

Identificar e Solucionar Problemas do Dot1x nos Catalyst 9000 Series Switches

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração básica](#)

[Verificar configuração e operações](#)

[Introdução ao 802.1x](#)

[Configuração](#)

[Sessão de autenticação](#)

[Acessibilidade ao Servidor de Autenticação](#)

[Troubleshooting](#)

[Metologia](#)

[Exemplo de sintomas](#)

[Utilitários específicos da plataforma](#)

[Exemplos de rastreamento](#)

[Informações adicionais](#)

[Configurações padrão](#)

[Configurações opcionais](#)

[Fluxogramas](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar, validar e solucionar problemas do controle de acesso à rede (NAC) 802.1x nos switches da série Catalyst 9000.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos.


- Catalyst 9000 Series Switches
- Identity services engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

 Observação: consulte o guia de configuração apropriado para obter os comandos usados para habilitar esses recursos em outras plataformas Cisco.

Informações de Apoio

O padrão 802.1x define um protocolo de autenticação e controle de acesso baseado em cliente-servidor que impede que clientes não autorizados se conectem a uma LAN através de portas publicamente acessíveis, a menos que sejam autenticados corretamente. O servidor de autenticação autentica cada cliente conectado a uma porta de switch antes de disponibilizar quaisquer serviços oferecidos pelo switch ou pela LAN.


A autenticação 802.1x envolve 3 componentes distintos:

Requerente - Cliente que envia credenciais para autenticação

Autenticador - O dispositivo de rede que fornece conectividade de rede entre o cliente e a rede e pode permitir ou bloquear o tráfego de rede.

Servidor de autenticação — O servidor que pode receber e responder a solicitações de acesso à rede informa ao autenticador se a conexão pode ser permitida e várias outras configurações que se aplicariam à sessão de autenticação.

O público-alvo deste documento são os engenheiros e a equipe de suporte que não estão necessariamente focados na segurança. Para obter mais informações sobre a autenticação baseada em porta 802.1x e componentes como o ISE, consulte o guia de configuração apropriado.

 Observação: consulte o guia de configuração apropriado para sua plataforma e versão de código específicas para obter a configuração de autenticação padrão 802.1x mais precisa.

Configuração básica

Esta seção descreve a configuração básica necessária para implementar a autenticação baseada em porta 802.1x. Uma explicação adicional sobre o recurso pode ser encontrada na guia de adendos deste documento. Há pequenas variações nos padrões de configuração de versão para versão. Valide sua configuração em relação ao guia de configuração da versão atual.

A autenticação, a autorização e a conta (AAA) devem ser habilitadas antes da configuração da autenticação 802.1x pós-baseada, e uma lista de métodos deve ser estabelecida.

- As listas de métodos descrevem a sequência e o método de autenticação a serem consultados para autenticar um usuário.
- 802.1x também deve ser habilitado 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
```

Definir um servidor RADIUS no 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
```

Ative 802.1x na interface do 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 configuração e operações

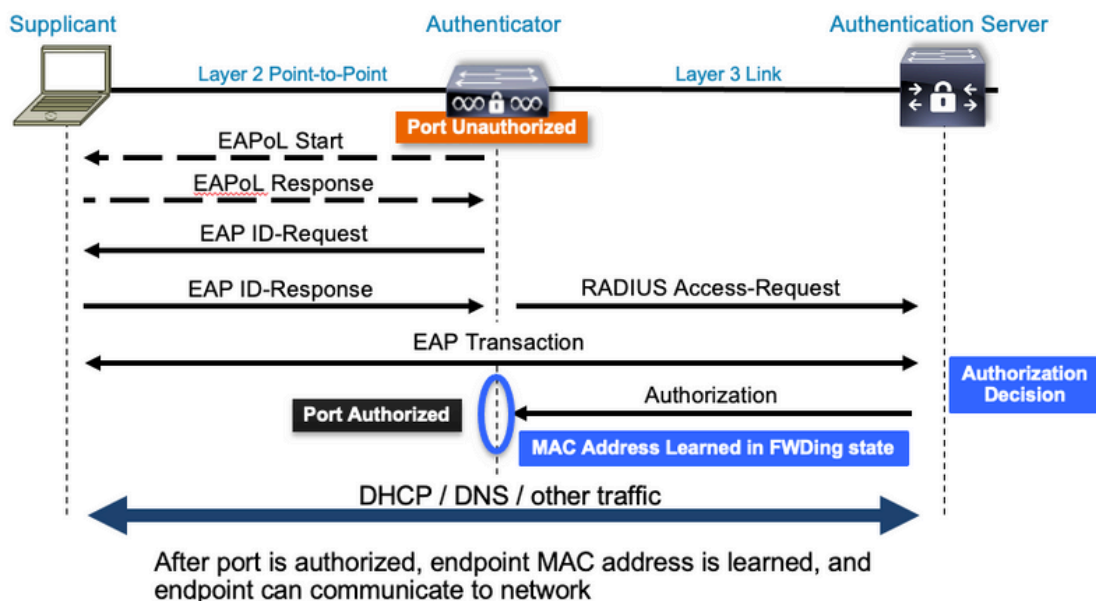
Esta seção fornece informações básicas sobre 802.1x e como verificar a configuração e as operações.

Introdução ao 802.1x

O 802.1x envolve dois tipos distintos de tráfego: tráfego de Cliente para Autenticador (ponto a ponto) sobre EAPoL (Extensible Authentication Protocol over LAN) e tráfego de Autenticador para Servidor de Autenticação que é encapsulado via RADIUS.

Este diagrama representa o fluxo de dados para uma transação dot1x simples

802.1X Message Exchange



O Autenticador (switch) e o Servidor de Autenticação (ISE, por exemplo) são frequentemente separados pela Camada 3. O tráfego RADIUS é roteado pela rede entre o autenticador e o servidor. O tráfego EAPoL é trocado no link direto entre o suplicante (cliente) e o autenticador.

Observe que o aprendizado de MAC ocorre após a autenticação e a autorização.

Aqui estão algumas perguntas a serem lembradas quando você aborda um problema que envolve 802.1x:

- Ele está configurado corretamente?
- O servidor de autenticação está acessível?
- Qual é o status do Authentication Manager?
- Há algum problema com a entrega de pacotes entre o cliente e o autenticador ou entre o autenticador e o servidor de autenticação?

Configuração

Algumas configurações variam um pouco entre as principais versões. Consulte o guia de configuração relevante para obter orientações específicas de plataforma/código.

O AAA deve ser configurado para utilizar a autenticação baseada em porta 802.1x.

- Uma lista de métodos de autenticação deve ser estabelecida para "dot1x". Isso representa uma configuração AAA comum onde 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 é um exemplo de configuração de interface em que 802.1x está habilitado. MAB (MAC Authentication Bypass) é um método de backup comum para autenticar clientes que não suportam suplicantes dot1x.

```
<#root>
```

```

C9300#

show running-config interface te1/0/4

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 se um endereço MAC é aprendido na interface com "show mac address-table interface <interface>". A interface só aprende um endereço MAC quando autenticada com êxito.

```

<#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

```

Sessão de autenticação

Os comandos show estão disponíveis para validação da autenticação 802.1x.

Use "show authentication sessions" ou "show authentication sessions <interface>" para exibir informações sobre as sessões de autenticação atuais. Neste exemplo, apenas Te1/0/4 tem uma sessão de autenticação ativa estabelecida.

```

<#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" fornece detalhes adicionais sobre uma sessão de autenticação de interface 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.

Se a autenticação estiver habilitada em uma interface e ainda não houver uma sessão ativa, a lista de métodos executáveis será exibida. "Nenhuma sessão corresponde aos critérios fornecidos" também é exibido.

```
<#root>
```

```
C9300#
```

```
show authentication sessions interface tel1/0/5
```

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

```
Runnable methods list:
```

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

Se nenhuma autenticação estiver habilitada na interface, nenhuma presença do Auth Manager será detectada na interface. "Nenhuma sessão corresponde aos critérios fornecidos" também é exibido.

```
<#root>
```

```
C9300#
```

```
show authentication sessions interface tel1/0/6
```

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

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

Acessibilidade ao Servidor de Autenticação

A acessibilidade ao Servidor de autenticação é um pré-requisito para o sucesso da autenticação 802.1x.

Use "ping <server_ip>" para um teste rápido de acessibilidade. Certifique-se de que o ping tenha origem na interface de origem 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

O comando "show aaa servers" identifica o estado do servidor e fornece estatísticas sobre transações com todos os 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 0
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
```

Use o utilitário "test aaa" para confirmar a acessibilidade do switch ao servidor de autenticação. Observe que esse utilitário foi preterido e não está disponível 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
```

Troubleshooting

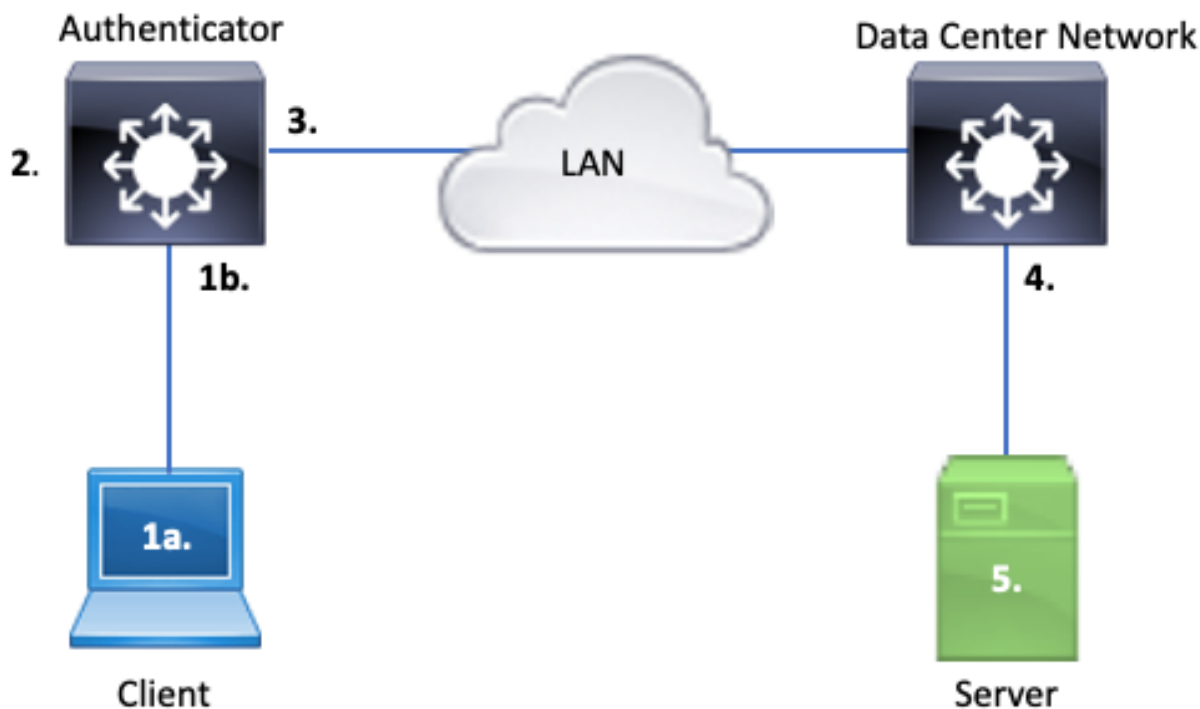
Esta seção fornece orientação sobre como solucionar a maioria dos problemas de 802.1x em um switch Catalyst.

Metologia

Aborde problemas que envolvem 802.1x e a autenticação metodicamente para obter melhores resultados. Algumas boas perguntas para responder são:

- O problema é isolado a um único switch? Uma única porta? Um único tipo de cliente?
- A configuração foi validada? O servidor de autenticação está acessível?
- O problema ocorre sempre ou é intermitente? Isso ocorre somente com reautenticação ou alteração de autorização?

Examine uma única transação com falha de ponta a ponta se os problemas persistirem após a exclusão óbvia. O melhor e mais completo conjunto de dados para investigação de uma transação 802.1x de cliente para servidor inclui:



1-A. Capturar no cliente e/ou

1-B. Na interface de acesso onde o cliente se conecta

Esse ponto de referência é crucial para nos dar uma ideia dos pacotes EAPoL trocados entre a porta de acesso onde o dot1x está habilitado e o cliente. O SPAN é a ferramenta mais confiável para visualizar o tráfego entre o cliente e o autenticador.

2. Depurações no autenticador

As depurações nos permitem rastrear a transação pelo autenticador.

- O autenticador deve apontar os pacotes EAPoL recebidos e gerar tráfego encapsulado em RADIUS unicast destinado ao servidor de autenticação.
- Certifique-se de que os níveis de depuração apropriados estejam definidos para máxima eficácia.

3. Capturar adjacente ao autenticador

Essa captura nos permite ver a conversa entre o Authenticator e o servidor de Autenticação.

- Essa captura exhibe com precisão toda a conversa da perspectiva do Authenticator.
- Quando emparelhado com a captura no ponto 4, você pode determinar se há perda entre o Servidor de autenticação e o Authenticator.

4. Capturar adjacente ao servidor de autenticação

Esta captura é um complemento da captura mencionada no ponto 3.

- Essa captura fornece toda a conversa da perspectiva do Servidor de autenticação.
- Quando emparelhado com a captura no ponto 3, você pode determinar se há perda entre o Authenticator e o Authentication Server.

5. Capturar, depurar, registrar no servidor de autenticação

A parte final do quebra-cabeça, as depurações de servidor nos dizem o que o servidor sabe sobre nossa transação.

- Com esse conjunto completo de dados, um engenheiro de rede pode determinar onde a transação é interrompida e descartar os componentes que não contribuem para o problema.

Exemplo de sintomas

Esta seção fornece uma lista de sintomas comuns e cenários de problemas.

- Sem resposta do cliente

Se o tráfego EAPoL gerado pelo switch não obter uma resposta, este syslog será visto:

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

O código de razão "No Response from Client" indica que o switch iniciou o processo dot1x, mas nenhuma resposta foi recebida do cliente dentro do período de timeout.

Isso significa que o cliente não recebeu ou entendeu o tráfego de autenticação enviado pela porta do switch ou que a resposta do cliente não foi recebida na porta do switch.

- Sessão de Abandonos do Cliente

Se uma sessão de autenticação for iniciada, mas não for concluída, o Servidor de autenticação (ISE, por exemplo) informará que o cliente iniciou uma sessão, mas abandonou a sessão antes da conclusão.

Frequentemente, isso significa que o processo de autenticação pode ser concluído apenas parcialmente.

Verifique se a transação inteira entre o switch autenticador e o servidor de autenticação é entregue de ponta a ponta e é interpretada corretamente pelo servidor de autenticação.

Se o tráfego RADIUS for perdido na rede, ou entregue de uma maneira em que ele não possa ser montado corretamente, a transação estará incompleta e o cliente tentará novamente a autenticação. O servidor, por sua vez, relata que o cliente abandonou sua sessão.

- Cliente MAB falha DHCP/retorna para APIPA

O MAC Authentication Bypass (MAB) permite a autenticação com base no endereço MAC. Frequentemente, os clientes que não suportam software suplicante autenticam-se através do MAB.

Se MAB for usado como um método de fallback para autenticação enquanto dot1x for o método preferencial e inicial executado em uma porta de switch, um cenário potencialmente resultará em um cenário em que o cliente não pode concluir o DHCP.

O problema resume-se à ordem das operações. Enquanto o dot1x é executado, a porta do switch consome pacotes diferentes de EAPoL até que a autenticação seja concluída ou o dot1x expire. O cliente, no entanto, tenta imediatamente obter um endereço IP e transmite suas mensagens de descoberta DHCP. Essas mensagens de descoberta são consumidas pela porta do switch até que o dot1x exceda seus valores de tempo limite configurados e o MAB possa ser executado. Se o intervalo de DHCP do cliente for menor que o intervalo de dot1x, o DHCP falhará e o cliente retornará ao APIPA ou a qualquer estratégia de recuo que ele determinar.

Esse problema é evitado de várias maneiras. Priorize o MAB nas interfaces onde os clientes autenticados MAB se conectam. Se dot1x precisar ser executado primeiro, tenha em mente o comportamento DHCP do cliente e ajuste os valores de tempo limite apropriadamente.

Tenha cuidado ao considerar o comportamento do cliente quando dot1x e MAB são usados. Uma configuração válida pode levar a um problema técnico, conforme descrito acima.

Utilitários específicos da plataforma

Esta seção descreve muitos dos utilitários específicos de plataforma disponíveis na família de switches Catalyst 9000 úteis para solucionar problemas de dot1x.

- Analisador de porta do switch (SPAN)

O SPAN permite que o usuário espelhe o tráfego de uma ou mais portas para uma porta de destino para captura e análise. O SPAN local é o utilitário de captura mais 'confiável'.

Consulte este guia de configuração para obter detalhes sobre configuração e implementação:

[Configurando SPAN e RSPAN, Cisco IOS XE Bengaluru 17.6.x \(Catalyst 9300\)](#)

- Captura de pacotes incorporada (EPC)

O EPC aproveita os recursos de CPU e memória para fornecer capacidade de captura de pacote local na placa.

Existem limitações ao EPC que afetam a sua eficácia na investigação de certos problemas. O EPC tem taxa limitada de 1000 pacotes por segundo. O EPC também não pode capturar com segurança pacotes injetados na CPU na saída de interfaces físicas. Isso é significativo quando o foco está na transação RADIUS entre o switch autenticador e o servidor de autenticação. Frequentemente, a taxa de tráfego na interface que enfrenta o servidor excede em muito 1000 pacotes por segundo. Além disso, um EPC na saída da interface voltada para o servidor não consegue capturar o tráfego gerado pelo switch autenticador.

Use listas de acesso bidirecionais para filtrar o EPC para evitar o impacto da limitação de 1000 pacotes por segundo. Se estiver interessado no tráfego RADIUS entre o autenticador e o servidor, concentre-se no tráfego entre o endereço da interface de origem RADIUS do autenticador e o endereço do servidor.

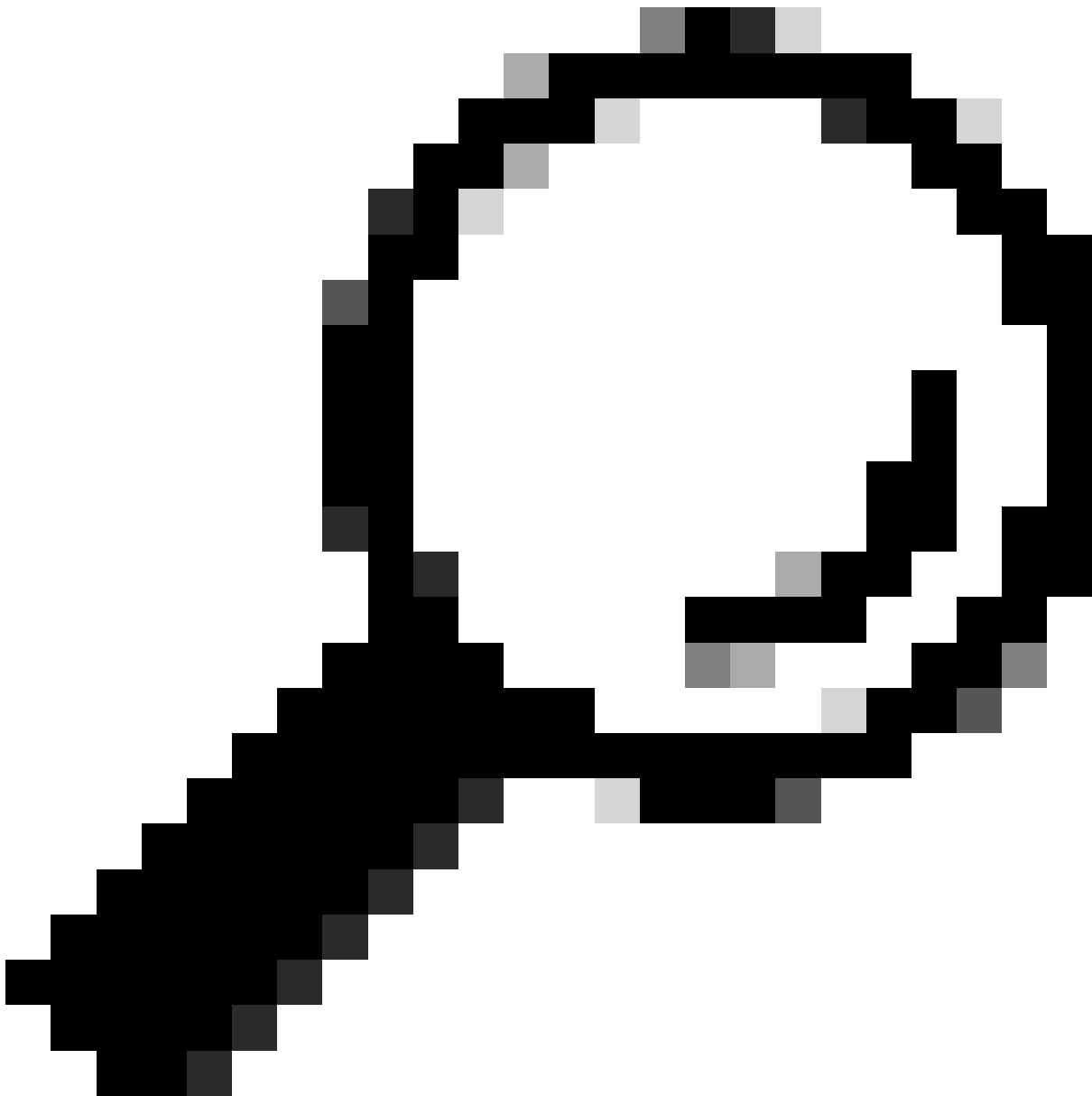
Se o próximo dispositivo upstream em direção ao servidor de autenticação for um switch Catalyst, use um EPC filtrado no downlink em direção ao switch autenticador para obter melhores resultados.

Consulte este guia de configuração para obter detalhes sobre configuração e implementação:

[Configurando a captura de pacotes, Cisco IOS Bengaluru 17.6.x \(Catalyst 9300\)](#)

- Depurações do Cisco IOS XE

Alterações na arquitetura de software que começam com o Cisco IOS XE versão 16.3.2 transferiram componentes AAA para um daemon Linux separado. As depurações familiares não permitem mais depurações visíveis no buffer de registro. Em vez disso,



Dica: as depurações tradicionais de AAA do IOS não fornecem mais saída nos logs do sistema para autenticação de porta do painel frontal dentro do buffer do syslog

Essas depurações clássicas do Cisco IOS para dot1x e RADIUS não permitem mais depurações visualizáveis dentro do buffer de registro do switch:

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

As depurações do componente AAA agora podem ser acessadas através do rastreamento do sistema no SMD (Session Manager Daemon).

- Como os syslogs tradicionais, o sistema Catalyst rastreia os relatórios em um nível padrão e deve ser instruído a coletar logs mais detalhados.
- Altere o nível de rastreamento de rotina para o subcomponente desejado com o 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 tabela mapeia as depurações tradicionais do IOS para seu equivalente de rastreamento.

Comando de estilo antigo	Comando Novo estilo
raio de #debug	#set software da plataforma 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	#set platform software trace smd switch active R0 epm-all debug

As depurações clássicas habilitam todos os rastreamentos de componentes relacionados para o nível 'debug'. Comandos de plataforma também são usados para ativar rastreamentos específicos, conforme necessário.

Use o comando "show platform software trace level smd switch active R0" para mostrar o nível de rastreamento atual para 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>
```

O nível de rastreamento do subcomponente pode ser restaurado para o padrão de duas maneiras.

- Use "undebug all" ou "set platform software trace smd switch active R0 <sub-component> notice" para restaurar.
- Se o dispositivo for recarregado, os níveis de rastreamento também serão restaurados para o padrão.

```
<#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.
```

Os logs de rastreamento de componentes podem ser exibidos no console ou gravados no arquivo e exibidos offline. Os rastreamentos são arquivados em arquivos binários zipados que exigem decodificação. Entre em contato com o TAC para obter assistência de depuração ao lidar com rastreamentos arquivados. Este fluxo de trabalho explica como exibir os rastreamentos no CLI.

Use o comando "show platform software trace message smd switch active R0" para exibir os logs de rastreamento armazenados na memória para o 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>

```

A saída é detalhada, portanto, é útil redirecioná-la para o arquivo.

- O arquivo pode ser lido via CLI com o uso do utilitário "more" ou movido offline para visualização no 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" é o utilitário atualizado para rastreamentos e o padrão na versão do Cisco IOS XE 17.9.x e posteriores.

```
<#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

```

O "Show logging process" fornece a mesma funcionalidade do "show platform software trace" em um formato mais elegante e acessível.

```
<#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

Exemplos de rastreamento

Esta seção inclui rastreamentos do gerenciador de sessão para componentes dot1x e radius para uma transação completa que falhou (o servidor rejeita as credenciais do cliente). Ele tem como objetivo fornecer uma diretriz básica para navegar pelos rastreamentos do sistema relacionados à autenticação do painel frontal.

- Um cliente de teste tenta se conectar a GigabitEthernet1/0/2 e é rejeitado.

Neste exemplo, os rastreamentos de componentes SMD são definidos como "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: INICIAR

```
[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: IDENTIDADE DE SOLICITAÇÃO 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: RESPOSTA EAP

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on 12
[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: SOLICITAÇÃO DE ACESSO

```
[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: DESAFIO DE ACESSO

```
[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: RESPOSTA 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-Identifier "C
02/15 14:01:28.990 [aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: SOLICITAÇÃO DE ACESSO

```
[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: DESAFIO DE ACESSO

```
[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: SOLICITAÇÃO 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: RESPOSTA 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: SOLICITAÇÃO DE ACESSO

```
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 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: REJEIÇÃO DE ACESSO

```
[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: EAP REJECT

```

[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

```

Informações adicionais

Configurações padrão

Recurso	Definição padrão
Estado de ativação do switch 802.1x	Desabilitado.
Estado de ativação 802.1x por porta	Desabilitado (autorizado pela força). A porta envia e recebe tráfego normal sem autenticação do cliente

Recurso	Definição padrão
	baseada em 802.1x.
AAA	Desabilitado.
servidor RADIUS <ul style="list-style-type: none"> • Endereço IP • Porta de autenticação UDP • Porta contábil padrão • Chave 	<ul style="list-style-type: none"> • Nenhum especificado. • 1645. • 1646. • Nenhum especificado.
Modo de host	Modo de host único.
Direção do controle	Controle bidirecional.
Reautenticação periódica	Desabilitado.
Número de segundos entre tentativas de reautenticação	3600 segundos.
Número de reautenticação	2 vezes (número de vezes que o switch reinicia o processo de autenticação antes que a porta mude para o estado não autorizado).
Período silencioso	60 segundos (número de segundos que o switch permanece no estado silencioso após uma falha na troca de autenticação com o cliente).
Tempo de retransmissão	30 segundos (número de segundos que o switch aguarda por uma resposta a uma solicitação EAP/quadro de identidade do cliente antes de reenviar a solicitação).
Número máximo de retransmissão	2 vezes (número de vezes que o switch envia um quadro de solicitação/identidade EAP antes de reiniciar o processo de autenticação).

Recurso	Definição padrão
Período de tempo limite do cliente	30 segundos (ao retransmitir uma solicitação do servidor de autenticação para o cliente, o tempo que o switch aguarda por uma resposta antes de reenviar a solicitação ao cliente.)
Período de tempo limite do servidor de autenticação	30 segundos (ao retransmitir uma resposta do cliente para o servidor de autenticação, a quantidade de tempo que o switch espera por uma resposta antes de reenviar a resposta para o servidor.) Você pode alterar esse período de timeout usando o comando de configuração de interface dot1x timeout server-timeout.
Tempo limite de inatividade	Desabilitado.
VLAN de convidado	Nenhum especificado.
Desvio de autenticação inacessível	Desabilitado.
VLAN restrita	Nenhum especificado.
Modo autenticador (switch)	Nenhum especificado.
Desvio de autenticação MAC	Desabilitado.
Segurança com reconhecimento de voz	Desabilitado.

Configurações opcionais

Reautenticação periódica

Você pode ativar a reautenticação periódica do cliente 802.1x e especificar a frequência com que ela ocorre:

- autenticação periódica - permite a reautenticação periódica do cliente

- inatividade — Intervalo em segundos após o qual, se não houver atividade do cliente, ele não será autorizado
- reauthenticate — Tempo em segundos após o qual uma tentativa de reautenticação automática é iniciada
- restartvalue — Intervalo em segundos após o qual é feita uma tentativa de autenticar uma porta não autorizada
- unauthorized value— Intervalo em segundos após o qual uma sessão não autorizada é excluída

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

Modos de violação

Você pode configurar uma porta 802.1x para que ela seja desativada, gere um erro de syslog ou descarte pacotes de um novo dispositivo quando um dispositivo se conecta a uma porta habilitada para 802.1x ou quando o número máximo de dispositivos permitidos sobre foi autenticado na porta.

- shutdown- Erro ao desativar a porta.
- restrict- Gera um erro de syslog.
- protect- Descarte os pacotes de qualquer novo dispositivo que envie tráfego para a porta.
- replace- Remove a sessão atual e autentica com o novo host.

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

Alterando o Período Silencioso

O comando de configuração de interface `authentication timer restart` controla o período ocioso, que determina o período de tempo definido em que o switch permanece ocioso depois que um switch não pode autenticar o cliente. O intervalo do valor é de 1 a 65535 segundos.

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

Alteração do tempo de retransmissão do switch para o cliente

O cliente responde ao quadro de solicitação/identidade EAP do switch com um quadro de resposta/identidade EAP. Se o switch não receber essa resposta, ele espera um período de tempo definido (conhecido como tempo de retransmissão) e, em seguida, reenvia o quadro.

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

Definindo o número de retransmissão de quadro do switch para o cliente

Você pode alterar o número de vezes que o switch envia um quadro de solicitação/identidade EAP (supondo que nenhuma resposta seja recebida) ao cliente antes de reiniciar o processo de autenticação. O intervalo é 1 a 10.

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

Configurando o modo de host

Você pode permitir vários hosts (clientes) em uma porta autorizada 802.1x.

- multi-auth- Permite vários clientes autenticados na VLAN de voz e na VLAN de dados.
- multi-host- Permite vários hosts em uma porta autorizada 802.1x após a autenticação de um único host.
- multi-domain- Permite que um host e um dispositivo de voz, como um telefone IP (Cisco ou não Cisco), sejam autenticados em uma porta autorizada IEEE 802.1x.

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

Ativando a movimentação do MAC

A movimentação de MAC permite que um host autenticado se mova de uma porta no dispositivo para outra.

```
authentication mac-move permit
```

Habilitando Substituição de MAC

A substituição de MAC permite que um host substitua um host autenticado em uma porta.

- protect - a porta descarta pacotes com endereços MAC inesperados sem gerar uma mensagem de sistema.
- restrict - os pacotes violadores são descartados pela CPU e uma mensagem do sistema é gerada.
- shutdown - a porta é desativada por erro quando recebe um endereço MAC inesperado.

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

Definindo o número de reautenticação

Você também pode alterar o número de vezes que o dispositivo reinicia o processo de autenticação antes que a porta mude para o estado não autorizado. O intervalo é 0 a 10

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

Configurando uma VLAN de convidado

Quando você configura uma VLAN de convidado, os clientes que não são compatíveis com 802.1x são colocados na VLAN de convidado quando o servidor não recebe uma resposta ao seu quadro de solicitação/identidade EAP.

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

Configurando uma VLAN restrita

Quando você configura uma VLAN restrita em um dispositivo, os clientes compatíveis com IEEE 802.1x são movidos para a VLAN restrita quando o servidor de autenticação não recebe um nome de usuário e uma senha válidos.

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

Configurando o número de tentativas de autenticação em uma VLAN restrita

Você pode configurar o número máximo de tentativas de autenticação permitidas antes de um usuário ser atribuído à VLAN restrita usando o comando de configuração de interface `authentication event fail retry count interface`. O intervalo de tentativas de autenticação permitidas

é de 1 a 3.

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

Configurando o desvio de autenticação inacessível 802.1x com VLAN de voz crítica

Você pode configurar uma VLAN de voz crítica em uma porta e ativar o recurso de desvio de autenticação inacessível.

- authorized - Mova todos os novos hosts que tentam se autenticar para a VLAN crítica especificada pelo usuário
- reinicializar - Mover todos os hosts autorizados na porta para a VLAN crítica especificada pelo usuário

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

Configurando a autenticação 802.1x com WoL

Você pode habilitar a autenticação 802.1x com Wake on LAN (WoL)

```
authentication control-direction both
```

Configurando o desvio de autenticação MAC

```
mab
```

Configurando pedidos de autenticação flexível

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

Configurando a segurança 802.1x com reconhecimento de voz

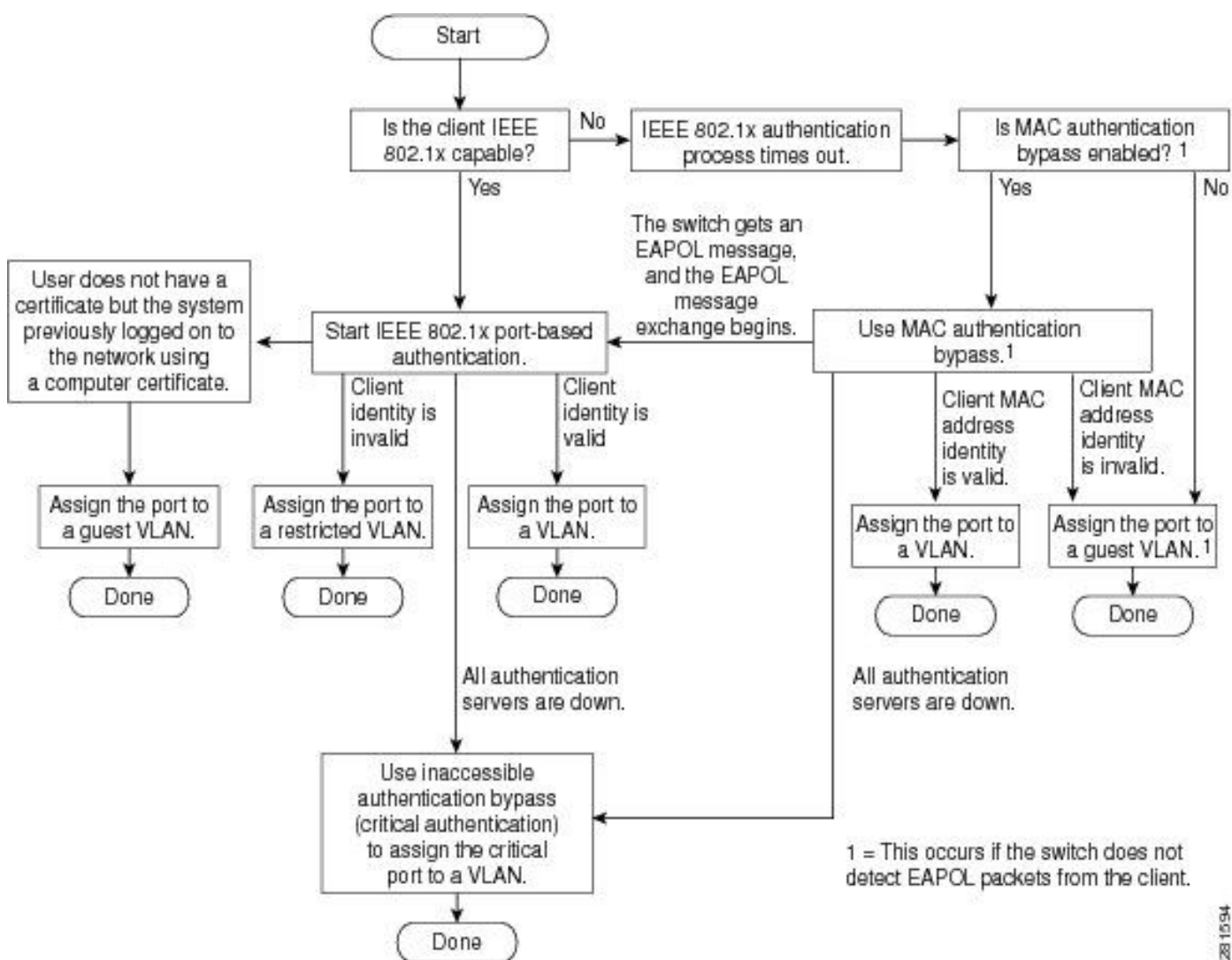
Você usa o recurso de segurança 802.1x com reconhecimento de voz no dispositivo para desativar apenas a VLAN na qual ocorre uma violação de segurança, seja ela uma VLAN de

dados ou de voz. Uma violação de segurança encontrada na VLAN de dados resulta no desligamento somente da VLAN de dados. Esta é uma configuração global.

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

Fluxogramas

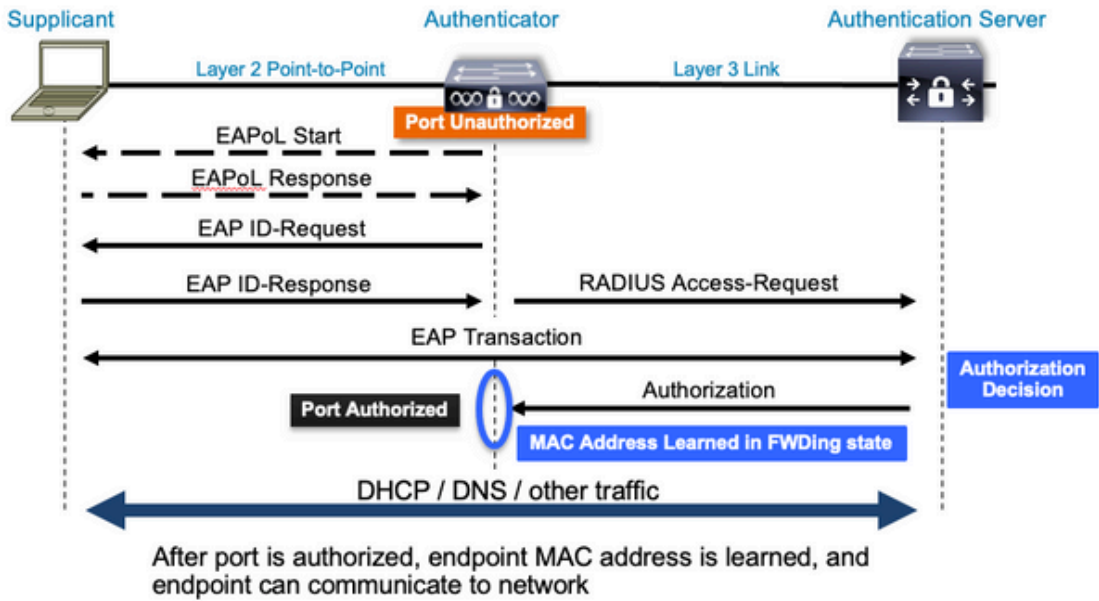
Fluxograma de autenticação



Iniciação de autenticação baseada em porta e troca de mensagens

Esta figura mostra o cliente iniciando a troca de mensagens para o servidor RADIUS.

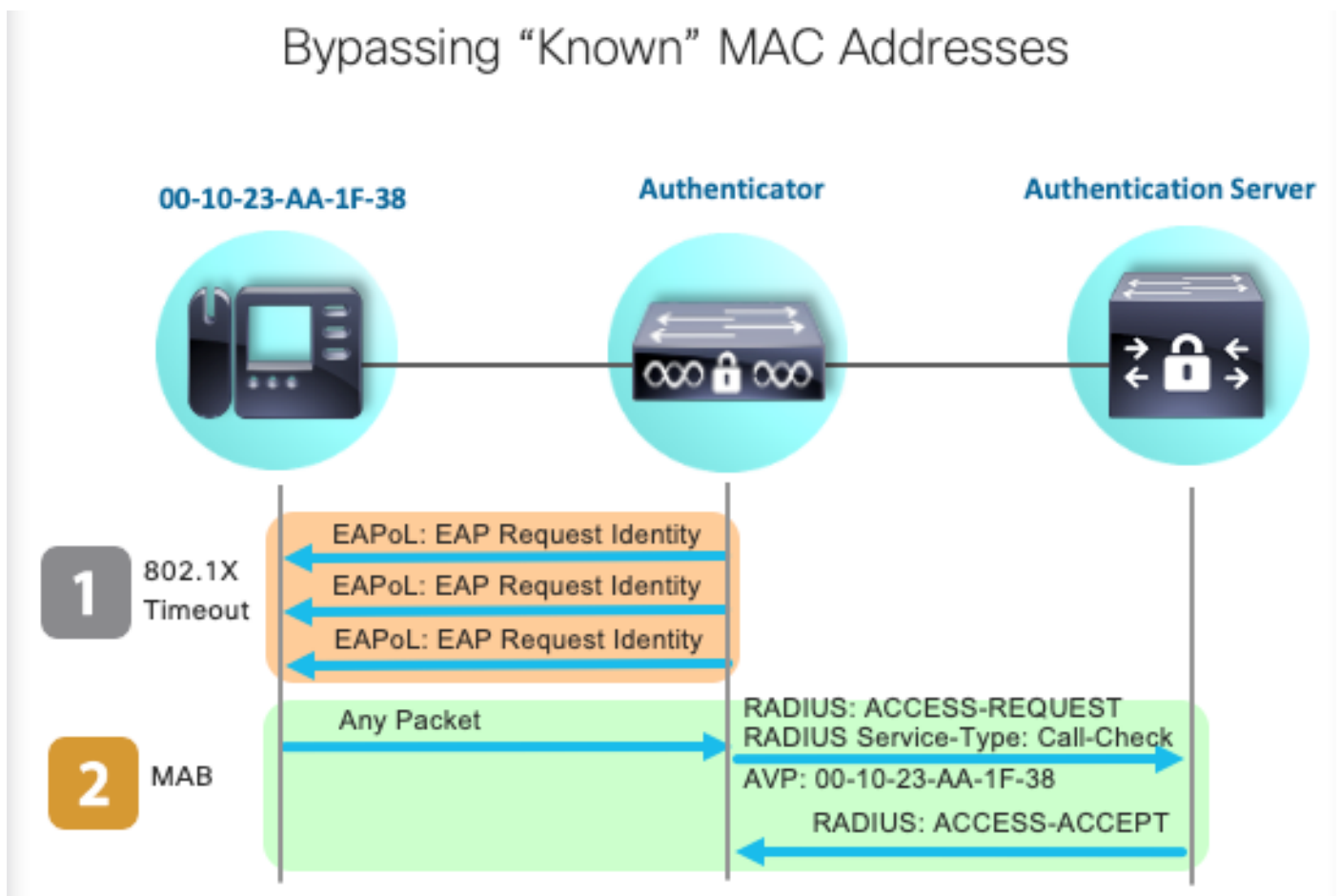
802.1X Message Exchange



Iniciação de autenticação MAB e troca de mensagens

Esta figura mostra a troca de mensagens durante o desvio de autenticação MAC (MAB)

Bypassing "Known" MAC Addresses



Informações Relacionadas

- [Desmistificando as configurações do servidor RADIUS](#)
- [Guia de implantação de desvio de autenticação MAC](#)
- [Guia de implantação 802.1x com fio](#)
- [Guia de configuração de SPAN do Catalyst 9300](#)
- [Guia de configuração do Catalyst 9300 EPC](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.