在自治AP上配置SSID和VLAN

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[配置VLAN-Switch和AP](#)
[配置AP和VLAN](#)
[配置交换机VLAN](#)
[SSID开放式身份验证 — AP的本征VLAN](#)
[SSID 802.1x — 内部RADIUS](#)
[SSID 802.1x — 外部RADIUS](#)
[SSID - PSK](#)
[SSID - MAC地址身份验证](#)
[SSID — 内部Web身份验证](#)
[SSID - Web直通](#)
[验证](#)
[故障排除](#)
[PSK](#)
[802.1x](#)
[MAC 验证](#)

简介

本文档说明如何为以下对象配置自主接入点(AP):

- 虚拟局域网 (VLAN)
- 开放式身份验证
- 802.1x，带内部远程身份验证拨入用户服务(RADIUS)
- 802.1x，带外部RADIUS
- 预共享密钥(PSK)
- MAC 地址身份验证
- Web身份验证（内部RADIUS）
- Web直通

先决条件

要求

思科建议您对以下主题有基本的了解：

- 802.1x
- PSK
- RADIUS
- Web 身份验证

使用的组件

本文档中的信息基于AP 3700版本15.3(3)JBB。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

> **提示**:这些示例也适用于ASA 5506内自治模式下的AP，其区别在于，不配置AP连接的交换机端口，而是将配置应用于ASA的Gig 1/9。

配置

> **注**: 属于同一VLAN的服务集标识符(SSID)不能同时应用于无线电。具有相同VLAN的SSID的配置示例未在同一AP上同时启用。

配置VLAN-Switch和AP

在AP和交换机上配置所需的VLAN。以下是本示例中使用的VLAN:

- VLAN 2401（本征）
- VLAN 2402
- VLAN 2403

配置AP和VLAN

配置接口千兆以太网

```
# 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
```

配置接口无线电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
```

注意: 802.11b无线电(interface dot11radio 0)未配置，因为它使用AP的本征VLAN。

配置交换机VLAN

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

配置AP所连接的接口：

```
# 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开放式身份验证 — AP的本征VLAN

此SSID没有安全性，它被广播（对客户端可见），加入WLAN的无线客户端被分配到本征VLAN。

步骤 1. 配置 SSID。

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

步骤2.将SSID分配给802.11b无线电。

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

SSID 802.1x — 内部RADIUS

此SSID将AP用作RADIUS服务器。请注意，AP作为RADIUS服务器仅支持LEAP、EAP-FAST和MAC身份验证。

步骤1.启用AP作为RADIUS服务器。

网络接入服务器(NAS)IP地址是AP的BVI，因为此IP地址是向自身发送身份验证请求的IP地址。此外

，创建用户名和密码。

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

步骤2.配置AP向其发送身份验证请求的RADIUS服务器，因为AP是本地RADIUS，所以IP地址是分配给AP的网桥虚拟接口(BVI)的IP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>
```

步骤3.将此RADIUS服务器分配给RADIUS组。

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

步骤4.将此RADIUS组分配给身份验证方法。

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

步骤5.创建SSID，将其分配给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
```

步骤6.将ssid分配给接口802.11a并指定密码模式。

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

SSID 802.1x — 外部RADIUS

配置与内部RADIUS几乎相同。

步骤1.配置aaa new-model。

第2步使用外部RADIUS IP地址，而不是AP的IP地址。

SSID - PSK

此SSID使用安全WPA2/PSK，并且此SSID上的用户被分配到VLAN 2402。

步骤 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
```

步骤2.将SSID分配给无线电接口并配置密码模式。

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

SSID - MAC地址身份验证

此SSID根据无线客户端的MAC地址对其进行身份验证。它使用MAC地址作为用户名/密码。在本示例中，AP充当本地RADIUS，因此AP存储MAC地址列表。同样的配置可应用于外部RADIUS服务器。

步骤1.启用AP作为RADIUS服务器。NAS IP地址是AP的BVI。为MAC地址为aaabbbbcccc的客户端创建条目。

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

步骤2.配置AP向其发送身份验证请求的RADIUS服务器（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>
```

步骤3.将此RADIUS服务器分配给RADIUS组。

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

步骤4.将此RADIUS组分配给身份验证方法。

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

步骤5.创建SSID，本示例将其分配给VLAN 2402。

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

步骤6.将SSID分配给接口802.11a。

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

SSID — 内部Web身份验证

连接到此SSID的用户被重定向到Web身份验证门户以输入有效的用户名/密码，如果身份验证成功，则他们有权访问网络。在本例中，用户存储在本地RADIUS服务器上。

在本例中，SSID被分配给VLAN 2403。

步骤1.启用AP作为RADIUS服务器。NAS IP地址是AP的BVI。

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

步骤2.配置AP向其发送身份验证请求的RADIUS服务器（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>
```

步骤3.将此RADIUS服务器分配给RADIUS组。

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

步骤4.将此RADIUS组分配给身份验证方法。

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

步骤5.创建准入策略。

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

步骤6.配置SSID。

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

步骤7.将SSID分配给接口。

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

步骤8.将策略分配到正确的子接口。

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

> 注意:**如果SSID在本地上工作，则策略将直接应用到接口，而不是子接口（dot11radio 0或dot11radio 1）。**

步骤9.为访客用户创建用户名/密码。

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

SSID - Web直通

当客户端通过Web直通配置连接到SSID时，它将重定向到Web门户以接受网络使用的条款和条件，如果不是，用户将无法使用该服务。

本示例将SSID分配给本征VLAN。

步骤1.创建准入策略。

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

步骤2.指定客户端连接到此SSID时要显示的消息。

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

步骤3.创建SSID。

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

步骤4.将SSID和准入策略分配给无线电

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

验证

使用本部分可确认配置能否正常运行。

show dot11 associations

这显示所连接的无线客户端的MAC地址、IPv4和IPv6地址、SSID名称。

```
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.bbbb.cccc

这显示了MAC地址中指定的无线客户端的更多详细信息，如RSSI、SNR、支持的数据速率等。

```
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

这将显示MAC地址、用于Web身份验证或Web传递的IPv4地址，以及如果SSID配置为Web身份验证的用户名。

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

show dot11 bssid

这显示了与每个无线电接口的WLAN关联的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
```

bridge verbose

这显示了子接口和网桥组之间的关系。

```
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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

 # clear dot11 client aaa.bbbb.cccc

此命令有助于断开无线客户端与网络的连接。

 # clear dot11 webauth webauth-user username

此命令有助于删除指定用户的Web身份验证会话。

运行以下debug命令以验证客户端的身份验证过程：

```
# 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 验证

```
 *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
```