자동 AP에서 SSID 및 VLAN 구성

목차

소개

이 문서에서는 다음에 대한 자동 액세스 포인트(AP)를 구성하는 방법에 대해 설명합니다.

- VLAN(Virtual Local Area Network)
- 개방형 인증
- 802.1x - 내부 원격 인증 전화 접속 사용자 서비스(RADIUS) 포함
- 802.1x(외부 RADIUS 포함)
- 사전 공유 키(PSK)
- MAC 주소 인증
- 웹 인증(내부 radius)
- 웹 통과

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- 802.1x
- PSK
- RADIUS
- 웹 인증

사용되는 구성 요소

이 문서의 정보는 AP 3700 버전 15.3(3)JBB를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

> **팁**: 이러한 예는 ASA 5506 내부의 자동 모드의 AP에도 적용되며, 차이점은 AP가 연결된 스위치 포트를 구성하는 대신 ASA의 Gig 1/9에 컨피그레이션이 적용된다는 것입니다.

구성

> **참고**: 동일한 VLAN에 속하는 SSID(서비스 집합 식별자)는 무선에 동시에 적용할 수 없습니다. 동일한 VLAN을 가진 SSID의 구성 예제는 동일한 AP에서 동시에 활성화되지 않았습니다.

VLAN 스위치 및 AP 구성

AP와 스위치 모두에서 필요한 VLAN을 구성합니다.다음은 이 예에서 사용되는 VLAN입니다.

- VLAN 2401(기본)
- VLAN 2402
- VLAN 2403

AP 및 VLAN 구성

인터페이스 기가비트 이더넷 구성

```
# 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 구성

```
# 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
```

참고: 802.11b 라디오(인터페이스 dot11radio 0)는 AP의 네이티브 VLAN을 사용하므로 구성되지 않습니다.

스위치 VLAN 구성

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

AP가 연결된 인터페이스를 구성합니다.

```
# 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 개방형 인증 - AP의 기본 VLAN

이 SSID에는 보안이 없으며, 브로드캐스트되고(클라이언트에 표시) WLAN에 연결하는 무선 클라이언트가 기본 VLAN에 할당됩니다.

1단계. SSID를 구성합니다.

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

2단계. 802.11b 무선에 SSID를 할당합니다.

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

SSID 802.1x - 내부 RADIUS

이 SSID는 AP를 RADIUS 서버로 사용합니다.RADIUS 서버로 AP는 LEAP, EAP-FAST 및 MAC 인증만 지원합니다.

1단계. AP를 RADIUS 서버로 활성화합니다.

NAS(Network Access Server) IP 주소는 AP의 BVI이며, 이 IP 주소는 인증 요청을 자신에게 보내는 주소입니다.또한 사용자 이름과 비밀번호를 생성합니다.

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

2단계. AP가 인증 요청을 보내는 RADIUS 서버를 구성합니다. 로컬 RADIUS인 경우 IP 주소는 AP의 BVI(Bridge Virtual Interface)에 할당된 것입니다.

```
# 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>
```

3단계. 이 RADIUS 서버를 RADIUS 그룹에 할당합니다.

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

4단계. 이 radius 그룹을 인증 방법에 할당합니다.

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

5단계. SSID를 생성하고 VLAN 2402에 할당합니다.

```
#  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
```

6단계. 인터페이스 802.11a에 ssid를 할당하고 암호화 모드를 지정합니다.

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

SSID 802.1x - 외부 RADIUS

컨피그레이션은 내부 RADIUS와 거의 동일합니다.

1단계. aaa **new-model을 구성합니다.**

2단계, AP의 IP 주소 대신 외부 RADIUS IP 주소를 사용합니다.

SSID - PSK

이 SSID는 보안 WPA2/PSK를 사용하며 이 SSID의 사용자는 VLAN 2402에 할당됩니다.

1단계. SSID를 구성합니다.

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

2단계. 무선 인터페이스에 SSID를 할당하고 암호화 모드를 구성합니다.

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

SSID - MAC 주소 인증

이 SSID는 MAC 주소를 기반으로 무선 클라이언트를 인증합니다.MAC 주소를 사용자 이름/비밀번호로 사용합니다.이 예에서 AP는 로컬 RADIUS로 작동하므로 AP는 MAC 주소 목록을 저장합니다.외부 RADIUS 서버에 동일한 컨피그레이션을 적용할 수 있습니다.

1단계. AP를 RADIUS 서버로 활성화합니다.NAS IP 주소는 AP의 BVI입니다.MAC 주소 aaabbcccc를 사용하여 클라이언트에 대한 항목을 만듭니다.

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

2단계. AP가 인증 요청을 보내는 RADIUS 서버를 구성합니다(AP 자체임).

```
# 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>
```

3단계. 이 RADIUS 서버를 RADIUS 그룹에 할당합니다.

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

4단계. 이 radius 그룹을 인증 방법에 할당합니다.

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

5단계. SSID를 생성합니다. 이 예에서는 VLAN 2402에 할당합니다.

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

6단계. 인터페이스 802.11a에 SSID를 할당합니다.

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

SSID - 내부 웹 인증

이 SSID에 연결하는 사용자는 유효한 사용자 이름/비밀번호를 입력하기 위해 웹 인증 포털로 리디렉션됩니다. 인증에 성공하면 네트워크에 액세스할 수 있습니다.이 예에서는 사용자가 로컬 RADIUS 서버에 저장됩니다.

이 예에서는 SSID가 VLAN 2403에 할당됩니다.

1단계. AP를 RADIUS 서버로 활성화합니다.NAS IP 주소는 AP의 BVI입니다.

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

2단계. AP가 인증 요청을 보내는 RADIUS 서버를 구성합니다(AP 자체임).

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

3단계. 이 radius 서버를 radius 그룹에 할당합니다.

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

4단계. 이 radius 그룹을 인증 방법에 할당합니다.

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

5단계. 가입 정책을 생성합니다.

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

6단계. SSID를 구성합니다.

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

7단계. 인터페이스에 SSID를 할당합니다.

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

8단계. 오른쪽 하위 인터페이스에 정책을 할당합니다.

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

> **참고**: SSID가 기본에서 작동하면 하위 인터페이스(dot11radio 0 또는 dot11radio 1)가 아니라 인터페이스에 정책이 직접 적용됩니다.

9단계. 게스트 사용자의 사용자 이름/비밀번호를 생성합니다.

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

SSID - 웹 통과

클라이언트가 Web Pass-through 컨피그레이션을 사용하여 SSID에 연결되면 네트워크 사용 약관에 동의하기 위해 웹 포털로 리디렉션됩니다. 그렇지 않으면 사용자가 서비스를 사용할 수 없습니다.

이 예에서는 네이티브 VLAN에 SSID를 할당합니다.

1단계. 수락 정책을 생성합니다.

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

2단계. 클라이언트가 이 SSID에 연결할 때 표시할 메시지를 지정합니다.

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

3단계. SSID를 생성합니다.

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

4단계. SSID 및 수락 정책을 무선에 할당합니다.

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

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

 # show dot11 연결

연결된 무선 클라이언트의 MAC 주소, IPv4 및 IPv6 주소, SSID의 이름을 표시합니다.

```
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 연결 aaaa.bbbb.cccc

MAC 주소에 RSSI, SNR, 지원되는 데이터 전송률 등으로 지정된 무선 클라이언트에 대한 자세한

정보가 표시됩니다.

```
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

웹 인증을 위해 SSID가 구성된 경우 MAC 주소, 웹 인증 또는 웹 패스스루를 위한 IPv4 주소 및 사용자 이름을 표시합니다.

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

show dot11 bssid

라디오 인터페이스당 WLAN에 연결된 BSSID를 표시합니다.

```
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

하위 인터페이스와 브리지 그룹 간의 관계를 보여 줍니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

clear dot11 client aaa.bbbb.cccc

이 명령은 네트워크에서 무선 클라이언트의 연결을 끊는 데 도움이 됩니다.

clear dot11webauth webauth-user 사용자 이름

이 명령은 지정된 사용자의 웹 인증 세션을 삭제하는 데 도움이 됩니다.

다음 debug 명령을 실행하여 클라이언트의 인증 프로세스를 확인합니다.

```
# 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 인증

```
 *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
```