Примеры настройки проверки подлинности на контроллерах беспроводной сети

Содержание

Введение

Этот документ предоставляет примеры конфигурации, которые объясняют, как настроить различные типы Уровня 1, Уровня 2 и методов аутентификации Уровня 3 на Контроллерах беспроводной локальной сети (WLC).

Предварительные условия

Требования

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

- Знание конфигурации Облегченных точек доступа (LAP) и WLC Cisco
- Знание 802.11i стандарты безопасности

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- WLC Cisco 4400, который выполняет релиз микропрограммы 6.0.182.0
- Облегченные точки доступа Cisco 1000 серии
- Беспроводной клиентский адаптер Cisco 802.11a/b/g, использующий микропрограммное обеспечение версии 2.6
- Версия сервера 3.2 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.

Аутентификация на WLC

Единая беспроводная сеть Cisco (UWN) (UWN), решение по обеспечению безопасности связывает потенциально сложный Уровень 1, Уровень 2 и компоненты безопасности Точки доступа (AP) 802.11 Уровня 3 в простого менеджера политики, который настраивает политику безопасности в масштабе всей системы на на беспроводную локальную сеть (WLAN) основание. Cisco решение по обеспечению безопасности UWN предоставляет простые, объединенные, и систематические программные средства управления системой безопасности.

Эти механизмы обеспечения безопасности могут быть внедрены на WLC.

Решения для уровня 1

Ограничьте доступ клиента на основе количества последовательных неудачных попыток.

Решения уровня 2

Ни один Аутентификация — Когда эта опция выбрана от выпадающего списка безопасности уровня 2, Никакая аутентификация Уровня 2, не выполнен на WLAN. Это совпадает с открытой аутентификацией стандарта 802.11.

Static WEP (статический протокол защиты данных) — при статическом протоколе защиты данных (WEP) все AP и клиентские беспроводные сетевые карты в одной WLAN должны использовать единый шифровальный ключ. Каждая посылающая станция шифрует тело каждого кадра с Ключом WEP перед передачей, и принимающая станция дешифрует его с помощью идентичного ключа после приема.

802.1x — настраивает сеть WLAN на использование аутентификации стандарта 802.1x. Использование IEEE 802.1X предлагает эффективную платформу, чтобы аутентифицировать и управлять трафиком пользователя к защищенной сети, а также динамично варьироваться ключи шифрования. 802.1X связывает протокол под названием Протокол EAP и к проводным средам и к средам WLAN и поддерживает методы несколько

серверов проверок подлинности.

Static WEP + 802.1x — данный параметр безопасности уровня 2 включает как 802.1x, так и статический WEP. Клиенты могут или использовать Статический ключ WEP или аутентификацию 802.1x для соединения с сетью.

Wi-Fi Protected Access (WPA) (защищенный доступ Wi-Fi) — WPA или WPA1 и WPA2 являются основанными на стандартах решениями безопасности от объединения производителей Wi-Fi Alliance, предоставляющего системы защиты данных и контроля доступа для систем WLAN. WPA1 совместим со стандартом IEEE 802.11i, но был внедрен перед ратификацией стандарта. WPA2 является реализацией Wi-Fi Alliance ратифицированного стандарта IEEE 802.11i.

По умолчанию WPA1 использует Протокол TKIP и Message Integrity Check (MIC) для защиты данных. Использование WPA2 более сильное использование алгоритма шифрования Расширенного стандарта шифрования Отвечает на Режим Протоколом Кода аутентификации сообщения Cipher Block Chaining (CCMP AES). И WPA1 и WPA2 используют 802.1X для аутентифицируемого управления ключами по умолчанию. Однако эти опции также доступны: PSK, CCKM и CCKM+802.1x. При выборе CCKM Cisco только позволяет клиентам, которые поддерживают CCKM. При выборе CCKM+802.1x Cisco позволяет клиентам не-CCKM также.

CKIP — протокол проверки целостности ключа Cisco (CKIP) – это разработанный компанией Cisco протокол для шифрования носителей 802.11. CKIP улучшает безопасность 802.11 в режиме инфраструктуры с помощью ключевой перестановки, MIC и номера последовательности сообщений. Выпуск ПО 4.0 поддержки CKIP со статическим ключом. Для этой функции для работы правильно необходимо включить информационные элементы Aironet (IE) для WLAN. Параметры настройки CKIP, заданные в WLAN, являются обязательными для любого клиента, который пытается связаться. Если WLAN настроен и для ключевой перестановки CKIP и для MIC MMH, клиент должен поддержать обоих. Если WLAN настроен для только одной из этих функций, клиент должен поддерживать только эту функцию CKIP. WLC только поддерживают статический CKIP (как статический ключ WEP). WLC не поддерживают CKIP с 802.1x (динамический CKIP).

Решения уровня 3

Ни один — Когда эта опция выбрана от выпадающего списка безопасности уровня 3, никакая аутентификация Уровня 3, не выполнен на WLAN.

Примечание: Пример конфигурации ни для Какой аутентификации Уровня 3 и Никакой аутентификации Уровня 2 не объяснен ни в Одном Опознавательный раздел.

Веб-политика (Веб-аутентификация и Web pass-through (сквозное соединение)) — веб-аутентификация обычно используется пользователями, которым необходимо организовать сеть с гостевым доступом. В сети гостевого доступа существует начальная аутентификация имени пользователя и пароля, но безопасность не требуется для последующего трафика. Типичные развертывания могут включать местоположения "оперативной точки", такие как T-Mobile или Starbucks.

Web-аутентификация для WLC Cisco сделана локально. Вы создаете интерфейс и затем привязываете WLAN/идентификатор набора сервисов (SSID) к тому интерфейсу.

Web-аутентификация предоставляет простую проверку подлинности без соискателя или клиента. Следует иметь в виду, что web-аутентификация не предоставляет шифрование данных. Веб-проверка подлинности обычно используется в качестве простого гостевого доступа для так называемых "горячих точек" (точек общего доступа) или кампусов, где важна сама возможность подключения.

Веб-passthrough является решением, через которое пользователи беспроводной связи перенаправлены к приемлемой странице политики использования, не имея необходимость аутентифицироваться, когда они соединяются с Интернетом. Это перенаправление заботится о самим WLC. Единственное требование должно настроить WLC для веб-passthrough, который является в основном web-аутентификацией, не имея необходимость вводить любые учетные данные.

VPN Passthrough – это функция, позволяющая клиенту установить туннель только с определенным VPN-сервером. Поэтому, если необходимо надежно обратиться к настроенному серверу VPN, а также другому серверу VPN или Интернету, это не возможно с Passthrough VPN, включенным на контроллере.

В следующих разделах примеры конфигурации предоставлены для каждого из механизмов аутентификации.

Примеры конфигураций

Перед настройкой WLAN и типов проверки подлинности необходимо настроить WLC для главной операции и зарегистрировать облегченные точки доступа на контроллере. Этот документ предполагает, что WLC 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).

Решения по обеспечению безопасности уровня 1

Беспроводные клиенты могут быть ограниченным доступом на основе количества последовательных неудачных попыток для доступа к сети WLAN. Клиентское исключение происходит в этих условиях по умолчанию. Эти значения не могут быть изменены.

- Последовательная Ошибка проверки подлинности 802.11 (5 раз подряд, 6-я попытка исключена),
- Последовательные Сбои Ассоциации 802.11 (5 раз подряд, 6-я попытка исключена),
- Последовательные Ошибки проверки подлинности 802.1x (3 раза подряд, 4-я попытка исключена),
- Отказ сервера внешней политики
- Попытайтесь использовать IP-адрес, уже назначенный на другое устройство (Кража IP или Повторное использование IP)
- Последовательная Web-аутентификация (3 раза подряд, 4-я попытка исключена),

Для определения местоположения Клиентской Политики Исключения нажмите **Security** в главном меню, и затем выберите **Wireless Protection Policies> Client Exclusion Policies** навигация на левой части страницы.

Таймер исключения может быть настроен. Опции исключения могут быть включены или

отключены на контроллер. Таймер исключения может быть включен или отключен на WLAN.

Значение максимального количества одновременных входов для одного пользователя, установленное по умолчанию, равно 0. Можно ввести любое значение от 0 до 8. Этот параметр может быть установлен в SECURITY > AAA > User Login Policies и позволяет определить максимальное количество одновременных входов для одного клиента от 1 до 8 или 0 – не ограничено. Например:

Решения безопасности уровня 2

Ни один аутентификация

Данный пример показывает WLAN, настроенный без аутентификации.

Примечание: Данный пример также не работает ни для Какой аутентификации Уровня 3.

Настройте WLC ни для какой аутентификации

Выполните эти шаги для настройки WLC для этой настройки:

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 **Go** в заказе настроить новый WLAN.
3. Введите параметры для WLAN. Данный пример показывает конфигурацию для этого WLAN.
4. **Щелкните "Применить".**
5. В окне WLAN > Edit укажите параметры сети.
6. Нажмите **Вкладку Безопасность** и выберите **None for Layer 2** и безопасность уровня 3.**Примечание:** Для WLAN для становления активным должен быть включен статус. Для включения его установите флажок **Проверки состояния** под Вкладкой Общие.Это не включает аутентификации для этого WLAN.
7. Выберите другие параметры на основе своих требований к проектированию. Данный пример использует значения по умолчанию.
8. **Щелкните "Применить".**

Настройте беспроводного клиента ни для какой аутентификации

Выполните эти шаги для настройки клиента Беспроводной локальной сети для этой настройки:

Примечание: Этот документ использует Aironet 802.11a/b/g Клиентский адаптер, который выполняет микропрограммное обеспечение 3.5 и объясняет конфигурацию клиентского адаптера с версией ADU 3.5.

1. **Чтобы создать новый профиль, нажмите вкладку Profile Management в ADU.**
2. **Щелкните New.**
3. Когда появится окно "Profile Management (General)", то для того, чтобы задать имя профиля (Profile Name), имя клиента (Client Name) и идентификатор SSID, выполните

следующие действия:В поле "Profile Name" введите имя профиля.Данный пример использует *NoAuthentication* в качестве имени профиля.В поле "Client Name" введите имя клиента.Имя клиента используется для идентификации беспроводного клиента в сети WLAN. Эта конфигурация использует *Клиента 1* для имени клиента.В области "Network Names" укажите идентификатор SSID, который будет использоваться в этом профиле.SSID совпадает с SSID, который вы настроили на WLC. SSID в данном примере является *NullAuthentication.*

4. **Щелкните вкладку Безопасность.**
5. Нажмите кнопку с зависимой фиксацией **None** под Параметрами безопасности Набора, и затем нажмите **OK**.Когда SSID активирован, подключения беспроводного клиента к WLAN без любой аутентификации.

Статический ключ WEP

Данный пример показывает WLAN, настроенный со статическим ключом WEP.

Настройте WLC для статического ключа WEP

Выполните эти шаги для настройки WLC для этой настройки:

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.**
3. Введите SSID WLAN и ИДЕНТИФИКАТОР WLAN.В данном примере WLAN называют *StaticWEP*, и ИДЕНТИФИКАТОР WLAN равняется *2*.
4. **Щелкните "Применить".**
5. В окне WLAN > Edit укажите параметры сети.От выпадающего списка Уровня 2 выберите **Static WEP**.Это включает Статический ключ WEP для этого WLAN.Под параметрами Статического ключа WEP выберите размер Ключа WEP и ключевой индекс, и введите ключ шифрования статического ключа WEP.Размер ключа может составить или 40 битов или 104 бита. Ключевой индекс может быть между 1 и 4. Один уникальный Индекс КЛЮЧА WEP может быть применен к каждому WLAN. Поскольку существует только четыре Индекса КЛЮЧА WEP, только четыре WLAN могут быть настроены для шифрования Уровня 2 Статического ключа WEP. В данном примере используется WEP на 104 бита, и используемый Ключ WEP 1234567890abcdef.Проверьте, настроен ли сервер RADIUS для аутентификации. Сервер RADIUS может быть настроен на **Вкладке Безопасность**, расположенной в **AAA> Радиус> Аутентификация**. После того, как настроенный, сервер RADIUS должен быть назначен на WLAN для аутентификации. Перейдите **к> Security WLAN> AAA-серверы** для присвоения сервера RADIUS на WLAN для аутентификации.В данном примере, 10.77.244.196 сервер RADIUS.
6. Выберите другие параметры на основе своих требований к проектированию.Данный пример использует значения по умолчанию.
7. **Щелкните "Применить".Примечание:** WEP всегда представляется в шестнадцатеричном (hex). При вводе Ключа WEP в ASCII строка WEP ASCII преобразована в hex, который используется для шифрования пакета. Нет никакого

стандартного метода, который поставщики выполняют для преобразования hex в ASCII, поскольку некоторые сделают заполнение, в то время как другие не будут. Поэтому для максимальной совместимости межпоставщика, используйте hex для своих Ключей WEP.**Примечание:** Если вы хотите включить Проверку подлинности с общим ключом для WLAN, проверьте флажок **Allow Shared-Key Authentication** под Параметрами Статического ключа WEP. Таким образом, если клиент будет также настроен для Проверки подлинности с общим ключом, то Проверка подлинности с общим ключом, придерживавшаяся Шифрованием WEP пакетов, будет иметь место в WLAN.

Настройте беспроводного клиента для статического ключа WEP

Выполните эти шаги для настройки Клиента Беспроводной локальной сети для этой настройки:

1. **Чтобы создать новый профиль, нажмите вкладку Profile Management в ADU.**
2. **Щелкните New.**
3. Когда появится окно "Profile Management (General)", то для того, чтобы задать имя профиля (Profile Name), имя клиента (Client Name) и идентификатор SSID, выполните следующие действия:В поле "Profile Name" введите имя профиля.Данный пример использует *StaticWEP* в качестве имени профиля.В поле "Client Name" введите имя клиента.Имя клиента используется для идентификации беспроводного клиента в сети WLAN. Эта конфигурация использует *Клиента 2* для имени клиента.В области "Network Names" укажите идентификатор SSID, который будет использоваться в этом профиле.SSID совпадает с SSID, который вы настроили на WLC. SSID в данном примере является *StaticWEP*.
4. **Щелкните вкладку Безопасность.**
5. **Выберите Pre-Shared Key (Static WEP) в области Set Security Options.**
6. **Нажмите Configure и определите ключ WEP и его размер.**Это должно совпасть с Ключом WEP, настроенным на WLC для этого WLAN.
7. **Щелкните "Применить".**Когда SSID активирован, подключения беспроводного клиента к WLAN и пакетам зашифрованы с помощью статического ключа WEP.

Аутентификация 802.1x

Данный пример показывает WLAN, настроенный с аутентификацией 802.1x.

Настройте WLC для аутентификации 802.1x

Выполните эти шаги для настройки WLC для этой настройки:

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 *802.1x*, и ИДЕНТИФИКАТОР WLAN равняется *3*. Имя профиля должно также быть добавлено.
3. **Щелкните "Применить".**
4. В окне WLAN > Edit укажите параметры сети.От выпадающего списка Уровня 2

выберите **802.1x**.**Примечание:** Только Шифрование WEP доступно с 802.1x. Выберите или 40 битов или 104 бита для шифрования, и удостоверьтесь, что безопасность уровня 3 не установлена ни в Один.Это включает аутентификацию 802.1x для этого WLAN.Под параметрами сервера RADIUS выберите сервер RADIUS, который будет использоваться для аутентификации удостоверений клиента.Выберите другие параметры на основе своих требований к проектированию.Данный пример использует значения по умолчанию.

5. **Щелкните "Применить".Примечания:**При выборе *802.1x* для безопасности уровня 2 CCKM не может использоваться.При выборе *WPA 1* или *WPA 2 for Layer 2 security* эти опции появляются под Подлинным Управлением ключами:*802.1x+CCKM* — Если вы выбираете эту опцию, оба CCKM или клиенты не-CCKM поддерживаются (дополнительный CCKM).*802.1x* — при выборе этой опции, только клиенты 802.1x поддерживается.*CCKM* — при выборе этой опции, только клиенты CCKM поддерживается, где клиенты направлены к внешнему серверу для аутентификации.*PSK* — при выборе этой опции, предварительный общий ключ используется для WLC и клиента. Кроме того, все нормы установлены, чтобы использоваться к перед предварительными стандартами; например, WPA/WPA2 берет прецедент по CCKM, когда используется одновременно.Тип Аутентификации eap, используемой для проверки клиентов, зависит от типа EAP, настроенного на сервере RADIUS и беспроводных клиентах. Как только 802.1x включен на WLC, WLC позволяет всем типам пакетов EAP течь между LAP, беспроводным клиентом и сервером RADIUS.Эти документы предоставляют примеры конфигурации на некоторых типах Аутентификации eap:PEAP в единой беспроводной сети с ACS 4.0 и Windows 2004EAP-TLS в Unified Wireless Network с ACS 4.0 и Windows 2003Пример конфигурации аутентификации EAP в контроллерах WLAN (WLC)

Настройте беспроводного клиента для аутентификации 802.1x

Выполните эти шаги для настройки Клиента Беспроводной локальной сети для этой настройки:

1. **Чтобы создать новый профиль, нажмите вкладку Profile Management в ADU.**
2. **Щелкните New.**
3. Когда появится окно "Profile Management (General)", то для того, чтобы задать имя профиля (Profile Name), имя клиента (Client Name) и идентификатор SSID, выполните следующие действия:В поле "Profile Name" введите имя профиля.Данный пример использует *EAPAuth* в качестве имени профиля.В поле "Client Name" введите имя клиента.Имя клиента используется для идентификации беспроводного клиента в сети WLAN. Эта конфигурация использует *Клиента 3* для имени клиента.В области "Network Names" укажите идентификатор SSID, который будет использоваться в этом профиле.SSID совпадает с SSID, который вы настроили на WLC. SSID в данном примере является *802.1x*.
4. **Щелкните вкладку Безопасность.**
5. Нажмите кнопку с зависимой фиксацией **802.1x**.
6. От выпадающего списка Типа EAP 802.1x выберите используемый тип EAP.
7. **Нажмите Configure, чтобы настроить параметры, свойственные для данного типа EAP.**
8. **Щелкните "Применить".**Когда SSID активирован, подключения беспроводного клиента к WLAN с помощью аутентификации 802.1x. Динамические Ключи WEP используются

для сеансов.

Статический ключ WEP + аутентификация 802.1x

Данный пример показывает WLAN, настроенный со статическим ключом WEP + аутентификация 802.1x.

Выполните эти шаги для настройки WLC для этой настройки:

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.**
3. Введите SSID WLAN и ИДЕНТИФИКАТОР WLAN.В данном примере WLAN называют *WEP+802.1x*, и ИДЕНТИФИКАТОР WLAN равняется *4*.
4. **Щелкните "Применить".**
5. В окне WLAN > Edit укажите параметры сети.От выпадающего списка Уровня 2 выберите **Static-WEP+802.1x**.Это включает и Статический ключ WEP и аутентификацию 802.1x для этого WLAN.Под параметрами сервера RADIUS выберите сервер RADIUS, который будет использоваться, чтобы аутентифицировать удостоверения клиента с помощью 802.1x и настроить сервер RADIUS как показано в предыдущем примере.Под параметрами Статического ключа WEP выберите размер Ключа WEP и ключевой индекс, и введите ключ шифрования статического ключа WEP как показано в предыдущий образ.Выберите другие параметры на основе своих требований к проектированию.Данный пример использует значения по умолчанию.

Настройте беспроводного клиента для статического ключа WEP и 802.1x

Посмотрите Настраивать Беспроводного клиента для Аутентификации 802.1x и Настройте Беспроводного клиента для разделов Статического ключа WEP для получения информации о том, как настроить беспроводного клиента.

Как только клиентские профили созданы, клиенты, которые настроены для партнера статического ключа WEP с LAP. Используйте SSID WEP+802.1x для соединения с сетью.

Точно так же беспроводные клиенты, которые настроены для использования аутентификации 802.1x, аутентифицируются с помощью EAP и обращаются к сети с тем же SSID WEP+802.1x.

Защищенный доступ к Wi-Fi

Данный пример показывает WLAN, который настроен с WPA с 802.1x.

Настройте WLC для WPA

Выполните эти шаги для настройки WLC для этой настройки:

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 **Go** в заказе настроить новый WLAN.Выберите тип и имя профиля. В данном примере WLAN называют *WPA*, и ИДЕНТИФИКАТОР WLAN равняется *5*.
3. **Щелкните "Применить".**
4. В окне WLAN > Edit укажите параметры сети.Нажмите **Вкладку Безопасность**, нажмите **Таблицу уровня 2** и выберите **WPA1+WPA2** из выпадающего списка безопасности уровня 2.**В области WPA1+WPA2 Parameters, установите флажок WPA1 Policy для включения WPA1, флажок WPA2 Policy для включения WPA2, или оба флажка для включения WPA1 и WPA2.**Значение по умолчанию отключено и для WPA1 и для WPA2. При отъезде и WPA1 и WPA2 отключенными точки доступа дают объявление в их сигналах-маяках и зондируют элементы данных отклика только для метода управления ключа проверки подлинности, который вы выбираете.**Установите флажок AES для включения AES-шифрования данных или флажок TKIP для включения TKIP-шифрования данных для WPA1, WPA2 или для обоих алгоритмов.**Значения по умолчанию являются TKIP для WPA1 и AES для WPA2.Выберите один из этих методов управления ключами от Подлинного Ключевого выпадающего списка Mgmt:*802.1X* — при выборе этой опции, только клиенты 802.1x поддерживается.*CCKM* — при выборе этой опции, только клиенты CCKM поддерживается, где клиенты направлены к внешнему серверу для аутентификации.*PSK* — при выборе этой опции, предварительный общий ключ используется для WLC и клиента. Кроме того, все нормы установлены, чтобы использоваться к перед предварительными стандартами; например, WPA/WPA2 берет прецедент по CCKM, когда используется одновременно.*802.1X+CCKM* — Если вы выбираете эту опцию, оба CCKM или клиенты не-CCKM поддерживаются (дополнительный CCKM).Данный пример использует 802.1x.**Примечание:** Если вы выбираете PSK, выбираете **ASCII** или **hex** от выпадающего списка Формата PSK, и затем вводите предварительный общий ключ в пустое поле. Предварительные общие ключи WPA должны содержать 8 - 63 символа текста ASCII или 64 шестнадцатеричных символа.
5. Нажмите **Apply** для применения изменений.

Настройте беспроводного клиента для WPA

Выполните эти шаги для настройки клиента Беспроводной локальной сети для этой настройки:

1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**
2. Нажмите **Вкладку Общие** и введите имя профиля и SSID, который будет использовать клиентский адаптер.В данном примере имя профиля и SSID являются *WPA*. SSID должен совпасть с SSID, который вы настроили на WLC для WPA.
3. На Вкладке Безопасность нажмите кнопку с зависимой фиксацией **WPA/WPA2/CCKM** и выберите соответствующий тип EAP из выпадающего списка Типа EAP WPA/WPA2/CCKM. Этот шаг включает WPA.
4. **Нажмите Configure для настройки параметров EAP, специфичных для выбранного типа EAP.**
5. **Нажмите кнопку OK.Примечание:** Когда этот профиль активирован, клиент аутентифицируется с помощью 802.1x и когда аутентификация успешна, клиентские подключения к WLAN. Проверьте Текущий статус ADU, чтобы проверить, что клиент

использует шифрование TKIP (шифрование по умолчанию, используемое WPA1) и Аутентификация eap.

CKIP

Данный пример показывает WLAN, настроенный с CKIP.

Настройте WLC для CKIP

Выполните эти шаги для настройки WLC для этой настройки:

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.**Выберите тип и имя профиля. В данном примере WLAN называют *CKIP*, и ИДЕНТИФИКАТОР WLAN равняется *6*.
3. В окне WLAN > Edit укажите параметры сети.От выпадающего списка Уровня 2 выберите **CKIP**.Этот шаг включает CKIP для этого WLAN.Под параметрами CKIP выберите размер ключа и ключевой индекс, и введите статический ключ шифрования.Размер ключа может составить или 40 битов, 104 бита или 128 битов. Ключевой индекс может быть между 1 и 4. Один уникальный индекс Ключа WEP может быть применен к каждому WLAN. Поскольку существует только четыре индекса Ключа WEP, только четыре WLAN могут быть настроены для шифрования Уровня 2 статического ключа WEP.Для CKIP выберите **MMH Mode option**, или опцию **Key Permutation** или обоих.**Примечание:** Или один из этих параметров или оба должны быть выбраны для CKIP для работы как ожидалось. Если эти параметры не выбраны, WLAN остается в отключенном состоянии.В данном примере используется ключ на 104 бита, и ключ 1234567890abc.
4. Выберите другие параметры на основе своих требований к проектированию.Данный пример использует значения по умолчанию.
5. **Щелкните "Применить".Примечание:** CKIP функционален на 1100, 1130, и 1200 AP, но не AP 1000. IE aironet должен быть позволен для этой функции работать. CKIP разворачивает ключи шифрования до 16 байтов.

Настройте беспроводного клиента для CKIP

Выполните эти шаги для настройки Клиента Беспроводной локальной сети для этой настройки:

1. Для создания нового профиля нажмите вкладку **Profile Management** на ADU, и затем нажмите **New**.
2. Когда появится окно "Profile Management (General)", то для того, чтобы задать имя профиля (Profile Name), имя клиента (Client Name) и идентификатор SSID, выполните следующие действия:В поле "Profile Name" введите имя профиля.Данный пример использует *CKIP* в качестве имени профиля.В поле "Client Name" введите имя клиента.Имя клиента используется для идентификации беспроводного клиента в сети WLAN. Эта конфигурация использует *Client6* для имени клиента.В области "Network Names" укажите идентификатор SSID, который будет использоваться в этом

профиле.SSID совпадает с SSID, который вы настроили на WLC. SSID в данном примере является *CKIP*.
3. **Щелкните вкладку Безопасность.**
4. Выберите **Pre-Shared Key (Static WEP)** под Параметрами безопасности Набора, нажмите **Configure** и определите размер Ключа WEP и Ключ WEP.Эти значения должны совпасть с Ключом WEP, настроенным на WLC для этого WLAN.
5. **Нажмите кнопку ОК.**Когда SSID активирован, беспроводной клиент выполняет согласование с LAP и WLC для использования CKIP для шифрования пакеты.

Решения безопасности уровня 3

Веб-политика (Web-аутентификация и веб-Passthrough)

См. Пример настройки веб-аутентификации в контроллере беспроводной сети LAN для получения информации о том, как включить web-аутентификацию в сети WLAN.

См. Внешнюю веб-аутентификацию с Примером конфигурации Контроллеров беспроводной локальной сети для получения информации о том, как настроить внешнюю веб-аутентификацию и веб-сквозную аутентификацию в WLAN.

См. сеть Контроллера беспроводной локальной сети Транзитный Пример конфигурации для получения дополнительной информации о том, как включить веб-passthrough в сети WLAN.

Механизм Страницы-заставки является механизмом безопасности уровня 3, представленным в Версии 5.0 WLC, используемой для аутентификации клиента. См. Пример конфигурации Перенаправления Страницы-заставки Контроллера беспроводной локальной сети для получения дополнительной информации.

Passthrough VPN

См. Клиентскую VPN по Беспроводной локальной сети с Примером конфигурации WLC для получения информации о том, как настроить passthrough VPN в WLAN.

Устранение неполадок

Команды для устранения неполадок

Вы можете использовать эти команды debug для устранения неполадок конфигурации.

Отладки для web-аутентификации:

- *debug mac addr <MAC-адрес клиента xx:xx:xx:xx:xx:xx> - настраивает отладку MAC-адреса для клиента.*
- **debug aaa all enable - настраивает отладку всех сообщений AAA.**
- **debug pem state enable - настраивает отладку конечного автомата менеджера политик**
- **debug pem events enable - настраивает отладку событий менеджера политик.**
- **debug dhcp message enable - используйте эту команду для отображения отладочной информации о работе клиентов протокола динамической конфигурации хоста (DHCP) и**

наблюдения за состоянием пакетов DHCP.
- debug dhcp packet enable - используйте эту команду для отображения информации пакетного уровня DHCP.
- debug pm ssh-appgw enable - настраивает отладку шлюзов приложений.
- debug pm ssh-tcp enable – настраивает отладку обработки пакетов TCP менеджера политик

Отладки для WEP: Для WEP нет команды отладки, т.к. она производится на точке доступа, включите debug dot11 all enable.

Отладки для кэширования 802.1X/WPA/RSN/PMK:

- *debug mac addr <MAC-адрес клиента xx:xx:xx:xx:xx:xx> - настраивает отладку MAC-адреса для клиента.*
- debug dot1x all enable - используйте эту команду для отображения отладочной информации 802.1x.
- debug dot11 all enable - используйте эту команду для запуска отладки функций радиоблока.
- debug pem events enable - настраивает отладку событий менеджера политик.
- debug pem state enable - настраивает отладку конечного автомата менеджера политик.
- debug dhcp message enable - используйте эту команду для отображения отладочной информации о работе клиентов протокола динамической конфигурации хоста (DHCP) и наблюдения за состоянием пакетов DHCP.
- debug dhcp packet enable - используйте эту команду для отображения информации пакетного уровня DHCP.
- debug mobility handoff enable (для роуминга в пределах коммутатора) - настраивает отладку пакетов мобильности.
- *show client detail <MAC-адрес> - отображает подробную информацию о клиенте по MAC-адресу.* Проверьте WLAN и конфигурацию превышения времени ожидания сеанса RADIUS.

Дополнительные сведения

- Пример настройки ограничения доступа к WLAN на основе SSID с WLC и Cisco Secure ACS
- Пример конфигурации ACL на контроллере беспроводных LAN
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация