웨어 속도 제한을 구성합니다.속도 리미터는 하드웨어 데이터 경로에서 소프트웨어 데이터 경로로 유출되는 패킷을 속도 제한(rate-limiters)할 수 있습니다.속도 리미터는 구성된 속도를 초과하는 트래픽을 삭제하여 소프트웨어 제어 경로를 혼잡으로부터 보호합니다.속도 제한은 **mls rate-limit all ttl-failure** 명령을 사용하여 구성됩니다.

잘못된 케이블로 인한 VLAN의 물리적 통합

또한 CPU 사용률이 높으면 케이블 연결이 잘못되어 둘 이상의 VLAN을 결합할 수 있습니다.또한 VLAN 통합이 발생하는 포트에서 STP가 비활성화된 경우 높은 CPU 사용률이 발생할 수 있습니다.

이 문제를 해결하려면 케이블 연결 오류를 확인하고 수정하십시오.요구 사항에 따라 허용되는 경우 해당 포트에서 STP를 활성화할 수도 있습니다.

브로드캐스트 스톰

LAN 브로드캐스트 스톰은 브로드캐스트 또는 멀티캐스트 패킷이 LAN을 플러딩할 때 발생하며, 이로 인해 과도한 트래픽이 발생하고 네트워크 성능이 저하됩니다.프로토콜 스택 구현 또는 네트워크 컨피그레이션에서 오류가 발생하면 브로드캐스트 스톰이 발생할 수 있습니다.

Catalyst 6500 시리즈 플랫폼의 아키텍처 설계로 인해 브로드캐스트 패킷은 소프트웨어 레벨에서만 삭제되고 항상 삭제됩니다.

브로드캐스트 억제는 브로드캐스트 스톰에 의한 LAN 인터페이스 중단을 방지합니다.브로드캐스트 억제는 1초 동안 LAN에서 브로드캐스트 활동을 측정하는 필터링을 사용하며, 미리 정의된 임계값과 측정을 비교합니다.임계값에 도달하면 지정된 기간 동안 추가 브로드캐스트 활동이 억제됩니다.브로드캐스트 억제는 기본적으로 비활성화되어 있습니다.

참고: 브로드캐스트 스톰으로 인해 VRRP가 백업에서 마스터로 플래핑되면 CPU 사용률이 높을 수 있습니다.

브로드캐스트 억제의 작동 방식을 이해하고 기능을 활성화하려면 다음을 참조하십시오.

- 브로드캐스트 억제 구성(Cisco IOS 시스템 소프트웨어)
- 브로드캐스트 억제 구성(CatOS 시스템 소프트웨어)

BGP Next-Hop 주소 추적(BGP 스캐너 프로세스)

BGP 스캐너 프로세스는 BGP 테이블을 표시하고 다음 홉의 연결성을 확인합니다.이 프로세스에서는 또한 BGP가 조건 접두사를 광고할지 또는 경로 댐프닝을 수행해야 할지를 결정하기 위해 조건부 광고를 확인합니다.기본적으로 프로세스는 60초마다 스캔합니다.

대규모 인터넷 라우팅 테이블을 전달하는 라우터의 BGP 스캐너 프로세스 때문에 짧은 기간 동안 CPU 사용률이 높을 것으로 예상할 수 있습니다.분당 한 번, BGP 스캐너는 BGP RIB(Routing Information Base) 테이블을 표시하고 중요한 유지 관리 작업을 수행합니다.이러한 작업은 다음과 같습니다.

- 라우터 BGP 테이블에서 참조되는 다음 홉의 확인
- next-hop 장치에 연결할 수 있는지 확인

따라서 큰 BGP 테이블은 산책하고 검증하는 데 상당한 시간이 소요됩니다.BGP 스캐너 프로세스는 데이터 구조를 업데이트하고 경로 재배포를 위해 라우팅 테이블을 표시하기 위해 BGP 테이블을 확인합니다.두 테이블 모두 라우터 메모리에 개별적으로 저장됩니다.두 테이블 모두 매우 클 수 있으므로 CPU 사이클을 사용합니다.

BGP 스캐너 프로세스의 CPU 사용률에 대한 자세한 내용은 BGP 스캐너 또는 BGP Router Process로 인해 발생한 Troubleshooting High CPU*(문제 해결의 BGP 스캐너* 때문에 CPU High CPU) 섹션을 참조하십시오.

BGP Next-Hop Address Tracking 기능 및 스캔 간격을 활성화/비활성화하거나 조정하는 절차에 대한 자세한 내용은 BGP Support for Next-Hop Address Tracking을 참조하십시오.

비 RPF 멀티캐스트 트래픽

멀티캐스트 라우팅(유니캐스트 라우팅과 달리)은 지정된 멀티캐스트 데이터 스트림의 소스에만 적용됩니다.즉, 멀티캐스트 트래픽을 시작하는 디바이스의 IP 주소입니다.기본 원칙은 소스 디바이스가 정의되지 않은 수의 수신인(해당 멀티캐스트 그룹 내)에 스트림을 "푸시"한다는 것입니다. 모든 멀티캐스트 라우터는 모든 수신자에게 트래픽을 전달하기 위해 멀티캐스트 트래픽이 네트워크를 통과하는 경로를 제어하는 배포 트리를 생성합니다.멀티캐스트 분산 트리의 두 가지 기본 유형은 소스 트리 및 공유 트리입니다.RPF는 멀티캐스트 전달의 핵심 개념입니다.라우터가 멀티캐스트 트래픽을 배포 트리에서 올바르게 전달할 수 있습니다.RPF는 기존 유니캐스트 라우팅 테이블을 사용하여 업스트림 및 다운스트림 인접 디바이스를 결정합니다.라우터는 업스트림 인터페이스에서 수신되는 경우에만 멀티캐스트 패킷을 전달합니다.이 RPF 확인은 배포 트리가 루프 프리(loop-free)임을 보장하는 데 도움이 됩니다.

IEEE 802.3 CSMA/CD 사양에 따라 멀티캐스트 트래픽은 항상 브리지(레이어 2) LAN의 모든 라우터에서 볼 수 있습니다.802.3 표준에서 첫 번째 8진수의 비트 0은 브로드캐스트 및/또는 멀티캐스트 프레임을 나타내는 데 사용되며, 이 주소가 있는 모든 레이어 2 프레임은 플러딩됩니다.CGMP 또는 IGMP 스누핑이 구성된 경우에도 마찬가지입니다.이는 멀티캐스트 라우터가 멀티캐스트 트래픽을 확인해야 하기 때문에 적절한 포워딩 결정을 내릴 것으로 예상되기 때문입니다.여러 멀티캐스트 라우터가 각각 공통 LAN에 인터페이스를 가지고 있는 경우 하나의 라우터만 데이터를 전달합니다(선택 프로세스에서 선택). LAN의 플러딩 특성 때문에 이중화 라우터(멀티캐스트 트래픽을 전달하지 않는 라우터)는 해당 LAN의 아웃바운드 인터페이스에서 이 데이터를 수신합니다.이중화 라우터는 일반적으로 이 트래픽을 삭제합니다. 잘못된 인터페이스에 도달하여 RPF 확인에 실패하기 때문입니다.RPF 검사에 실패한 이 트래픽을 비 RPF 트래픽 또는 RPF 실패 패킷이라고 합니다. 이는 소스의 플로우에 대해 역방향으로 전송되었기 때문입니다.

MSFC가 설치된 Catalyst 6500은 본격적인 멀티캐스트 라우터로 작동하도록 구성할 수 있습니다.MMLS(Multicast Multi-Layer Switching)를 사용하면 일반적으로 스위치 내의 하드웨어에서 RPF 트

래픽을 전달합니다.ASIC에는 멀티캐스트 라우팅 상태(예: (*,G) 및 (S,G))에서 정보가 제공되므로 하드웨어 바로가기를 Netflow 및/또는 FIB 테이블에 프로그래밍할 수 있습니다.이 비 RPF 트래픽은 경우에 따라 여전히 필요하며 PIM 어설션 메커니즘의 MSFC CPU(프로세스 레벨)에 필요합니다.그렇지 않으면 소프트웨어 고속 스위칭 경로에 의해 삭제됩니다(RPF 인터페이스에서 소프트웨어 빠른 스위칭이 비활성화되지 않은 것으로 가정).

이중화를 사용하는 Catalyst 6500은 특정 토폴로지에서 비 RPF 트래픽을 효율적으로 처리하지 못할 수 있습니다.비 RPF 트래픽의 경우 일반적으로 중복 라우터에 (*,G) 또는 (S,G) 상태가 없으므로 패킷을 삭제하기 위해 하드웨어 또는 소프트웨어 바로 가기를 생성할 수 없습니다.각 멀티캐스트 패킷은 MSFC 경로 프로세서에서 개별적으로 검사해야 하며, 이를 CPU 인터럽트 트래픽이라고 합니다.동일한 라우터 세트를 연결하는 레이어 3 하드웨어 스위칭과 여러 인터페이스/VLAN을 통해 이중화 MSFC의 CPU에 도달하는 비 RPF 트래픽은 원래 소스 속도의 "N"으로 증폭됩니다(여기서 "N"은 라우터가 이중으로 연결된 LAN 수입니다). 비 RPF 트래픽의 속도가 시스템의 패킷 삭제 용량을 초과하면 CPU 사용률, 버퍼 오버플로우, 전체 네트워크 불안정을 야기할 수 있습니다.

Catalyst 6500에는 필터링을 유선 속도로 수행할 수 있는 액세스 목록 엔진이 있습니다.이 기능은 특정 상황에서 스파스 모드 그룹에 대해 비 RPF 트래픽을 효율적으로 처리하는 데 사용할 수 있습니다.sparse-mode 'stub networks' 내에서만 ACL 기반 메서드를 사용할 수 있습니다. 이 모드에서는 다운스트림 멀티캐스트 라우터(및 해당 수신기)가 없습니다. 또한 Catalyst 6500의 패킷 포워딩 설계로 인해 내부적으로 이중화된 MSFC는 이 구현을 사용할 수 없습니다.이는 Cisco 버그 ID CSCdr74908(등록된 고객만 해당) 내에서 설명합니다. 고밀도 모드 그룹의 경우 PIM 어설션 메커니즘이 제대로 작동하려면 라우터에서 비 RPF 패킷을 확인해야 합니다.CEF 또는 Netflow 기반 속도 제한 및 QoS와 같은 다양한 솔루션을 사용하여 덴스 모드 네트워크와 스파스 모드 트랜짓 네트워크에서 RPF 장애를 제어합니다.

Catalyst 6500에는 필터링을 유선 속도로 수행할 수 있는 액세스 목록 엔진이 있습니다.이 기능을 사용하여 스파스 모드 그룹에 대해 비 RPF 트래픽을 효율적으로 처리할 수 있습니다.이 솔루션을 구현하려면 'stub network'의 수신 인터페이스에 액세스 목록을 배치하여 'stub network'에서 시작되지 않은 멀티캐스트 트래픽을 필터링합니다. 액세스 목록이 스위치의 하드웨어로 푸시됩니다.이 액세스 목록은 CPU가 패킷을 볼 수 없게 하며 하드웨어가 비 RPF 트래픽을 삭제할 수 있도록 합니다.

참고: 이 액세스 목록을 전송 인터페이스에 배치하지 마십시오.stub 네트워크에만 사용됩니다(호스트만 있는 네트워크).

자세한 내용은 다음 문서를 참조하십시오.

- Stub 네트워크에서 IP 멀티캐스트를 통한 이중화 라우터 문제
- 비 RPF 트래픽 처리

show 명령

show 명령을 실행할 때의 CPU 사용률은 항상 거의 100%입니다.**show** 명령을 실행할 때 CPU 사용률이 높은 것은 정상이며 일반적으로 몇 초 동안만 유지됩니다.

예를 들어, **show tech-support** 명령을 실행하면 Virtual Exec 프로세스가 높아지는 것은 정상적인 현상입니다. 이 출력은 인터럽트 중심 출력이기 때문입니다.**show** 명령이 아닌 다른 프로세스에서 CPU가 높은 유일한 문제입니다.

show cef not-cef-switched 명령**은** 패킷이 MSFC에 펀딩되는 이유(receive, ip 옵션, 인접성 없음 등) 및 몇 개인지 보여줍니다.예:

```
Switch#show cef not-cef-switched
CEF Packets passed on to next switching layer
Slot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     Frag
RP      6222       0         136        0    60122        0        0        0
5          0       0           0        0        0        0        0        0
IPv6 CEF Packets passed on to next switching layer
Slot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTU
RP         0       0           0        0        0        0        0        0
```

show ibc 및 **show ibc brief** 명령은 CPU 대기열을 표시하며 CPU 상태를 모니터링할 때 사용할 수 있습니다.

실행 프로세스

Cisco IOS Software의 Exec 프로세스는 라우터의 TTY 회선(콘솔, 보조, 비동기)에서 통신을 담당합니다.Virtual Exec 프로세스는 VTY 회선(텔넷 세션)을 담당합니다. Exec 및 Virtual Exec 프로세스는 중간 우선 순위 프로세스이므로 우선 순위가 높은 다른 프로세스(높음 또는 중요)가 있을 경우 우선 순위가 높은 프로세스가 CPU 리소스를 가져옵니다.

이러한 세션을 통해 전송되는 데이터가 많으면 EXEC 프로세스에 대한 CPU 사용률이 증가합니다.이는 라우터가 이러한 회선을 통해 단순 문자를 전송하려는 경우 라우터가 일부 CPU 리소스를 사용하기 때문입니다.

- 콘솔(Exec)의 경우 라우터는 문자당 하나의 인터럽트를 사용합니다.
- VTY 회선(Virtual Exec)의 경우 텔넷 세션은 문자당 하나의 TCP 패킷을 구축해야 합니다.

이 목록은 EXEC 프로세스에서 CPU 사용률이 높은 몇 가지 가능한 이유를 자세히 설명합니다.

- **콘솔 포트를 통해 전송된 데이터가 너무 많습니다.**show debugging **명령**을 사용하여 라우터에서 디버그가 시작되었는지 **확인합니다**.logging console 명령의 **no** 형식으로 라우터에서 콘솔 로깅을 **비활성화합니다.**긴 출력이 콘솔에 인쇄되는지 확인합니다.예를 들어, **show tech-support** 또**는 show memory 명령**이 있습니다.
- **exec 명령은 비동기 및 보조 회선에 대해 구성됩니다.**회선에 발신 트래픽만 있는 경우 이 회선에 대해 Exec 프로세스를 비활성화합니다.이 라인에 연결된 디바이스(예: 모뎀)가 일부 요청되지 않은 데이터를 전송하는 경우 이 행에서 실행 프로세스가 시작됩니다.라우터가 터미널 서버로 사용되는 경우(다른 장치 콘솔에 대한 역방향 텔넷의 경우) 다른 장치의 콘솔에 연결된 행에서 **no exec** 명령을 구성하는 것이 좋습니다.콘솔에서 다시 들어오는 데이터는 CPU 리소스를 사용하는 Exec 프로세스를 시작할 수 있습니다.

Virtual Exec 프로세스에서 CPU 사용률이 높은 이유는 다음과 같습니다.

- **텔넷 세션을 통해 전송된 데이터가 너무 많습니다.**Virtual Exec 프로세스에서 CPU 사용률이 높은 가장 일반적인 이유는 너무 많은 데이터가 라우터에서 텔넷 세션으로 전송되기 때문입니다.이는 **show tech-support**, **show memory** 등과 같은 긴 출력이 있는 명령이 텔넷 세션에서 실행될 때 발생할 수 있습니다.각 VTY 세션을 통해 전송되는 데이터의 양은 **show tcp vty *<line number>* 명령**으로 확인할 수 있습니다.

L3 에이징 프로세스

L3 에이징 프로세스에서 NDE(NetFlow Data Export)를 사용하여 많은 *ifindexus* 값을 내보내면 CPU 사용량이 100%에 달할 수 있습니다.

이 문제가 발생하면 다음 두 명령이 활성화되었는지 확인합니다.

```
set mls nde destination-ifindex enable

set mls nde source-ifindex enable
```
이러한 명령을 활성화한 경우 NDE를 사용하여 모든 대상 및 소스 인덱스 값을 내보내야 합니다.L3 에이징 프로세스 사용률은 높은 수준입니다. 모든 대상 및 소스 *ifindex* 값에 대해 FIB 조회를 수행해야 하기 때문입니다.이 때문에 테이블이 가득 차고 L3 에이징 프로세스가 높고 CPU 사용량이 100% 증가합니다.

이 문제를 해결하려면 다음 명령을 비활성화합니다.

```
set mls nde destination-ifindex disable

set mls nde source-ifindex disable
```
다음 명령을 사용하여 값을 확인합니다.

- mls cef 요약 표시
- show mls cef maximum routes

BPDU 스톰

스패닝 트리는 이중화 스위치 및 브리지 네트워크에서 루프 프리 레이어 2 환경을 유지합니다 .STP가 없으면 프레임 루프 및/또는 무한대로 곱합니다.트래픽이 높으면 브로드캐스트 도메인의 모든 디바이스가 중단되므로 네트워크 용해가 발생합니다.

어떤 면에서 STP는 처음에는 느린 소프트웨어 기반 브리지 사양(IEEE 802.1D)을 위해 개발된 초기 프로토콜이지만, STP는 이러한 기능을 갖춘 대규모 스위치드 네트워크에서 성공적으로 구현하기 위해 복잡할 수 있습니다.

- 많은 VLAN
- STP 도메인의 많은 스위치
- 멀티벤더 지원
- 새로운 IEEE 개선 사항

네트워크가 스패닝 트리 계산을 자주 하거나 스위치가 더 많은 BPDU를 처리해야 하는 경우 CPU가 높고 BPDU가 떨어질 수 있습니다.

이러한 문제를 해결하려면 다음 단계 중 하나 또는 전체를 수행하십시오.

1. 스위치에서 VLAN을 정리합니다.
2. MST와 같은 향상된 STP 버전을 사용합니다.
3. 스위치의 하드웨어를 업그레이드합니다.

네트워크에서 스패닝 트리 프로토콜을 구현하기 위한 모범 사례도 참조하십시오.

- CatOS 구성 및 관리를 실행하는 Catalyst 4500/4000, 5500/5000 및 6500/6000 Series 스위치에 대한 모범 사례
- Cisco IOS 소프트웨어를 실행하는 Catalyst 6500/6000 Series 및 Catalyst 4500/4000 Series 스위치의 모범 사례

SPAN 세션

Catalyst 6000/6500 Series 스위치의 아키텍처를 기반으로 하는 SPAN 세션은 스위치의 성능에 영향을 미치지 않지만 SPAN 세션에 높은 트래픽/업링크 포트 또는 EtherChannel이 포함된 경우 프로세서의 로드를 증가시킬 수 있습니다.그러면 특정 VLAN을 분리하면 워크로드가 더 증가합니다.링크에 불량 트래픽이 있는 경우, 이는 워크로드를 더 증가시킬 수 있습니다.

일부 시나리오에서 RSPAN 기능은 루프를 발생시킬 수 있으며 프로세서의 로드가 증가합니다.자세한 내용은 SPAN 세션에서 브리징 루프를 만드는 이유를 참조하십시오.

모든 것이 하드웨어이기 때문에 이 스위치는 트래픽을 평소와 같이 전달할 수 있지만, 어떤 트래픽을 전송할지 알아내려고 하면 CPU가 고전을 겪을 수 있습니다.필요한 경우에만 SPAN 세션을 구성하는 것이 좋습니다.

%CFIB-SP-STBY-7-CFIB_EXCEPTION:FIB TCAM 예외, 일부 항목은 소프트웨어 스위치드

```
%CFIB-SP-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software switched
%CFIB-SP-STBY-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software
switched
```

이 오류 메시지는 TCAM에서 사용 가능한 공간의 양을 초과할 때 수신됩니다.따라서 CPU가 높습니다.이는 FIB TCAM 제한 사항입니다.TCAM이 가득 차면 플래그가 설정되고 FIB TCAM 예외가 수신됩니다.이렇게 하면 TCAM에 새 경로가 추가되지 않습니다.따라서 모든 것이 소프트웨어 스위칭이 될 것입니다.경로를 제거해도 하드웨어 스위칭이 재개되지는 않습니다.TCAM이 예외 상태가 되면 시스템을 다시 로드해야 해당 상태를 벗어날 수 있습니다.TCAM에 설치할 수 있는 최대 경로는 mls cef **maximum-routes** 명령에 의해 증가합니다.

높은 CPU를 사용하는 Catalyst 6500/6000에는 L4 포트를 사용하는 IPv6 ACL이 있음

mls **ipv6 acl 압축 주소 유니캐스트를 활성화합니다.**IPv6 ACL이 L4 프로토콜 포트 번호와 일치하는 경우 이 명령이 필요합니다.이 명령이 활성화되지 않으면 소프트웨어 처리를 위해 IPv6 트래픽이 CPU에 펀딩됩니다.이 명령은 기본적으로 구성되지 않습니다.

구리 SPF

Cisco ME 6500 Series Ethernet 스위치에서 구리 SFP는 다른 유형의 SFP보다 더 많은 펌웨어 상호 작용이 필요하므로 CPU 사용률이 증가합니다.

구리 SFP를 관리하는 소프트웨어 알고리즘은 Cisco IOS SXH 릴리스에서 개선되었습니다.

모듈형 IOS

모듈형 IOS 소프트웨어를 실행하는 Cisco Catalyst 6500 Series 스위치에서 일반적인 CPU 사용률은 비모듈형 IOS 소프트웨어보다 약간 높습니다.

모듈형 IOS 소프트웨어는 활동당 패킷 당 비용을 지불하는 것보다 더 많은 비용을 지불합니다.모듈형 IOS 소프트웨어는 패킷이 많지 않더라도 특정 CPU를 사용하여 프로세스를 유지하므로 CPU 소비량은 실제 트래픽을 기반으로 하지 않습니다.그러나 패킷이 처리되면 모듈형 IOS 소프트웨어에서 사용되는 CPU가 비모듈형 IOS 소프트웨어보다 높지 않아야 합니다.

CPU 사용률 확인

CPU 사용률이 높으면 **show processes cpu** 명령을 먼저 실행합니다.출력은 스위치의 CPU 사용률과 각 프로세스의 CPU 사용률을 보여줍니다.

```
Router#show processes cpu
CPU utilization for five seconds: 57%/48%; one minute: 56%; five minutes: 48%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         5          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2          12     18062          0  0.00%  0.00%  0.00%   0 Load Meter
   4      164532     13717      11994  0.00%  0.21%  0.17%   0 Check heaps
   5           0         1          0  0.00%  0.00%  0.00%   0 Pool Manager
!--- Output is suppressed. 172 0 9 0 0.00% 0.00% 0.00% 0 RPC aapi_rp 173      243912   2171455
112  9.25%  8.11%  7.39%   0 SNMP ENGINE
 174          68       463        146  0.00%  0.00%  0.00%   0 RPC pm-mp
!--- Output is suppressed.
```

이 출력에서 총 CPU 사용률은 57%이고 인터럽트 CPU 사용률은 48%입니다.이 백분율은 굵은 글꼴로 표시됩니다.CPU에 의한 트래픽의 인터럽트 스위치로 인해 인터럽트 CPU 사용률이 발생합니다.명령 출력에는 두 활용률 간의 차이를 일으키는 프로세스가 나열됩니다.이 경우 SNMP 프로세스가 원인입니다.

CatOS를 실행하는 수퍼바이저 엔진에서 출력은 다음과 같습니다.

```
Switch> (enable) show processes cpu


CPU utilization for five seconds:  99.72%
                     one minute: 100.00%
                    five minutes: 100.00%

PID Runtime(ms) Invoked    uSecs    5Sec    1Min    5Min    TTY Process
--- ----------- ---------- -------- ------- ------- ------- --- ---------------
1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and Idle
2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat
3   0           1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr
4   0           1          0          0.00%   0.00%   0.00% -2  L2L3PatchRev
!--- Output is suppressed. 61 727295 172025 18000 0.82% 0.00% 0.00% -2 SptTimer 62  18185410
3712736    106000    22.22%  21.84%  21.96% -2  SptBpduRx
63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

이 출력에서 첫 번째 프로세스는 `Kernel Idle`로 유휴 CPU 사용률을 표시합니다.다른 프로세스에서 CPU 사이클을 사용하지 않는 한 이 프로세스는 일반적으로 높습니다.이 예에서 SptBpduRx CPU 사용률이 높습니다.

이러한 프로세스 중 하나로 인해 CPU 사용률이 높은 경우 문제를 해결하고 이 프로세스가 높은 이유를 확인할 수 있습니다.그러나 CPU로 트래픽을 포밍하여 CPU가 높은 경우 트래픽이 펀딩되는 이유를 결정해야 합니다.이러한 결정을 통해 트래픽이 무엇인지 파악할 수 있습니다.

문제 해결을 위해 CPU 사용률이 높은 경우 스위치에서 출력을 수집하려면 다음 EEM 스크립트 예를 사용합니다.

```
event manager applet cpu_stats

event snmp oid "1.3.6.1.4.1.9.9.109.1.1.1.1.3.1" get-type exact entry-op gt entry-val "70"
```

```
exit-op lt exit-val "50" poll-interval 5

action 1.01 syslog msg "------HIGH CPU DETECTED----, CPU:$_snmp_oid_val%"

action 1.02 cli command "enable"

action 1.03 cli command "show clock | append disk0:cpu_stats"

action 1.04 cli command "show proc cpu sort | append disk0:cpu_stats"

action 1.05 cli command "Show proc cpu | exc 0.00% | append disk0:cpu_stats"

action 1.06 cli command "Show proc cpu history | append disk0:cpu_stats"

action 1.07 cli command "show logging | append disk0:cpu_stats "

action 1.08 cli command "show spanning-tree detail | in ieee|occurr|from|is exec | append
disk0:cpu_stats"

action 1.09 cli command "debug netdr cap rx | append disk0:cpu_stats"

action 1.10 cli command "show netdr cap | append disk0:cpu_stats"

action 1.11 cli command "undebug all"
!
```

참고: debug **netdr capture rx** 명령은 하드웨어 대신 패킷의 프로세스 스위칭으로 인해 CPU가 높은 경우 유용합니다.명령이 실행될 때 CPU로 들어오는 4096개의 패킷을 캡처합니다.이 명령은 완전히 안전하며 6500에서 높은 CPU 문제를 해결하기 위한 가장 편리한 툴입니다.CPU에 추가 부하가 발생하지 않습니다.

CPU에 펀딩되는 트래픽을 결정하는 유틸리티 및 툴

이 섹션에서는 이 트래픽을 확인하는 데 도움이 되는 몇 가지 유틸리티 및 툴을 설명합니다.

Cisco IOS 시스템 소프트웨어

Cisco IOS Software에서 수퍼바이저 엔진의 스위치 프로세서를 SP라고 하며 MSFC를 RP라고 합니다.

show **interface** 명령은 인터페이스의 상태와 인터페이스의 트래픽 속도에 대한 기본 정보를 제공합니다.이 명령은 오류 카운터도 제공합니다.

```
Router#show interface gigabitethernet 4/1
GigabitEthernet4/1 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 000a.42d1.7580 (bia 000a.42d1.7580)
  Internet address is 100.100.100.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 5/75/1/24075 (size/max/drops/flushes); Total output drops: 2
```

```
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 7609000 bits/sec, 14859 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 0 pkt, 184954624 bytes - mcast: 1 pkt, 500 bytes
  L3 in Switched: ucast: 2889916 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
     2982871 packets input, 190904816 bytes, 0 no buffer
     Received 9 broadcasts, 0 runts, 0 giants, 0 throttles
     1 input errors, 1 CRC, 0 frame, 28 overrun, 0 ignored
     0 input packets with dribble condition detected
     1256 packets output, 124317 bytes, 0 underruns
     2 output errors, 1 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

이 출력에서는 수신 트래픽이 Layer 2-switched 대신 Layer 3-switched임을 확인할 수 있습니다.이는 트래픽이 CPU에 펀딩되고 있음을 나타냅니다.

show processes **cpu** 명령은 이러한 패킷이 일반 트래픽 패킷인지 또는 제어 패킷인지 알려줍니다.

```
Router#show processes cpu | exclude 0.00
CPU utilization for five seconds: 91%/50%; one minute: 89%; five minutes: 47%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   5      881160     79142      11133  0.49%  0.19%  0.16%   0 Check heaps
  98      121064   3020704         40 40.53% 38.67% 20.59%   0 IP Input
 245      209336    894828        233  0.08%  0.05%  0.02%   0 IFCOM Msg Hdlr
```

패킷이 프로세스 스위칭되는 경우 `IP` 프로세스가 높게 실행되는 것을 볼 수 있습니다.다음 패킷을 보려면 이 명령을 실행합니다.

[show buffers input interface]

```
Router#show buffers input-interface gigabitethernet 4/1 packet

Buffer information for Small buffer at 0x437874D4
  data_area 0x8060F04, refcount 1, next 0x5006D400, flags 0x280
  linktype 7 (IP), enctype 1 (ARPA), encsize 14, rxtype 1
  if_input 0x505BC20C (GigabitEthernet4/1), if_output 0x0 (None)
  inputtime 00:00:00.000 (elapsed never)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x8060F7A, datagramsize 60, maximum size 308
  mac_start 0x8060F7A, addr_start 0x8060F7A, info_start 0x0
  network_start 0x8060F88, transport_start 0x8060F9C, caller_pc 0x403519B4

  source: 100.100.100.1, destination: 100.100.100.2, id: 0x0000, ttl: 63,
  TOS: 0 prot: 17, source port 63, destination port 63

08060F70:                         000A 42D17580            ..BQu.
08060F80: 00000000 11110800 4500002E 00000000  ........E.......
08060F90: 3F11EAF3 64646401 64646402 003F003F  ?.jsddd.ddd..?.?
08060FA0: 001A261F 00010203 04050607 08090A0B  ..&.............
08060FB0: 0C0D0E0F 101164                      ......d
```

트래픽이 **인터럽트 스위치드**로 전환된 경우 **show buffers input-interface** 명령으로 해당 패킷을 볼 수 없습니다.인터럽트 스위칭을 위해 RP에 펀딩된 패킷을 보려면 RP 포트의 SPAN(Switched Port Analyzer) 캡처를 수행할 수 있습니다.

참고: 인터럽트 스위치드 CPU 사용률과 프로세스 스위치드 CPU 사용률에 대한 자세한 내용은 이

문서를 참조하십시오.

- *Troubleshooting High CPU Utilization on Cisco Routers(*Cisco 라우터의 높은 CPU 사용률 문제 해결) 섹션의 인터럽트로 *인한 높은 CPU 사용률*

SPAN RP-Inband 및 SP-Inband

Cisco IOS Software의 RP 또는 SP 포트에 대한 SPAN은 Cisco IOS Software 릴리스 12.1(19)E 이상에서 사용할 수 있습니다.

명령 구문은 다음과 같습니다.

```
test monitor session 1-66 add {rp-inband | sp-inband} [rx | tx | both]
```

Cisco IOS Software 12.2 SX 릴리스에 다음 구문을 사용합니다.

```
test monitor add {1..66} {rp-inband | sp-inband} {rx | tx | both}
```

참고: SXH 릴리스의 경우 로컬 SPAN 세션을 구성하려면 **monitor session** 명령을 사용한 다음 이 명령을 사용하여 SPAN 세션을 CPU와 연결해야 합니다.

```
source {cpu {rp | sp}} | single_interface | interface_list | interface_range |
mixed_interface_list | single_vlan | vlan_list | vlan_range | mixed_vlan_list} [rx | tx | both]
```

참고: 이 명령에 대한 자세한 내용은 *Catalyst 6500 릴리스 12.2SX 소프트웨어 구성 설명서*의 로컬 SPAN(SPAN 컨피그레이션 모드) *구성을* 참조하십시오.

다음은 RP 콘솔의 예입니다.

```
Router#monitor session 1 source interface fast 3/3
!--- Use any interface that is administratively shut down. Router#monitor session 1 destination
interface 3/2
```

이제 SP 콘솔로 이동합니다.예를 들면 다음과 같습니다.

```
Router-sp#test monitor session 1 add rp-inband rx
```

참고: Cisco IOS 12.2 SX 릴리스에서는 **테스트 모니터 추가 1 rp-inband rx**로 명령이 변경되었습니다.

```
Router#show monitor
Session 1
---------
Type : Local Session
Source Ports :
```

```
Both : Fa3/3
Destination Ports : Fa3/2
SP console:
Router-sp#test monitor session 1 show
Ingress Source Ports: 3/3 15/1
Egress Source Ports: 3/3
Ingress Source Vlans: <empty>
Egress Source Vlans: <empty>
Filter Vlans: <empty>
Destination Ports: 3/2
```

참고: Cisco IOS 12.2 SX 릴리스에서는 명령이 **테스트 모니터 show 1**로 변경되었습니다.

다음은 SP 콘솔의 예입니다.

```
Router-sp#test monitor session 1 show
Ingress Source Ports: 3/3 15/1
Egress Source Ports: 3/3
Ingress Source Vlans: <empty>
Egress Source Vlans: <empty>
Filter Vlans: <empty>
Destination Ports: 3/2
```

CatOS 시스템 소프트웨어

CatOS 시스템 소프트웨어를 실행하는 스위치의 경우 수퍼바이저 엔진은 CatOS를 실행하고 MSFC는 Cisco IOS 소프트웨어를 실행합니다.

show mac 명령을 실행하면 MSFC에 펀팅된 프레임 수를 확인할 수 있습니다.포트 15/1은 MSFC에 대한 수퍼바이저 엔진 연결입니다.

참고: 포트는 슬롯 2의 수퍼바이저 엔진의 경우 16/1입니다.

```
Console> (enable) show mac 15/1

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
15/1                  193576                    0                    1

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
15/1                        3                    0                    0

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
15/1                18583370                    0

MAC      Dely-Exced MTU-Exced  In-Discard Out-Discard
-------- ---------- ---------- ---------- -----------
15/1              0          -          0           0
```

이 수의 빠른 증가는 패킷이 MSFC에 펀딩되어 CPU 사용률이 높음을 나타냅니다.그런 다음 다음과 같은 방법으로 패킷을 볼 수 있습니다.

- SPAN MSFC 포트 15/1 또는 16/1
- SPAN sc0

SPAN MSFC 포트 15/1 또는 16/1

소스가 MSFC 포트 15/1(또는 16/1)이고 대상이 이더넷 포트인 SPAN 세션을 설정합니다.

예를 들면 다음과 같습니다.

```
Console> (enable) set span 15/1 5/10
Console> (enable) show span

Destination      : Port 5/10
Admin Source     : Port 15/1
Oper Source      : None
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Status           : active
```

포트 5/10에서 스니퍼 추적을 수집하는 경우 스니퍼 추적은 MSFC와 주고받는 패킷을 표시합니다. MSFC에서 전송되지 않고 MSFC로 향하는 패킷을 캡처하기 위해 SPAN 세션을 tx로 구성합니다.

SPAN sc0

수퍼바이저 엔진 CPU로 이동하는 프레임을 캡처하려면 **sc0** 인터페이스를 소스로 사용하여 SPAN 세션을 설정합니다.

```
Console> (enable) set span ?
  disable                  Disable port monitoring
  sc0                      Set span on interface sc0
  <mod/port>               Source module and port numbers
  <vlan>                   Source VLAN numbers
```

참고: OSM(Optical Services Module)의 경우 트래픽의 SPAN 캡처를 수행할 수 없습니다.

권장 사항

수퍼바이저 엔진 CPU 사용률은 스위치의 하드웨어 포워딩 성능을 반영하지 않습니다.그러나 수퍼바이저 엔진 CPU 사용률을 베이스라인 설정 및 모니터링해야 합니다.

1. 정상 트래픽 패턴과 부하가 있는 정상 상태 네트워크에서 스위치의 수퍼바이저 엔진 CPU 사용률을 기준화합니다.어떤 프로세스에서 가장 높은 CPU 사용률을 생성하는지 확인합니다.
2. CPU 사용률을 트러블슈팅할 때 다음 질문을 고려하십시오.가장 높은 활용률을 창출하는 프로세스는 무엇입니까?이러한 프로세스가 베이스라인과 다른가요?CPU가 기준보다 지속적으로 증가합니까?또는 활용률이 높은 후 기준 레벨로 돌아가는 경우가 있습니까?네트워크에 TCN(Topology Change Notifications)이 있습니까?**참고:** STP PortFast가 비활성화된 포트 또는 호스트 포트의 플래핑 때문에 TCN이 발생합니다.관리 서브넷/VLAN에 과도한 브로드캐스트 또는 멀티캐스트 트래픽이 있습니까?스위치에 SNMP 폴링과 같은 과도한 관리 트래픽이 있습니까?
3. CPU가 높은 시간 동안(CPU가 75% 이상인 경우) 다음 명령에서 출력을 수집합니다.시계 표시 버전 표시프로세스 cpu 정렬됨show proc cpu 기록로그 표시
4. 가능하면 사용자 데이터 트래픽, 특히 브로드캐스트 트래픽이 많은 VLAN에서 관리 VLAN을 격리합니다.이러한 트래픽 유형의 예로는 IPX RIP/SAP(Service Advertising Protocol), AppleTalk 및 기타 브로드캐스트 트래픽이 있습니다.이러한 트래픽은 수퍼바이저 엔진 CPU

사용률에 영향을 미칠 수 있으며, 극단적인 경우 스위치의 정상적인 작동을 방해할 수 있습니다.

5. RP에 대한 트래픽의 풍력으로 인해 CPU가 높게 실행되는 경우 해당 트래픽이 무엇이고 트래픽이 펀딩되는 이유를 확인합니다.이를 확인하려면 유틸리티 및 도구에서 CPU 섹션에 펀딩된 트래픽을 확인하기 위해 설명하는 유틸리티를 사용합니다.

관련 정보

- Sup720을 사용하는 catalyst 6500에서 높은 CPU를 트러블슈팅하는 데 유용한 명령
- Catalyst 6000/6500 Series 스위치의 일반적인 CatOS 오류 메시지
- Cisco IOS 소프트웨어를 실행하는 Catalyst 6500/6000 Series 스위치의 일반적인 오류 메시지
- Cisco IOS 시스템 소프트웨어를 실행하는 Catalyst 6500/6000 Series 스위치의 하드웨어 및 공통 문제 해결
- 스위치드 캠퍼스 네트워크의 유니캐스트 플러딩
- Cisco Catalyst 6500 Series 스위치 제품 지원
- 간헐적 CPU 문제 중 데이터 수집을 위한 EEM 스크립트
- LAN 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems