

Resolución de problemas Dot1x en switches Catalyst serie 9000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración Básica](#)

[Verificar configuración y operaciones](#)

[Introducción a 802.1x](#)

[Configuración](#)

[Sesión de autenticación](#)

[Accesibilidad al servidor de autenticación](#)

[Troubleshoot](#)

[Metodología](#)

[Ejemplo de síntomas](#)

[Utilidades específicas de la plataforma](#)

[Ejemplos de seguimiento](#)

[Additional Information](#)

[Configuración predeterminada](#)

[Configuración opcional](#)

[Diagrama de flujo](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar, validar y resolver problemas de control de acceso a la red (NAC) 802.1x en switches Catalyst serie 9000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.


- Catalyst 9000 Series Switch
- Identity Services Engine (ISE)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.6.x y posterior
- ISE-VM-K9 versión 3.0.0.458

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

 Nota: Consulte la guía de configuración correspondiente para conocer los comandos que se utilizan para habilitar estas funciones en otras plataformas de Cisco.

Antecedentes

El estándar 802.1x define un control de acceso basado en cliente-servidor y un protocolo de autenticación que impide que los clientes no autorizados se conecten a una LAN a través de puertos de acceso público a menos que estén autenticados correctamente. El servidor de autenticación autentica cada cliente conectado a un puerto de switch antes de poner a disposición cualquier servicio ofrecido por el switch o la LAN.


La autenticación 802.1x incluye 3 componentes distintos:

Suplicante: cliente que envía credenciales para la autenticación

Autenticador: dispositivo de red que proporciona conectividad de red entre el cliente y la red y puede permitir o bloquear el tráfico de red.

Servidor de autenticación: Servidor que puede recibir y responder a solicitudes de acceso a la red, indica al autenticador si se puede permitir la conexión y varias otras configuraciones que se aplicarían a la sesión de autenticación.

El público objetivo de este documento son los ingenieros y el personal de soporte técnico que no se centran necesariamente en la seguridad. Para obtener más información sobre la autenticación basada en puertos 802.1x y componentes como ISE, consulte la guía de configuración adecuada.

 Nota: Consulte la guía de configuración adecuada para su plataforma específica y la versión de código para obtener la configuración de autenticación 802.1x predeterminada más precisa.

Configuración Básica

En esta sección se describe la configuración básica necesaria para implementar la autenticación basada en puertos 802.1x. Encontrará una explicación adicional de las funciones en la pestaña de adiciones de este documento. Existen ligeras variaciones en los estándares de configuración de una versión a otra. Valide la configuración con la guía de configuración de la versión actual.

La autenticación, autorización y cuenta (AAA) deben estar habilitadas antes de configurar la autenticación basada en correo 802.1x, y debe establecerse una lista de métodos.

- Las listas de métodos describen la secuencia y el método de autenticación que se consultará para autenticar a un usuario.
- 802.1x también se debe habilitar globalmente.

```
<#root>
```

```
C9300>
```

```
enable
```

```
C9300#
```

```
configure terminal
```

```
C9300(config)#
```

```
aaa new-model
```

```
C9300(config)#
```

```
aaa authentication dot1x default group radius
```

```
C9300(config)#
```

```
dot1x system-auth-control
```

Defina un servidor RADIUS en el switch

```
<#root>
```

```
C9300(config)#
```

```
radius server RADIUS_SERVER_NAME
```

```
C9300(config-radius-server)#
```

```
address ipv4 10.0.1.12
```

```
C9300(config-radius-server)#
```

```
key rad123
```

```
C9300(config-radius-server)#
```

```
exit
```

Active 802.1x en la interfaz cliente.

```
<#root>
```

```
C9300(config)#
```

```
interface TenGigabitEthernet 1/0/4
```

```
C9300(config-if)#
```

```
switchport mode access
```

```
C9300(config-if)#
```

```
authentication port-control auto
```

```
C9300(config-if)#
```

```
dot1x pae authenticator
```

```
C9300(config-if)#
```

```
end
```

Verificar configuración y operaciones

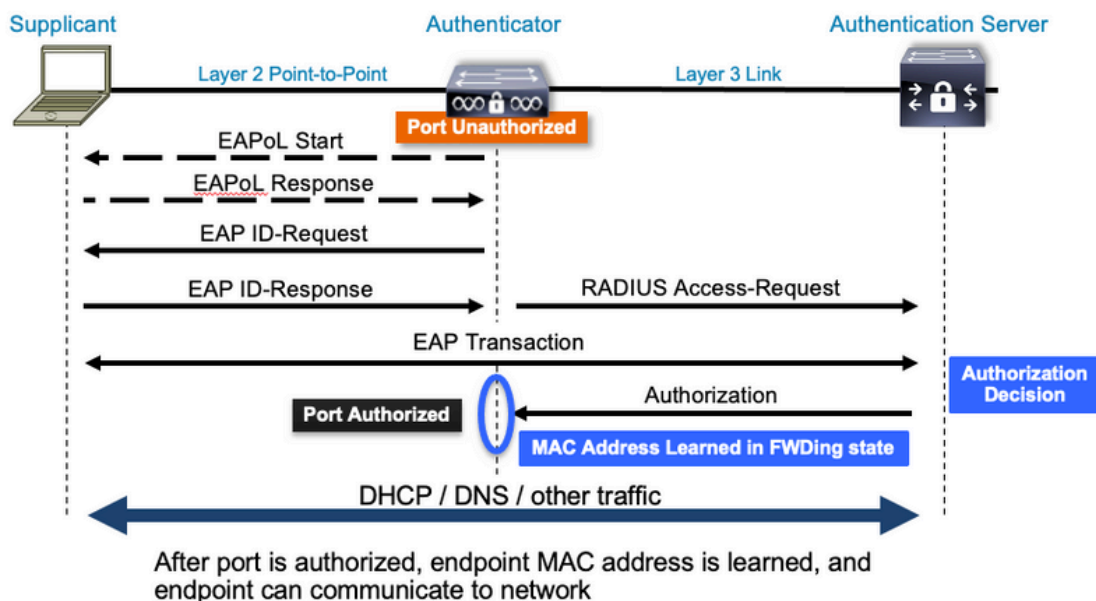
Esta sección proporciona información general sobre 802.1x y sobre cómo verificar la configuración y las operaciones.

Introducción a 802.1x

802.1x implica dos tipos distintos de tráfico: tráfico de cliente a autenticador (punto a punto) a través de EAPoL (protocolo de autenticación extensible sobre LAN) y tráfico de autenticador a servidor de autenticación que se encapsula a través de RADIUS.

Este diagrama representa el flujo de datos para una simple transacción dot1x

802.1X Message Exchange



El autenticador (switch) y el servidor de autenticación (ISE, por ejemplo) suelen estar separados por la capa 3. El tráfico RADIUS se enruta a través de la red entre el autenticador y el servidor. El tráfico EAPoL se intercambia en el link directo entre el solicitante (cliente) y el autenticador.

Tenga en cuenta que el aprendizaje de MAC se produce después de la autenticación y la autorización.

A continuación, se incluyen algunas preguntas que debe tener en cuenta a la hora de abordar un problema relacionado con 802.1x:

- ¿Está configurado correctamente?
- ¿Es accesible el servidor de autenticación?
- ¿Cuál es el estado del Administrador de autenticación?
- ¿Hay algún problema con la entrega de paquetes entre el cliente y el autenticador o entre el autenticador y el servidor de autenticación?

Configuración

Algunas configuraciones varían ligeramente entre las versiones principales. Consulte la guía de configuración pertinente para obtener información específica de la plataforma o el código.

AAA se debe configurar para utilizar la autenticación basada en puerto 802.1x.

- Se debe establecer una lista de métodos de autenticación para "dot1x". Esto representa una configuración AAA común donde 802.1X está habilitado.

<#root>

C9300#

show running-config | section aaa

```

aaa new-model

<-- This enables AAA.

aaa group server radius ISEGROUP

<-- This block establishes a RADIUS server group named "ISEGROUP".
server name DOT1x

ip radius source-interface Vlan1
aaa authentication dot1x default group ISEGROUP

<-- This line establishes the method list for 802.1X authentication. Group ISEGROUP is be used.
aaa authorization network default group ISEGROUP

aaa accounting update newinfo periodic 2880
aaa accounting dot1x default start-stop group ISEGROUP

C9300#

show running-config | section radius

aaa group server radius ISEGROUP
server name DOT1x
ip radius source-interface Vlan1

<-- Notice 'ip radius source-interface' configuration exists in both global configuration and the aaa se

ip radius source-interface Vlan1
radius server DOT1x
address ipv4 10.122.141.228 auth-port 1812 acct-port 1813

<-- 1812 and 1813 are default auth-port and acct-port, respectively.

key secretKey

```

Este es un ejemplo de configuración de interfaz donde 802.1x está habilitado. MAB (MAC Authentication Bypass) es un método de respaldo común para autenticar clientes que no soportan suplicantes dot1x.

<#root>

```

C9300#

show running-config interface tel1/0/4

Building configuration...

Current configuration : 148 bytes
!
interface TenGigabitEthernet1/0/4
switchport access vlan 50
switchport mode access
authentication order dot1x mab

<-- Specifies authentication order, dot1x and then mab

authentication priority dot1x mab

<-- Specifies authentication priority, dot1x and then mab

```

```

authentication port-control auto
<-- Enables 802.1x dynamic authentication on the port

mab
<-- Enables MAB

dot1x pae authenticator
<-- Puts interface into "authenticator" mode.

end

```

Determine si se aprende una dirección MAC en la interfaz con "show mac address-table interface <interface>". La interfaz solo detecta una dirección MAC cuando se autentica correctamente.

```

<#root>
C9300#
show mac address-table interface te1/0/4

      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
50      0800.2766.efc7   STATIC  Te1/0/4

<-- The "type" is STATIC and the MAC persists until the authentication session is cleared.

Total Mac Addresses for this criterion: 1

```

Sesión de autenticación

Los comandos Show están disponibles para la validación de la autenticación 802.1x.

Utilice "show authentication sessions" o "show authentication sessions <interface>" para mostrar información sobre las sesiones de autenticación actuales. En este ejemplo, sólo Te1/0/4 tiene establecida una sesión de autenticación activa.

```

<#root>
C9300#
show authentication sessions interface te1/0/4

Interface                MAC Address      Method  Domain  Status Fg  Session ID
-----
Te1/0/4                  0800.2766.efc7  dot1x   DATA   Auth           13A37A0A0000011DC85C34C5

<-- "Method" and "Domain" in this example are dot1x and DATA, respectfully. Multi-domain authentication

```

Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker

Runnable methods list:

Handle	Priority	Name
13	5	dot1xSup
1	5	dot1x
2	10	webauth
14	15	mab

"Show authentication sessions interface <interface> details" proporciona detalles adicionales sobre una sesión de autenticación de interfaz específica.

<#root>

C9300#

show authentication session interface te1/0/4 details

```
Interface: TenGigabitEthernet1/0/4
  IIF-ID: 0x14D66776
  MAC Address: 0800.2766.efc7
  IPv6 Address: Unknown
  IPv4 Address: Unknown
  User-Name: alice
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Acct update timeout: 172800s (local), Remaining: 152363s
  Common Session ID: 13A37A0A0000011DC85C34C5
  Acct Session ID: 0x00000002
  Handle: 0xe8000015
  Current Policy: POLICY_Te1/0/4
```

<-- If a post-authentication ACL is applied, it is listed here.

Local Policies:

Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Server Policies:

Method status list:

Method	State
--------	-------


```
dot1x          Authc Success
```

```
<-- This example shows a successful 801.1x authentication session.
```

Si la autenticación está habilitada en una interfaz pero no hay ninguna sesión activa, se muestra la lista de métodos ejecutables. También se muestra "No hay sesiones que coincidan con los criterios proporcionados".

```
<#root>
```

```
C9300#
```

```
show authentication sessions interface te1/0/5
```

```
No sessions match supplied criteria.
```

```
Runnable methods list:
```

Handle	Priority	Name
13	5	dot1xSup
1	5	dot1x
2	10	webauth
14	15	mab

Si no se habilita la autenticación en la interfaz, no se detecta ninguna presencia de Auth Manager en la interfaz. También se muestra "No hay sesiones que coincidan con los criterios proporcionados".

```
<#root>
```

```
C9300#
```

```
show authentication sessions interface te1/0/6
```

```
No sessions match supplied criteria.
```

```
No Auth Manager presence on this interface
```

Accesibilidad al servidor de autenticación

El acceso al servidor de autenticación es un requisito previo para que la autenticación 802.1x se realice correctamente.

Utilice "ping <server_ip>" para realizar una prueba rápida de disponibilidad. Asegúrese de que el ping se origina en la interfaz de origen RADIUS.

```
<#root>
```

```
C9300#
```

```
ping 10.122.141.228 source vlan 1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.122.141.228, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.122.163.19
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

El comando "show aaa servers" identifica el estado del servidor y proporciona estadísticas sobre las transacciones con todos los servidores AAA configurados.

```
<#root>
```

```
C9300#
```

```
show aaa servers
```

```
RADIUS: id 3, priority 1, host 10.122.141.228, auth-port 1812, acct-port 1813, hostname DOT1x <-- Speci
```

```
State: current UP, duration 84329s, previous duration 0s <-- Current State
```

```
Dead: total time 0s, count 1
```

```
Platform State from SMD: current UP, duration 24024s, previous duration 0s
```

```
SMD Platform Dead: total time 0s, count 45
```

```
Platform State from WNCN (1) : current UP
```

```
Platform State from WNCN (2) : current UP
```

```
Platform State from WNCN (3) : current UP
```

```
Platform State from WNCN (4) : current UP
```

```
Platform State from WNCN (5) : current UP
```

```
Platform State from WNCN (6) : current UP
```

```
Platform State from WNCN (7) : current UP
```

```
Platform State from WNCN (8) : current UP, duration 0s, previous duration 0s
```

```
Platform Dead: total time 0s, count 0UP
```

```
Quarantined: No
```

```
Authen: request 510, timeouts 468, failover 0, retransmission 351 <-- Authentication Statistics
```

```
Response: accept 2, reject 2, challenge 38
```

```
Response: unexpected 0, server error 0, incorrect 12, time 21ms
```

```
Transaction: success 42, failure 117
```

```
Throttled: transaction 0, timeout 0, failure 0
```

```
Malformed responses: 0
```

```
Bad authenticators: 0
```

```
Dot1x transactions:
```

```
Response: total responses: 42, avg response time: 21ms
```

```
Transaction: timeouts 114, failover 0
```

```
Transaction: total 118, success 2, failure 116
```

```
MAC auth transactions:
```

```
Response: total responses: 0, avg response time: 0ms
```

```
Transaction: timeouts 0, failover 0
```

```
Transaction: total 0, success 0, failure 0
```

```
Author: request 0, timeouts 0, failover 0, retransmission 0
```

```
Response: accept 0, reject 0, challenge 0
```

```
Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

```
Transaction: success 0, failure 0
```

```
Throttled: transaction 0, timeout 0, failure 0
```

```
Malformed responses: 0
```

```
Bad authenticators: 0
```

```
MAC author transactions:
```

```
Response: total responses: 0, avg response time: 0ms
Transaction: timeouts 0, failover 0
Transaction: total 0, success 0, failure 0
Account: request 3, timeouts 0, failover 0, retransmission 0
Request: start 2, interim 0, stop 1
Response: start 2, interim 0, stop 1
Response: unexpected 0, server error 0, incorrect 0, time 11ms
Transaction: success 3, failure 0
Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0
Elapsed time since counters last cleared: 1d3h4m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
Consecutive Response Failures: total 115
  SMD Platform : max 113, current 0 total 113
  WNCB Platform: max 0, current 0 total 0
  IOSD Platform : max 2, current 2 total 2
Consecutive Timeouts: total 466
  SMD Platform : max 455, current 0 total 455
  WNCB Platform: max 0, current 0 total 0
  IOSD Platform : max 11, current 11 total 11
Requests per minute past 24 hours:
  high - 23 hours, 25 minutes ago: 4
  low  - 3 hours, 4 minutes ago: 0
  average: 0
```

Utilice la utilidad "test aaa" para confirmar la disponibilidad del switch al servidor de autenticación. Tenga en cuenta que esta utilidad está obsoleta y no está disponible indefinidamente.

```
<#root>
```

```
C9300#
```

```
debug radius <-- Classic Cisco IOS debugs are only useful in certain scenarios. See "Cisco IOS XE Debugs"
```

```
C9300#
```

```
test aaa group ISE username password new-code <-- This sends a RADIUS test probe to the identified server
```

```
User rejected
```

```
<-- This means that the RADIUS server received our test probe, but rejected our user. We can conclude that
```

```
*Jul 16 21:05:57.632: %PARSER-5-HIDDEN: Warning!!! ' test platform-aaa group server-group ISE user-name
*Jul 16 21:05:57.644: RADIUS/ENCODE(00000000):Orig. component type = Invalid
*Jul 16 21:05:57.644: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6 on-for
*Jul 16 21:05:57.644: RADIUS(00000000): Config NAS IP: 10.122.161.63
*Jul 16 21:05:57.644: vrfid: [65535] ipv6 tableid : [0]
*Jul 16 21:05:57.644: idb is NULL
*Jul 16 21:05:57.644: RADIUS(00000000): Config NAS IPv6: ::
*Jul 16 21:05:57.644: RADIUS(00000000): sending
*Jul 16 21:05:57.644: RADIUS/DECODE(00000000): There is no General DB. Want server details may not be s
*Jul 16 21:05:57.644: RADIUS(00000000): Send Access-Request to 10.122.141.199:1812 id 1645/8, len 50
```

```
<-- Sending Access-Request to RADIUS server
```

```
RADIUS: authenticator 3B 65 96 37 63 E3 32 41 - 3A 93 63 B6 6B 6A 5C 68
```

```
*Jul 16 21:05:57.644: RADIUS: User-Password [2] 18 *
```

```
*Jul 16 21:05:57.644: RADIUS: User-Name [1] 6 "username"
```

```
*Jul 16 21:05:57.644: RADIUS: NAS-IP-Address [4] 6 10.122.161.63
```

```
*Jul 16 21:05:57.644: RADIUS(00000000): Sending a IPv4 Radius Packet
```

```
*Jul 16 21:05:57.644: RADIUS(00000000): Started 5 sec timeout
```

```
*Jul 16 21:05:57.669: RADIUS: Received from id 1645/8 10.122.141.199:1812, Access-Reject, len 20
```

```
<-- Receiving the Access-Reject from RADIUS server
```

```
RADIUS: authenticator 1A 11 32 19 12 F9 C3 CC - 6A 83 54 DF 0F DB 00 B8
```

```
*Jul 16 21:05:57.670: RADIUS/DECODE(00000000): There is no General DB. Reply server details may not be
```

```
*Jul 16 21:05:57.670: RADIUS(00000000): Received from id 1645/8
```

Troubleshoot

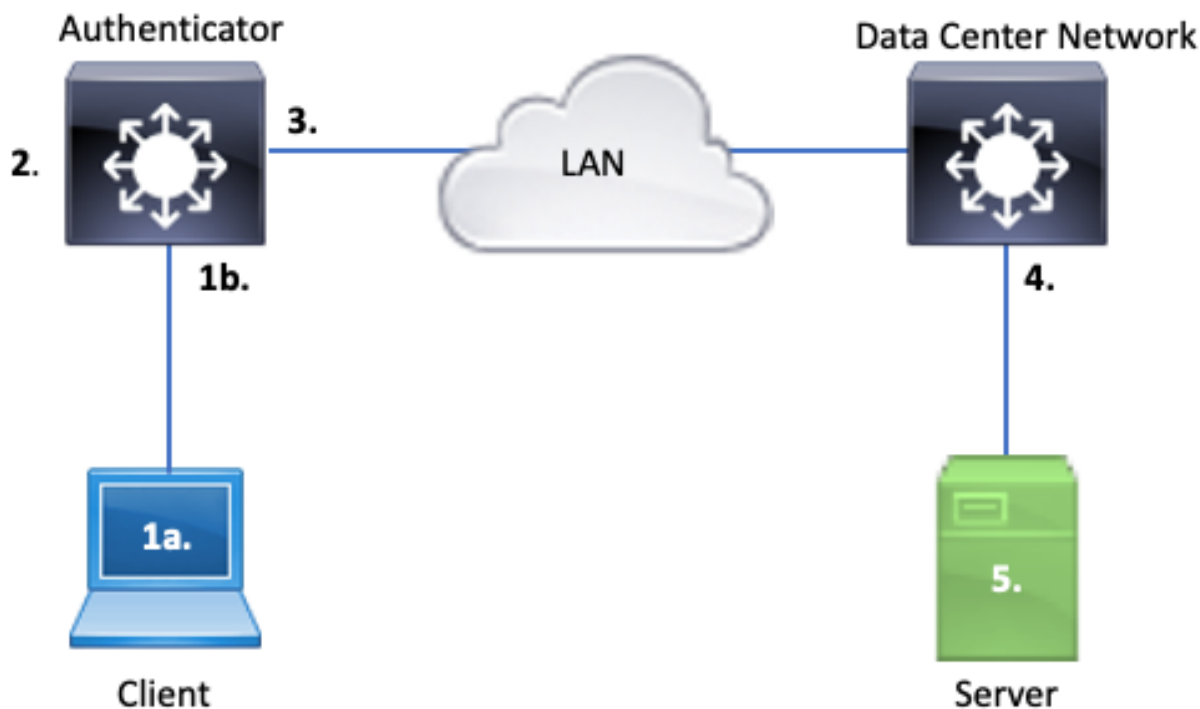
Esta sección proporciona orientación sobre cómo resolver la mayoría de los problemas de 802.1x en un switch Catalyst.

Metodología

Abordar problemas que impliquen 802.1x y autenticación metódicamente para obtener los mejores resultados. Algunas buenas preguntas a responder son:

- ¿El problema está aislado en un solo switch? ¿Un solo puerto? ¿Un único tipo de cliente?
- ¿Se ha validado la configuración? ¿Es accesible el servidor de autenticación?
- ¿Se produce la avería cada vez o es intermitente? ¿Ocurre únicamente con la reautenticación o el cambio de autorización?

Examine una única transacción fallida de extremo a extremo si persisten los problemas después de descartar lo obvio. El mejor y más completo conjunto de datos para investigar una transacción 802.1x de cliente a servidor incluye:



1 bis. Capturar en cliente y/o

1 ter. En la interfaz de acceso en la que se conecta el cliente

Este punto de referencia es crucial para darnos una idea de los paquetes EAPoL intercambiados entre el puerto de acceso donde se habilita dot1x y el cliente. SPAN es la herramienta más fiable para ver el tráfico entre el cliente y el autenticador.

2. Depuraciones en el autenticador

Las depuraciones nos permiten rastrear la transacción a través del autenticador.

- El autenticador debe colocar los paquetes EAPoL recibidos y generar tráfico encapsulado RADIUS de unidifusión destinado al servidor de autenticación.
- Asegúrese de establecer los niveles de depuración adecuados para obtener la máxima eficacia.

3. Captura adyacente al autenticador

Esta captura nos permite ver la conversación entre el autenticador y el servidor de autenticación.

- Esta captura muestra con precisión toda la conversación desde la perspectiva del autenticador.
- Cuando se empareja con la captura del punto 4, puede determinar si hay pérdida entre el Servidor de autenticación y el Autenticador.

4. Captura adyacente al servidor de autenticación

Esta captura es complementaria de la captura del punto 3.

- Esta captura proporciona la totalidad de la conversación desde la perspectiva del Servidor de autenticación.
- Cuando se empareja con la captura del punto 3, puede determinar si hay pérdida entre Authenticator y Authentication Server.

5. Capturar, depurar, registros en el servidor de autenticación

La última pieza del rompecabezas, las depuraciones del servidor, nos dicen lo que el servidor sabe sobre nuestra transacción.

- Con este conjunto integral de datos, un ingeniero de redes puede determinar dónde se interrumpe la transacción y descartar los componentes que no contribuyen al problema.

Ejemplo de síntomas

Esta sección proporciona una lista de síntomas comunes y escenarios de problemas.

- No hay respuesta del cliente

Si el tráfico EAPoL generado por el switch no genera una respuesta, se ve este syslog:

```
Aug 23 11:23:46.387 EST: %DOT1X-5-FAIL: Switch 1 R0/0: sessmgrd: Authentication failed for client (aaaa
```

El código de motivo "No Response from Client" indica que el switch ha iniciado el proceso dot1x, pero no se ha recibido ninguna respuesta del cliente dentro del período de tiempo de espera. Esto significa que el cliente no recibió o no entendió el tráfico de autenticación enviado por el puerto del switch, o que la respuesta del cliente no se recibió en el puerto del switch.

- El cliente abandona la sesión

Si se inicia una sesión de autenticación pero no se completa, el servidor de autenticación (ISE, por ejemplo) informa de que el cliente ha iniciado una sesión, pero la ha abandonado antes de completarse.

A menudo, esto significa que el proceso de autenticación sólo puede completarse parcialmente.

Asegúrese de que la transacción completa entre el switch autenticador y el servidor de autenticación se entregue de extremo a extremo y que el servidor de autenticación la interprete correctamente.

Si el tráfico RADIUS se pierde en la red, o se entrega de una manera en la que no se puede ensamblar correctamente, la transacción está incompleta y el cliente reintenta la autenticación. El servidor, a su vez, informa de que el cliente ha abandonado su sesión.

- El cliente MAB no supera DHCP y vuelve a APIPA

El desvío de autenticación MAC (MAB) permite la autenticación basada en la dirección MAC. A menudo, los clientes que no admiten el software del solicitante se autentican a través de MAB.

Si MAB se utiliza como método de reserva para la autenticación mientras dot1x es el método preferido e inicial que se ejecuta en un puerto de switch, un escenario puede resultar en que el cliente no pueda completar DHCP.

El problema se reduce al orden de las operaciones. Mientras se ejecuta dot1x, el puerto del switch consume paquetes que no sean EAPoL hasta que se completa la autenticación o se agota el tiempo de espera dot1x. Sin embargo, el cliente intenta obtener inmediatamente una dirección IP y transmite sus mensajes de detección DHCP. El puerto del switch consume estos mensajes de detección hasta que dot1x excede los valores de tiempo de espera configurados y MAB puede ejecutarse. Si el período de tiempo de espera DHCP del cliente es menor que el período de tiempo de espera dot1x, DHCP falla y el cliente recurre a APIPA o a lo que dicte su estrategia de repliegue.

Este problema se evita de varias maneras. Favorezca el MAB en las interfaces donde se conectan los clientes autenticados MAB. Si dot1x debe ejecutarse primero, tenga en cuenta el comportamiento DHCP del cliente y ajuste los valores de tiempo de espera de manera apropiada.

Tenga cuidado de considerar el comportamiento del cliente cuando se utiliza dot1x y MAB. Una configuración válida puede dar lugar a un problema técnico, como se ha descrito anteriormente.

Utilidades específicas de la plataforma

Esta sección describe muchas de las utilidades específicas de la plataforma disponibles en los switches de la familia Catalyst 9000 útiles para resolver problemas de dot1x.

- Analizador de puertos de switch (SPAN)

SPAN permite al usuario duplicar el tráfico de uno o más puertos a un puerto de destino para la captura y el análisis. SPAN local es la utilidad de captura más "fiable".

Consulte esta guía de configuración para obtener detalles sobre la configuración y la implementación:

[Configuración de SPAN y RSPAN, Cisco IOS XE Bengaluru 17.6.x \(Catalyst 9300\)](#)

- Captura de paquetes integrada (EPC)

EPC aprovecha los recursos de memoria y CPU para proporcionar capacidad de captura de paquetes local integrada.

Existen limitaciones al EPC que afectan su eficacia para investigar ciertos problemas. EPC tiene una velocidad limitada de 1000 paquetes por segundo. EPC tampoco puede capturar paquetes inyectados por la CPU de manera confiable en la salida de interfaces físicas. Esto es significativo cuando el foco está en la transacción RADIUS entre el switch autenticador y el servidor de

autenticación. A menudo, la velocidad del tráfico en la interfaz que se enfrenta al servidor supera en gran medida los 1000 paquetes por segundo. Además, un EPC en salida de interfaz que se enfrenta al servidor no puede capturar el tráfico generado por el switch autenticador.

Utilice listas de acceso bidireccionales para filtrar el EPC y evitar el impacto de la limitación de 1000 paquetes por segundo. Si está interesado en el tráfico RADIUS entre el autenticador y el servidor, céntrese en el tráfico entre la dirección de la interfaz de origen RADIUS del autenticador y la dirección del servidor.

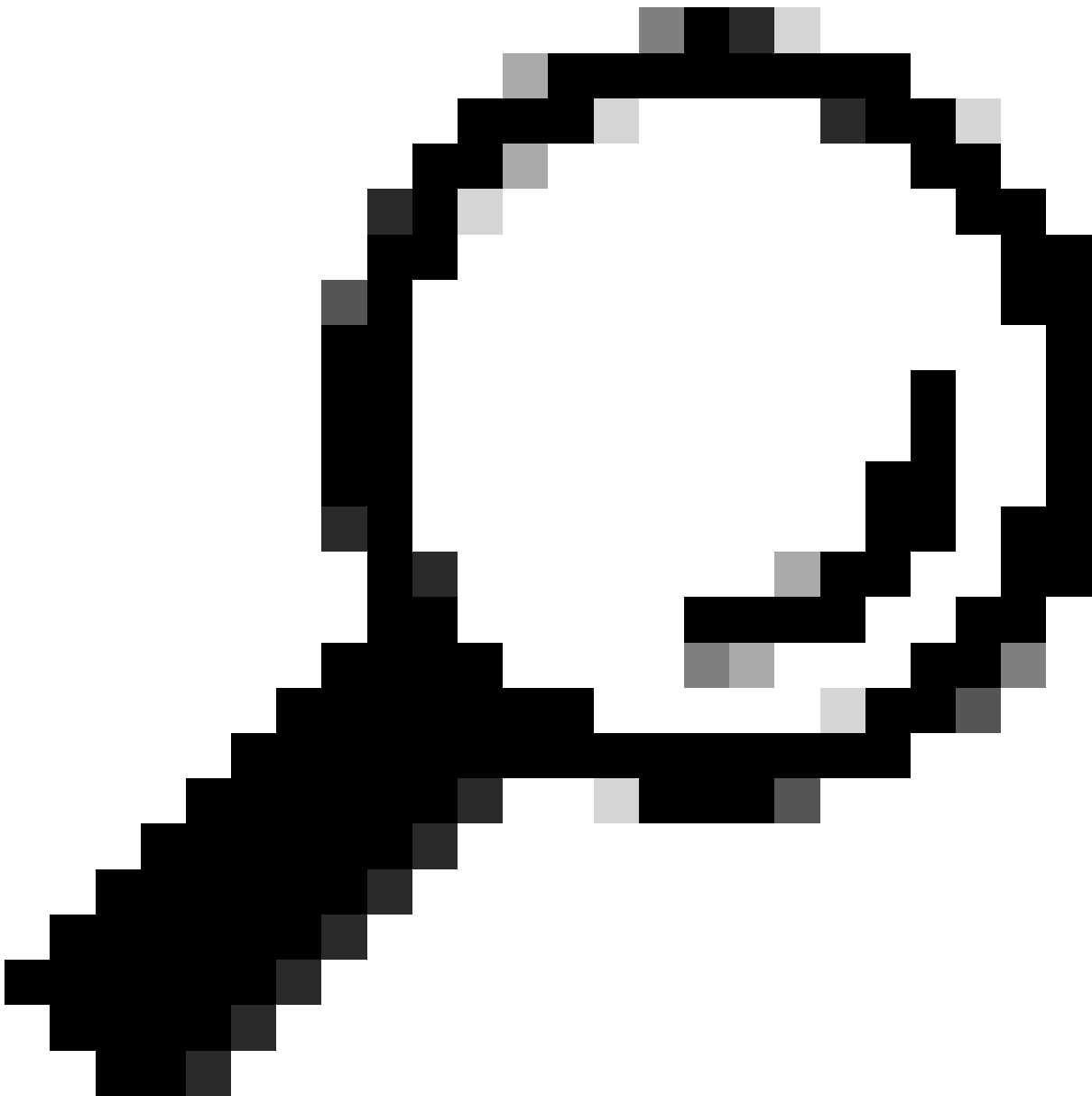
Si el siguiente dispositivo ascendente hacia el servidor de autenticación es un switch Catalyst, utilice un EPC filtrado en el enlace descendente hacia el switch autenticador para obtener los mejores resultados.

Consulte esta guía de configuración para obtener detalles sobre la configuración y la implementación:

[Configuración de la captura de paquetes, Cisco IOS Bengaluru 17.6.x \(Catalyst 9300\)](#)

- Depuraciones de Cisco IOS XE

Los cambios en la arquitectura de software que comienzan con la versión 16.3.2 de Cisco IOS XE trasladaron los componentes AAA a un demonio de Linux independiente. Los debugs familiares ya no habilitan debugs visibles en el buffer de registro. En su lugar,



Sugerencia: Las depuraciones AAA de IOS tradicionales ya no proporcionan salida en los registros del sistema para la autenticación de puertos del panel frontal dentro del búfer de syslog

Estos debugs clásicos de Cisco IOS para dot1x y RADIUS ya no habilitan debugs visibles dentro del buffer de registro del switch:

```
debug radius
debug access-session all
debug dot1x all
```

Ahora se puede acceder a las depuraciones de componentes AAA a través del seguimiento del

sistema en SMD (Session Manager Daemon).

- Al igual que los syslogs tradicionales, los seguimientos del sistema Catalyst informan a un nivel predeterminado y se les debe indicar que recopilen registros más detallados.
- Cambie el nivel de seguimiento de rutina para el subcomponente deseado con el comando "set platform software trace smd switch active r0 <component> debug".

```
<#root>
```

```
Switch#
```

```
set platform software trace smd switch active R0 auth-mgr debug
```

```
<<<--- This sets the "auth-mgr" subcomponent to "debug" log level.
```

Esta tabla asigna los debugs IOS tradicionales a su equivalente de seguimiento.

Comando de estilo antiguo	Nuevo estilo, comando
#debug RADIUS	#set platform software trace smd switch active R0 radius debug
#debug dot1x all	#set platform software trace smd switch active R0 dot1x-all debug
#debug access-session all	#set platform software trace smd switch active R0 auth-mgr-all debug
#debug epm all	#set platform software trace smd switch active R0 epm-all debug

Las depuraciones clásicas habilitan todos los seguimientos de componentes relacionados al nivel 'debug'. Los comandos de plataforma también se utilizan para habilitar seguimientos específicos según sea necesario.

Utilice el comando "show platform software trace level smd switch active R0" para mostrar el nivel de seguimiento actual para los subcomponentes SMD.

```
<#root>
```

```
Switch#
```

```
show platform software trace level smd switch active R0
```

```
Module Name                Trace Level
```

```
-----
```

```
aaa
```

```
Notice
```

```
<--- Default level is "Notice"
```

```
aaa-acct                    Notice
```

```
aaa-admin                   Notice
```

```
aaa-api                Notice
aaa-api-attr          Notice
<snip>
auth-mgr

Debug <--- Subcomponent "auth-mgr" traces at "debug" level
```

```
auth-mgr-all         Notice
<snip>
```

El nivel de seguimiento de subcomponentes se puede restaurar al valor predeterminado de dos maneras.

- Utilice "undebug all" o "set platform software trace smd switch active R0 <sub-component> Notice" para restaurar.
- Si el dispositivo se recarga, los niveles de seguimiento también se restauran a los valores predeterminados.

```
<#root>
```

```
Switch#
undebug all
```

```
All possible debugging has been turned off
```

```
or
```

```
Switch#
set platform software trace smd switch active R0 auth-mgr notice
```

```
<--- Sets sub-component "auth-mgr" to trace level "Notice", the system default.
```

Los registros de seguimiento de componentes se pueden ver en la consola o se pueden escribir para archivar y ver sin conexión. Los seguimientos se archivan en archivos binarios comprimidos que requieren decodificación. Póngase en contacto con el TAC para obtener asistencia de depuración cuando trate con rastros archivados. Este flujo de trabajo explica cómo ver los seguimientos en CLI.

Utilice el comando "show platform software trace message smd switch active R0" para ver los registros de seguimiento almacenados en la memoria para el componente SMD.

```
<#root>
```

```
Switch#
show platform software trace message smd switch active R0
```

```

2016/11/26 03:32:24.790 [auth-mgr]: [1422]: UUID: 0, ra: 0 (info): [0000.0000.0000:unknown] Auth-mgr aa
2016/11/26 03:32:29.678 [btrace]: [1422]: UUID: 0, ra: 0 (note): Single message size is greater than 10
2016/11/26 03:32:24.790 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Delay-Time [41] 6 0 RADI
2016/11/26 03:32:24.790 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1646/52 10.4
2016/11/26 03:32:24.758 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeo
2016/11/26 03:32:24.758 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radi
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Output-Packets [48] 6 0
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Input-Packets [47] 6 8
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Output-Octets [43] 6 0
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Input-Octets [42] 6 658
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Session-Time [46] 6 125
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Event-Timestamp [55] 6 148013
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Status-Type [40] 6 Stop
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 36 36 33 36 36 39 30 30 2f 33
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 68 72 65 6e 65 6b 2d 69 73 65
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 30 30 30 32 41 39 45 41 45 46
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Class [25] 63
RADIUS: 43 41 43 53 3a 30 41 30 30 30 41 46 45 30 30 30 [CACS:0A000AFE000]
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Terminate-Cause[49] 6 ad
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Authentic [45] 6 Remote
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Session-Id [44] 10 "0000
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50108
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitE
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 17 "C3850
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 10.48.44
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "0
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Called-Station-Id [30] 19 "00
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 12 "method=m
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 18
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-se
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 19 "00-50-56-99
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Framed-IP-Address [8] 6 10.0.
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 205 "cts-pac
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 211
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 95 52 40 05 8f
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Accounting-Req
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): abcdefghijklmno:NO EAP-MESSAGE
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): sending
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Config NAS IP: 10.4
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): Config for source interface found in
<snip>

```

El resultado es detallado, por lo que es útil redirigir el resultado a un archivo.

- El archivo se puede leer a través de CLI con el uso de la utilidad "more" o se puede mover fuera de línea para verlo en el editor de texto.

```
<#root>
```

```
Switch#
```

```
show platform software trace message smd switch active R0 | redirect flash:SMD_debugs.txt
```

```
Switch#more flash:SMD_debugs.txt
```

This command is being deprecated. Please use 'show logging process' command.
executing cmd on chassis 1 ...

```
2022/12/02 15:04:47.434368 {smd_R0-0}{2}: [auth-mgr] [16908]: (debug): [0800.27dd.3016:Gi2/0/11] Starte
2022/12/02 15:04:47.434271 {smd_R0-0}{2}: [auth-mgr] [16908]: (info): [0800.27dd.3016:Gi2/0/11] Account
2022/12/02 15:04:43.366688 {smd_R0-0}{2}: [auth-mgr] [16908]: (debug): [5057.a8e1.6f49:Gi2/0/11] Starte
2022/12/02 15:04:43.366558 {smd_R0-0}{2}: [auth-mgr] [16908]: (info): [5057.a8e1.6f49:Gi2/0/11] Account
2022/12/02 15:01:03.629116 {smd_R0-0}{2}: [smd] [16908]: (warn): Setting trace for 52:7
2022/12/02 15:00:19.350560 {smd_R0-0}{2}: [smd] [16908]: (warn): Setting trace for 52:7
2022/12/02 01:28:39.841376 {smd_R0-0}{2}: [auth-mgr] [16908]: (ERR): [0000.0000.0000:unknown] sm ctx un
<snip>
```

"Show logging process" es la utilidad actualizada para los seguimientos y el estándar en la versión Cisco IOS XE 17.9.x y posterior.

<#root>

C9300#

show logging process smd ?

```
<0-25>          instance number
end             specify log filtering end location
extract-pcap   Extract pcap data to a file
filter        specify filter for logs
fru           FRU specific commands
internal      select all logs. (Without the internal keyword only
              customer curated logs are displayed)
level         select logs above specific level
metadata      CLI to display metadata for every log message
module        select logs for specific modules
reverse       show logs in reverse chronological order
start         specify log filtering start location
switch        specify switch number
to-file        decode files stored in disk and write output to file
trace-on-failure show the trace on failure summary
|             Output modifiers
```

"Show logging process" proporciona la misma funcionalidad que "show platform software trace" en un formato más elegante y accesible.

<#root>

C9300#

clear auth sessions

C9300#

show logging process smd reverse

Logging display requested on 2023/05/02 16:44:04 (UTC) for Hostname: [C9300], Model: [C9300X-24HX], Ver

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis 1 ...

```
=====
UTM [LUID NOT FOUND] ..... 0
UTM [PCAP] ..... 0
UTM [MARKER] ..... 0
UTM [APP CONTEXT] ..... 0
UTM [TDL TAN] ..... 5
UTM [MODULE ID] ..... 0
UTM [DYN LIB] ..... 0
UTM [PLAIN TEXT] ..... 6
UTM [ENCODED] ..... 85839
UTM [Skipped / Rendered / Total] .. 85128 / 722 / 85850
Last UTM TimeStamp ..... 2023/05/02 16:44:03.775663010
First UTM TimeStamp ..... 2023/05/02 15:52:18.763729918
=====
```

----- Decoder Output Information -----

```
=====
MRST Filter Rules ..... 1
UTM Process Filter ..... smd
Total UTM To Process ... 85850
Total UTF To Process ... 1
Num of Unique Streams .. 1
=====
```

----- Decoder Input Information -----

===== Unified Trace Decoder Information/Statistics =====

```
=====
2023/05/02 16:44:03.625123675 {smd_R0-0}{1}: [radius] [22624]: (ERR): Failed to mark Identifier for reu
2023/05/02 16:44:03.625123382 {smd_R0-0}{1}: [radius] [22624]: (ERR): RSPE- Set Identifier Free for Re
2023/05/02 16:44:03.625116747 {smd_R0-0}{1}: [radius] [22624]: (info): Valid Response Packet, Free the
2023/05/02 16:44:03.625091040 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: authenticator 2b f4 ea
2023/05/02 16:44:03.625068520 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Received from id 1813/9
2023/05/02 16:44:03.610151863 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Started 5 sec timeout
2023/05/02 16:44:03.610097362 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Acct-Delay-Time [41
2023/05/02 16:44:03.610090044 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Event-Timestamp [55
2023/05/02 16:44:03.610085857 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Acct-Status-Type [40
2023/05/02 16:44:03.610040912 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Class [25
2023/05/02 16:44:03.610037444 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Acct-Authentic [45
2023/05/02 16:44:03.610032802 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Acct-Session-Id [44
2023/05/02 16:44:03.610028677 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Called-Station-Id [30
2023/05/02 16:44:03.610024641 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Nas-Identifier [32
2023/05/02 16:44:03.610020641 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Calling-Station-Id [31
2023/05/02 16:44:03.610016809 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: NAS-Port [5]
2023/05/02 16:44:03.610012487 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: NAS-Port-Type [61
2023/05/02 16:44:03.610007504 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: NAS-Port-Id [87
2023/05/02 16:44:03.610003581 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: NAS-IP-Address [4]
2023/05/02 16:44:03.609998136 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Calling-Station-Id [31
2023/05/02 16:44:03.609994109 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Called-Station-Id [30
2023/05/02 16:44:03.609989329 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Cisco AVpair [1]
2023/05/02 16:44:03.609985171 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Vendor, Cisco [26
2023/05/02 16:44:03.609981606 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Cisco AVpair [1]
2023/05/02 16:44:03.609976961 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Vendor, Cisco [26
2023/05/02 16:44:03.609969166 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: User-Name [1]
2023/05/02 16:44:03.609963241 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: authenticator 0b 99 e3
2023/05/02 16:44:03.609953614 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Send Accounting-Request
2023/05/02 16:44:03.609863172 {smd_R0-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Handl
2023/05/02 16:44:03.609695649 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAPOL pa
2023/05/02 16:44:03.609689224 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:unknown] Pkt body
2023/05/02 16:44:03.609686794 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAP Pack
2023/05/02 16:44:03.609683919 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Sent EAP
```

```
2023/05/02 16:44:03.609334292 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Sending
2023/05/02 16:44:03.609332867 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Setting
2023/05/02 16:44:03.609310820 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Posting
2023/05/02 16:44:03.609284841 {smd_R0-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Raisi
```

Ejemplos de seguimiento

Esta sección incluye seguimientos del administrador de sesiones para los componentes dot1x y radius para una transacción completa fallida (el servidor rechaza las credenciales del cliente). Su objetivo es proporcionar una guía básica para navegar por los seguimientos del sistema relacionados con la autenticación del panel frontal.

- Un cliente de prueba intenta conectarse a GigabitEthernet1/0/2 y se rechaza.

En este ejemplo, los seguimientos de componentes SMD se establecen en "debug".

```
<#root>
```

```
C9300#
```

```
set platform software trace smd sw active r0 dot1x-all
```

```
C9300#
```

```
set platform software trace smd sw active r0 radius debug
```

EAPoL: INICIO

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPoL pkt (size=92) on 12 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] queuing an EAPoL pkt on Auth Q
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 0,TYPE= 0,LEN= 0
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Couldn't find the supplicant in the 1
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] New client detected, sending session
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: initialising
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: disconnected
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering restart
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Sending create new context event to E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering init state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering idle state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Created a client entry (0x0A00000E)
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Dot1x authentication started for 0x0A0
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting !EAP_RESTART on Client 0x0A0
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enter connecting state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: restart connecting
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RX_REQ on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: authenticating state ent
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:connecting authenticating
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_START for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state
```

EAPoL: IDENTIDAD DE SOLICITUD EAP

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:idle request action
```

EAPoL: RESPUESTA EAP

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on 12 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL pkt on Authenticator
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 2,TYPE= 1,LEN= 14
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering response state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to the server from 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:request response action
[aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick method list 'default'
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.28.99.147 for Radius
[radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifier "C9300"
[aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: SOLICITUD DE ACCESO

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 59 c9 e0 be 4d b5 1c 11 - 02 cb 5b eb
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
0e 01 69 78 69 61 5f 64 61 74 61 [ ixia_data]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 16
69 87 3c 61 80 3a 31 a8 73 2b 55 76 f4 [ Ei<a:1s+Uv]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```


RADIUS: DESAFÍO DE ACCESO

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/82 172.28.99.252:0, Access-Cha
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014 RADIUS: authenticator 82 71 61
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
RADIUS: 01 f9 00 06 0d 20 [ ]
02/15 14:01:28.986 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 8
RADIUS: 78 66 ec be 2c a4 af 79 5e ec c6 47 8b da 6a c2 [ xf,y^Gj]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 11, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/82
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_REQ for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state###
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response request action
```

EAPoL: RESPUESTA EAP

```
02/15 14:01:28.988 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pk
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL p
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enteri
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to t
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:reques
02/15 14:01:28.989 [aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick met
02/15 14:01:28.990 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.
02/15 14:01:28.990 [radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifler "C
02/15 14:01:28.990 [aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: SOLICITUD DE ACCESO

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 3d 31 3f ee 14 b8 9d 63 - 7a 8b 52 90
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
RADIUS: 02 f9 00 06 03 04
02/15 14:01:28.991 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 8
```

```
RADIUS: 8b 2a 2e 75 90 a2 e1 c9 06 84 c9 fe f5 d0 98 39 [ *.u9]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```

RADIUS: DESAFÍO DE ACCESO

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/83 172.28.99.252:0, Access-Cha
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 0c 8d 49 80 0f 51 89 fa - ba 22 2f 96
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
RADIUS: 01 fa 00 21 04 10 5b d0 b6 4e 68 37 6b ca 5e 6f 5a 65 78 04 77 bf 69 73 65 2d [![Nh7k^oZexwise-
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 35
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 70 6f 6c 2d 65 73 63 [ pol-esc]
RADIUS: a3 0d b0 02 c8 32 85 2c 94 bd 03 b3 22 e6 71 1e [ 2,"q]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 11, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/83
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_REQ for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state
```

EAPoL: SOLICITUD EAP

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response request action
```

EAPoL: RESPUESTA EAP

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on 12 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL pkt on Authenticator
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 2,TYPE= 4,LEN= 31
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering response state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to the server from 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:request response action
[aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick method list 'default'
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.28.99.147 for Radius
[radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifier "C9300"
[aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: SOLICITUD DE ACCESO

```
radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645 i
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 41 4d 76 8e 03 93 9f 05 - 5e fa f1 d6
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
RADIUS: 02 fa 00 1f 04 10 02 b6 bc aa f4 91 2b d6 cf 9e 3b d5 44 96 78 d5 69 78 69 61 5f 64 61 74 61 [
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 33
RADIUS: 3b 70 b1 dd 97 ac 47 ae 81 ca f8 78 5b a3 7b fe [ ;pGx[{}
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```

RADIUS: ACCESO RECHAZADO

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/84 172.28.99.252:0, Access-Rej
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator d1 a3 eb 43 11 45 6b 8f - 07 a7 34 dd
RADIUS: 04 fa 00 04
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 6
```

```

RADIUS: 80 77 07 f7 4d f8 a5 60 a6 b0 30 e4 67 85 ae ba [ wM`0g]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 3, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/84
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Received an EAP Fail
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_FAIL for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering fail state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response fail action
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering idle state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_FAIL on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting authenticating state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering authc result state
[errmsg]: [16498]: UUID: 0, ra: 0 (note): %DOT1X-5-FAIL: Authentication failed for client (0040.E93E.0000:Gi1/0/2)
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Added username in dot1x
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Dot1x did not receive any key data
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Received Authz fail (result: 2) for t
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting_AUTHZ_FAIL on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: held

```

EAPoL: RECHAZO DE EAP

```

[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting FAILOVER_RETRY on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: exiting held state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering restart
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Sending create new context event to E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:restart action called
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RESTART on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting !EAP_RESTART on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enter connecting state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: restart connecting
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RX_REQ on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: authenticating state ent
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:connecting authenticating
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_START for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state

```

Additional Information

Configuración predeterminada

Función	Configuración predeterminada
Estado de activación del switch 802.1x	Inhabilitado.

Función	Configuración predeterminada
Estado de activación de 802.1x por puerto	Desactivado (autorizado por la fuerza). El puerto envía y recibe tráfico normal sin autenticación del cliente basada en 802.1x.
AAA	Inhabilitado.
servidor RADIUS <ul style="list-style-type: none"> • Dirección IP • puerto de autenticación UDP • Puerto de contabilidad predeterminado • Clave 	<ul style="list-style-type: none"> • No se ha especificado ninguno. • 1645. • 1646. • No se ha especificado ninguno.
Modo de host	Modo de host único.
Dirección de control	Control bidireccional.
Reautenticación periódica	Inhabilitado.
Número de segundos entre intentos de reautenticación	3600 segundos.
Número de reautenticación	2 veces (número de veces que el switch reinicia el proceso de autenticación antes de que el puerto cambie al estado no autorizado).
Período tranquilo	60 segundos (número de segundos que el switch permanece en el estado silencioso después de un intercambio de autenticación fallido con el cliente).
Tiempo de retransmisión	30 segundos (número de segundos que el switch espera una respuesta a una solicitud EAP/trama de identidad del cliente antes de reenviar la solicitud).

Función	Configuración predeterminada
Número máximo de retransmisión	2 veces (número de veces que el switch envía una trama de solicitud/identidad EAP antes de reiniciar el proceso de autenticación).
Tiempo de espera del cliente	30 segundos (cuando se transmite una solicitud del servidor de autenticación al cliente, la cantidad de tiempo que el switch espera una respuesta antes de volver a enviar la solicitud al cliente).
Periodo de tiempo de espera del servidor de autenticación	<p>30 segundos (cuando se transmite una respuesta del cliente al servidor de autenticación, la cantidad de tiempo que el switch espera una respuesta antes de volver a enviar la respuesta al servidor).</p> <p>Puede cambiar este período de tiempo de espera mediante el comando de configuración <code>dot1x timeout server-timeout interface</code>.</p>
Tiempo de inactividad	Inhabilitado.
VLAN de invitado	No se ha especificado ninguno.
Omisión de autenticación inaccesible	Inhabilitado.
VLAN restringida	No se ha especificado ninguno.
Modo de autenticador (switch)	No se ha especificado ninguno.
derivación de autenticación MAC	Inhabilitado.
Seguridad con reconocimiento de voz	Inhabilitado.

Configuración opcional

Reautenticación periódica

Puede habilitar la reautenticación periódica de clientes 802.1x y especificar la frecuencia con que ocurre:

- `authentication periodic` - habilita la reautenticación periódica del cliente
- `inactividad`: intervalo en segundos tras el cual, si no hay actividad del cliente, no se autoriza
- `reauthenticate`: tiempo en segundos después del cual se inicia un intento automático de reautenticación
- `restartvalue`: intervalo en segundos tras el cual se intenta autenticar un puerto no autorizado
- `unauthorizedvalue`: intervalo en segundos tras el cual se elimina una sesión no autorizada

```
authentication periodic
authentication timer {[inactivity | reauthenticate | restart | unauthorized]} {value}}
```

Modos de infracción

Puede configurar un puerto 802.1x para que se apague, genere un error de syslog o descarte paquetes de un nuevo dispositivo cuando un dispositivo se conecta a un puerto habilitado para 802.1x o se haya autenticado el número máximo de dispositivos permitidos en el puerto.

- `shutdown`: error al deshabilitar el puerto.
- `restrict`: genera un error de syslog.
- `protect`: descarta paquetes de cualquier dispositivo nuevo que envíe tráfico al puerto.
- `replace`: elimina la sesión actual y se autentica con el nuevo host.

```
authentication violation {shutdown | restrict | protect | replace}
```

Cambio del Período Tranquilo

El comando de configuración de interfaz `authentication timer restart` controla el período inactivo, que determina el período de tiempo establecido en el que el switch permanece inactivo después de que un switch no puede autenticar al cliente. El intervalo para el valor es de 1 a 65535 segundos.

```
authentication timer restart {seconds}
```

Cambio del Tiempo de Retransmisión de Switch a Cliente

El cliente responde a la trama de solicitud/identidad EAP desde el switch con una trama de identidad/respuesta EAP. Si el switch no recibe esta respuesta, espera un período de tiempo establecido (conocido como el tiempo de retransmisión) y luego reenvía la trama.

```
authentication timer reauthenticate {seconds}
```

Configuración del Número de Retransmisión de Trama de Switch a Cliente

Puede cambiar el número de veces que el switch envía una trama de solicitud/identidad EAP (suponiendo que no se reciba ninguna respuesta) al cliente antes de reiniciar el proceso de autenticación. El rango va de 1 a 10.

```
dot1x max-reauth-req {count}
```

Configuración del Modo Host

Puede permitir varios hosts (clientes) en un puerto autorizado 802.1x.

- multi-auth: permite varios clientes autenticados en la VLAN de voz y la VLAN de datos.
- multi-host: permite varios hosts en un puerto autorizado 802.1x después de que se haya autenticado un único host.
- multidominio: permite autenticar un host y un dispositivo de voz, como un teléfono IP (de Cisco o no), en un puerto autorizado por IEEE 802.1x.

```
authentication host-mode [multi-auth | multi-domain | multi-host | single-host]
```

Activación de MAC Move

El movimiento de MAC permite que un host autenticado se mueva de un puerto del dispositivo a otro.

```
authentication mac-move permit
```

Activación de MAC Replace

La sustitución de MAC permite que un host sustituya a un host autenticado en un puerto.

- protect - el puerto descarta paquetes con direcciones MAC inesperadas sin generar un mensaje del sistema.
- restrict - la CPU descarta los paquetes infractores y se genera un mensaje del sistema.
- shutdown - el puerto es error disabled cuando recibe una dirección MAC inesperada.

```
authentication violation {protect | replace | restrict | shutdown}
```

Configuración del número de reautenticación

También puede cambiar el número de veces que el dispositivo reinicia el proceso de autenticación antes de que el puerto cambie al estado no autorizado. El rango es 0 a 10

```
dot1x max-req {count}
```

Configuración de una VLAN de invitado

Cuando configura una VLAN de invitado, los clientes que no son compatibles con 802.1x se colocan en la VLAN de invitado cuando el servidor no recibe una respuesta a su trama de solicitud/identidad EAP.

```
authentication event no-response action authorize vlan {vlan-id}
```

Configuración de una VLAN restringida

Cuando configura una VLAN restringida en un dispositivo, los clientes que cumplen con IEEE 802.1x se mueven a la VLAN restringida cuando el servidor de autenticación no recibe un nombre de usuario y contraseña válidos.

```
authentication event fail action authorize vlan {vlan-id}
```

Configuración del Número de Intentos de Autenticación en una VLAN Restringida

Puede configurar el número máximo de intentos de autenticación permitidos antes de que un usuario se asigne a la VLAN restringida mediante el comando de configuración authentication

event fail retry retry. El rango de intentos de autenticación permitidos es de 1 a 3.

```
authentication event fail retry {retry count}
```

Configuración del Bypass de Autenticación Inaccesible 802.1x con VLAN de Voz Crítica

Puede configurar una VLAN de voz crítica en un puerto y habilitar la función de omisión de autenticación inaccesible.

- autorizar: mueva cualquier nuevo host que intente autenticarse a la VLAN crítica especificada por el usuario
- reinitialize - Mueva todos los hosts autorizados en el puerto a la VLAN crítica especificada por el usuario

```
authentication event server dead action {authorize | reinitialize} vlanvlan-id]
authentication event server dead action authorize voice
```

Configuración de la Autenticación 802.1x con WoL

Puede habilitar la autenticación 802.1x con Wake on LAN (WoL)

```
authentication control-direction both
```

Configuración de MAC Authentication Bypass

```
mab
```

Configuración de pedidos de autenticación flexible

```
authentication order [ dot1x | mab ] | {webauth}
authentication priority [ dot1x | mab ] | {webauth}
```

Configuración de la seguridad 802.1x con reconocimiento de voz

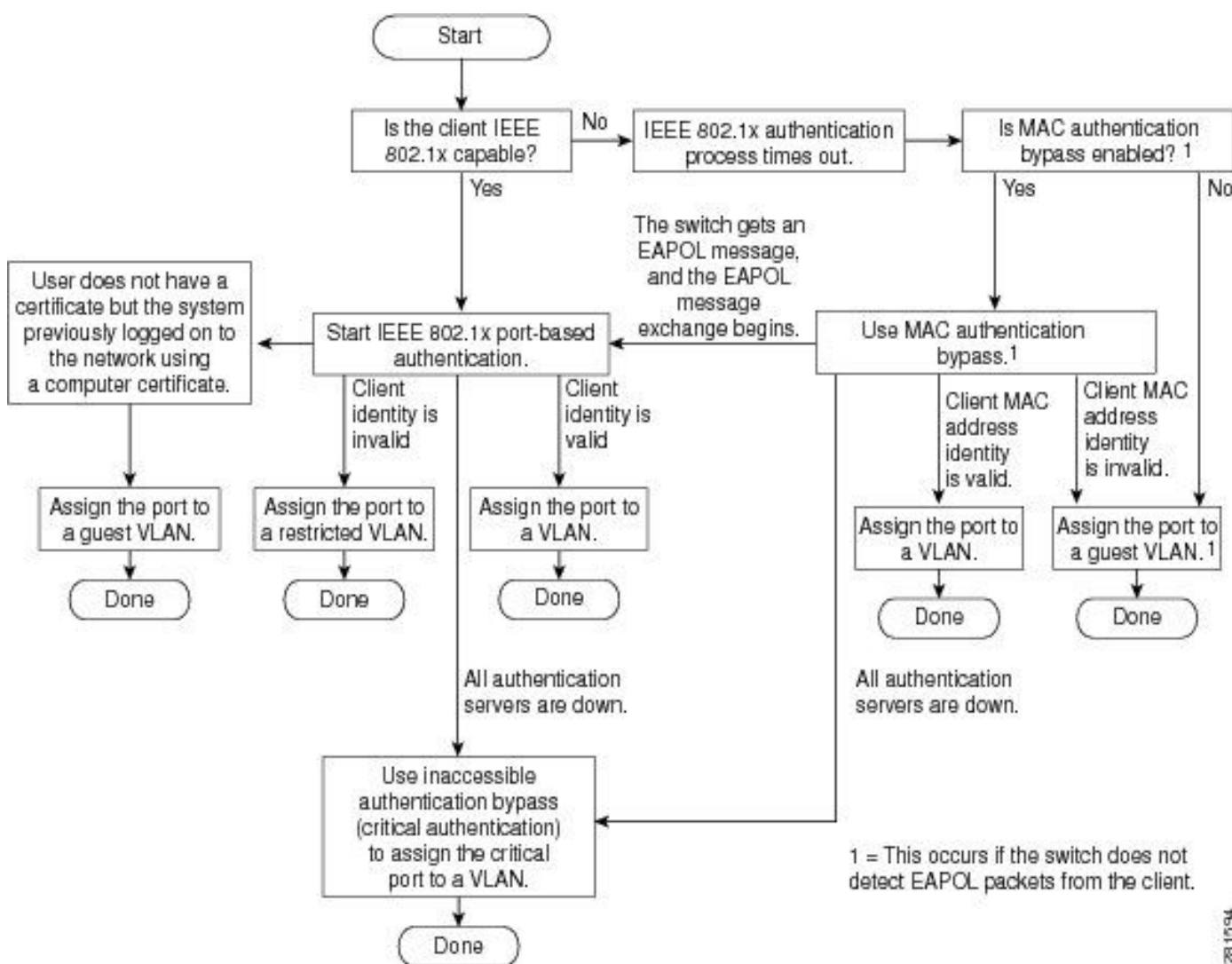
La función de seguridad 802.1x con reconocimiento de voz se utiliza en el dispositivo para deshabilitar solo la VLAN en la que se produce una violación de seguridad, ya sea una VLAN de

datos o de voz. Una violación de seguridad encontrada en la VLAN de datos resulta en el cierre de solamente la VLAN de datos. Esta es una configuración global.

```
errdisable detect cause security-violation shutdown vlan
errdisable recovery cause security-violation
```

Diagrama de flujo

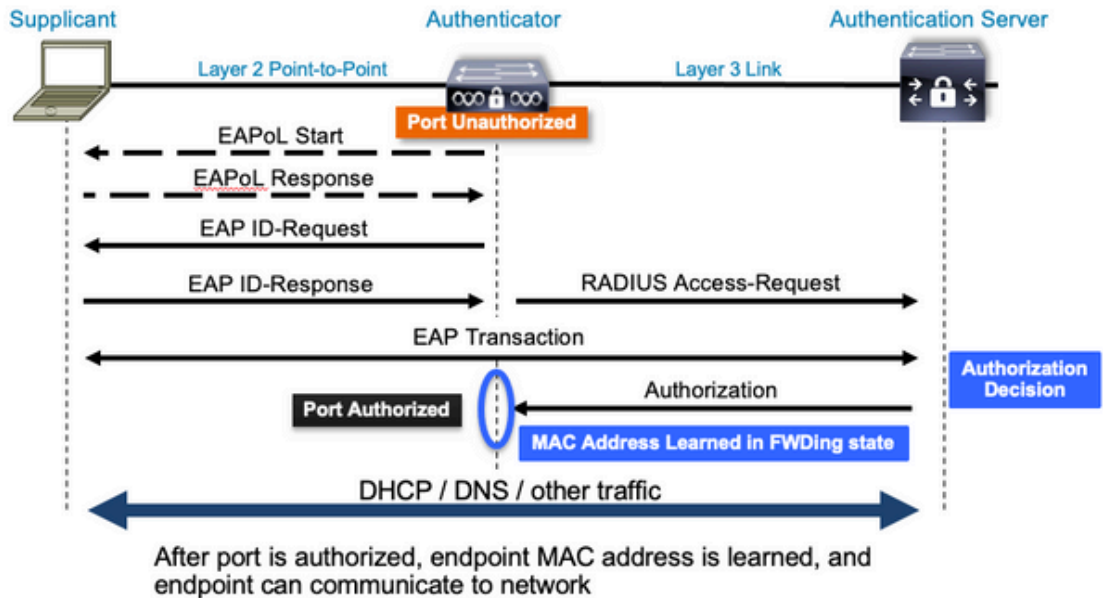
Diagrama de autenticación



Iniciación de autenticación basada en puerto e intercambio de mensajes

Esta figura muestra el cliente que inicia el intercambio de mensajes con el servidor RADIUS.

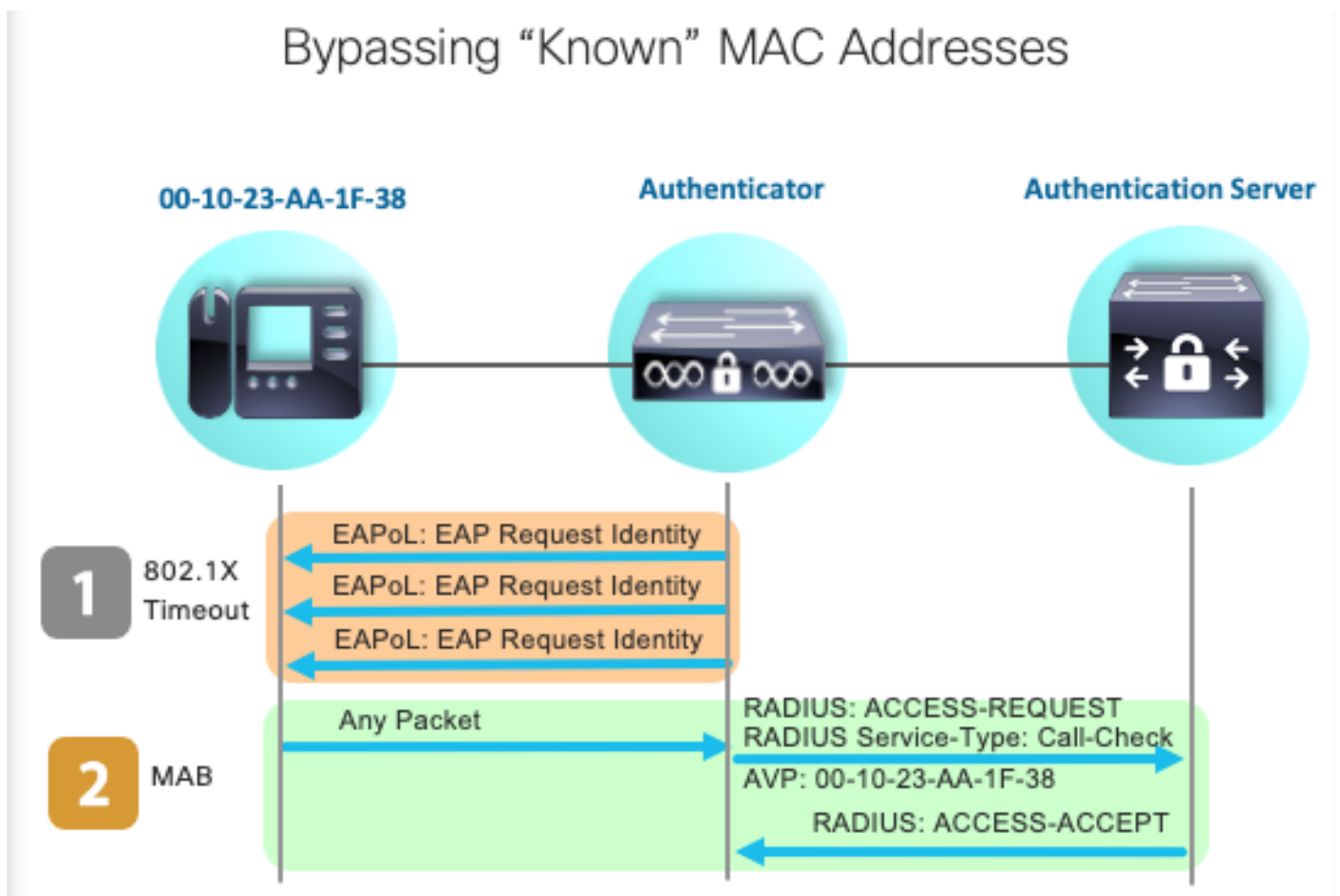
802.1X Message Exchange



Iniciación de autenticación MAB e intercambio de mensajes

Esta figura muestra el intercambio de mensajes durante la omisión de autenticación MAC (MAB)

Bypassing "Known" MAC Addresses



Información Relacionada

- [Desmitificación de Configuraciones de Servidor RADIUS](#)
- [Guía de implementación de derivación de autenticación MAC](#)
- [Guía de implementación de 802.1x por cable](#)
- [Guía de Configuración de Catalyst 9300 SPAN](#)
- [Guía de configuración de Catalyst 9300 EPC](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).