Configure SSIDs and VLANs on Autonomous APs

Contents

Introduction

This document explains how to configure autonomous Access Points (APs) for:

- Virtual Local Area Networks (VLANs)
- Open authentication
- 802.1x with internal Remote Authentication Dial-In User Service (RADIUS)
- 802.1x with external RADIUS
- Pre-shared Key (PSK)
- MAC address authentication
- Web authentication (internal radius)
- Web Pass-through

Prerequisites

Requirements

Cisco recommends you have a basic knowledge of these topics:

- 802.1x
- PSK
- RADIUS
- Web Authentication

Components Used

The information in this document is based on 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. If your network is live, ensure that you understand the potential impact of any command.

> **Tip**: These examples also applies to the AP in autonomous mode inside ASA 5506, the difference is that instead of configure the switch port where the AP is connected, the configuration is applied to the ASA's Gig 1/9.

Configure

> **Note**: The Service Set Identifiers (SSIDs) that belong to the same VLAN cannot be applied to a radio at the same time. The configuration examples of the SSIDs with the same VLAN were not enabled at the same time on the same AP.

Configure VLAN-Switch and AP

Configure the required VLANs on both the AP and switch. These are the VLANs used in this example:

- VLAN 2401 (Native)
- VLAN 2402
- VLAN 2403

Configure APs and VLANs

Configure 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
```

Configure Interface Radio 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
```

> **Note**: 802.11b radio (interface dot11radio 0) is not configured, as it uses the native VLAN of the AP.

Configure Switch VLAN

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

Configure the interface where the AP is connected:

```
# 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 - AP's Native VLAN

This SSID does not have security, it is broadcasted (visible to clients) and the wireless clients that joins the WLAN are assigned to the native VLAN.

Step 1. Configure the SSID.

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

Step 2. Assign the SSID to the 802.11b radio.

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

SSID 802.1x - Internal RADIUS

This SSID uses the AP as RADIUS server. Be aware that AP as RADIUS server only supports LEAP, EAP-FAST and MAC authentication.

Step 1. Enable AP as radius server.

The Network Access Server(NAS) IP address is the AP's BVI, as this IP address is the one that sends the authentication request to itself. Also, create a username and password.

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

Step 2. Configure the RADIUS server to which the AP sends the authentication request, as it is local RADIUS, the IP address is the one assigned to AP's Bridge Vitrual 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>
```

Step 3. Assign this RADIUS server to a radius group.

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

Step 4. Assign this radius group to an authentication method.

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

Step 5. Create the SSID, assign it to 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
```

Step 6. Assign the ssid to the interface 802.11a and specify the cipher mode.

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

SSID 802.1x - External RADIUS

The configuration is almost the same as Internal RADIUS.

Step 1. Configure **aaa new-model.**

Step 2, Instead of the AP's IP address, use the external RADIUS IP address.

SSID - PSK

This SSID uses security WPA2/PSK and users on this SSID are assigned to VLAN 2402.

Step 1. Configure the 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
```

Step 2. Assign the SSID to the radio interface and configure the cipher mode.

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

SSID - MAC Address Authentication

This SSID authenticates the wireless clients based on their MAC address. It uses the MAC address as username/password. In this example the AP acts as local RADIUS, so the AP stores the MAC address list. The same configuration can be applied with external RADIUS server.

Step 1. Enable AP as RADIUS server. The NAS IP address is the AP's BVI. Create the entry for the client with MAC address aaaabbbbcccc.

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

Step 2. Configure the RADIUS server to which the AP sends the authentication request (it is the AP itself).

```
# 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>
```

Step 3. Assign this RADIUS server to a radius group.

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

Step 4. Assign this radius group to an authentication method.

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

Step 5. Create the SSID, this example assigns it to VLAN 2402.

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

Step 6. Assign the SSID to the interface 802.11a.

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

SSID - Internal Web Authentication

Users that connect to this SSID are redirected to a web authentication portal to enter a valid username/password, if authentication is successful, they have access to the network. In this example, the users are stored on the local RADIUS server.

In this example, the SSID is assigned to VLAN 2403.

Step 1. Enable AP as RADIUS server. The NAS IP address is the AP's BVI.

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

Step 2. Configure the RADIUS server to which the AP sends the authentication request (it is the AP itself).

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

Step 3. Assign this radius server to a radius group.

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

Step 4. Assign this radius group to an authentication method.

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

Step 5. Create the admission policies.

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

Step 6. Configure the SSID.

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

Step 7. Assign the SSID to the interface.

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

Step 8. Assign the policy to the right sub-interface.

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

> **Note**: If the SSID works on the native, then the policy is applied directly to the interface, not to the sub-interface (dot11radio 0 or dot11radio 1).

Step 9. Create the username/password for the guest users.

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

SSID - Web Pass-Through

When a client connects to an SSID with Web Pass-through configuration, it will be redirected to a web portal to accept the terms & conditions of the network usage, if not, the user will not be able to use the service.

This example assigns the SSID to the native VLAN.

Step 1. Create the admission policy.

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

Step 2. Specify the message to be displayed when clients connect to this SSID.

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

Step 3. Create the SSID.

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

Step 4. Assign the SSID and the admission policy to the radio

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

Verify

Use this section in order to confirm that your configuration works properly.

show dot11 associations

This shows the mac address, IPv4 and IPv6 address, SSID's name of the wireless clients connected.

```
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

This shows more details of the wireless client specified in the mac address as RSSI, SNR, data rates supported and others.

```
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

This shows the mac address, the IPv4 address for web authentication or web pass-through and the username if the SSID is configured for web authentication.

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

 # show dot11 bssid

This shows the BSSIDs associated to the WLANs 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
```

 # show bridge verbose

This shows the relation between sub-interfaces and bridge groups.

```
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
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

 # clear dot11 client aaa.bbbb.cccc

This command helps to disconnect a wireless client from the network.

 # clear dot11 webauth webauth-user username

This command helps to delete the web authentication session of the specified user.

Run these debug commands in order to verify the authentication process of the 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
```

MAC Authentication

```
 *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
```