Установившийся доступ 5760, 3850, и EAP-FAST WLC серии 3650 с примером конфигурации внутреннего сервера RADIUS

ID документа: 117664

Обновлено : 18 апреля 2014

Внесенный BG Surendra, специалистом службы технической поддержки Cisco.

Родственные продукты

- Wireless, LAN (WLAN)

Содержание

Введение

Этот документ описывает, как настроить Cisco Сходившийся Доступ 5760, 3850, и Контроллеры беспроводной локальной сети серии 3650 (WLC) для действия как серверы RADIUS, которые выполняют Гибкую аутентификацию для расширяемого протокола аутентификации Cisco с помощью Защищенного протокола (EAP-FAST в данном примере)

для аутентификации клиента.

Обычно внешний сервер RADIUS используется для аутентификации пользователей, который не является Осуществимым решением в некоторых случаях. В этих ситуациях Установившийся WLC Доступа может действовать как сервер RADIUS, где пользователи аутентифицируются против локальной базы данных, которая настроена в WLC. Это называют функцией Локального сервера RADIUS.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с темами в данном документе перед началом конфигурации:

- GUI Cisco IOS® или CLI с установившимся доступом 5760, 3850, и WLC серии 3650
- Понятия Протокола EAP
- Конфигурация Идентификаторов наборов сервисов (SSID)
- RADIUS

Используемые компоненты

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

- Cisco выпуск 3.3.2 WLC серии 5760 (Коммутационный шкаф следующего поколения [NGWC])
- Cisco облегченная точка доступа серии 3602 (AP)
- Microsoft Windows XP с Intel соискатель PROset
- Cisco Catalyst 3560 Series Switches

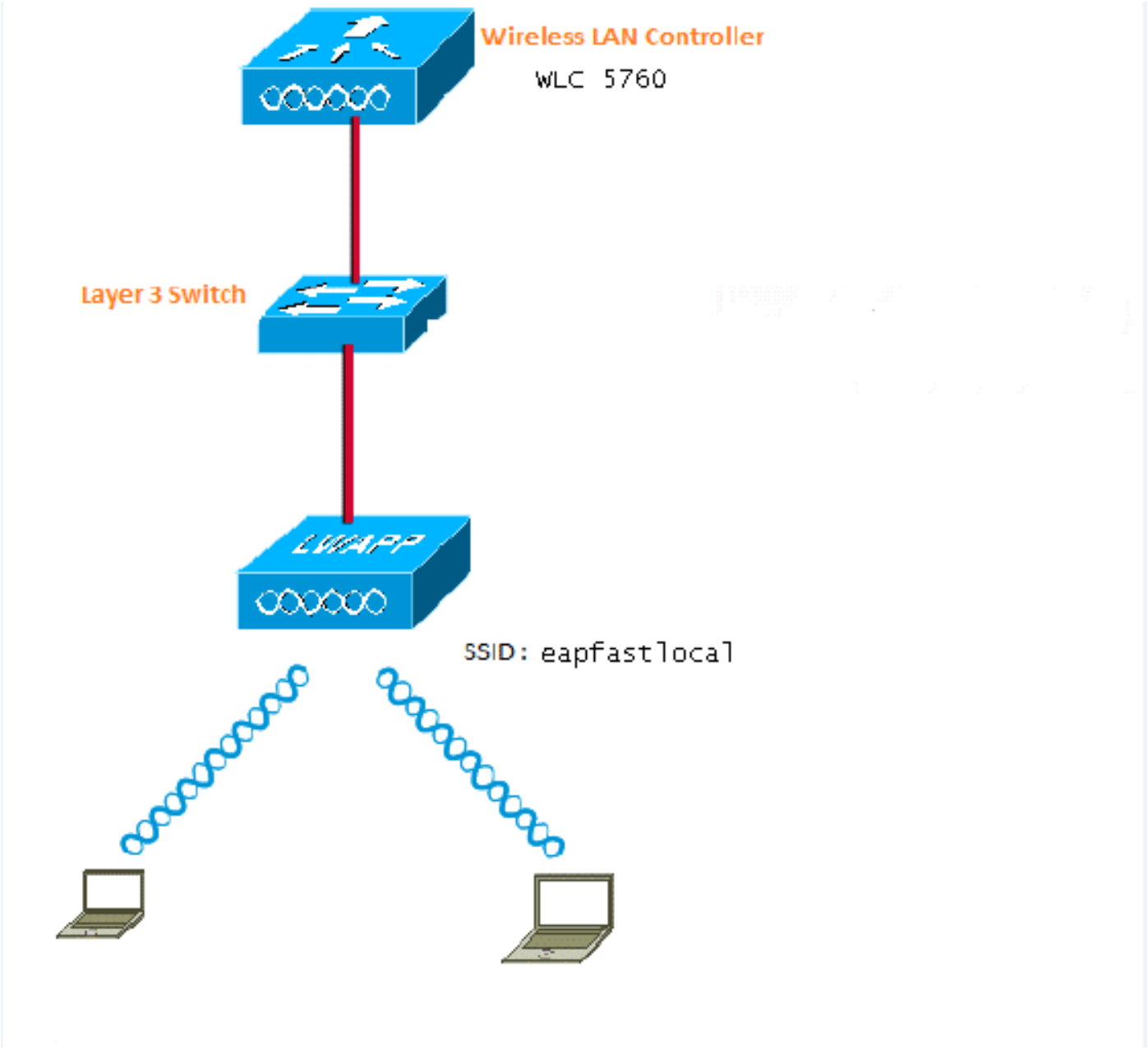
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

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

Схема сети

Этот образ предоставляет пример схемы сети:



Обзор конфигурации

Эта конфигурация завершена в двух шагах:

1. Настройте WLC для локального метода EAP и связанных профилей проверки подлинности и авторизация с CLI или GUI.

2. Настройте WLAN и сопоставьте список методов, который имеет профили проверки подлинности и авторизация.

Настройте WLC с CLI

Выполните эти шаги для настройки WLC с CLI:

1. Включите модель AAA на WLC:

```
aaa new-model
```

2. Определите проверку подлинности и авторизация:

```
aaa local authentication eapfast authorization eapfast

aaa authentication dot1x eapfast local
aaa authorization credential-download eapfast local
aaa authentication dot1x default local
```

3. Настройте локального EAP profile, и метод (EAP-FAST используется в данном примере):

```
eap profile eapfast
 method fast
!
```

4. Настройте усовершенствованные параметры EAP-FAST:

```
eap method fast profile eapfast
 description test
 authority-id identity 1
 authority-id information 1
 local-key 0 cisco123
```

5. Настройте WLAN и сопоставьте профиль локальной проверки подлинности с WLAN:

```
wlan eapfastlocal 13 eapfastlocal
 client vlan VLAN0020
 local-auth eapfast
 session-timeout 1800
 no shutdown
```

6. Настройте инфраструктуру для поддержки клиентского подключения:

```
ip dhcp snooping vlan 12,20,30,40,50
ip dhcp snooping
!
ip dhcp pool vlan20
 network 20.20.20.0 255.255.255.0
 default-router 20.20.20.251
 dns-server 20.20.20.251
interface TenGigabitEthernet1/0/1
 switchport trunk native vlan 12
 switchport mode trunk
 ip dhcp relay information trusted
 ip dhcp snooping trust
```

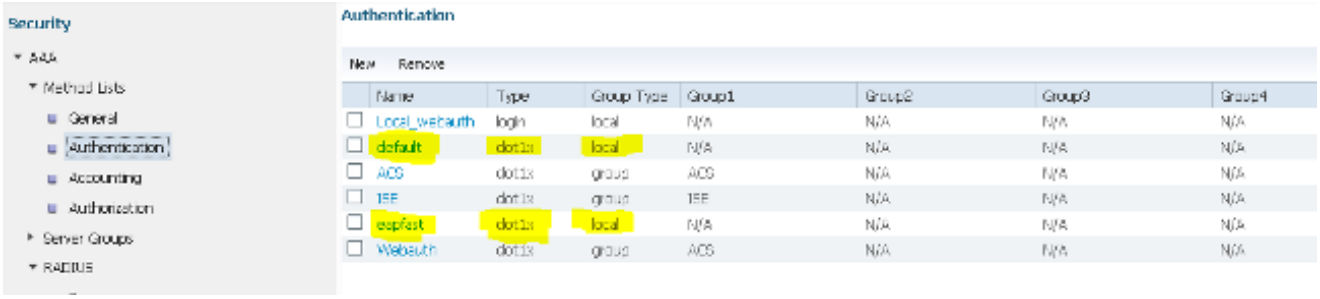
Настройте WLC с GUI

Выполните эти шаги для настройки WLC с GUI:

1. Настройте список методов для Аутентификации:

   Настройте Тип **eapfast** как **Dot1x**.

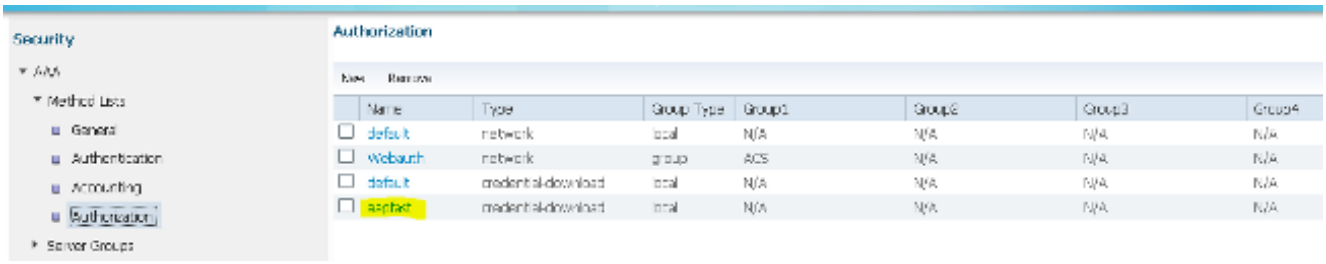
   Настройте **eapfast** Тип группы как **Локальный**.



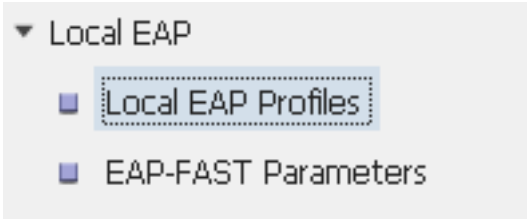
2. Настройте список методов для Авторизации:

   Настройте Тип **eapfast** как **Учетную Загрузку**.

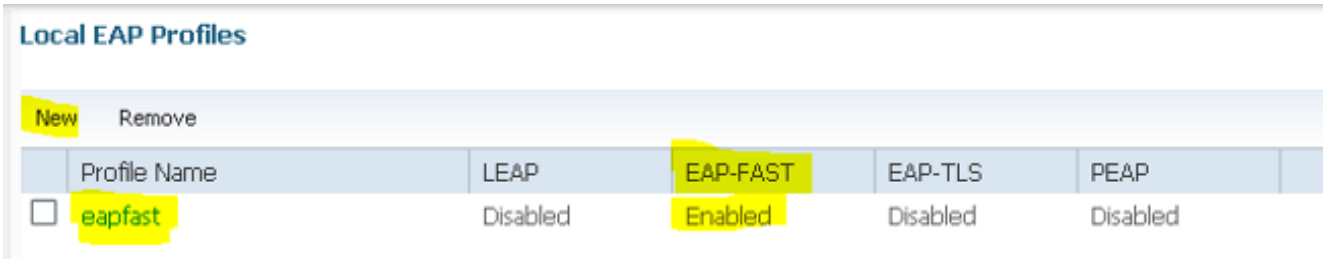
   Настройте **eapfast** Тип группы как **Локальный**.



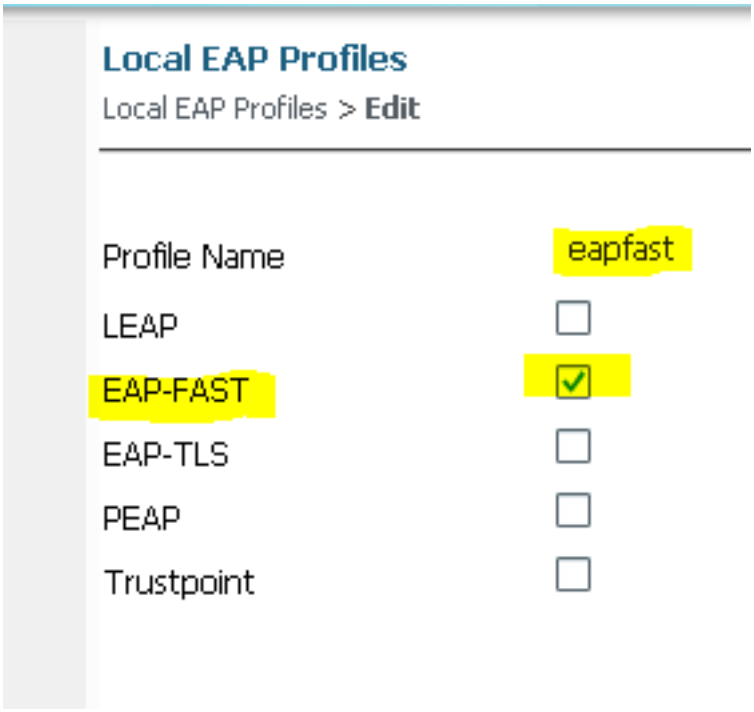
3. Настройте Локального EAP profile:



4. Создайте новый профиль и выберите тип EAP:

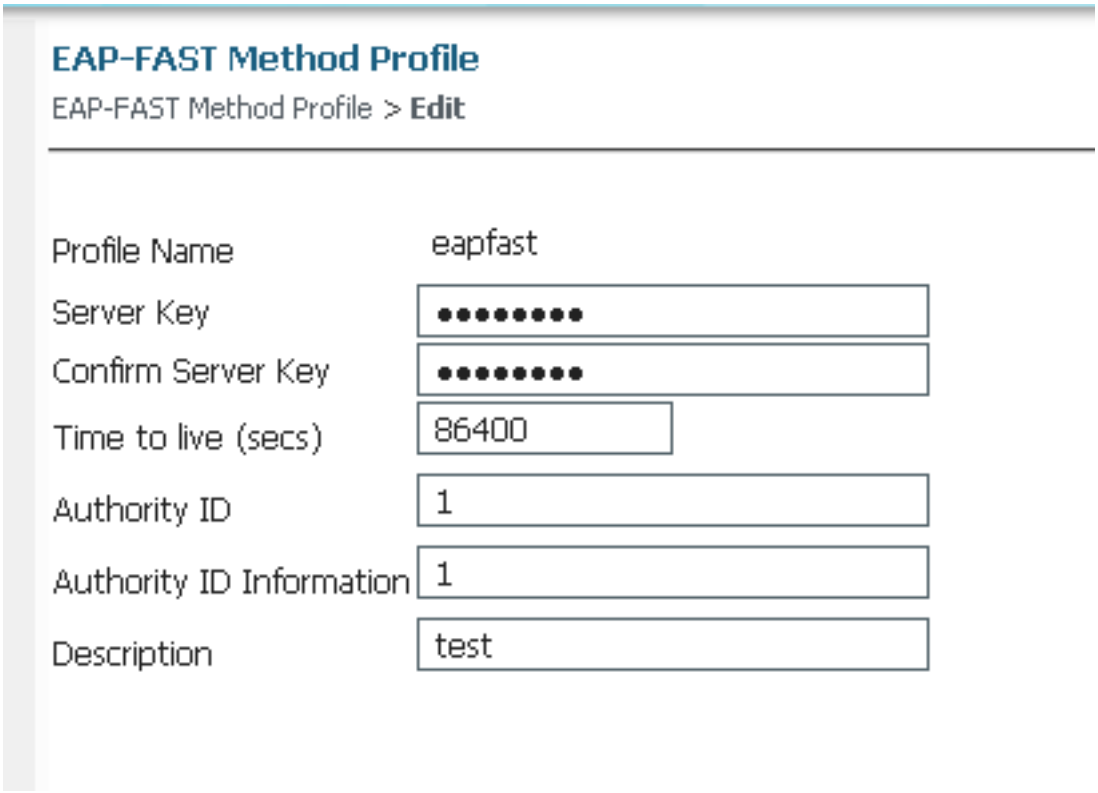


   Имя профиля является **eapfast**, и выбранный тип EAP является **EAP-FAST**:

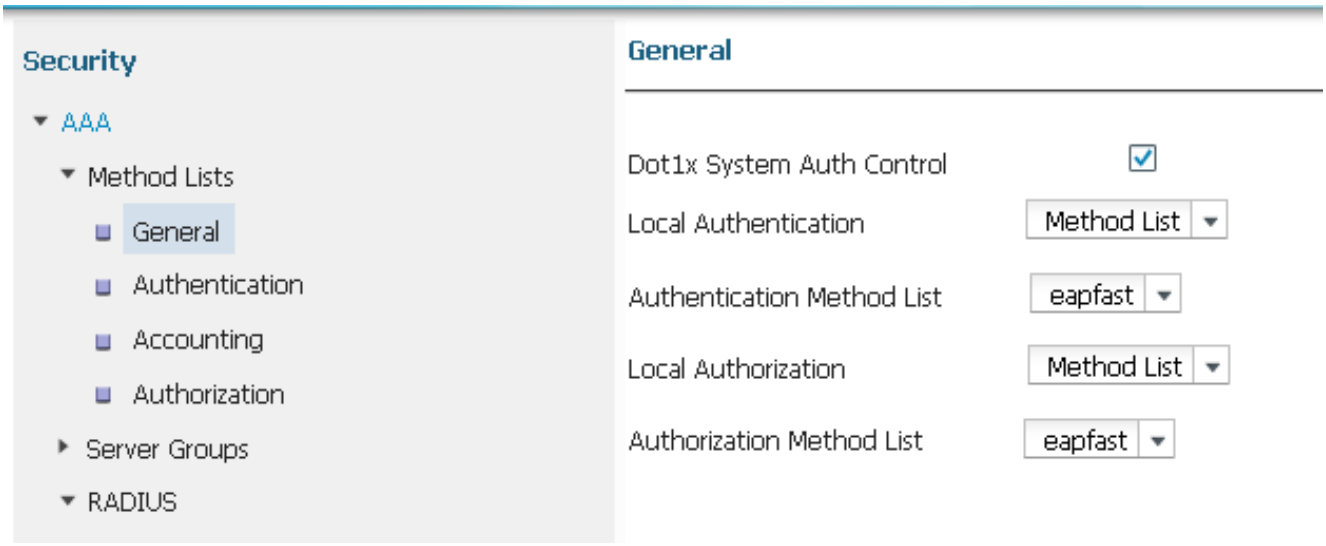


5. Настройте параметры метода EAP-FAST:

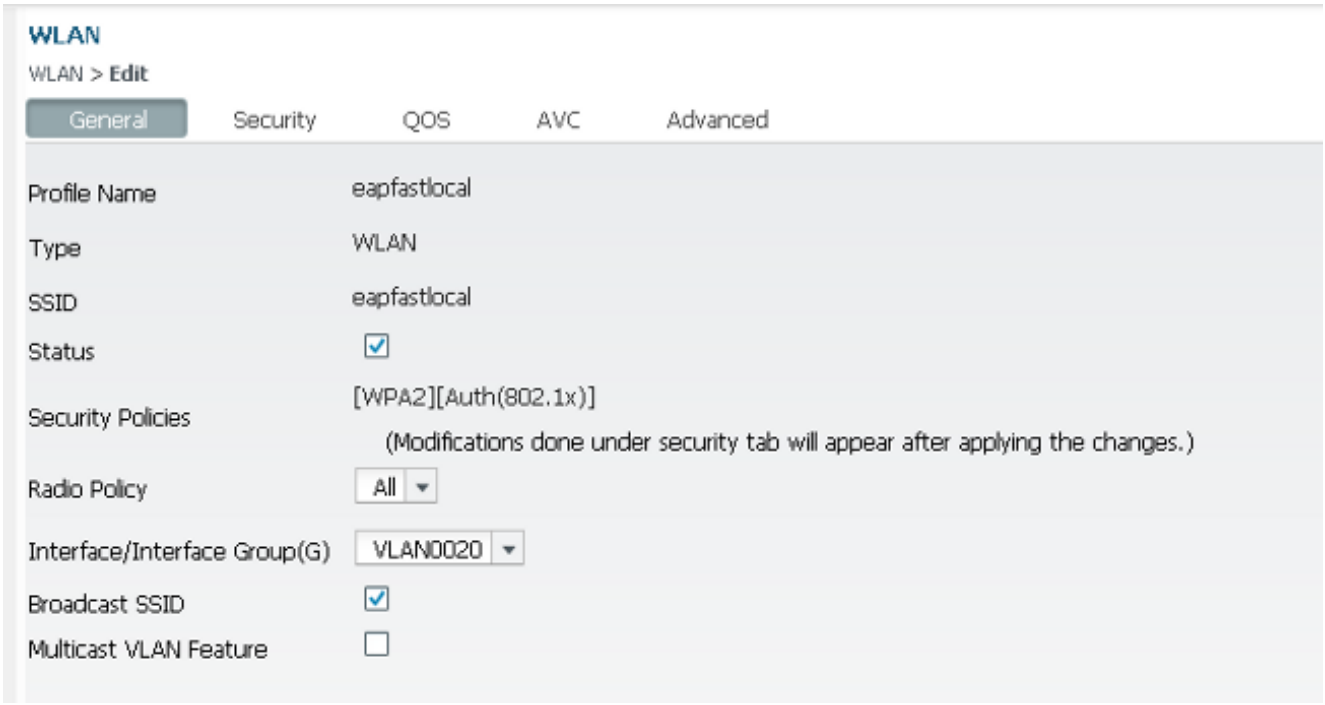
Серверный ключ настроен как **Cisco123**.

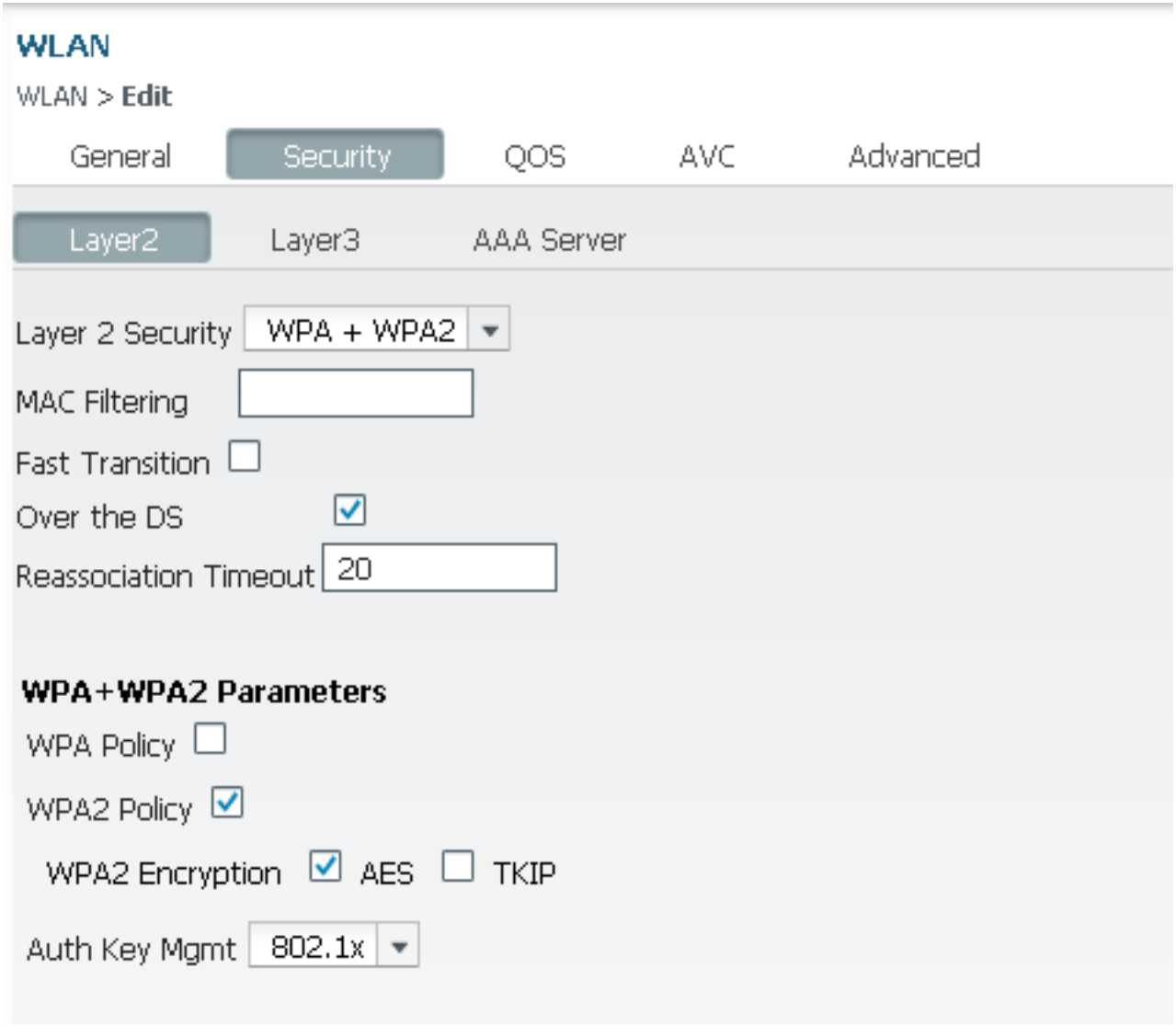


6. Проверьте флажок **Dot1x System Auth Control** и выберите **eapfast** для Списков методов. Это помогает вам выполнять локальную EAP-аутентификацию.

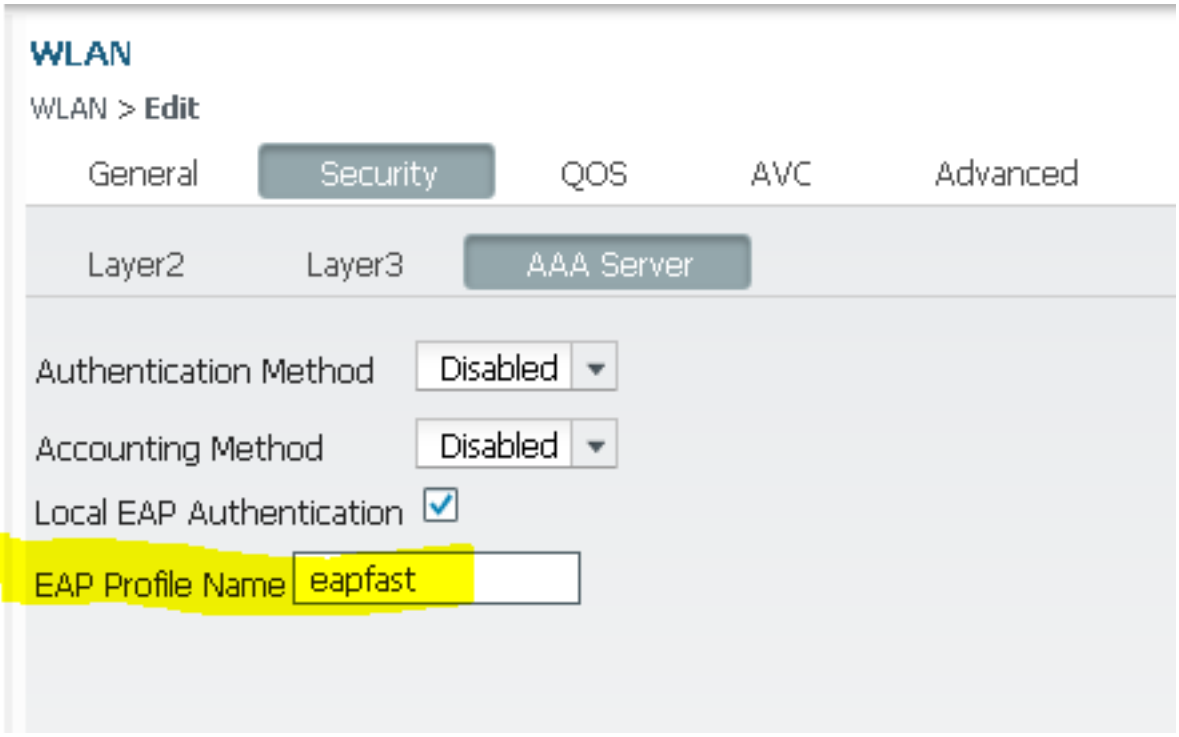


7. Настройте WLAN для шифрования AES WPA2:





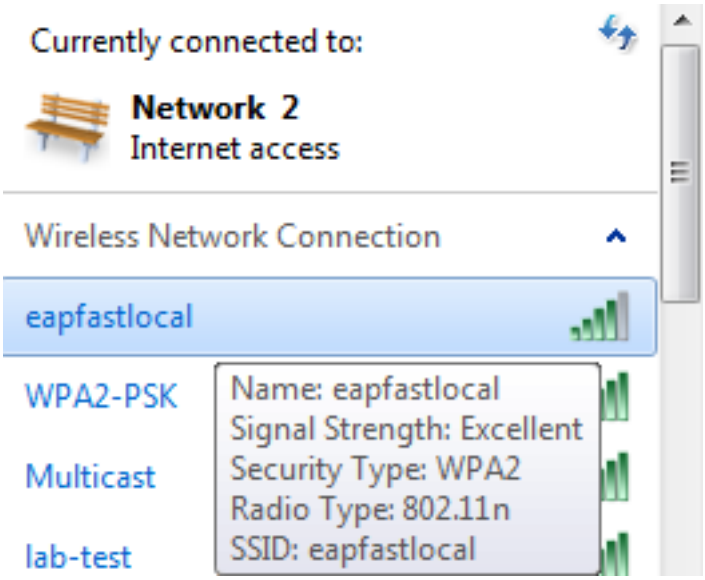
8. На вкладке **AAA Server** сопоставьте Название EAP Profile **eapfast** с WLAN:



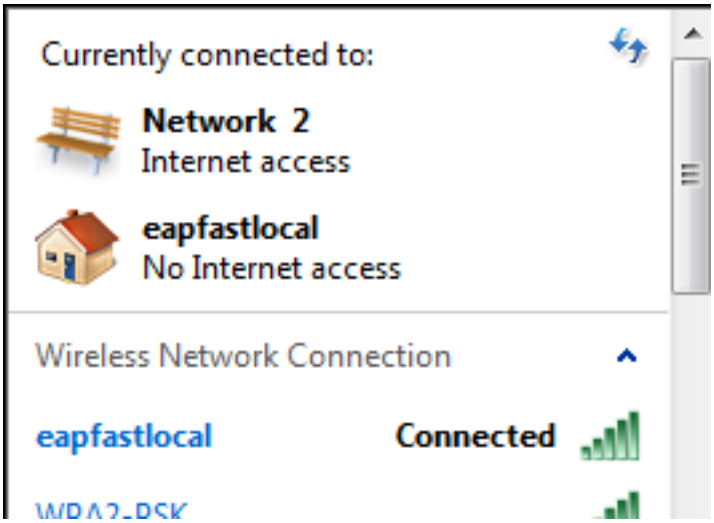
Проверка

Выполните эти шаги, чтобы проверить, что ваша конфигурация работает должным образом:

1. Подключите клиента с WLAN:



2. Проверьте, что всплывающее окно учетных данных для защищенного доступа (PAC) появляется и что необходимо принять для успешной аутентификации:



Устранение неполадок

Cisco рекомендует использовать трассировки для решения беспроводных проблем. Трассировки сохранены в кольцевом буфере и не являются сом интенсивной загрузкой процессора.

Разрешите эти трассировки для получения Уровня 2 (L2) подлинные журналы:

- **set trace group-wireless-secure отладка уровня**
- **set trace group-wireless-secure фильтрует mac0021.6a89.51ca**

Разрешите эти трассировки для получения журналов событий DHCP:

- **отладка уровня событий dhcp set trace**
- **события dhcp set trace фильтруют mac 0021.6a89.51ca**

Вот некоторые примеры успешных трассировок:

```
[04/10/14 18:49:50.719 IST 3 8116] 0021.6a89.51ca Association received from
 mobile on AP c8f9.f983.4260

[04/10/14 18:49:50.719 IST 4 8116] 0021.6a89.51ca qos upstream policy is
 unknown and downstream policy is unknown
[04/10/14 18:49:50.719 IST 5 8116] 0021.6a89.51ca apChanged 1 wlanChanged 0
 mscb ipAddr 20.20.20.6, apf RadiusOverride 0x0, numIPv6Addr=0
[04/10/14 18:49:50.719 IST 6 8116] 0021.6a89.51ca Applying WLAN policy on MSCB.
[04/10/14 18:49:50.719 IST 7 8116] 0021.6a89.51ca Applying WLAN ACL policies
 to client

[04/10/14 18:49:50.719 IST 9 8116] 0021.6a89.51ca Applying site-specific IPv6
 override for station 0021.6a89.51ca - vapId 13, site 'default-group',
 interface 'VLAN0020'
[04/10/14 18:49:50.719 IST a 8116] 0021.6a89.51ca Applying local bridging
 Interface Policy for station 0021.6a89.51ca - vlan 20, interface 'VLAN0020'
[04/10/14 18:49:50.719 IST b 8116] 0021.6a89.51ca STA - rates (8):
 140 18 152 36 176 72 96 108 48 72 96 108 0 0 0 0

[04/10/14 18:49:50.727 IST 2f 8116] 0021.6a89.51ca Session Manager Call Client
```

57ca4000000048, uid 42, capwap id 50b94000000012,Flag 4, Audit-Session ID 0a6987b253468efb0000002a, method list

[04/10/14 18:49:50.727 IST 30 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca3] Session update from Client[1] for 0021.6a89.51ca, ID list 0x00000000
[04/10/14 18:49:50.727 IST 31 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca3] (UPD): method: Dot1X, method list: none, aaa id: 0x0000002A
[04/10/14 18:49:50.727 IST 32 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca3] (UPD): eap profile: eapfast

[04/10/14 18:49:50.728 IST 4b 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] Posting AUTH_START for 0xF700000A
[04/10/14 18:49:50.728 IST 4c 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:entering request state
[04/10/14 18:49:50.728 IST 4d 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3] Sending EAPOL packet
[04/10/14 18:49:50.728 IST 4e 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3] Platform changed src mac of EAPOL packet
[04/10/14 18:49:50.728 IST 4f 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3] EAPOL packet sent to client 0xF700000A
[04/10/14 18:49:50.728 IST 50 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:idle request action
[04/10/14 18:49:50.761 IST 51 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL message (len 5) from mobile
[04/10/14 18:49:50.761 IST 52 8116] 0021.6a89.51ca 1XA: Received EAPOL-Start from mobile
[04/10/14 18:49:50.761 IST 53 8116] 0021.6a89.51ca 1XA: EAPOL-Start - EAPOL start message from mobile as mobile is in Authenticating state, restart authenticating

[04/10/14 18:49:50.816 IST 95 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:entering response state
[04/10/14 18:49:50.816 IST 96 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3] Response sent to the server from 0xF700000A
[04/10/14 18:49:50.816 IST 97 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:ignore response action
[04/10/14 18:49:50.816 IST 98 203] Parsed CLID MAC Address = 0:33:106:137:81:202
[04/10/14 18:49:50.816 IST 99 203] AAA SRV(00000000): process authen req
[04/10/14 18:49:50.816 IST 9a 203] AAA SRV(00000000): Authen method=LOCAL

[04/10/14 18:49:50.846 IST 11d 181] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca3] Session authz status notification sent to Client[1] for 0021.6a89.51ca with handle FE000052, list 630007B2
[04/10/14 18:49:50.846 IST 11e 181]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3] Received Authz Success for the client 0xF700000A (0021.6a89.51ca)
[04/10/14 18:49:50.846 IST 11f 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] Posting AUTHZ_SUCCESS on Client 0xF700000A
[04/10/14 18:49:50.846 IST 120 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:entering authenticated state
[04/10/14 18:49:50.846 IST 121 271]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3] EAPOL success packet was sent earlier.

[04/10/14 18:49:50.846 IST 149 8116] 0021.6a89.51ca 1XA:authentication succeeded
[04/10/14 18:49:50.846 IST 14a 8116] 0021.6a89.51ca 1XK: Looking for BSSID c8f9.f983.4263 in PMKID cache
[04/10/14 18:49:50.846 IST 14b 8116] 0021.6a89.51ca 1XK: Looking for BSSID c8f9.f983.4263 in PMKID cache
[04/10/14 18:49:50.846 IST 14c 8116] 0021.6a89.51ca **Starting key exchange with mobile - data forwarding is disabled**
[04/10/14 18:49:50.846 IST 14d 8116] 0021.6a89.51ca 1XA: **Sending EAPOL message to mobile, WLAN=13 AP WLAN=13**
[04/10/14 18:49:50.858 IST 14e 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL

```
 message (len 123) from mobile
[04/10/14 18:49:50.858 IST 14f 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from
 mobile
[04/10/14 18:49:50.858 IST 150 8116] 0021.6a89.51ca 1XK: Received EAPOL-key in
 PTK_START state (msg 2) from mobile
[04/10/14 18:49:50.858 IST 151 8116] 0021.6a89.51ca 1XK: Stopping retransmission
 timer
[04/10/14 18:49:50.859 IST 152 8116] 0021.6a89.51ca 1XA: Sending EAPOL message
 to mobile, WLAN=13 AP WLAN=13
[04/10/14 18:49:50.862 IST 153 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
 message (len 99) from mobile
[04/10/14 18:49:50.862 IST 154 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from
 mobile
[04/10/14 18:49:50.862 IST 155 8116] 0021.6a89.51ca 1XK: Received EAPOL-key in
 PTKINITNEGOTIATING state (msg 4) from mobile

[04/10/14 18:49:50.863 IST 172 338] [WCDB] wcdb_ffcp_cb: client (0021.6a89.51ca)
 client (0x57ca4000000048): FFCP operation (UPDATE) return code (0)
[04/10/14 18:49:50.914 IST 173 273] dhcp pkt processing routine is called for pak
 with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 174 219] sending dhcp packet outafter processing with
 SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 175 256] DHCPD: address 20.20.20.6 mask 255.255.255.0
[04/10/14 18:49:54.279 IST 176 273] dhcp pkt processing routine is called for pak
 with SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
[04/10/14 18:49:54.279 IST 177 219] sending dhcp packet outafter processing with
 SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
```


Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.

Обновлено : 18 апреля 2014
ID документа: 117664