Unified Wireless Network: клиенты выдал устранения неполадок

Содержание

Введение

Среда радиочастот (RF) является сложной и динамичной. Различные факторы, как должны полагать, создают хорошую Беспроводную среду. В этом документе поясняются различные проблемы, с которыми можно столкнуться при подключении беспроводного клиента в среде унифицированной беспроводной сети Cisco, а также шаги, которые необходимо предпринять для диагностики и решения этих проблем.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Решение для Унифицированной беспроводной связи Cisco
- Контроллеры беспроводной локальной сети Cisco (WLC) базовые конфигурации GUI

Используемые компоненты

Этот документ применим ко всем устройствам, которые участвуют в унифицированной среде Cisco, но не ограничен определенными версиями программного и аппаратного обеспечения.

Условные обозначения

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

Общие сведения

В Унифицированной среде Cisco WLC принимает центральную роль. Это управляет всей беспроводной сетью. Облегченные точки доступа (LAP), которые служат беспроводным клиентам, регистрируют себя к WLC и загружают полную конфигурацию от WLC. Первый шаг должен проверить, зарегистрирован ли LAP к WLC. Нажмите меню wireless от GUI WLC и проверку, если LAP перечислен на странице.

Проблемы конфигурации

Для успешного беспроводного соединения важно, что конфигурация на WLC реализована правильно. В этом разделе описываются некоторые обычно замеченные проблемы конфигурации.

Несоответствие SSID

Клиент использует его SSID, чтобы определить и связаться к беспроводной сети, поэтому гарантируйте, что SSID настроен тождественно на WLC и клиенте. Чтобы проверить, что SSID, настроенный на WLC, нажимает **страницу WLANs**. Нажмите соответствующий *WLAN* и проверьте *SSID*, настроенный под *Вкладкой Общие*.

Примечание: *При сравнении сетевых имен учитывается регистр символов.* Если вы удаляете и воссоздаете WLAN, это могло бы помочь беспроводному клиенту связываться к WLAN.

Несоответствие безопасности

Конфигурации безопасности должны совпасть между WLC и клиентом. Если типом проверки подлинности является Статический ключ WEP, проверьте если соответствующий ключ шифрования / ключевой индекс на соответствиях WLC тот из клиента. Если тип проверки

подлинности является 802.1x или WPA, гарантируйте, что тип проверки подлинности / размер ключа шифрования совпадает между клиентом и WLC. Для получения дополнительной информации о том, как настроить WLC и клиента для различных решений по обеспечению безопасности, обратитесь к Аутентификации на Примерах конфигурации Контроллеров беспроводной локальной сети.

Примечание: Решения для безопасности уровня 2, такие как WPA или 802.1x, не могут использоваться для WLAN, настроенного с решениями для безопасности уровня 3, такими как web-аутентификация или passthrough. Для получения дополнительной информации о совместимых решениях по обеспечению безопасности обращаются к Уровню 2 Контроллера беспроводной локальной сети и Матрице совместимости безопасности уровня 3.

Отключенный WLAN

Для успешного беспроводного соединения соответствующий WLAN должен быть активным на WLC. По умолчанию статус WLAN не включен на WLC. Для активации WLAN нажмите меню **WLAN** в WLC. Список WLAN настроен на показах WLC. Нажмите WLAN, который настроен с SSID, к которому клиент хочет связаться. Под Вкладкой Общие **WLAN> страница Edit**, установите флажок статуса.

Неподдерживаемые скорости передачи данных

Для определенного стандарта, или 802.11b/g или 802.11a, можно дополнительно установить определенные скорости передачи данных столь же обязательные и другие скорости передачи данных, как поддерживается или отключено на WLC. Для успешной ассоциации беспроводной клиент должен поддержать скорости передачи данных, которые настроены как обязательные на WLC. Чтобы проверить, что скорости передачи данных, настроенные на WLC, нажимают **меню Wireless** на GUI WLC и проверяют скорости передачи данных, настроенные под **802.11b/g/n> Сеть или 802.11a/n> Параметр Network**, который появляется на левой стороне страницы. Проверьте страницу технической поддержки клиентского поставщика для определения этого. При обновлении драйвера клиента это может помочь клиенту поддерживать скорости требуемых данных.

Примечание: Для лучшего подключения, набор самая низкая скорость передачи данных к **обязательному** на WLC и другие скорости передачи данных к **поддерживаемому**.

Отключенные клиенты

На WLC существует опция для ручного отключения клиентов. Эта функция помогает препятствовать тому, чтобы посторонние клиенты пытались обратиться к сети. Проверьте, найден ли MAC-адрес клиента, который неспособен связаться, в Отключенном списке Клиентов, и, если так, удалите его. Можно найти список отключенных клиентов при нажатии **Disabled Clients option** в соответствии с **Меню системы безопасности** в GUI.

Примечание: Клиенты могут быть запрещенной ассоциацией к сети, если они не соблюдают Клиентскую политику Исключения по умолчанию, настроенную на WLC. Для получения дополнительной информации о Клиентской политике Исключения обратитесь к разделу Политики Исключения Клиента Настройки руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 4.2.

Радио-преамбулы

Радио-преамбула (иногда названный заголовком) является разделом данных во главе пакета, который содержит информацию, в которой нуждаются беспроводные устройства, когда они передают и получают пакеты.

Некоторые клиенты не поддерживают **короткую преамбулу**, таким образом, они не могут соединиться с WLAN, которому включили **короткую преамбулу**. Короткие преамбулы улучшают производительность пропускной способности, таким образом, им включают по умолчанию на WLC. Для отключения **короткой преамбулы** нажмите **меню Wireless** GUI WLC. Затем нажмите **802.11b/g> сетевое** меню на левой стороне. *Снимите* **короткий** флажок **преамбулы**.

Функции Cisco Properietary - выходят с клиентами третьей стороны

. Если устройства клиента устройствами не марки CISCO, отключая некоторые результаты специальных средств Cisco в успешном подключении, которые неспособны соединиться с сетью являются, для списка функций, что поддержки клиентов, свяжитесь с поставщиком стороннего устройства клиента.

Это некоторые важные специальные средства:

- **IE aironet** — IE Aironet содержит информацию, такую как название точки доступа, загрузка, количество связанных клиентов, и так далее отосланных точкой доступа в маяке и тестовых ответах WLAN. Клиенты CCX используют эту информацию для выбора лучшей точки доступа, с которой можно связаться.
- **MFP** — Защита кадра управления является функцией, представленной для обеспечения целостности кадров управления, таких как de-аутентификация, разъединение, сигналы-маяки, и зондирует в чем точку доступа, защищает кадры управления, которые это передает, когда это добавляет Информационный элемент Message Integrity Check (IE MIC) к каждому кадру. Любая попытка, предпринятая злоумышленниками для копирования, изменитесь или воспроизведите кадр, лишает законной силы MIC, который вызывает любую точку доступа получения, которая настроена, чтобы обнаружить кадры MFP, сообщить о несоответствии.Эти опции активированы по умолчанию для любого WLAN, который создан на WLC. Для отключения этих опций нажмите меню **WLAN** в WLC. Список WLAN настроен на показах WLC. Нажмите WLAN, к которому клиент хочет связаться. Под **Вкладкой Дополнительно WLAN> страница Edit**, снимите флажки, которые соответствуют **IE Aironet и MFP**.
- **Радио-Преамбулы** — радио-преамбула (иногда названный заголовком) является разделом данных во главе пакета, который содержит информацию, что беспроводное устройство и устройства клиента должны передать и получить пакеты. Можно установить радио-преамбулу в длинный или короткое, в зависимости от которого установка поддерживается на беспроводном клиенте.
- **Преобразование Инкапсуляции Ethernet** — Когда беспроводное устройство получает пакеты данных, которые не являются 802.3 пакетами, беспроводное устройство, должно использовать метод преобразования инкапсуляции для форматирования пакетов к 802.3. Вот два метода преобразования:802.1H: Этот метод предоставляет оптимальную производительность для беспроводных продуктов Cisco Aironet. 802.1H настройка по умолчанию.RFC1042: Используйте эту установку для обеспечения совместимости оборудованием Беспроводной связи aironet не-Cisco. RFC1042 не предоставляет преимущества совместимости 802.1H, но используется другими изготовителями

беспроводного оборудования.

- **таймаут квитирования wpa** — Некоторым поставщикам нужны дольше wpa таймауты квитирования. Можно использовать **команду dot11 wpa handshake timeout** для изменения таймаута квитирования wpa.
- **ssid** — Некоторые поставщики требуют, чтобы был передан ssid. Для широковещательной передачи ssid включите *гостевой режим* под конфигурацией ssid.

Проблемы IP-адреса

Беспроводным клиентам нужны действительные IP - адреса для передачи с остатком сети.

Контроллер ведет себя как маршрутизатор со вспомогательным IP - адресом. Т.е. это заполняет IP-адрес шлюза и одноадресно передает его к серверу DHCP через динамический интерфейс, на котором установлен клиент. Так знайте, что DHCP, snooping на коммутаторах, по умолчанию, заблокирует эти пакеты DHCP на ненадежных портах.

В возвращенном предложении DHCP контроллер заменяет IP-адрес DHCP-сервера своим виртуальным IP-адресом. Причина, которую это делает это вызвано тем, что, когда Windows перемещается между AP, первая вещь, которую это делает, попытаться связаться с сервером DHCP и возобновить его адрес.

С адресом сервера DHCP 1.1.1.1 (который является типичным виртуальным IP - адресом на контроллере), контроллер может перехватить тот пакет и обмануть Windows. Это также, почему виртуальный IP - адрес является тем же на всех контроллерах. Если ноутбук с ОС Windows будет перемещен к точке доступа на другом контроллере, то он попробует обратиться к виртуальному интерфейсу контроллера. Из-за события mobility и передачи контекста, новый контроллер, к которому Windows - клиент переместился уже, имеет всю информацию для обманывания Windows снова.

Если вы хотите использовать внутренний сервер DHCP, все, что необходимо сделать, помещен управление IP-адресами как сервер DHCP на динамическом интерфейсе, который вы создаете для подсети. Затем этот интерфейс нужно назначить беспроводной локальной сети (WLAN). Причина, по которой контроллеру нужен IP-адрес в каждой подсети, — это возможность заполнить адрес шлюза DHCP в запросе DHCP.

Мы видим много DHCP / проблемы IP-адреса. Вот причины, и шагает для решения этих вопросов:

1. Если тип настроенной аутентификации является одним из решений для безопасности уровня 2, таких как 802.1x или WPA, клиент должен успешно аутентифицироваться для получения действительного IP - адреса. Первая проверка, если успешно аутентифицируется клиент.**Примечание:** Исключение - то, если клиент настроен для решений для безопасности уровня 3, таких как web-аутентификация, или веб-транзитному клиенту назначают IP-адрес перед аутентификацией.
2. Каждый WLAN, определенный на WLC, сопоставлен с динамическим интерфейсом WLC, который настроен с VLAN, которая принадлежит уникальной подсети. Клиенты, которые связываются к этому WLAN, являются назначенными IP - адресами от интерфейсной подсети VLAN. Проверьте, определены ли IP-подсеть и шлюз этого WLAN на сервере DHCP для клиента для получения IP-адреса на этой подсети. См. документацию соответствующего поставщика для настройки сервера

DHCP.**Примечание:** Как предпосылка, проверьте, достижим ли сервер DHCP от WLC и если включен сервис DHCP.

3. Удостоверьтесь, что IP-адрес сервера DHCP определен правильно в интерфейсе WLC, который сопоставлен с WLAN. Для проверки этого нажмите **меню Controller** в GUI. Нажмите меню **Interfaces** на левой стороне и проверьте поле **сервера DHCP**. На той же странице проверьте, что интерфейс сопоставлен с *физическим портом*, который подключен и активен. Для устранения проблем связанных проблем DHCP использование**, которое пакет debug dhcp** команд **включает** и **сообщение debug dhcp, включает** на WLC.**Примечание:** Можно также настроить WLC как сервер DHCP. Для получения дополнительной информации о том, как настроить DHCP, разъединяют на WLC, обращаются к Использованию GUI Настроить раздел DHCP руководства по конфигурированию контроллера Cisco Wireless LAN документа, Выпуска 5.0.
4. Прокси DHCP включен по умолчанию на WLC. WLC одноадресно передает пакет к серверу DHCP, настроенному на интерфейсе WLAN или самом WLAN. Если сервер DHCP не поддерживает поведение прокси Cisco DHCP, отключите прокси DHCP на WLC. Для получения дополнительной информации о том, как отключить Прокси DHCP на WLC, обратитесь к разделу Прокси DHCP Настройки руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 5.2.
5. WLC обычно соединяется с проводной сетью через коммутатор. Проверьте, настроены ли порты коммутатора, которые связаны с WLC и сервером DHCP, как транк и что соответствующие VLAN позволены на тех портах. Для получения дополнительной информации о том, как настроить коммутаторы Cisco, обратитесь к Настраиванию порта Коммутатора уровня 2 который Подключения к WLC как раздел Магистрального порта Гостевого WLAN документа и Внутреннего WLAN с помощью Примера конфигурации WLC.
6. Статическим клиентам не разрешают связаться к WLAN если **Addr DHCP. Поле Assignment** включено для WLAN. Эта опция требует этого всего клиенты, которые связываются к этому WLAN, должен получить IP-адреса через DHCP. Чтобы проверить, включена ли эта опция, нажмите меню WLAN в GUI WLC. Список WLAN настроен на показах WLC. Нажмите соответствующий WLAN. Перейдите **к Вкладке Дополнительно** и найдите поле **назначения адреса DHCP**.
7. Некоторые серверы DHCP, такие как Межсетевой экран Cisco PIX, не поддерживают сервисы ретрансляции DHCP. Они принимают только широковещательные пакеты DHCP, не любые одноадресные пакеты от агента ретрансляции DHCP, поэтому гарантируйте, что клиенты DHCP напрямую подключаются к интерфейсу, на котором включен сервер.**Примечание:** Проверьте соответствующий документ поставщика для поддержки ретранслятора DHCP.

Проблемы клиентов

Одинаково важно, чтобы вещи существовали на клиентской стороне. Выполните они проверяют клиентскую сторону:

1. Иногда, клиентская карта не распознана компьютером. В этом случае попробуйте карту на другом слоте. Если это не работает, попробуйте его на другом компьютере. Для получения дополнительной информации о проблемах в установке обратитесь к Разделу устранения проблем документа Cisco Aironet 340, 350, и Руководство по

установке и конфигурированию Клиентских адаптеров беспроводной сети CB20A для Windows.**Примечание:** Удостоверьтесь, что беспроводная карта совместима с операционной системой, которая установлена на машине. Это может быть проверено из таблицы данных клиентской карты.

2. Проверьте, установлен ли клиент должным образом на машине. Статус клиентской карты может быть проверен с экрана **Windows Device Manager**. Ищите сообщение, которое читает, *"Это устройство работает должным образом".* Если это не, это указывает, что драйверы не установлены должным образом. Попытайтесь деинсталлировать драйвер и повторно установить драйверы на машине. Для удаления драйверов щелкните правой кнопкой мыши беспроводной адаптер с экрана Device Manager и нажмите **Uninstall**. Для получения дополнительной информации о том, как повторно установить клиентский адаптер, обратитесь к Установке раздела Клиентского адаптера документа Cisco Aironet 340, 350, и Руководство по установке и конфигурированию Клиентских адаптеров беспроводной сети CB20A для Windows.**Примечание:** При использовании ACU для настройки клиентской карты, удостоверьтесь, что радио не отключено на ACU. Кроме того, проверьте, включен ли статус карты при **Сетевом подключении** на Windows Control Panel.**Примечание:** Используйте только одно программное обеспечение соискателя для беспроводной карты. Всегда рекомендуется использовать предоставленного поставщиками соискателя для карты. Как опция secondary, можно или использовать ту, предоставленную поставщиком ПК или WZC, предоставленным Windows.**Примечание:** Выполните эти шаги для отладки WZC:Используйте **netsh ras отслеживание набора * выполненная** команда для включения отладки WZC.Используйте **netsh ras отслеживание набора * отключенная** команда для выключения отладки WZC.Журналы записаны в *C:\Windows\tracing*. *eapol.log*, *rastls.log*, и *wzctrace.log* являются самыми важными журналами.**Примечание:** См. беспроводное Диагностирование и устранение проблем для получения дополнительной информации.
3. Конфигурация на клиенте должна совпасть с конфигурацией WLC. Это в основном обращается к SSID и конфигурации безопасности на клиенте. При использовании служебной программы Cisco для настройки клиента, обратитесь к Использованию Менеджера Профиля раздел документа Cisco Aironet 340, 350, и Руководство по установке и конфигурированию Клиентских адаптеров беспроводной сети CB20A для Windows.
4. Если вы неспособны передать данные, даже после успешной связи с беспроводным устройством, попытайтесь отключить все другие адаптеры, а также те из VPN и соединенных проводом адаптеров. Если существует несколько беспроводных адаптеров в машине, отключите другие адаптеры для предотвращения конфликтов между ними.
5. При обнаружении проблем с подключением только с одиночным клиентом попытайтесь обновить драйверы и микропрограммное обеспечение того клиента. Если вы находите проблемы с подключением с большинством клиентов и исключение других проблем примите решение обновить WLC.
6. Гарантируйте, что устройства, т.е. клиент и WLC, являются Wi-Fi, который, как сертифицируют, избегал любых проблем совместимости, отнесенных к безопасности и операциям.
7. При использовании машины Windows удостоверьтесь, что вы установили все последние патчи безопасности или заплаты, доступные от Microsoft. При использовании утилиты Windows - клиента удостоверьтесь, что вы установили

последнее исправление, доступное от Microsoft.

8. Некоторые клиенты медленно отвечают на Аутентификацию eap. Это приводит к таймаутам на WLC, и можно получить это сообщение об ошибках на WLC:

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station <Mac address of the client>
```

В ответ на это сообщение увеличьте стоимости таймаута EAP на WLC для обеспечения достаточного времени для клиента для аутентификации. Используйте эти команды для регулировки таймеров EAP на WLC:

```
config advanced eap identity-request-timeout <1-120 secs>
config advanced eap identity-request-retries <1-20>
 !--- Specifies the amount of time and the maximum number of times the WLC attempts to send an EAP identity request to wireless clients. config advanced eap request-timeout <1-120>
config advanced eap request-retries <1-20>
 !--- Specifies the amount of time and the maximum number of t imes the WLC attempts to send EAP request to the Radius Server . config advanced eap eapol-key-timeout <1-5>
config advanced eap eapol-key-retries <0-4>
 !--- Specifies the amount of time and the maximum number of times the WLC attempts to negotiate the encryption key.
```

Проблемы RF

Радиочастотная помеха является одной из основных причин для ненадежного соединения. Интерференция может быть вызвана смежными сетями 802.11 или другими источниками, такими как Микроволновые печи или беспроводные телефоны, которые работают в той же самой частоте. Интерференция, вызванная смежными сетями 802.11, имеет два типа:

- **Помехи от соседних каналов:** Когда точки доступа, зона уверенного приема которых накладывается, настроены в том же канале или каналах с перекрывающимися частотами, это вызывает проблемы с подключением для клиентов в области перекрытия зон обслуживания. Во избежание этой проблемы, или изменить номер канала на не-Перекрытый канал или переместить точку доступа дальше так, чтобы не накладываются их зоны уверенного приема. Например, в 802.11b/g, сетевые каналы 1, 6, и 11 являются не-Перекрытыми каналами.
- **Помеха от соседнего канала:** Когда точки доступа размещены слишком близкие друг к другу или используют уровни мощности высокой производительности, это вызывает интерференцию, даже когда точки доступа настроены на не-Перекрытых каналах. Уменьшите питание точки доступа устранить эту проблему.**Примечание:** Не-Перекрытые каналы также называют соседними каналами, который объясняет *помеху от соседнего канала* названия.

Используйте анализаторы спектра для определения местоположения источников помех, таких как микроволновые печи или беспроводные телефоны, которые работают в диапазоне на 2.4 ГГц или устройствах, которые работают в диапазоне на 5 ГГц. Удалите источники помех, как только они определены. Также можно изменить стандарт, на который беспроводная сеть воздействует, например, от 802.11b/g до 802.11a для предотвращения интерференции.

Другим важным аспектом для эффективной связи RF является уровень сигнала. Сила слабого сигнала приводит к нестационарному соединению. Препятствия, такие как стены, металлы, поглощают и отражают энергию RF, которая уменьшает уровень сигнала. Увеличьте питание до требуемого уровня на точке доступа для предоставления подробной страховой защиты. Можно также использовать высокие коэффициенты усиления антенны

для расширения диапазона и уровня сигнала, но гарантировать, что это - FCC, согласилось работать с устройством.

Примечание: Signal to Noise Ratio (SNR), который является различием между уровнем сигнала и шумом RF (радиочастотный сигнал или энергия из других источников, которая действует в той же самой частоте в качестве беспроводной сети), является ключевым фактором для измерения качества ссылки. Более высокий SNR указывает на хорошее качество канала, которое приводит к более быстрой передаче данных. Минимальное значение указывает на низкое качество, которое приводит к прерывистому подключению или низкой производительности. Беспроводной Пакет анализаторы/узел рассматривают программное обеспечение, может показать вам SNR и пропускную способность в конкретном расположении.

В унифицированной среде Cisco существует понятие под названием Управление радиоресурсами (RRM), внедренное на WLC. RRM является программным обеспечением, встроенным в контроллер, который действует как встроенный инженер RF для последовательного обеспечения управления RF в реальном времени беспроводной сети. Это автоматически заботится обо всех упомянутых проблемах RF. Для получения дополнительной информации о RRM обратитесь к разделу Управления радиоресурсами Настройки руководства по конфигурированию контроллера Cisco Wireless LAN документа, Выпуска 5.0.

Сообщения об ошибках

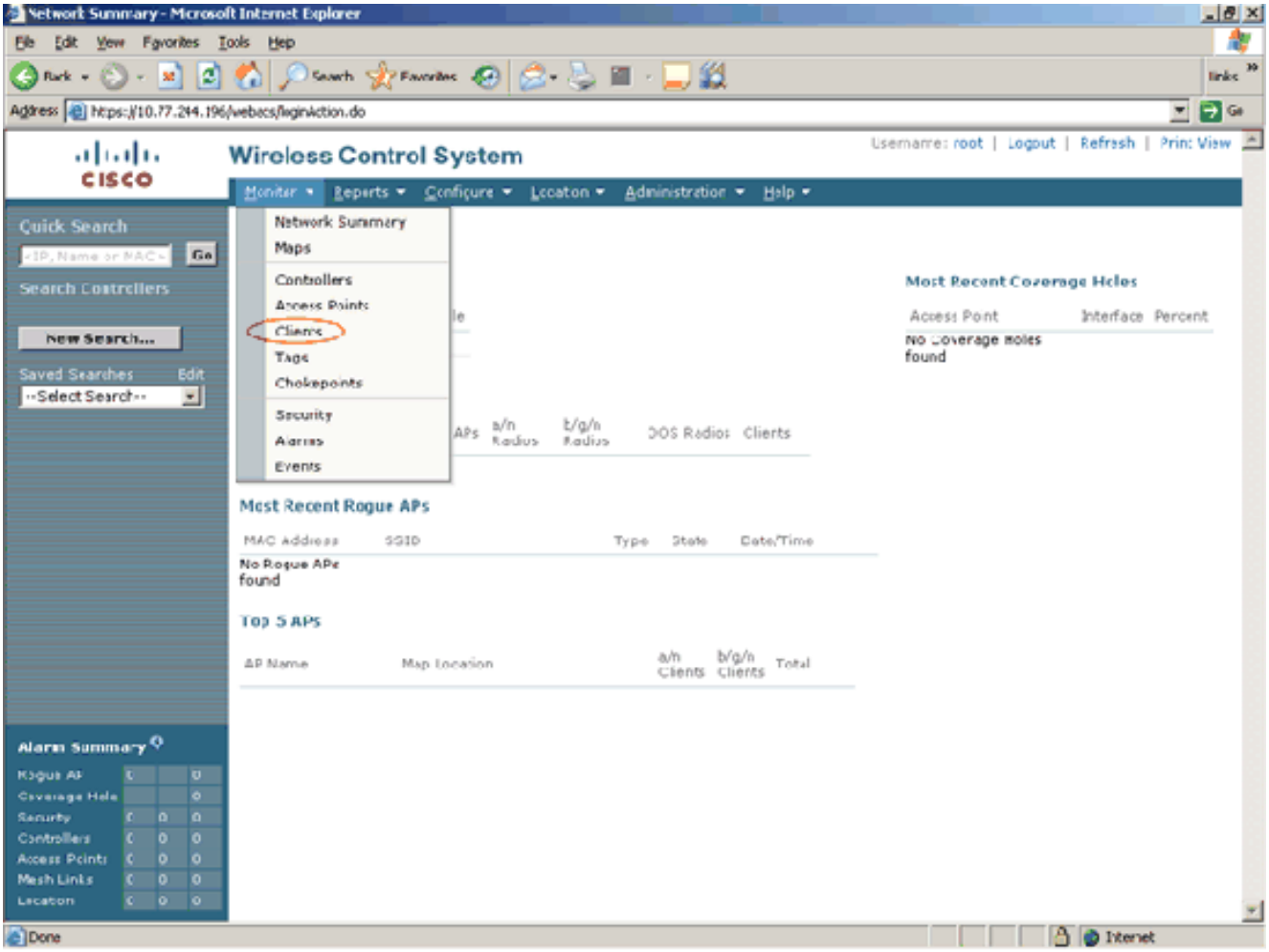
В условиях курса клиентского подключения можно получить несколька сообщений об ошибках, и на WLC и на клиентских сторонах.

- **Клиент или неспособен получить IP-адрес или задержку обнаружения получения IP-адреса через DHCP. Debug dhcp на контроллере указывает на это:**
  `Sun Nov 9 22:09:05 2008: <mac address of the client> DHCP processing DHCP NAK` *NAK DHCP* обычно передается сервером DHCP для указания на попытку клиента получить IP-адрес от подсети, до которой это не принадлежит. Это обычно происходит, когда клиент перемещается от одного WLC до другого, где тому же WLAN назначают другая VLAN.Настройте прокси DHCP на WLC для обеспечения исправления для этого.

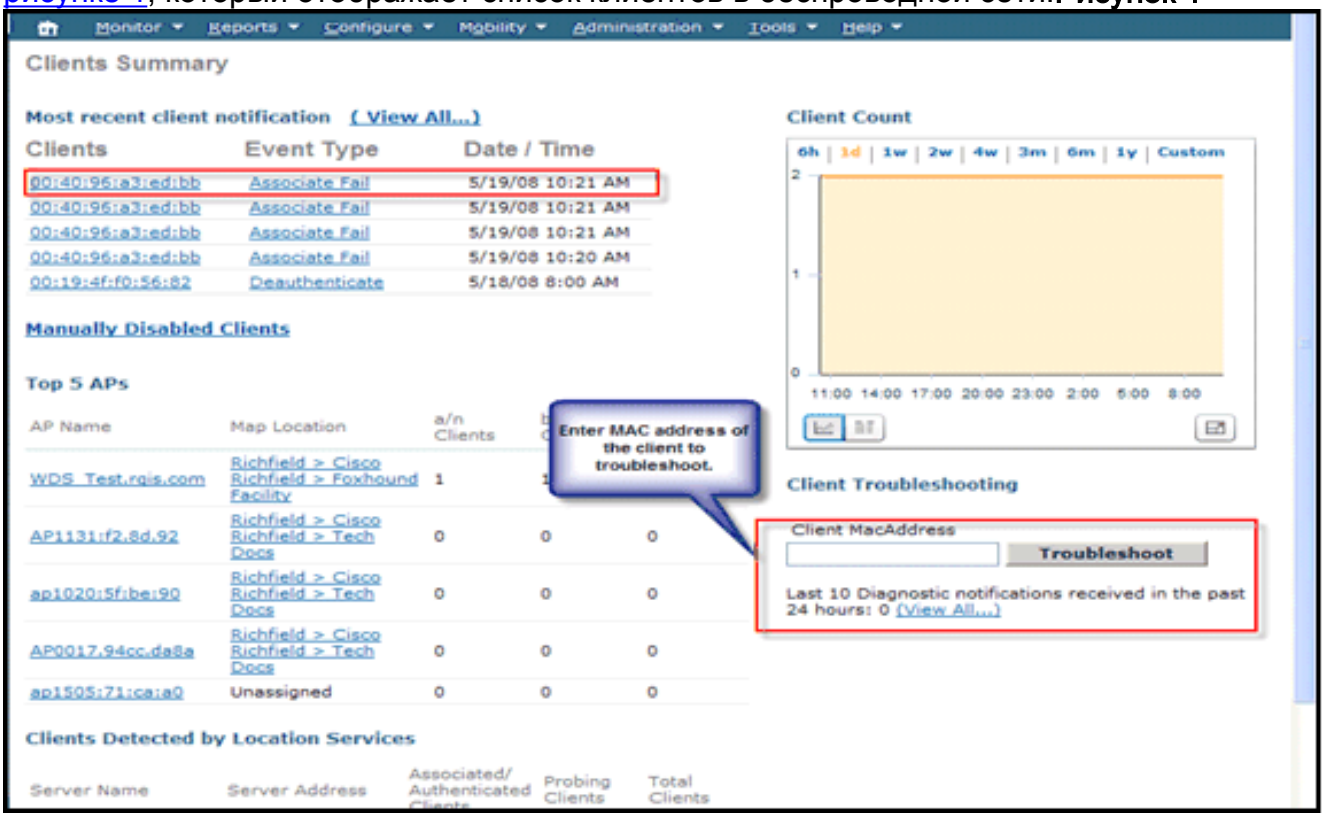
Устранение проблем клиентов выдал с WCS

WCS может использоваться для решения связанных с клиентом проблем в Беспроводной среде. Это делает это с помощью Средства устранения проблем, встроенного в WCS. Для устранения проблем клиента через WCS пользователи должны выполнить эти шаги

1. От страницы WCS Dashboard нажмите меню **Monitor** и выберите **Clients** из списка.

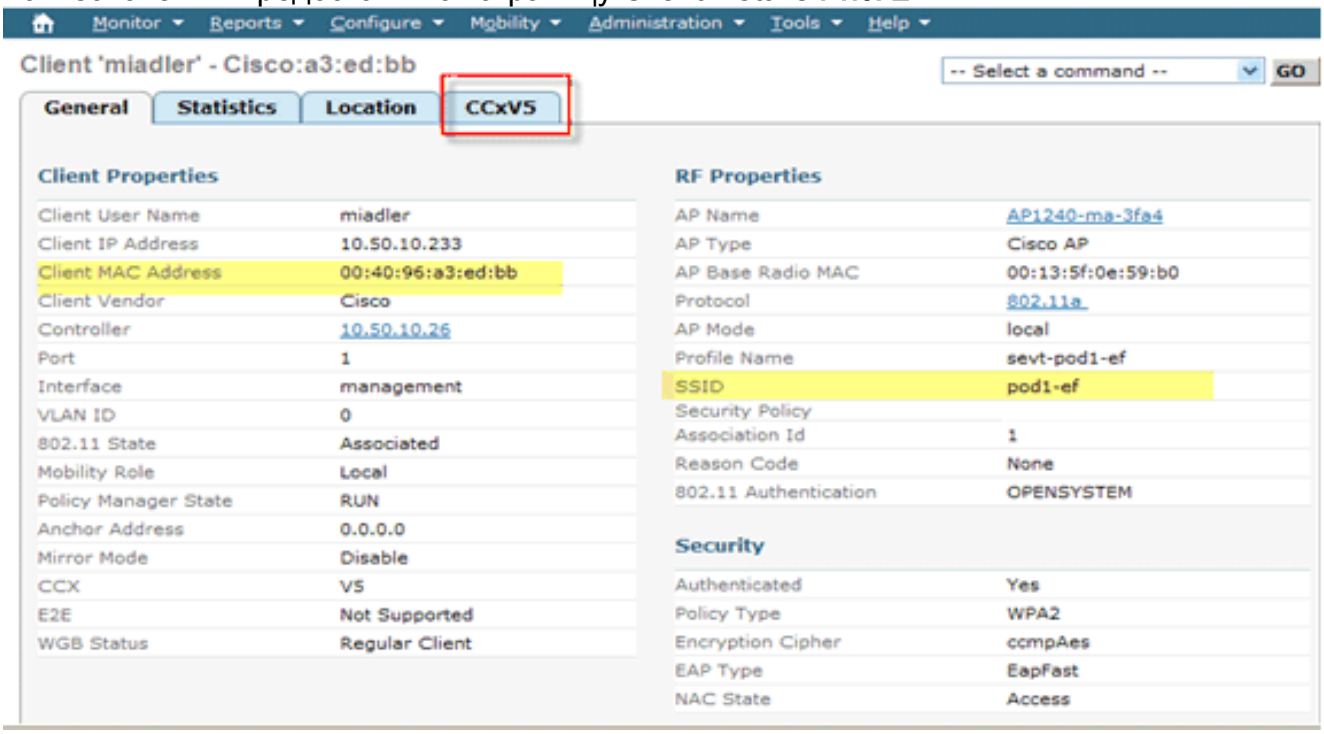


2. Это переводит Клиентскую Сводную страницу в рабочее состояние как показано на рисунке 1, который отображает список клиентов в беспроводной сети.**Рисунок 1**



3. Нажмите клиента для получения подробных данных, таких как SSID или метод аутентификации конкретного клиента. Рисунок 2 показывает пример этого. Диалоговое окно **Troubleshoot** в правой нижней стороне Клиентской Сводной страницы, показанной

на рисунке 1, позволяет пользователям входить в MAC-адресе устройства для устранения проблем. Это приносит вам к странице Troubleshooting Tool как показано на рисунке 3. После идентификации и выбора клиента для устранения проблем пользователям предоставляют страницу Client Details:**Рис. 2**



Устранение проблем WEP

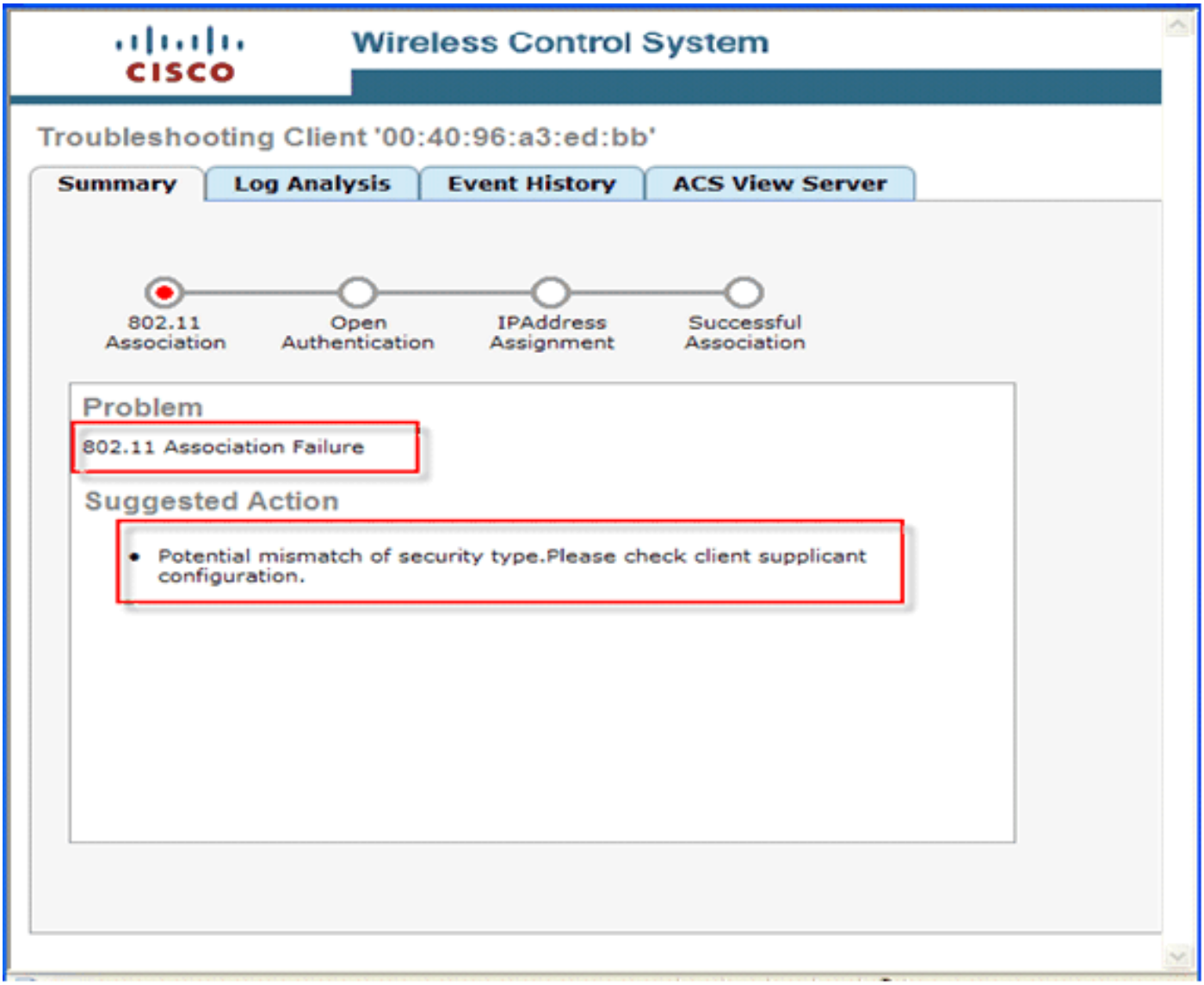
Устаревших беспроводных клиентов, которые все еще используют механизмы обеспечения безопасности WEP, часто трудно устранить неполадки. Выполните они проверяют клиента и AP:

- Длина ключа WEP (и основная несогласованность)
- Индекс ключа WEP (и несоответствия конфигурации)
- Сконфигурированный способ аутентификации (открываются по сравнению с общим ключом),

Опознавательное несоответствие

Несмотря на то, что перехват пакетов может быть утомительным процессом, инструмент диагностики клиентов WCS может легко выручить точку, где существует проблема. Часто, этот небольшой “совет” - то, что уменьшает время устранения проблем. Рисунок 2 показывает **средство устранения проблем WCS**. Как представлено на рисунке, проблематичный этап определяется и визуализируется, который готовит почву для подробного анализа.

Рис. 3



Несоответствие индекса КЛЮЧА WEP

В целом можно настроить до 4 Ключей WEP на клиенте и AP. Один из ключей выбран в качестве ключа передачи. Это должно совпасть между клиентом и AP. Например, если Ключевые 2 выбраны в качестве ключа передачи на клиенте, это должно совпасть с Ключевыми 2 на AP, но AP может иметь другой ключ, чем ключ передачи. Другая проблема часто - это: клиентские и поставщики инфраструктур интерпретируют спецификации по-другому, который вызывает другие реализации в продукте. Одним общим примером является использование ключевых индексов от 0 до 3 по сравнению с ключевыми индексами от 1 до 4. Это может привести к попыткам сбоя подключения и несовпадению конфигурации. В той точке обратите пристальное внимание на “Ключевой ID”, поданный в пакете, декодируют, который говорит, является ли это основной причиной проблемы.

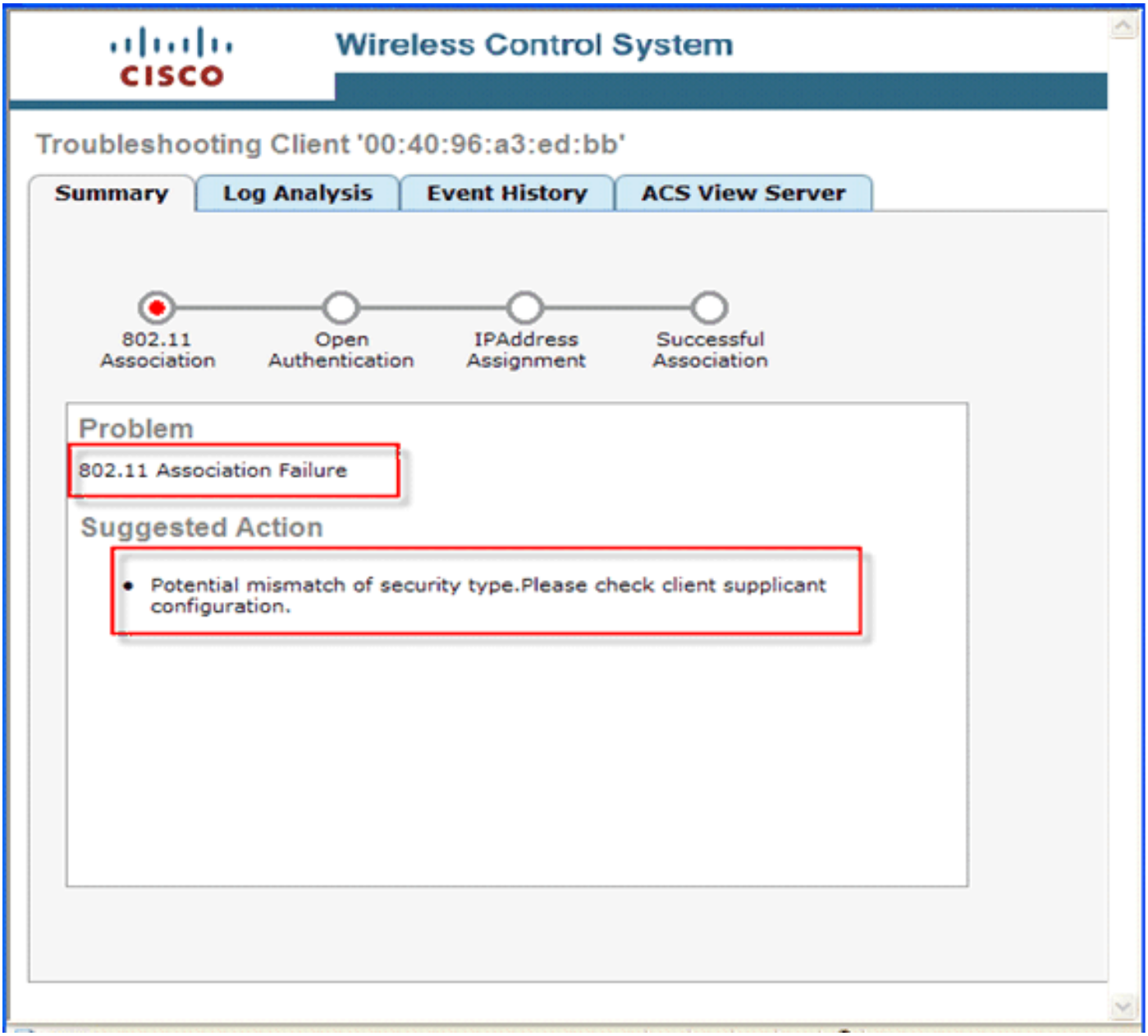
Устранение проблем WPA-PSK

Устранение проблем WPA-PSK подобно WEP во многих отношениях. Большинство неудачных попыток происходит из-за неверных конфигураций в ключе. С Инструментом диагностики клиентов WCS администраторы могут собрать журналы транзакции WPA. Журналы, как выделено ниже, отображаются, где потенциальная проблема может быть *(неправильная конфигурация предварительного общего ключа на клиенте в этом конкретном примере)* и получена из вкладки **Log Analysis** инструмента диагностики клиентов

WCS. Установите WLAN с WPA-PSK как политика безопасности уровня 2 и настройте клиентского соискателя с неправильным PSK. Это журналы ключей PSK неверна настроенного в событиях:

```
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received.
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client.
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting requires 802 1x authentication.
<TIMESTAMP> INFO 10.10.10.2
   Client moved to associated state successfully.
<TIMESTAMP> ERROR 10.10.10.2
   802.1x authentication message received, static dynamic wep supported.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
```

Client 802.1x authentication failure exceeded the limit. <TIMESTAMP> ERROR 10.10.10.2 **EAPOL-key has possible incorrect psk configuration**.

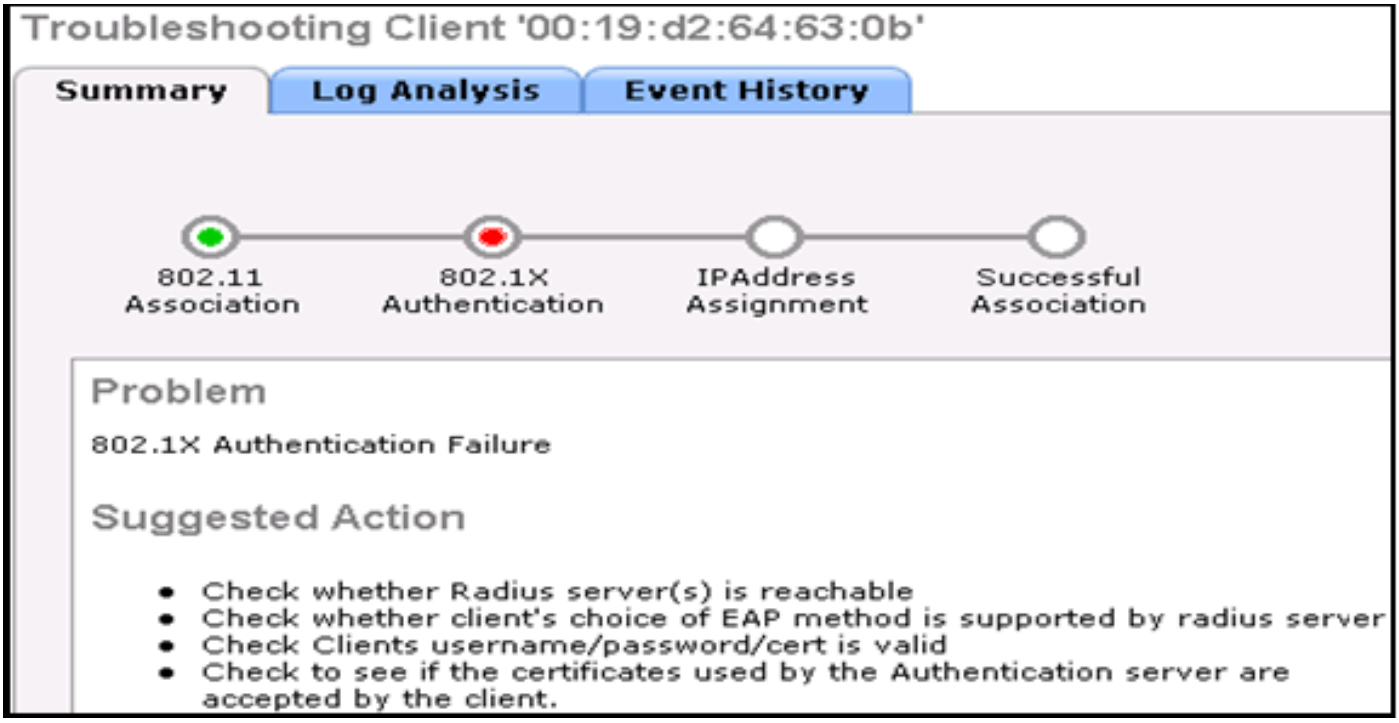


Устранение проблем 802.1X

Поскольку принятие WLAN становится распространяющимся, устаревшие клиенты постепенно сокращают; 802.1x является направлением для большинства будущих развертываний. Может быть множество связанных с неверной конфигурацией проблем в цепочке (клиент <> AP <> сеть WLC <> L2/L3 <> AAA-сервер). Здесь предполагается, что вещи существуют между WLC и AAA-сервером. Проблемы, которые возникают между соискателем (клиент) и AAA-сервером обычно, являются ими:

- Неправильный тип EAP
- Неправильные учетные данные / просроченные сертификаты
- Неправильный EAP внутренний метод

На клиентской стороне модифицируйте учетные данные пользователя при параметрах безопасности; например, введите неправильный пароль и повторно выполните тот же тест. Средство устранения проблем точно указывает, где проблема заключается, а также предлагаемое действие.



Нажмите вкладку **Log Analysis** на рисунке, показанном выше, и проверьте журналы для любой индикации относительно неуспешной аутентификации 802.1x.

```
<TIMESTAMP> INFO 10.10.10.2
   Received EAP Response from the client.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> INFO 10.10.10.2
   Received Access-Challenge from the RADIUS server for the client
<TIMESTAMP> INFO 10.10.10.2
   Sending EAP request to client from radius server.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> ERROR 10.10.10.2 Received Access-Reject from the RADIUS server for the client.
<TIMESTAMP> ERROR 10.10.10.2 Received eap failurefrom the client.
```

Устранение проблем Веб-Аутентификации

В целом хорошее осуществление на практике устранения проблем должно включать проверку “Менеджера Политики Состояние” клиента, который имеет проблемы. Как это подтверждено в снимке экрана WCS ниже, рассматриваемый клиент застревает в состоянии *WEBAUTH_REQD*. Это означает, что процесс 802.11 завершен без любых ошибок, и эти возможные проблемы могут произойти:

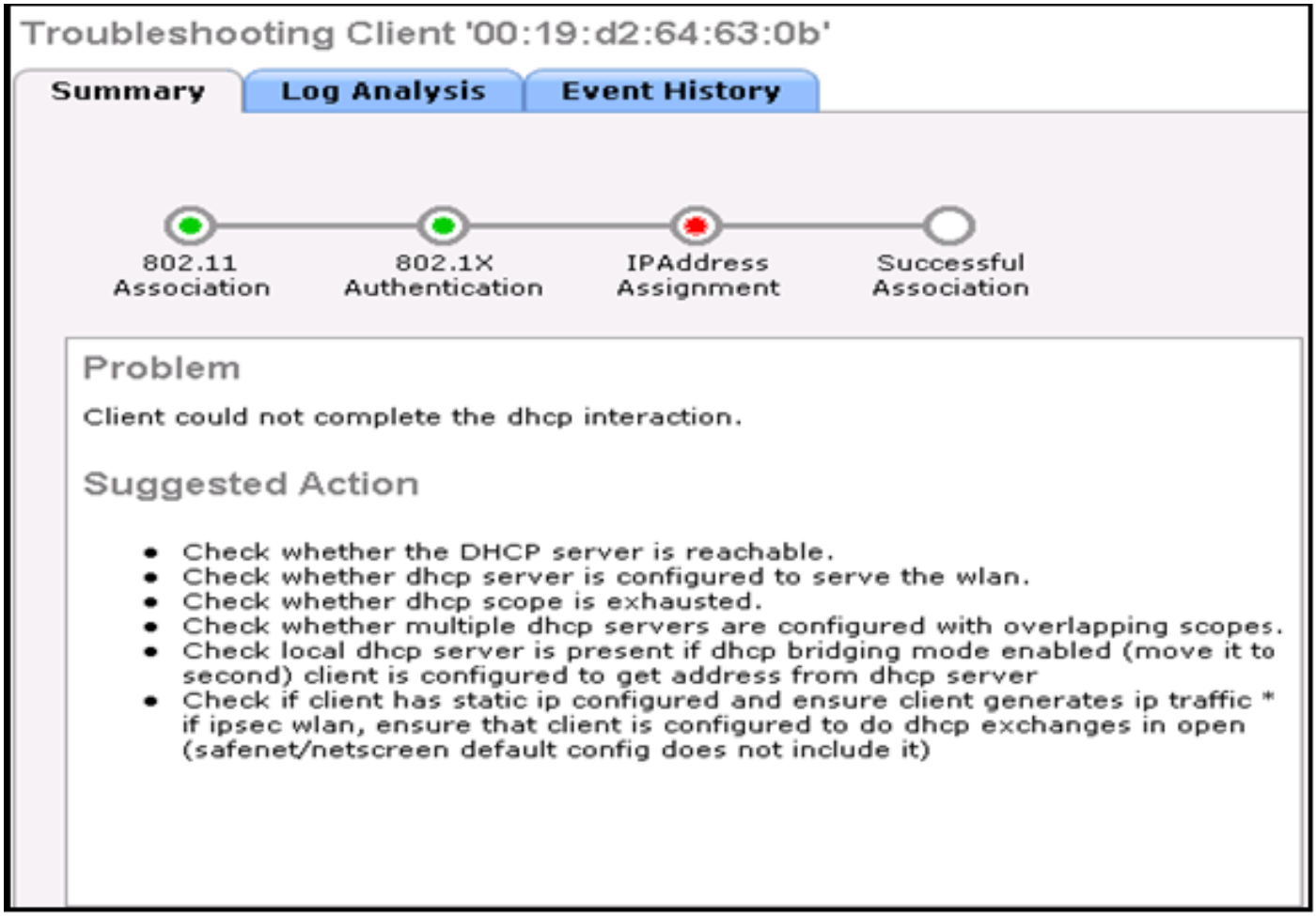
- Неверное имя пользователя / пароль
- Неправильная реализация ACL (для достижения сервера проверки подлинности внешней web - страницы, если таковые имеются)
- DNS, не настроенный должным образом и больше**Примечание:** Для получения дополнительной информации об устранении проблем web-аутентификации обратитесь к Примеру конфигурации Web-аутентификации Контроллера документа.

Журналы собрали от показа WCS, что веб-подлинный процесс не был успешен. Если вы устанавливаете политику Уровня 3 WLAN в веб-аутентификацию и не завершаете веб-подлинный процесс или вводите учетные данные входа в систему incorrect/non-existent, такая ситуация может быть моделирована в лабораторной работе. Проверьте раздел Краткие выводы инструмента диагностики клиентов для знания, где произошла проблема. Вы видите этот вход в систему WCS:

```
 <TIMESTAMP> INFO 10.10.10.2
   Controller association request message received
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting does not require 802 1x authentication
<TIMESTAMP> INFO 10.10.10.2
   Client web authentication is required <TIMESTAMP> INFO 10.10.10.2 Client moved to associated
state successfully <TIMESTAMP> INFO 10.10.10.2 Controller association request message received
```

Устранение проблем DHCP и IP-адресации

Часто, устройства клиента используются в нескольких беспроводных сетях. Примером может быть использование сотрудника корпоративного устройства на доме или открытой сети. У сотрудника может быть назначенный статический IP - адрес в домашней сети. Он/она соединяется с корпоративной сетью с ранее назначенным статическим IP - адресом без его/ее ведома. Это приводит к проблеме с подключением, на которую можно легко указать при помощи Клиента WCS Устранение проблем комплекта (как отображено ниже). Большинство проблем в этой области лежит на беспроводном клиенте, но это может также указать к потенциальной проблеме на проводной инфраструктуре, такой как исчерпанная область, неправильная область, и т.д. Попытка создать этот сценарий, когда вы назначаете неправильный статический IP - адрес на клиенте или изменяете параметры области DHCP на коммутаторе.



Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 5.1
- Управление радиоресурсами при использовании Unified Wireless Network
- Cisco Systems – техническая поддержка и документация