Configurer les SSID et les VLAN sur les AP autonomes

Contenu

Introduction

Ce document explique comment configurer des points d'accès autonomes pour :

- Réseaux locaux virtuels (VLAN)
- Authentification ouverte
- 802.1x avec service d'accès à distance interne (RADIUS)
- 802.1x avec RADIUS externe
- Clé prépartagée (PSK)
- Authentification d’adresse MAC
- Authentification Web (rayon interne)
- Accès Web

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir une connaissance de base de ces sujets :

- 802.1x
- PSK
- RADIUS
- Authentification Web

Components Used

Les informations contenues dans ce document sont basées sur AP 3700 Version 15.3(3)JBB.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

> **Conseil** : Ces exemples s'appliquent également à l'AP en mode autonome dans ASA 5506, la différence est qu'au lieu de configurer le port de commutateur où l'AP est connecté, la configuration est appliquée au Gig 1/9 de l'ASA.

Configuration

> **Remarque** : Les identificateurs SSID (Service Set Identifiers) appartenant au même VLAN ne peuvent pas être appliqués simultanément à une radio. Les exemples de configuration des SSID avec le même VLAN n'ont pas été activés simultanément sur le même AP.

Configurer le commutateur VLAN et le point d’accès

Configurez les VLAN requis sur le point d’accès et le commutateur. Voici les VLAN utilisés dans cet exemple :

- VLAN 2401 (natif)
- VLAN 2402
- VLAN 2403

Configurer les points d’accès et les VLAN

Configurer l'interface 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
```

Configuration de la radio d'interface 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
```

> **Remarque** : la radio 802.11b (interface dot11radio 0) n'est pas configurée, car elle utilise le VLAN natif de l'AP.

Configurer le VLAN du commutateur

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

Configurez l'interface sur laquelle le point d'accès est connecté :

```
# 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 Authentication - VLAN natif du point d'accès

Ce SSID n'a pas de sécurité, il est diffusé (visible par les clients) et les clients sans fil qui se connectent au WLAN sont affectés au VLAN natif.

Étape 1. Configurez le SSID.

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

Étape 2. Attribuez le SSID à la radio 802.11b.

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

SSID 802.1x - RADIUS interne

Ce SSID utilise l'AP comme serveur RADIUS. N'oubliez pas que AP en tant que serveur RADIUS prend uniquement en charge l'authentification LEAP, EAP-FAST et MAC.

Étape 1. Activez AP comme serveur radius.

L'adresse IP du serveur d'accès réseau (NAS) est l'interface BVI du point d'accès, car cette adresse IP est celle qui envoie la demande d'authentification à elle-même. Créez également un nom d'utilisateur et un mot de passe.

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

Étape 2. Configurez le serveur RADIUS vers lequel le point d'accès envoie la demande d'authentification, car il s'agit d'un RADIUS local, l'adresse IP est celle attribuée à l'interface virtuelle de pont (BVI) du point d'accès.

```
# 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>
```

Étape 3. Attribuez ce serveur RADIUS à un groupe radius.

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

Étape 4. Attribuez ce groupe radius à une méthode d'authentification.

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

Étape 5. Créez le SSID, attribuez-le au 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
```

Étape 6. Attribuez le ssid à l’interface 802.11a et spécifiez le mode de chiffrement.

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

SSID 802.1x - RADIUS externe

La configuration est presque identique à celle de RADIUS interne.

Étape 1. Configurer un nouveau modèle.

Étape 2, utilisez l'adresse IP RADIUS externe au lieu de l'adresse IP de l'AP.

SSID - PSK

Ce SSID utilise la sécurité WPA2/PSK et les utilisateurs de ce SSID sont affectés au VLAN 2402.

Étape 1. Configurez le 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
```

Étape 2. Attribuez le SSID à l'interface radio et configurez le mode de chiffrement.

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

SSID - Authentification d'adresse MAC

Ce SSID authentifie les clients sans fil en fonction de leur adresse MAC. Il utilise l'adresse MAC comme nom d'utilisateur/mot de passe. Dans cet exemple, le point d'accès agit en tant que RADIUS local, de sorte que le point d'accès stocke la liste d'adresses MAC. La même configuration peut être appliquée avec un serveur RADIUS externe.

Étape 1. Activez AP en tant que serveur RADIUS. L'adresse IP NAS est l'interface BVI du point d'accès. Créez l'entrée du client avec l'adresse MAC aaabbbcccc.

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

Étape 2. Configurez le serveur RADIUS auquel le point d'accès envoie la demande d'authentification (c'est le point d'accès lui-même).

```
# 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>
```

Étape 3. Attribuez ce serveur RADIUS à un groupe radius.

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

Étape 4. Attribuez ce groupe radius à une méthode d'authentification.

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

Étape 5. Créez le SSID, cet exemple l'attribue au VLAN 2402.

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

Étape 6. Attribuez le SSID à l'interface 802.11a.

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

SSID - Authentification Web interne

Les utilisateurs qui se connectent à ce SSID sont redirigés vers un portail d'authentification Web pour entrer un nom d'utilisateur/mot de passe valide. Si l'authentification réussit, ils ont accès au réseau. Dans cet exemple, les utilisateurs sont stockés sur le serveur RADIUS local.

Dans cet exemple, le SSID est attribué au VLAN 2403.

Étape 1. Activez AP en tant que serveur RADIUS. L'adresse IP NAS est l'interface BVI du point d'accès.

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

Étape 2. Configurez le serveur RADIUS auquel le point d'accès envoie la demande d'authentification (c'est le point d'accès lui-même).

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

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

Étape 3. Attribuez ce serveur RADIUS à un groupe RADIUS.

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

Étape 4. Attribuez ce groupe radius à une méthode d'authentification.

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

Étape 5. Créez les stratégies d'admission.

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

Étape 6. Configurez le SSID.

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

Étape 7. Attribuez le SSID à l'interface.

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

Étape 8. Attribuez la stratégie à la sous-interface de droite.

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

> **Remarque** : si le SSID fonctionne sur le routeur natif, la stratégie est appliquée directement à l'interface et non à la sous-interface (dot11radio 0 ou dot11radio 1).

Étape 9. Créez le nom d'utilisateur/mot de passe des utilisateurs invités.

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

SSID - Accès Web

Lorsqu'un client se connecte à un SSID avec une configuration Web Pass-through, il est redirigé vers un portail Web pour accepter les conditions générales d'utilisation du réseau, sinon, l'utilisateur ne pourra pas utiliser le service.

Cet exemple attribue le SSID au VLAN natif.

Étape 1. Créez la politique d'admission.

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

Étape 2. Spécifiez le message à afficher lorsque les clients se connectent à ce SSID.

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

Étape 3. Créez le SSID.

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

Étape 4. Attribuez le SSID et la politique d'admission à la radio

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

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

show dot11 associations

Affiche l'adresse MAC, l'adresse IPv4 et IPv6, le nom SSID des clients sans fil connectés.

```
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

Cela montre plus de détails sur le client sans fil spécifié dans l'adresse mac comme RSSI, SNR, les débits de données pris en charge et d'autres.

```
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

Affiche l'adresse MAC, l'adresse IPv4 pour l'authentification Web ou le transfert Web et le nom d'utilisateur si le SSID est configuré pour l'authentification Web.

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

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

show dot11 bssid

Ceci montre les BSSID associés aux WLAN par interface 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
```

show bridge verbose

Ceci montre la relation entre les sous-interfaces et les groupes de ponts.

```
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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

clear dot11 client aaa.bbbb.cccc

Cette commande permet de déconnecter un client sans fil du réseau.

clear dot11 webauth webauth-user username

Cette commande aide à supprimer la session d'authentification Web de l'utilisateur spécifié.

Exécutez ces commandes debug afin de vérifier le processus d'authentification du 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
```

Authentification 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
```