Настройте SSIDs и VLAN на автономных AP

Содержание

Введение

Этот документ объясняет, как настроить автономные точки доступа (AP) для:

- Виртуальные локальные сети (VLAN)
- Открытая проверка подлинности
- 802.1x с внутренним Служба удаленной аутентификации пользователей коммутируемого доступа (RADIUS)
- 802.1x с внешним RADIUS
- Предварительный общий ключ (PSK)
- Аутентификация с использованием MAC-адреса
- Web-аутентификация (внутренний радиус)
- Веб-passthrough

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- 802.1x
- PSK
- RADIUS
- Web-аутентификация

Используемые компоненты

Сведения в этом документе основываются на версии 15.3 (3) AP 3700 JBB.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

> **Совет:** Эти примеры также применяются к AP в автономном режиме в ASA 5506, различие - то, что вместо настраивают порт коммутатора, где AP связан, конфигурация применена к Концерту ASA 1/9.

Настройка

> **Примечание:** Идентификаторы наборов сервисов (SSIDs), которые принадлежат той же VLAN, не могут быть применены к радио в то же время. Примеры конфигурации SSIDs с той же VLAN не были включены в то же время на том же AP.

Настройте коммутатор VLAN и AP

Настройте требуемые VLAN на обоих AP и коммутатор. Это VLAN, используемые в данном примере:

- VLAN 2401 (Собственный компонент)
- VLAN 2402
- VLAN 2403

Настройте AP и VLAN

Настройте интерфейсный гигабитный 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
```

Настройте интерфейсное радио 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
```

> **Примечание:** 802.11 миллиарда радио (интерфейсный dot11radio 0) не настроены, поскольку это использует собственный VLAN AP.

Настройте VLAN коммутатора

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

Настройте интерфейс, где связан AP:

```
# 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
```

Открытая аутентификация SSID - собственный VLAN AP

Этот SSID не имеет безопасности, он широковещательно передан (видимый клиентам) и беспроводные клиенты, который присоединяется, WLAN назначены на собственный VLAN.

Шаг 1. Настройте SSID.

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

Шаг 2. Назначьте SSID на 802.11b радио.

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

802.1x SSID - внутренний RADIUS

Этот SSID использует AP в качестве сервера RADIUS. Знайте, что AP как сервер RADIUS только поддерживает LEAP, EAP-FAST и проверку подлинности MAC.

Шаг 1. Включите AP как сервер RADIUS.

IP-адрес Сервера доступа к сети (NAS) является BVI AP, как этот IP-адрес является тем,

который передает запрос аутентификации к себе. Кроме того, создайте имя пользователя и пароль.

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

Шаг 2. Настройте сервер RADIUS, к которому AP передает запрос аутентификации, поскольку это - локальный RADIUS, IP-адрес является тем, назначенным на Мост интерфейс Vitrual (BVI) 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>
```

Шаг 3. Назначьте этот сервер RADIUS на группу радиуса.

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

Шаг 4. . Назначьте эту группу радиуса на метод аутентификации.

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

Шаг 5. . Создайте SSID, назначьте его на 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
```

Шаг 6. Назначьте ssid на интерфейс 802.11a и задайте режим шифра.

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

802.1x SSID - внешний RADIUS

Конфигурация является почти тем же как Внутренним RADIUS.

Шаг 1. Настройте **aaa new-model.**

Шаг 2, Вместо IP-адреса AP, использует внешний IP-адрес RADIUS.

SSID - PSK

Этот SSID использует WPA2/PSK безопасности, и пользователей на этом SSID назначают на VLAN 2402.

Шаг 1. Настройте 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
```

Шаг 2. Назначьте SSID на радиоинтерфейс и настройте режим шифра.

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

SSID - аутентификация с использованием MAC-адреса

Этот SSID аутентифицирует беспроводных клиентов на основе их MAC-адреса. Это использует MAC-адрес в качестве имени пользователя/пароля. В данном примере действия AP как локальный RADIUS, таким образом, AP хранит список MAC-адреса. Одинаковая конфигурация может быть применена с внешним сервером RADIUS.

Шаг 1. Включите AP как сервер RADIUS. IP-адрес NAS является BVI AP. Создайте запись для клиента с MAC-адресом aaaabbbbcccc.

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

Шаг 2. Настройте сервер RADIUS, к которому AP передает запрос аутентификации (это - сам 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>
```

Шаг 3. Назначьте этот сервер RADIUS на группу радиуса.

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

Шаг 4. . Назначьте эту группу радиуса на метод аутентификации.

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

Шаг 5. . Создайте SSID, данный пример назначает его на VLAN 2402.

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

Шаг 6. Назначьте SSID на интерфейс 802.11a.

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

SSID - внутренняя веб-аутентификация

Пользователи, которые соединяются с этим SSID , перенаправлены к порталу web-аутентификации для ввода допустимого имени пользователя / пароль, если аутентификация успешна, у них есть доступ к сети. В данном примере пользователи сохранены на локальном сервере RADIUS.

В данном примере SSID назначен на VLAN 2403.

Шаг 1. Включите AP как сервер RADIUS. IP-адрес NAS является BVI AP.

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

Шаг 2. Настройте сервер RADIUS, к которому AP передает запрос аутентификации (это - сам AP).

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

Шаг 3. Назначьте этот сервер RADIUS на группу радиуса.

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

Шаг 4. . Назначьте эту группу радиуса на метод аутентификации.

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

Шаг 5. . Создайте политику разрешения.

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

Шаг 6. Настройте SSID.

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

Шаг 7. Назначьте SSID на интерфейс.

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

Шаг 8. Назначьте политику на правильный подчиненный интерфейс.

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

> **Примечание:** Если SSID работает на собственный компонент, то политика применена непосредственно к интерфейсу, не к подчиненному интерфейсу (dot11radio 0 или dot11radio 1).

Шаг 9. Создайте имя пользователя/пароль для гостей.

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

SSID - веб-passthrough

Когда клиент соединится с SSID с веб-Транзитной конфигурацией, это будет перенаправлено к веб-порталу для принятия положений и условий использования сети, в противном случае пользователь не будет в состоянии использовать сервис.

Данный пример назначает SSID на собственный VLAN.

Шаг 1. Создайте политику разрешения.

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

Шаг 2. Задайте сообщение, которое будет отображено, когда клиенты соединятся с этим SSID.

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

Шаг 3. Создайте SSID.

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

Шаг 4. . Назначьте SSID и политику разрешения к радио

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

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Show dot11 associations

Это показывает мак адрес, IPv4 и адрес IPv6, имя SSID беспроводных клиентов соединилось.

```
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

Это показывает больше подробных данных беспроводного клиента, заданного в мак адресе как RSSI, SNR, поддерживаемые скорости передачи данных и другие.

```
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
```

показывают webauth-сеансы dot11

Если SSID настроен для web-аутентификации, это показывает мак адрес, адрес IPv4 для web-аутентификации или веб-passthrough и имени пользователя.

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

Show dot11 bssid

Это показывает BSSIDs, привязанный к WLAN на радиоинтерфейс.

```
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
```

Многословный show bridge

Это показывает отношение между подчиненными интерфейсами и мостовыми группами.

```
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
```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Clear dot11 client # aaa.bbbb.cccc

Эта команда помогает разъединять беспроводного клиента от сети.

очищают dot11 webauth webauth-имя-пользователя

Эта команда помогает удалять сеанс web-аутентификации указанного пользователя.

Выполните эти команды отладки для проверки процесса проверки подлинности клиента:

```
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
```

Аутентификация протокола управления доступом к среде передачи (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
```