Configurar SSID e VLAN em AP autônomos

Índice

Introdução

Este documento explica como configurar os Access point autônomos (AP) para:

- Redes de área local virtual (VLAN)
- Autenticação aberta
- 802.1x com Remote Authentication Dial-In User Service (RADIUS) interno
- 802.1x com RAIO externo
- Chave pré-compartilhada (PSK)
- Autenticação do MAC address
- Autenticação da Web (raio interno)
- Web Passagem-através de

Pré-requisitos

Requisitos

Cisco recomenda-o tem um conhecimento básico destes assuntos:

- 802.1x
- PSK
- RADIUS
- Autenticação da Web

Componentes Utilizados

A informação neste documento é baseada na versão 15.3(3)JBB AP 3700.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

> Dica: Estes exemplos igualmente aplicam-se ao AP no modo autônomo dentro de ASA 5506, a diferença são aquele em vez de configuram a porta de switch onde o AP é conectado, a configuração são aplicados à atuação 1/9 do ASA.

Configurar

> Nota: Os service set identifier (SSID) que pertencem ao mesmo VLAN não podem ser aplicados a um rádio ao mesmo tempo. Os exemplos de configuração dos SSID com o mesmo VLAN não foram permitidos ao mesmo tempo no mesmo AP.

Configurar o VLAN-interruptor e o AP

Configurar os VLAN exigidos no AP e comute-os. Estes são os VLAN usados neste exemplo:

- VLAN 2401 (nativo)
- VLAN 2402
- VLAN 2403

Configurar AP e VLAN

Configurar o Gigabit Ethernet da relação

```
# 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
```

Configurar a relação 802.11a de rádio

```
# 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: 802.11b transmitem por rádio (relação dot11radio 0) não são configurados, porque usam o VLAN nativo do AP.

Configurar o interruptor VLAN

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

Configurar a relação onde o AP é 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
```

Autenticação aberta SSID - O VLAN nativo do AP

Este SSID não tem a Segurança, é transmitido (visível aos clientes) e os clientes Wireless que se junta ao WLAN são atribuídos ao VLAN nativo.

Etapa 1. Configurar o SSID.

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

Etapa 2. Atribua o SSID ao rádio 802.11b.

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

802.1x SSID - RAIO interno

Este SSID usa o AP como o servidor Radius. Esteja ciente que AP como os apoios do servidor Radius somente PULAM, EAP-FAST e autenticação de MAC.

Etapa 1. Permita o AP como o servidor Radius.

O IP address de Server(NAS) do acesso de rede é o BVI do AP, porque este endereço IP de Um ou Mais Servidores Cisco ICM NT é esse que se envia o pedido de autenticação. Também, crie um nome de usuário e senha.

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

Etapa 2. Configurar o servidor Radius a que o AP envia o pedido de autenticação, como é RAIO local, o endereço IP de Um ou Mais Servidores Cisco ICM NT é esse atribuído à relação de Vitrual da ponte do AP (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>
```

Etapa 3. Atribua este servidor Radius a um grupo do raio.

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

Etapa 4. Atribua este grupo do raio a um método de autenticação.

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

Etapa 5. Crie o SSID, atribua-o a 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
```

Etapa 6. Atribua o ssid à relação 802.11a e especifique o modo da cifra.

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

802.1x SSID - RAIO externo

A configuração é quase a mesma que o RAIO interno.

Etapa 1. Configurar o **novo modelo aaa.**

Etapa 2, em vez do IP address do AP, usa o endereço IP de Um ou Mais Servidores Cisco ICM NT externo do RAIO.

SSID - PSK

Este SSID usa a Segurança WPA2/PSK e os usuários neste SSID é atribuído a VLAN 2402.

Etapa 1. Configurar o 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
```

Etapa 2. Atribua o SSID à interface de rádio e configurar o modo da cifra.

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

SSID - Autenticação do MAC address

Este SSID autentica os clientes Wireless baseados em seu MAC address. Usa o MAC address como o username/senha. Neste exemplo o AP atua como o RAIO local, assim que o AP armazena a lista do MAC address. A mesma configuração pode ser aplicada com servidor de raio externo.

Etapa 1. Permita o AP como o servidor Radius. O IP address NAS é o BVI do AP. Crie a entrada para o cliente com o aaaabbbbcccc do MAC address.

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

Etapa 2. Configurar o servidor Radius a que o AP envia o pedido de autenticação (é o AP próprio).

```
# 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>
```

Etapa 3. Atribua este servidor Radius a um grupo do raio.

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

Etapa 4. Atribua este grupo do raio a um método de autenticação.

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

Etapa 5. Crie o SSID, este exemplo atribui-o a VLAN 2402.

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

Etapa 6. Atribua o SSID à relação 802.11a.

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

SSID - Autenticação do web interna

Os usuários que conectam a este SSID são reorientados a um portal da autenticação da Web para incorporar um nome de usuário válido/senha, se a autenticação é bem sucedida, eles têm o acesso à rede. Neste exemplo, os usuários são armazenados no servidor Radius local.

Neste exemplo, o SSID é atribuído a VLAN 2403.

Etapa 1. Permita o AP como o servidor Radius. O IP address NAS é o BVI do AP.

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

Etapa 2. Configurar o servidor Radius a que o AP envia o pedido de autenticação (é o AP próprio).

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

Etapa 3. Atribua este servidor Radius a um grupo do raio.

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

Etapa 4. Atribua este grupo do raio a um método de autenticação.

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

Etapa 5. Crie as políticas de admissão.

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

Etapa 6. Configurar o SSID.

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

```
# mbssid guest-mode
```

Etapa 7. Atribua o SSID à relação.

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

Etapa 8. Atribua a política à secundário-relação direita.

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

> Nota: Se o SSID trabalha no nativo, a seguir a política está aplicada diretamente à relação, não à secundário-relação (dot11radio 0 ou dot11radio 1).

Etapa 9. Crie o username/senha para os usuários convidado.

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

SSID - Web Passagem-através de

Quando um cliente conecta a um SSID com a Web Passagem-através da configuração, estará reorientada a um portal da web para aceitar os termos & as condições do USO de rede, se não, o usuário não poderão usar o serviço.

Este exemplo atribui o SSID ao VLAN nativo.

Etapa 1. Crie a política de admissão.

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

Etapa 2. Especifique a mensagem a ser indicada quando os clientes conectam a este SSID.

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

Etapa 3. Crie o SSID.

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

Etapa 4. Atribua o SSID e a política de admissão ao rádio

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

associações do dot11 da mostra

Isto mostra o MAC address, o endereço do IPv4 e do IPv6, o nome do SSID dos clientes Wireless 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
```

associações aaaa.bbbb.cccc do dot11 da mostra

Isto mostra mais detalhes do cliente Wireless especificados no MAC address como o RSSI, SNR, taxas de dados apoiou e outro.

```
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-sessões do dot11 da mostra

Isto mostra o MAC address, o endereço do IPv4 para a autenticação da Web ou a Web passagem-através de e o username se o SSID é configurado para a autenticação da Web.

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

bssid do dot11 da mostra

Isto mostra o BSSIDs associado aos WLAN pela interface de rádio.

```
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
```

ponte da mostra verboso

Isto mostra a relação entre subinterfaces e 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 seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

cliente claro aaa.bbbb.cccc do dot11

Este comando ajuda a desligar um cliente Wireless da rede.

 # username claro do webauth webauth-USER do dot11

Este comando ajuda a suprimir da sessão da autenticação da Web do usuário especificado.

Execute estes comandos debug a fim verificar o processo de autenticação do 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
```

Autenticação 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
```