

# Catalyst 9000シリーズスイッチのDot1xのトラブルシューティング

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[基本設定](#)

[設定と動作の確認](#)

[802.1xの概要](#)

[コンフィギュレーション](#)

[認証セッション](#)

[認証サーバへの到達可能性](#)

[トラブルシューティング](#)

[方法](#)

[症状の例](#)

[プラットフォーム固有の利点](#)

[トレースの例](#)

[追加情報](#)

[デフォルト設定](#)

[オプション設定](#)

[フローチャート](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Catalyst 9000シリーズスイッチでの802.1xネットワークアクセスコントロール(NAC)の設定、検証、およびトラブルシューティングの方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Catalyst 9000 シリーズ スイッチ
- Identity Services Engine ( ISE )


## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.6.x以降
- ISE-VM-K9バージョン3.0.0.458

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

---

 注：シスコの他のプラットフォームでこれらの機能を有効にするために使用されるコマンドについては、該当するコンフィギュレーションガイドを参照してください。

---

## 背景説明

802.1x標準は、クライアントサーバベースのアクセス制御と認証プロトコルを定義し、正しく認証されない限り、許可されていないクライアントが、一般にアクセス可能なポートを通じてLANに接続するのを防ぎます。認証サーバは、スイッチポートに接続された各クライアントを認証してから、スイッチまたはLANによって提供されるサービスを利用できるようにします。

802.1x認証には、3つの個別のコンポーネントが必要です。


サブリカント：認証のためにクレデンシャルを送信するクライアント

オーセンティケータ：クライアントとネットワークの間のネットワーク接続を提供し、ネットワークトラフィックを許可またはブロックできるネットワークデバイス。

認証サーバ：ネットワークアクセスの要求を受信して応答できるサーバであり、接続を許可できるかどうか、および認証セッションに適用されるその他のさまざまな設定をオーセンティケータに指示します。

このドキュメントの対象読者は、必ずしもセキュリティに重点を置いていないエンジニアおよびサポート担当者です。802.1xポートベース認証およびISEなどのコンポーネントの詳細については、該当するコンフィギュレーションガイドを参照してください。

---

 注：最も正確なデフォルトの802.1x認証設定については、使用しているプラットフォームおよびコードのバージョンに該当するコンフィギュレーションガイドを参照してください。

---

## 基本設定

このセクションでは、802.1xポートベース認証の実装に必要な基本設定について説明します。そ

の他の機能の説明は、このドキュメントの「付録」タブに記載されています。バージョンによって、設定標準にわずかな違いがあります。現在のバージョンの構成ガイドに照らして構成を検証します。

認証、許可、およびアカウント(AAA)は、802.1xポストベース認証を設定する前に有効にする必要があります。また、方式リストを確立する必要があります。

- 方式リストには、ユーザを認証するために照会する順序と認証方式が記述されています。
- 802.1xもグローバルに有効にする必要があります。

```
<#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
```

スイッチ上でRADIUSサーバを定義します

```
<#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
```

クライアントインターフェイスで802.1xを有効にします。

```
<#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
```

## 設定と動作の確認

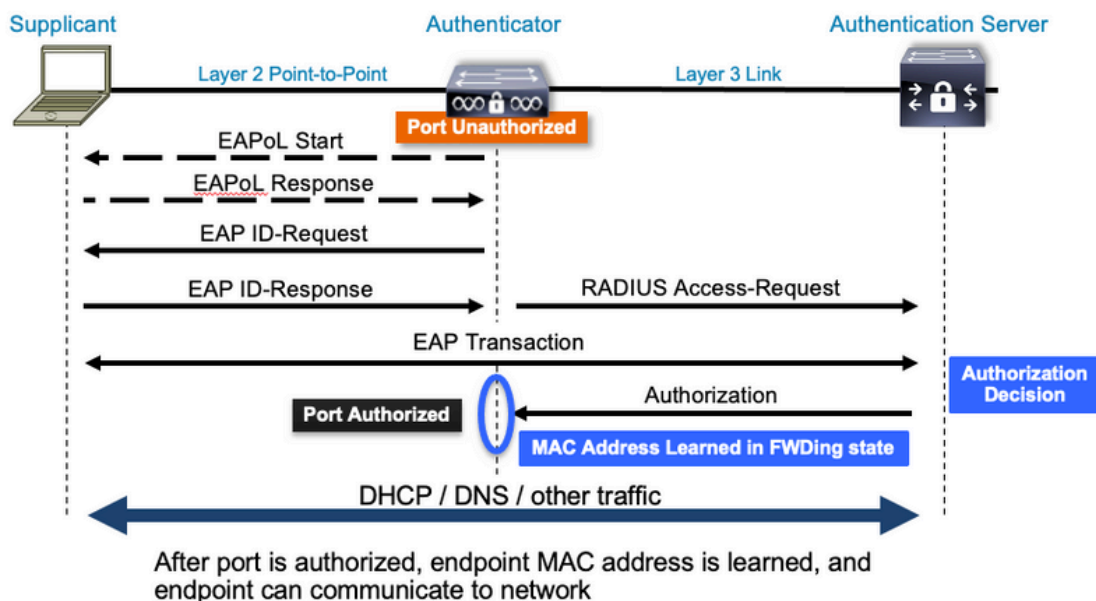
このセクションでは、801.1xの背景情報と、設定および動作の確認方法について説明します。

### 802.1xの概要

802.1xには、EAPoL(Extensible Authentication Protocol over LAN)を介したクライアントからオーセンティケータ ( ポイントツーポイント ) へのトラフィックと、RADIUSを介してカプセル化されたオーセンティケータから認証サーバへのトラフィックの2種類のトラフィックが関係します。

次の図は、単純なdot1xトランザクションのデータフローを表しています

# 802.1X Message Exchange



オーセンティケーター (スイッチ) と認証サーバ (ISEなど) は、通常、レイヤ3で分離されています。RADIUSトラフィックは、オーセンティケーターとサーバ間のネットワーク上でルーティングされます。EAPoLトラフィックは、サブリカント (クライアント) とオーセンティケーター間の直接リンクで交換されます。

MACラーニングは認証と許可の後に行われることに注意してください。

802.1xに関連する問題に取り組む際に注意すべき点がいくつかあります。

- 正しく設定されているか。
- 認証サーバは到達可能ですか。
- Authentication Managerのステータスを教えてください。
- クライアントとオーセンティケーター間、またはオーセンティケーターと認証サーバ間のパケット配信に問題がありますか。

## コンフィギュレーション

一部の設定は、メジャーリリースによって若干異なります。プラットフォームおよびコード固有のガイダンスについては、関連する設定ガイドを参照してください。

AAAは、802.1xポートベース認証を使用するように設定する必要があります。

- 「dot1x」に対して認証方式リストを確立する必要があります。これは、802.1Xが有効になっている一般的なAAA設定を表します。

```
<#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

```

次に、802.1xが有効になっているインターフェイス設定の例を示します。MAB ( MAC認証バイパス ) は、dot1xサブリカントをサポートしないクライアントを認証するための一般的なバックアップ方法です。

```
<#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

```

「show mac address-table interface <interface>」を使用して、インターフェイス上でMACアドレスが学習されているかどうかを判別します。インターフェイスがMACアドレスを学習するのは、認証に成功した場合だけです。

```

<#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

```

## 認証セッション

showコマンドは、802.1x認証の検証に使用できません。

「show authentication sessions」または「show authentication sessions <interface>」を使用して、現在の認証セッションに関する情報を表示します。この例では、アクティブな認証セッションが確立されているのはTe1/0/4だけです。

```

<#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」は、特定のインターフェイス認証セッションの追加詳細を提供します。

<#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.
```

インターフェイスで認証が有効になっているにもかかわらずアクティブなセッションがない場合は、実行可能なメソッドの一覧が表示されます。「No sessions match supplied criteria」も表示されます。

```
<#root>
```

```
C9300#
```

```
show authentication sessions interface tel/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

インターフェイスで認証が有効になっていない場合、そのインターフェイスでは認証マネージャのプレゼンスは検出されません。「No sessions match supplied criteria」も表示されます。

```
<#root>
```

```
C9300#
```

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

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

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

## 認証サーバへの到達可能性

認証サーバへの到達可能性は、802.1x認証が成功するための前提条件です。

到達可能性をすばやくテストするには、「ping <server\_ip>」を使用します。pingの送信元がRADIUS送信元インターフェイスであることを確認します。

```
<#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
```

コマンド「show aaa servers」はサーバの状態を識別し、設定されたすべてのAAAサーバとのトランザクションに関する統計情報を提供します。

```
<#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
```

test aaaユーティリティを使用して、スイッチから認証サーバへの到達可能性を確認します。このユーティリティは非推奨であり、無期限には使用できないことに注意してください。

```
<#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
```

## トラブルシューティング

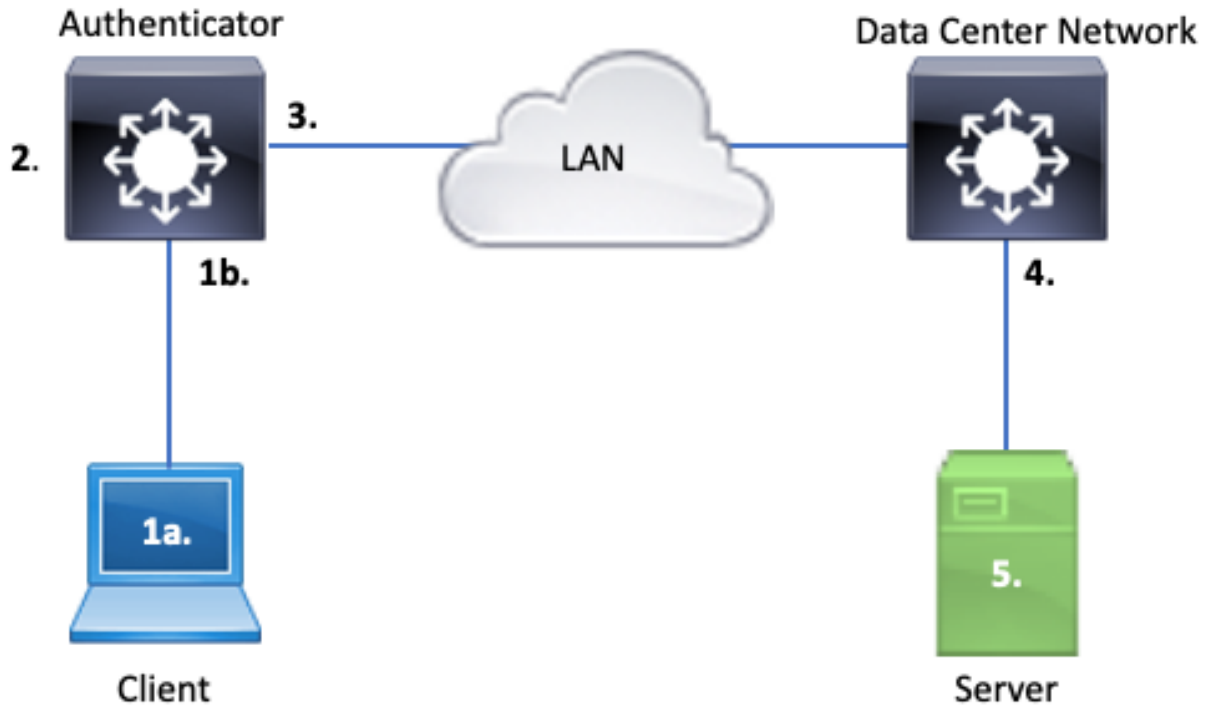
このセクションでは、Catalystスイッチのほとんどの802.1x問題のトラブルシューティング方法について説明します。

### 方法

802.1xおよび認証に関連する問題に対して系統的にアプローチし、最良の結果を得る。次の質問に答えてください。

- 問題は単一のスイッチに切り分けられていますか。単一のポート？単一のクライアントタイプですか。
- 設定は検証されていますか。認証サーバは到達可能ですか。
- 問題は毎回発生しますか。それとも、断続的に発生しますか。これは、再認証または認可変更でのみ発生しますか。

明白な問題が除外された後も問題が解決しない場合は、失敗したトランザクションをエンドツーエンドで精査します。クライアントからサーバへの802.1xトランザクションの調査に最も適したデータセットは、次のとおりです。



1a. クライアント上でのキャプチャ

1b. クライアントが接続するアクセスインターフェイス

この参照点は、dot1xが有効になっているアクセスポートとクライアントの間で交換されるEAPoLパケットについて理解するために非常に重要です。SPANは、クライアントとオーセンティケーター間のトラフィックを表示するための最も信頼性の高いツールです。

2. オーセンティケーターのデバッグ

デバッグを使用すると、オーセンティケーター全体のトランザクションをトレースできます。

- オーセンティケーターは、受信したEAPoLパケットをパントし、認証サーバ宛てのユニキャストRADIUSカプセル化トラフィックを生成する必要があります。
- 最大限の効果を得るために、適切なデバッグレベルが設定されていることを確認します。

3. オーセンティケーターに隣接するデバイスのキャプチャ

このキャプチャを使用すると、オーセンティケーターと認証サーバ間の通信を確認できます。

- このキャプチャは、オーセンティケーターの観点からカンバセーション全体を正確に表示します。
- ポイント4のキャプチャと組み合わせると、認証サーバとオーセンティケーターの間に損失があるかどうかを確認できます。

#### 4. 認証サーバに隣接するキャプチャ

このキャプチャは、ポイント3のキャプチャに付随するものです。

- このキャプチャは、認証サーバの観点から会話の全体を提供します。
- ポイント3のキャプチャと組み合わせると、オーセンティケータと認証サーバの間に損失があるかどうかを確認できます。

#### 5. 認証サーバのキャプチャ、デバッグ、ログ

最後に、サーバのデバッグから、サーバがトランザクションについて認識していることが分かります。

- このエンドツーエンドのデータセットを使用して、ネットワークエンジニアはトランザクションがどこで発生しているかを特定し、問題の原因となっていないコンポーネントを除外できます。

### 症状の例

このセクションでは、一般的な症状と問題のシナリオのリストを示します。

- クライアントからの応答なし

スイッチによって生成されたEAPoLトラフィックが応答を得ない場合、次のsyslogが表示されます。

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

理由コード「No Response from Client」は、スイッチがdot1xプロセスを開始したが、タイムアウト期間内にクライアントから応答が受信されなかったことを示します。

これは、クライアントがスイッチポートから送信された認証トラフィックを受信しなかったか認識しなかったか、またはクライアントからの応答がスイッチポートで受信されなかったことを意味します。

- クライアント放棄セッション

認証セッションが開始されたが完了しなかった場合、認証サーバ (ISEなど) は、クライアントがセッションを開始したが、完了前にセッションを放棄したことを報告します。

多くの場合、これは認証プロセスが部分的にしか完了できないことを意味します。

オーセンティケータスイッチと認証サーバ間の全体のトランザクションがエンドツーエンドで配信され、認証サーバによって正しく解釈されることを確認します。

RADIUSトラフィックがネットワーク上で失われた場合、または正しく構成できない方法で配信された場合、トランザクションは不完全になり、クライアントは認証を再試行します。サーバは、クライアントがセッションを放棄したことを報告します。

- MABクライアントがDHCPに失敗し、APIPAにフォールバックする

MAC認証バイパス(MAB)により、MACアドレスに基づく認証が可能になります。サブリカントソフトウェアをサポートしていないクライアントは、MABを介して認証されることがよくあります。

dot1xがスイッチポートで実行される推奨方式で初期方式である場合、認証のフォールバック方式としてMABが使用されると、クライアントがDHCPを完了できないシナリオが発生する可能性があります。

問題は操作の順序にまで及びます。dot1xの実行中、スイッチポートは認証が完了するか、dot1xがタイムアウトするまで、EAPoL以外のパケットを消費します。ただし、クライアントはすぐにIPアドレスの取得を試み、DHCP Discoverメッセージをブロードキャストします。これらの検出メッセージは、dot1xが設定されたタイムアウト値を超えてMABが実行できるようになるまで、スイッチポートによって消費されます。クライアントのDHCPタイムアウト期間がdot1xタイムアウト期間よりも短い場合、DHCPは失敗し、クライアントはAPIPA、またはそのフォールバック戦略に従ってフォールバックします。

この問題はさまざまな方法で防止できます。MAB認証されたクライアントが接続するインターフェイスでMABを優先します。dot1xを最初に行う必要がある場合は、クライアントのDHCP動作に注意し、タイムアウト値を適切に調整します。

dot1xおよびMABを使用する場合は、クライアントの動作を考慮する必要があります。有効な設定は、前述のように技術的な問題を引き起こす可能性があります。

## プラットフォーム固有の利点

このセクションでは、dot1xの問題のトラブルシューティングに役立つCatalyst 9000ファミリスイッチで使用できるプラットフォーム固有のユーティリティの多くについて説明します。

- スwitchポートアナライザ(SPAN)

SPANでは、キャプチャと分析のために、1つ以上のポートからのトラフィックを宛先ポートにミラーリングできます。ローカルSPANは、最も「信頼できる」キャプチャユーティリティです。

設定と実装の詳細については、次の設定ガイドを参照してください。

[SPANおよびRSPANの設定、Cisco IOS XE Bengaluru 17.6.x\(Catalyst 9300\)](#)

- 組み込みパケットキャプチャ (EPC)

EPCはCPUとメモリリソースを活用して、オンボードのローカルパケットキャプチャ機能を提供します。

EPCには、特定の問題を調査する効果に影響を与える制限があります。EPCは、毎秒1000パケットのレート制限を受けます。また、EPCでは、物理インターフェイスの出力側でCPUによって注入されたパケットを確実にキャプチャすることもできません。これは、オーセンティケータスイッチと認証サーバ間のRADIUSランザクションに重点を置く場合に重要です。多くの場合、サーバ側のインターフェイスのトラフィックレートは毎秒1000パケットを大幅に超えます。また、

サーバ側のインターフェイスの出力のEPCは、オーセンティケータスイッチによって生成されたトラフィックをキャプチャできません。

双方向アクセスリストを使用してEPCをフィルタリングし、1000パケット/秒の制限による影響を回避します。オーセンティケータとサーバ間のRADIUSトラフィックに関心がある場合は、オーセンティケータRADIUS送信元インターフェイスアドレスとサーバのアドレス間のトラフィックに注目してください。

認証サーバに向かう次のアップストリームデバイスがCatalystスイッチである場合、最適な結果を得るには、オーセンティケータスイッチに向かうダウンリンクでフィルタリングされたEPCを使用します。

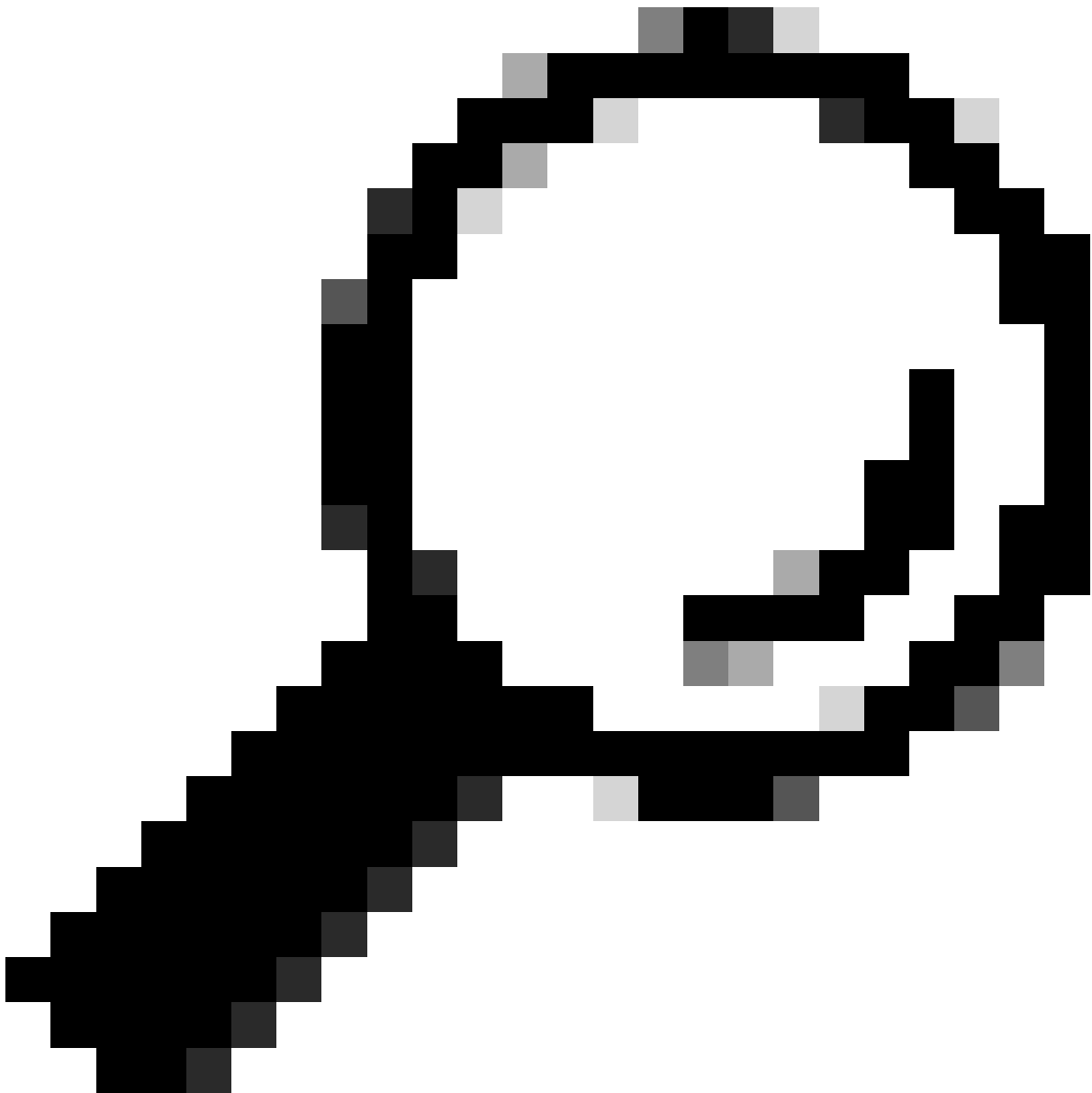
設定と実装の詳細については、次の設定ガイドを参照してください。

### [パケットキャプチャの設定、Cisco IOSバンガロール17.6.x\(Catalyst 9300\)](#)

- Cisco IOS XEのデバッグ

Cisco IOS XEバージョン16.3.2以降のソフトウェアアーキテクチャの変更により、AAAコンポーネントが別のLinuxデーモンに移動されました。使い慣れたデバッグでは、ロギングバッファで表示可能なデバッグが有効ではなくなりました。代わりに、





ヒント：従来のIOS AAAデバッグでは、syslogバッファ内の前面パネルポート認証用の出力がシステムログに表示されなくなりました

---

dot1xおよびRADIUSに関するこれらの従来のCisco IOSデバッグでは、スイッチのロギングバッファ内で表示可能なデバッグが有効ではなくなりました。

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

AAAコンポーネントのデバッグは、SMD (セッションマネージャデーモン) の下のシステムトレースからアクセスできるようになりました。

- 従来のsyslogと同様に、Catalystシステムトレースはデフォルトレベルで報告を行うので、より詳細なログを収集するように指示する必要があります。
- コマンド「set platform software trace smd switch active r0 <component> debug」を使用して、目的のサブコンポーネントのルーチントレースレベルを変更します。

```
<#root>
```

```
Switch#
```

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

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

この表は、従来のIOSデバッグを対応するトレースにマッピングしています。

古いスタイルのコマンド	新しいスタイルコマンド
#debug半径	#set platform software trace smd switch active R0 radius debug
#debug dot1x all	#set platform software trace smd switch active R0 dot1x-allデバッグ
#debug access-session all (すべてのアクセスセッション)	#set platform software trace smd switch active R0 auth-mgr-allデバッグ
#debug epmすべて	#setプラットフォームソフトウェアアトレースsmd switch active R0 epm-allデバッグ

従来のデバッグでは、関連するすべてのコンポーネントトレースを「デバッグ」レベルに設定できません。必要に応じて特定のトレースを有効にするために、プラットフォームコマンドも使用します。

SMDサブコンポーネントの現在のトレースレベルを表示するには、コマンド「show platform software trace level smd switch active R0」を使用します。

```
<#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>
```

サブコンポーネントトレースレベルは、2つの方法でデフォルトに戻すことができます。

- 復元するには、「undebug all」または「set platform software trace smd switch active R0 <sub-component> notice」を使用します。
- デバイスがリロードすると、トレースレベルもデフォルトに戻ります。

```
<#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.
```

コンポーネントのトレースログは、コンソールで表示したり、アーカイブに書き込んだり、オフラインで表示したりできます。トレースは、デコードが必要な圧縮バイナリアーカイブにアーカイブされます。アーカイブされたトレースを処理する際のデバッグのサポートについては、TACにお問い合わせください。このワークフローでは、CLIでトレースを表示する方法について説明します。

show platform software trace message smd switch active R0コマンドを使用して、SMDコンポーネントのメモリに格納されたトレースログを表示します。

```
<#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>

```

出力は詳細であるため、出力をファイルにリダイレクトすると便利です。

- このファイルは、CLIで「more」ユーティリティを使用して読み取るか、オフラインにしてテキストエディタで表示することができます。

```
<#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」は、Cisco IOS XE 17.9.x以降のバージョンのトレースおよび標準の更新ユーティリティです。

<#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」は、「show platform software trace」と同じ機能をより洗練された形式で提供します。

<#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
```

## トレースの例

このセクションには、完全に失敗したトランザクション（サーバがクライアントのクレデンシャルを拒否する）のdot1xおよびradiusコンポーネントに対するセッションマネージャトレースが含まれています。前面パネル認証に関連するシステムトレースをナビゲートするための基本的なガイドラインを提供することを目的としています。

- テストクライアントがGigabitEthernet1/0/2への接続を試みましたが、拒否されました。

この例では、SMDコンポーネントトレースは「debug」に設定されます。

```
<#root>
```

```
C9300#
```

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

```
C9300#
```

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

## EAPoL : 開始

```
[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 0x0A
[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:EAP要求ID

```
[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:EAP応答

```
[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 : アクセス要求

```
[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:ACCESS-CHALLENGE

```
[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:EAP応答

```
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 : アクセス要求

```
[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:ACCESS-CHALLENGE

```
[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:EAP要求

```
[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:EAP应答

```
[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 : アクセス要求

```
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 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 : アクセス拒否

```
[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拒否

```

[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

```

## 追加情報

### デフォルト設定

機能	デフォルト設定
スイッチ802.1x enable状態	無効

機能	デフォルト設定
ポート単位の802.1xイネーブルステート	無効（強制的に承認）。 ポートは、クライアントの802.1xベースの認証なしで、通常のトラフィックを送受信します。
[AAA]	無効
RADIUS サーバ <ul style="list-style-type: none"> <li>• IP アドレス</li> <li>• UDP認証ポート</li> <li>• デフォルトのアカウントリングポート</li> <li>• キー</li> </ul>	<ul style="list-style-type: none"> <li>• 指定されていません。</li> <li>• 1645 .</li> <li>• 1646 .</li> <li>• 指定されていません。</li> </ul>
ホストモード	単一ホストモード。
制御方向	双方向制御。
定期的な再認証	無効
再認証の試行間隔（秒）	3600 seconds.
再認証番号	2回（ポートが無許可ステートに変更されるまでにスイッチが認証プロセスを再起動する回数）
休止期間	60秒（クライアントとの認証交換に失敗した後、スイッチが待機状態を維持する秒数）
再送信時間	30秒（スイッチがクライアントからのEAP要求/IDフレームへの応答を待機する秒数）。
最大再送信数	2回（認証プロセスを再開する前にスイッチがEAP要求/IDフレームを送信した回数）。

機能	デフォルト設定
クライアントタイムアウト期間	30秒 ( 認証サーバからクライアントに要求をリレーするとき、スイッチがクライアントに要求を再送信するまでに応答を待機する時間 )
認証サーバタイムアウト期間	30秒 ( クライアントから認証サーバに応答をリレーするとき、スイッチが応答を待ってからサーバに応答を再送信するまでの時間 ) このタイムアウト期間は、dot1x timeout server-timeout インターフェイスコンフィギュレーションコマンドを使用して変更できます。
非アクティブタイムアウト	無効
GUEST VLAN	指定されていません。
アクセス不能認証バイパス	無効
制限されたVLAN	指定されていません。
オーセンティケータ ( スイッチ ) モード	指定されていません。
MAC認証バイパス	無効
音声対応セキュリティ	無効

## オプション設定

### 定期的な再認証

定期的な802.1xクライアントの再認証を有効にして、その頻度を指定できます。

- authentication periodic : クライアントの定期的な再認証をイネーブルにします。
- inactivity : クライアントからアクティビティがない場合に認証されない間隔 ( 秒単位 )
- reauthenticate : 自動再認証の試行が開始されるまでの秒数
- restartvalue : 許可されていないポートを認証しようとする間隔 ( 秒単位 )
- unauthorizedvalue : 許可されていないセッションが削除されるまでの間隔 ( 秒 )

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

## 違反モード

802.1x対応ポートにデバイスが接続する場合、またはポートで認証されたデバイスに関する許可された最大数に達する場合に、シャットダウンするか、syslogエラーを生成するか、新しいデバイスからパケットを廃棄するように、802.1xポートを設定できます。

- shutdown : ポートをエラーディセーブルにします。
- restrict:syslogエラーを生成します。
- protect : ポートにトラフィックを送信する新しいデバイスからのパケットをドロップします。
- replace : 現在のセッションを削除し、新しいホストで認証します。

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

## 休止期間の変更

authentication timer restart インターフェイス設定コマンドで、アイドル期間を制御します。アイドル期間は、スイッチがクライアントを認証できない後にスイッチがアイドル状態を維持する、設定された期間を指定します。値の範囲は1 ~ 65535秒です。

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

## スイッチからクライアントへの再送信時間の変更

クライアントは、スイッチからのEAP-request/identityフレームにEAP-response/identityフレームで応答します。スイッチはこの応答を受信しない場合、設定された時間(再送信時間)待機してからフレームを再送信します。

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

## スイッチからクライアントへのフレーム再送信番号の設定

認証プロセスを再開する前に、スイッチがEAP要求/IDフレーム(応答を受信しないと仮定した場

合) をクライアントに送信する回数を変更できます。範囲は 1 ~ 10 です。

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

## ホストモードの設定

802.1x認証ポートで複数のホスト(クライアント)を許可できます。

- multi-auth : 音声VLANとデータVLANの両方で複数の認証されたクライアントを許可します。
- multi-host : 単一のホストが認証された後、802.1x認証ポートで複数のホストを許可します。
- multi-domain : ホストと音声デバイス(IP Phone ( シスコ製またはシスコ以外 ) の両方を、IEEE 802.1x認証済みポートで認証できるようにします。

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

## MAC移動の有効化

MACの移動により、認証されたホストはデバイス上のあるポートから別のポートに移動できます。

```
authentication mac-move permit
```

## MAC置換の有効化

MAC replaceを使用すると、ホストはポート上の認証されたホストを置き換えることができます。

- protect:ポートは、システムメッセージを生成せずに、予期しないMACアドレスのパケットをドロップします。
- restrict - 違反したパケットはCPUによってドロップされ、システムメッセージが生成されません。
- shutdown:ポートは、予期しないMACアドレスを受信したときにエラーディセーブルになります。



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

## 再認証番号の設定

また、ポートが無許可ステートに変わるまでにデバイスが認証プロセスを再起動する回数も変更できます。範囲は0 ~ 10です

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

## ゲストVLANの設定

ゲストVLANを設定すると、802.1x対応ではないクライアントは、サーバがEAP要求/アイデンティティフレームに対する応答を受信しない場合にゲストVLANに配置されます。

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

## 制限付きVLANの設定

デバイスで制限付きVLANを設定すると、認証サーバが有効なユーザ名とパスワードを受信していない場合に、IEEE 802.1xに準拠しているクライアントは制限付きVLANに移動されます。

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

## 制限付きVLANでの認証試行回数の設定

authentication event fail retryretry countinterface設定コマンドを使用すると、制限されたVLANにユーザが割り当てられるまでに許可される最大認証試行回数を設定できます。認証の試行可能範囲は1 ~ 3です。

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

## 重要な音声VLANでの802.1xアクセス不能認証バイパスの設定

ポートに重要な音声VLANを設定し、アクセス不能認証バイパス機能を有効にできます。

- authorize : 認証を試みる新しいホストをユーザ指定の重要なVLANに移動します。
- reinitialize : ポート上のすべての承認済みホストを、ユーザ指定の重要なVLANに移動します

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

## WoLを使用した802.1x認証の設定

802.1x認証を有効にするには、Wake on LAN(WoL)を使用します

```
authentication control-direction both
```

## MAC認証バイパスの設定

```
mab
```

## フレキシブル認証オーダーの設定

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

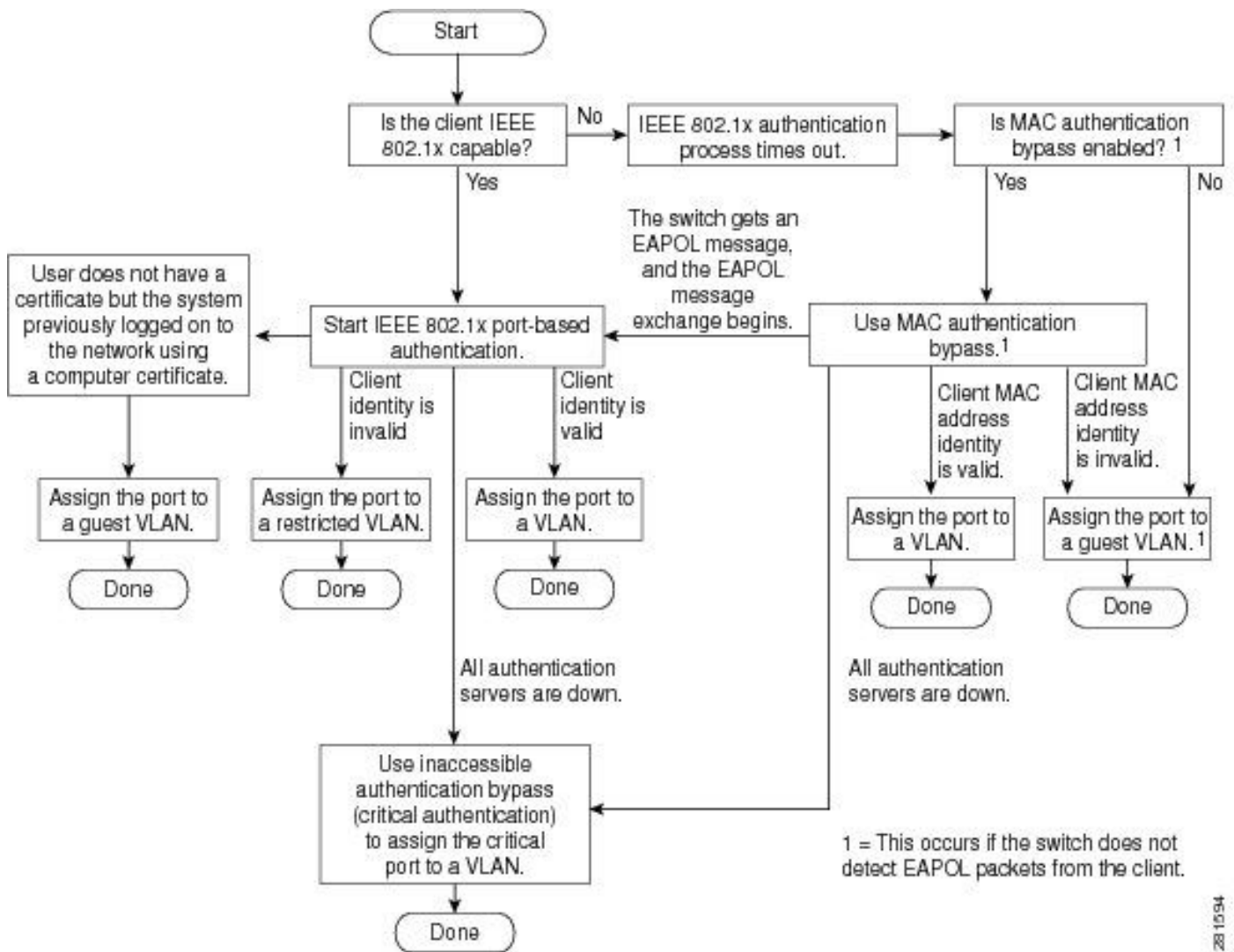
## 音声対応802.1xセキュリティの設定

デバイスで音声対応802.1xセキュリティ機能を使用すると、データVLANでも音声VLANでも、セキュリティ違反が発生したVLANのみを無効にできます。データVLANでセキュリティ違反が見つかると、データVLANだけがシャットダウンされます。これはグローバル設定です。

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

## フローチャート

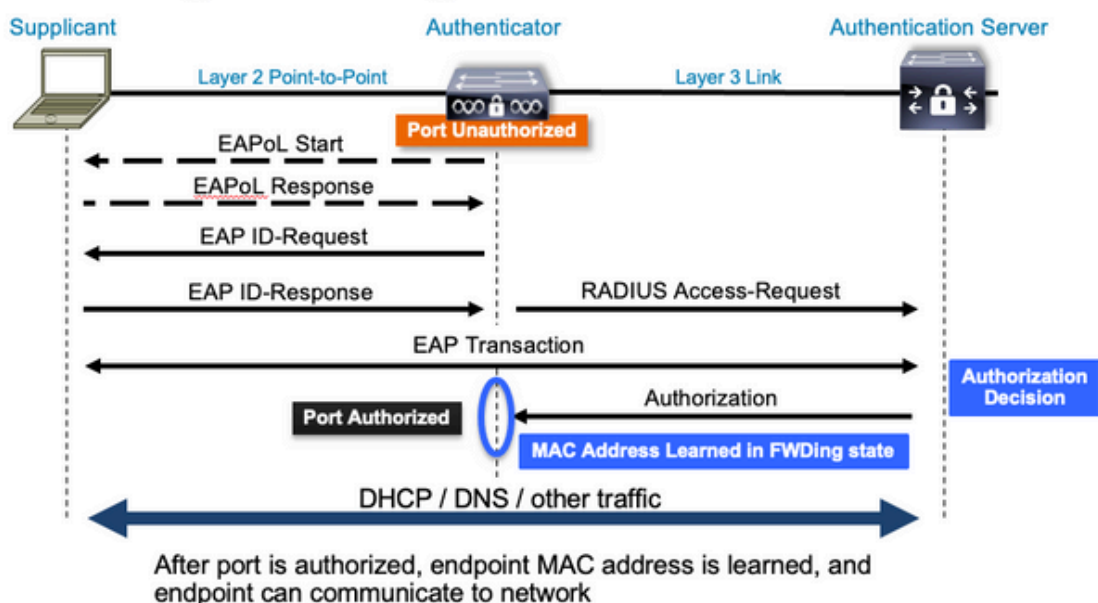
認証フローチャート



### ポートベースの認証の開始とメッセージ交換

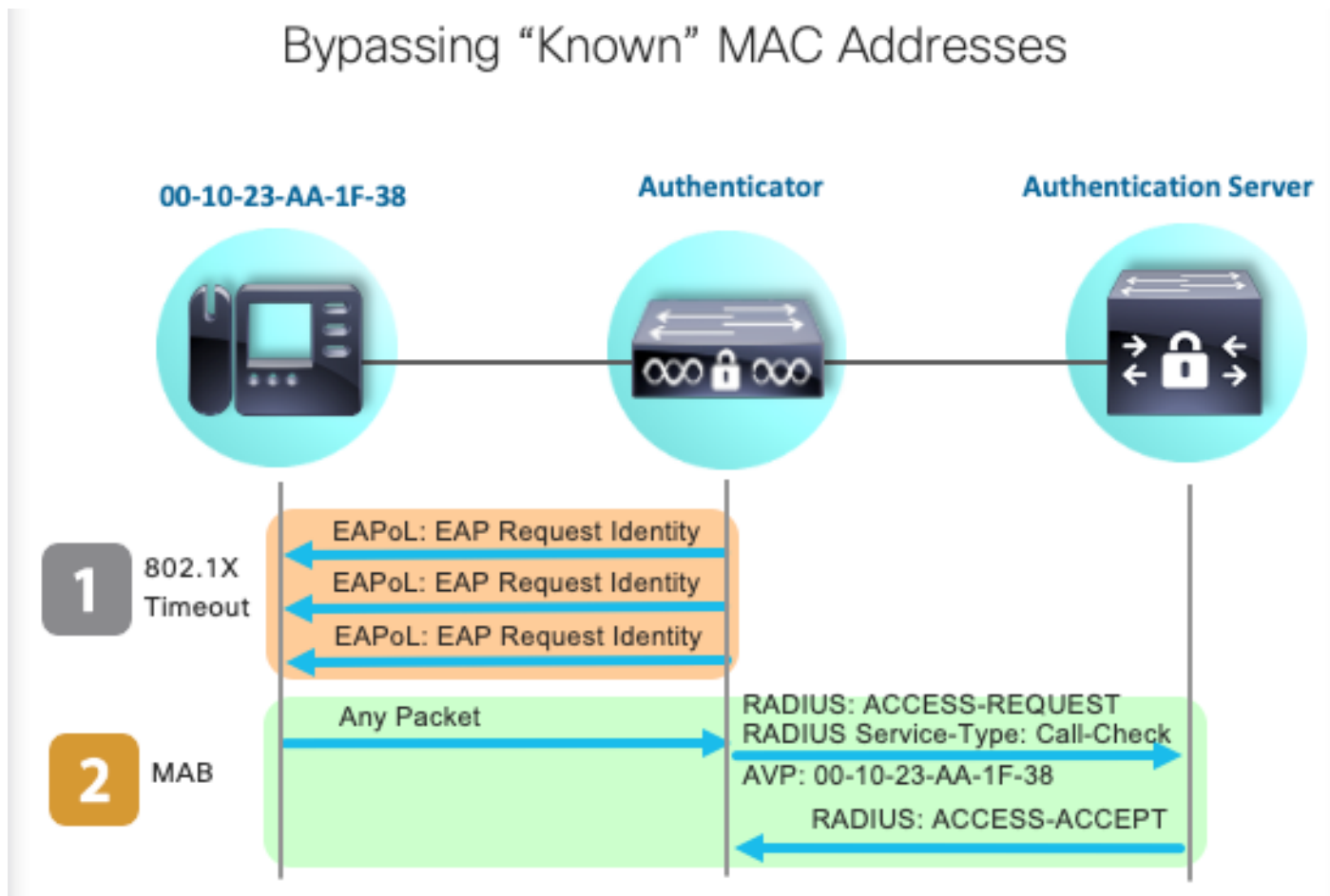
この図は、RADIUSサーバへのメッセージ交換を開始するクライアントを示しています。

## 802.1X Message Exchange



## MAB認証の開始とメッセージ交換

次の図は、MAC認証バイパス(MAB)中のメッセージ交換を示しています



## 関連情報

- [RADIUSサーバ設定の簡素化](#)
- [MAC認証バイパス導入ガイド](#)
- [有線802.1x導入ガイド](#)
- [Catalyst 9300 SPANコンフィギュレーションガイド](#)
- [Catalyst 9300 EPCコンフィギュレーションガイド](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。