SSID's en VLAN's configureren op autonome AP's

Inhoud

Inleiding

Dit document legt uit hoe u autonome access points (AP's) kunt configureren voor:

- Virtual Local Area Networks (VLAN's)
- Open authenticatie
- 802.1x met interne externe verificatie-inbelservice (RADIUS)
- 802.1x met externe RADIUS
- Vooraf gedeelde sleutel (PSK)
- MAC-adresverificatie
- Webverificatie (interne straal)
- Web Pass-Through

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis van deze onderwerpen te hebben:

- 802,1x
- PSK
- RADIUS
- Web verificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op AP 3700, versie 15.3(3)JBB.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

> **Tip**: Deze voorbeelden zijn ook van toepassing op AP in autonome modus binnen ASA 5506. Het verschil is dat in plaats van de switchpoort te configureren waar de AP is aangesloten, de configuratie wordt toegepast op Gig 1/9 van de ASA.

Configureren

> **Opmerking**: De Service Set Identifier(s) die tot hetzelfde VLAN behoren, kan niet tegelijkertijd op een radio worden toegepast. De configuratievoorbeelden van SSID's met hetzelfde VLAN zijn niet tegelijkertijd op dezelfde AP ingeschakeld.

VLAN-switch en -AP configureren

Configureer de gewenste VLAN's op zowel de AP als de schakelaar. Dit zijn de VLAN's die in dit voorbeeld worden gebruikt:

- VLAN 2401 (standaard)
- VLAN 2402
- VLAN 2403

APs en VLAN's configureren

Interface Gigabit Ethernet configureren

```
# 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
```

Interface-radio 802.11a configureren

```
# 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
```

> **Opmerking**: 802.11b-radio (interface dot11radio 0) is niet geconfigureerd, omdat het het native VLAN van het AP gebruikt.

Switch VLAN configureren

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

Configuratie van de interface waar AP wordt aangesloten:

```
# 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
```

SSID Open Verificatie - Native VLAN van AP

Deze SSID heeft geen beveiliging, wordt het uitgezonden (zichtbaar voor klanten) en de draadloze klanten die zich bij WLAN voegen worden toegewezen aan het inheemse VLAN.

Stap 1. Configureer de SSID's.

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

Stap 2. Pas de SSID aan de 802.11b-radio.

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

SSID 802.1x - interne RADIUS

Deze SSID gebruikt AP als RADIUS-server. Let erop dat AP als RADIUS-server alleen LEAP, EAP-FAST en MAC-verificatie ondersteunt.

Stap 1. Schakel AP als Straalserver in.

Het IP-adres van Network Access Server (NAS) is de BVI van AP, omdat dit IP-adres het adres is dat de verificatieaanvraag naar zichzelf stuurt. Maak ook een gebruikersnaam en wachtwoord.

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

Stap 2. Het configureren van de RADIUS-server waarop AP de authenticatieaanvraag stuurt, omdat dit een lokale RADIUS is, is het IP-adres het adres dat is toegewezen aan AP's Bridge Virtual Interface (BVI).

```
# 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>
```

Stap 3. Pas deze RADIUS-server aan een straal-groep toe.

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

Stap 4. Pas deze Straalgroep aan een authenticatiemethode toe.

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

Stap 5. Maak de SSID's (SSID) en verdeel deze aan 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
```

Stap 6. Pas de hulp aan de interface 802.11a toe en specificeer de algoritme modus.

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

SSID 802.1x - externe RADIUS

De configuratie is vrijwel dezelfde als interne RADIUS.

Stap 1. **Configuratie van een nieuw model.**

Stap 2 Gebruik in plaats van het IP-adres van het AP het externe RADIUS IP-adres.

SSID - PSK

Deze SSID gebruikt veiligheid WAP2/PSK en de gebruikers op deze SSID worden toegewezen aan VLAN 2402.

Stap 1. Configureer de SSID's.

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

Stap 2. Pas de SSID aan de radio-interface en stel de algoritme in.

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

SSID - MAC-adresverificatie

Deze SSID bevestig de draadloze cliënten op basis van hun MAC-adres. Het gebruikt het MAC-adres als gebruikersnaam/wachtwoord. In dit voorbeeld werkt AP als lokale RADIUS, zodat AP de MAC adreslijst opslaat. Dezelfde configuratie kan worden toegepast met een externe RADIUS-server.

Stap 1. Schakel AP als RADIUS-server in. Het NAS IP-adres is de BVI van het AP. Maak de ingang voor de client met MAC-adresbalk.

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

Stap 2. Configureer de RADIUS-server waarop de AP de verificatieaanvraag stuurt (dit is de AP zelf).

```
# 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>
```

Stap 3. Pas deze RADIUS-server aan een straal-groep toe.

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

Stap 4. Pas deze Straalgroep aan een authenticatiemethode toe.

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

Stap 5. Maak de SSID, dit voorbeeld wijst het aan VLAN 2402 toe.

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

Stap 6. Pas de SSID aan de interface 802.11a.

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

SSID - interne webverificatie

Gebruikers die verbinding maken met deze SSID worden naar een webauthenticatieportal omgeleid om een geldige gebruikersnaam/wachtwoord in te voeren, als verificatie succesvol is, hebben zij toegang tot het netwerk. In dit voorbeeld worden de gebruikers opgeslagen op de lokale RADIUS-server.

In dit voorbeeld, wordt SSID toegewezen aan VLAN 2403.

Stap 1. Schakel AP als RADIUS-server in. Het NAS IP-adres is de BVI van het AP.

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

Stap 2. Configureer de RADIUS-server waarop de AP de verificatieaanvraag stuurt (dit is de AP zelf).

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

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

Stap 3. Pas deze Straalserver aan een Straalgroep toe.

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

Stap 4. Pas deze Straalgroep aan een authenticatiemethode toe.

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

Stap 5. Maak het toelatingsbeleid.

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

Stap 6. Configureer de SSID's.

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

Stap 7. Pas de SSID aan de interface toe.

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

Stap 8. Wijs het beleid aan de juiste subinterface toe.

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

> **Opmerking**: Als de SSID op de projector werkt, wordt het beleid direct op de interface toegepast, niet op de subinterface (dot11radio 0 of dot11radio 1).

Stap 9. Maak de gebruikersnaam/het wachtwoord voor de gastgebruikers.

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

SSID's (Web Pass Through)

Wanneer een client verbinding maakt met een SSID met een Web Pass-Through-configuratie, wordt deze opnieuw naar een webportal gericht om de bepalingen en voorwaarden van het netwerkgebruik te accepteren, indien niet, kan de gebruiker de service niet gebruiken.

Dit voorbeeld wijst SSID aan het inheemse VLAN toe.

Stap 1. Maak het toelatingsbeleid.

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

Stap 2. Specificeer het bericht dat moet worden weergegeven wanneer klanten verbinding maken met deze SSID.

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

Stap 3. Maak de SSID.

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

Stap 4: Toewijzing van de SSID en het toegangsbeleid aan de radio

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

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

show dot11 associaties

Dit toont het hoofdadres, IPv4 en IPv6 adres, de naam van SSID van de draadloze verbonden

cliënten.

```
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
```

 # show dot11 associaties aa.bbbb.ccc

Dit toont meer details van de draadloze client die in het hoofdadres is gespecificeerd als RSSI, SNR, ondersteunde gegevenssnelheden en andere.

```
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-sessies

Dit toont het hoofdadres, het IPv4 adres voor web authenticatie of web pass-through en de gebruikersnaam als SSID voor web authenticatie is ingesteld.

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

#show dot11

Dit toont de BSSID's die aan de WLAN's zijn gekoppeld per radio-interface.

```
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
```

#-toonbridge breedband

Dit toont het verband tussen subinterfaces en bruggroepen.

```
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
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Clear dot11 client aa.bb.cc

Deze opdracht helpt een draadloze client uit het netwerk te koppelen.

duidelijke dot11 webauth-gebruiker

Deze opdracht helpt de webauthenticatiesessie van de gespecificeerde gebruiker te verwijderen.

Start deze debug-opdrachten om het verificatieproces van de client te controleren:

```
# 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
```

MAC-verificatie

```
 *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
```