Konfigurieren von SSIDs und VLANs auf unabhängigen APs

Inhalt

Einführung

In diesem Dokument wird erläutert, wie autonome Access Points (APs) für folgende Aufgaben konfiguriert werden:

- Virtual Local Area Networks (VLANs)
- Offene Authentifizierung
- 802.1x mit internem RADIUS (Remote Authentication Dial-In User Service)
- 802.1x mit externem RADIUS
- Vorinstallierter Schlüssel (PSK)
- MAC-Adressauthentifizierung
- Webauthentifizierung (interner Radius)
- Web-Pass-Through

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- 802.1x
- PSK
- RADIUS
- Webauthentifizierung

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf AP 3700 Version 15.3(3)JBB.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

> **Tipp**: Diese Beispiele gelten auch für den Access Point im Autonomous-Modus der ASA 5506. Der Unterschied besteht darin, dass die Konfiguration nicht auf den Switch-Port angewendet wird, an den der Access Point angeschlossen ist, sondern auf den Gig 1/9 der ASA.

Konfigurieren

> **Hinweis**: Die Service Set Identifiers (SSIDs), die demselben VLAN angehören, können nicht gleichzeitig auf ein Funkmodul angewendet werden. Die Konfigurationsbeispiele der SSIDs mit demselben VLAN wurden nicht gleichzeitig auf demselben WAP aktiviert.

VLAN-Switch und AP konfigurieren

Konfigurieren Sie die erforderlichen VLANs auf dem Access Point und Switch. Dies sind die in diesem Beispiel verwendeten VLANs:

- VLAN 2401 (nativ)
- VLAN 2402
- VLAN 2403

Konfigurieren von APs und VLANs

Konfigurieren von 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
```

Konfigurieren der Schnittstellenfunk-Funktion 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
```

> **Hinweis**: 802.11b Radio (interface dot11radio 0) ist nicht konfiguriert, da es das native VLAN des AP verwendet.

Switch-VLAN konfigurieren

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

Konfigurieren Sie die Schnittstelle, an die der Access Point angeschlossen ist:

```
# 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 - natives VLAN des AP

Diese SSID verfügt über keine Sicherheitsfunktionen, sondern wird übertragen (für Clients sichtbar) und die Wireless-Clients, die zum WLAN gehören, werden dem nativen VLAN zugewiesen.

Schritt 1: Konfigurieren Sie die SSID.

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

Schritt 2: Weisen Sie den SSID dem 802.11b-Funkmodul zu.

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

SSID 802.1x - Interner RADIUS

Diese SSID verwendet den AP als RADIUS-Server. Beachten Sie, dass AP als RADIUS-Server nur LEAP-, EAP-FAST- und MAC-Authentifizierung unterstützt.

Schritt 1: Aktivieren Sie AP als Radius-Server.

Die IP-Adresse des Network Access Server (NAS) ist die BVI des Access Points, da diese IP-Adresse die Authentifizierungsanforderung an sich selbst sendet. Erstellen Sie außerdem einen Benutzernamen und ein Kennwort.

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

Schritt 2: Konfigurieren Sie den RADIUS-Server, an den der Access Point die Authentifizierungsanforderung sendet, da es sich um einen lokalen RADIUS handelt. Die IP-Adresse ist die Adresse, die der Bridge Virtual Interface (BVI) des Access Points zugewiesen ist.

```
# 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>
```

Schritt 3: Weisen Sie diesen RADIUS-Server einer Radius-Gruppe zu.

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

Schritt 4: Weisen Sie diese Radius-Gruppe einer Authentifizierungsmethode zu.

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

Schritt 5: Erstellen Sie die SSID, und weisen Sie sie VLAN 2402 zu.

```
#  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
```

Schritt 6: Weisen Sie der Schnittstelle 802.11a die ssid zu, und geben Sie den Verschlüsselungsmodus an.

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

SSID 802.1x - Externes RADIUS

Die Konfiguration entspricht fast der internen RADIUS-Konfiguration.

Schritt 1: Konfigurieren **eines neuen Modells**

Schritt 2: Verwenden Sie anstelle der IP-Adresse des Access Points die externe RADIUS-IP-Adresse.

SSID - PSK

Diese SSID verwendet WPA2/PSK, und die Benutzer dieser SSID sind VLAN 2402 zugewiesen.

Schritt 1: Konfigurieren Sie die 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
```

Schritt 2: Weisen Sie der Funkschnittstelle die SSID zu, und konfigurieren Sie den Verschlüsselungsmodus.

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

SSID = MAC Address Authentication

Diese SSID authentifiziert die Wireless-Clients anhand ihrer MAC-Adresse. Die MAC-Adresse wird als Benutzername/Kennwort verwendet. In diesem Beispiel agiert der Access Point als lokaler RADIUS, sodass der Access Point die MAC-Adressliste speichert. Dieselbe Konfiguration kann mit einem externen RADIUS-Server angewendet werden.

Schritt 1: Aktivieren Sie AP als RADIUS-Server. Die NAS-IP-Adresse ist die BVI des Access Points. Erstellen Sie den Eintrag für den Client mit der MAC-Adresse aaabbbcccc.

```
# aaa new-model
```

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

Schritt 2: Konfigurieren Sie den RADIUS-Server, an den der Access Point die Authentifizierungsanforderung sendet (dies ist der Access Point selbst).

```
# 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>
```

Schritt 3: Weisen Sie diesen RADIUS-Server einer Radius-Gruppe zu.

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

Schritt 4: Weisen Sie diese Radius-Gruppe einer Authentifizierungsmethode zu.

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

Schritt 5: Erstellen Sie die SSID. In diesem Beispiel wird diese dem VLAN 2402 zugewiesen.

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

Schritt 6: Weisen Sie die SSID der Schnittstelle 802.11a zu.

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

SSID = Internal Web Authentication

Benutzer, die eine Verbindung zu dieser SSID herstellen, werden an ein Web-Authentifizierungsportal weitergeleitet, um einen gültigen Benutzernamen/ein gültiges Kennwort einzugeben. Wenn die Authentifizierung erfolgreich ist, haben sie Zugriff auf das Netzwerk. In diesem Beispiel werden die Benutzer auf dem lokalen RADIUS-Server gespeichert.

In diesem Beispiel wird die SSID VLAN 2403 zugewiesen.

Schritt 1: Aktivieren Sie AP als RADIUS-Server. Die NAS-IP-Adresse ist die BVI des Access Points.

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

Schritt 2: Konfigurieren Sie den RADIUS-Server, an den der Access Point die Authentifizierungsanforderung sendet (dies ist der Access Point selbst).

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

Schritt 3: Weisen Sie diesen Radius-Server einer Radius-Gruppe zu.

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

Schritt 4: Weisen Sie diese Radius-Gruppe einer Authentifizierungsmethode zu.

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

Schritt 5: Erstellen Sie die Zugangsrichtlinien.

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

Schritt 6: Konfigurieren Sie die SSID.

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

Schritt 7: Weisen Sie der Schnittstelle die SSID zu.

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

Schritt 8: Weisen Sie die Richtlinie der richtigen Subschnittstelle zu.

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

Hinweis: Wenn die SSID auf dem nativen Gerät funktioniert, wird die Richtlinie direkt auf die Schnittstelle und nicht auf die Subschnittstelle (dot11radio 0 oder dot11radio 1) angewendet.

Schritt 9: Erstellen Sie den Benutzernamen/das Kennwort für die Gastbenutzer.

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

SSID = Web Pass-Through

Wenn ein Client eine Verbindung zu einer SSID mit einer Web-Pass-Through-Konfiguration herstellt, wird er an ein Webportal umgeleitet, um die Bedingungen für die Netzwerknutzung zu akzeptieren. Andernfalls kann der Benutzer den Dienst nicht verwenden.

In diesem Beispiel wird die SSID dem nativen VLAN zugewiesen.

Schritt 1: Erstellen Sie die Zugangsrichtlinie.

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

Schritt 2: Geben Sie die Meldung an, die angezeigt werden soll, wenn die Clients eine Verbindung zu dieser SSID herstellen.

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

Schritt 3: Erstellen Sie die SSID.

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

Schritt 4: Zuweisung der SSID und der Zugangsrichtlinie zur Funkübertragung

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

dot11 Verknüpfungen anzeigen

Dies zeigt die MAC-Adresse, die IPv4- und die IPv6-Adresse, den Namen der SSID der angeschlossenen Wireless-Clients.

```
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 dot1 Associates aaaa.bbb.cccc

Hier werden weitere Details zum Wireless-Client angezeigt, der in der MAC-Adresse als RSSI, SNR, unterstützte Datenraten usw. angegeben ist.

```
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
```

Anzahl Webauth-Sitzungen auf Dots11 anzeigen

Dies zeigt die MAC-Adresse, die IPv4-Adresse für Webauthentifizierung oder Web-Pass-Through und den Benutzernamen, wenn der SSID für die Webauthentifizierung konfiguriert ist.

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

show dot11 bssid

Dies zeigt die BSSIDs, die den WLANs pro Funkschnittstelle zugeordnet sind.

```
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

Dies zeigt die Beziehung zwischen Sub-Schnittstellen und Bridge-Gruppen.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

clear dot11 client aaa.bbb.cccc

Mit diesem Befehl kann die Verbindung zwischen einem Wireless-Client und dem Netzwerk getrennt werden.

clear dot11 webauth webauth-user username

Mit diesem Befehl kann die Webauthentifizierungssitzung des angegebenen Benutzers gelöscht werden.

Führen Sie diese Debugbefehle aus, um den Authentifizierungsprozess des Clients zu überprüfen:

```
# 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-Authentifizierung

```
 *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
```