Catalyst 9000系列交换机上的Dot1x故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

基本配置

检验配置和操作

- 802.1x简介
- 配置
- 身份验证会话
- 与身份验证服务器的可达性

故障排除

- 方法
- 示例症状
- 平台特定最终版本
  - 跟踪示例

其他信息

- 默认设置
- 可选设置
- 流程图

相关信息

简介

本文档介绍如何在Catalyst 9000系列交换机上配置、验证802.1x网络访问控制(NAC)并对其进行故障排除。

先决条件

要求

Cisco建议您了解这些主题。

- Catalyst 9000 系列交换机
- 身份服务引擎 (ISE)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.6.x及更高版本
- ISE-VM-K9版本3.0.0.458

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

注意：有关在其他思科平台上启用这些功能的命令，请参阅相应的配置指南。

背景信息

802.1x标准定义了基于客户端-服务器的访问控制和身份验证协议，该协议可防止未经授权的客户端通过可公开访问的端口连接到LAN，除非这些客户端经过正确的身份验证。身份验证服务器对连接到交换机端口的每个客户端进行身份验证，然后才提供交换机或LAN提供的任何服务。

802.1x身份验证包含3个不同的组件：

Supplicant客户端 -提交凭据以供身份验证的客户端
身份验证程序 -在客户端与网络之间提供网络连接，并且允许或阻止网络流量的网络设备。
身份验证服务器 -可接收和响应网络访问请求的服务器，告诉身份验证器是否可以允许连接以及要应用于身份验证会话的各种其他设置。

本文档的目标受众是未必注重安全的工程师和支持人员。有关基于802.1x端口的身份验证和组件（例如ISE）的详细信息，请参阅相应的配置指南。

注意：有关最准确的默认802.1x身份验证配置，请参阅适用于您的特定平台和代码版本的相应配置指南。

基本配置

本节介绍实施基于802.1x端口的身份验证所需的基本配置。其他功能说明可在本文档的附录选项卡中找到。不同版本的配置标准略有不同。根据当前版本配置指南验证配置。

在配置基于802.1x后台的身份验证之前，必须启用身份验证、授权和帐户(AAA)，并且必须建立方法列表。

- 方法列表描述了验证用户时要查询的序列和验证方法。
- 还必须全局启用802.1x。

<#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
```

在交换机上定义RADIUS服务器

```
<#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
```

在客户端接口上启用802.1x。

```
<#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
```

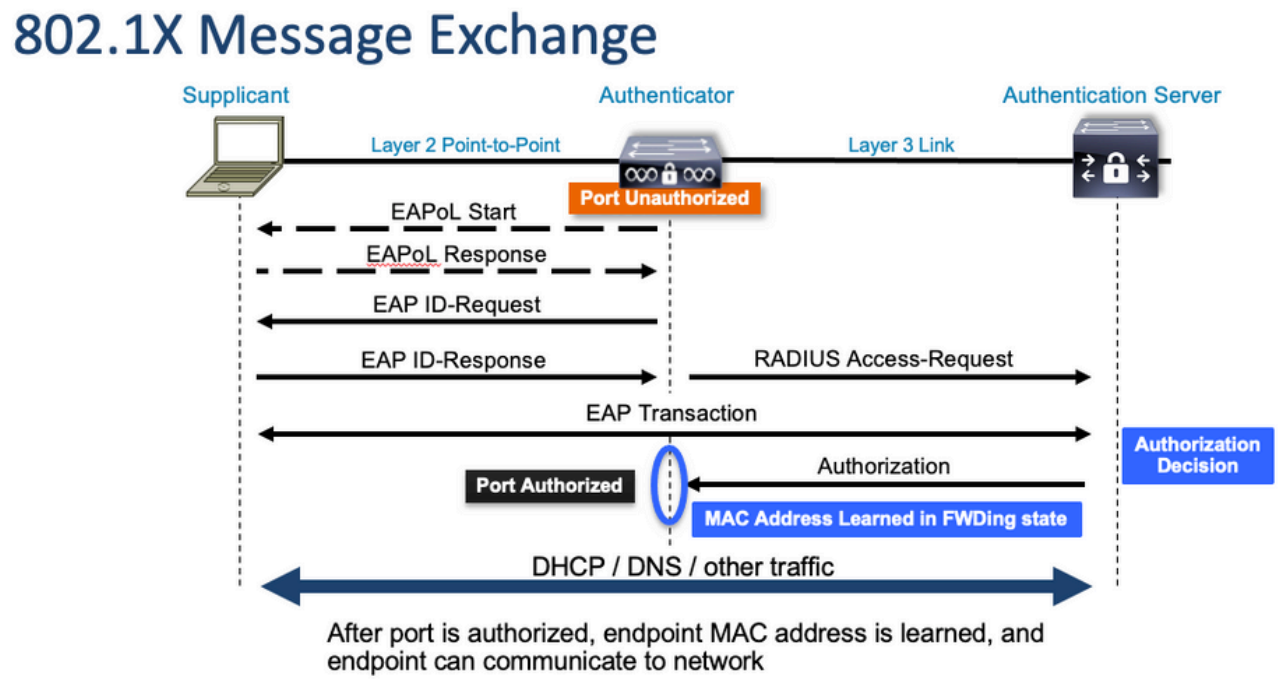
检验配置和操作

本节提供有关801.1x的背景信息，以及如何验证配置和操作。

802.1x简介

802.1x涉及两种不同类型的流量-基于EAPoL（LAN上的可扩展身份验证协议）的客户端到身份验证器（点对点）流量和通过RADIUS封装的身份验证器到身份验证服务器流量。

下图显示简单dot1x事务的数据流



身份验证器（交换机）和身份验证服务器（例如ISE）通常由第3层分隔。RADIUS流量在身份验证器和服务器之间通过网络路由。EAPoL流量通过请求方（客户端）和身份验证器之间的直接链路交换。

请注意，MAC学习发生在身份验证和授权之后。

在处理涉及802.1x的问题时，请记住以下几个问题：

- 配置是否正确？
- 身份验证服务器是否可达？
- Authentication Manager的状态是什么？
- 客户端与身份验证器之间或身份验证器与身份验证服务器之间的数据包传送是否存在任何问题？

配置

某些配置在主要版本之间略有不同。有关平台/代码特定的指南，请参阅相关的配置指南。

必须将AAA配置为使用基于802.1x端口的身份验证。

- 必须为“dot1x”建立身份验证方法列表。这表示启用802.1X的常见AAA配置。

<#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
```

这是启用802.1x的接口配置示例。MAB（MAC身份验证绕行）是一种常见的备份方法，用于对不支

持dot1x请求方的客户端进行身份验证。

<#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
```

使用“show mac address-table interface <interface>”确定是否在接口上获知MAC地址。成功通过身份验证后，接口只学习MAC地址。

<#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
```

身份验证会话

Show命令可用于验证802.1x身份验证。

使用“show authentication sessions”或“show authentication sessions <interface>”显示有关当前身份验证会话的信息。在本示例中，只有Te1/0/4建立了主动身份验证会话。

<#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提供有关特定接口身份验证会话的其他详细信息。

<#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.
```

如果在接口上启用了身份验证但没有任何活动会话，则会显示可运行方法列表。“No sessions match provided criteria”也会显示。

```
<#root>

C9300#

show authentication sessions interface te1/0/5

No sessions match supplied criteria.

Runnable methods list:
  Handle  Priority  Name
      13         5  dot1xSup
       1         5  dot1x
       2        10  webauth
      14        15  mab
```

如果在接口上未启用身份验证，则不会在接口上检测到身份验证管理器存在。“No sessions match provided criteria”也会显示。

```
<#root>

C9300#

show authentication sessions interface te1/0/6


No sessions match supplied criteria.
No Auth Manager presence on this interface
```

与身份验证服务器的可达性

能否连接到身份验证服务器是802.1x身份验证成功的先决条件。

使用“ping <server_ip>”快速测试可接通性。确保您的ping源自RADIUS源接口。

<#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
```

命令“show aaa servers”可标识服务器状态，并提供有关与所有已配置AAA服务器进行交易的统计信息。

<#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 WNCD (1) : current UP
     Platform State from WNCD (2) : current UP
     Platform State from WNCD (3) : current UP
     Platform State from WNCD (4) : current UP
     Platform State from WNCD (5) : current UP
     Platform State from WNCD (6) : current UP
     Platform State from WNCD (7) : current UP
     Platform State from WNCD (8) : current UP, duration 0s, previous duration 0s
     Platform Dead: total time 0s, count 0UP
     Quarantined: No

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

             Response: accept 2, reject 2, challenge 38
             Response: unexpected 0, server error 0, incorrect 12, time 21ms
             Transaction: success 42, failure 117
             Throttled: transaction 0, timeout 0, failure 0
             Malformed responses: 0
             Bad authenticators: 0
             Dot1x transactions:
             Response: total responses: 42, avg response time: 21ms
```

```
        Transaction: timeouts 114, failover 0
        Transaction: total 118, success 2, failure 116
        MAC auth transactions:
        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0
    Author: request 0, timeouts 0, failover 0, retransmission 0
        Response: accept 0, reject 0, challenge 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        MAC author transactions:
        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0
    Account: request 3, timeouts 0, failover 0, retransmission 0
        Request: start 2, interim 0, stop 1
        Response: start 2, interim 0, stop 1
        Response: unexpected 0, server error 0, incorrect 0, time 11ms
        Transaction: success 3, failure 0
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
    Elapsed time since counters last cleared: 1d3h4m
    Estimated Outstanding Access Transactions: 0
    Estimated Outstanding Accounting Transactions: 0
    Estimated Throttled Access Transactions: 0
    Estimated Throttled Accounting Transactions: 0
    Maximum Throttled Transactions: access 0, accounting 0
    Consecutive Response Failures: total 115
        SMD Platform : max 113, current 0 total 113
        WNCD 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
        WNCD 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
```

使用“test aaa”实用程序可确认从交换机到身份验证服务器的可达性。请注意，此实用程序已弃用，不能无限期使用。

<#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 serve

```
User rejected
```

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

```
*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
```

故障排除

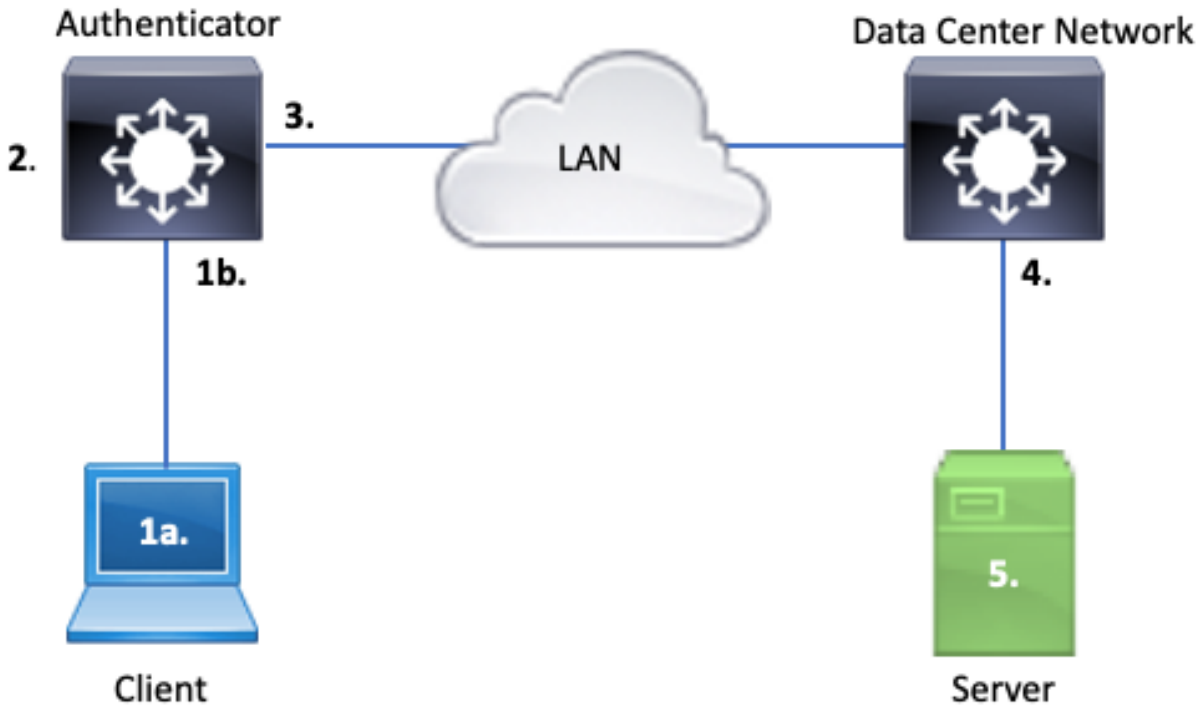
本部分提供有关如何排除Catalyst交换机上大多数802.1x问题的指南。

方法

系统地处理涉及802.1x和身份验证的问题，以获得最佳效果。以下是一些不错的答案：

- 此问题是否只存在于一台交换机上？单个端口？单一客户端类型？
- 配置是否已验证？身份验证服务器是否可达？
- 问题是否每次都出现，或者间歇性出现？它是否只发生在重新身份验证或授权更改时？

在排除明显故障后，如果问题仍然存在，请端到端检查单个失败的交易。用于调查从客户端到服务器的802.1x事务的最佳、最完整的数据集包括：



1a。 捕获客户端和/或

1b。在客户端连接的访问接口上

此参考点对我们了解在启用dot1x的接入端口和客户端之间交换的EAPoL数据包至关重要。SPAN是查看客户端和身份验证器之间的流量的最可靠工具。

2. 身份验证器上的调试

通过调试，我们可以通过身份验证器跟踪事务。

- 身份验证器必须传送收到的EAPoL数据包，并生成以身份验证服务器为目标的单播RADIUS封装流量。
- 确保设置了适当的调试级别，以实现最大效率。

3. 在身份验证器旁捕获

通过此捕获，我们可以查看身份验证器和身份验证服务器之间的会话。

- 此捕获从身份验证器的角度准确显示整个会话。
- 当与点4中的捕获配对时，您可以确定身份验证服务器和身份验证器之间是否存在丢失现象。

4. 捕获身份验证服务器旁的流量

此捕获是第3点捕获的伙伴。

- 此捕获从身份验证服务器的角度提供了整个会话。
- 当与点3中的捕获配对时，您可以确定身份验证器和身份验证服务器之间是否存在丢失现象。

5. 捕获、调试和登录身份验证服务器

最后一个难解之处是，服务器调试告诉我们服务器对我们的事务了解多少。

- 借助这些端到端数据，网络工程师可以确定事务中断的位置并排除不导致问题的组件。

示例症状

本部分列出了常见症状和问题情景。

- 客户端无响应

如果交换机生成的EAPoL流量未引发响应，则会看到以下系统日志：

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

原因代码“No Response from Client”表示交换机已启动dot1x进程，但在超时期间内未从客户端收到任何响应。
这意味着客户端未收到或无法理解交换机端口发送的身份验证流量，或者交换机端口未收到来自客户端的响应。

- 客户端放弃会话

如果身份验证会话已启动但未完成，则身份验证服务器（例如ISE）会报告客户端已启动会话，但在完成之前已放弃该会话。
通常，这意味着身份验证过程只能部分完成。

确保身份验证程序交换机和身份验证服务器之间的整个事务都是端到端传送的，并且身份验证服务器能够正确解释这些事务。

如果RADIUS流量在网络上丢失，或者以无法正确组装的方式传输，则事务不完整，客户端将重试身份验证。服务器反过来报告客户端已放弃其会话。

- MAB客户端无法通过DHCP/回退到APIPA

MAC身份验证绕行(MAB)允许基于MAC地址进行身份验证。通常，不支持请求方软件的客户端会通过MAB进行身份验证。

如果MAB用作身份验证的回退方法，而dot1x是在交换机端口上运行的首选初始方法，则可能导致客户端无法完成DHCP的情况。

问题归结为操作顺序。当dot1x运行时，交换机端口会使用EAPoL以外的数据包，直到身份验证完成或dot1x超时。但是，客户端会立即尝试获取IP地址并广播其DHCP发现消息。这些发现消息由交换机端口使用，直到dot1x超过其配置的超时值，并且MAB能够运行。如果客户端DHCP超时时间小于

dot1x超时时间，则DHCP会失败，并且客户端会回退到APIPA或其回退策略规定的任何值。

可以通过多种方式防止此问题。在通过MAB身份验证的客户端连接的接口上支持MAB。如果dot1x必须首先运行，请注意客户端DHCP行为，并相应地调整超时值。

当使用dot1x和MAB时，请注意考虑客户端行为。如上所述，有效的配置可能会导致技术问题。

平台特定最终版本

本部分概述了Catalyst 9000系列交换机上提供的许多平台特定的实用程序，这些实用程序可用于解决dot1x的问题。

- 交换端口分析器 (SPAN)

SPAN允许用户将来自一个或多个端口的流量镜像到目标端口以进行捕获和分析。本地SPAN是最“可信”的捕获实用程序。

有关配置和实施的详细信息，请参阅以下配置指南：

配置SPAN和RSPAN，Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300)

- 嵌入式数据包捕获(EPC)

EPC利用CPU和内存资源提供板载本地数据包捕获功能。

EPC存在一些局限性，这些局限性影响了其调查某些问题的效率。EPC的速率限制为每秒1000个数据包。EPC还无法在物理接口出口可靠地捕获CPU注入的数据包。当重点是身份验证器交换机和身份验证服务器之间的RADIUS事务时，这一点很重要。通常，面向服务器的接口上的流量速率大大超过每秒1000个数据包。此外，面向服务器的接口出口上的EPC无法捕获身份验证器交换机生成的流量。

使用双向访问列表过滤EPC，避免受到每秒1000个数据包限制的影响。如果对身份验证器和服务器之间的RADIUS流量感兴趣，请重点关注身份验证器RADIUS源接口地址与服务器地址之间的流量。

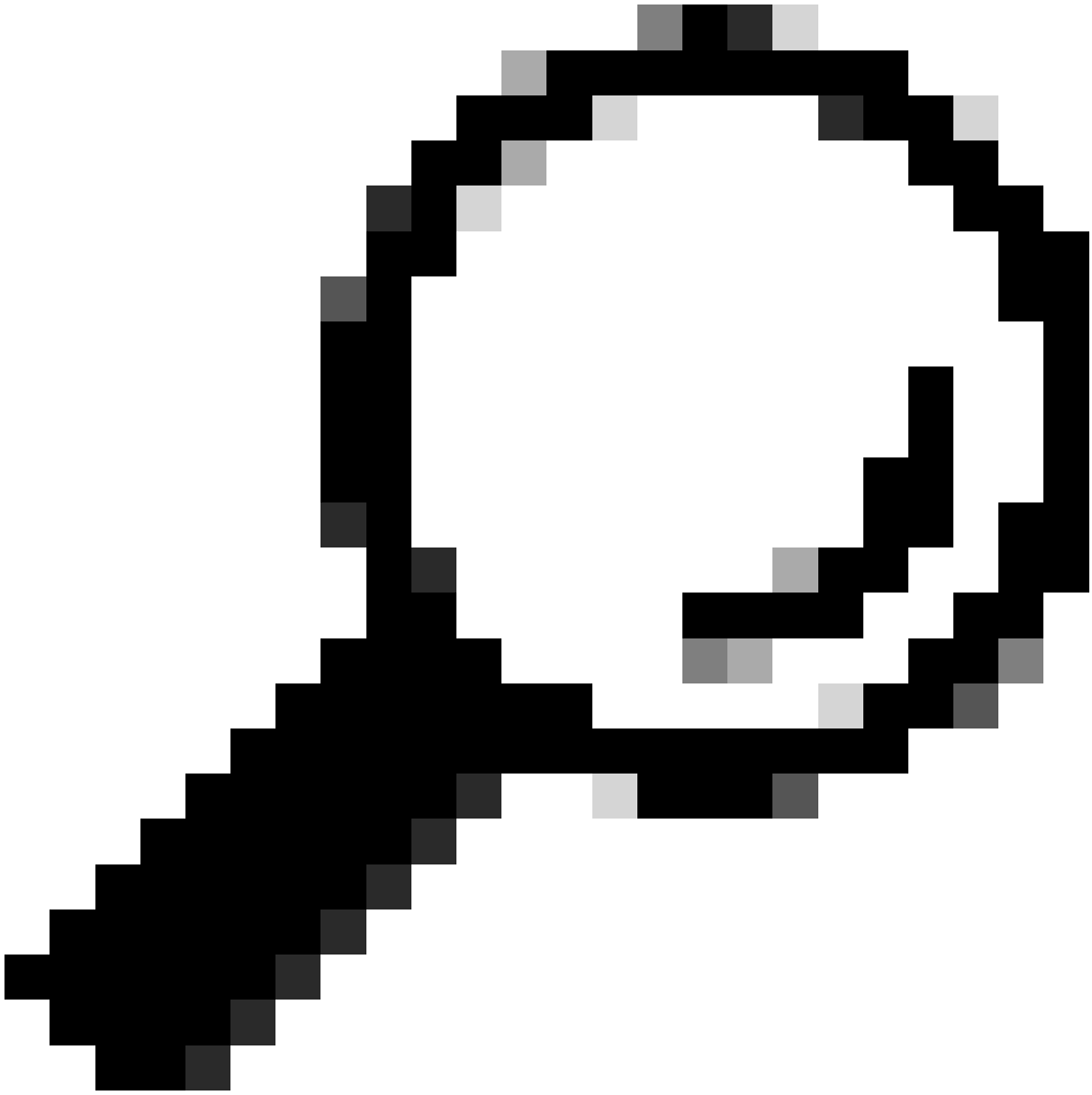
如果通向身份验证服务器的下一个上游设备是Catalyst交换机，请在通向身份验证器交换机的下行链路上使用经过过滤的EPC，以获得最佳结果。

有关配置和实施的详细信息，请参阅以下配置指南：

配置数据包捕获，Cisco IOS Bengaluru 17.6.x (Catalyst 9300)

- Cisco IOS XE调试

从Cisco IOS XE版本16.3.2开始的软件架构更改将AAA组件移至单独的Linux后台程序。熟悉的调试不再启用日志记录缓冲区中的可查看调试。相反，



提示：传统IOS AAA调试在系统日志中不再提供用于系统日志缓冲区中前面板端口身份验证的输出

以下用于dot1x和RADIUS的传统Cisco IOS调试不再启用交换机的交换机日志记录缓冲区中的可查看调试：

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

现在，可以通过SMD（会话管理器守护程序）下的系统跟踪来访问AAA组件调试。

- 与传统系统日志一样，Catalyst系统跟踪报告在默认级别，必须指示其收集更多深度日志。
- 使用命令“set platform software trace smd switch active r0 <component> debug”更改所需子组件的例行跟踪级别。

<#root>

```
Switch#
```

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

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

此表将传统IOS调试映射到对应的跟踪。

旧式命令	新建样式命令
#debug radius	#set platform software trace smd switch active R0 radius debug
#debug dot1x all	#set platform software trace smd switch active R0 dot1x-all debug
#debug access-session all	#set platform software trace smd switch active R0 auth-mgr-all debug
#debug epm all	#set platform software trace smd switch active R0 epm-all debug

传统调试支持所有相关的组件跟踪到“调试”级别。平台命令还用于根据需要启用特定跟踪。

使用命令“show platform software trace level smd switch active R0”显示SMD子组件的当前跟踪级别。

<#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>
```

子组件跟踪级别可通过两种方式恢复为默认值。

- 使用“undebug all”或“set platform software trace smd switch active R0 <sub-component> notice”进行恢复。
- 如果设备重新加载，跟踪级别也会恢复为默认值。

<#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.

组件跟踪日志可以在控制台上查看，也可以写入存档并脱机查看。 跟踪在需要解码的压缩二进制存档中存档。在处理已存档的跟踪时，请联系TAC以获得调试帮助。此工作流程说明如何在CLI中查看跟踪。

使用命令“show platform software trace message smd switch active R0”查看存储在SMD组件的内存中的跟踪日志。

<#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>
```

输出是详细的，因此将输出重定向到文件很有用。

- 可以使用“more”实用程序通过CLI读取文件，也可以将其脱机移动以便在文本编辑器中查看。

<#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] Started
2022/12/02 15:04:47.434271 {smd_R0-0}{2}: [auth-mgr] [16908]: (info): [0800.27dd.3016:Gi2/0/11] Accounti
2022/12/02 15:04:43.366688 {smd_R0-0}{2}: [auth-mgr] [16908]: (debug): [5057.a8e1.6f49:Gi2/0/11] Started
2022/12/02 15:04:43.366558 {smd_R0-0}{2}: [auth-mgr] [16908]: (info): [5057.a8e1.6f49:Gi2/0/11] Accounti
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 unl
<snip>
```

Show logging process是Cisco IOS XE 17.9.x版本及后续版本中用于跟踪和标准的更新实用程序。

<#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”和“show platform software trace”具有相同的功能，提供的格式更简洁、更易于访问。

<#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_RO-0}{1}: [radius] [22624]: (ERR): Failed to mark Identifier for reu
2023/05/02 16:44:03.625123382 {smd_RO-0}{1}: [radius] [22624]: (ERR): RSPE-  Set Identifier Free for Re
2023/05/02 16:44:03.625116747 {smd_RO-0}{1}: [radius] [22624]: (info): Valid Response Packet, Free the
2023/05/02 16:44:03.625091040 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  authenticator 2b f4 ea
2023/05/02 16:44:03.625068520 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS: Received from id 1813/9
2023/05/02 16:44:03.610151863 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS: Started 5 sec timeout
2023/05/02 16:44:03.610097362 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Delay-Time     [41]
2023/05/02 16:44:03.610090044 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Event-Timestamp     [55]
2023/05/02 16:44:03.610085857 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Status-Type    [40]
2023/05/02 16:44:03.610040912 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Class              [25]
2023/05/02 16:44:03.610037444 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Authentic      [45]
2023/05/02 16:44:03.610032802 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Session-Id     [44]
2023/05/02 16:44:03.610028677 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Called-Station-Id   [30]
2023/05/02 16:44:03.610024641 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Nas-Identifier      [32]
2023/05/02 16:44:03.610020641 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Calling-Station-Id  [31]
2023/05/02 16:44:03.610016809 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port           [5]
2023/05/02 16:44:03.610012487 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port-Type       [61]
2023/05/02 16:44:03.610007504 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port-Id         [87]
2023/05/02 16:44:03.610003581 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-IP-Address      [4]
2023/05/02 16:44:03.609998136 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Calling-Station-Id  [31]
2023/05/02 16:44:03.609994109 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Called-Station-Id   [30]
2023/05/02 16:44:03.609989329 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:   Cisco AVpair       [1]
2023/05/02 16:44:03.609985171 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Vendor, Cisco       [26]
2023/05/02 16:44:03.609981606 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:   Cisco AVpair       [1]
2023/05/02 16:44:03.609976961 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Vendor, Cisco       [26]
2023/05/02 16:44:03.609969166 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  User-Name           [1]
2023/05/02 16:44:03.609963241 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  authenticator 0b 99 e3
2023/05/02 16:44:03.609953614 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS: Send Accounting-Request
2023/05/02 16:44:03.609863172 {smd_RO-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Handl
2023/05/02 16:44:03.609695649 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAPOL pa
2023/05/02 16:44:03.609689224 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:unknown] Pkt body
2023/05/02 16:44:03.609686794 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAP Pack
2023/05/02 16:44:03.609683919 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Sent EAP
2023/05/02 16:44:03.609334292 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Sending
2023/05/02 16:44:03.609332867 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Setting
2023/05/02 16:44:03.609310820 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Posting
2023/05/02 16:44:03.609284841 {smd_RO-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Raisi
```

跟踪示例

此部分包括完全失败事务（服务器拒绝客户端凭证）的dot1x和radius组件的会话管理器跟踪。它旨在为导航与前面板身份验证相关的系统跟踪提供基本指导。

- 测试客户端尝试连接到GigabitEthernet1/0/2，但被拒绝。

在本示例中，SMD组件跟踪设置为“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：开始

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 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 l
[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请求身份

```
[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:idle request action
```

EAPoL：EAP响应

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 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 0x0A
[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 Radiu
[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：访问请求

```
[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：访问质询

```
[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 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响应

```
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：访问请求

```
[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 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：访问质询

```
[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 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请求

```
[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 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response request action
```

EAPoL：EAP响应

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 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 0x0A
[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 Radiu
[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：访问请求

```
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 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：访问拒绝

```
[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 0x0A0000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting authenticating st
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering authc result sta
[errmsg]: [16498]: UUID: 0, ra: 0 (note): %DOT1X-5-FAIL: Authentication failed for client (0040.E93E.00
[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 0x0A000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: held
```

EAPoL：EAP拒绝

```
[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] Posting FAILOVER_RETRY on Client 0x0A
[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 EA
[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 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 ente
[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
```

其他信息

默认设置

功能	默认设置
交换机802.1x启用状态	禁用.
每端口802.1x启用状态	已禁用（强制授权）。 端口发送和接收正常流量，而无需对客户端进行基于802.1x的身份验证。
AAA	禁用.
RADIUS 服务器 • IP 地址 • UDP身份验证端口 • 默认记帐端口 • 密钥	• 未指定。 • 1645. • 1646. • 未指定。

功能	默认设置
主机模式	单主机模式。
控制方向	双向控制。
定期重新进行身份验证	禁用.
重新身份验证尝试之间的秒数	3600 秒.
重新验证号码	2次（端口变为未授权状态之前交换机重新启动身份验证过程的次数）。
等待周期	60秒（在与客户端进行身份验证交换失败后交换机保持静默状态的秒数）。
重新传输时间	30秒（在重新发送请求之前，交换机等待来自客户端的EAP请求/身份帧响应的秒数）。
最大重新传输次数	2次（在重新启动身份验证过程之前，交换机发送EAP请求/身份帧的次数）。
客户端超时时间	30秒（将来自身份验证服务器的请求中继到客户端时，交换机在将请求重新发送到客户端之前等待响应的时间。）
身份验证服务器超时时间	30秒（当从客户端向身份验证服务器中继响应时，交换机在将响应重新发送到服务器之前等待应答的时间。） 您可以使用dot1x timeout server-timeout接口配置命令更改此超时时段。
非活动超时	禁用.
访客 VLAN	未指定。
无法访问的身份验证绕行	禁用.

功能	默认设置
受限制的VLAN	未指定。
身份验证器（交换机）模式	未指定。
MAC身份验证绕行	禁用.
语音感知安全	禁用.

可选设置

定期重新进行身份验证

您可以启用定期802.1x客户端重新身份验证并指定其发生频率：

- authentication periodic -启用客户端的定期重新身份验证
- inactivity -以秒为单位的时间间隔，如果在此间隔后没有来自客户端的活动，则表示它未经授权
- reauthenticate -以秒为单位的时间，超过此时间将自动重新身份验证尝试启动
- restartvalue -尝试对未授权的端口进行身份验证之前经过的间隔（以秒为单位）
- unauthorizedvalue —删除未授权会话之前经过的秒间隔

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

违规模式

您可以配置802.1x端口，使其关闭、生成系统日志错误，或者在设备连接到已启用802.1x的端口或端口上已验证有关设备的最大允许数量时丢弃来自新设备的数据包。

- shutdown -禁用端口时出错。
- restrict -生成系统日志错误。
- protect -丢弃来自向端口发送流量的任何新设备的数据包。
- replace -删除当前会话并使用新主机进行身份验证。

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

更改静默期

authentication timer restart 接口配置命令控制空闲期，它规定了交换机无法对客户端进行身份验证之后保持空闲的设置时间段。值的范围是1到65535秒。

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

更改交换机到客户端的重传时间

客户端使用EAP响应/身份帧响应来自交换机的EAP请求/身份帧。如果交换机没有收到此响应，它将等待一段时间（称为重新传输时间），然后重新发送帧。

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

设置交换机到客户端的帧重新传输编号

您可以更改交换机在重新启动身份验证过程之前向客户端发送EAP请求/身份帧（假设未收到响应）的次数。 范围是从 1 到 10。

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

配置主机模式

您可以在802.1x授权端口上允许多个主机（客户端）。

- multi-auth -在语音VLAN和数据VLAN上允许使用多个经过身份验证的客户端。
- 多主机- 在单个主机通过身份验证后，允许在802.1x授权的端口上存在多个主机。
- multi-domain -允许在采用IEEE 802.1x授权的端口上同时验证主机和语音设备，例如IP电话（思科或非思科）。

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

启用MAC移动

MAC移动允许经过身份验证的主机从设备的一个端口移动到另一个端口。

```
authentication mac-move permit
```

启用MAC替换

MAC replace允许主机替换端口上经过身份验证的主机。

- 保护-端口丢弃具有意外MAC地址的数据包而不生成系统消息。
- restrict - CPU将丢弃违规数据包，并生成系统消息。
- shutdown - 端口在收到意外的MAC地址时因错误而被禁用。

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

设置重新身份验证号码

您还可以更改端口变为未授权状态之前设备重新启动身份验证过程的次数。 范围为0至10

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

配置访客VLAN

配置访客VLAN时，如果服务器未收到对其EAP请求/身份帧的响应，则不支持802.1x的客户端将被放入访客VLAN中。

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

配置受限制的VLAN

在设备上配置受限制的VLAN时，如果身份验证服务器未收到有效的用户名和密码，则符合IEEE 802.1x标准的客户端将移至受限制的VLAN。

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

在受限制的VLAN上配置身份验证尝试次数

您可以使用authentication event fail retryretry countinterface configuration命令配置将用户分配到受限制的VLAN之前允许的最大身份验证尝试次数。允许的身份验证尝试的范围是1到3。

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

为关键语音VLAN配置802.1x无法访问的身份验证绕行

您可以在端口上配置重要的语音VLAN并启用无法访问的身份验证绕行功能。

- authorize - 将尝试进行身份验证的任何新主机移到用户指定的关键VLAN
- reinitialize - 将端口上的所有授权主机移到用户指定的关键VLAN

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

配置使用WoL的802.1x身份验证

您可以启用LAN唤醒(WoL)的802.1x身份验证

```
authentication control-direction both
```

配置MAC身份验证绕行

```
mab
```

配置灵活的身份验证排序

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

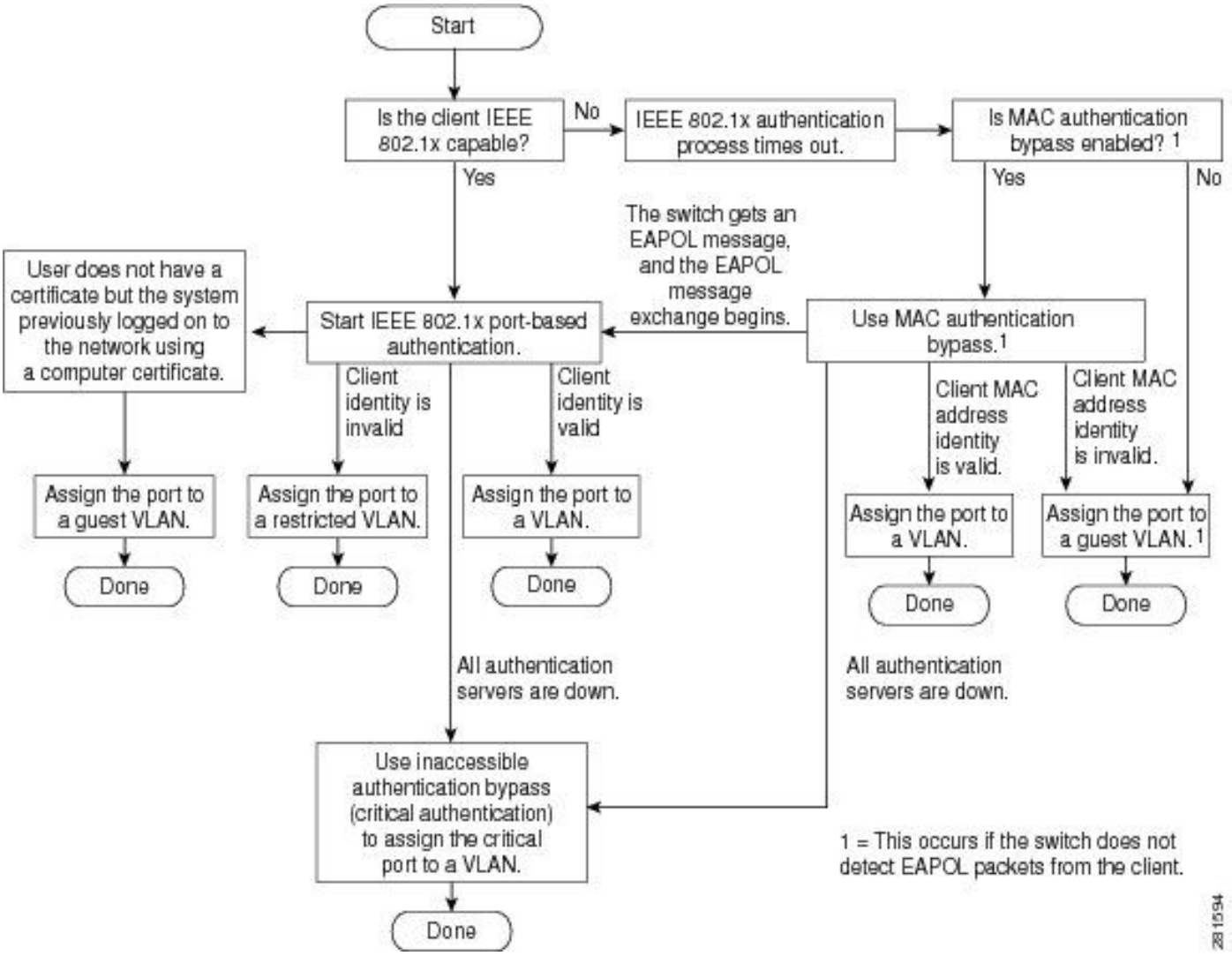
配置语音感知802.1x安全

在设备上使用语音感知802.1x安全功能可以只禁用发生安全违规的VLAN，无论是数据还是语音VLAN。 在数据VLAN上发现的安全违规仅导致数据VLAN关闭。这是全局配置。

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

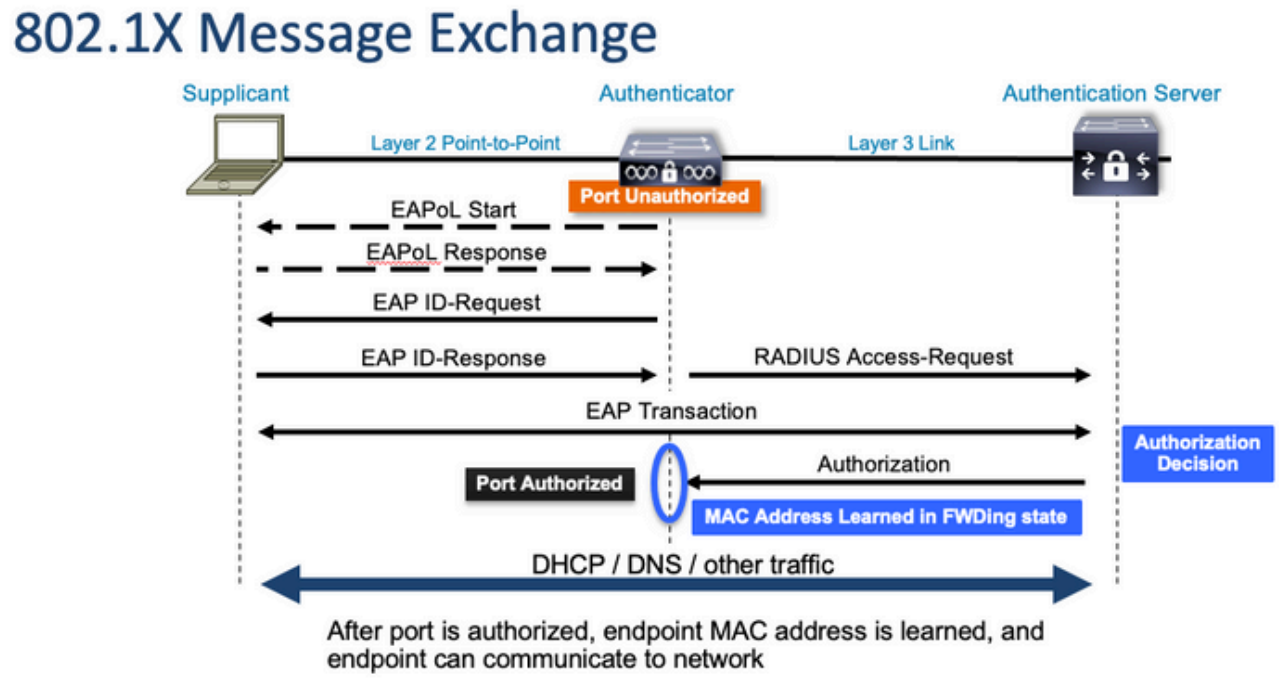
流程图

身份验证流程图



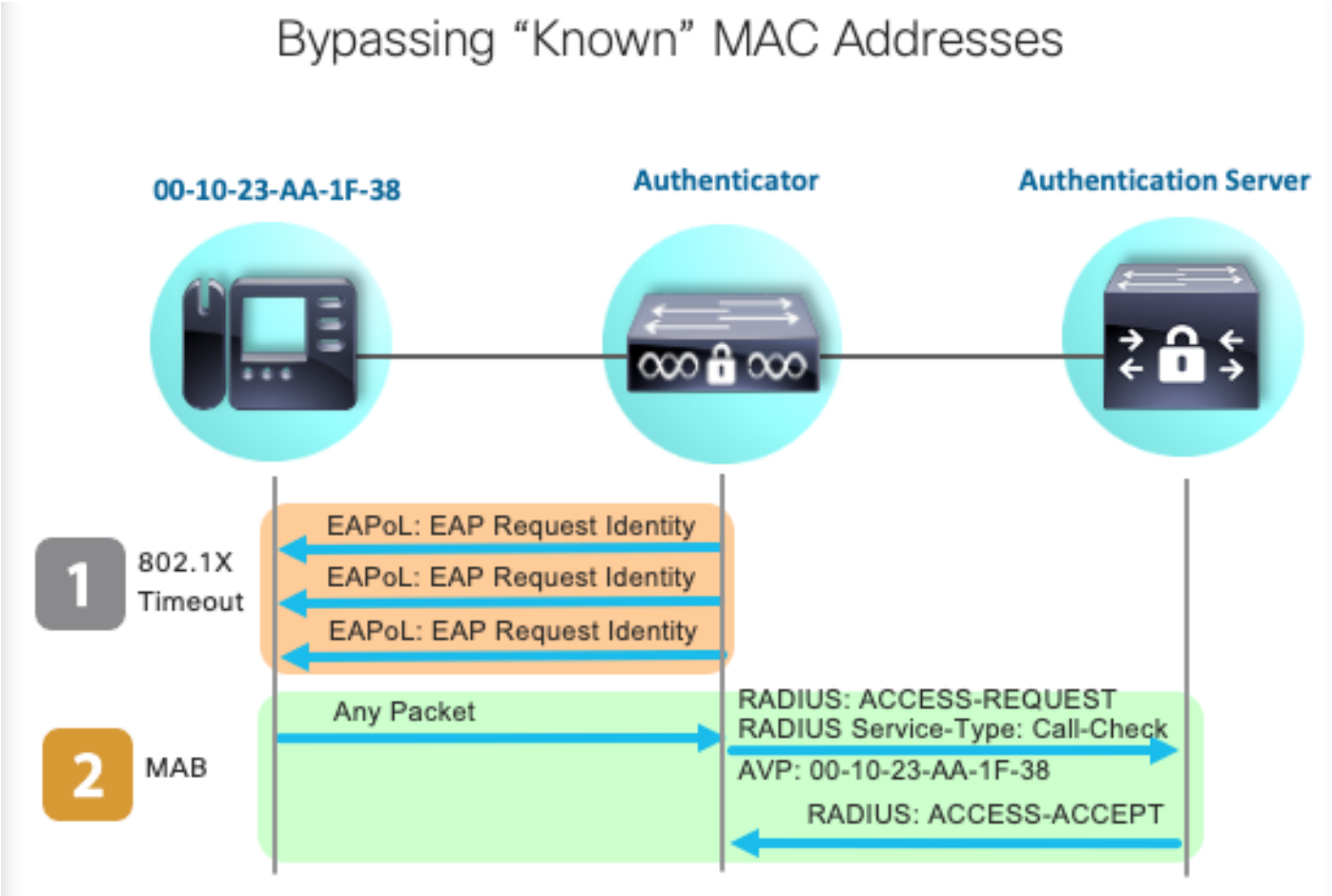
基于端口的身份验证发起和消息交换

此图显示客户端发起到RADIUS服务器的消息交换。



MAB身份验证启动和消息交换

此图显示MAC身份验证绕行(MAB)期间的消息交换



相关信息

- 解密RADIUS服务器配置
- MAC身份验证绕行部署指南
- 有线802.1x部署指南
- Catalyst 9300 SPAN配置指南
- Catalyst 9300 EPC配置指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。