Configurazione di SSID e VLAN su access point autonomi

Sommario

Introduzione

In questo documento viene spiegato come configurare gli access point (AP) autonomi per:

- VLAN (Virtual Local Area Network)
- Autenticazione aperta
- 802.1x con servizio utente RADIUS (Remote Authentication Dial-In) interno
- 802.1x con RADIUS esterno
- Chiave già condivisa (PSK)
- Autenticazione indirizzo MAC
- Autenticazione Web (raggio interno)
- Pass-through Web

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- 802.1x
- PSK
- RAGGIO
- Autenticazione Web

Componenti usati

Il riferimento delle informazioni contenute in questo documento è AP 3700 versione 15.3(3)JBB.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Suggerimento**: questi esempi si applicano anche all'access point in modalità autonoma all'interno di ASA 5506; la differenza è che invece di configurare la porta dello switch a cui è connesso l'access point, la configurazione viene applicata all'access point ASA Gig 1/9.

Configurazione

> **Nota**: gli SSID (Service Set Identifier) che appartengono alla stessa VLAN non possono essere applicati a una radio contemporaneamente. Gli esempi di configurazione degli SSID con la stessa VLAN non sono stati abilitati contemporaneamente sullo stesso access point.

Configurazione dello switch VLAN e del punto di accesso

Configurare le VLAN richieste sull'access point e sullo switch. Di seguito vengono riportate le VLAN usate nell'esempio:

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

Configurazione di AP e VLAN

Configurazione interfaccia 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
```

Configura interfaccia Radio 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
```

> **Nota**: la radio 802.11b (interfaccia dot11radio 0) non è configurata, in quanto usa la VLAN nativa dell'access point.

Configurazione della VLAN dello switch

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

Configurare l'interfaccia a cui è connesso l'access point:

```
# 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
```

Autenticazione aperta SSID - VLAN nativa del punto di accesso

Questo SSID non è protetto, viene trasmesso (visibile ai client) e i client wireless che si uniscono alla WLAN vengono assegnati alla VLAN nativa.

Passaggio 1. Configurare il SSID.

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

Passaggio 2. Assegnare l'SSID alla radio 802.11b.

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

SSID 802.1x - RAGGIO interno

Questo SSID utilizza il punto di accesso come server RADIUS. Tenere presente che AP come server RADIUS supporta solo l'autenticazione LEAP, EAP-FAST e MAC.

Passaggio 1. Abilitare il punto di accesso come server radius.

L'indirizzo IP del server di accesso alla rete (NAS) è la BVI dell'access point, in quanto è l'indirizzo IP che invia la richiesta di autenticazione a se stesso. Inoltre, creare un nome utente e una password.

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

Passaggio 2. Configurare il server RADIUS a cui l'access point invia la richiesta di autenticazione, poiché si tratta di un server RADIUS locale, l'indirizzo IP è quello assegnato all'interfaccia virtuale bridge (BVI) dell'access point.

```
# 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>
```

Passaggio 3. Assegnare il server RADIUS a un gruppo RADIUS.

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

Passaggio 4. Assegnare questo gruppo radius a un metodo di autenticazione.

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

Passaggio 5. Creare l'SSID e assegnarlo alla 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
```

Passaggio 6. Assegnare il SSID all'interfaccia 802.11a e specificare la modalità di cifratura.

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

SSID 802.1x - RAGGIO esterno

La configurazione è quasi identica a quella del RADIUS interno.

Passaggio 1. Configurare **aa new-model.**

2. Anziché l'indirizzo IP dell'access point, usare l'indirizzo IP RADIUS esterno.

SSID - PSK

Questo SSID utilizza la sicurezza WPA2/PSK e gli utenti su questo SSID vengono assegnati alla VLAN 2402.

Passaggio 1. Configurare il 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
```

Passaggio 2. Assegnare il SSID all'interfaccia radio e configurare la modalità di cifratura.

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

SSID - Autenticazione indirizzo MAC

Questo SSID autentica i client wireless in base all'indirizzo MAC. Utilizza l'indirizzo MAC come nome utente/password. In questo esempio l'access point agisce come server RADIUS locale, quindi memorizza l'elenco indirizzi MAC. La stessa configurazione può essere applicata al server RADIUS esterno.

Passaggio 1. Abilitare il punto di accesso come server RADIUS. L'indirizzo IP del NAS è la BVI dell'access point. Creare la voce per il client con indirizzo MAC aaabbcccc.

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

Passaggio 2. Configurare il server RADIUS a cui l'access point invia la richiesta di autenticazione (è l'access point stesso).

```
# 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>
```

Passaggio 3. Assegnare il server RADIUS a un gruppo RADIUS.

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

Passaggio 4. Assegnare questo gruppo radius a un metodo di autenticazione.

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

Passaggio 5. Creare l'SSID. In questo esempio viene assegnato alla VLAN 2402.

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

Passaggio 6. Assegnare l'SSID all'interfaccia 802.11a.

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

SSID - Autenticazione Web interna

Gli utenti che si connettono a questo SSID vengono reindirizzati a un portale di autenticazione Web per immettere un nome utente/password valido. Se l'autenticazione ha esito positivo, hanno accesso alla rete. In questo esempio gli utenti vengono archiviati nel server RADIUS locale.

nell'esempio, l'SSID è assegnato alla VLAN 2403.

Passaggio 1. Abilitare il punto di accesso come server RADIUS. L'indirizzo IP del NAS è la BVI dell'access point.

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

Passaggio 2. Configurare il server RADIUS a cui l'access point invia la richiesta di autenticazione (è l'access point stesso).

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

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

Passaggio 3. Assegnare il server radius a un gruppo radius.

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

Passaggio 4. Assegnare questo gruppo radius a un metodo di autenticazione.

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

Passaggio 5. Creare le regole di ammissione.

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

Passaggio 6. Configurare il SSID.

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

Passaggio 7. Assegnare l'SSID all'interfaccia.

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

Passaggio 8. Assegnare il criterio all'interfaccia secondaria destra.

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

> Nota: se l'SSID funziona sull'interfaccia nativa, il criterio viene applicato direttamente all'interfaccia e non alla sottointerfaccia (dot11radio 0 o dot11radio 1).

Passaggio 9. Creare il nome utente/password per gli utenti guest.

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

SSID - Pass-through Web

Quando un client si connette a un SSID con configurazione Web Pass-through, verrà reindirizzato a un portale Web per accettare i termini e le condizioni dell'utilizzo della rete. In caso contrario, l'utente non sarà in grado di utilizzare il servizio.

In questo esempio l'SSID viene assegnato alla VLAN nativa.

Passaggio 1. Creare il criterio di ammissione.

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

Passaggio 2. Specificare il messaggio da visualizzare quando i client si connettono a questo SSID.

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

Passaggio 3. Creare il SSID.

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

Passaggio 4. Assegnare l'SSID e i criteri di ammissione alla radio

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

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

show dot11 associazioni

Mostra l'indirizzo MAC, l'indirizzo IPv4 e IPv6, il nome SSID dei client wireless connessi.

```
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
```

N. show dot11 associazioni aaaa.bbbb.ccc

Vengono mostrati ulteriori dettagli sul client wireless specificato nell'indirizzo MAC come RSSI, SNR, velocità dati supportate e altri.

```
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 sessioni webauth

Qui vengono mostrati l'indirizzo MAC, l'indirizzo IPv4 per l'autenticazione Web o l'accesso Web e il nome utente se il SSID è configurato per l'autenticazione Web.

```
ap# show dot11 webauth-sessions
```

```
c4b3.01d8.5c9d 172.16.0.122  connected
```

show dot11 bssid

In questo modo vengono mostrati i BSSID associati alle WLAN per interfaccia 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
```

visualizzazione dettagliata del bridge

Questo comando mostra la relazione tra sottointerfacce e gruppi di 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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

clear dot11 client aaa.bbbb.ccc

Questo comando consente di disconnettere un client wireless dalla rete.

clear dot11 webauth nome utente-webauth

Questo comando consente di eliminare la sessione di autenticazione Web dell'utente specificato.

Eseguire questi comandi di debug per verificare il processo di autenticazione del client:

```
# 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
```

Autenticazione 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
```