Configurar SSIDs e VLANs em APs autônomos

Contents

Introduction

Este documento explica como configurar access points (APs) autônomos para:

- Redes locais virtuais (VLANs)
- Autenticação aberta
- 802.1x com Remote Authentication Dial-In User Service (RADIUS)
- 802.1x com RADIUS externo
- Chave pré-compartilhada (PSK)
- autenticação de endereço MAC
- Autenticação da Web (raio interno)
- Passagem da Web

Prerequisites

Requirements

A Cisco recomenda que você tenha um conhecimento básico sobre estes tópicos:

- 802,1x
- PSK
- RADIUS
- Autenticação da Web

Componentes Utilizados

As informações neste documento são baseadas no AP 3700 versão 15.3(3)JBB.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

> **Dica**: esses exemplos também se aplicam ao AP no modo autônomo dentro do ASA 5506, a diferença é que, em vez de configurar a porta do switch onde o AP está conectado, a configuração é aplicada ao Gig 1/9 do ASA.

Configurar

> **Observação**: os SSIDs (Service Set Identifiers Identificadores do Conjunto de Serviços) que pertencem à mesma VLAN não podem ser aplicados a um rádio ao mesmo tempo. Os exemplos de configuração dos SSIDs com a mesma VLAN não foram ativados ao mesmo tempo no mesmo AP.

Configurar VLAN-Switch e AP

Configure as VLANs necessárias no AP e no switch. Estas são as VLANs usadas neste exemplo:

- VLAN 2401 (nativa)
- VLAN 2402
- VLAN 2403

Configurar APs e VLANs

Configurar a interface Gigabit Ethernet

```
# conf t

# interface gig 0.2401
# encapsulation dot1q 2401 native

# interface gig 0.2402
# encapsulation dot1q 2402
# bridge-group 242

# interface gig 0.2403
# encapsulation dot1q 2403
# bridge-group 243
```

Configurar o rádio de interface 802.11a

```
# interface dot11radio 1.2401
# encapsulation dot1q 2401 native

# interface dot11radio 1.2402
# encapsulation dot1q 2402
# bridge-group 242

# interface dot11radio 1.2403
# encapsulation dot1q 2403
# bridge-group 243
```

> **Observação**: o rádio 802.11b (interface dot11radio 0) não está configurado, pois usa a VLAN nativa do AP.

Configurar a VLAN do Switch

```
# conf t
# vlan 2401-2403
```

Configure a interface onde o AP está conectado:

```
# conf t
# interface <port-id-where-AP-is-connected>
# switchport trunk encapsulation dot1q
# switchport mode trunk
# switchport trunk native vlan 2401
# switchport trunk allowed vlan 2401-2403
# spanning-tree portfast trunk
```

Autenticação aberta de SSID - VLAN nativa do AP

Esse SSID não tem segurança, é transmitido (visível aos clientes) e os clientes sem fio que se conectam à WLAN são atribuídos à VLAN nativa.

Etapa 1. Configure o SSID.

```
# dot11 ssid OPEN
# authentication open
# guest-mode
```

Etapa 2. Atribua o SSID ao rádio 802.11b.

```
# interface dot11radio 0
# ssid OPEN
```

SSID 802.1x - RADIUS interno

Esse SSID usa o AP como servidor RADIUS. Esteja ciente de que o AP como servidor RADIUS suporta apenas a autenticação LEAP, EAP-FAST e MAC.

Etapa 1. Ative o AP como servidor radius.

O endereço IP do NAS (Network Access Server, servidor de acesso à rede) é o BVI do AP, pois esse endereço IP é o que envia a solicitação de autenticação para si mesmo. Além disso, crie um nome de usuário e uma senha.

```
# aaa new-model
# radius-server local
# nas <a.b.c.d> key 0 <shared-key>
# user <username> password 0 <password>
```

Etapa 2. Configure o servidor RADIUS para o qual o AP envia a solicitação de autenticação, já que é um RADIUS local, o endereço IP é o atribuído à Interface Virtual de Bridge (BVI) do AP.

```
# radius server <radius-server-name>
# address ipv4 <a.b.c.d> auth-port 1812 acct-port 1813
# timeout 10
# retransmit 3
# key 0 <shared-key>
```

Etapa 3. Atribua este servidor RADIUS a um grupo radius.

```
# aaa group server radius <radius-group>
# server name <radius-server-name>
```

Etapa 4. Atribua esse grupo radius a um método de autenticação.

```
# aaa authentication login <eap-method-name> group <radius-group>
```

Etapa 5. Crie o SSID, atribua-o à VLAN 2402.

```
#  dot11 ssid internal-radius
#  vlan 2402
#  authentication open eap <eap-method-name>
#  authentication network-eap <eap-method-name>
#  authentication key-management wpa version 2
#  mbssid guest-mode
```

Etapa 6. Atribua o ssid à interface 802.11a e especifique o modo de cifra.

```
# interface dot11radio 1
# mbssid
```

```
# encryption vlan 2402 mode ciphers aes-ccm
# ssid internal-radius
```

SSID 802.1x - RADIUS externo

A configuração é quase a mesma do RADIUS interno.

Etapa 1. Configurar **um novo modelo.**

Etapa 2, em vez do endereço IP do AP, use o endereço IP RADIUS externo.

SSID - PSK

Esse SSID usa WPA2/PSK de segurança e os usuários nesse SSID estão atribuídos à VLAN 2402.

Etapa 1. Configure o SSID.

```
# conf t
# dot11 ssid PSK-ex
# authentication open
# authentication key-management wpa version 2
# wpa-psk ascii 0 <password>
# mbssid guest-mode
# vlan 2402
```

Etapa 2. Atribua o SSID à interface de rádio e configure o modo cifra.

```
# interface dot11radio 1
# encryption vlan 2402 mode ciphers aes-ccm
# ssid PSK-ex
```

SSID - Autenticação de Endereço MAC

Esse SSID autentica os clientes sem fio com base em seu endereço MAC. Ele usa o endereço MAC como nome de usuário/senha. Neste exemplo, o AP atua como RADIUS local, de modo que o AP armazene a lista de endereços MAC. A mesma configuração pode ser aplicada com o servidor RADIUS externo.

Etapa 1. Ative o AP como servidor RADIUS. O endereço IP NAS é o BVI do AP. Crie a entrada para o cliente com o endereço MAC aaaabbbcccc.

```
# aaa new-model
# radius-server local
# nas <a.b.c.d> key 0 <shared-key>
# user aaaabbbbcccc password 0 aaaabbbbcccc mac-auth-only
```

Etapa 2. Configure o servidor RADIUS para o qual o AP envia a solicitação de autenticação (é o próprio AP).

```
# radius server <radius-server-name>
# address ipv4 <a.b.c.d> auth-port 1812 acct-port 1813
# timeout 10
# retransmit 3
# key 0 <shared-key>
```

Etapa 3. Atribua este servidor RADIUS a um grupo radius.

```
# aaa group server radius <radius-group>
# server name <radius-server-name>
```

Etapa 4. Atribua esse grupo radius a um método de autenticação.

```
# aaa authentication login <mac-method> group <radius-group>
```

Etapa 5. Crie o SSID, este exemplo o atribui à VLAN 2402.

```
#  dot11 ssid mac-auth
#  vlan 2402
#  authentication open mac-address <mac-method>
#  mbssid guest-mode
```

Etapa 6. Atribua o SSID à interface 802.11a.

```
# interface dot11radio 1
# mbssid
# ssid mac-auth
```

SSID - Autenticação interna da Web

Os usuários que se conectam a esse SSID são redirecionados para um portal de autenticação da Web para inserir um nome de usuário/senha válidos. Se a autenticação for bem-sucedida, eles terão acesso à rede. Neste exemplo, os usuários são armazenados no servidor RADIUS local.

Neste exemplo, o SSID é atribuído à VLAN 2403.

Etapa 1. Ative o AP como servidor RADIUS. O endereço IP NAS é o BVI do AP.

```
# aaa new-model
# radius-server local
# nas <a.b.c.d> key 0 <shared-key>
```

Etapa 2. Configure o servidor RADIUS para o qual o AP envia a solicitação de autenticação (é o próprio AP).

```
# radius server <radius-name>
# address ipv4 <a.b.c.d> auth-port 1812 acct-port 1813
# timeout 10
# retransmit 3
# key 0 <shared-key>
```

Etapa 3. Atribua este servidor radius a um grupo radius.

```
# aaa group server radius <radius-group>
# server name <radius-name>
```

Etapa 4. Atribua esse grupo radius a um método de autenticação.

```
# aaa authentication login <web-method> group <radius-group>
```

Etapa 5. Crie as políticas de admissão.

```
# ip admission name webauth-pol proxy http
# ip admission name webauth-pol method-list authentication <web-method>
```

Etapa 6. Configure o SSID.

```
# conf t
# dot11 ssid webauth-autonomous
# authentication open
# web-auth
# vlan 2403
# mbssid guest-mode
```

Passo 7. Atribua o SSID à interface.

```
# conf t
# int dot11radio 1
# ssid webauth-autonomous
```

Etapa 8. Atribua a política à subinterface correta.

```
# conf t
# int dot11radio 1.2403
# ip admission webauth-pol
```

> **Observação**: se o SSID funcionar no nativo, a política será aplicada diretamente à interface, não à subinterface (dot11radio 0 ou dot11radio 1).

Etapa 9. Crie o nome de usuário/senha para os usuários convidados.

```
# conf t
# dot11 guest
# username <username> lifetime 35000 password <password>
```

SSID - Passagem pela Web

Quando um cliente se conecta a um SSID com a configuração do Web Pass-through, ele será redirecionado para um portal da Web para aceitar os termos e as condições do uso da rede; caso contrário, o usuário não poderá usar o serviço.

Este exemplo atribui o SSID à VLAN nativa.

Etapa 1. Crie a política de admissão.

```
# config t
# ip admission name web-passth consent
```

Etapa 2. Especifique a mensagem a ser exibida quando os clientes se conectarem a este SSID.

```
# ip admission consent-banner text %
                                    ======= WELCOME ======
                                   Message to be displayed to clients
                                                          .........
                                                          .........
                                                          .........
                                                          .........
                                                          .........
%
```

Etapa 3. Crie o SSID.

```
# dot11 ssid webpassth-autonomous
# web-auth
# authentication open
# guest-mode
```

Etapa 4. Atribuir o SSID e a política de admissão ao rádio

```
# interface dot11radio { 0 | 1 }
# ssid webpassth-autonomous
# ip admission web-passth
```

Verificar

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

show dot11 associations

Mostra o endereço MAC, o endereço IPv4 e IPv6, o nome SSID dos clientes sem fio conectados.

```
ap# show dot11 associations

802.11 Client Stations on Dot11Radio0:
```

```
SSID [webpassth-autonomous] :

MAC Address    IP address      IPV6 address                              Device        Name
Parent         State
c4b3.01d8.5c9d 172.16.0.122    ::                                        unknown       -
self           Assoc
```

Nº show dot11 associations aaaa.bbb.cccc

Mostra mais detalhes do cliente sem fio especificado no endereço mac como RSSI, SNR, taxas de dados suportadas e outros.

```
ap# show dot11 associations c4b3.01d8.5c9d

Address : c4b3.01d8.5c9d Name : NONE
IP Address : 172.16.0.122 IPv6 Address : ::
Gateway Address : 0.0.0.0
Netmask Address : 0.0.0.0 Interface : Dot11Radio 0
Bridge-group : 1
reap_flags_1 : 0x0 ip_learn_type : 0x0 transient_static_ip : 0x0
Device : unknown Software Version : NONE
CCX Version : NONE Client MFP : Off

State : Assoc Parent : self
SSID : webpassth-autonomous
VLAN : 0
Hops to Infra : 1 Association Id : 1
Clients Associated: 0 Repeaters associated: 0
Tunnel Address : 0.0.0.0
Key Mgmt type : NONE Encryption : Off
Current Rate : m15b2 Capability : WMM ShortHdr ShortSlot
Supported Rates : 1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0-2 m1-2 m2-2 m3-2 m4-
2 m5-2 m6-2 m7-2 m8-2 m9-2 m10-2 m11-2 m12-2 m13-2 m14-2 m15-2
Voice Rates : disabled Bandwidth : 20 MHz
Signal Strength : -30 dBm Connected for : 447 seconds
Signal to Noise : 56 dB Activity Timeout : 56 seconds
Power-save : On Last Activity : 4 seconds ago
Apsd DE AC(s) : NONE

Packets Input : 1035 Packets Output : 893
Bytes Input : 151853 Bytes Output : 661627
Duplicates Rcvd : 1 Data Retries : 93
Decrypt Failed : 0 RTS Retries : 0
MIC Failed : 0 MIC Missing : 0
Packets Redirected: 0 Redirect Filtered: 0
IP source guard failed : 0 PPPoE passthrough failed : 0
DAI failed : IP mismatch : 0 src MAC mismatch : 0 target MAC mismatch : 0
Existing IP failed : 0 New IP failed : 0
11w Status       : Off
```

show dot11 webauth-sessions

Mostra o endereço mac, o endereço IPv4 para autenticação da Web ou passagem da Web e o nome de usuário se o SSID estiver configurado para autenticação da Web.

```
ap# show dot11 webauth-sessions
c4b3.01d8.5c9d 172.16.0.122  connected
```

show dot11 bssid

Isso mostra os BSSIDs associados às WLANs por interface de rádio.

```
ap# show dot11 bssid

Interface      BSSID         Guest  SSID
Dot11Radio0   00c8.8b1b.49f0  Yes  webpassth-autonomous
Dot11Radio1   00c8.8b04.ffb0  Yes  PSK-ex
Dot11Radio1   00c8.8b04.ffb1  Yes  mac-auth
```

show bridge verbose

Isso mostra a relação entre subinterfaces e grupos de bridge.

```
ap# show bridge verbose

Total of 300 station blocks, 297 free
Codes: P - permanent, S - self


Flood ports (BG 1)           RX count    TX count
Dot11Radio0                         0           0
Dot11Radio1.2401                    0           7
GigabitEthernet0.2401              31         225


Flood ports (BG 242)         RX count    TX count
Dot11Radio1.2402                    0           0
GigabitEthernet0.2402               0           0


Flood ports (BG 243)         RX count    TX count
Dot11Radio1.2403                    0           0
GigabitEthernet0.2403               0           0
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

clear dot11 client aaa.bbb.ccc

Esse comando ajuda a desconectar um cliente sem fio da rede.

clear dot11 webauth webauth-user username

Este comando ajuda a excluir a sessão de autenticação da Web do usuário especificado.

Execute estes comandos debug para verificar o processo de autenticação do cliente:

```
# debug condition mac-address <H.H.H>
# debug dot11 client
# debug radius authentication
# debug dot11 mgmt ssid
# debug dot11 mgmt interface
```

PSK

```
*Apr 16 02:06:47.885: (6c94.f871.3b73): SM: ---Open Authentication 0x9630924: AuthReq (0)SM:
Init (0) --> Auth_not_Assoc (1)
*Apr 16 02:06:47.885: dot11_mgmt: [2A937303] send auth=0, status[0] to dst=6c94.f871.3b73,
src=f07f.06f4.4430, bssid=f07f.06f4.4430, seq=2, if=Dot11Radio1
*Apr 16 02:06:47.885: (6c94.f871.3b73): SM: ---Open Authentication 0x9630924: AssocReq (1)SM:
Auth_not_Assoc (1) --> DONT CHANGE STATE (255)
*Apr 16 02:06:47.889: (0000.0000.0000): dot11_mgmt: insert mac 6c94.f871.3b73 into ssid[PSK-ex]
tree

!----- Authentication frame received from the client and response

*Apr 16 02:06:47.889: (6c94.f871.3b73): SM: ---Open Authentication 0x9630924: IAPP-Resp (3)SM:
IAPP_get (5) --> DONT CHANGE STATE (255)
*Apr 16 02:06:47.889: (6c94.f871.3b73): SM: ---Open Authentication 0x9630924: Drv Add Resp
(8)SM:    Drv_Add_InProg (8) --> DONT CHANGE STATE (255)
*Apr 16 02:06:47.889: (0000.0000.0000): dot11_mgmt: [2A937B59] send assoc resp, status[0] to
dst=6c94.f871.3b73, aid[1] on Dot11Radio1

!------ Association frame received from client and response

*Apr 16 02:06:47.889: (0000.0000.0000): dot11_aaa: Starting wpav2 4-way handshake for PSK or pmk
cache supplicant 6c94.f871.3b73
*Apr 16 02:06:47.889: (0000.0000.0000): dot11_aaa: sending eapol to client on BSSID
f07f.06f4.4430
*Apr 16 02:06:47.889: (0000.0000.0000): dot11_aaa: [count = 1] Sent PTK msg 1 to client, no
timer set
*Apr 16 02:06:47.893: (0000.0000.0000): dot11_aaa: Received wpav2 ptk msg2
*Apr 16 02:06:47.901: (0000.0000.0000): dot11_aaa: sending eapol to client on BSSID
f07f.06f4.4430
*Apr 16 02:06:47.901: (0000.0000.0000): dot11_aaa: [count = 1] Sent PTK msg 3 to client, no
timer set
*Apr 16 02:06:47.901: (0000.0000.0000): dot11_aaa: Received EAPOL packet from client
*Apr 16 02:06:47.901: (0000.0000.0000): dot11_aaa: wpav2 recv PTK MSG4
*Apr 16 02:06:47.901: (0000.0000.0000): dot11_aaa: 4-way Handshake pass for client

!----- Successfull 4-way-handshake

*Apr 16 02:06:47.901: (0000.0000.0000): dot11_aaa: Sending auth response: 2 for client
*Apr 16 02:06:47.901: (6c94.f871.3b73): SM: ---Open Authentication 0x9630924: AAA Auth OK (5)SM:
AAA_Auth (6) --> Assoc (2)
*Apr 16 02:06:47.901: %DOT11-6-ASSOC: Interface Dot11Radio1, Station   6c94.f871.3b73 Associated
KEY_MGMT[WPAv2 PSK]
*Apr 16 02:06:47.901: (0000.0000.0000): dot11_aaa: client Associated

!----- Authentication completed

*Apr 16 02:06:50.981: (0000.0000.0000): dot11_mgmt: Updating the client IP (172.16.0.91) to the
controller

!-------Client's IP address updated on the AP database
```

802,1x

```
 *Apr 14 09:54:03.083: (38b1.db54.26ff): SM: ---Open Authentication 0x9630924: AuthReq (0)SM:
Init (0) --> Auth_not_Assoc (1)
*Apr 14 09:54:03.083: dot11_mgmt: [75F0D029] send auth=0, status[0] to dst=38b1.db54.26ff,
src=f07f.06f4.4430, bssid=f07f.06f4.4430, seq=2, if=Dot11Radio1
```

```
!----- Authentication frame received from the client and response


*Apr 14 09:54:03.091: (38b1.db54.26ff): SM: ---Open Authentication 0x9630924: AssocReq (1)SM:
Auth_not_Assoc (1) --> DONT CHANGE STATE (255)
*Apr 14 09:54:03.091: (0000.0000.0000): dot11_mgmt: insert mac 38b1.db54.26ff into
ssid[internal-radius] tree
*Apr 14 09:54:03.091: (0000.0000.0000): dot11_mgmt: [75F0F8AE] send assoc resp, status[0] to
dst=38b1.db54.26ff, aid[1] on Dot11Radio1

!------ Association frame received from client and response


*Apr 14 09:54:03.091: (0000.0000.0000): dot11_aaa: Received dot11_aaa_auth_request for
clientSSID: internal-radius, auth_algorithm 0, key_mgmt 1027073
*Apr 14 09:54:03.095: (0000.0000.0000): dot11_aaa: eap list name: eap-method
*Apr 14 09:54:03.095: (0000.0000.0000): dot11_aaa: Send auth request for this client to local
Authenticator
*Apr 14 09:54:03.095: (0000.0000.0000): dot11_auth: Sending EAPOL to requestor
*Apr 14 09:54:03.095: (0000.0000.0000): dot11_aaa: Received DOT11_AAA_EAP from Local
Authenticator
*Apr 14 09:54:03.095: (0000.0000.0000): dot11_aaa: sending eapol to client on BSSID
f07f.06f4.4430
*Apr 14 09:54:05.103: (0000.0000.0000): dot11_aaa: Received EAPOL packet from client

*Apr 14 09:54:05.107: RADIUS(0000003B): Send Access-Request to 172.16.0.48:1812 id 1645/12, len
194
*Apr 14 09:54:05.107: RADIUS:  User-Name           [1]   7   "user1"
.
.
.
*Apr 14 09:54:05.119: RADIUS: Received from id 1645/14 172.16.0.48:1812, Access-Accept, len 214
*Apr 14 09:54:05.119: RADIUS:  User-Name           [1]   28  "user1                       "

!------ 802.1x Authentication success

*Apr 14 09:54:05.119: (0000.0000.0000): dot11_auth: Checking for Airespace-Vlan-Name in server
attributes
*Apr 14 09:54:05.119: (0000.0000.0000): dot11_auth: Checking for VLAN ID in server attributes
*Apr 14 09:54:05.119: (0000.0000.0000): dot11_auth: Checking for Airespace-Acl-Name in server
attributes
*Apr 14 09:54:05.119: (0000.0000.0000): dot11_auth: client authenticated, node_type 64 for
application 0x1

!------ AP verifies if there is any attribute pushed by the RADIUS server


*Apr 14 09:54:05.119: (0000.0000.0000): dot11_aaa: [count = 1] Sent PTK msg 1 to client, no
timer set
*Apr 14 09:54:05.123: (0000.0000.0000): dot11_aaa: Received wpav2 ptk msg2
*Apr 14 09:54:05.131: (0000.0000.0000): dot11_aaa: [count = 1] Sent PTK msg 3 to client, no
timer set
*Apr 14 09:54:05.131: (0000.0000.0000): dot11_aaa: wpav2 recv PTK MSG4
*Apr 14 09:54:05.131: (0000.0000.0000): dot11_aaa: 4-way Handshake pass for client
*Apr 14 09:54:05.131: (38b1.db54.26ff): SM: ---Open Authentication 0x9630924: AAA Auth OK (5)SM:
AAA_Auth (6) --> Assoc (2)

!------ 4-way-handshake process completed


*Apr 14 09:54:05.131: %DOT11-6-ASSOC: Interface Dot11Radio1, Station   38b1.db54.26ff Associated
KEY_MGMT[WPAv2]
*Apr 14 09:54:05.131: (0000.0000.0000): dot11_aaa: client Associated
```

```
!----- Authentication completed



*Apr 14 09:54:05.611: (0000.0000.0000): dot11_mgmt: Updating the client IP (172.16.0.90) to the
controller

 !-------Client's IP address updated on the AP database
```

Autenticação MAC

```
 *Apr 16 03:42:14.819: (2477.033a.e00c): SM: ---Open Authentication 0x947A804: AuthReq (0)SM:
Init (0) --> Auth_not_Assoc (1)
*Apr 16 03:42:14.819: dot11_mgmt: [EE8DFCD2] send auth=0, status[0] to dst=2477.033a.e00c,
src=f07f.06f4.4430, bssid=f07f.06f4.4430, seq=2, if=Dot11Radio1

!----- Authentication frame received from the client and response


*Apr 16 03:42:14.823: (2477.033a.e00c): SM: ---Open Authentication 0x947A804: AssocReq (1)SM:
Auth_not_Assoc (1) --> DONT CHANGE STATE (255)
*Apr 16 03:42:14.823: (0000.0000.0000): dot11_mgmt: insert mac 2477.033a.e00c into ssid[mac-
auth] tree
*Apr 16 03:42:14.823: (0000.0000.0000): dot11_mgmt: [EE8E12C4] send assoc resp, status[0] to
dst=2477.033a.e00c, aid[1] on Dot11Radio1

!------ Association frame received from client and response

*Apr 16 03:42:14.823: (0000.0000.0000): dot11_aaa: Received dot11_aaa_auth_request for
clientSSID: mac-auth, auth_algorithm 0, key_mgmt 0
*Apr 16 03:42:14.823: (0000.0000.0000): dot11_aaa: Start local Authenticator request
*Apr 16 03:42:14.823: (0000.0000.0000): dot11_auth: Start auth method MAC

*Apr 16 03:42:14.827: RADIUS(00000050): Send Access-Request to 172.16.0.48:1812 id 1645/81, len
169
*Apr 16 03:42:14.827: RADIUS:  User-Name           [1]   14  "2477033ae00c"
*Apr 16 03:42:14.827: RADIUS:  Calling-Station-Id  [31]  16  "2477.033a.e00c"

*Apr 16 03:42:14.827: RADIUS: Received from id 1645/81 172.16.0.48:1812, Access-Accept, len 116
*Apr 16 03:42:14.827: RADIUS:  User-Name           [1]   28  "2477033ae00c

!------ MAC Authentication success


*Apr 16 03:42:14.827: (0000.0000.0000): dot11_auth: Checking for SSID in server attributes
*Apr 16 03:42:14.827: (0000.0000.0000): dot11_auth: Checking for Airespace-Vlan-Name in server
attributes
*Apr 16 03:42:14.827: (0000.0000.0000): dot11_auth: Checking for VLAN ID in server attributes
*Apr 16 03:42:14.827: (0000.0000.0000): dot11_auth: Checking for Airespace-Acl-Name in server
attributes

!------ AP verifies if there is any attribute pushed by the RADIUS server


*Apr 16 03:42:14.827: (0000.0000.0000): dot11_auth: client authenticated, node_type 64 for
application 0x1
*Apr 16 03:42:14.827: (0000.0000.0000): dot11_aaa: Received DOT11_AAA_SUCCESS from Local
Authenticator
*Apr 16 03:42:14.827: (2477.033a.e00c): SM: ---Open Authentication 0x947A804: AAA Auth OK (5)SM:
AAA_Auth (6) --> Assoc (2)
*Apr 16 03:42:14.827: %DOT11-6-ASSOC: Interface Dot11Radio1, Station   2477.033a.e00c Associated
KEY_MGMT[NONE]
```

!----- Authentication completed

*Apr 16 03:42:16.895: (0000.0000.0000): dot11_mgmt: Updating the client IP (172.16.0.92) to the controller

!-------Client's IP address updated on the AP database