

# 在ACS 5.3的EAP验证用接入点

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[与GUI的配置](#)

[定义身份验证服务器](#)

[配置 ACS](#)

[配置SSID](#)

[与CLI的配置](#)

[验证](#)

[故障排除](#)

[调试dot11 aaa验证器状态机](#)

[debug radius authentication](#)

[debug aaa authentication](#)

## 简介

本文描述基于Cisco IOS软件的接入点(AP)的配置示例无线用户的可扩展的认证协议(EAP)验证的RADIUS服务器访问的数据库。

AP桥接从客户端的无线数据包到有线的数据包被注定对认证服务器反之亦然。由于AP在EAP扮演此被动角色，此配置与实际上所有EAP方法一起使用。这些方法包括，但是没有被限制对，轻的EAP (LEAP)， Protected EAP (PEAP) -微软询问握手认证协议(MSCHAP)版本2， PEAP通用的令牌卡(GTC)， EAP灵活验证通过获取建立隧道(快速)， 传输层安全(TLS)和EAP被建立隧道的TLS (TTL)。必须针对每种 EAP 方法适当配置身份验证服务器。

本文描述如何配置AP和RADIUS服务器，是思科安全访问控制服务器(ACS) 5.3在此配置示例方面。

## [先决条件](#)

## [要求](#)

Cisco 建议您了解以下主题：

- 与Cisco IOS软件GUI或命令行界面(CLI)的熟悉

- 与EAP验证的概念的熟悉

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Aironet运行Cisco IOS软件版本15.2(2)JB的3602接入点
- 思科安全访问控制服务器5.3

此配置示例假设只有在网络的一个VLAN。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

本文使用此配置GUI和CLI：

- AP的IP地址是10.105.136.11。
- RADIUS服务器(ACS)的IP地址是10.106.55.91。

## 与GUI的配置

### 定义身份验证服务器

此步骤描述如何定义认证服务器和建立与它的一关系。

1. 在AP GUI中，请导航给**安全>Server管理器**。
2. 在公司服务器中请在服务器字段区分，输入认证服务器(**10.106.55.91**)的IP地址。
3. 指定共享塞克雷、认证端口和计费端口。您能使用端口1813，1814或者1645，1646。
4. 单击**应用**为了创建定义和填充下拉列表。
5. 在默认服务器优先级部分，设置EAP验证Priority1字段为服务器IP地址(**10.106.55.91**)。
6. 单击 **Apply**。

### 配置 ACS

如果派遣用户到外部RADIUS服务器，AP需要是此外部RADIUS服务器的一个验证、授权和统计(AAA)客户端。此步骤描述如何配置ACS。

1. 在Cisco Secure ACS GUI中，请点击**网络资源**。在ACS 5.3，设备可以由位置分组。

2. 创建位置。在网络设备组下，请点击**位置**。单击**创建新的位置**。在Name字段，请输入位置名称(IOS\_lab)。输入一说明(IOS LAB)此位置的。选择常规**所有位置**作为帕伦特位置。单击**提交验证**。

3. 创建IOS的AP一组。点击**设备类型**。单击**创建**创建一新的组。在Name字段，请输入组名(IOS\_APs)。输入一说明(IOS AP在实验室里)此组的。选择**所有设备类型**作为帕伦特。单击**提交验证**。

4. 添加AP。点击**网络设备和AAA客户端**。在Name字段，请输入名称您的IOS AP (AP)。输入该AP的(IOS AP)一说明。

在网络设备组下，在Location字段旁边，请点击**精选**，在IOS\_lab旁边检查方框，并且点击OK键验证。在IP地址下，单个IP地址请务必启用，并且输入您的AP (10.105.136.11)的IP地址。

在认证选项下，请检查**RADIUS**。在**共享秘密**字段，请输入机密(思科)。保持其他值对他们的默认。单击**提交验证**。

5. 添加无线用户凭证。导航给**用户，并且标识存储>标识组**。单击**创建**创建一新的组。在Name字段，请输入组名(EAP\_Users)。输入说明(EAP无线的用户)。单击**提交验证**。

6. 创建一个用户在此组中。点击**用户**。单击**创建**创建新用户。在Name字段，请输入用户名(radius)。保证用户状态**启用**。输入用户的(测验radius)一说明。在标识Group字段旁边，请点击**精选**，在EAP\_Users旁边检查方框，并且点击OK键验证。

在密码信息下，请进入在密码的<password>并且确认密码字段。由于对网络的此用户需要访问，但是不需要对任何Cisco设备的访问管理的，没有需要对于特权密码。

7. 单击**提交验证**。新用户列表出现，并且ACS当前准备好。

8. 导航对**策略元素>授权和权限>网络访问>授权配置文件**为了验证用户是授权访问权限。应该有PermitAccess配置文件。接收此配置文件的用户是授权访问对网络。

9. 导航到**访问策略>Access Services>默认设备Admin**检查授权。确保**标识、组映射和授权**被检查。

10. 点击**允许Protocols选项**，选择需要的EAP方法的方框，并且单击**提交验证**。

## 配置SSID

此步骤描述如何配置在AP的服务集标识(SSID)。

1. 在Cisco Secure ACS GUI中，请导航给**安全> SSID管理器**。点击**新**，输入SSID名称 (**radius**)，启用两个无线接口，并且单击**应用**。

2. 导航给**安全>加密管理器**，挑选**AES CCMP**作为密码器，并且点击**全部应用**应用在两无线电的此加密。

3. 导航给**安全> SSID管理器**，并且选择**radius** SSID。在客户端验证设置部分，请用从下拉列表和检查**网络EAP的EAP检查开放式验证**，精选。

在客户端验证密钥管理部分，请选择**必须**从密钥管理下拉列表，检查**Enable (event) WPA**，并且选择从下拉列表的**WPAv2**。单击 **Apply**。

4. 为了广播在两无线电的此SSID，请查找关于同一个页的**guest模式/基础结构SSID**设置部分。对于两无线电，设置信标模式为**单个BSSID**，并且选择SSID名称(**radius**)从集合单个**guest模式** SSID下拉列表。单击 **Apply**。

5. 导航对**网络>网络接口> Radio0-802.11n 2G.Hz >设置>enable**为了启用两个无线接口。

6. 测试客户端连接。

## 与CLI的配置

注意：

使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

这是在CLI内被执行的相同的配置：

```
show run
Building configuration...

Current configuration : 2511 bytes
!
! Last configuration change at 01:17:48 UTC Mon Mar 1 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$1u04$j7DG0DC5KZ6bVaSYUhck0
!
aaa new-model
!
!
aaa group server radius rad_eap
  server 10.106.55.91
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
!
!
!
aaa session-id common
ip cef
!
ip dhcp pool test
!
!
!
dot11 syslog
!
dot11 ssid radius
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2
  guest-mode
!
!
```

```
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
no ip address
!
encryption mode ciphers aes-ccm
!
ssid radius
!
antenna gain 0
stbc
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
!
encryption mode ciphers aes-ccm
!
ssid radius
!
antenna gain 0
dfs band 3 block
stbc
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
duplex auto
speed auto
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface BVI1
ip address 10.105.136.11 255.255.255.128
!
ip default-gateway 10.105.136.1
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.105.136.1
ip radius source-interface BVI1
```

```
!  
radius-server attribute 32 include-in-access-req format %h  
radius-server host 10.106.55.91 key 7 00271A1507545A545C606C  
radius-server vsa send accounting  
!  
bridge 1 route ip  
!  
!  
!  
line con 0  
line vty 0 4  
  transport input all  
!  
end
```

## 验证

使用本部分可确认配置能否正常运行。

联络客户端;在成功认证以后，这是在AP GUI出版的配置汇总：

**注意：** [命令输出解释程序工具 \( 仅限注册用户 \)](#) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

在CLI中，请输入**show dot11 associations**命令为了确认配置：

```
ap#show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [radius] :
```

MAC Address	IP address	Device	Name	Parent	State
f8db.7f75.7804	10.105.136.116	unknown	-	self	EAP-Assoc

您能也输入**show radius server-group all**命令为了显示所有已配置的RADIUS服务器组列表AP的。

## 故障排除

此步骤描述如何排除故障您的配置。

1. 在客户端工具或软件里，请创建一新配置文件或连接以同样或相似的参数为了保证什么都没变得损坏在客户端配置里。
2. 无线电频率(RF)问题可以防止成功认证。临时禁用验证为了排除此可能性：

从CLI，请输入这些命令：

**没有验证开放eap eap\_methods没有authentication network-eap eap\_methods开放的验证**

从GUI，在SSID管理器页，请不选定**网络EAP**，检查**开放**，并且设置下拉列表为**没有新增内容**。

如果客户端成功关联，则 RF 与关联问题无关。

### 3. 验证共享加密口令同步在AP和认证服务器之间。否则，您也许收到此错误消息：

Invalid message authenticator in EAP request从CLI，请检查线路：

radius-server host x.x.x.x auth-port x acct-port x key <shared\_secret>从GUI，在Server Manager页，请在共享秘密字段重新输入适当的服务器的共享机密。

AP的共享秘密条目在RADIUS服务器必须包含同样共享的加密口令。

### 4. 从 RADIUS 服务器删除所有用户组。冲突能发生在基础域的RADIUS服务器定义的用户组和用户组之间。检查RADIUS服务器的日志失败的尝试和失败的原因。

**注意：**使用 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

请使用这些调试指令为了调查和显示在设备中的协商：

- `debug dot11 aaa 验证器状态机`
- `debug radius authentication`
- `debug aaa authentication`

## 调试dot11 aaa验证器状态机

此命令显示主要部门(或状态)在客户端和认证服务器之间的协商。这是从成功认证的一个输出示例：

```
ap#debug dot11 aaa authenticator state-machine
state machine debugging is on
ap#
*Mar 1 01:38:34.919: dot11_auth_dot1x_send_id_req_to_client: Sending identity request to f8db.7f75.7804
*Mar 1 01:38:34.919: dot11_auth_dot1x_send_id_req_to_client: Client f8db.7f75.7804 timer started for 30 seconds
*Mar 1 01:38:35.431: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT, CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.431: dot11_auth_dot1x_send_response_to_server: Sending client f8db.7f75.7804 data to server
*Mar 1 01:38:35.431: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds
*Mar 1 01:38:35.435: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT, SERVER_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.435: dot11_auth_dot1x_send_response_to_client: Forwarding server message to client f8db.7f75.7804
*Mar 1 01:38:35.435: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 30 seconds
*Mar 1 01:38:35.443: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT, CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.443: dot11_auth_dot1x_send_response_to_server: Sending client f8db.7f75.7804 data to server
*Mar 1 01:38:35.443: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds
*Mar 1 01:38:35.447: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT, SERVER_REPLY) for f8db.7f75.7804
```



```

*Mar 1 01:38:35.447: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:35.447: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
-----Lines Omitted for simplicity-----
*Mar 1 01:38:36.663: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar 1 01:38:36.663: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:36.663: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar 1 01:38:36.667: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:36.667: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar 1 01:38:36.667: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar 1 01:38:36.671: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_PASS) for f8db.7f75.7804
*Mar 1 01:38:36.671: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:36.671: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar 1 01:38:36.719: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]

```

## debug radius authentication

此命令显示在服务器和客户端之间的RADIUS协商，其中之二由AP桥接。这是从成功认证的一个输出示例：

```
ap#debug radius authentication
```

```

*Mar 1 01:50:50.635: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: ssid [347] 6
*Mar 1 01:50:50.635: RADIUS: 72 61 64 69 [ radi]
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: service-type [345] 4 1
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: interface [222] 3
*Mar 1 01:50:50.635: RADIUS: 32 [ 2]
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IPv6:
*Mar 1 01:50:50.635: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.635: RADIUS(000001F6): sending
*Mar 1 01:50:50.635: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
id 1645/73, len 140
*Mar 1 01:50:50.635: RADIUS: authenticator 0F 74 18 0E F3 08 ED 51 -
8B EA F7 31 AC C9 CA 6B
*Mar 1 01:50:50.635: RADIUS: User-Name [1] 8 "radius"
*Mar 1 01:50:50.635: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 01:50:50.635: RADIUS: Called-Station-Id [30] 26 "1C-E6-C7-E1-D8-90:
radius"
*Mar 1 01:50:50.635: RADIUS: Calling-Station-Id [31] 16 "f8db.7f75.7804"
*Mar 1 01:50:50.635: RADIUS: Service-Type [6] 6 Login [1]
*Mar 1 01:50:50.635: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.635: RADIUS: E3 E1 50 F8 2B 22 26 84 C1 F1 76 28 79 70 5F 78
[ P+"&v{yp_x}]
*Mar 1 01:50:50.635: RADIUS: EAP-Message [79] 13
*Mar 1 01:50:50.635: RADIUS: 02 01 00 0B 01 72 61 64 69 75 73
[ radius]
*Mar 1 01:50:50.635: RADIUS: NAS-Port-Type [61] 6 802.11 wireless
[19]

```

```

*Mar 1 01:50:50.635: RADIUS: NAS-Port [5] 6 282
*Mar 1 01:50:50.635: RADIUS: NAS-Port-Id [87] 5 "282"
*Mar 1 01:50:50.635: RADIUS: NAS-IP-Address [4] 6 10.105.136.11
*Mar 1 01:50:50.635: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 01:50:50.635: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:50.635: RADIUS(000001F6): Started 5 sec timeout
*Mar 1 01:50:50.639: RADIUS: Received from id 1645/73 10.106.55.91:1645, Access
-Challenge, len 94
*Mar 1 01:50:50.639: RADIUS: authenticator 5E A4 A7 B9 01 CC F4 20 -
2E D0 2A 1A A4 58 05 9E
*Mar 1 01:50:50.639: RADIUS: State [24] 32
*Mar 1 01:50:50.639: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.639: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [ 1
/165489511/9;]
*Mar 1 01:50:50.639: RADIUS: EAP-Message [79] 24
*Mar 1 01:50:50.639: RADIUS: 01 DC 00 16 11 01 00 08 00 CB 2A 0A 74 B3 77 AF
72 61 64 69 75 73 [ *twradius]
*Mar 1 01:50:50.639: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.643: RADIUS: CC 44 D5 FE FC 86 BC 2D B0 89 61 69 4F 34 D1 FF
[ D-ai04]
*Mar 1 01:50:50.643: RADIUS(000001F6): Received from id 1645/73
*Mar 1 01:50:50.643: RADIUS/DECODE: EAP-Message fragments, 22, total 22 bytes
*Mar 1 01:50:50.647: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: ssid [347] 6
*Mar 1 01:50:50.647: RADIUS: 72 61 64 69 [ radi]
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: service-type [345] 4
1
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: interface [222] 3
*Mar 1 01:50:50.647: RADIUS: 32 [ 2]
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IPv6:
*Mar 1 01:50:50.647: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.647: RADIUS(000001F6): sending
*Mar 1 01:50:50.647: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
id 1645/74, len 167
*Mar 1 01:50:50.647: RADIUS: authenticator C6 54 54 B8 58 7E ED 60 - F8 E0 2E
05 B0 87 3B 76
*Mar 1 01:50:50.647: RADIUS: User-Name [1] 8 "radius"
*Mar 1 01:50:50.647: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 01:50:50.647: RADIUS: Called-Station-Id [30] 26 "1C-E6-C7-E1-D8-90:
radius"
*Mar 1 01:50:50.647: RADIUS: Calling-Station-Id [31] 16 "f8db.7f75.7804"
*Mar 1 01:50:50.647: RADIUS: Service-Type [6] 6 Login
[1]
*Mar 1 01:50:50.647: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.647: RADIUS: FE 15 7B DB 49 FE 27 C5 BC E2 FE 83 B9 25 8C 1F
[ {I'?}
*Mar 1 01:50:50.647: RADIUS: EAP-Message [79] 8
*Mar 1 01:50:50.647: RADIUS: 02 DC 00 06 03 19
*Mar 1 01:50:50.647: RADIUS: NAS-Port-Type [61] 6 802.11 wireless
[19]
*Mar 1 01:50:50.647: RADIUS: NAS-Port [5] 6 282
*Mar 1 01:50:50.647: RADIUS: NAS-Port-Id [87] 5 "282"
*Mar 1 01:50:50.647: RADIUS: State [24] 32
*Mar 1 01:50:50.647: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.647: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [ 1
/165489511/9;]
*Mar 1 01:50:50.647: RADIUS: NAS-IP-Address [4] 6 10.105.136.11
*Mar 1 01:50:50.647: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 01:50:50.647: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:50.647: RADIUS(000001F6): Started 5 sec timeout

```

```

*Mar 1 01:50:50.647: RADIUS: Received from id 1645/74 10.106.55.91:1645, Access
-Challenge, len 78
*Mar 1 01:50:50.647: RADIUS: authenticator 0E 81 99 9E EE 39 50 FB - 6E 6D 93
8C 8E 29 94 EC
*Mar 1 01:50:50.647: RADIUS: State [24] 32
*Mar 1 01:50:50.651: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.651: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [ 1
/165489511/9;]
*Mar 1 01:50:50.651: RADIUS: EAP-Message [79] 8
*Mar 1 01:50:50.651: RADIUS: 01 DD 00 06 19 21 [ !]
*Mar 1 01:50:50.651: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.651: RADIUS: A8 54 00 89 1F 2A 01 52 FE FA D2 58 2F E5 F2 86
[ T*RX/]
*Mar 1 01:50:50.651: RADIUS(000001F6): Received from id 1645/74
*Mar 1 01:50:50.651: RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
*Mar 1 01:50:50.655: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: ssid [347] 6
*Mar 1 01:50:50.655: RADIUS: 72 61 64 69 [ radi]
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: service-type [345] 4
1
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: interface [222] 3

```

-----Lines Omitted for simplicity-----

```

11 [ l2^w$qM{60]
*Mar 1 01:50:51.115: RADIUS: NAS-Port-Type [61] 6 802.11 wireless
[19]
*Mar 1 01:50:51.115: RADIUS: NAS-Port [5] 6 282
*Mar 1 01:50:51.115: RADIUS: NAS-Port-Id [87] 5 "282"
*Mar 1 01:50:51.115: RADIUS: State [24] 32
*Mar 1 01:50:51.115: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:51.115: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [ 1
/165489511/9;]
*Mar 1 01:50:51.115: RADIUS: NAS-IP-Address [4] 6 10.105.136.11
*Mar 1 01:50:51.115: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 01:50:51.115: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:51.115: RADIUS(000001F6): Started 5 sec timeout
*Mar 1 01:50:51.115: RADIUS: Received from id 1645/80 10.106.55.91:1645, Access
-Challenge, len 115
*Mar 1 01:50:51.115: RADIUS: authenticator 74 CF 0F 34 1F 1B C1 CF -
E9 27 79 D5 F8 9C 5C 50
*Mar 1 01:50:51.467: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]

```

## debug aaa authentication

此命令显示验证的AAA协商在客户端设备和认证服务器之间。

```
ap#debug radius authentication
```

```

*Mar 1 01:50:50.635: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: ssid [347] 6
*Mar 1 01:50:50.635: RADIUS: 72 61 64 69 [ radi]
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: service-type [345] 4 1
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: interface [222] 3
*Mar 1 01:50:50.635: RADIUS: 32 [ 2]
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IPv6:
*Mar 1 01:50:50.635: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11

```

```

*Mar 1 01:50:50.635: RADIUS(000001F6): sending
*Mar 1 01:50:50.635: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
id 1645/73, len 140
*Mar 1 01:50:50.635: RADIUS: authenticator 0F 74 18 0E F3 08 ED 51 -
8B EA F7 31 AC C9 CA 6B
*Mar 1 01:50:50.635: RADIUS: User-Name [1] 8 "radius"
*Mar 1 01:50:50.635: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 01:50:50.635: RADIUS: Called-Station-Id [30] 26 "1C-E6-C7-E1-D8-90:
radius"
*Mar 1 01:50:50.635: RADIUS: Calling-Station-Id [31] 16 "f8db.7f75.7804"
*Mar 1 01:50:50.635: RADIUS: Service-Type [6] 6 Login [1]
*Mar 1 01:50:50.635: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.635: RADIUS: E3 E1 50 F8 2B 22 26 84 C1 F1 76 28 79 70 5F 78
[ P+"&v(yp_x)]
*Mar 1 01:50:50.635: RADIUS: EAP-Message [79] 13
*Mar 1 01:50:50.635: RADIUS: 02 01 00 0B 01 72 61 64 69 75 73
[ radius]
*Mar 1 01:50:50.635: RADIUS: NAS-Port-Type [61] 6 802.11 wireless
[19]
*Mar 1 01:50:50.635: RADIUS: NAS-Port [5] 6 282
*Mar 1 01:50:50.635: RADIUS: NAS-Port-Id [87] 5 "282"
*Mar 1 01:50:50.635: RADIUS: NAS-IP-Address [4] 6 10.105.136.11
*Mar 1 01:50:50.635: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 01:50:50.635: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:50.635: RADIUS(000001F6): Started 5 sec timeout
*Mar 1 01:50:50.639: RADIUS: Received from id 1645/73 10.106.55.91:1645, Access
-Challenge, len 94
*Mar 1 01:50:50.639: RADIUS: authenticator 5E A4 A7 B9 01 CC F4 20 -
2E D0 2A 1A A4 58 05 9E
*Mar 1 01:50:50.639: RADIUS: State [24] 32
*Mar 1 01:50:50.639: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.639: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [ 1
/165489511/9;]
*Mar 1 01:50:50.639: RADIUS: EAP-Message [79] 24
*Mar 1 01:50:50.639: RADIUS: 01 DC 00 16 11 01 00 08 00 CB 2A 0A 74 B3 77 AF
72 61 64 69 75 73 [ *twradius]
*Mar 1 01:50:50.639: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.643: RADIUS: CC 44 D5 FE FC 86 BC 2D B0 89 61 69 4F 34 D1 FF
[ D-ai04]
*Mar 1 01:50:50.643: RADIUS(000001F6): Received from id 1645/73
*Mar 1 01:50:50.643: RADIUS/DECODE: EAP-Message fragments, 22, total 22 bytes
*Mar 1 01:50:50.647: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: ssid [347] 6
*Mar 1 01:50:50.647: RADIUS: 72 61 64 69 [ radi]
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: service-type [345] 4
1
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: interface [222] 3
*Mar 1 01:50:50.647: RADIUS: 32 [ 2]
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IPv6:
*Mar 1 01:50:50.647: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.647: RADIUS(000001F6): sending
*Mar 1 01:50:50.647: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
id 1645/74, len 167
*Mar 1 01:50:50.647: RADIUS: authenticator C6 54 54 B8 58 7E ED 60 - F8 E0 2E
05 B0 87 3B 76
*Mar 1 01:50:50.647: RADIUS: User-Name [1] 8 "radius"
*Mar 1 01:50:50.647: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 01:50:50.647: RADIUS: Called-Station-Id [30] 26 "1C-E6-C7-E1-D8-90:
radius"
*Mar 1 01:50:50.647: RADIUS: Calling-Station-Id [31] 16 "f8db.7f75.7804"
*Mar 1 01:50:50.647: RADIUS: Service-Type [6] 6 Login

```

```
[1]
*Mar 1 01:50:50.647: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.647: RADIUS: FE 15 7B DB 49 FE 27 C5 BC E2 FE 83 B9 25 8C 1F
[ {I'?' ]
*Mar 1 01:50:50.647: RADIUS: EAP-Message [79] 8
*Mar 1 01:50:50.647: RADIUS: 02 DC 00 06 03 19
*Mar 1 01:50:50.647: RADIUS: NAS-Port-Type [61] 6 802.11 wireless
[19]
*Mar 1 01:50:50.647: RADIUS: NAS-Port [5] 6 282
*Mar 1 01:50:50.647: RADIUS: NAS-Port-Id [87] 5 "282"
*Mar 1 01:50:50.647: RADIUS: State [24] 32
*Mar 1 01:50:50.647: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.647: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [ 1
/165489511/9;]
*Mar 1 01:50:50.647: RADIUS: NAS-IP-Address [4] 6 10.105.136.11
*Mar 1 01:50:50.647: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 01:50:50.647: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:50.647: RADIUS(000001F6): Started 5 sec timeout
*Mar 1 01:50:50.647: RADIUS: Received from id 1645/74 10.106.55.91:1645, Access
-Challenge, len 78
*Mar 1 01:50:50.647: RADIUS: authenticator 0E 81 99 9E EE 39 50 FB - 6E 6D 93
8C 8E 29 94 EC
*Mar 1 01:50:50.647: RADIUS: State [24] 32
*Mar 1 01:50:50.651: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.651: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [ 1
/165489511/9;]
*Mar 1 01:50:50.651: RADIUS: EAP-Message [79] 8
*Mar 1 01:50:50.651: RADIUS: 01 DD 00 06 19 21 [ !]
*Mar 1 01:50:50.651: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.651: RADIUS: A8 54 00 89 1F 2A 01 52 FE FA D2 58 2F E5 F2 86
[ T*RX/]
*Mar 1 01:50:50.651: RADIUS(000001F6): Received from id 1645/74
*Mar 1 01:50:50.651: RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
*Mar 1 01:50:50.655: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: ssid [347] 6
*Mar 1 01:50:50.655: RADIUS: 72 61 64 69 [ radi]
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: service-type [345] 4
1
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: interface [222] 3
```

-----Lines Omitted for simplicity-----

```
11 [ 12^w$QM{60]
*Mar 1 01:50:51.115: RADIUS: NAS-Port-Type [61] 6 802.11 wireless
[19]
*Mar 1 01:50:51.115: RADIUS: NAS-Port [5] 6 282
*Mar 1 01:50:51.115: RADIUS: NAS-Port-Id [87] 5 "282"
*Mar 1 01:50:51.115: RADIUS: State [24] 32
*Mar 1 01:50:51.115: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:51.115: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [ 1
/165489511/9;]
*Mar 1 01:50:51.115: RADIUS: NAS-IP-Address [4] 6 10.105.136.11
*Mar 1 01:50:51.115: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 01:50:51.115: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:51.115: RADIUS(000001F6): Started 5 sec timeout
*Mar 1 01:50:51.115: RADIUS: Received from id 1645/80 10.106.55.91:1645, Access
-Challenge, len 115
*Mar 1 01:50:51.115: RADIUS: authenticator 74 CF 0F 34 1F 1B C1 CF -
E9 27 79 D5 F8 9C 5C 50
*Mar 1 01:50:51.467: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]
```