

# Solución de problemas de CPU alta en switches con dot1x/Mab debido a EAP Framework y AAA Manager

## Contenido

[Introducción](#)

[Antecedentes](#)

[Configuración](#)

[Troubleshoot](#)

[Errores](#)

## Introducción

Este documento describe cómo resolver problemas de CPU/memoria alta debido al marco de protocolo de autenticación extensible (EAP) y al administrador de autenticación, autorización y contabilidad (AAA). Esto se ve en los switches que utilizan la autenticación dot1x/mab.

## Antecedentes

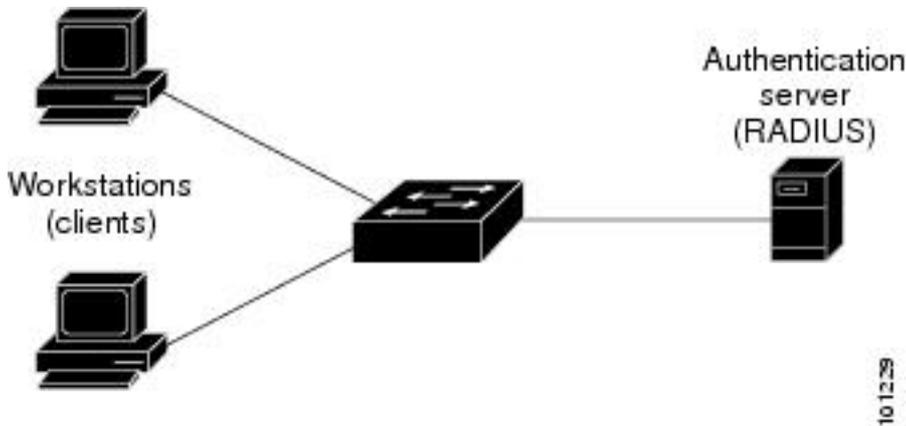
Cisco IOS Auth Manager gestiona las solicitudes de autenticación de red y aplica las políticas de autorización independientemente del método de autenticación. El Administrador de autenticación mantiene los datos operativos para todos los intentos, autenticaciones, autorizaciones y desconexiones de conexión de red basada en puerto y, funciona como administrador de sesiones.

El switch actúa como intermediario (proxy) entre el cliente y el servidor de autenticación, solicita información de identidad del cliente, verifica esa información con el servidor de autenticación y transmite una respuesta al cliente. El switch incluye el cliente RADIUS, que encapsula y desencapsula las tramas EAP e interactúa con el servidor de autenticación.

## Configuración

Esta sección muestra un switch de Cisco que realiza la autenticación MAB/DOT1X (MAC AuthenticationBypass).

Debe comprender los conceptos del control de acceso a la red basado en puertos y comprender cómo configurar el control de acceso a la red basado en puertos en su plataforma Cisco. Esta imagen ilustra las estaciones de trabajo que tienen autenticación dot1x/MAB.



Este es un ejemplo de configuración:

```
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
```

## Troubleshoot

Los switches que utilizan la autenticación dot1x/MAB a veces tienen picos de CPU/memoria elevados debido al EAP Framework y al administrador AAA. Esto puede afectar a la producción ya que las solicitudes de autenticación se descartan.

Para resolver esto, se recomiendan estos pasos:

Paso 1. Ingrese el comando **show proc cpu sort** para verificar el uso elevado de la CPU en el switch y asegúrese de que los procesos EAP Framework y Auth Manager tengan el uso más alto como se muestra en este ejemplo:

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

```

Paso 2. Verifique el uso de memoria en el switch para los procesos como Auth Manager y RADIUS con el comando **show process cpu memory** como se muestra en este ejemplo.

```

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

```

Paso 3. Si se enfrenta a un uso elevado de los recursos en el switch, es posible que vea los siguientes registros para las fallas de autenticación como se muestra a continuación:

Ingrese el comando **show logging**.

```

%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

```

Paso 4. Establezca el temporizador de reautenticación en un valor mayor (por ejemplo, 3600 segundos) para asegurarse de que no se autentica con frecuencia para los clientes, lo que aumenta la carga en el switch.

Para validar la configuración, ingrese el comando **show run interface <interface-name>**:

```
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
```

Paso 5. Determine cuántas sesiones se ven para los procesos MAB/dot1x, porque a veces un gran número de sesiones autenticadas también puede conducir a un uso excesivo de la CPU. Para verificar el número de sesiones activas, ingrese estos comandos:

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**

Paso 6. Para verificar la versión y los posibles errores de funcionamiento, ingrese el comando **show version**.

Si el error no aparece en la sección "Errores", abra un caso con el Centro de asistencia técnica (TAC) y adjunte todos los registros de los pasos 1 a 5.

## Errores

[CSCus46997](#) Pérdida de memoria y uso elevado de la CPU en IP Host Track y Administrador de autenticación

[CSCtz06177](#) Un Catalyst 2960 puede funcionar con poca memoria.

[CSCty49762](#) EAP Framework y AAA AttrL Sub utilizan toda la memoria de proceso

**Consejo:** Para obtener más detalles, consulte los ID de bug de Cisco [CSCus46997](#), [CSCtz06177](#) y [CSCty49762](#).