Авторизация облегченной точки доступа (LAP) в примере конфигурации единой беспроводной сети Cisco (UWN)

Содержание

Введение

Этот документ объясняет, как настроить контроллеры беспроводных локальных сетей (WLC) для авторизации облегченных точек доступа (LAP) на основе MAC-адреса LAP.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Базовые знания о том, как настроить сервер Cisco Secure Access Control Server (ACS) для аутентификации беспроводных клиентов
- Знание конфигурации LAP Cisco Aironet и WLC Cisco
- Знание решений по обеспечению безопасности унифицированной беспроводной связи Cisco

Используемые компоненты

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

- Cisco WLC серии 4400, который выполняет Версию 5.0.148.0
- LAP Cisco Aironet серии 1000
- LAP Cisco Aironet серии 1200
- Версия сервера 4.2 Cisco Secure ACS

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Авторизация облегченной точки доступа (LAP)

Во время процесса регистрации LAP, LAP и WLC взаимно сертификаты X.509 используемой аутентификации.

Сертификаты X.509 врезается в защищенную флэш-память и на точке доступа (AP) и на WLC на фабрике Cisco. На AP установленные сертификаты фабрики называют производством установленных сертификатов (MIC). Все AP Cisco, произведенные после 18 июля 2005, имеют MIC.

Cisco Aironet 1200, 1130, и 1240 AP, произведенных до 18 июля 2005, которые были обновлены от автономного IOS до IOS Протокола LWAPP, генерирует подписанный сертификат (SSC) во время процесса обновления. Для получения информации о том, как управлять AP с SSCs, обратитесь к Обновлению Автономных точек доступа Cisco Aironet к Облегченному режиму.

В дополнение к этой обоюдной проверке подлинности, которая происходит во время процесса регистрации, WLC могут также ограничить LAP, которые регистрируются в них на основе MAC-адреса LAP.

Отсутствие стойкого пароля при помощи MAC-адреса LAP не должно быть проблемой, потому что контроллер использует MIC для аутентификации AP прежде, чем авторизовать AP через сервер RADIUS. Использование MIC предоставляет строгую проверку подлинности.

Авторизация LAP может быть выполнена двумя способами:

- Использование Внутреннего Списка авторизации на WLC
- Использование базы данных MAC-адреса по AAA-серверу

Способы поведения LAP отличаются на основе используемого сертификата:

- LAP с SSCs — WLC будет только использовать Внутренний Список авторизации и не передаст запрос к серверу RADIUS для этих LAP.
- LAP с MIC — WLC могут использовать или Внутренний Список авторизации, настроенный на WLC, или использовать сервер RADIUS для авторизации LAP

Этот документ обсуждает авторизацию LAP с помощью и Внутреннего Списка авторизации

и AAA-сервера.

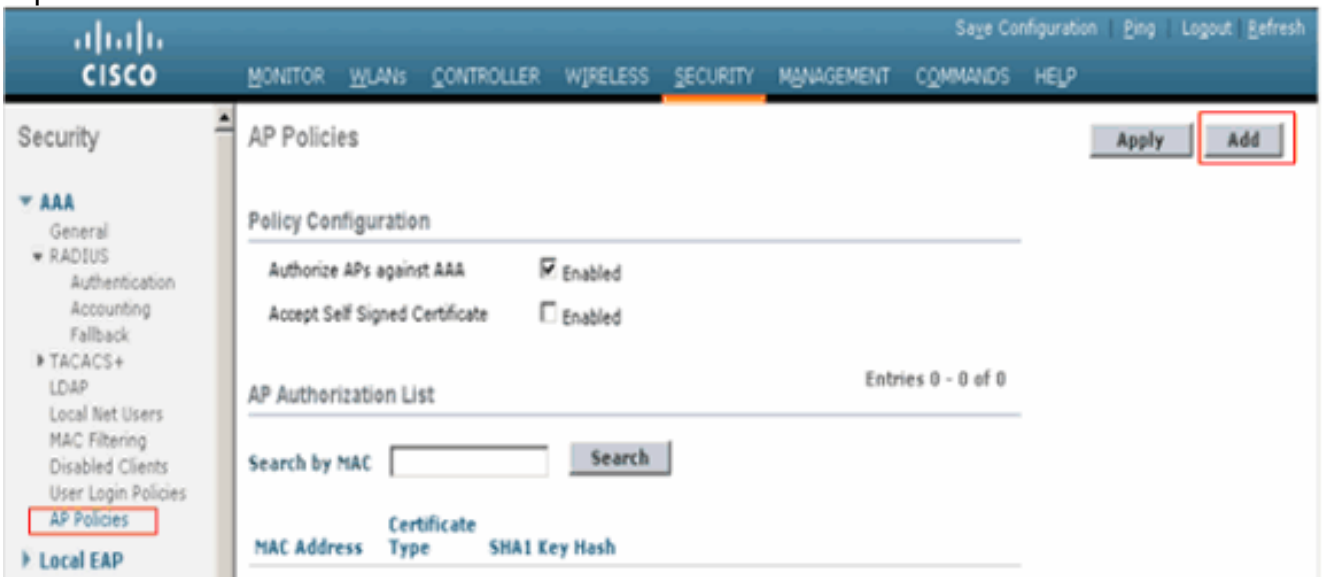
Использование внутреннего списка авторизации на WLC

На WLC используйте список авторизации AP для ограничения LAP на основе их MAC-адреса. Список авторизации AP доступен под **Безопасностью> Политика AP** в GUI WLC.

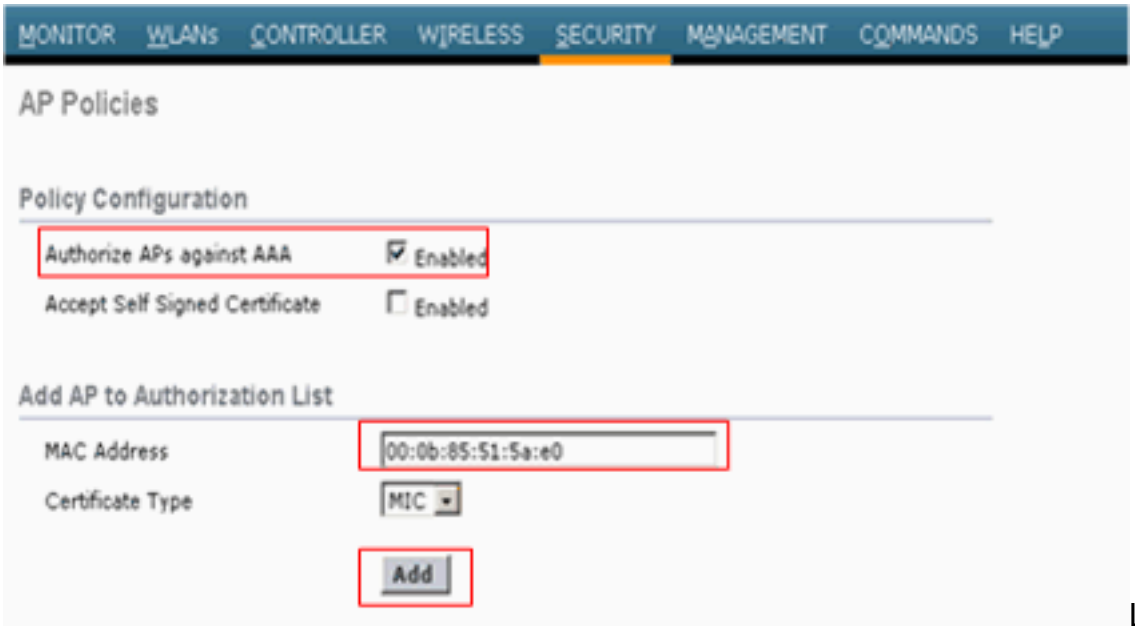
Данный пример показывает, как добавить LAP с MAC-адресом **00:0b:85:5b:fb:d0**.

Выполните следующие действия:

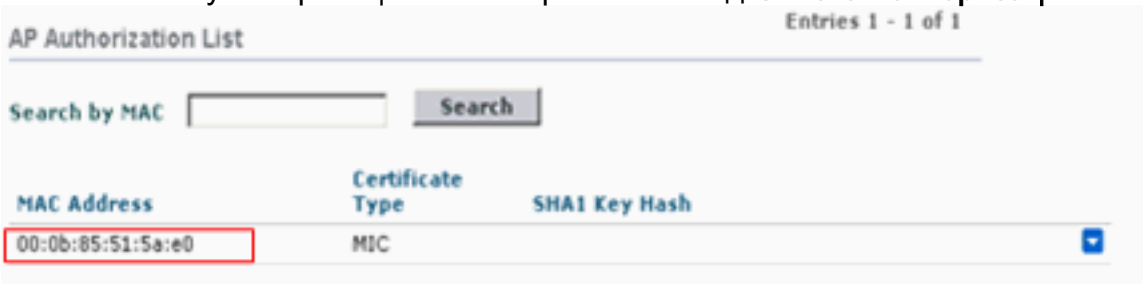
1. От графического интерфейса контроллера WLC нажмите **Security> AP Policies**.Страница AP Policies появляется.
2. Под Конфигурацией политики установите флажок для**, Авторизуют AP против AAA**.Когда этот параметр выбран, WLC проверяет, что локальная проверка подлинности перечисляет сначала. Если MAC LAP не присутствует, он проверяет сервер RADIUS.
3. Нажмите **кнопку Add** на правой стороне экрана.



4. Под Добавляют AP к Списку авторизации, вводят MAC-адрес AP. Затем выберите Тип сертификата и **нажмите Add**.В данном примере добавлен LAP с сертификатом MIC.**Примечание:** Для LAP с SSCs выберите **SSC** под Типом сертификата.



LAP добавлен к списку авторизации AP и перечислен под **Списком авторизации AP**.



Проверка

Для проверки этой конфигурации необходимо подключить LAP с MAC-адресом 00:0b:85:51:5a:e0 к сети и монитору. Используйте **команды событию debug lwapp включают и debug aaa all enable** для выполнения этого.

Когда MAC-адрес LAP не присутствует в списке авторизации AP, эти выходные данные показывают отладки:

Примечание: Некоторые линии в выходных данных были перемещены во вторую линию из-за пространственных ограничений.

```
debug lwapp events enable Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY
REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Wed Sep 12 17:42:39 2007:
00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on
Port 1 Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0
Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed Sep 12
17:42:50 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0
LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Wed Sep 12
17:42:50 2007: spamRadiusProcessResponse: AP Authorization failure for 00:0b:85:51:5a:e0 debug
aaa all enable Wed Sep 12 17:56:26 2007: Unable to find requested user entry for 000b85515ae0
Wed Sep 12 17:56:26 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:26 2007:
Callback.....0x8108e2c Wed Sep 12 17:56:26 2007:
protocolType.....0x00000001 Wed Sep 12 17:56:26 2007:
proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet
contains 8 AVPs (not shown) Wed Sep 12 17:56:26 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No
```

Server' (-7) for mobile 00:0b:85:51:5a:e0 Wed Sep 12 17:56:26 2007: AuthorizationResponse: 0xbadff7d4 Wed Sep 12 17:56:26 2007: structureSize...................28 Wed Sep 12 17:56:26 2007: resultCode.....................-7 Wed Sep 12 17:56:26 2007: protocolUsed.....................0xffffffff Wed Sep 12 17:56:26 2007: proxyState.....................00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet contains 0 AVPs: Wed Sep 12 17:56:31 2007: Unable to find requested user entry for 000b85515ae0 Wed Sep 12 17:56:31 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:31 2007: Callback.....................0x8108e2c Wed Sep 12 17:56:31 2007: protocolType.....................0x00000001 Wed Sep 12 17:56:31 2007: proxyState.....................00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:31 2007: Packet contains 8 AVPs (not shown) Wed Sep 12 17:56:31 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No Server' (-7) for mobile 00:0b:85:51:5a:e0

Эти выходные данные show отладки, когда MAC-адрес LAP добавлен к списку авторизации AP:

Примечание: Некоторые линии в выходных данных были перемещены во вторую линию из-за пространственных ограничений.

debug lwapp events enable Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0 (index 58)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 debug aaa all enable** Wed Sep 12 17:57:44 2007: **User 000b85515ae0 authenticated** Wed Sep 12 17:57:44 2007: **00:0b:85:51:5a:e0 Returning AAA Error 'Success' (0) for mobile 00:0b:85:51:5a:e0** Wed Sep 12 17:57:44 2007: AuthorizationResponse: 0xbadff96c Wed Sep 12 17:57:44 2007: structureSize.....................70 Wed Sep 12 17:57:44 2007: resultCode.....................0 Wed Sep 12 17:57:44 2007: protocolUsed.....................0x00000008 Wed Sep 12 17:57:44 2007: proxyState.....................00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:57:44 2007: Packet contains 2 AVPs: Wed Sep 12 17:57:44 2007: AVP[01] Service-Type..... 0x00000065 (101) (4 bytes) Wed Sep 12 17:57:44 2007: AVP[02] Airespace / WLAN-Identifier..... 0x00000000 (0) (4 bytes)

Авторизация AP против AAA-сервера

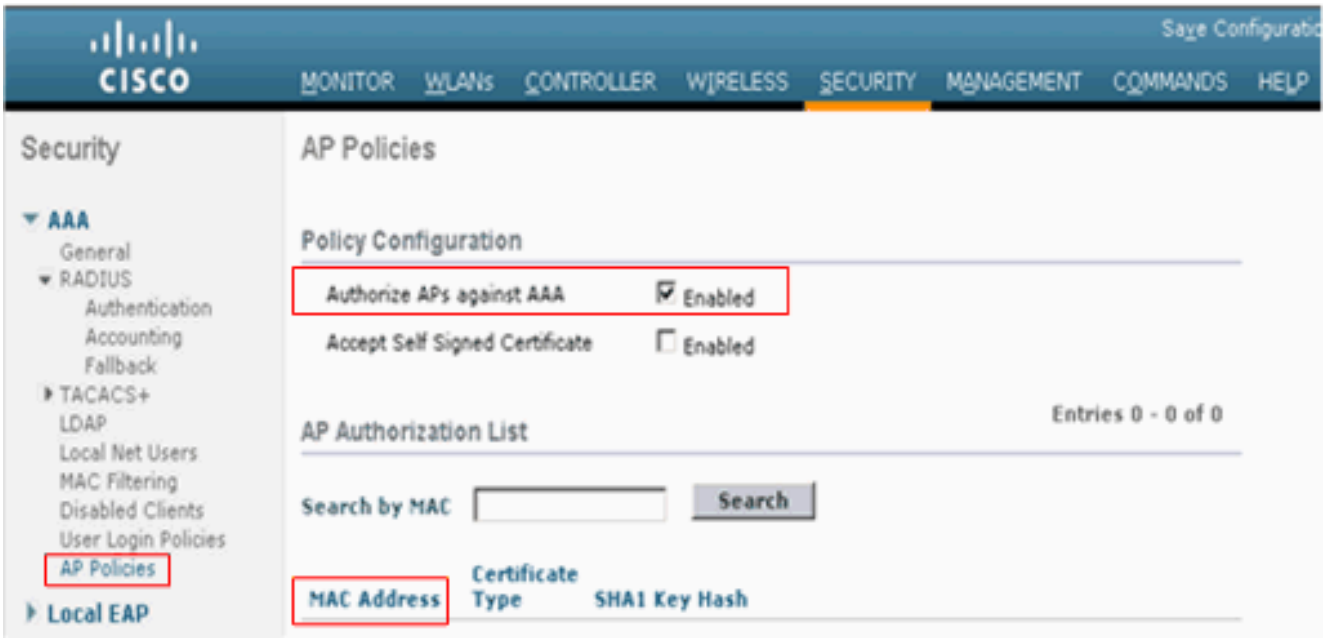
Можно также настроить WLC для использования серверов RADIUS для авторизации AP с помощью MIC. WLC использует MAC-адрес LAP в качестве обоих имя пользователя и пароль при передаче информации к серверу RADIUS. Например, если MAC-адрес AP является 000b85229a70, оба, которые имя пользователя и пароль, используемое контроллером для авторизации AP, является 000b85229a70.

Примечание: При использовании MAC-адрес в качестве имени пользователя и пароля для аутентификации AP на AAA-сервере RADIUS, не используйте тот же AAA-сервер для аутентификации клиента. Причина для этого состоит в том, если хакеры узнают MAC-адрес AP, то они могут использовать тот MAC в качестве учетных данных имени пользователя и пароля для получения на сеть.

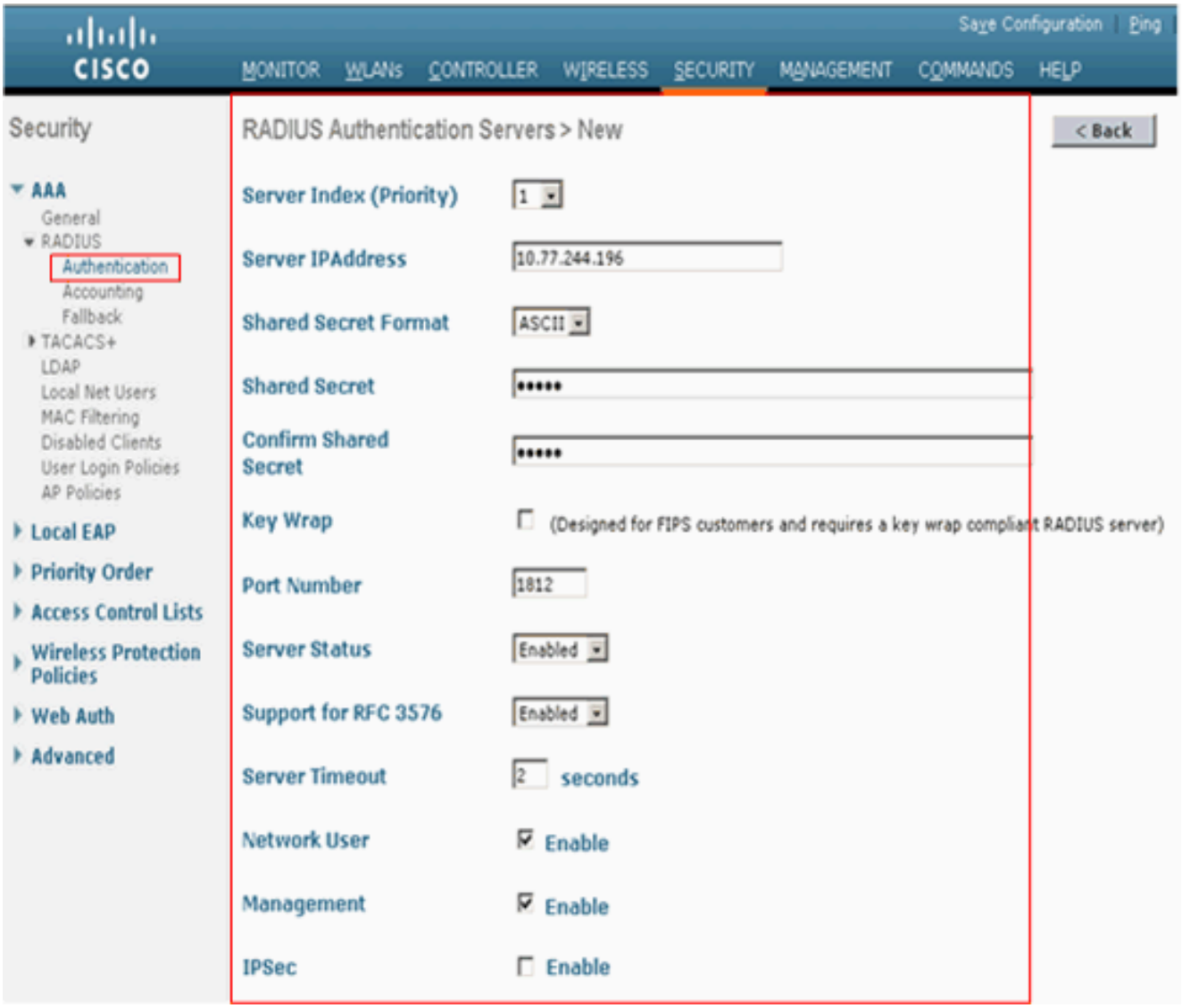
Данный пример показывает, как настроить WLC для авторизации LAP с помощью Cisco Secure ACS.

Выполните эти шаги на WLC:

1. От графического интерфейса контроллера WLC нажмите **Security> AP Policies**.Страница AP Policies появляется.
2. Под Конфигурацией политики установите флажок для**, Авторизуют AP против AAA**.Когда этот параметр выбран, WLC проверяет базу данных локального MAC - адреса сначала. Поэтому удостоверьтесь, что Локальная база данных пуста путем очистки MAC-адресов под Списком авторизации AP. Если MAC-адрес LAP не присутствует, он тогда проверяет сервер RADIUS.



3. **Нажмите Security и RADIUS Authentication в контроллере GUI, чтобы открыть страницу "RADIUS Authentication Servers". Чтобы определить сервер RADIUS, нажмите New.**



4. Определите параметры сервера RADIUS на странице **RADIUS Authentication Servers> New**. В их числе: RADIUS Server IP Address, Shared Secret, Port Number и Server Status.Данный пример использует Cisco Secure ACS в качестве сервера RADIUS с IP-адресом 10.77.244.196.
5. **Щелкните "Применить".**

Настройте Cisco Secure ACS для авторизации LAP

Чтобы позволить Cisco Secure ACS авторизовать LAP, необходимо выполнить эти шаги:

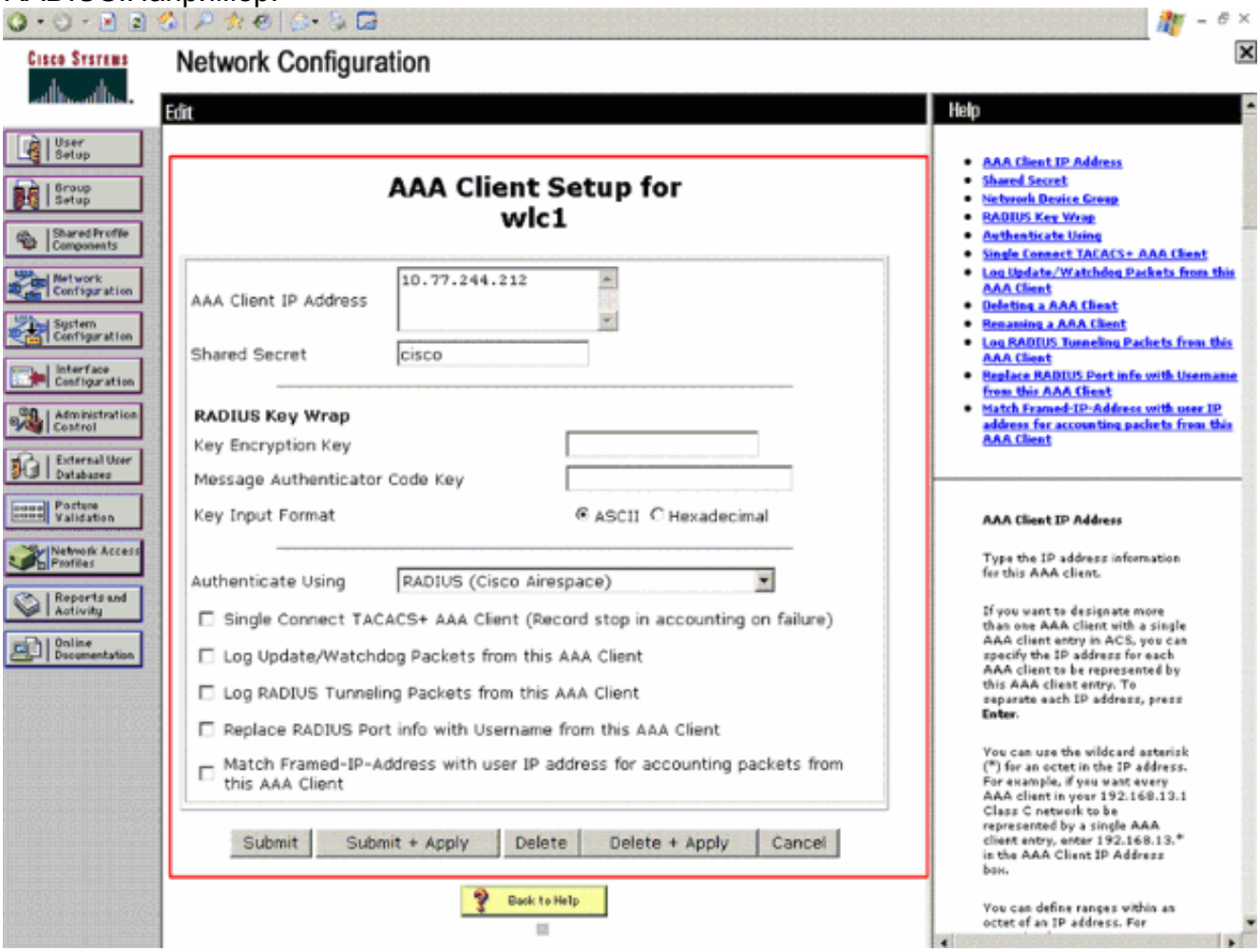
1. Настройте WLC как клиента AAA на Cisco Secure ACS
2. Добавьте MAC-адреса LAP к базе данных пользователей на Cisco Secure ACS

Настройте WLC как клиента AAA на Cisco Secure ACS

Выполните эти шаги для настройки WLC как клиент AAA на Cisco Secure ACS:

1. Нажмите **Network Configuration> Add AAA Client**.Страница Add AAA Client появляется.
2. На этой странице определите имя системы WLC, IP-адрес Интерфейса управления, Общий секретный ключ и Airespace RADIUS Используемой аутентификации.**Примечание:** Также можно попробовать опцию Authenticate с

помощью Aironet
RADIUS.Например:

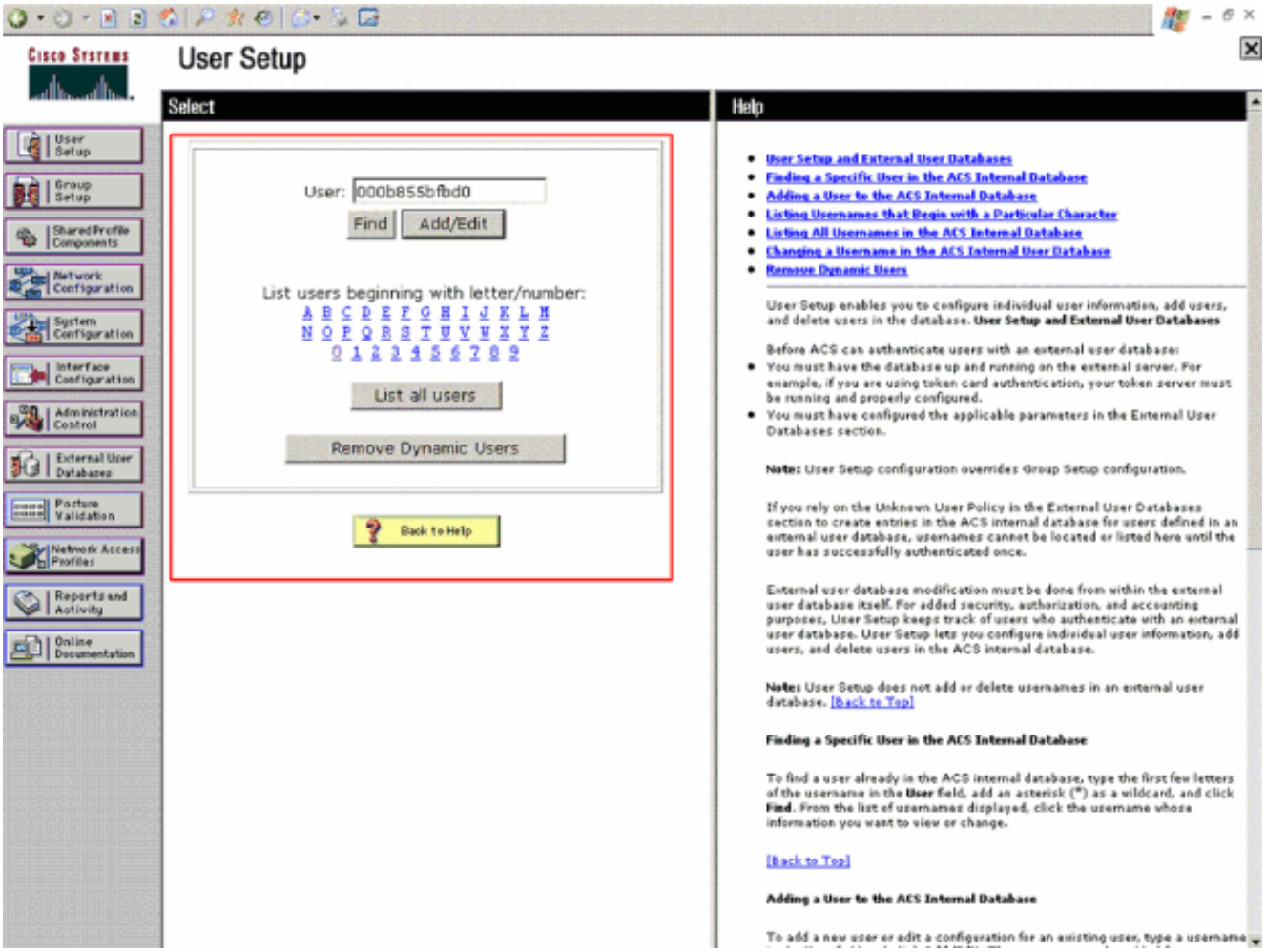


3. **Нажмите кнопку Submit+Apply (Отправить и применить).**

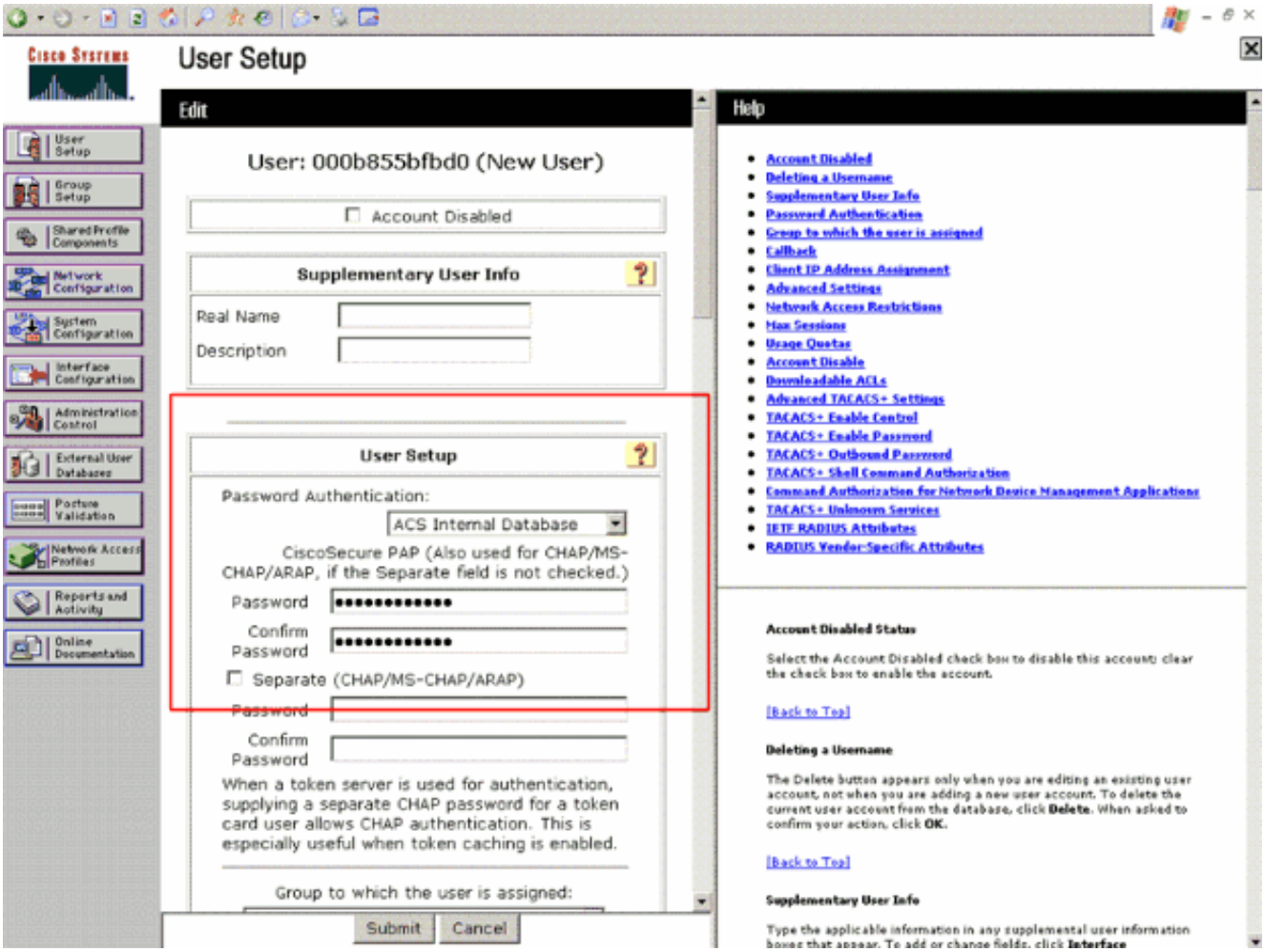
Добавьте MAC-адреса LAP к базе данных пользователей на Cisco Secure ACS

Выполните эти шаги для добавления MAC-адресов LAP к Cisco Secure ACS:

1. **В ACS GUI выберите User Setup, введите имя пользователя и нажмите Add/Edit.**Имя пользователя должно быть MAC-адресом LAP, который вы хотите авторизовать. MAC-адрес не должен содержать двоеточия или дефисы.В данном примере LAP добавлен с MAC-адресом
000b855bfbd0:



2. Когда страница User Setup появится, определите пароль для этого LAP в поле Password как показано.Пароль должен также быть MAC-адресом LAP. В данном примере это - **000b855bfbd0**.



3. **Нажмите кнопку Submit (Отправить).**
4. Повторите эту процедуру для добавления большего количества LAP к базе данных Cisco Secure ACS.

Проверка

Для проверки этой конфигурации необходимо подключить LAP с MAC-адресом 00:0b:85:51:5a:e0 к сети и монитору. Используйте **команды событию debug lwapp включают и debug aaa all enable** для выполнения этого.

Как замечено по отладкам, WLC передал MAC-адрес LAP серверу RADIUS 10.77.244.196, и сервер успешно аутентифицировал LAP. LAP тогда регистрируется в контроллере.

Примечание: Некоторые линии в выходных данных были перемещены во вторую линию из-за пространственных ограничений.

```
debug aaa all enable Thu Sep 13 13:54:39 2007: AuthenticationRequest: 0xac48778 Thu Sep 13
13:54:39 2007: Callback.....................0x8108e2c Thu Sep 13 13:54:39 2007:
protocolType.....................0x00000001 Thu Sep 13 13:54:39 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:39 2007: Packet
contains 8 AVPs (not shown) Thu Sep 13 13:54:39 2007: 00:0b:85:51:5a:e0 Successful transmission
of Authentication Packet (id 123) to 10.77.244.196:1812, proxy state 00:0b:85:51:5a:e0-85:51 Thu
Sep 13 13:54:39 2007: 00000000: 01 7b 00 72 00 00 00 00 00 00 00 00 00 00 00 00 .{.r............
Thu Sep 13 13:54:39 2007: 00000010: 00 00 00 00 01 0e 30 30 30 62 38 35 35 31 35 61
......000b85515a Thu Sep 13 13:54:39 2007: 00000020: 65 30 1e 13 30 30 2d 30 62 2d 38 35 2d 33
33 2d e0..00-0b-85-33- Thu Sep 13 13:54:39 2007: 00000030: 35 32 2d 38 30 1f 13 30 30 2d 30 62
2d 38 35 2d 52-80..00-0b-85- Thu Sep 13 13:54:39 2007: 00000040: 35 31 2d 35 61 2d 65 30 05 06
```

00 00 00 01 04 06 51-5a-e0..... Thu Sep 13 13:54:39 2007: 00000050: 0a 4d f4 d4 20 06 77 6c 63 31 02 12 03 04 0e 12 .M....wlc1..... Thu Sep 13 13:54:39 2007: 00000060: 84 9c 03 8f 63 40 2a be 9d 38 42 91 06 06 00 00 ....c@*..8B..... Thu Sep 13 13:54:39 2007: 00000070: 00 0a .. Thu Sep 13 13:54:40 2007: 00000000: 02 7b 00 30 aa fc 40 4b fe 3a 33 10 f6 5c 30 fd .{.0..@K.:3..\0. Thu Sep 13 13:54:40 2007: 00000010: 12 f3 6e fa 08 06 ff ff ff ff 19 16 43 41 43 53 ..n.....CACS Thu Sep 13 13:54:40 2007: 00000020: 3a 30 2f 39 37 37 2f 61 34 64 66 34 64 34 2f 31 :0/977/a4df4d4/1 Thu Sep 13 13:54:40 2007: ****Enter processIncomingMessages: response code=2 Thu Sep 13 13:54:40 2007: ****Enter processRadiusResponse: response code=2 Thu Sep 13 13:54:40 2007: **00:0b:85:51:5a:e0 Access-Accept received from RADIUS server 10.77.244.196 for mobile 00:0b:85:51:5a:e0** receiveId = 0 Thu Sep 13 13:54:40 2007: AuthorizationResponse: 0x9845500 Thu Sep 13 13:54:40 2007: structureSize.....84 Thu Sep 13 13:54:40 2007: resultCode.....0 Thu Sep 13 13:54:40 2007: protocolUsed.....0x00000001 Thu Sep 13 13:54:40 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:40 2007: Packet contains 2 AVPs: Thu Sep 13 13:54:40 2007: AVP[01] Framed-IP-Address..... 0xffffffff (-1) (4 bytes) Thu Sep 13 13:54:40 2007: AVP[02] Class..... CACS:0/977/a4df4d4/1 (20 bytes) **debug lwapp events enable** Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 57)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1**

Устранение неполадок

Используйте эти команды для устранения проблем конфигурации:

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

- **debug lwapp events enable** отладку Событий lwapp и ошибок.
- **debug lwapp packetenable** отладку трассировки Пакета lwapp.
- **debug aaa all enable – настраивает отладку сообщений AAA.**

Дополнительные сведения

- Модернизация автономных точек доступа Cisco Aironet до упрощенного режима
- Подсказки по устранению неполадок инструмента обновления LWAPP
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация