在自發 AP 上設定 SSID 和 VLAN

目錄

簡介

本文件說明如何設定自發存取點 (AP)：

- 虛擬區域網路(VLAN)
- 開放式身份驗證
- 具有內部遠端驗證撥入使用者服務(RADIUS)的802.1x
- 含外部RADIUS的802.1x
- 預先共用金鑰(PSK)
- MAC地址身份驗證
- Web驗證（內部radius）
- Web傳輸

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 802.1x
- PSK
- RADIUS
- Web驗證

採用元件

本檔案中的資訊是根據AP 3700版本15.3(3)JBB。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

> **提示**：這些示例同樣適用於ASA 5506內處於自主模式的AP，不同之處在於，配置應用於ASA的Gig 1/9，而不是配置AP所連線的交換機埠。

設定

> **註**:屬於同一VLAN的服務集識別符號(SSID)不能同時應用於無線電。具有相同VLAN的SSID的配置示例未在同一台AP上同時啟用。

配置VLAN交換機和AP

在AP和交換機上配置所需的VLAN。以下是此範例中使用的VLAN:

- VLAN 2401（本徵）
- VLAN 2402
- VLAN 2403

配置AP和VLAN

配置介面Gigabit乙太網

```
# 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
```

配置介面無線電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
```

註:802.11b radio(interface dot11radio 0)未配置，因為它使用AP的本徵VLAN。

配置交換機VLAN

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

配置AP連線的介面：

```
# 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開放式身份驗證 — AP的本徵VLAN

此SSID沒有安全性，它被廣播（對客戶端可見），並且加入WLAN的無線客戶端被分配給本徵VLAN。

步驟1.配置SSID。

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

步驟2.將SSID分配給802.11b無線電。

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

SSID 802.1x — 內部RADIUS

此SSID使用AP作為RADIUS伺服器。請注意，作為RADIUS伺服器的AP僅支援LEAP、EAP-FAST和MAC身份驗證。

步驟1.啟用AP作為RADIUS伺服器。

網路訪問伺服器(NAS)的IP地址是AP的BVI，因為此IP地址是將身份驗證請求傳送到自身的地址。另外，建立使用者名稱和密碼。

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

步驟2.配置AP向其傳送身份驗證請求的RADIUS伺服器，因為它是本地RADIUS，所以IP地址是分配給AP的網橋虛擬介面(BVI)的地址。

```
# 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>
```

步驟3.將此RADIUS伺服器分配給RADIUS組。

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

步驟4.將此radius組分配給身份驗證方法。

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

步驟5.建立SSID，將其分配給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
```

步驟6.將ssid分配給介面802.11a並指定密碼模式。

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

SSID 802.1x — 外部RADIUS

組態幾乎與內部RADIUS相同。

步驟1. 設定aaa new-model。

步驟2，使用外部RADIUS IP地址代替AP的IP地址。

SSID - PSK

此SSID使用安全WPA2/PSK，並將此SSID上的使用者分配到VLAN 2402。

步驟1.配置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
```

步驟2.將SSID分配給無線電介面並配置密碼模式。

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

SSID - MAC地址身份驗證

此SSID根據無線客戶端的MAC地址對其進行身份驗證。它使用MAC地址作為使用者名稱/密碼。在本示例中，AP充當本地RADIUS，因此AP儲存MAC地址清單。外部RADIUS伺服器可以套用相同的組態。

步驟1.啟用AP作為RADIUS伺服器。NAS IP地址是AP的BVI。為MAC地址為aaabbbcccc的客戶端建立條目。

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

步驟2.配置AP向其傳送身份驗證請求的RADIUS伺服器（它是AP本身）。

```
# 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>
```

步驟3.將此RADIUS伺服器分配給RADIUS組。

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

步驟4.將此radius組分配給身份驗證方法。

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

步驟5.建立SSID，此示例將其分配給VLAN 2402。

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

步驟6.將SSID分配給介面802.11a。

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

SSID — 內部Web驗證

連線到此SSID的使用者將被重定向到Web身份驗證門戶以輸入有效的使用者名稱/密碼，如果身份驗證成功，則他們可以訪問網路。在此範例中，使用者儲存在本地RADIUS伺服器上。

在本示例中，SSID分配給VLAN 2403。

步驟1.啟用AP作為RADIUS伺服器。NAS IP地址是AP的BVI。

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

步驟2.配置AP向其傳送身份驗證請求的RADIUS伺服器（它是AP本身）。

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

步驟3.將此radius伺服器分配給radius組。

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

步驟4.將此radius組分配給身份驗證方法。

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

步驟5.建立准入策略。

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

步驟6.配置SSID。

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

步驟7.將SSID分配給介面。

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

步驟8.將策略分配到正確的子介面。

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

> **注意**：如果SSID在本機上運行，則策略將直接應用到介面，而不是子介面（dot11radio 0或dot11radio 1）。

步驟9.為訪客使用者建立使用者名稱/密碼。

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

SSID - Web傳輸

當客戶端連線到具有Web傳遞配置的SSID時，它將重定向到Web門戶，接受網路使用的條款和條件，否則，使用者將無法使用該服務。

此示例將SSID分配給本徵VLAN。

步驟1.建立准入策略。

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

步驟2.指定客戶端連線到此SSID時要顯示的消息。

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

步驟3.建立SSID。

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

步驟4.將SSID和許可策略分配給無線電

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

驗證

使用本節內容，確認您的組態是否正常運作。

 # show dot11 associations

顯示所連線的無線客戶端的mac地址、IPv4和IPv6地址以及SSID名稱。

```
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 associations aaaa.bbb.cccc

這顯示在mac地址中指定為RSSI、SNR、支援的資料速率等無線客戶端的詳細資訊。

```
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

顯示MAC地址、用於Web身份驗證或Web傳遞的IPv4地址以及使用者名稱（如果為Web身份驗證配置了SSID）。

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

show dot11 bssid

這顯示每個無線電介面與WLAN關聯的BSSID。

```
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

這會顯示子介面和橋接群組之間的關係。

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

clear dot11 client aaa.bbb.cccc

此命令有助於斷開無線客戶端與網路的連線。

clear dot11 webauth webauth-user username

此命令有助於刪除指定使用者的Web驗證作業階段。

執行以下debug命令以驗證使用者端的驗證程式：

```
# 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身份驗證

```
 *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
```