Configuración SSID y VLA N en los AP autónomos

Contenido

Introducción

Este documento explica cómo configurar el (APS) autónomo de los Puntos de acceso para:

- Redes de área local virtuales (VLA N)
- Autenticación abierta
- 802.1x con el Remote Authentication Dial-In User Service (RADIUS) interno
- 802.1x con el externo RADIUS
- Clave previamente compartida (PSK)
- Autenticación de la dirección MAC
- Autenticación Web (radio interno)
- Paso de la red

Prerrequisitos

Requisitos

Cisco le recomienda tiene un conocimiento básico de estos temas:

- 802.1x
- PSK
- RADIUS
- Autenticación Web

Componentes Utilizados

La información en este documento se basa en la versión 15.3(3)JBB AP 3700.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

> Consejo: Estos ejemplos también se aplican al AP en el modo autónomo dentro de ASA 5506, la diferencia son ése en vez de configuración el puerto del switch en donde el AP está conectado, la configuración se aplican al carruaje 1/9 ASA.

Configurar

> Nota: Los identificadores del conjunto de servicio (SSID) que pertenecen al mismo VLA N no se pueden aplicar a una radio al mismo tiempo. Los ejemplos de configuración de los SSID con el mismo VLA N no fueron habilitados al mismo tiempo en el mismo AP.

VLA N-Switch de la configuración y AP

Configure los VLA N requeridos en el AP y conmutelos. Éstos son los VLA N usados en este ejemplo:

- VLA N 2401 (natural)
- VLA N 2402
- VLA N 2403

Configuración AP y VLA N

Interfaces Gigabit Ethernet de la configuración

```
# 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
```

802.11a de la radio de la interfaz de la configuración

```
# 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
```

> Nota: la radio del 802.11b (interfaz dot11radio 0) no se configura, pues utiliza el VLAN nativo del AP.

VLA N del Switch de la configuración

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

Configure la interfaz donde el AP está conectado:

```
# 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
```

Autenticación abierta SSID - El VLAN nativo AP

Este SSID no tiene Seguridad, se transmite (visible a los clientes) y asignan los clientes de red inalámbrica que se une a la red inalámbrica (WLAN) al VLAN nativo.

Paso 1. Configure el SSID.

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

Paso 2. Asigne el SSID a la radio del 802.11b.

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

802.1x SSID - RADIUS interno

Este SSID utiliza el AP como servidor de RADIUS. Sea consciente que AP como los soportes del servidor de RADIUS solamente SALTAN, EAP-FAST y autenticación de MAC.

Paso 1. Permiso AP como servidor de RADIUS.

El IP address de Server(NAS) del acceso a la red es el BVI AP, pues esta dirección IP es la que envía el pedido de autenticación a sí mismo. También, cree un nombre de usuario y contraseña.

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

Paso 2. Configure al servidor de RADIUS a quien el AP envía el pedido de autenticación, como es RADIUS local, la dirección IP es el que está asignado al (BVI) de la interfaz de Vitrual del Bridge AP.

```
# 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>
```

Paso 3. Asigne a este servidor de RADIUS a un grupo del radio.

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

Paso 4. Asigne este grupo del radio a un método de autentificación.

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

Paso 5. Cree el SSID, asígnelo al VLA N 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
```

Paso 6. Asigne el ssid al 802.11a de la interfaz y especifique el modo de la cifra.

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

802.1x SSID - Externo RADIUS

La configuración casi es lo mismo que el RADIUS interno.

Paso 1. Configuración **aaa de modelo nuevo.**

El paso 2, en vez del IP address AP, utiliza la dirección IP del externo RADIUS.

SSID - PSK

Este SSID utiliza la Seguridad WPA2/PSK y a los usuarios en este SSID se asigna al VLA N 2402.

Paso 1. Configure el 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
```

Paso 2. Asigne el SSID a la interfaz radio y configure el modo de la cifra.

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

SSID - Autenticación de la dirección MAC

Este SSID autentica a los clientes de red inalámbrica basados en su dirección MAC. Utiliza la dirección MAC como el nombre de usuario/contraseña. En este ejemplo el AP actúa como RADIUS local, así que el AP salva la lista de la dirección MAC. La misma configuración se puede aplicar con el servidor RADIUS externo.

Paso 1. Permiso AP como servidor de RADIUS. El IP address NAS es el BVI AP. Cree la entrada para el cliente con el aaaabbbbcccc de la dirección MAC.

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

Paso 2. Configure al servidor de RADIUS a quien el AP envía el pedido de autenticación (es el AP sí mismo).

```
# 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>
```

Paso 3. Asigne a este servidor de RADIUS a un grupo del radio.

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

Paso 4. Asigne este grupo del radio a un método de autentificación.

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

Paso 5. Cree el SSID, este ejemplo lo asigna al VLA N 2402.

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

Paso 6. Asigne el SSID al 802.11a de la interfaz.

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

SSID - Autenticación del Web interna

Reorientan a los usuarios que conectan con este SSID a un portal de la autenticación Web para ingresar un nombre de usuario válido/una contraseña, si la autenticación es acertada, ellos tienen acceso a la red. En este ejemplo, salvan a los usuarios en el servidor de RADIUS local.

En este ejemplo, el SSID se asigna al VLA N 2403.

Paso 1. Permiso AP como servidor de RADIUS. El IP address NAS es el BVI AP.

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

Paso 2. Configure al servidor de RADIUS a quien el AP envía el pedido de autenticación (es el AP sí mismo).

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

Paso 3. Asigne a este servidor de RADIUS a un grupo del radio.

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

Paso 4. Asigne este grupo del radio a un método de autentificación.

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

Paso 5. Cree las directivas de admisión.

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

Paso 6. Configure el SSID.

```
# conf t
```

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

Paso 7. Asigne el SSID a la interfaz.

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

Paso 8. Asigne la directiva a la sub-interfaz correcta.

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

> Nota: Si el SSID trabaja en el nativo, después la directiva se aplica directamente a la interfaz, no a la sub-interfaz (dot11radio 0 o dot11radio 1).

Paso 9. Cree el nombre de usuario/la contraseña para los Usuarios invitados.

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

SSID - Paso de la red

Cuando un cliente conecta con un SSID con la configuración del paso de la red, será reorientada a un portal web para validar los términos y las condiciones del USO de la red, si no, el usuario no podrán utilizar el servicio.

Este ejemplo asigna el SSID al VLAN nativo.

Paso 1. Cree la directiva de admisión.

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

Paso 2. Especifique el mensaje que se visualizará cuando los clientes conectan con este SSID.

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

Paso 3. Cree el SSID.

```
# dot11 ssid webpassth-autonomous
```

```
# web-auth
# authentication open
# guest-mode
```

Paso 4. Asigne el SSID y la directiva de admisión a la radio

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

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

asociaciones del dot11 de la demostración

Esto muestra el MAC address, el direccionamiento del IPv4 y del IPv6, el nombre SSID de los clientes de red inalámbrica conectados.

```
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
```

asociaciones aaaa.bbbb.cccc del dot11 de la demostración

Esto muestra a más detalles del cliente de red inalámbrica especificados en el MAC address como el RSSI, SNR, las velocidades de datos soportó y otras.

```
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
```

webauth-sesiones del dot11 de la demostración

Esto muestra el MAC address, el direccionamiento del IPv4 para el paso de la autenticación Web o de la red y el nombre de usuario si el SSID se configura para la autenticación Web.

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

bssid del dot11 de la demostración

Esto muestra el BSSIDs asociado a los WLAN por la interfaz 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
```

Bridge de la demostración prolijo

Esto muestra la relación entre los subinterfaces y los Grupos de Bridge.

```
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
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

cliente claro aaa.bbbb.cccc del dot11

Este comando ayuda a desconectar a un cliente de red inalámbrica de la red.

nombre de usuario claro del webauth-usuario del webauth del dot11

Este comando ayuda a borrar la sesión de la autenticación Web del usuario específicado.

Funcione con estos comandos debug para verificar el proceso de autenticación del cliente:

```
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
```

PSK

```
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
```

802.1x

```
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
```

Autenticación de MAC

```
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
```