# Autenticação de EAP em ACS 5.3 com Access point

## Índice



## Introdução

Este documento descreve uma configuração de exemplo de um Access Point (AP) com base no software do ® do Cisco IOS para a autenticação do Extensible Authentication Protocol (EAP) dos usuários Wireless contra um base de dados alcançado por um servidor Radius.

O AP constrói uma ponte sobre pacotes wireless do cliente nos pacotes prendidos destinados ao Authentication Server e vice-versa. Porque o AP joga este papel passivo no EAP, esta configuração é usada com virtualmente todos os métodos de EAP. Estes métodos incluem, mas não são limitados a, EAP claro (PULO), EAP protegido (PEAP) - versão 2 do protocolo microsoft challenge handshake authentication (MSCHAP), a placa de token PEAP-genérica (GTC), a Autenticação Flexível de EAP através do Tunelamento seguro (RÁPIDO), a Segurança da camada do EAP-transporte (TLS), e TLS EAP-em túnel (TTL). Você deve apropriadamente configurar o Authentication Server para cada um destes métodos de EAP.

Este documento descreve como configurar o AP e o servidor Radius, que é um Serviço de controle de acesso Cisco Secure (ACS) 5.3 nesta configuração de exemplo.

## Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Familiaridade com o Cisco IOS Software GUI ou o comando line interface(cli)
- Familiaridade com os conceitos da autenticação de EAP

## Componentes Utilizados

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

- Cisco Aironet 3602 Access point que executa o Cisco IOS Software Release 15.2(2)JB
- Serviço de controle de acesso Cisco Secure 5.3

Este exemplo de configuração supõe que há somente um VLAN na rede.

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

# Configurar

Este documento usa esta configuração para o GUI e o CLI:

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do AP é 10.105.136.11.
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius (o ACS) é 10.106.55.91.

## Configuração com GUI

### Defina o Authentication Server

Este procedimento descreve como definir o Authentication Server e estabelecer um relacionamento com ele.

1. No AP GUI, navegue à **Segurança > ao gerenciador do servidor**.
2. Nos servidores corporativos secione, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do Authentication Server (**10.106.55.91**) ao campo do server.
3. Especifique o segredo compartilhado, a porta de autenticação, e a porta de relatório. Você pode usar as portas 1813, 1814 ou 1645, 1646.
4. Clique **aplicam-se** a fim criar a definição e povoar as listas de drop-down.
5. Na seção de prioridades do server do padrão, ajuste o campo da prioridade 1 da

autenticação de EAP ao endereço IP do servidor (**10.106.55.91**).

6. Clique em Apply.

## Configurar o ACS

Se você envia usuários a um servidor de raio externo, o AP precisa de ser um cliente do Authentication, Authorization, and Accounting (AAA) para este servidor de raio externo. Este procedimento descreve como configurar o ACS.

1. No Cisco Secure ACS GUI, **recursos de rede do** clique. Em ACS 5.3, os dispositivos podem ser agrupados por lugar.

2. Crie um lugar. Sob grupos de dispositivo de rede, clique o **lugar**. O clique **cria o lugar novo**. No campo de nome, dê entrada com um nome do lugar (**IOS_lab**). Incorpore uma descrição (**LABORATÓRIO IO**) para este lugar. Selecione o general **todos os lugar** como o lugar do pai. O clique **submete-se** para validar.

3. Crie um grupo para os IO AP. Clique o **tipo de dispositivo**. O clique **cria** para criar um grupo novo. No campo de nome, dê entrada com um nome do grupo (**IOS_APs**). Incorpore uma descrição (**IO AP no LABORATÓRIO**) para este grupo. Selecione **todos os tipos de dispositivo** como o pai. O clique **submete-se** para validar.

4. Adicionar o AP. Clique **dispositivos de rede e clientes de AAA**. No campo de nome, dê entrada com o nome de seus IO AP (**AP**). Incorpore uma descrição para esse AP (**IO AP**).

   Sob grupos de dispositivo de rede, ao lado do campo do lugar, clique **seleto**, verifique a caixa ao lado de IOS_lab, e clique a **APROVAÇÃO** para validar. Sob o endereço IP de Um ou Mais Servidores Cisco ICM NT, seja certo que o único endereço IP de Um ou Mais Servidores Cisco ICM NT está permitido, e incorpora o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu AP (**10.105.136.11**).

   Sob opções de autenticação, verifique o **RAIO**. No campo **secreto compartilhado**, incorpore um segredo (**Cisco**). Mantenha os outros valores a seus padrões. O clique **submete-se** para validar.

5. Adicionar as credenciais do usuário Wireless. Navegue aos **usuários e a identidade armazena > grupos da identidade**. O clique **cria** para criar um grupo novo. No campo de nome, dê entrada com um nome do grupo (**EAP_Users**). Incorpore uma descrição (**usuários para o Sem fio EAP**). O clique **submete-se** para validar.

6. Crie um usuário neste grupo. Clique **usuários**. O clique **cria** para criar um novo usuário. No campo de nome, incorpore um username (**raio**). Assegure-se de que o estado do usuário **esteja permitido**. Incorpore uma descrição para o usuário (**raio do teste**). Ao lado do campo do grupo da identidade, clique **seleto**, verifique a caixa ao lado de EAP_Users, e clique a **APROVAÇÃO** para validar.

   Sob a informação de senha, inscreva o **<password> na** senha e confirme campos de senha. Porque este usuário precisa o acesso à rede mas não precisa o acesso a nenhum dispositivo Cisco para o Gerenciamento, não há nenhuma necessidade para uma senha da possibilidade.

7. O clique **submete-se** para validar. O novo usuário aparece na lista, e o ACS está agora pronto.

8. Navegue aos **elementos da política >** à **autorização e às permissões >** aos **perfis do acesso de rede >** da **autorização** a fim verificar que o usuário está concedido a permissão de acesso. Deve haver um perfil de PermitAccess. Os usuários que recebem este perfil são concedidos o acesso à rede.

9. Navegue ao **dispositivo Admin das políticas de acesso >** dos **serviços >** do **padrão do acesso** para examinar a autorização. Certifique-se de que a **identidade**, o **mapeamento do grupo**, e a **autorização** estão verificados.

10. Clique os **protocolos permitidos** aba, selecione as caixas para métodos de EAP exigidos, e o clique **submete-se** para validar.

## Configurar o SSID

Este procedimento descreve como configurar o Service Set Identifier (SSID) no AP.

1. No Cisco Secure ACS GUI, navegue à **Segurança >** ao **gerenciador de SSID**. Clique **novo**, dê entrada com o nome SSID (**raio**), permita ambas as interfaces de rádio, e o clique **aplica-se**.

2. Navegue à **Segurança >** ao **gerenciador de criptografia**, **AES** seleto **CCMP** como a cifra, e o clique **Aplicar tudo-se** para aplicar esta criptografia em ambos os rádios.

3. Navegue à **Segurança >** ao **gerenciador de SSID**, e selecione o **raio** SSID. Na authenticação do cliente os ajustes secionam, verificam a **autenticação aberta**, seleta **com o EAP da** lista de drop-down, e da **rede EAP da** verificação.

   No cliente a seção de gerenciamento chave autenticada, **imperativo** seleto da lista de drop-down do gerenciamento chave, verificação **permite o WPA**, e seleciona **WPAv2 da** lista de drop-down. Clique em Apply.

4. A fim transmitir este SSID em ambos os rádios, encontre a seção dos ajustes do modo de convidado/infraestrutura SSID na mesma página. Para ambos os rádios, ajuste o modo da baliza **para escolher BSSID**, e para selecionar o nome SSID (**raio**) da lista de drop-down do único modo de convidado SSID do grupo. Clique em Apply.

5. Navegue à **rede >** à **interface de rede >** ao **Radio0-802.11n 2G.Hz > ajustes > permitem** a fim permitir ambas as interfaces de rádio.

6. Teste a conectividade de cliente.

## Configuração com CLI

Notas:

Use a Command Lookup Tool ( somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Esta é a mesma configuração feita dentro do CLI:

```
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$1u04$jr7DG0DC5KZ6bVaSYUhck0
!
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
```

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Conecte o cliente; após a autenticação bem sucedida, este é o sumário de configuração que aparece no AP GUI:

> **Note**: Os determinados comandos de exibição dos apoios da ferramenta Output Interpreter (clientes registrados somente). Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

No CLI, inscreva o **comando show dot11 associations** a fim confirmar a configuração:

```
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
```

Você pode igualmente inscrever o **comando show radius server-group all** a fim indicar uma lista de todos os grupos de servidores configurados do RAIO no AP.

# Troubleshooting

Este procedimento descreve como pesquisar defeitos sua configuração.

1. Na utilidade ou no software do lado do cliente, crie um perfil ou uma conexão nova com o mesmo ou os parâmetros similares a fim assegurar-se de que nada se torne corrompido na configuração de cliente.

2. As edições do Radio Frequency (RF) podem impedir a autenticação bem sucedida. Temporariamente autenticação do desabilitação a fim eliminar esta possibilidade:

   Do CLI, incorpore estes comandos:

   **nenhuns eap_methods abertos do eap da autenticaçãonenhuns eap_methods da autenticação rede-EAPautenticação aberta**

   Do GUI, na página do gerenciador de SSID, desmarcar a **Rede EAP**, verifique **aberto**, e ajuste a lista de drop-down a **nenhuma adição**.

   Se o cliente associa com sucesso, o RF não contribui ao problema de associação.

3. Verifique que as senhas secundárias compartilhadas estão sincronizadas entre o AP e o Authentication Server. Se não, você pôde receber este Mensagem de Erro:

`Invalid message authenticator in EAP request`

Do CLI, verifique a linha:

**`radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>`**

Do GUI, na página do gerenciador do servidor, reenter o segredo compartilhado para o server apropriado no campo secreto compartilhado.

A entrada secreta compartilhada para o AP no servidor Radius deve conter a mesma senha secundária compartilhada.

4. Remova todos os grupos de usuário do servidor RADIUS. Os conflitos podem ocorrer entre os grupos de usuário definidos pelo servidor Radius e os grupos de usuário no domínio subjacente. Verifique os logs do servidor Radius falhas de tentativa e para ver se há as razões para as falhas.

**Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Use estes comandos debug a fim investigar e indicar as negociações entre dispositivos:

- **debugar a estado-máquina do autenticador aaa do dot11**
- **debugar a autenticação RADIUS**
- **debug aaa authentication**

## debugar a estado-máquina do autenticador aaa do dot11

Este comando indica divisões principais (ou estados) da negociação entre o cliente e o Authentication Server. Este é um exemplo de saída de uma autenticação bem sucedida:

```
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]
```

## debugar a autenticação RADIUS

Este comando indica as negociações de RADIUS entre o server e o cliente, ambo são construídas uma ponte sobre pelo AP. Este é um exemplo de saída de uma autenticação bem sucedida:

```
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-aiO4]
*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

Este comando indica as negociações AAA de autenticação entre o dispositivo do cliente e o Authentication Server.

```
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-aiO4]
*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]
```