Пример конфигурации фильтров с MAC с контроллерами беспроводных LAN (WLC)

Содержание

Введение

В этом документе поясняется настройка фильтров MAC с контроллерами беспроводных локальных сетей (WLC) и приводится пример конфигурации. Также рассматривается способ авторизации облегченных точек доступа (LAP) на сервере AAA (аутентификации, авторизации и учета).

Предварительные условия

Требования

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

- Основные сведения о конфигурации точек LAPи контроллеров Cisco WLC
- Базовые знания о Решениях по обеспечению безопасности унифицированной беспроводной связи Cisco

Используемые компоненты

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

- WLC Cisco 4400, который работает под управлением ПО версии 5.2.178.0
- LAP Cisco 1230AG Series
- Беспроводной клиентский адаптер a/b/g 802.11 с микропрограммным обеспечением 4.4
- Версия 4.4 Служебной программы рабочего стола Aironet (ADU)

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.

Фильтр MAC - адреса (проверка подлинности MAC) на WLC

Когда вы создаете Фильтр MAC - адреса на WLC, пользователей предоставляют или запрещенный доступ к сети WLAN на основе MAC-адреса клиента, которого они используют.

Существует два типа проверки подлинности MAC, которые поддерживаются на WLC:

- Аутентификация Локального MAC - адреса
- Проверка подлинности MAC с помощью сервера RADIUS

С аутентификацией локального MAC - адреса пользовательские MAC-адреса сохранены в базе данных по WLC. Когда пользователь пытается обратиться к WLAN, который настроен для фильтрации по MAC-адресам, MAC - адрес клиента проверен против локальной базы данных на WLC, и клиент является предоставленным доступом к WLAN, если аутентификация успешна.

По умолчанию локальная база данных WLC поддерживает до 512 вводов пользователя.

База локальных пользователей ограничена максимумом записей 2048 года. Локальная база данных хранит записи для этих элементов:

- Пользователи локального управления, который включает послов лобби
- Пользователи локальной сети, который включает гостей
- Записи фильтра MAC
- Записи списка исключения
- Записи списка авторизации точки доступа

Пользователи всех этих типов вместе не могут превышать настроенный размер базы данных.

Для увеличения локальной базы данных используйте эту команду от CLI:

```
<Cisco Controller>config database size ? <count> Enter the maximum number of entries (512-2048)
```

Также Аутентификация с использованием MAC-адреса может также быть выполнена с помощью сервера RADIUS. Единственная разница - то, что пользовательская база данных MAC-адреса сохранена в сервере RADIUS вместо WLC. Когда база данных пользователей сохранена на сервере RADIUS WLC вперед MAC-адрес клиента к серверу RADIUS для клиентской проверки. Затем сервер RADIUS проверяет MAC-адрес на основе базы данных, которую это имеет. Если аутентификация клиента успешна, клиент является предоставленным доступом к WLAN. Любой сервер RADIUS, который поддерживает Аутентификацию с использованием MAC-адреса, может использоваться.

Настройте аутентификацию локального MAC - адреса на WLC

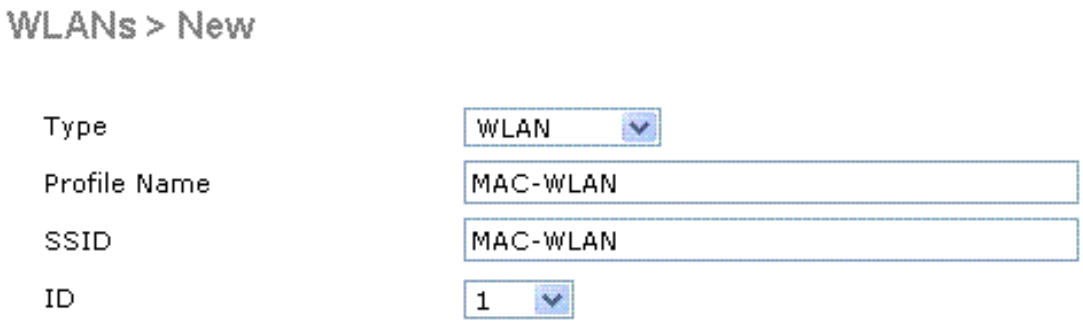
Выполните эти шаги для настройки аутентификации локального MAC - адреса на WLC:

1. Настройте WLAN и включите фильтрацию по MAC-адресам
2. Настройте локальную базу данных на WLC с MAC - адресами клиента**Примечание:** Перед настройкой проверки подлинности MAC необходимо настроить WLC для главной операции и зарегистрировать облегченные точки доступа на контроллере. Этот документ предполагает, что WLC уже настроен для главной операции и что LAP зарегистрированы к WLC. Если вы - новый пользователь, пытающийся устанавливать WLC для главной операции с LAP, обратитесь к регистрации облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC).**Примечание:** Нет никакой специальной конфигурации, необходимой на беспроводном клиенте для поддержки проверки подлинности MAC.

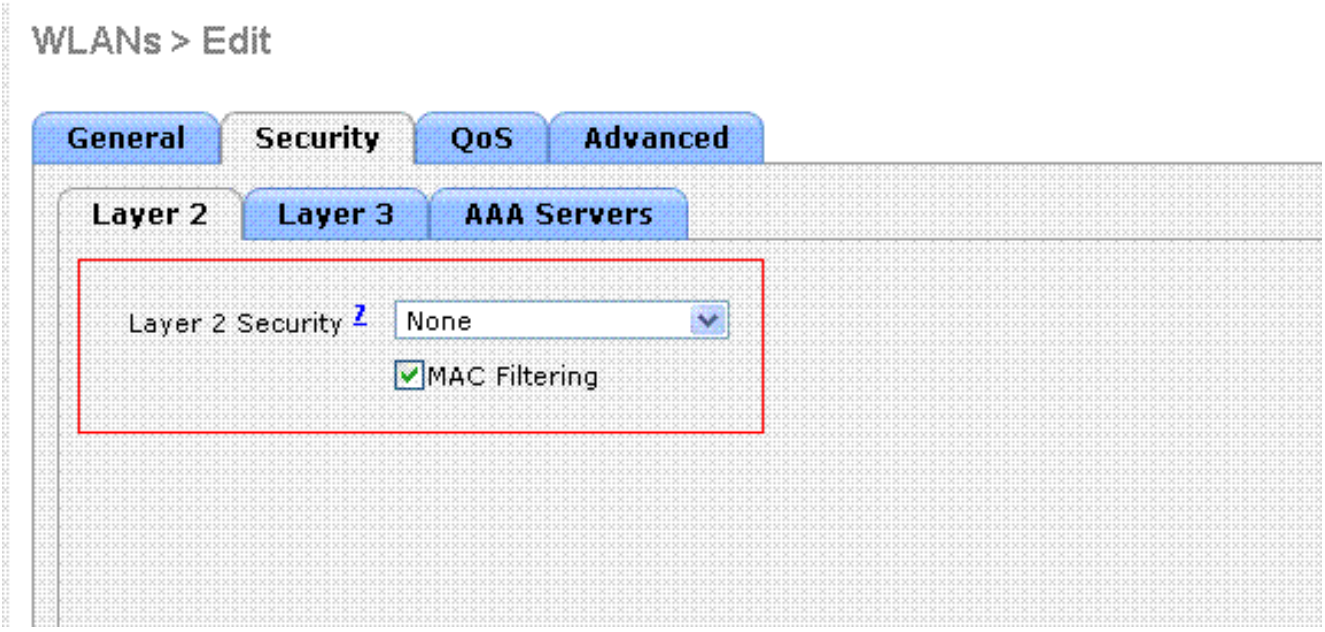
Настройте WLAN и включите фильтрацию по MAC-адресам

Выполните эти шаги для настройки WLAN с фильтрацией по MAC-адресам:

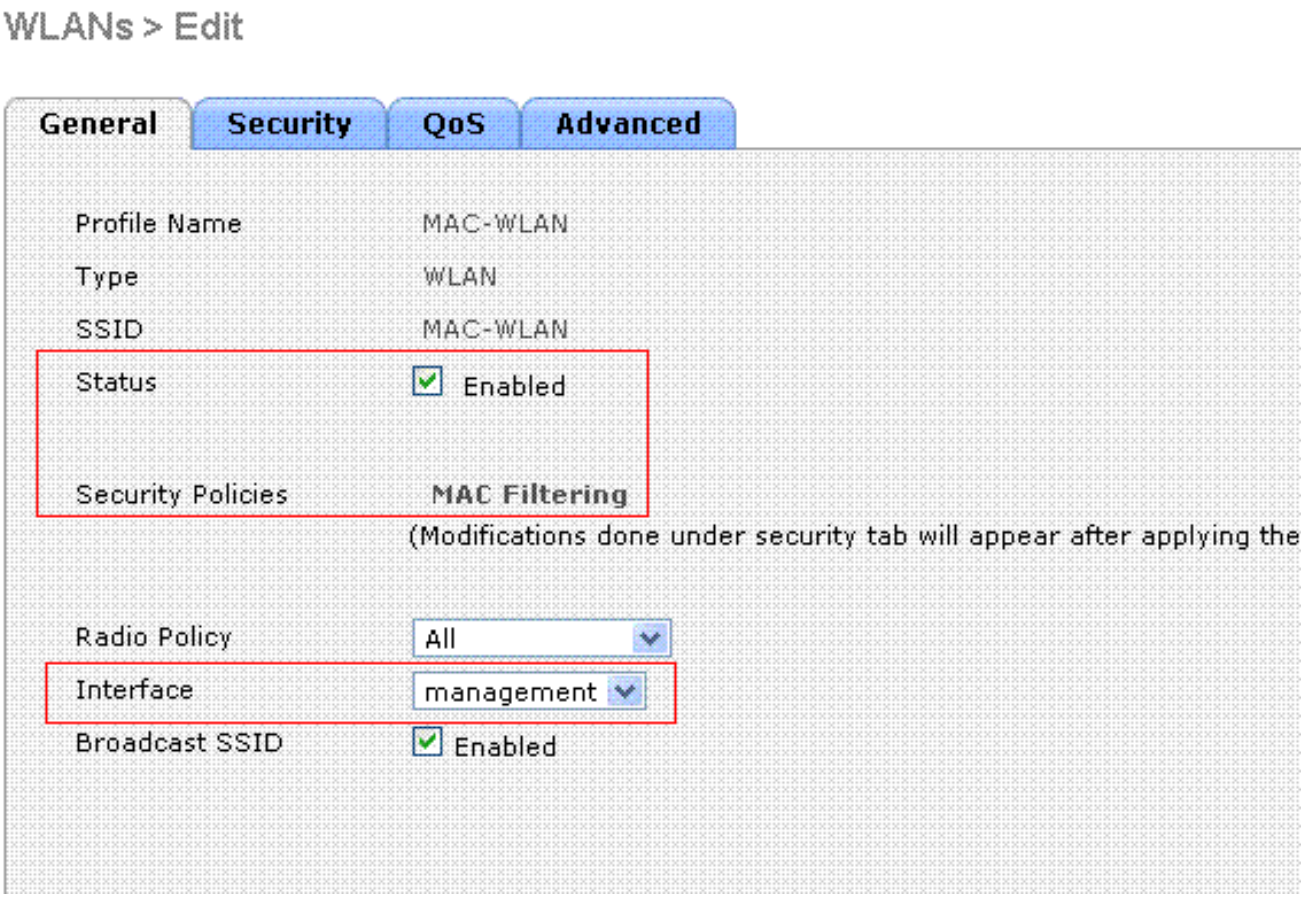
1. **Нажмите WLANs в графическом интерфейсе контроллера для создания WLAN.**Откроется окно WLAN. В данном окне находится список сетей WLAN, настроенных на контроллере.
2. **Нажмите New для настройки новой WLAN.**В данном примере WLAN называют *WLAN MAC*, и ИДЕНТИФИКАТОР WLAN равняется
   1.



3. **Щелкните "Применить".**
4. В окне WLAN > Edit укажите параметры сети.



Под Политикой безопасности> безопасность уровня 2, проверьте флажок **MAC Filtering**.Это включает проверку подлинности MAC для WLAN.В соответствии с Общей политикой> Имя интерфейса, выберите интерфейс, с которым сопоставлен WLAN.В данном примере WLAN сопоставлен с интерфейсом управления.Выберите другие параметры, которые зависят от требований к проектированию WLAN.**Щелкните "Применить".**



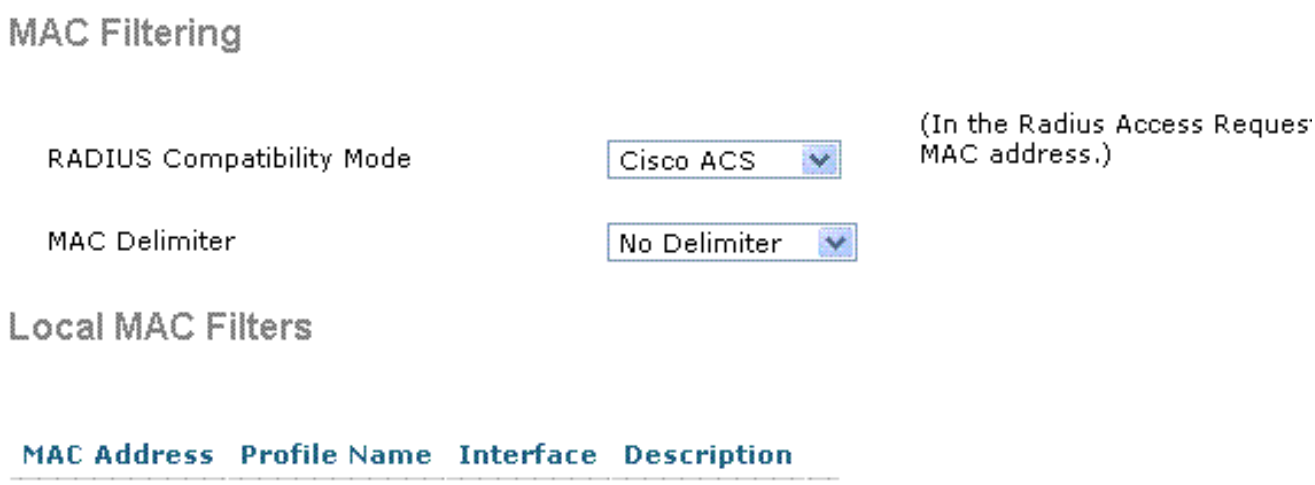
Следующий шаг должен настроить локальную базу данных на WLC с MAC - адресами клиента.

См. VLAN на Примере конфигурации Контроллеров беспроводной локальной сети для получения информации о том, как настроить динамические интерфейсы (VLAN) на WLC.

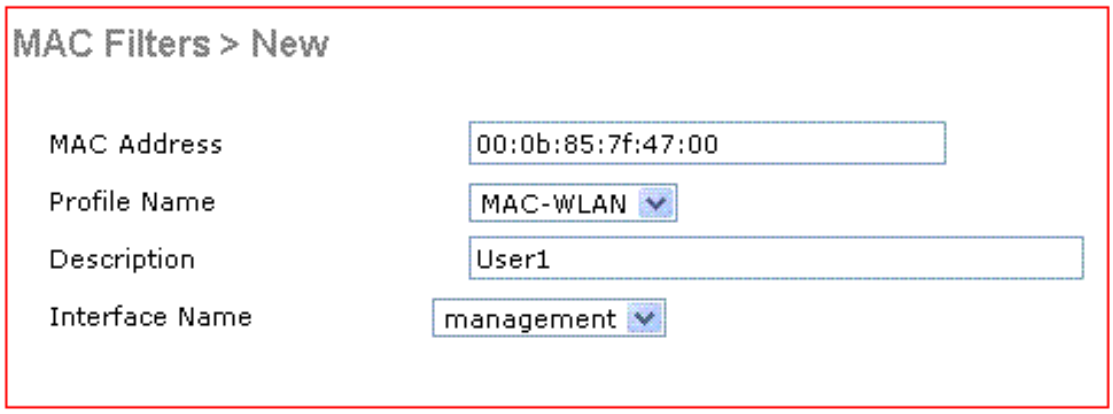
Настройте локальную базу данных на WLC с MAC - адресами клиента

Выполните эти шаги для настройки локальной базы данных с MAC - адресом клиента на WLC:

1. Нажмите **Security** от графического интерфейса контроллера, и затем нажмите **MAC Filtering** из левого бокового меню.Окно MAC Filtering появляется.



2. Нажмите **New** для создания Записи MAC - адресов локальной базы данных на WLC.
3. В Фильтрах MAC> Новое окно, введите MAC-адрес, Имя профиля, Описание и Имя интерфейса для клиента.Например:



4. **Щелкните "Применить".**
5. Повторите шаги 2-4 для добавления большего количества клиентов к локальной базе данных.Теперь, когда клиенты соединяются с этим WLAN, WLC проверяет MAC-адрес клиентов против локальной базы данных и если проверка успешна, клиент является предоставленным доступом к сети.**Примечание:** В данном примере использовался только Фильтр MAC - адрес без любого другого механизма безопасности уровня 2. Cisco рекомендует, чтобы Аутентификация с использованием MAC-адреса использовалась наряду с другим Уровнем 2 или методами безопасности уровня 3. Не желательно использовать только Аутентификацию с использованием MAC-адреса для обеспечения сети WLAN, потому что это не предоставляет сильный механизм обеспечения безопасности.

Настройте Проверку подлинности MAC с помощью сервера RADIUS

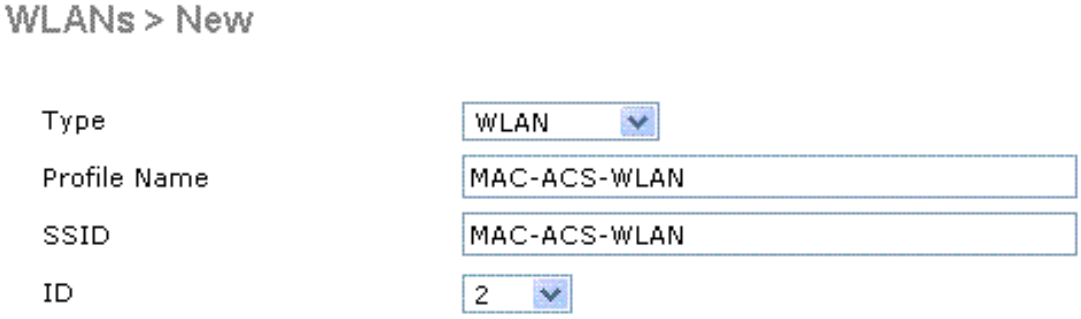
Выполните эти шаги для настройки проверки подлинности MAC с помощью сервера RADIUS. В данном примере сервер Cisco Secure ACS используется в качестве сервера RADIUS.

1. Настройте WLAN и включите фильтрацию по MAC-адресам
2. Настройте сервер RADIUS с MAC - адресами клиента

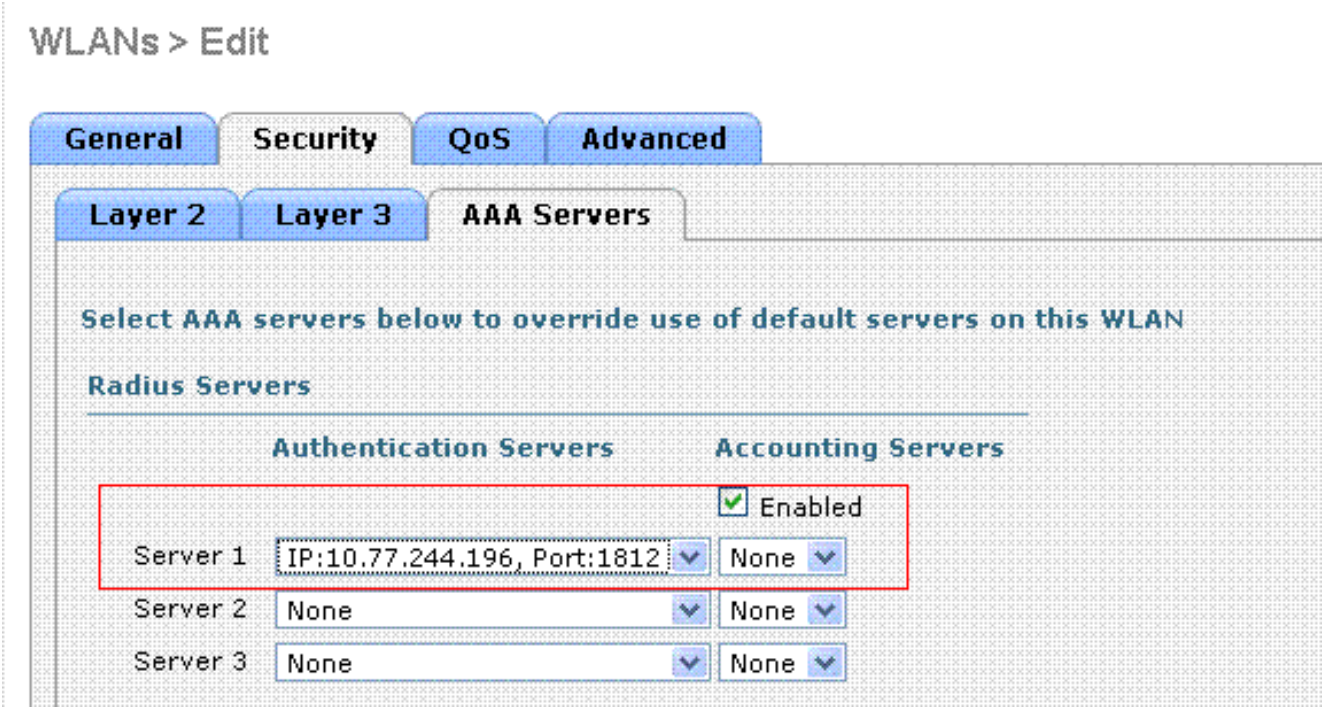
Настройте WLAN и включите фильтрацию по MAC-адресам

Выполните эти шаги для настройки WLAN с фильтрацией по MAC-адресам:

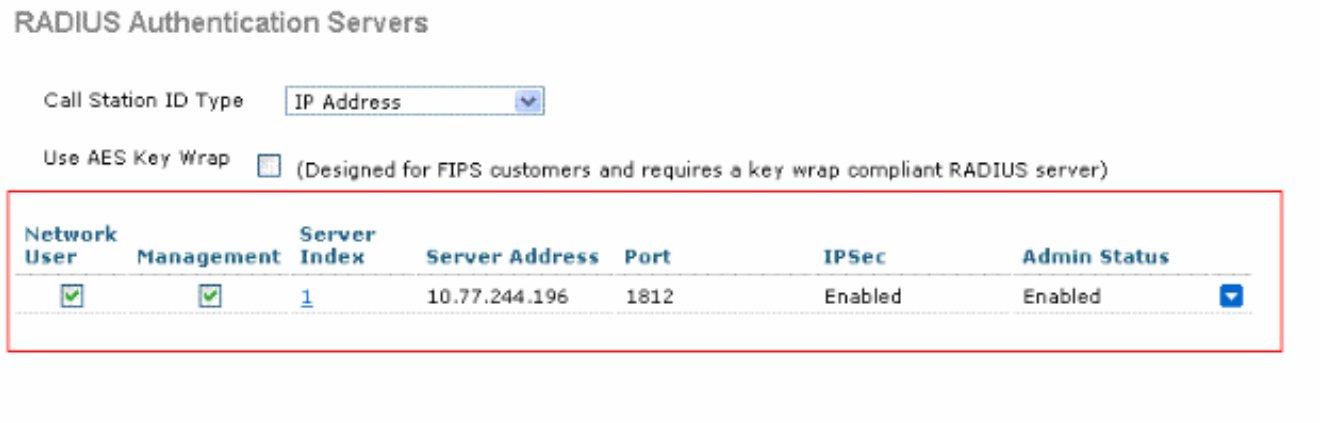
1. **Нажмите WLANs в графическом интерфейсе контроллера для создания WLAN.**Откроется окно WLAN. В данном окне находится список сетей WLAN, настроенных на контроллере.
2. **Нажмите New для настройки новой WLAN.**В данном примере WLAN называют *WLAN ACS MAC*, и ИДЕНТИФИКАТОР WLAN равняется *2*.



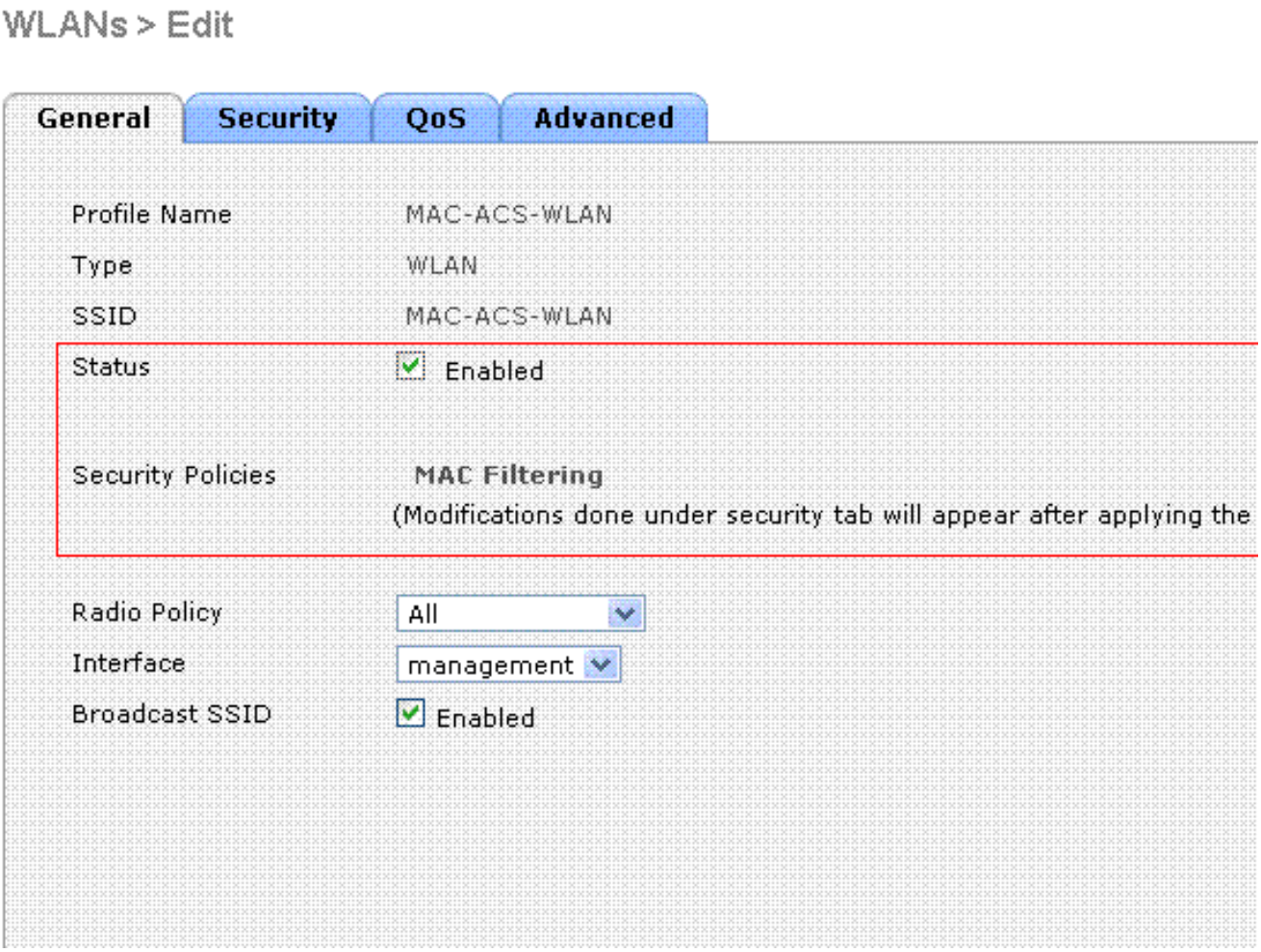
3. **Щелкните "Применить".**
4. В окне WLAN > Edit укажите параметры сети.Под Политикой безопасности> безопасность уровня 2, проверьте флажок **MAC Filtering**.Это включает проверку подлинности MAC для WLAN.В соответствии с Общей политикой> Имя интерфейса, выберите интерфейс, с которым сопоставлен WLAN.Под серверами RADIUS выберите сервер RADIUS, который будет использоваться для проверки подлинности MAC.



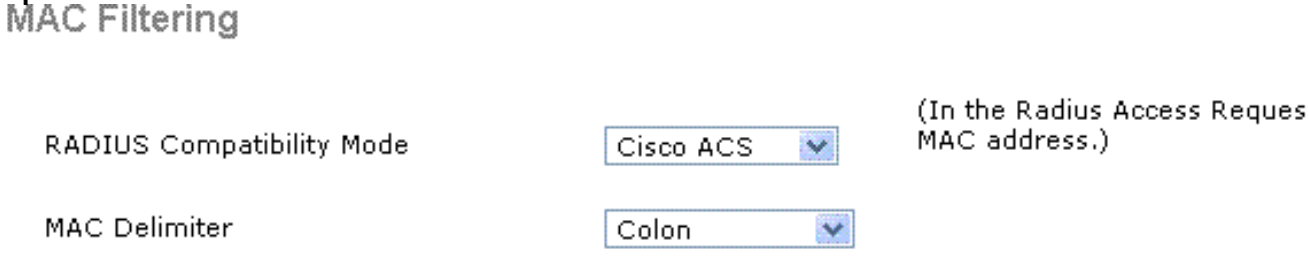
Примечание: Прежде чем можно будет выбрать сервер RADIUS от окна WLANs> Edit, необходимо определить сервер RADIUS в окне Security> Radius Authentication и включить сервер
RADIUS.



Выберите другие параметры, которые зависят от требований к проектированию WLAN.**Щелкните**
"Применить".



5. Нажмите **Security> MAC Filtering**.
6. В окне MAC Filtering выберите тип сервера RADIUS под Режимом совместимости RADIUS.Данный пример использует ACS Cisco.
7. От выпадающее меню Разделителя MAC выберите разделитель MAC.Данный пример использует Двоеточие.
8. **Щелкните "Применить".**



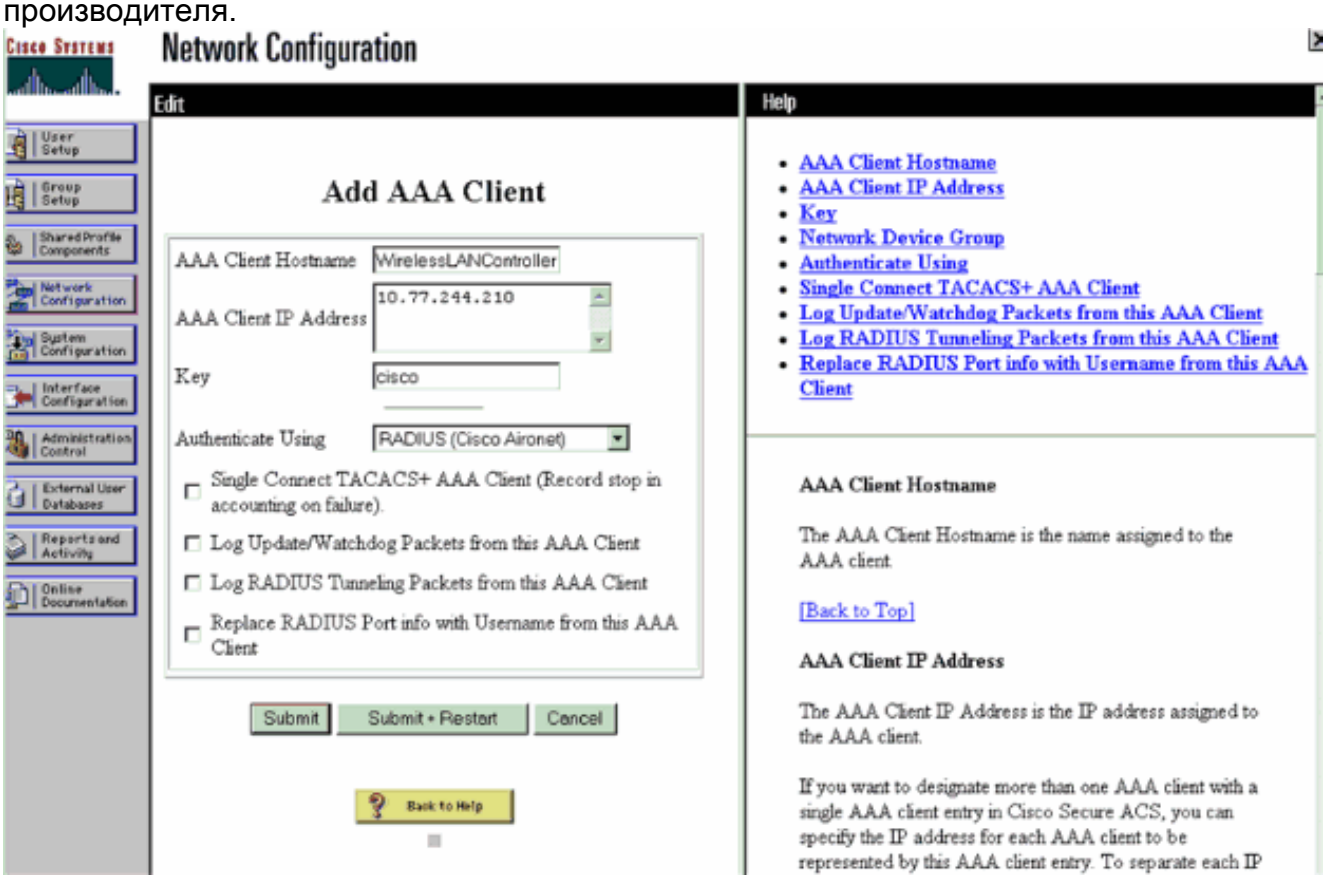
Следующий шаг должен настроить сервер ACS с MAC - адресами клиента.

Настройте сервер RADIUS с MAC - адресами клиента

Выполните эти шаги для добавления MAC-адреса к ACS:

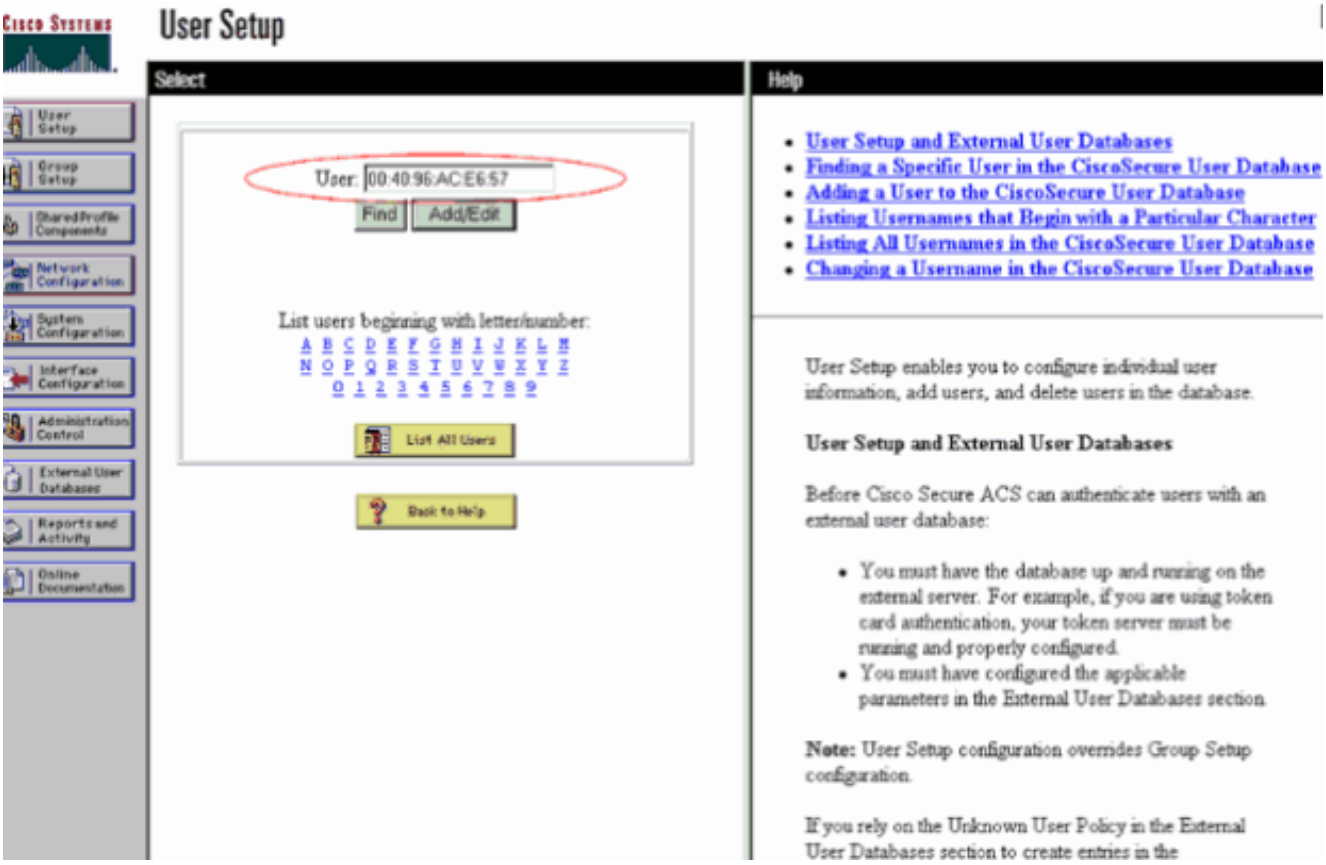
1. Определите WLC как клиента AAA на сервере ACS. **В ACS GUI нажмите Network Configuration.**
2. Когда окно Network Configuration появится, определите название WLC, IP-адреса, общего секретного ключа и метода аутентификации (Cisco Aironet RADIUS или Airespace RADIUS).Сведения о серверах аутентификации, отличной от ACS, см. в

документации от
производителя.



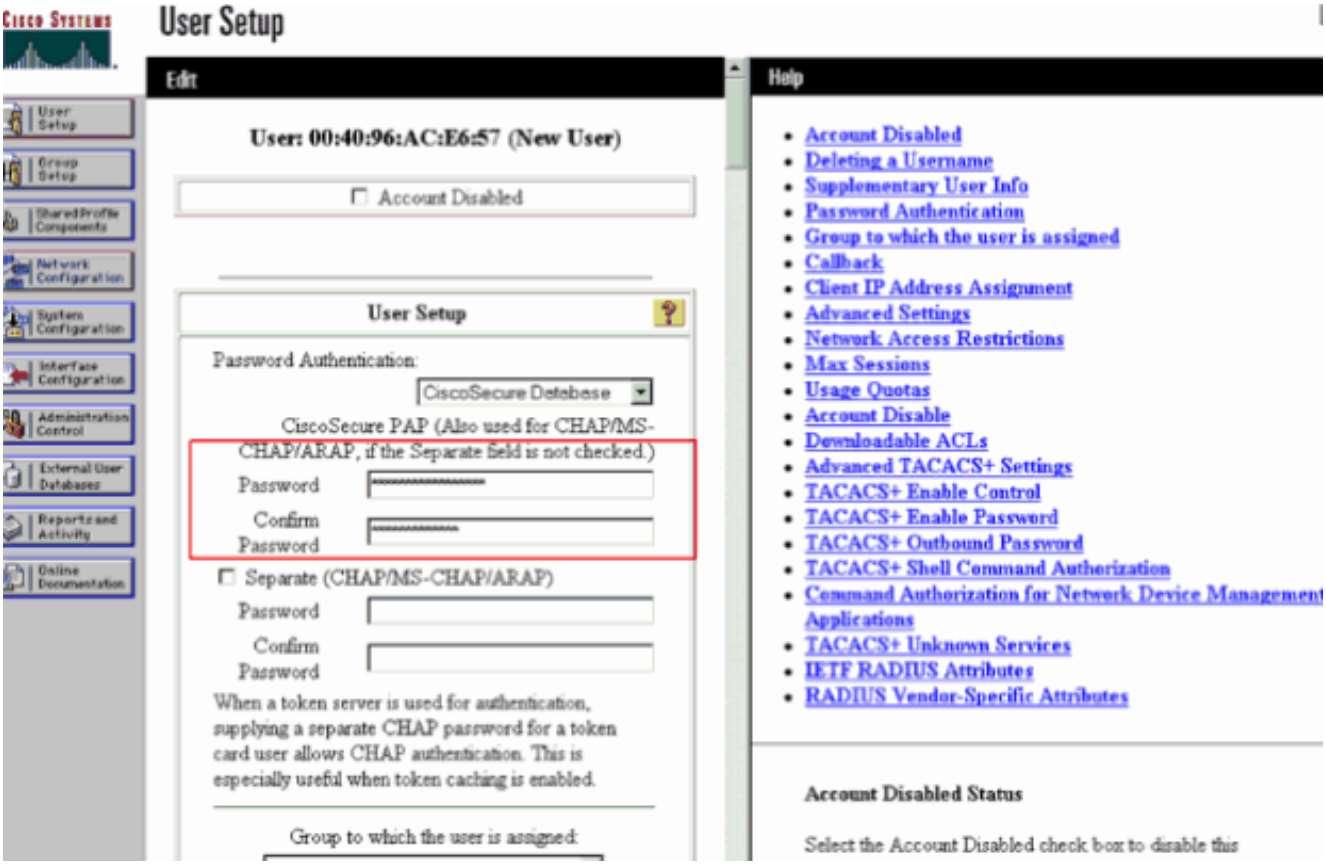
Примечание: Общий секретный ключ на WLC и сервере ACS должны совпадать. При вводе общего секретного ключа необходимо учитывать регистр.

3. Из главного меню ACS нажмите **User Setup**.
4. В коробке Пользовательского текста введите MAC-адрес для добавления к базе данных
пользователей.



Примечание: MAC-адрес должен быть точно, когда он передается WLC и за именем пользователя и за паролем. Если аутентификация отказывает, проверьте журнал неудачных попыток, чтобы видеть, как о MAC сообщает WLC. Не вырезайте и вставить MAC-адрес, поскольку это может представить фантомные символы.

5. В окне User Setup введите MAC-адрес в текстовое поле Безопасного пароля PAP.



Примечание: MAC-адрес должен быть точно, когда он передается WLC и за именем

пользователя и за паролем. Если аутентификация отказывает, проверьте журнал неудачных попыток, чтобы видеть, как о MAC сообщает AP. Не вырезайте и вставить MAC-адрес, поскольку это может представить фантомные символы.

6. **Нажмите кнопку Submit (Отправить).**
7. Повторите шаги 2-5 для добавления большего количества пользователей к базе данных ACS.Теперь, когда клиенты соединяются с этим WLAN, WLC передает учетные данные к серверу ACS. Сервер ACS проверяет учетные данные против базы данных ACS. Если MAC - адрес клиента присутствует в базе данных, сервер RADIUS ACS возвращает успешную аутентификацию к WLC, и клиент будет предоставленным доступом к WLAN.

Используйте CLI для Настройки фильтра MAC на WLC

Этот документ ранее обсудил, как использовать GUI WLC для настройки фильтров MAC. Можно также использовать CLI для настройки фильтров MAC на WLC. Можно использовать эти команды для настройки фильтра MAC на WLC:

- Выполните **команду config wlan mac-filtering enable wlan_id** для включения фильтрации по MAC-адресам. bEnter **команда show wlan**, чтобы проверить, что вам включили фильтрацию по MAC-адресам для WLAN.
- **команда config macfilter add**:**Команда config macfilter add** позволяет вам добавить macfilter, интерфейс, описание, и т.д.Используйте **команду config macfilter add** для создания записи фильтра MAC на контроллере WLAN Cisco. Используйте эту команду для добавления клиента локально к беспроводной локальной сети на контроллере WLAN Cisco. Этот фильтр обходит процесс Проверки подлинности RADIUS.
  config macfilter add MAC_address wlan_id [interface_name] [description] [IP address]
  Пример:Введите статический MAC К СОПОСТАВЛЕНИЮ IP-АДРЕСОВ. Это может быть сделано для поддержки *пассивного клиента*, т.е. тот, который не использует DHCP и не передает незапрашиваемые пакеты IP.>**config macfilter add** 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
- **команда config macfilter ip-address**Команда **config macfilter ip-address** позволяет вам сопоставить существующий фильтр MAC с IP-адресом. Используйте эту команду для настройки IP-адреса в базу данных фильтра локального MAC - адреса:
  config macfilter ip-address MAC_address IP address **Пример:**>**config macfilter add** 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51

Настройте таймаут для отключенных клиентов

Можно настроить таймаут для отключенных клиентов. Клиенты, которые не в состоянии аутентифицироваться три раза во время попыток связаться, автоматически отключены от дальнейших попыток ассоциации. После того, как период ожидания истекает, клиенту разрешают повторить аутентификацию, пока это не привязывает или не отказывает аутентификацию и исключено снова.

Введите **команду config wlan exclusionlist wlan_id timeout** для настройки таймаута для отключенных клиентов. Значение таймаута может быть с 1 до 65535 секунд, или можно войти 0 для постоянного отключения клиента.

Проверка

Используйте эти команды, чтобы проверить, настроен ли фильтр MAC правильно:

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show macfilter summary** — Отображает сводку всех записей фильтра MAC.
- **подробность show macfilter** *<MAC - адрес клиента>* — Подробный показ MAC фильтрует запись.

Вот пример **команды show macfilter summary**:

```
(Cisco Controller) >show macfilter summary MAC Filter RADIUS Compatibility mode.....
Cisco ACS MAC Filter Delimiter..... None Local Mac Filter Table MAC
Address WLAN Id Description ---------------------- ------------- ----------------------------
--- 00:40:96:ac:e6:57 1 Guest (Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57
```

Вот пример **команды show macfilter detail**:

```
(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57 MAC
Address..................................... 00:40:96:ac:e6:57 WLAN
Identifier.................................. 1 Interface Name.................................
mac-client Description..................................... Guest
```

Устранение неполадок

Можно использовать эти команды для устранения проблем конфигурации:

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

- **debug aaa all enable** — Предоставляет отладку всех сообщений AAA.
- **адрес debug mac <***MAC - адрес клиента xx:xx:xx:xx:xx:xx***>** — для настройки отладки MAC, используйте **команду debug mac**.

Вот пример **команды debug aaa all enable**:

```
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657 Wed May 23 11:13:55 2007:
Looking up local blacklist 004096ace657 Wed May 23 11:13:55 2007: User 004096ace657
authenticated Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Returning AAA Error 'Success' (0) for
mobile 00:40:96:ac:e6:57 Wed May 23 11:13:55 2007: AuthorizationResponse: 0xbadff97c Wed May 23
11:13:55 2007: structureSize.............................76 Wed May 23 11:13:55 2007:
resultCode.................................0 Wed May 23 11:13:55 2007:
protocolUsed................................0x00000008 Wed May 23 11:13:55 2007:
proxyState.................................. 00:40:96:AC:E6:57-00:00 Wed May 23 11:13:55 2007:
Packet contains 2 AVPs: Wed May 23 11:13:55 2007: AVP[01] Service-
Type........................... 0x0000000a (10) (4 bytes) Wed May 23 11:13:55 2007: AVP[02]
Airespace / Interface-Name.............. staff-vlan (10 bytes) Wed May 23 11:13:55 2007:
00:40:96:ac:e6:57 processing avps[0]: attribute 6 Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57
processing avps[1]: attribute 5 Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Applying new AAA
override for station 00:40:96:ac:e6:57 Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Override
values for station 00:40:96:ac:e6:57 source: 2, valid bits: 0x200 qosLevel: -1, dscp:
0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1,
rTimeBurstC: -1 vlanIfName: 'mac-client'
```

Когда беспроводной клиент не присутствует в базе данных MAC-адреса по WLC (локальная база данных), или по серверу RADIUS пытается связаться к WLAN, тот клиент будет исключен. Вот пример **команды debug aaa all enable** для неуспешной проверки подлинности MAC:

```
Wed May 23 11:05:06 2007: Unable to find requested user entry for 004096ace657 Wed May 23
11:05:06 2007: AuthenticationRequest: 0xa620e50 Wed May 23 11:05:06 2007:
Callback.....................................0x807e724 Wed May 23 11:05:06 2007:
protocolType.................................0x00000001 Wed May 23 11:05:06 2007:
proxyState..................................... 00:40:96:AC:E6:57-00:00 Wed May 23 11:05:06 2007:
Packet contains 14 AVPs (not shown) Wed May 23 11:05:06 2007: 00:40:96:ac:e6:57 Returning AAA
Error 'No Server' (-7) for mobile 00:40:96:ac:e6:57 Wed May 23 11:05:06 2007:
AuthorizationResponse: 0xbadff7e4 Wed May 23 11:05:06 2007:
structureSize................................28 Wed May 23 11:05:06 2007:
resultCode...................................-7 Wed May 23 11:05:06 2007:
protocolUsed.................................0xffffffff Wed May 23 11:05:06 2007:
proxyState..................................... 00:40:96:AC:E6:57-00:00 Wed May 23 11:05:06 2007:
Packet contains 0 AVPs:
```

Беспроводные клиенты, которые Отклонена Попытка Аутентифицироваться MAC-адресом; Отчёт об Ошибке проверки подлинности Показывает Внутренние ошибки

Когда вы используете ACS 4.1, который работает на Корпоративном сервере Microsoft Windows 2003 года, отклонены клиенты, которые пытаются аутентифицироваться MAC-адресом. Когда клиент AAA передает Service-Type=10 значение атрибута к AAA-серверу, это происходит. Это вызвано тем, что идентификатора ошибки Cisco CSCsh62641 (только зарегистрированные клиенты). Клиенты AAA, на которых влияет этот дефект, включают WLC и коммутаторы тот Обход Проверки подлинности MAC использования.

Способы разрешения проблемы таковы:

- Понизьте до ACS 4.0.или
- Добавьте MAC-адреса, которые будут аутентифицироваться на Защите доступа к сети (NAP) под внутренней таблицей MAC-адресов DB ACS.

Не способный добавить фильтр MAC с помощью GUI WLC

Это может произойти becaue идентификатора ошибки Cisco CSCsj98722 (только зарегистрированные клиенты). Ошибка исправлена в 4.2 выпусках кода. Если вы - рабочие версии ранее, чем 4.2, можно обновить микропрограммное обеспечение к 4.2 или использовать эти два обходных пути для этой проблемы.

- Используйте CLI для настройки Фильтра MAC с этой командой:
  config macfilter add <MAC address> <WLAN ID#> <Interface>
- От веб-GUI контроллера выберите **Any WLAN** под Вкладкой Безопасность и введите MAC-адрес, который будет фильтроваться.

Тихий клиент, не размещенный в выполненное состояние

Если требуемый DHCP не настроен на контроллере, AP изучают IP-адрес беспроводных клиентов, когда беспроводные клиенты отсылают первый пакет IP или ARP. Если беспроводные клиенты являются пассивными устройствами, например, устройствами, которые не инициируют связь, то AP не в состоянии изучать IP-адрес беспроводных устройств. В результате контроллер ждет десять секунд клиента для передачи пакета IP. Если нет никакого ответа от пакета от клиента, то контроллер отбрасывает любые пакеты пассивным беспроводным клиентам. Эта проблема задокументирована в идентификатор ошибки Cisco CSCsq46427 (только зарегистрированные клиенты)

Как рекомендуемый обходной прием для пассивных устройств как принтеры, беспроводной PLC качает и т.д, необходимо установить WLAN для фильтрации по MAC-адресам и иметь замену AAA, проверенную, чтобы позволить этим устройствам быть связанными.

Фильтр MAC - адреса может быть создан на контроллере, который сопоставляет MAC-адрес беспроводного устройства к IP-адресу.

Примечание: Это требует, чтобы фильтрация MAC-адреса была включена на конфигурации WLAN для безопасности уровня 2. Это также требует, AAA быть включенным в параметрах настройки усовершенствования конфигурации WLAN.

От CLI введите эту команду для создания Фильтра MAC - адресов:

```
config macfilter add <STA MAC addr> <WLAN id> [interface name] [description] [STA IP address]
```

Например:

```
config macfilter add 00:01:02:03:04:05 1 my_interface "Zebra Printer"
192.168.1.1
```

Дополнительные сведения

- Пример конфигурации ACL на контроллере беспроводных LAN
- Примеры настройки проверки подлинности на контроллерах беспроводной сети
- Пример конфигурации сетей VLAN на контроллерах беспроводной LAN
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.1
- Страница технической поддержки беспроводной технологии
- Cisco Systems – техническая поддержка и документация