Wired Equivalent Privacy (WEP) на Примерах конфигураций точек доступа Aironet и мостов

Содержание

Введение

В этом документе представлены способы настройки протокола защиты WEP на элементах беспроводной локальной сети (WLAN) Cisco Aironet.

Примечание: См. Статический веб-раздел Ключей Главы 6 - WLAN Настройки для получения дополнительной информации о конфигурации WEP на контроллерах беспроводной локальной сети (WLC).

WEP является алгоритмом шифрования, встроенным в 802.11 (Wi-Fi) стандарт. Шифрование WEP использует Поточный шифр Кода 4 Рона (RC4) с 40-или 104-разрядные ключи и 24-разрядный Вектор инициализации (IV).

Поскольку стандарт задает, WEP использует алгоритм RC4 с 40-разрядным или 104-разрядным ключом и 24-разрядным IV. RC4 является симметричным алгоритмом, потому что он использует тот же ключ для шифрования и описания данных. При включении WEP все радиостанции получают ключи. Ключ используется для скремблирования данных перед передачей в эфир. Если станция получает пакет, который не скремблируется с соответствующим ключом, от пакета сбрасывают и никогда не отправляют хосту.

WEP может прежде всего использоваться для домашнего офиса или малого офиса, который не требует очень сильной безопасности.

Реализация WEP aironet находится в аппаратных средствах. Поэтому минимальное влияние на производительность заканчивается при использовании WEP.

Примечание: Существуют некоторые известные неполадки с WEP, который делает его не методом строгого шифрования. Проблемы:

- Существует много административной служебной информации для поддержания совместно используемого Ключа WEP.
- WEP имеет ту же проблему как все системы на основе общих ключей. Любая тайна, данная одному человеку, становится достоянием общественности после периода времени.
- IV, который отбирает алгоритм WEP, передается в открытом тексте.
- Контрольная сумма WEP линейна и предсказуема.

Протокол TKIP был создан для решения этих проблем WEP. Подобный WEP, TKIP использует шифрование RC4. Однако TKIP улучшает WEP путем добавления мер, таких как попакетное хеширование ключей, Message Integrity Check (MIC) и Ротация (широковещательных) ключей для адресации к известной уязвимости WEP. TKIP использует поточный шифр RC4 с 128-разрядными ключами для шифрования и 64-разрядными ключами для аутентификации.

Предварительные условия

Требования

Этот документ предполагает, что можно сделать административное соединение к устройствам WLAN и что устройства обычно функционируют в нешифрованной среде.

Для настройки стандартного 40-разрядного WEP у вас должно быть два или больше радиоустройства, которые связываются друг с другом.

Примечание: Продукты Aironet могут установить WEP-подключения 40-bit с продуктами неCisco IEEE 802.11b-compliant. Этот документ не адресует конфигурацию других устройств.

Для создания 128-разрядной ссылки WEP продукты Cisco только взаимодействуют с другими продуктами Cisco.

Используемые компоненты

Используйте эти компоненты с этим документом:

- Два или больше радиоустройства, которые связываются друг с другом
- Административное соединение к устройству WLAN

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.

Настройте WEP на точках доступа Aironet

Точки доступа Aironet, на которых запущена операционная система VxWorks

Выполните следующие действия:

1. Сделайте соединение с Точкой доступа (AP).
2. Перейдите к Меню шифрования радиоданных AP.Используйте один из этих путей:**Summary Status> Setup> Радио AP / Аппаратное Шифрование данных> Radio (WEP)> Шифрование данных Радио AP> SecuritySetup (настройка безопасности)> Security Summary Status> Setup: Radio Data Encryption (WEP)> Шифрование данных Радио APПримечание:** Для внесения изменений в эту страницу необходимо быть администратором с возможностями Идентичности и Записи.**Просмотр с помощью веб-браузера меню шифрования радиоданных точки доступа**

Параметры настройки VxWorks

Страница AP Radio Data Encryption представляет многообразие параметров для использования. Некоторые опции являются обязательными для WEP. Этот раздел обращает внимание на эти обязательные параметры. Другие опции не необходимы для WEP для функционирования, но им рекомендуют.

- **Использование шифрования данных станциями – это:**Используйте это приводящее в порядок, чтобы выбрать, должны ли клиенты использовать шифрование данных, когда они связываются с AP. Ниспадающее меню перечисляет три опции:**Никакое Шифрование (по умолчанию)** — Требования клиента для передачи с AP без любого шифрования данных. Эта установка не рекомендуется.**Дополнительный** — Позволяет клиентам связываться с AP или с или без шифрования данных. Как правило, вы используете эту опцию, когда у вас есть устройства клиента, которые не могут сделать WEP - подключение, такой как клиенты не-Cisco в 128-разрядной среде WEP.**Полное шифрование (RECOMMENDED)** — Требования клиента для использования шифрования данных, когда они связываются с AP. Клиентам, которые не используют шифрование данных, не разрешают связаться. Если вы хотите увеличить безопасность своего WLAN, эта опция рекомендуется.**Примечание:** Необходимо установить Ключ WEP, прежде чем вы включите шифрование использование. Посмотрите **Ключ шифрования (ОБЯЗАТЕЛЬНЫЙ)** раздел этого списка.
- **Типы аутентификации приема**Можно выбрать Open, Shared Key или обе из этих опций для установки аутентификаций, которые распознает AP.**Open (RECOMMENDED)** — Эта настройка по умолчанию позволяет любому устройству, независимо от его Ключей WEP, аутентифицироваться и пытаться связаться.**Общий ключ** — Эта установка говорит AP передавать простой текст, запрос общего ключа к любому устройству, которое пытается связаться с AP.**Примечание:** Этот запрос может оставить AP открытым для атаки с известным текстом от злоумышленников. Поэтому эта установка не так

безопасна как Значение Open.

- **Передача с ключом**Эти кнопки позволяют вам выбирать ключ, который AP использует во время передачи данных. Можно выбрать только один ключ за один раз. Любые из ключей набора могут использоваться для получения данных. Необходимо установить ключ перед определением его как Ключа передачи.
- **Ключ шифрования (ОБЯЗАТЕЛЬНЫЙ)**Эти поля позволяют вам вводить Ключи WEP. Введите 10 шестнадцатеричных цифр для 40-разрядных Ключей WEP или 26 шестнадцатеричных цифр для 128-разрядных Ключей WEP. Ключи могут быть любой комбинацией этих цифр:От 0 до 9к fK FДля защиты безопасности Ключа WEP существующие Ключи WEP не появляются в открытом тексте в полях ввода данных. В последних версиях AP можно удалить существующие ключи. Однако вы не можете отредактировать существующие ключи.**Примечание:** Необходимо установить Ключи WEP для сети, AP и устройств клиента точно таким же образом. Например, если вы устанавливаете КЛЮЧ WEP 3 на вашем AP к 0987654321 и выбираете этот ключ как активный ключ, необходимо также установить КЛЮЧ WEP 3 на устройстве клиента к тому же значению.
- **(ОБЯЗАТЕЛЬНЫЙ) размер ключа**Эта установка устанавливает ключи или к 40-разрядному или к 128-разрядному WEP. Если "not set" появляется для этого выбора, ключ является "not set".**Примечание:** Вы не можете удалить ключ путем выбора "not set".
- **Кнопки выполнения**Четыре командных кнопки управляют параметрами настройки. Если JavaScript включен на вашем web-браузере, окно всплывающего диалогового окна подтверждения появляется после нажатия любой кнопки, кроме Отмены.**Применитесь** — Эта кнопка активирует новые установки значения. Браузер остается на странице.**OK** — Эта кнопка применяет новые параметры настройки и кладет обратно браузер к главной странице настройки.**Отмена** — Эта кнопка отмены, устанавливающие изменения и, возвращает параметры настройки к ранее хранимые значения. Вы тогда возвращаетесь к главной странице настройки.**Настройки по умолчанию восстановления** — Эта кнопка изменяет все настройки на этой странице назад к заводским настройкам.

Примечание: В недавних версиях Cisco IOS® AP только кнопки управления **Apply и Cancel** доступны для этой страницы.

Разрез данных эмуляции терминала меню шифрования данных Представление эмуляции терминала последовательности конфигурации КЛЮЧА WEP (программное обеспечение Cisco IOS)

AP aironet, который выполненное программное обеспечение Cisco IOS

Выполните следующие действия:

1. Сделайте соединение с AP.
2. Из МЕНЮ СИСТЕМЫ БЕЗОПАСНОСТИ OPTION на левой части окна выберите **Encryption Manager** для радиоинтерфейса, к которому вы хотите настроить свои статические ключи WEP.**Представление web-браузера меню security encryption Manager AP**

Настройте мосты Aironet

При использовании VxWorks, выполняете эти шаги:

1. Сделайте соединение с Мостом.
2. Перейдите к Меню Конфиденциальность.Выберите **Main Menu>> Radio Configuration>> Privacy I80211**.Меню Конфиденциальность управляет использованием шифрования на пакете данных, который передан по воздуху радио. Алгоритм RC4 RSA и один максимум из четырех известных ключей используются для шифрования пакетов. Каждый узел в радиоячейке должен знать все ключи в использовании, но любой из ключей может быть выбран для передачи данных.**Вид меню конфиденциальности эмулятора терминала**

См. Наборы шифров Настройки и WEP - Мост серии 1300 и WEP Настройки и Функции WEP - Мост серии 1400 для получения информации о том, как настроить WEP в 1300 и Мосты серии 1400 через режим интерфейса командой строки.

Для использования GUI, чтобы настроить Бриджеса серии 1400 и 1300 года, завершить ту же процедуру, объяснил в AP Aironet Который раздел программного обеспечения Cisco IOS Выполнения этого документа.

Параметры настройки VxWorks

Меню Конфиденциальность представляет ряд опций, которые необходимо настроить. Некоторые опции являются обязательными для WEP. Этот раздел обращает внимание на эти обязательные параметры. Другие опции не необходимы для WEP для функционирования, но им рекомендуют.

Этот раздел представляет опции меню в заказе, что они появляются в Представлении эмуляции терминала Меню Конфиденциальность. Однако настройте опции в этом заказе:

1. Ключ
2. Передача
3. Auth
4. Клиент
5. Шифрование

Конфигурация в этом заказе гарантирует, что необходимые предварительные условия установлены, поскольку вы настраиваете каждую установку.

Это опции:

- **Ключ (ОБЯЗАТЕЛЬНЫЙ)**Опция Key программирует ключи шифрования в Мост. Вам предлагают установить один из этих четырех ключей. Вам предлагают дважды ввести ключ. Для определения ключа необходимо ввести или 10 или 26 шестнадцатеричных цифр, который зависит от того, является ли Конфигурация моста для 40-разрядных или 128-разрядных ключей. Используйте любую комбинацию этих цифр:От 0 до 9к fK FКлючи должны совпасть во ***всех*** узлах в радиоячейке, и необходимо ввести ключи в том же заказе. Вы не должны определять все четыре ключа, пока количество соответствия ключей в каждом устройстве в WLAN.
- **Передача**Опция Transmit говорит радио, какие ключи использовать для передачи пакетов. Каждое радио в состоянии дешифровать полученные пакеты, которые передаются с любым из этих четырех ключей.
- **Auth**Вы используете параметр аутентификации на мостах повторителя для определения который режим аутентификации использование модуля для соединения с его

родителем. Позволенные значения Открыты или Общий ключ. Протокол 802.11 задает процедуру, в которой клиент должен аутентифицироваться с родителем, прежде чем сможет связаться клиент.**Open (RECOMMENDED)** — Этот режим аутентификации является по существу фиктивной операцией. Всем клиентам разрешают аутентифицироваться.**Общий ключ** — Этот режим позволяет родителю передавать клиенту текст запроса, который клиент шифрует и возвращает к родителю. Если родитель успешно дешифрует текст запроса, клиент аутентифицируется.**Внимание. :** Не используйте режим Общего ключа. При использовании его простой текст и зашифрованная версия тех же данных передают в эфире. Это ничего не получает. Если пользовательский ключ является неправильным, модуль не дешифрует пакеты, и пакеты не могут получить доступ к сети.

- **Клиент**Параметр клиента определяет режим аутентификации что использование узлов клиента для соединения к модулю. Это значения, которые позволены:**Open (RECOMMENDED)** — Этот режим аутентификации является по существу фиктивной операцией. Всем клиентам разрешают аутентифицироваться.**Общий ключ** — Этот режим позволяет родителю передавать клиенту текст запроса, который клиент шифрует и возвращает к родителю. Если родитель успешно дешифрует текст запроса, клиент аутентифицируется.**Оба** — Этот режим позволяет клиенту использовать любой режим.
- **ШифрованиеВыключено** — при установке Параметра шифрования в Выключено никакое шифрование не сделано. Данные передают в ясном.**На (ОБЯЗАТЕЛЬНОМ)** — при установке Параметра шифрования в На зашифрованы все пакеты передаваемых данных, и сбрасывают от любых незашифрованных полученных пакетов.**Смешанный** — В Смешанном режиме, root или мосту повторителя принимает ассоциацию от клиентов, которым включили или выключили шифрование также. В этом случае, только пакеты данных между узлами, что зашифрована обе поддержки. Пакеты групповой адресации представлены ясное. Все узлы видят пакеты.**Внимание. :** Не используйте Смешанный режим. Если клиент, которому включили шифрование, передает пакет групповой адресации его родителю, пакет зашифрован. Родитель дешифрует пакет и повторно передает пакет в ясном ячейке, и другие узлы видят пакет. Способность просмотреть пакет в обеих зашифрованных и незашифрованных формах может способствовать ломке ключа. Включение смешанного режима только для совместимости с другими поставщиками.

Настройте клиентские адаптеры

Необходимо выполнить два основных шага для устанавливания WEP на Клиентском адаптере Aironet:

1. Настройте Ключ WEP/, вводит Менеджера шифрования клиента.
2. Включите WEP в Aironet Client Utility (ACU).

Установите ключи WEP

Выполните эти шаги для устанавливания Ключей WEP на клиентских адаптерах:

1. Открытый ACU и выбирает **Profile Manager**.
2. Выберите профиль, где вы хотите включить WEP и нажать **Edit**.

3. Нажмите **Вкладку Сетевая безопасность**, чтобы отобразить параметры безопасности и нажать **Use Static WEP Keys**.Это действие активирует параметры конфигурации WEP, которые недоступны, когда не выбран Никакой WEP.
4. Для Ключа WEP, который вы хотите создать, выберите или **40 битов** или **128 битов** под Размером КЛЮЧА WEP на правой части окна.**Примечание:** 128-разрядные клиентские адаптеры могут использовать 40-разрядные или 128-разрядные ключи. Но 40-разрядные адаптеры могут только использовать 40-разрядные ключи.**Примечание:** Ваш Ключ WEP клиентского адаптера должен совпасть с Ключом WEP, что другие компоненты WLAN, с которыми вы передаете использование.При установке нескольких Ключей WEP необходимо назначить Ключи WEP на те же номера Ключа WEP для всех устройств. Ключи WEP должны состоять из шестнадцатеричных символов и должны содержать 10 символов для 40-разрядных Ключей WEP или 26 символов для 128-разрядных Ключей WEP. Шестнадцатеричные символы могут быть:От 0 до 9к fK F**Примечание:** Ключи WEP Текста ASCII не поддерживаются на AP Aironet. Если вы планируете использовать свой клиентский адаптер с этими AP, Поэтому необходимо выбрать Hexadecimal (0-9, A-F) опция.**Примечание:** После создания Ключа WEP можно переписать его. Но вы не можете отредактировать или удалить его.**Примечание:** При использовании более поздней версии служебной программы рабочего стола Aironet (ADU) вместо ACU как служебная программа клиента можно также удалить созданный Ключ WEP и заменить его новым.
5. Нажмите кнопку **Transmit Key**, которая является около одного из ключей, которые вы создали.С этим действием вы указываете, что этот ключ является ключом, который вы хотите использовать для передачи пакетов.
6. Нажмите **Persistent** под типом КЛЮЧА WEP.Это действие позволяет вашему клиентскому адаптеру сохранять этот Ключ WEP, даже когда питание к адаптеру удалено или в перезагрузке компьютера, в котором установлен ключ. Когда питание удалено из клиентского адаптера, при выборе Temporary для этой опции Ключ WEP потерян.
7. **Нажмите кнопку ОК.**

Включите WEP

Выполните следующие действия:

1. Открытый ACU и выбирает **Edit Properties** из строки меню.
2. Нажмите **Вкладку Сетевая безопасность** для отображения параметров безопасности.
3. Проверьте флажок **Enable WEP** для активации WEP.

См. WEP Настройки в ADU для шагов для настройки WEP с помощью ADU в качестве служебной программы клиента.

Настройте мосты рабочей группы

Существуют различия между Aironet Мост рабочей группы серии 340 и Aironet Мост серии 340. Однако конфигурация Моста рабочей группы для использования WEP почти идентична конфигурации Моста. Посмотрите Настраивать раздел Мостов Aironet для конфигурации Моста.

1. Соединитесь с мостом рабочей группы.

2. Перейдите к Меню Конфиденциальность.Выберите **Main> Configuration> Radio>> Privacy I80211** для доступа к меню Privacy VxWorks.

Параметры настройки

Меню Конфиденциальность представляет параметры настройки, которые перечисляет этот раздел. Настройте опции на Мосту рабочей группы в этом заказе:

1. Ключ
2. Передача
3. Auth
4. Шифрование

Это опции:

- **Ключ**Опция Key устанавливает Ключ WEP, который мост использует для получения пакетов. Значение должно совпасть с ключом, что AP или другое устройство, с которым Мост рабочей группы передает использование. Ключ состоит максимум из 10 шестнадцатеричных символов для 40-разрядного шифрования или 26 шестнадцатеричных символов для 128-разрядного шифрования. Шестнадцатеричные символы могут быть любой комбинацией этих цифр:От 0 до 9к fK F
- **Передача**Опция Transmit устанавливает Ключ WEP, который мост использует для передачи пакетов. Можно выбрать использовать тот же ключ, который вы использовали для опции Key. При выборе другого ключа необходимо установить соответствие, включают AP.Только один Ключ WEP может использоваться когда-то для передач. Ключ WEP, который вы используете для передачи данных, должен быть установлен в то же значение на Мосту рабочей группы и других устройствах, с которыми это связывается.
- **Аутентификация (Аутентификация)**Параметр Auth определяет, какой метод проверки подлинности система использует. Имеются следующие варианты:**Open (RECOMMENDED)** — Значение Open по умолчанию позволяет любому AP, независимо от его Параметров настройки WEP, аутентифицироваться и затем пытаться связаться с мостом.**Общий ключ** — Эта установка дает мосту команду передавать простой текст, запрос общего ключа к AP в попытке связаться с мостом. Параметр Общий ключ может оставить мост открытым для атаки с известным текстом от злоумышленников. Поэтому эта установка не так безопасна как Значение Open.
- **Шифрование**Параметр шифрования устанавливает параметры шифрования на всех пакетах данных, кроме пакетов связывания и некоторых управляющих пакетов. Существует четыре опции:**Примечание:** AP должен иметь активное шифрование и кнопочный телефонный аппарат должным образом.**Выключено** — Это - настройка по умолчанию. Все шифрование выключено. Мост рабочей группы не связывается с AP с использованием WEP.**На (RECOMMENDED)** — Эта установка требует шифрования всех передач данных. Мост рабочей группы только передает с AP тот WEP использования.**Смешанный на** — Эта установка означает, что мост всегда использует WEP для передачи с AP. Однако AP связывается со всеми устройствами, используют ли они WEP или не используют WEP.**Смешанный прочь** — Эта установка означает, что мост не использует WEP для передачи с AP. Однако AP связывается со всеми устройствами, используют ли они WEP или не используют WEP.**Внимание. :** Если вы выбираете На или Mixed на как категория WEP, и вы настраиваете мост через его радио соединение, подключение в мост потеряно при установке Ключа WEP неправильно.

Удостоверьтесь, что вы используете точно те же параметры настройки при установке Ключа WEP на Мосту рабочей группы и Ключа WEP на других устройствах на WLAN.

Дополнительные сведения

- Ассоциация стандартов IEEE
- Оборудование для беспроводных LAN Aironet 340
- Ресурсы поддержки беспроводных сетей
- Страница поддержки беспроводных сетей LAN
- Руководство по конфигурации программного обеспечения Cisco IOS для точек доступа Cisco Aironet
- Руководство по настройке ПО Cisco IOS для внешней точки доступа Cisco Aironet серии 1300 / мост
- Руководство по конфигурации программного обеспечения точки доступа Cisco Aironet для VxWorks
- Руководство по конфигурации программного обеспечения моста Cisco Aironet серии 1400
- Руководства по конфигурации клиентских адаптеров беспроводной локальной сети Cisco Aironet
- Общие сведения по обеспечению безопасности беспроводной сети LAN Cisco
- Беспроводные сети (мобильность) беспроводные сети обеспечения
- Пример конфигурации точки доступа в качестве моста рабочей группы
- Часто задаваемые вопросы о мосте рабочей группы Cisco Aironet
- Password Recovery Procedure for the Cisco Aironet Equipment
- Cisco Aironet Access Point FAQ
- Cisco Systems – техническая поддержка и документация