

EAP 프레임워크 및 AAA Manager로 인해 dot1x/Mab를 사용하는 스위치에서 높은 CPU 문제 해결

목차

[소개](#)

[배경 정보](#)

[구성](#)

[문제 해결](#)

[버그](#)

소개

이 문서에서는 EAP(Extensible Authentication Protocol) 프레임워크 및 AAA(Authentication, Authorization, and Accounting) 관리자으로 인한 높은 CPU/메모리 문제를 해결하는 방법에 대해 설명합니다. dot1x/mab 인증을 사용하는 스위치에서 볼 수 있습니다.

배경 정보

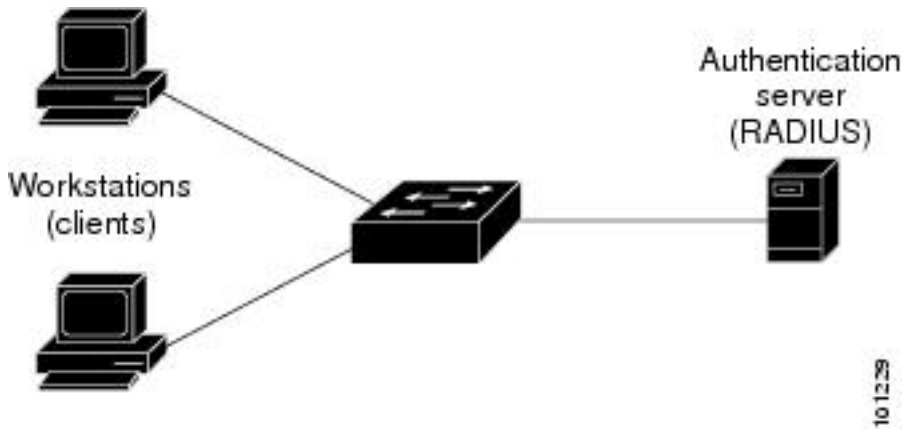
Cisco IOS Auth Manager는 네트워크 인증 요청을 처리하고 인증 방법과 상관없이 권한 부여 정책을 적용합니다. 인증 관리자는 모든 포트 기반 네트워크 연결 시도, 인증, 권한 부여 및 연결 해제에 대한 운영 데이터를 유지 관리하고 세션 관리자 역할을 합니다.

스위치는 클라이언트와 인증 서버 간의 중간(프록시) 역할을 하며, 클라이언트로부터 ID 정보를 요청하고, 인증 서버와의 정보를 확인하고, 클라이언트에 응답을 릴레이합니다. 스위치에는 EAP 프레임워크를 캡슐화하고 캡슐화하여 인증 서버와 상호 작용하는 RADIUS 클라이언트가 포함됩니다.

구성

이 섹션에서는 MAB/DOT1X(MAC Authentication Bypass) 인증을 수행하는 Cisco 스위치를 보여줍니다.

포트 기반 네트워크 액세스 제어의 개념을 이해하고 Cisco 플랫폼에서 포트 기반 네트워크 액세스 제어를 구성하는 방법을 이해해야 합니다. 이 이미지는 dot1x/MAB 인증이 있는 워크스테이션을 보여줍니다.



다음은 샘플 컨피그레이션입니다.

```
interface FastEthernet0/8
  switchport access vlan 23
  switchport mode access
  switchport voice vlan 42
  authentication host-mode multi-domain
  authentication order mab dot1x
  authentication priority mab dot1x---> Priority order
  authentication port-control auto
  authentication periodic
  authentication timer reauthenticate <value in sec>---->(Time after which the client auth would
be re-negotiated)
  authentication violation protect mab mls qos trust dscp dot1x pae authenticator dot1x timeout
tx-period 3 storm-control broadcast level 2.00 no cdp enable spanning-tree portfast spanning-
tree bpduguard enable service-policy input Marking end
```

문제 해결

dot1x/MAB 인증을 사용하는 스위치는 EAP 프레임워크 및 AAA 관리자 때문에 CPU/메모리 스파이크가 자주 발생하는 경우가 있습니다. 이는 인증 요청이 삭제되기 때문에 운영에 영향을 미칠 수 있습니다.

이 문제를 해결하려면 다음 단계를 권장합니다.

1단계. **show proc cpu sort** 명령을 입력하여 스위치에서 높은 CPU 사용량을 확인하고 다음 예와 같이 EAP Framework 및 Auth 관리자 프로세스가 가장 높은 사용량을 가지고 있는지 확인합니다.

PU utilization for five seconds:

97%

/2%; one minute: 90%; five minutes: 89%

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
149	178566915	140683416	1269					

64.04% 47.11% 45.63% 0 EAP Framework

141	130564594	55418491	2355					
-----	-----------	----------	------	--	--	--	--	--

21.61% 29.05% 29.59% 0 Auth Manager

```

121 305295906 487695245 519 1.74% 1.84% 1.78% 0 Hulc LED Process
144 12070918 31365536 384 0.63% 0.43% 0.49% 0 MAB Framework
258 117344878 885817567 132 0.47% 0.79% 0.86% 0 RADIUS

```

2단계. 이 예와 같이 **show process cpu memory** 명령을 사용하여 Auth Manager 및 RADIUS와 같은 프로세스에 대한 스위치의 메모리 사용량을 확인합니다.

```

Processor Pool Total: 22559064 Used: 16485936 Free: 6073128
I/O Pool Total: 4194304 Used: 2439944 Free: 1754360
Driver te Pool Total: 1048576 Used: 40 Free: 1048536

```

```

PID TTY Allocated Freed Holding Getbufs Retbufs Process
0 0 29936164 13273256 13856236 0 0 *Init*
0 0 34797632 32603736 1091560 2481468 263240 *Dead*
59 0 366860 6760 317940 0 0 Stack Mgr Notifi
141 0

```

569580564 3357129696

174176 2986956

0

Auth Manager

258 0

1212276148 2456764884 140684 21066696

0

RADIUS

```

131 0 552345134 541235441 90736 20304 0 HRPC qos reque

```

3단계. 스위치에서 리소스 사용량이 많은 경우 다음과 같이 인증 실패에 대한 로그가 표시될 수 있습니다.

show logging 명령을 입력합니다.

```

%DOT1X-5-FAIL: Authentication failed for client (7446.a04b.1495) on Interface Fa0/17
AuditSessionID 0A73340200000224870C28AA
%AUTHMGR-7-RESULT:

```

Authentication result 'no-response'

```

from 'dot1x' for client (7446.a04b.1495) on Interface Fa0/17 AuditSessionID
0A73340200000224870C28AA
%AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (7446.a04b.1495) on Interface Fa0/17
AuditSessionID 0A73340200000224870C28AA

```

4단계. 클라이언트에 대해 자주 인증하지 않도록 재인증 타이머를 더 높은 값(예: 3600초)으로 설정하여 스위치의 부하를 늘립니다.

컨피그레이션을 검증하려면 **show run interface <interface-name>** 명령을 입력합니다.

```
interface FastEthernet0/8
switchport access vlan 23
switchport mode access
switchport voice vlan 42
authentication host-mode multi-domain
authentication order mab dot1x
authentication priority mab dot1x
authentication port-control auto
authentication periodic
```

authentication timer reauthenticate 60----->Make sure we do not have any

```
aggressive timers set
authentication violation protect
```

5단계. MAB/dot1x 프로세스에 대해 표시되는 세션 수를 결정합니다. 인증 세션 수가 많으면 CPU가 많을 수 있습니다. 활성 세션 수를 확인하려면 다음 명령을 입력합니다.

SW#

show authentication registrations

Auth Methods registered with the Auth Manager:

Handle	Priority	Name
100	0	dot1x
3	1	mab
1	2	webauth

SW#Show authentication method dot1x

SW#Show authentication method mab

SW#Show authentication sessions

6단계. 버전 및 잠재적 버그를 확인하려면 **show version** 명령을 입력합니다.

버그가 "버그" 섹션에 나열되지 않은 경우 TAC(Technical Assistance Center)에서 케이스를 열고 1단계에서 5단계까지 모든 로그를 연결합니다.

버그

[CSCus46997](#) IP 호스트 트랙 및 인증 관리자의 메모리 누수 및 높은 CPU

[CSCtz06177](#) A Catalyst 2960의 메모리가 부족할 수 있습니다.

[CSCty49762](#) EAP 프레임워크 및 AAA AttrL 하위 사용 모든 프로세스 메모리

팁:자세한 내용은 Cisco 버그 ID CSCus[46997](#), CSCtz[06177](#) 및 CSCty49762를 [참조하십시오](#)