

EAP フレームワークと AAA マネージャが原因の、dot1x/Mab のスイッチにおける高 CPU 使用率のトラブルシューティング

内容

[概要](#)

[背景説明](#)

[コンフィギュレーション](#)

[トラブルシュート](#)

[バグ](#)

概要

このドキュメントでは、Extensible Authentication Protocol(EAP)フレームワークおよび Authentication, Authorization, and Accounting(AAA)マネージャによるHigh CPU/メモリ(HRAM)のトラブルシューティング方法について説明します。これは、dot1x/mab認証を使用するスイッチで発生します。

背景説明

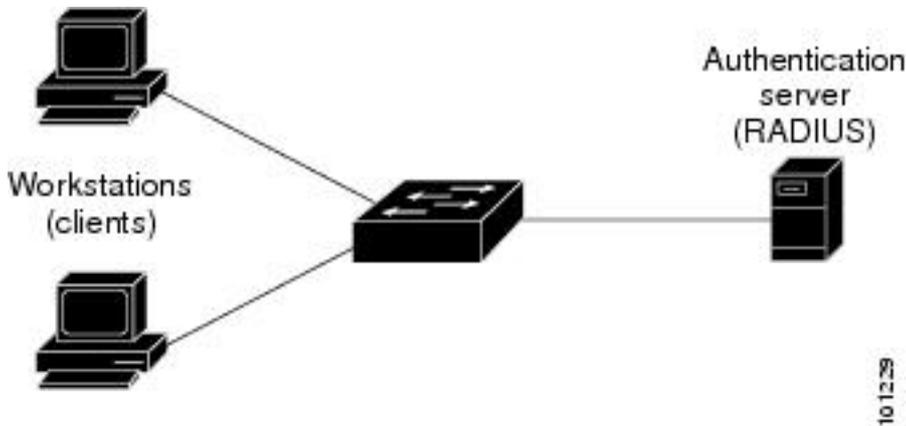
Cisco IOS Auth Managerはネットワーク認証要求を処理し、認証方式に関係なく認証ポリシーを適用します。認証マネージャは、すべてのポートベースのネットワーク接続試行、認証、許可、および切断の運用データを保持し、セッションマネージャとして機能します。

スイッチは、クライアントと認証サーバの間の仲介（プロキシ）として機能し、クライアントからID情報を要求し、その情報を認証サーバで確認し、クライアントへの応答を中継します。スイッチにはRADIUSクライアントが含まれ、RADIUSクライアントはEAPフレームをカプセル化およびカプセル化解除し、認証サーバと対話します。

コンフィギュレーション

このセクションでは、MAB/DOT1X(MAC Authentication Bypass)認証を行うシスコスイッチを示します。

ポートベースのネットワークアクセスコントロールの概念を理解し、シスコプラットフォームでポートベースのネットワークアクセスコントロールを設定する方法を理解しておく必要があります。この図は、dot1x/MAB認証を持つワークステーションを示しています。



設定例を次に示します。

```
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
```

トラブルシューティング

dot1x/MAB認証を使用するスイッチでは、EAPフレームワークとAAAマネージャが原因で、CPUとメモリの使用率が高くなる場合があります。これは、認証要求がドロップされるため、実稼働に影響を与える可能性があります。

これを解決するには、次の手順を実行することを推奨します。

ステップ1: `show proc cpu sort` コマンドを入力して、スイッチのCPU使用率が高いことを確認し、次の例に示すようにEAP FrameworkプロセスとAuth managerプロセスの使用率が最も高いことを確認します。

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

```

ステップ2 : 次の例に示すように、**show process cpu memory**コマンドを使用して、Auth ManagerやRADIUSなどのプロセスについて、スイッチのメモリ使用量を確認します。

```

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

```

ステップ3 : スイッチでリソースの使用率が高い場合は、次に示すように認証失敗のログが表示されることがあります。

show logging コマンドを入力します。

```

%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

```

ステップ4 : 再認証タイマーを高い値 (たとえば、3600秒) に設定して、クライアントの認証が頻繁に行われないようにします。これにより、スイッチの負荷が増大します。

設定を検証するには、**show run interface <interface-name>**コマンドを入力します。

```
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
```

ステップ5:MAB/dot1xプロセスに対して表示されるセッション数を決定します。認証済みセッションの数が多くなると、CPUの使用率が高くなる可能性があります。アクティブセッションの数を確認するには、次のコマンドを入力します。

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

ステップ6：バージョンと潜在的なバグを確認するには、**show version**コマンドを入力します。

このバグが「バグ」セクションに記載されていない場合は、Technical Assistance Center(TAC)でケースをオープンし、ステップ1～5のすべてのログを添付してください。

バグ

[CSCus46997](#) IP Host Track and Auth ManagerのメモリリークとCPU高使用率

[CSCtz06177](#) Catalyst 2960のメモリが不足している可能性があります。

[CSCty49762](#) EAP FrameworkとAAA AttrLサブがすべてのプロセスメモリを使用

ヒント：詳細については、Cisco Bug ID [CSCus46997](#)、[CSCtz06177](#)、および [CSCty49762](#)を参照してください。