Пример настройки защищенного доступа Wi-Fi 2 (WPA 2)

Содержание

Введение
Предварительные условия
- Требования
- Используемые компоненты
- Условные обозначения

Общие сведения
- Поддержка WPA 2 при помощи оборудования Cisco Aironet

Настройка в режиме enterprise
- Настройка сети
- Настройка точки доступа
- Настройка клиентского адаптера
- Проверка
- Поиск и устранение неисправностей

Настройка в режиме personal
- Настройка сети
- Настройка точки доступа
- Настройка клиентского адаптера
- Проверка
- Поиск и устранение неисправностей

Дополнительные сведения

Введение

В настоящем документе описываются преимущества использования защищенного доступа Wi-Fi 2 (WPA 2) в беспроводных LAN (WLAN). Документ содержит два примера настройки WPA 2 на WLAN. Первый пример демонстрирует настройку WPA 2 в корпоративном режиме, а второй – настройку WPA 2 в персональном режиме.

Примечание: WPA работает при помощи протокола расширенной аутентификации (EAP).

Предварительные условия

Требования

Перед проведением настройки необходимо получить следующие общие знания:

- WPA
- Способы обеспечения безопасности WLAN

  Примечание: Для получения информации о способах обеспечения безопасности WLAN Cisco см. Обзор системы безопасности беспроводных LAN Cisco Aironet.

Используемые компоненты

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

- Точка доступа (AP) и мост Cisco Aironet 1310G, использующие программное обеспечение Cisco IOS® релиза 12.3(2)JA
- Клиентский адаптер Aironet 802.11a/b/g CB21AG, использующий микропрограмму 2.5
- Aironet Desktop Utility (ADU), использующий микропрограмму 2.5

Примечание: Программное обеспечение клиентских адаптеров Aironet CB21AG и PI21AG несовместимо с программным обеспечением других клиентских адаптеров Aironet. Необходимо использовать ADU с платами CB21AG и PI21AG, а также Aironet Client Utility (ACU) всех других клиентских адаптеров Aironet. Для получения дополнительной информации о том, как настроить плату CB21AG и ADU, обратитесь к документу Установка клиентского адаптера.

Примечание: Данный документ касается точки доступа или моста, имеющих встроенную антенну. Если вы используете точку доступа или мост, требующие установки внешней антенны, необходимо убедиться в том, что антенны подключены к точке доступа или мосту. Иначе точка доступа или мост не сможет подключиться к беспроводной сети. Некоторые модели точек доступа или мостов производятся со встроенными антеннами, в то время как другим нужна для работы внешняя антенна. Для получения информации о том, какие модели точек доступа или мостов поставляются с встроенными, а какие с внешними антеннами, обратитесь к руководству по заказу или руководству по продукту соответствующего устройства.

Сведения, представленные в данном документе, были получены на тестовом оборудовании в специально созданных лабораторных условиях. При написании данного документа использовались только данные, полученные от устройств с конфигурацией по умолчанию. В рабочей сети необходимо понимать последствия выполнения всех команд.

Условные обозначения

Для получения дополнительной информации об условных обозначениях в документе обратитесь к разделу Условные обозначения технических терминов Cisco.

Общие сведения

WPA – это стандартный способ обеспечения безопасности Wi-Fi Alliance, учитывающий уязвимые места в сетях WLAN. WPA обеспечивает улучшенную защиту данных и контроль доступа к системам WLAN. WPA учитывает все известные уязвимые места протокола шифрования в беспроводной связи (WEP) исходного механизма обеспечения безопасности IEEE 802.11 и обеспечивает безопасность сетей WLAN на предприятиях, в домашних сетях и небольших компаниях.

WPA 2 – это следующее поколение систем безопасности Wi-Fi. WPA 2 – это совместимая с Wi-Fi Alliance улучшенная версия одобренного стандарта IEEE 802.11i. WPA 2 выполнен на основе рекомендованного Национальным институтом стандартов и технологий (NIST) алгоритма шифрования AES (улучшенного стандарта шифрования) с использованием режима счетчика и протокола CCMP. Режим счетчика AES – это блочный шрифт, за раз шифрующий 128 битовый блок данных при помощи 128 битового ключа шифрования. Алгоритм CCMP генерирует код целостности сообщений (MIC), обеспечивающий беспроводному фрейму проверку подлинности происхождения данных и целостность данных.

Примечание: CCMP также может называться CBC-MAC.

WPA 2 предлагает более высокий уровень безопасности, чем WPA, так как AES обеспечивает более стойкое шифрование, нежели протокол TKIP. TKIP – это протокол шифрования, используемый WPA. WPA 2 создает новые ключи сеанса при каждом сопоставлении. Ключи шифрования, используемые для каждого клиента сети, являются уникальными для этого клиента. В итоге каждый пакет, посылаемый в эфир, зашифрован при помощи уникального ключа. Система безопасности улучшена использованием нового и уникального ключа шифрования, так как повторно ключ не используется. WPA все еще считается безопасным, а протокол TKIP не был взломан. Тем не менее, Cisco рекомендует своим клиентам как можно скорее перейти на WPA 2. Для получения дополнительной информации о WPA и WPA 2 обратитесь к документу Защищенный доступ Wi-Fi, WPA2 и IEEE 802.11i.

WPA и WPA 2 поддерживают два режима работы:

- Режим enterprise
- Режим personal

Настоящий документ рассматривает применение этих двух режимов WPA 2.

Поддержка WPA 2 при помощи оборудования Cisco Aironet

WPA 2 поддерживается следующим оборудованием:

- Точки доступа серии Aironet 1130AG и серии 1230AG
- Точки доступа серии Aironet 1100
- Точки доступа серии Aironet 1200
- Точки доступа серии Aironet 1300

Примечание: Эти точки доступа необходимо оборудовать радиоприемниками 802.11g и программным обеспечением Cisco IOS релиза 12.3(2)JA или более поздних.

WPA 2 и AES поддерживаются также на:

- Радио модулях серии Aironet 1200 с шифрами компонента AIR-RM21A и AIR-RM22A

  Примечание: Радио модуль Aironet 1200 с шифром компонента AIR-RM20A не поддерживает WPA 2.
- Клиентских адаптерах Aironet 802.11a/b/g, использующих микропрограмму 2.5

Примечание: Продукты серии Cisco Aironet 350 не поддерживают WPA 2, так как у их радиоприемников отсутствует поддержка AES.

Примечание: WPA 2 не поддерживается на маршрутизаторе ISR или точках доступа на платах интерфейса высокоскоростных WAN (HWIC).

Примечание: Беспроводные мосты серии Cisco Aironet 1400 не поддерживают WPA 2 или AES.

Настройка в режиме enterprise

Термин **режим enterprise** относится к продуктам, имеющим возможность взаимодействия с режимами работы аутентификации Pre-Shared Key (PSK) и IEEE 802.1x. Режим 802.1x считается более безопасным, чем любая другая существующая инфраструктура аутентификации, благодаря своей гибкости в поддержке разнообразных механизмов аутентификации и стойким алгоритмам шифрования. WPA 2 в режиме enterprise осуществляет аутентификацию в два этапа. В первой фазе происходит настройка открытой аутентификации. Во второй фазе происходит аутентификация 802.1x с одним из методов EAP. AES обеспечивает механизм шифрования.

В режиме enterprise клиенты и сервера аутентификации подтверждают подлинность друг друга при помощи метода аутентификации EAP, а затем и клиент и сервер генерируют PMK (Pairwise Master Key). При использовании WPA 2 сервер динамически генерирует PMK и передает его на точку доступа.

В данном разделе рассматривается настройка, необходимая для реализации WPA 2 в режиме работы enterprise.

Настройка сети

В данной настройке точка доступа или мост Aironet 1310G, использующие протокол Cisco LEAP (протокол облегченной расширенной аутентификации), аутентифицируют пользователя с WPA 2-совместимым клиентским адаптером. Управление ключами происходит при помощи WPA 2, для которого настроено шифрование AES-CCMP. Точка доступа настроена как локальный RADIUS сервер,

выполняющий LEAP аутентификацию. Для реализации этой настройки необходимо настроить клиентский адаптер и точку доступа. Разделы Настройка AP и Настройка клиентского адаптера описывают настройку точки доступа и клиентского адаптера.

Настройка точки доступа

Необходимо выполнить следующие действия:

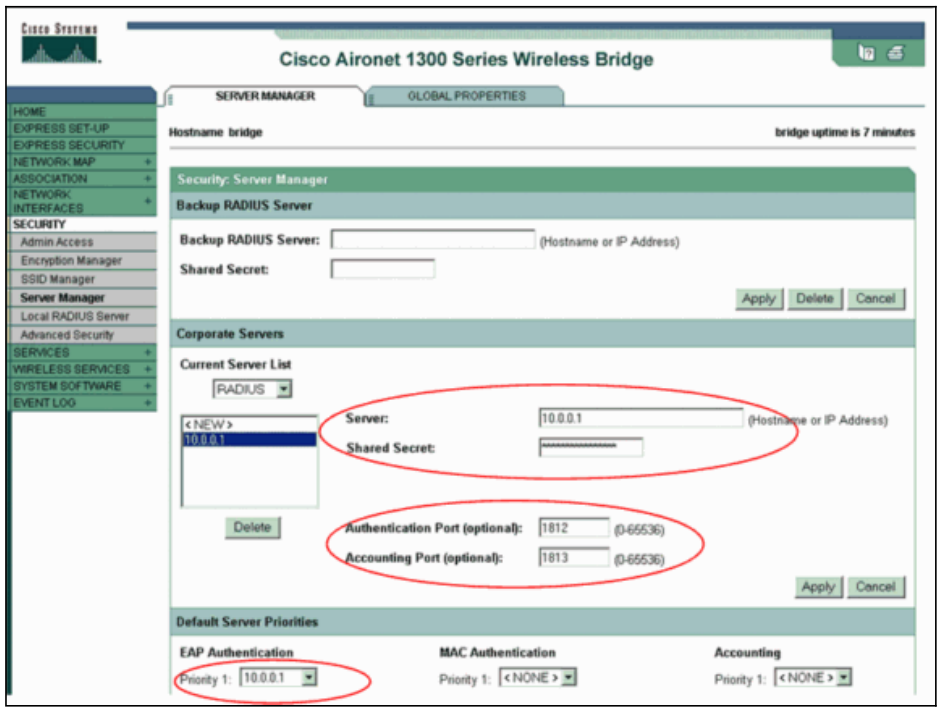
1. Настроить точку доступа как локальный RADIUS сервер, выполняющий LEAP аутентификацию.

    1. Выбрать **Security > Server Manager** в меню слева и определить IP адрес, порты и общий секретный ключ RADIUS сервера.

        Так как при данной конфигурации точка доступа настроена как RADIUS сервер, нужно использовать IP адрес точки доступа. Для работы локального RADIUS сервера необходимо использовать порты 1812 и 1813.

    2. В зоне Default Server Priorities определить приоритет EAP аутентификации по умолчанию как 10.0.0.1.

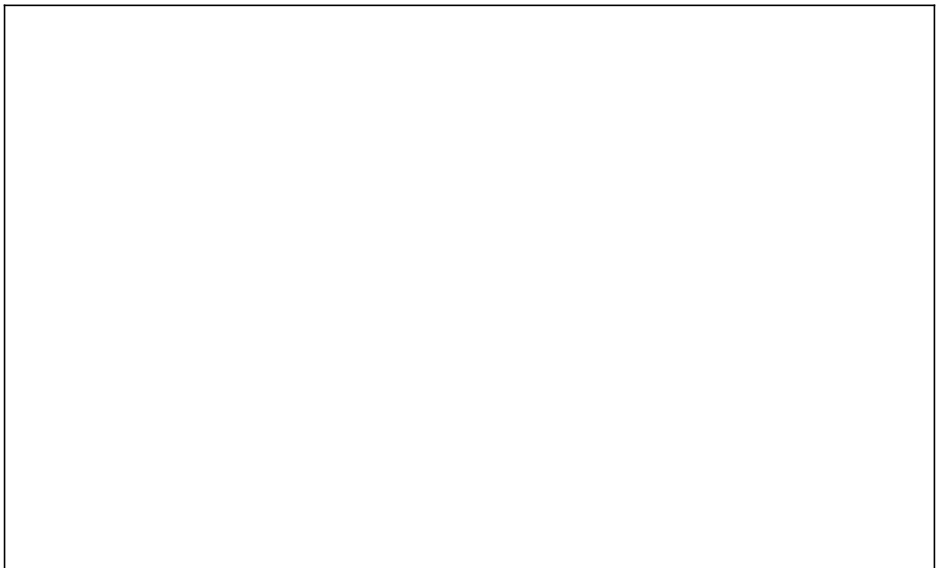
        Примечание: 10.0.0.1 – это локальный RADIUS сервер.



2. Выбрать **Security > Encryption Manager** из меню слева и выполнить следующие действия:

    1. Из меню Cipher, выбрать **AES CCMP**.

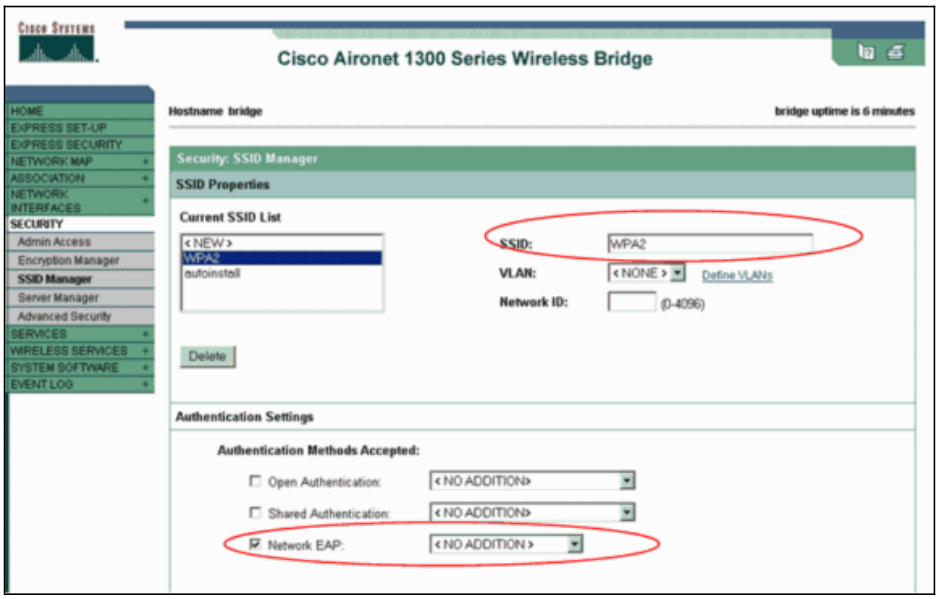
        Это действие включает AES шифрование с использованием режима счетчика с CBC-MAC.



2. Нажать **Apply**.

3. Выбрать **Security > SSID Manager** и создать новый Service Set Identifier (SSID – идентификатор набора служб) для использования с WPA 2.

1. Установить флажок **Network EAP** в зоне Authentication Methods Accepted.



Примечание: При настройке типа аутентификации на интерфейсах радиоприемников необходимо пользоваться следующими указаниями:

- Клиентами Cisco должен использоваться сетевой EAP.
- Клиентами стороннего производителя (включая продукты, совместимые с CCX [разрешения, совместимые с Cisco]) должна использоваться открытая аутентификация с EAP.
- Использующим сочетание клиентских устройств Cisco и сторонних производителей необходимо выбрать и сетевой EAP и открытую аутентификацию с EAP.

2. Выполнить прокрутку вниз окна Security SSID Manager до зоны Authenticated Key Management и выполнить следующие действия:

1. Из меню Key Management, выбрать **Mandatory**.
2. Установить флажок **WPA** справа.

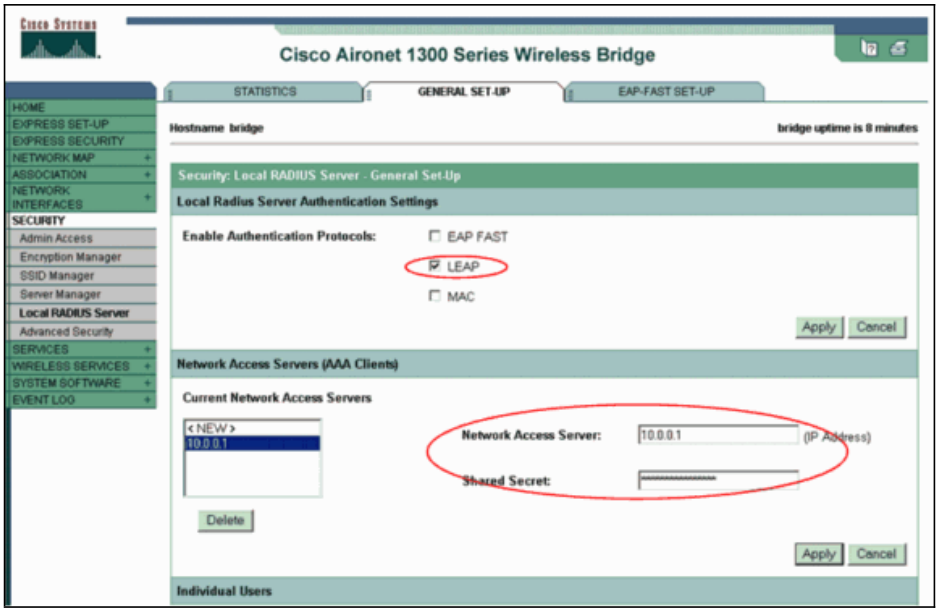
3. Нажать **Apply**.

Примечание: Определение VLAN является необязательным. Если VLAN будет определена, то клиентские устройства, связанные с использованием данного SSID, сгруппируются в VLAN. Для получения дополнительной информации о реализации VLAN см. раздел Настройка VLAN.

4. Выбрать **Security > Local Radius Server** и выполнить следующие действия:

   1. Нажать на закладку **General Set-Up**, расположенную вверху окна.
   2. Установить флажок **LEAP** и нажать **Apply**.
   3. В зоне Network Access Servers определить IP адрес и общий секретный ключ RADIUS сервера.

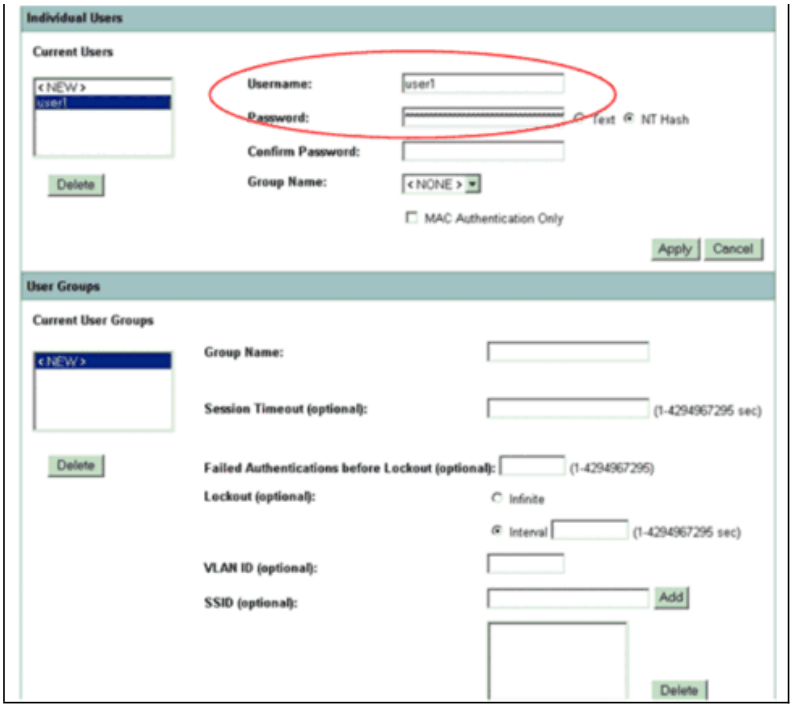
      Для локального RADIUS сервера необходимо использовать IP адрес точки доступа.



   4. Нажать **Apply**.

5. Выполнить прокрутку вниз окна General Set-Up до зоны Individual Users и определить индивидуальных пользователей.

   Определение групп пользователей является необязательным.



Такая конфигурация определяет пользователя с именем "user1" и пароль. Также конфигурация выбирает NT хеш для пароля. После выполнения процедуры, описанной в данном разделе, точка доступа готова принимать запросы на аутентификацию от клиентов. Следующим шагом является настройка клиентского адаптера.

Настройка клиентского адаптера

Необходимо выполнить следующие действия:

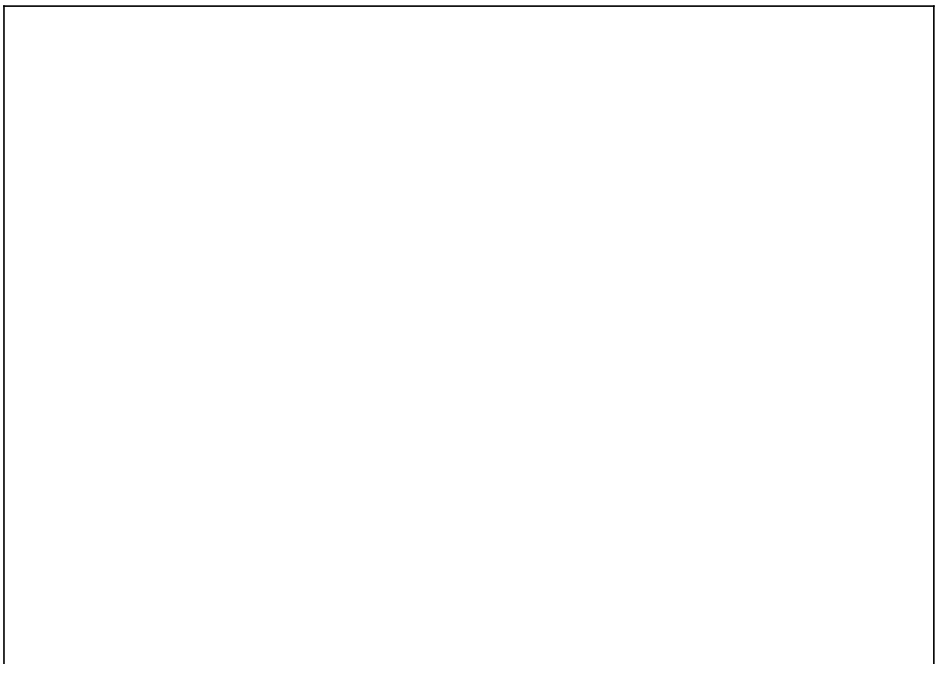
Примечание: В настоящем документе используется клиентский адаптер Aironet 802.11a/b/g, работающий под управлением микропрограммы 2.5, а также описывается настройка клиентского адаптера с ADU версии 2.5.

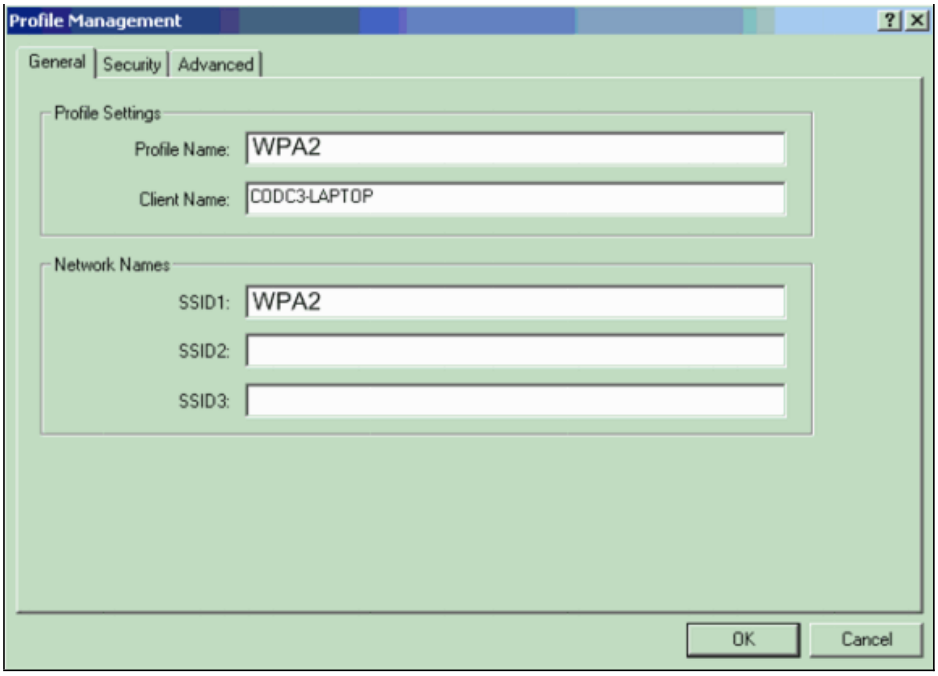
1. В окне Profile Management на ADU необходимо нажать **New**, чтобы создать новый профиль.

   Отобразится новое окно, в котором можно задать конфигурацию режима работы WPA 2 enterprise. На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.

   В этом примере именем профиля и SSID является WPA2:

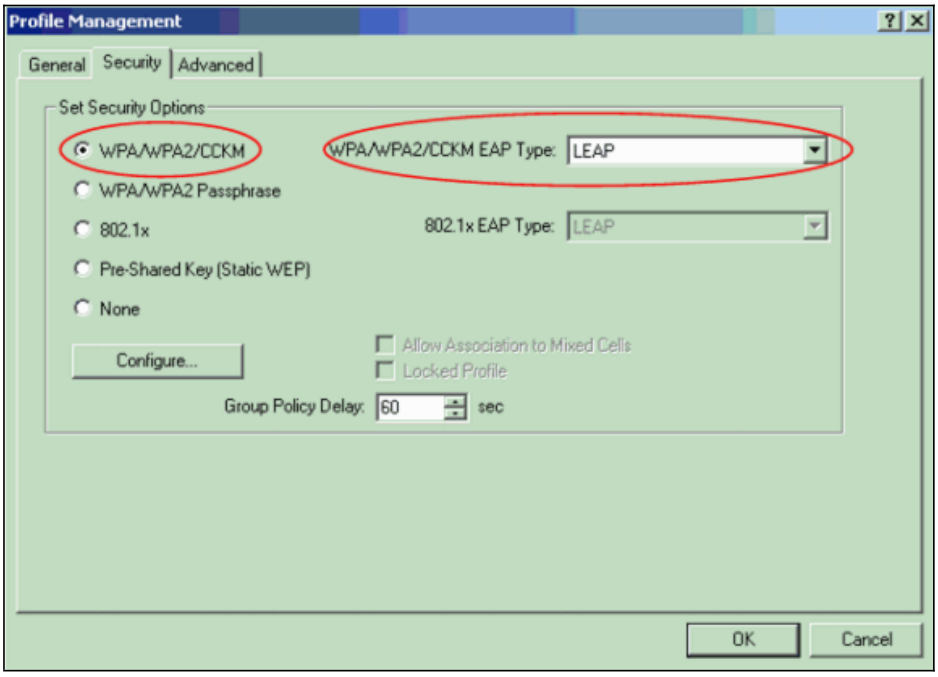
   Примечание: SSID должен соответствовать SSID, настроенному для WPA 2 на точке доступа.





2. Нажать на закладку **Security**, нажать **WPA/WPA2/CCKM**и выбрать **LEAP** из меню WPA/WPA2/CCKM EAP Type.

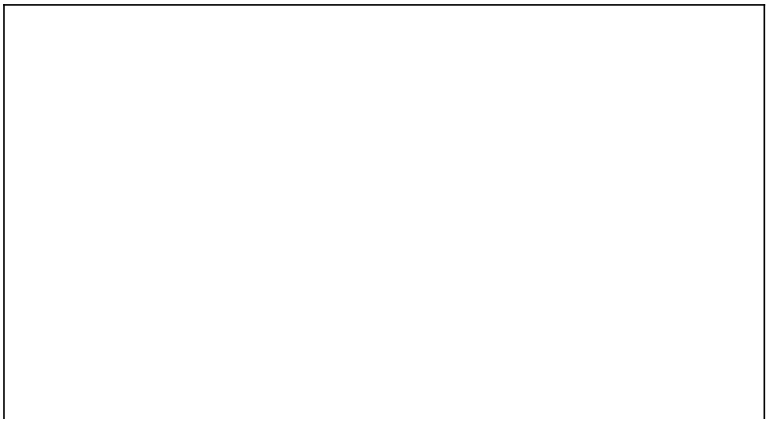
   Это действие подключает WPA или WPA 2, в зависимости от того, что было настроено на точке доступа.

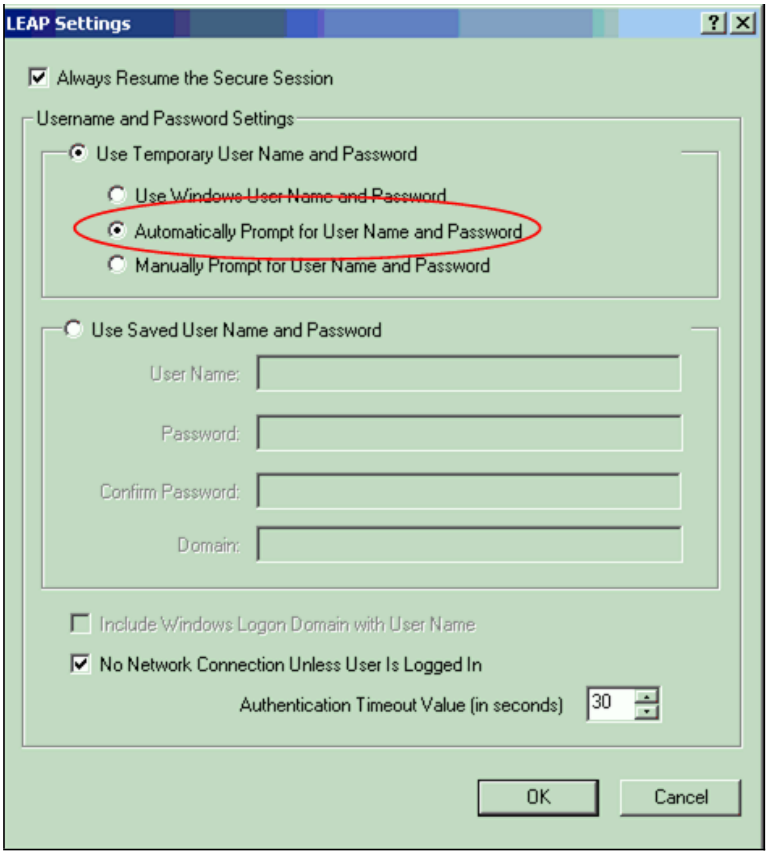


3. Нажать **Configure** для определения установок LEAP.

4. Выбрать на основании требований соответствующие имя пользователя (Username) и установки пароля (Password Settings) и нажать **OK**.

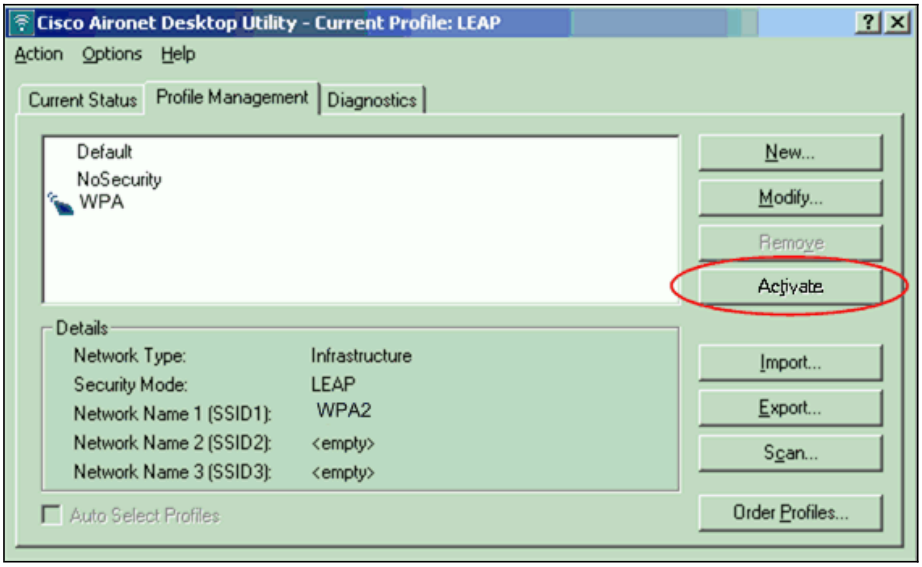
   Даная конфигурация выбирает опцию Automatically Prompt для имени пользователя и пароля. Эта опция позволяет при использовании LEAP аутентификации вручную ввести имя пользователя и пароль.





5. Нажать **OK**, чтобы выйти из окна Profile Management.

6. Нажать **Activate**, чтобы активировать этот профиль на клиентском адаптере.



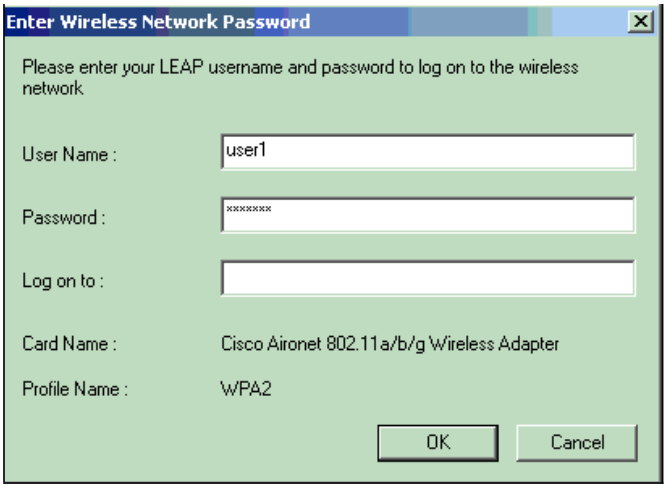
Примечание: При использовании для настройки клиентского адаптера нулевой конфигурации беспроводных сетей Microsoft (WZC) по умолчанию WPA 2 будет недоступным. Поэтому для того, чтобы позволить клиентам с включенной WZC использовать WPA 2, необходимо установить hot fix для Microsoft Windows XP. Для установки обратитесь к ресурсу Центр загрузки ПО Microsoft – Обновления для Windows XP (KB893357) .

После установки hot fix можно настроить WPA 2 при использовании WZC.

Проверка

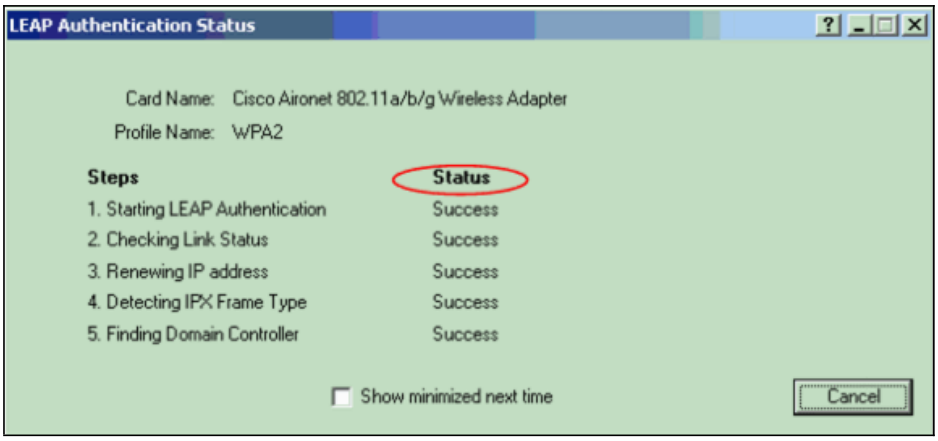
Этот раздел позволить проверить правильность работы конфигурации.

1. При отображении окна Enter Wireless Network Password введите имя пользователя и пароль.



Следующее окно – LEAP Authentication Status. На этой фазе учетные записи пользователей проверяются на локальном RADIUS сервере.

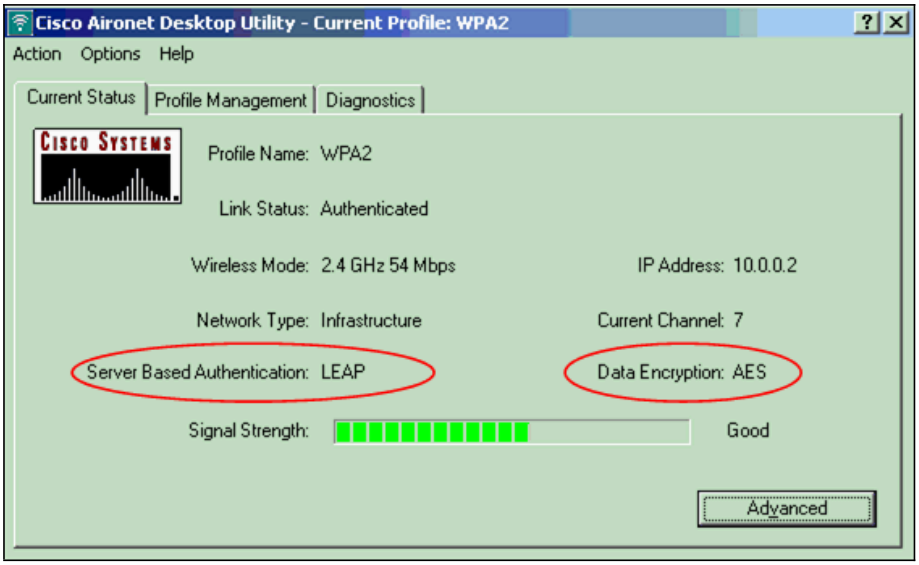
2. Для того, чтобы увидеть результат аутентификации, необходимо проверить зону Status.



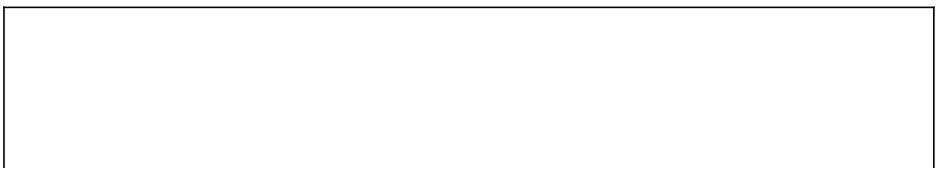
При успешном завершении аутентификации клиент подключится к беспроводной LAN.

3. Чтобы убедиться в том, что клиент использует AES шифрование и LEAP аутентификацию, необходимо проверить ADU Current Status.

Это покажет, что в WLAN был реализован WPA 2 с LEAP аутентификацией и AES шифрованием.



4. Чтобы убедиться в том, что клиент успешно прошел аутентификацию при помощи WPA 2, необходимо проверить журнал событий точки доступа/моста.



Поиск и устранение неисправностей

В настоящее время для данной конфигурации отсутствуют специфические рекомендации по поиску и устранению неисправностей.

Настройка в режиме personal

Термин **режим personal** относится к продуктам, имеющим возможность взаимодействия с режимом работы аутентификации PSK-only. Данный режим предполагает ручную настройку PSK на точке доступа и клиенте. PSK аутентифицирует пользователей при помощи пароля или идентификационного кода на клиентской станции и на точке доступа. Сервер аутентификации не требуется. Клиент может получить доступ к сети только если пароль клиента соответствует паролю точки доступа. Пароль также обеспечивает ключевой материал, используемый TKIP или AES для генерации ключа шифрования для шифрования пакетов данных. Режим personal нацелен на среды SOHO, а также считается безопасным для сред предприятий. В данном разделе рассматривается настройка, необходимая для реализации WPA 2 в режиме работы personal.

Настройка сети

В данной настройке пользователь с клиентским адаптером, совместимым с WPA 2, аутентифицируется на точке доступа или мосту Aironet 1310G. Управление ключами происходит при помощи WPA 2 PSK, для которого настроено шифрование AES-CCMP. Разделы Настройка AP и Настройка клиентского адаптера описывают настройку точки доступа и клиентского адаптера.

Настройка AP

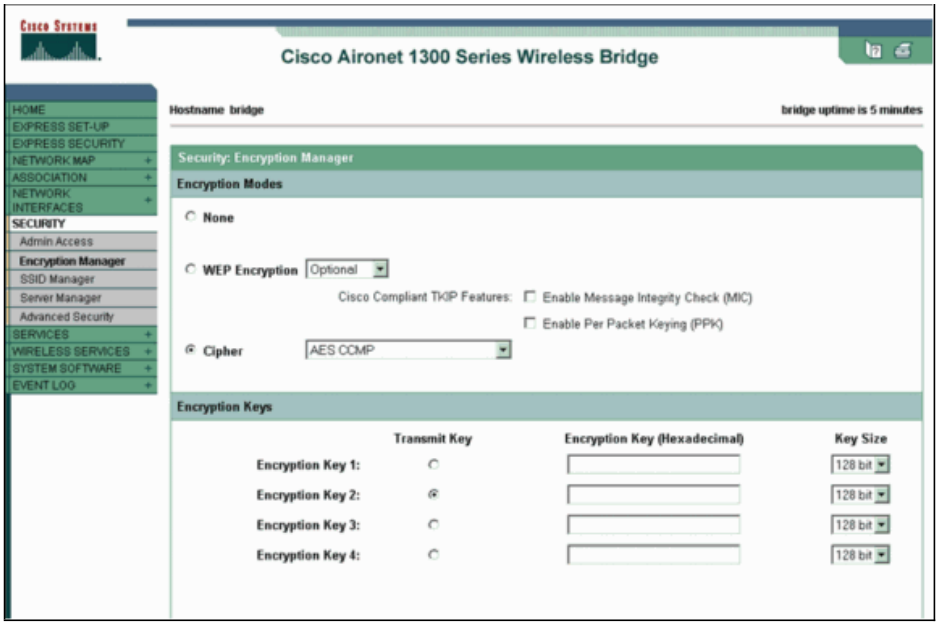
Необходимо выполнить следующие действия:

1. Выбрать **Security > Encryption Manager** в меню слева и выполнить следующие действия:

    1. Из меню Cipher, выбрать **AES CCMP**.

        Это действие включает AES шифрование с использованием режима счетчика с CCMP.

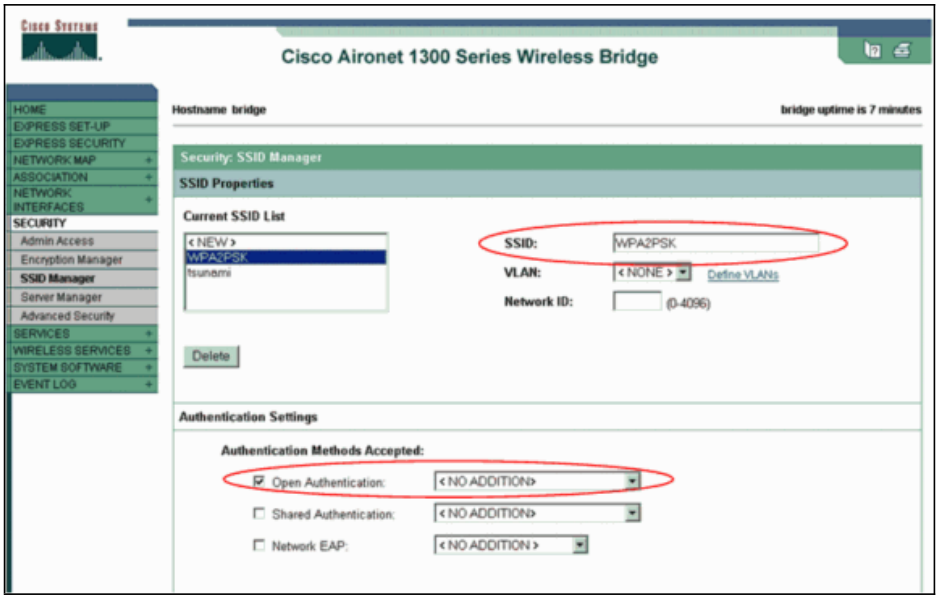
        



2. Нажать **Apply**.

2. Выбрать **Security > SSID Manager** и создать новый SSID для использования с WPA 2.

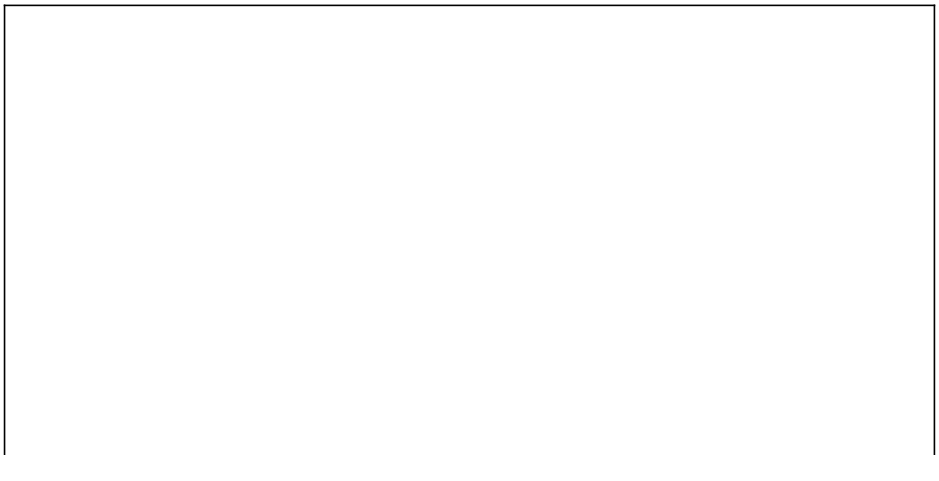
1. Установить флажок **Open Authentication**.



2. Выполнить прокрутку вниз по окну Security: SSID Manager до зоны Authenticated Key Management и выполнить следующие действия:

1. Из меню Key Management, выбрать **Mandatory**.

2. Установить флажок **WPA** справа.



3. Ввести общий секретный ключ WPA PSK или ключ идентификационной фразы WPA PSK.

   Этот ключ должен соответствовать ключу WPA PSK, настроенному на клиентском адаптере.

4. Нажать **Apply**.

Теперь точка доступа может получать запросы на аутентификацию от беспроводных клиентов.

Настройка клиентского адаптера

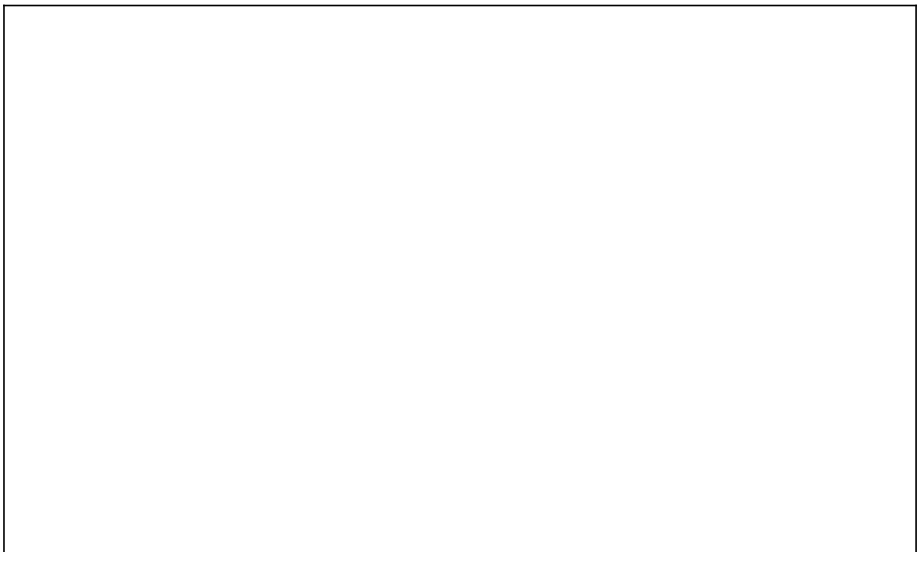
Необходимо выполнить следующие действия:

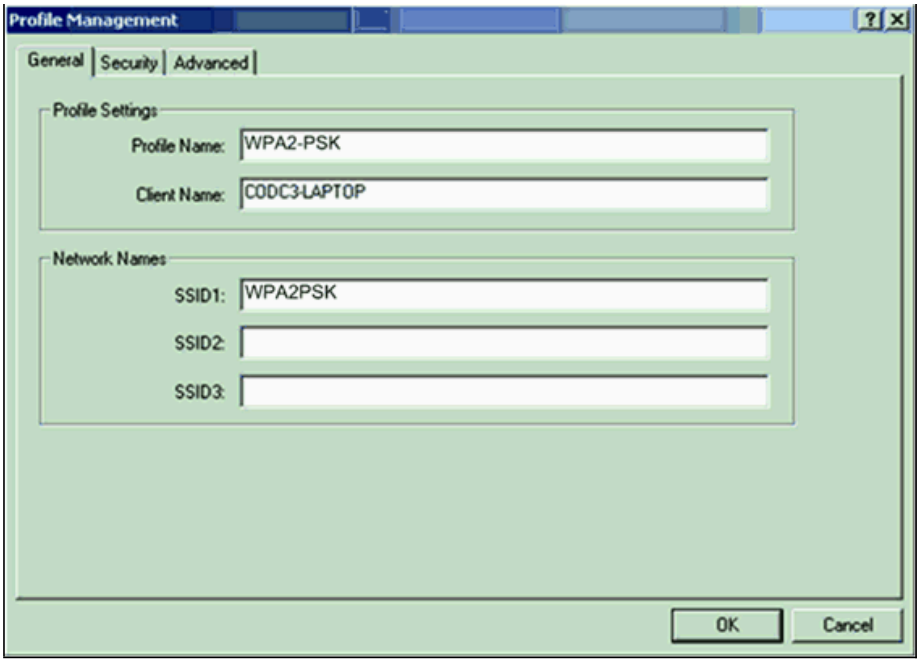
1. В окне Profile Management на ADU необходимо нажать **New**, чтобы создать новый профиль.

   Отобразится новое окно, в котором можно задать конфигурацию режима работы WPA 2 PSK. На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.

   В этом примере используется имя профиля WPA2-PSK и SSID – WPA2PSK:

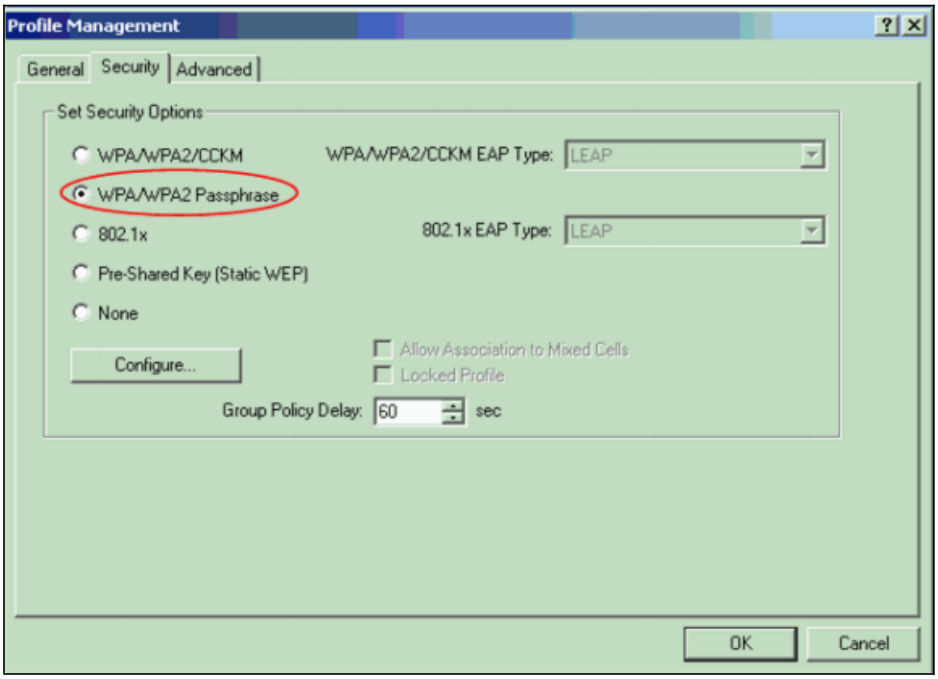
   Примечание: SSID должен соответствовать SSID, настроенному для WPA 2 PSK на точке доступа.





2. Нажать закладку **Security** и нажать **WPA/WPA2 Passphrase**.

   Это действие подключает WPA PSK или WPA 2 PSK , в зависимости от того, что было настроено на точке доступа.



3. Нажать **Configure**.

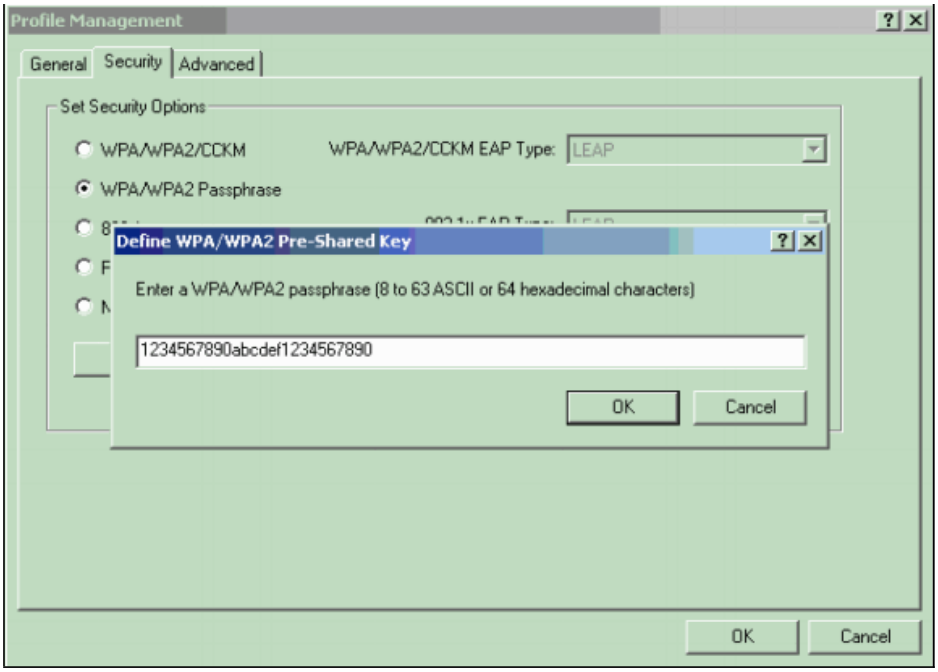
   Отобразится окно Define WPA/WPA2 Pre-Shared Key.

4. Необходимо получить у системного администратора идентификационную фразу WPA/WPA2 и ввести ее в поле WPA/WPA2 passphrase.

   Необходимо получить идентификационную фразу для точки доступа в инфраструктуре сети или идентификационную фразу для других клиентов в специальной сети.

   При введении идентификационной фразы необходимо придерживаться следующих указаний:

   - Идентификационные фразы WPA/WPA2 должны содержать от 8 до 63 ASCII текстовых символов или 64 шестнадцатеричных символа.
   - Идентификационная фраза клиентского адаптера должна соответствовать идентификационной фразе точки доступа, с которой планируется взаимодействовать.



5. Нажать **OK**, чтобы сохранить идентификационную фразу и вернуться в окно Profile Management.

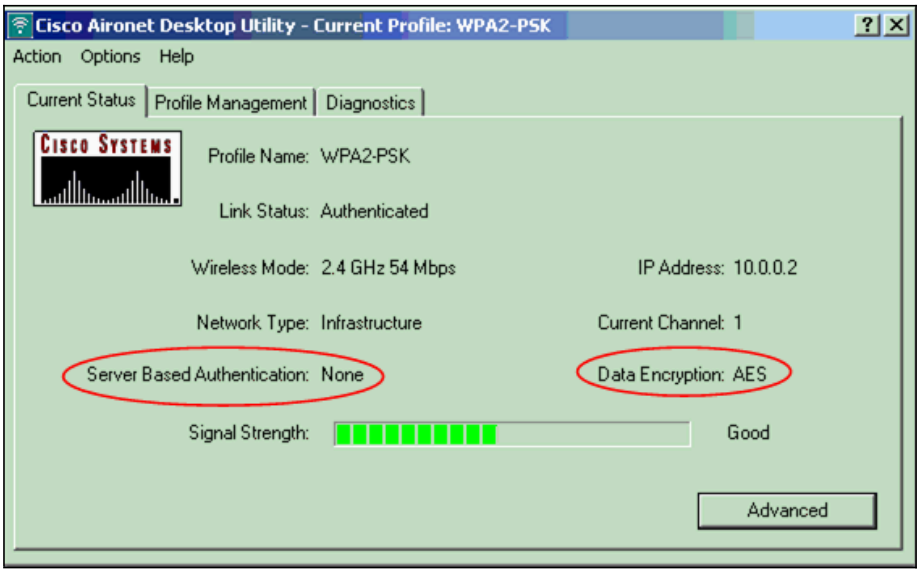
Проверка

Этот раздел позволить проверить правильность работы конфигурации.

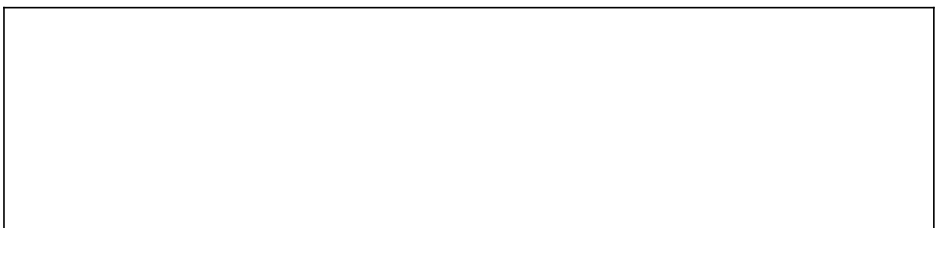
После активации профиля WPA 2 PSK точка доступа аутентифицирует клиента на основании идентификационной фразы WPA 2 (PSK) и обеспечивает доступ к WLAN.

1. Чтобы убедиться в том, что клиент успешно прошел аутентификацию, необходимо проверить ADU Current Status.

   Следующее окно содержит пример. В окне показано, что использовалось шифрование AES и не выполнялась серверная аутентификация:



2. Чтобы убедиться в том, что клиент успешно прошел аутентификацию при помощи режима аутентификации WPA 2 PSK, необходимо проверить журнал событий точки доступа/моста.



Поиск и устранение неисправностей

В настоящее время для данной конфигурации отсутствуют специфические рекомендации по поиску и устранению неисправностей.

Дополнительные сведения

- **Настройка Cipher Suites и WEP**
- **Настройка типов аутентификации**
- **Обзор конфигураций WPA**
- **WPA2 – защищенный доступ Wi-Fi 2**
- **Защищенный доступ Wi-Fi, WPA2 и IEEE 802.11i**
- **Страница поддержки беспроводных сетей**
- **Техническая поддержка и документация – Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92051/wpa2_config.shtml