Configuración SSID y de los VLA N en los Puntos de acceso autónomos

Contenido

Introducción

Este documento explica cómo configurar un (APS) autónomo de los Puntos de acceso para:

- VLA N (redes de área local virtuales)
- Autenticación abierta
- 802.1x con el Remote Authentication Dial-In User Service (RADIUS) interno
- 802.1x con el externo RADIUS
- PSK (clave previamente compartida)
- Autenticación de la dirección MAC
- Autenticación Web (radio interno)
- Paso de la red

Prerrequisitos

Cisco le recomienda tiene un conocimiento básico de estos temas:

- 802.1x
- PSK

- RADIUS
- Autenticación Web

Componentes Utilizados

Versión 15.3(3)JBB AP 3700

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

> Consejo: Estos ejemplos también se aplican al AP en el modo autónomo dentro de ASA 5506, la diferencia son ése en vez de configuración el puerto del switch en donde el AP está conectado, la configuración se aplican al carruaje 1/9 ASA.

Configurar

> Nota: Los SSID (identificadores del conjunto de servicio) que pertenece al mismo VLA N no se pueden aplicar a una radio al mismo tiempo. Los ejemplos de configuración de los SSID con el mismo VLA N no fueron habilitados al mismo tiempo en el mismo AP.

Switch y AP - Configuración de VLAN

Configure los VLA N requeridos en el AP y conmutelos. Éstos son los VLA N usados en este ejemplo:

- VLA N 2401 (natural)
- VLA N 2402
- VLA N 2403

Configuración de los VLA N AP

Configuración de las interfaces 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
```

Configuración de radio del 802.11a de la interfaz

```
# 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
```

> Nota: Note que la radio del 802.11b (interfaz dot11radio 0) no está configurada, pues utiliza el VLAN nativo del AP

Conmute la configuración de VLAN

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

Configuración de la interfaz donde el 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
```

Autenticación abierta SSID - El VLAN nativo AP

Este SSID no tiene Seguridad, se transmite (visible a los clientes) y asignan los clientes de red inalámbrica que se une a la red inalámbrica (WLAN) al VLAN nativo.

Paso 1. Configure el SSID.

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

Paso 2. Asigne el SSID a la radio del 802.11b.

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

802.1x SSID - RADIUS interno

Este SSID utiliza el AP como servidor de RADIUS sí mismo. Sea consciente que AP como los soportes del servidor de RADIUS solamente SALTAN, EAP-FAST y autenticación de MAC

Paso 1. Permiso AP como servidor de RADIUS.

El IP Address de Server(NAS) del acceso a la red es el BVI AP, pues esta dirección IP es la que envía el pedido de autenticación a sí mismo. También, cree un nombre de usuario y contraseña.

```
# aaa new-model
```

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

Paso 2. Configure al servidor de RADIUS a quien el AP envía el pedido de autenticación, como es RADIUS local, la dirección IP es el que está asignado al BVI 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>
```

Paso 3. Asigne a este servidor de RADIUS a un grupo del radio.

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

Paso 4. Asigne este grupo del radio a un método de autentificación.

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

Paso 5. Cree el SSID, asígnelo al VLA N 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
```

Paso 6. Asigne el ssid al 802.11a de la interfaz y especifique el modo de la cifra.

```
# interface dot11radio 1
# mbssid
# encryption vlan 2402 mode ciphers aes-ccm
# ssid internal-radius
```

802.1x SSID - Externo RADIUS

La configuración casi es lo mismo que el radio interno. De la configuración **aaa del** paso 1 solamente **de modelo nuevo.**

En el paso 2, en vez del IP address AP, utilice la dirección IP del externo RADIUS.

SSID - PSK

Este SSID utiliza la Seguridad WPA2/PSK y a los usuarios en este ssid se asigna al VLA N 2402.

Paso 1. Configure el 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
```

Paso 2. Asigne el SSID a la interfaz radio y configure el modo de la cifra.

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

SSID - Autenticación de la dirección MAC

Este SSID autentica a los clientes de red inalámbrica basados en su dirección MAC. Utiliza la dirección MAC como el nombre de usuario/contraseña. En este ejemplo el AP actúa como RADIUS local, así que el AP salva la lista de la dirección MAC. La misma configuración se puede aplicar con el servidor RADIUS externo.

Paso 1. Permiso AP como servidor de RADIUS. El IP address NAS es el BVI AP. Cree la entrada para el cliente con el aaaabbbbcccc de la dirección MAC.

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

Paso 2. Configure al servidor de RADIUS a quien el AP envía el pedido de autenticación (es el AP sí mismo).

```
# 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>
```

Paso 3. Asigne a este servidor de RADIUS a un grupo del radio.

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

Paso 4. Asigne este grupo del radio a un método de autentificación.

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

Paso 5. Cree el SSID, este ejemplo lo asigna al VLA N 2402.

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

Paso 6. Asigne el ssid al 802.11a de la interfaz.

```
# interface dot11radio 1
```

```
# mbssid
# ssid mac-auth
```

SSID - Autenticación del Web interna

Reorientan a los usuarios que conecta con este SSID a un portal de la autenticación Web para ingresar un nombre de usuario válido/una contraseña, si la autenticación es acertada, ellos tienen acceso a la red. En este ejemplo, salvan a los usuarios en el servidor de RADIUS local.

En este ejemplo, el SSID se asigna al VLA N 2403

Paso 1. Permiso AP como servidor de RADIUS. El IP address NAS es el BVI AP.

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

Paso 2. Configure al servidor de RADIUS a quien el AP envía el pedido de autenticación (es el AP sí mismo).

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

Paso 3. Asigne a este servidor de RADIUS a un grupo del radio.

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

Paso 4. Asigne este grupo del radio a un método de autentificación.

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

Paso 5. Cree las directivas de admisión.

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

Paso 6. Configure el SSID.

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

Paso 7. Asigne el SSID a la interfaz.

```
# conf t
# int dot11radio 1
```

```
# ssid webauth-autonomous
```

Paso 8. Asigne la directiva a la sub-interfaz correcta.

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

> Nota: Si el ssid trabaja en el nativo, después la directiva se aplica directamente a la interfaz, no a la sub-interfaz (dot11radio 0 o dot11radio 1)

Paso 9. Cree el nombre de usuario/la contraseña para los Usuarios invitados.

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

SSID - Paso de la red

Cuando un cliente conecta con un SSID con la configuración del paso de la red, será reorientada a un portal web para validar los términos y las condiciones del USO de la red, si no, el usuario no podrán utilizar el servicio.

Este ejemplo asigna el SSID al VLAN nativo.

Paso 1. Cree la directiva de admisión.

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

Paso 2. Especifique el mensaje que se visualizará cuando los clientes conectan con este SSID.

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

Paso 3. Cree el SSID.

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

Paso 4. Asigne el SSID y la directiva de admisión a la radio

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

Verificación

asociaciones del dot11 de la demostración

Muestra el MAC address, el direccionamiento del IPv4 y del IPv6, el nombre SSID de los clientes de red inalámbrica 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
```

asociaciones aaaa.bbbb.cccc del dot11 de la demostración

Muestra a más detalles del cliente de red inalámbrica especificados en el MAC address como el RSSI, SNR, las velocidades de datos soportó y otras.

```
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
```

webauth-sesiones del dot11 de la demostración

Muestra el MAC address, el direccionamiento del IPv4 para el paso de la autenticación Web o de la red y el nombre de usuario si el SSID se configura para la autenticación Web.

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

bssid del dot11 de la demostración

Muestra el BSSIDs asociado a los WLAN por la interfaz radio

```
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
```

Bridge de la demostración prolijo

Muestra la relación entre los subinterfaces y los 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
```

Troubleshooting

cliente claro aaa.bbbb.cccc del dot11

Desconecte a un cliente de red inalámbrica de la red

nombre de usuario claro del webauth-usuario del webauth del dot11

Borre la sesión de la autenticación Web del usuario específicado

Funcione con estos comandos debug para verificar el proceso de autenticación del 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
```

Autenticación de 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
```