Аутентификация eap на ACS 5.3 с точками доступа

Содержание

Введение

Этот документ описывает пример конфигурации Cisco IOS® программная точка доступа (AP) для аутентификации Протокола EAP пользователей беспроводной связи против базы данных, к которой обращается сервер RADIUS.

AP соединяет беспроводные пакеты от клиента в проводные пакеты, предназначенные к серверу проверки подлинности и наоборот. Поскольку AP играет эту пассивную роль в EAP, эта конфигурация используется с фактически всеми методами EAP. Эти методы включают, но не ограничены, Световой EAP (LEAP), Защищенный EAP (PEAP) - Протокол Квитирования с аутентификацией Microsoft (MSCHAP) версия 2, (GTC) Карта с переменым паролем Общего назначения PEAP, Гибкая аутентификация EAP через Безопасный, Туннелирующий (FAST), Transport Layer Security EAP (TLS), и Туннелированы EAP TLS (TTLS). Необходимо соответствующим образом настроить сервер аутентификации для каждого из методов EAP.

Этот документ описывает, как настроить AP и сервер RADIUS, который является сервером Cisco Secure Access Control Server (ACS) 5.3 в этом примере конфигурации.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знакомство с GUI программного обеспечения Cisco IOS или интерфейсом командной строки (CLI)
- Знакомство с понятиями Аутентификации eap

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Aironet 3602 точки доступа, которые выполняют Cisco IOS Software Release 15.2 (2) JB
- Сервер Cisco Secure Access Control Server 5.3

Этот пример конфигурации предполагает, что в сети существует только одна VLAN.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Этот документ использует эту конфигурацию и для GUI и для CLI:

- IP-адрес AP 10.105.136.11.
- IP-адрес сервера RADIUS (ACS) 10.106.55.91.

Конфигурация с GUI

Определите сервер проверки подлинности

Эта процедура описывает, как определить сервер проверки подлинности и установить отношение с ним.

1. В GUI AP перейдите к **Безопасности> Диспетчер серверов**.

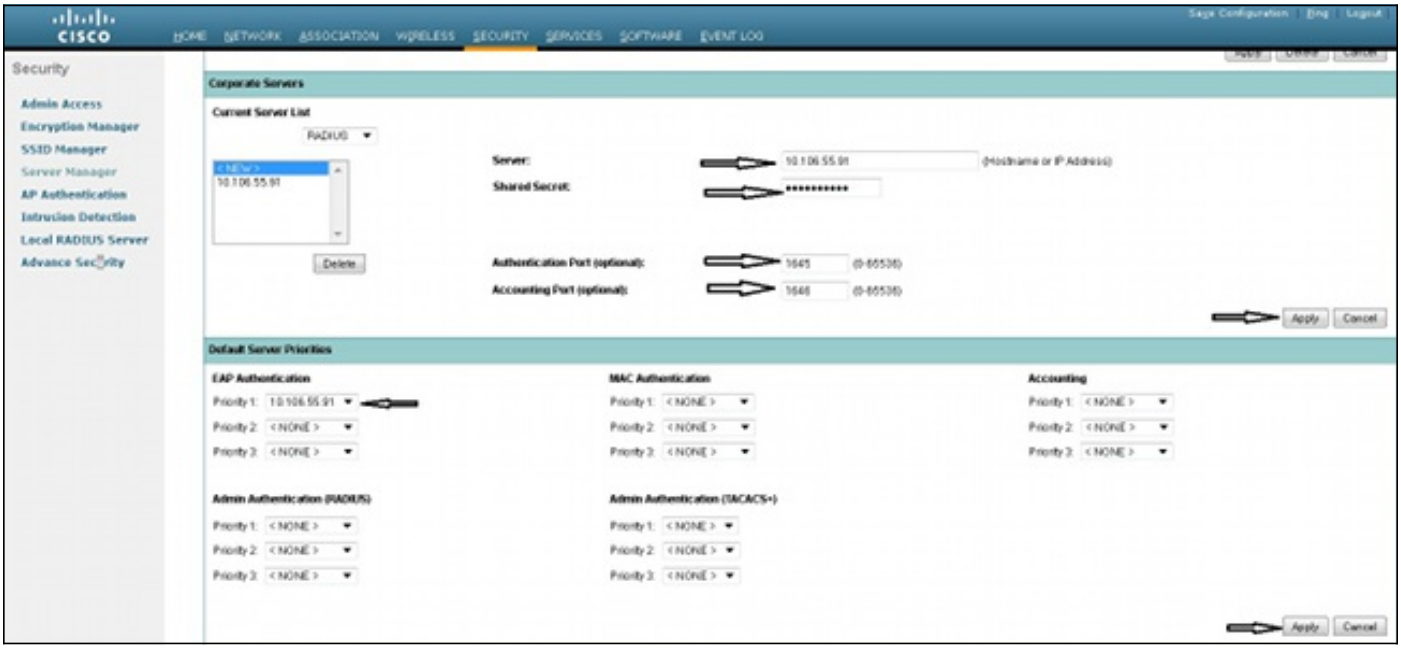
2. В разделе Корпоративных серверов введите IP-адрес сервера проверки подлинности **(10.106.55.91)** в поле Server.

3. Задайте Общий секретный ключ, Порт аутентификации и Порт учета. Можно использовать порты 1813, 1814 или 1645, 1646.

4. **Нажать Apply для того, чтобы создать определение и заполнить выпадающие списки.**

5. В разделе Приоритетов Сервера По умолчанию, набор поле EAP Authentication Priority 1 к IP-адресу сервера **(10.106.55.91)**.

6. **Щелкните "Применить".**

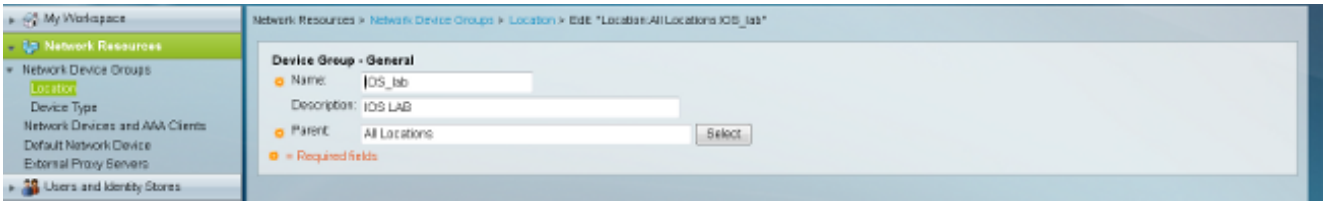


Настройте ACS

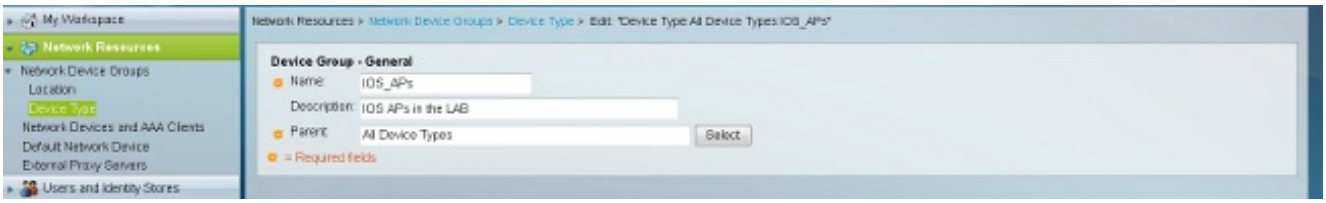
Если вы передаете пользователям к внешнему серверу RADIUS, AP должен быть клиентом аутентификации, авторизации и учета (AAA) для этого внешнего сервера RADIUS. Эта процедура описывает, как настроить ACS.

1. В GUI Cisco Secure ACS нажмите **Network Resources**. В ACS 5.3 устройства могут быть сгруппированы местоположениями.

2. Создайте местоположение. Под Группами сетевых устройств нажмите **Location**. Щелчок **создает новое местоположение**. В Поле имени введите имя местоположения **(IOS_lab)**. Введите описание (**LAB IOS**) для этого местоположения. Выберите общие сведения **Все Местоположения** как Родительское местоположение. Нажмите **Submit** для проверки.



3. Создайте группу для AP IOS. Нажмите **Device Type**. Нажмите **Create** для создания новой группы. В Поле имени введите имя группы **(IOS_APs)**. Введите описание (**AP IOS в LAB**) для этой группы. Выберите **All Device Types** как Родителя. Нажмите **Submit** для проверки.

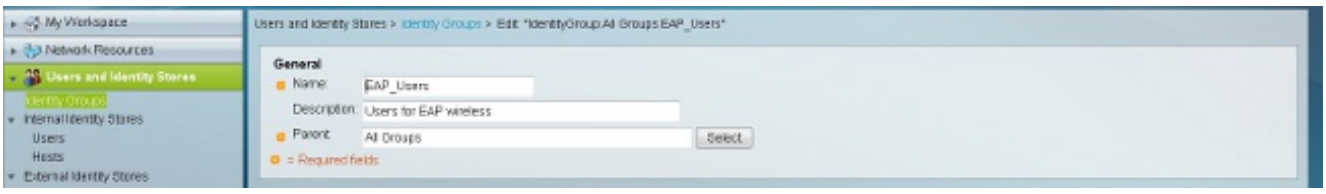


4. Добавьте AP. Нажмите **Network Devices и AAA Clients**. В Поле имени введите имя своего AP IOS **(AP)**. Введите описание для того AP (**AP IOS**).

   Под Группами сетевых устройств, рядом с полем Location, нажимают **Select**, устанавливают флажок рядом с IOS_lab и нажимают **OK** для проверки. Под IP-адресом быть уверенным включен Один IP-адрес, и введите IP-адрес своего AP **(10.105.136.11)**.

   Под Параметрами проверки подлинности проверьте **RADIUS**. В поле **Shared Secret** введите тайну **(Cisco)**. Поддержите другие значения к их настройкам по умолчанию. Нажмите **Submit** для проверки.

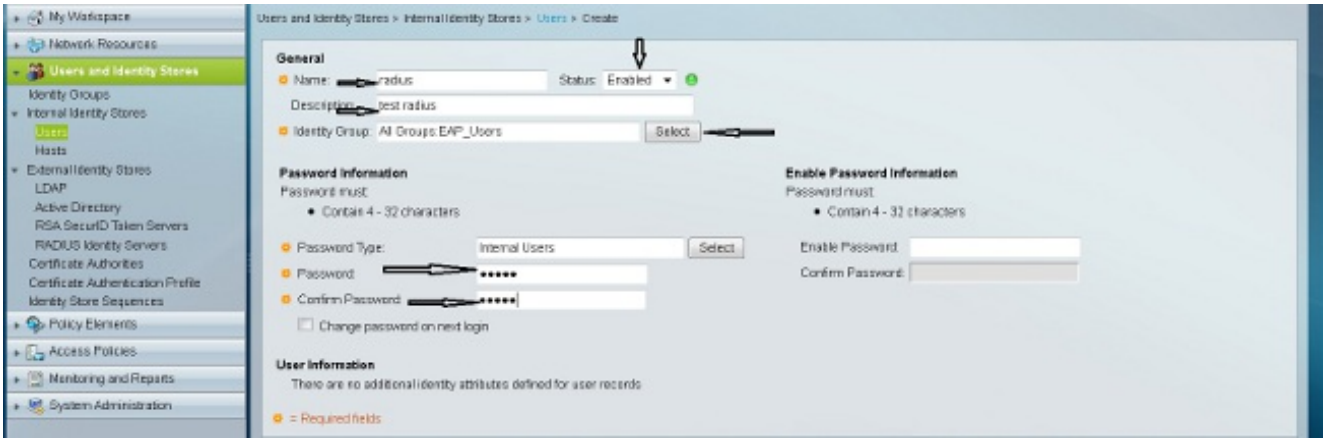
5. Добавьте учетные данные пользователя беспроводной связи. Перейдите **Пользователям и Идентификационным Хранилищам> Identity Groups**. Нажмите **Create** для создания новой группы. В Поле имени введите имя группы **(EAP_Users)**. Введите описание (**Пользователи для радио EAP**). Нажмите **Submit** для проверки.



6. Создайте пользователя в этой группе. Нажмите **Users**. Нажмите **Create** для создания нового пользователя. В Поле имени введите имя пользователя **(радиус)**. Гарантируйте,

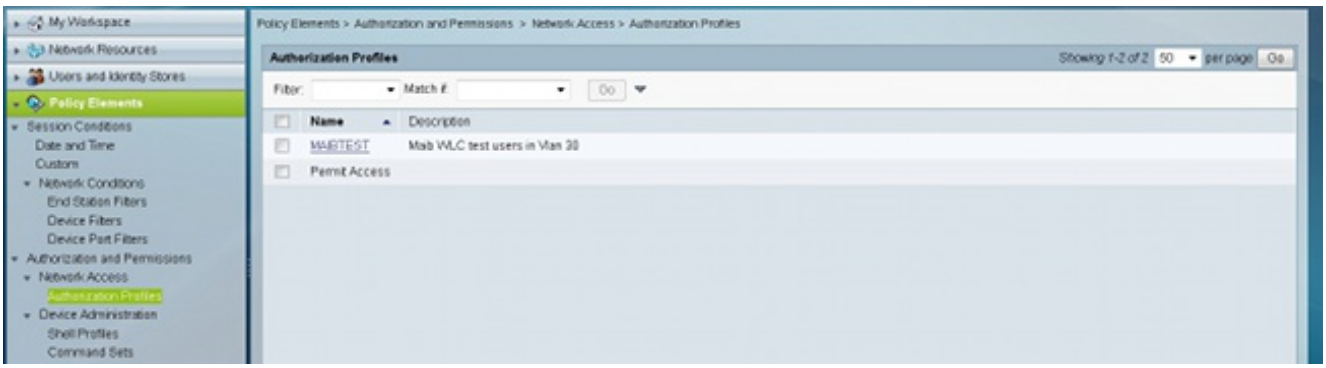
что **Включен** пользовательский Статус. Введите описание для пользователя (**тестовый радиус**). Рядом с полем Identity Group нажмите **Select**, установите флажок рядом с EAP_Users и нажмите **OK** для проверки.

Под Сведениями о пароле введите **<password>** в Пароль и поля подтверждения пароля. Поскольку этот пользователь должен обратиться к сети, но не должен обращаться к любому устройству Cisco для управления, нет никакой потребности в Enable Password.

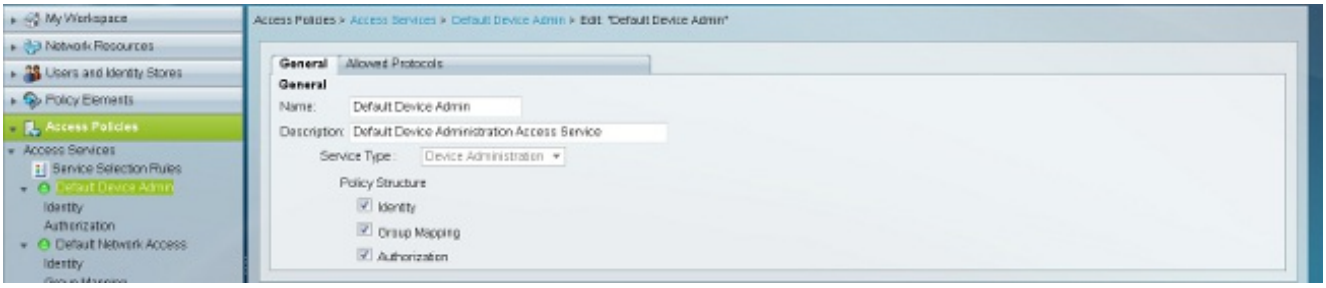


7. Нажмите **Submit** для проверки. Новый пользователь появляется в списке, и ACS теперь готов.

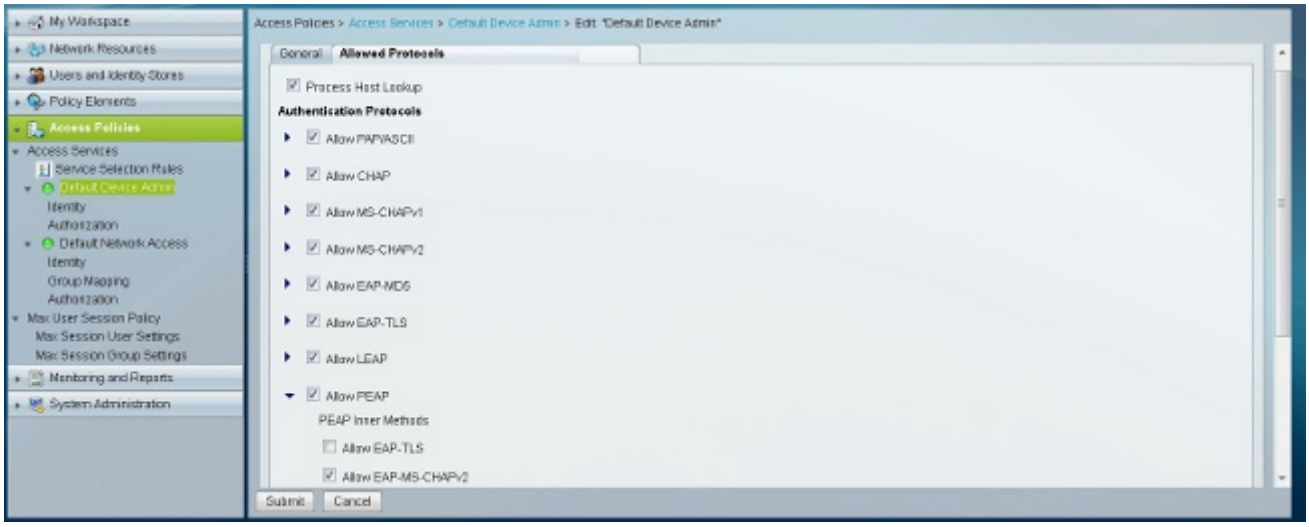
8. Перейдите к **Элементам Политики> Авторизация и Разрешения> Доступ к сети> Профили Авторизации**, чтобы проверить, что пользователю предоставляют разрешение доступа. Должен быть профиль PermitAccess. Пользователи, которые получают этот профиль, являются предоставленным доступом к сети.



9. Перейдите к **Политике доступа> Службы доступа> Администратор устройства по умолчанию** для исследования авторизации. Удостоверьтесь, что проверены **Идентичность**, **Сопоставление Группы** и **Авторизация**.



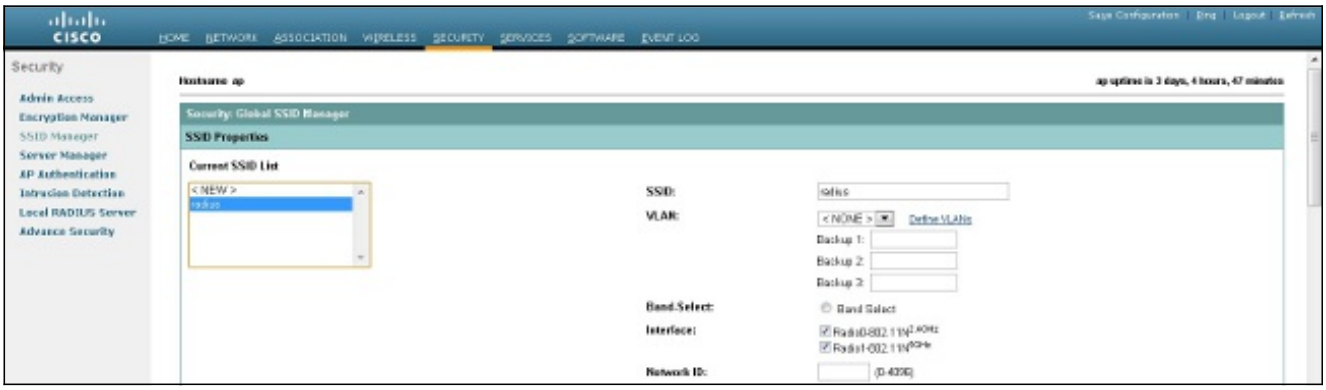
10. Нажмите вкладку **Allowed Protocols**, выберите коробки для требуемых методов EAP и нажмите **Submit** для проверки.



Настройте SSID

Эта процедура описывает, как настроить идентификатор набора сервисов (SSID) на AP.

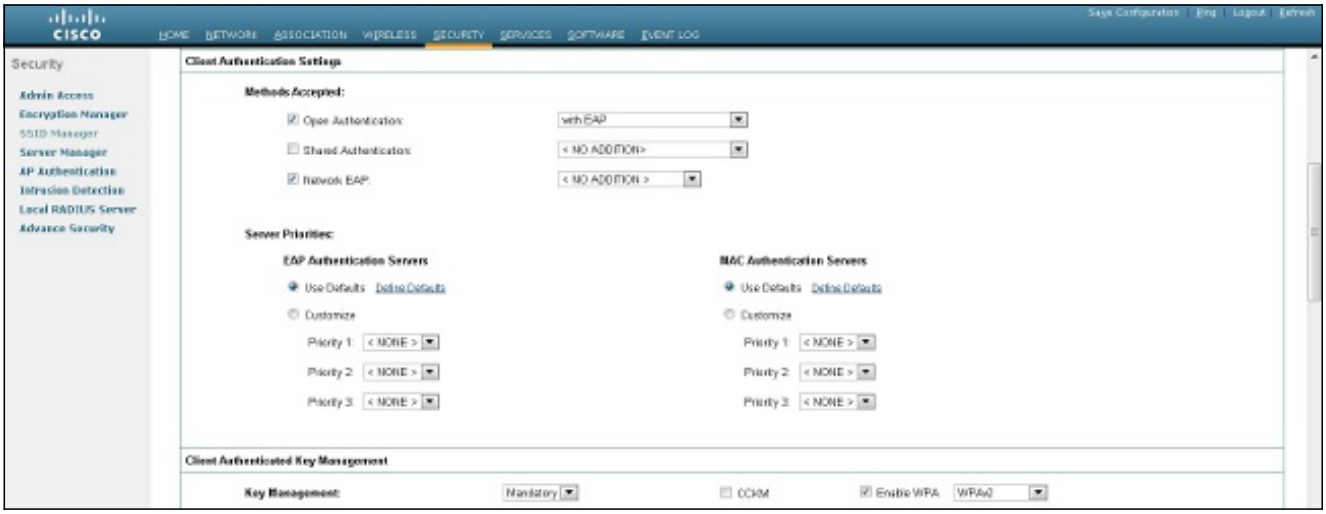
1. В GUI Cisco Secure ACS перейдите к **Безопасности> Диспетчер SSID**. Нажмите **New**, введите имя SSID **(радиус)**, включите оба радиоинтерфейса и нажмите **Apply**.



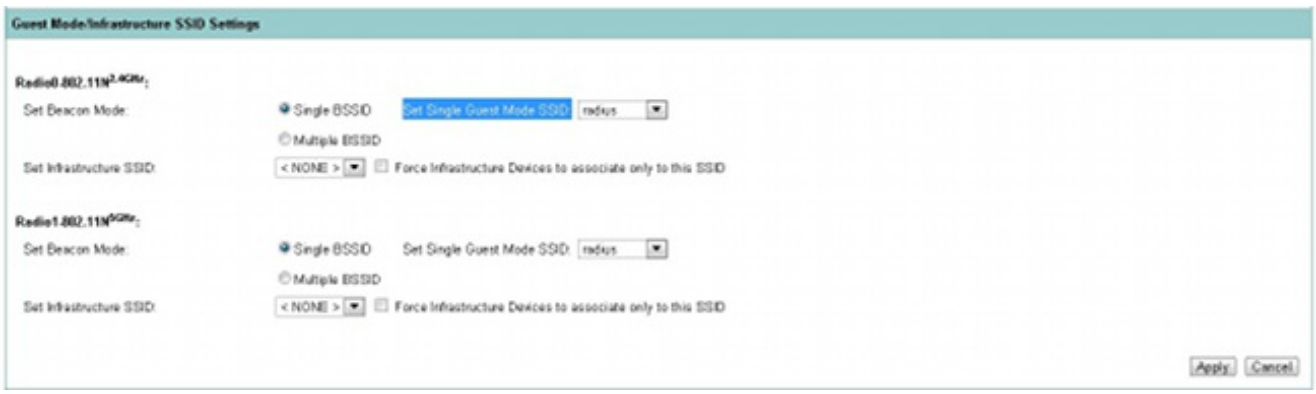
2. Перейдите к **Безопасности> Диспетчер шифрования**, выберите **AES CCMP** как Шифр и нажмите **Apply-All** для применения этого шифрования по обоим радио.

3. Перейдите к **Безопасности> Диспетчер SSID** и выберите SSID **радиуса**. В разделе Параметров настройки Аутентификации клиента проверьте **Открытую аутентификацию**, выберите **EAP** от выпадающего списка и **EAP Сети** проверки.

   В Клиентском Аутентифицируемом разделе Управления ключами выберите **Mandatory** от выпадающего списка Управления ключами, проверка **Включают WPA** и выбирают **WPAv2** от выпадающего списка. **Щелкните "Применить".**



4. Для широковещательной передачи этого SSID по обоим радио найдите Гостевой режим / разделом Параметров настройки SSID Инфраструктуры на той же странице. Для обоих радио, устанавливает Режим Маяка в **Одиночный BSSID**, и выбирать название SSID **(радиус)** от Набора Одиночный выпадающий список SSID Гостевого режима. **Щелкните "Применить".**



5. Перейдите к **Сети> Сетевой интерфейс> Radio0-802.11n 2G.Hz>, Параметры настройки> Включают** для включения обоих радиоинтерфейсов.

6. Протестируйте клиентское подключение.

Конфигурация с CLI

Примечания:

Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Это - одинаковая конфигурация, сделанная в CLI:

```
show run
Building configuration...

Current configuration : 2511 bytes
!
! Last configuration change at 01:17:48 UTC Mon Mar 1 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$1u04$jr7DG0DC5KZ6bVaSYUhck0
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.106.55.91
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
```

```
!
!
!
aaa session-id common
ip cef
!
ip dhcp pool test
!
!
!
dot11 syslog
!
dot11 ssid radius
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
 encryption mode ciphers aes-ccm
 !
 ssid radius
 !
 antenna gain 0
 stbc
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 !
 encryption mode ciphers aes-ccm
 !
 ssid radius
 !
 antenna gain 0
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
```

```
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address 10.105.136.11 255.255.255.128
!
ip default-gateway 10.105.136.1
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.105.136.1
ip radius source-interface BVI1
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.106.55.91 key 7 00271A1507545A545C606C
radius-server vsa send accounting
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
 transport input all
!
end
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Подключите клиента; после успешной аутентификации это - сводка конфигурации, которая появляется в GUI AP:

> **Примечание:** Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

В CLI введите **команду show dot11 associations** для подтверждения конфигурации:

```
ap#show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:

SSID [radius] :

MAC Address   IP address     Device       Name        Parent     State
f8db.7f75.7804 10.105.136.116 unknown      -           self       EAP-Assoc
```

Можно также ввести **show radius server-group вся** команда для отображения списка всех настроенных server-group RADIUS на AP.

Устранение неполадок

Эта процедура описывает, как устранить неполадки вашей конфигурации.

1. В клиентской утилите или программном обеспечении, создайте новый профиль или соединение с теми же или подобными параметрами, чтобы гарантировать, что ничто не стало поврежденным в конфигурации клиента.

2. Проблемы радиочастот (RF) могут предотвратить успешную аутентификацию. Временно отключите аутентификацию для устранения этой возможности:

   От CLI введите эти команды:

   никакой eap authentication open eap_methodsникакой authentication network-eap eap_methodsauthentication open

   От GUI, на странице SSID Manager, **Network-EAP** снятия, **Открытая** проверка, и устанавливают выпадающий список ни в **Какое Добавление**.

   Если клиент будет успешно сопоставлен, то радиочастота не вызовет проблем сопоставления.

3. Проверьте, что общие секретные пароли синхронизируются между AP и сервером проверки подлинности. В противном случае вы могли бы получить это сообщение об ошибках:

   `Invalid message authenticator in EAP request`От CLI проверьте линию:

   `radius-server host x.x.x.x auth-port x acct-port x key` **<shared_secret>**От GUI, на странице Server Manager, повторно вводят общий секретный ключ для соответствующего сервера в поле Shared Secret.

   Запись общего секретного ключа для AP на сервере RADIUS должна содержать тот же общий секретный пароль.

4. Удалите все группы пользователей с сервера RADIUS. Конфликты могут произойти между группами пользователей, определенными сервером RADIUS и группами пользователей в базовом домене. Проверьте журналы сервера RADIUS для неудачных попыток и по причинам для сбоев.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Используйте эти команды отладки, чтобы исследовать и отобразить согласования среди устройств:

- конечный автомат средства проверки подлинности debug dot11 aaa
- debug radius authentication
- debug aaa authentication

конечный автомат средства проверки подлинности debug dot11 aaa

Эта команда отображает крупнейшие подразделения (или состояния) согласования между клиентом и сервером проверки подлинности. Это - пример вывода от успешной аутентификации:

```
ap#debug dot11 aaa authenticator state-machine
state machine debugging is on
ap#
*Mar 1 01:38:34.919: dot11_auth_dot1x_send_id_req_to_client: Sending identity
request to f8db.7f75.7804
*Mar 1 01:38:34.919: dot11_auth_dot1x_send_id_req_to_client: Client
f8db.7f75.7804 timer started for 30 seconds
*Mar 1 01:38:35.431: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.431: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar 1 01:38:35.431: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar 1 01:38:35.435: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.435: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:35.435: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar 1 01:38:35.443: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.443: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar 1 01:38:35.443: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar 1 01:38:35.447: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.447: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:35.447: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
------------------Lines Omitted for simplicity------------------
*Mar 1 01:38:36.663: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar 1 01:38:36.663: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:36.663: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar 1 01:38:36.667: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:36.667: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar 1 01:38:36.667: dot11_auth_dot1x_send_response_to_server: Started timer
```

```
server_timeout 60 seconds
*Mar 1 01:38:36.671: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_PASS) for f8db.7f75.7804
*Mar 1 01:38:36.671: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:36.671: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar 1 01:38:36.719: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]
```

debug radius authentication

Эта команда отображает Согласования RADIUS между сервером и клиентом, оба из которых соединены AP. Это - пример вывода от успешной аутентификации:

```
ap#debug radius authentication

*Mar 1 01:50:50.635: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: ssid [347] 6
*Mar 1 01:50:50.635: RADIUS:  72 61 64 69 [ radi]
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: service-type [345] 4 1
*Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: interface [222] 3
*Mar 1 01:50:50.635: RADIUS:  32 [ 2]
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IPv6:
*Mar  1 01:50:50.635: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.635: RADIUS(000001F6): sending
*Mar 1 01:50:50.635: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
id 1645/73, len 140
*Mar 1 01:50:50.635: RADIUS: authenticator 0F 74 18 0E F3 08 ED 51 -
8B EA F7 31 AC C9 CA 6B
*Mar 1 01:50:50.635: RADIUS: User-Name  [1]  8  "radius"
*Mar 1 01:50:50.635: RADIUS: Framed-MTU [12] 6  1400
*Mar 1 01:50:50.635: RADIUS: Called-Station-Id  [30] 26 "1C-E6-C7-E1-D8-90:
radius"
*Mar 1 01:50:50.635: RADIUS: Calling-Station-Id [31] 16 "f8db.7f75.7804"
*Mar 1 01:50:50.635: RADIUS: Service-Type [6]  6  Login  [1]
*Mar 1 01:50:50.635: RADIUS: Message-Authenticato[80]  18
*Mar 1 01:50:50.635: RADIUS:  E3 E1 50 F8 2B 22 26 84 C1 F1 76 28 79 70 5F 78
[ P+"&v(yp_x]
*Mar 1 01:50:50.635: RADIUS: EAP-Message [79] 13
*Mar 1 01:50:50.635: RADIUS:  02 01 00 0B 01 72 61 64 69 75 73
[ radius]
*Mar 1 01:50:50.635: RADIUS: NAS-Port-Type      [61] 6  802.11 wireless
[19]
*Mar 1 01:50:50.635: RADIUS: NAS-Port  [5]  6  282
*Mar 1 01:50:50.635: RADIUS: NAS-Port-Id  [87] 5  "282"
*Mar 1 01:50:50.635: RADIUS: NAS-IP-Address [4]  6  10.105.136.11
*Mar 1 01:50:50.635: RADIUS: Nas-Identifier  [32] 4  "ap"
*Mar 1 01:50:50.635: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:50.635: RADIUS(000001F6): Started 5 sec timeout
*Mar 1 01:50:50.639: RADIUS: Received from id 1645/73 10.106.55.91:1645, Access
-Challenge, len 94
*Mar 1 01:50:50.639: RADIUS: authenticator 5E A4 A7 B9 01 CC F4 20 -
2E D0 2A 1A A4 58 05 9E
*Mar 1 01:50:50.639: RADIUS: State              [24] 32
*Mar 1 01:50:50.639: RADIUS:  32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.639: RADIUS:  31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B   [ 1
/165489511/9;]
*Mar 1 01:50:50.639: RADIUS: EAP-Message        [79] 24
```

```
*Mar 1 01:50:50.639: RADIUS:  01 DC 00 16 11 01 00 08 00 CB 2A 0A 74 B3 77 AF
72 61 64 69 75 73        [ *twradius]
*Mar 1 01:50:50.639: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.643: RADIUS:  CC 44 D5 FE FC 86 BC 2D B0 89 61 69 4F 34 D1 FF
[ D-aiO4]
*Mar 1 01:50:50.643: RADIUS(000001F6): Received from id 1645/73
*Mar 1 01:50:50.643: RADIUS/DECODE: EAP-Message fragments, 22, total 22 bytes
*Mar  1 01:50:50.647: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: ssid             [347] 6
*Mar 1 01:50:50.647: RADIUS:  72 61 64 69             [ radi]
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: service-type     [345] 4
1
*Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: interface        [222] 3
*Mar 1 01:50:50.647: RADIUS:  32                [ 2]
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IPv6:
*Mar 1 01:50:50.647: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar 1 01:50:50.647: RADIUS(000001F6): sending
*Mar 1 01:50:50.647: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
 id 1645/74, len 167
*Mar 1 01:50:50.647: RADIUS: authenticator C6 54 54 B8 58 7E ED 60 - F8 E0 2E
05 B0 87 3B 76
*Mar 1 01:50:50.647: RADIUS: User-Name          [1]  8  "radius"
*Mar 1 01:50:50.647: RADIUS: Framed-MTU         [12] 6  1400
*Mar 1 01:50:50.647: RADIUS: Called-Station-Id  [30] 26 "1C-E6-C7-E1-D8-90:
radius"
*Mar 1 01:50:50.647: RADIUS: Calling-Station-Id [31] 16 "f8db.7f75.7804"
*Mar 1 01:50:50.647: RADIUS: Service-Type       [6]  6  Login
[1]
*Mar 1 01:50:50.647: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.647: RADIUS:  FE 15 7B DB 49 FE 27 C5 BC E2 FE 83 B9 25 8C 1F
[ {I'?]
*Mar 1 01:50:50.647: RADIUS: EAP-Message        [79] 8
*Mar 1 01:50:50.647: RADIUS:  02 DC 00 06 03 19
*Mar 1 01:50:50.647: RADIUS: NAS-Port-Type      [61] 6  802.11 wireless
[19]
*Mar 1 01:50:50.647: RADIUS: NAS-Port           [5]  6  282
*Mar 1 01:50:50.647: RADIUS: NAS-Port-Id        [87] 5  "282"
*Mar 1 01:50:50.647: RADIUS: State              [24] 32
*Mar 1 01:50:50.647: RADIUS:  32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.647: RADIUS:  31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B   [ 1
/165489511/9;]
*Mar 1 01:50:50.647: RADIUS: NAS-IP-Address     [4]  6  10.105.136.11
*Mar 1 01:50:50.647: RADIUS: Nas-Identifier     [32] 4  "ap"
*Mar 1 01:50:50.647: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:50.647: RADIUS(000001F6): Started 5 sec timeout
*Mar 1 01:50:50.647: RADIUS: Received from id 1645/74 10.106.55.91:1645, Access
-Challenge, len 78
*Mar 1 01:50:50.647: RADIUS: authenticator 0E 81 99 9E EE 39 50 FB - 6E 6D 93
8C 8E 29 94 EC
*Mar 1 01:50:50.647: RADIUS: State              [24] 32
*Mar 1 01:50:50.651: RADIUS:  32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:50.651: RADIUS:  31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B   [ 1
/165489511/9;]
*Mar 1 01:50:50.651: RADIUS: EAP-Message        [79] 8
*Mar 1 01:50:50.651: RADIUS:  01 DD 00 06 19 21               [ !]
*Mar 1 01:50:50.651: RADIUS: Message-Authenticato[80] 18
*Mar 1 01:50:50.651: RADIUS:  A8 54 00 89 1F 2A 01 52 FE FA D2 58 2F E5 F2 86
[ T*RX/]
*Mar 1 01:50:50.651: RADIUS(000001F6): Received from id 1645/74
*Mar 1 01:50:50.651: RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
```

```
*Mar 1 01:50:50.655: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: ssid             [347] 6
*Mar 1 01:50:50.655: RADIUS:  72 61 64 69             [ radi]
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: service-type     [345] 4
1
*Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: interface        [222] 3

------------------Lines Omitted for simplicity------------------

11       [ l2^w$qM{60]
*Mar 1 01:50:51.115: RADIUS: NAS-Port-Type      [61] 6  802.11 wireless
[19]
*Mar 1 01:50:51.115: RADIUS: NAS-Port           [5]  6  282
*Mar 1 01:50:51.115: RADIUS: NAS-Port-Id        [87] 5   "282"
*Mar 1 01:50:51.115: RADIUS: State              [24] 32
*Mar 1 01:50:51.115: RADIUS:  32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar 1 01:50:51.115: RADIUS:  31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B   [ 1
/165489511/9;]
*Mar 1 01:50:51.115: RADIUS: NAS-IP-Address     [4]  6  10.105.136.11
*Mar 1 01:50:51.115: RADIUS: Nas-Identifier     [32] 4  "ap"
*Mar 1 01:50:51.115: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar 1 01:50:51.115: RADIUS(000001F6): Started 5 sec timeout
*Mar 1 01:50:51.115: RADIUS: Received from id 1645/80 10.106.55.91:1645, Access
-Challenge, len 115
*Mar 1 01:50:51.115: RADIUS: authenticator 74 CF 0F 34 1F 1B C1 CF -
E9 27 79 D5 F8 9C 5C 50
*Mar 1 01:50:51.467: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]
```

debug aaa authentication

Эта команда отображает согласования AAA для аутентификации между устройством клиента и сервером проверки подлинности.

```
ap#debug aaa authentication
AAA Authentication debugging is on
ap#term mon
ap#
*Mar 1 01:55:52.335: AAA/BIND(000001F9): Bind i/f
*Mar 1 01:55:52.859: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:52.867: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:52.875: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:52.895: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.219: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.379: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.395: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.807: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.879: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.939: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]
```