



Пример выполнения базовых настроек для беспроводного соединения LAN

Содержание

Введение

Предварительные условия

- Требования
- Используемые компоненты
- Схема сети
- Условные обозначения

Конфигурация

- Настройка точки доступа Cisco
- Пошаговые инструкции
- Настройка адаптера беспроводного клиента
- Пошаговые инструкции

Проверка

Устранение неполадок

Дополнительные сведения

Введение

В настоящем документе рассматривается пример настройки базового беспроводного соединения LAN (WLAN) посредством точки беспроводного доступа Cisco Aironet (Cisco Aironet Access Point) и компьютеров, оснащенных клиентскими адаптерами, совместимыми с оборудованием Cisco. В приводимом примере используется графический интерфейс пользователя.

Предварительные условия

Требования

Перед выполнением настройки убедитесь, что выполняются следующие условия:

- Знание основ технологии беспроводного (радио-) доступа
- Знакомство с базовыми принципами доступа к точке доступа Cisco

В настоящем документе предполагается, что на ПК уже установлены все необходимые драйверы и клиентские беспроводные карты.

Используемые компоненты

Сведения, содержащиеся в данном документе, получены в результате использования следующих версий программного и аппаратного обеспечения:

- Одна точка доступа Aironet 1200 Series, использующая ПО Cisco IOS® Software версии 12.3(7)JA

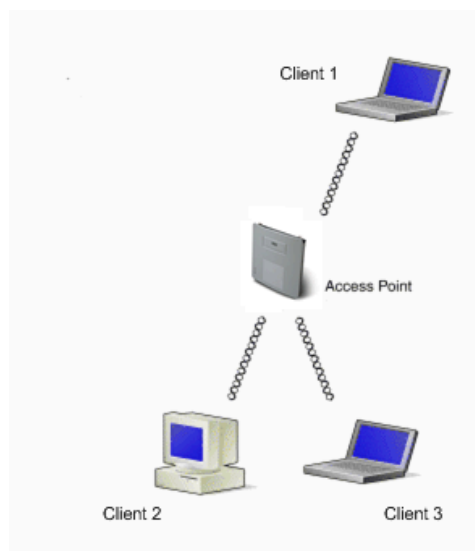
- Три клиентских адаптера точки Aironet 802.11a/b/g, использующие микропрограмму версии 2.5
- Утилита Aironet Desktop Utility (ADU) версии 2.5

Примечание: В настоящем документе описывается точка доступа, оснащенная внутренней (встроенной) антенной. Если вы используете точку доступа, имеющую внешнюю антенну, тогда убедитесь, что эта антенна подключена к точке доступа. В противном случае точка доступа не сможет подключиться к беспроводной сети. Некоторые модели точек доступа оснащены встроенными антеннами, в то время как другие модели требуют наличия внешней антенны. Для получения сведений об точках доступа, оснащенных внешними или внутренними антеннами, обратитесь к справочному руководству, которое прилагается к соответствующему устройству.

Информация, представленная в этом документе, была получена при использовании устройств в специальных лабораторных условиях. При написании данного документа использовались только устройства с "чистой" (стандартной) конфигурацией. При работе в условиях реальной сети оператор должен понимать последствия использования любой команды или изменений, внесенных в графическом интерфейсе пользователя.

Схема сети

В данном документе используется следующая схема сети:



На схеме сети изображены три клиентских адаптера Aironet 802.11a/b/g, подключенных к точке доступа 1200 AP. В документе описывается настройка клиентских адаптеров, которая позволяет адаптерам взаимодействовать друг с другом посредством беспроводного интерфейса.

Точка доступа использует следующие настройки:

- Идентификатор набора служб (Service Set Identifier – SSID): **CISCO123**
- Базовая аутентификация: Открытая аутентификация с шифрованием WEP (Wired Equivalent Privacy)

В настоящем документе описывается процедура настройки точки доступа и клиентских адаптеров.

Примечание: можно также использовать и другие методы шифрования и аутентификации. Более подробно о поддерживаемых методах аутентификации см. Настройка типов аутентификации. Более подробно о различных поддерживаемых методах шифрования см. Настройка пакетов Cipher Suites и WEP.

Условные обозначения

См. Технические советы Cisco. Условные обозначения для получения дополнительной информации об условных обозначениях в документах.

Настройка

Настройка точки доступа

Точку доступа можно настроить при помощи одного из следующих средств:

- Графический интерфейс пользователя
- Интерфейс командной строки (после установления сеанса Telnet)
- Консольный порт

Примечание: чтобы подключиться к точке доступа через консольный порт, последовательный порт RS-232 точки доступа необходимо соединить с СОМ-портом ПК посредством 9-штырькового прямого последовательного кабеля DB-9. Для установления соединения с точкой доступа необходимо настроить эмулятор терминала. Для настройки соединения через эмулятор терминала необходимо использовать следующие настройки:

- 9600 baud (9600 бод)
- 8 data bits (8 бит данных)
- No parity (Четность не проверяется)
- 1 stop bit (1 стоповый бит)
- No flow control (Управление потоком отключено)

Примечание: приведенные выше настройки являются настройками по умолчанию. Если после настройки терминала с использованием приведенных выше установок вы не можете подключиться к устройству, то это может означать, что устройство не использует настройки по умолчанию. Попробуйте изменить настройки, начав со скорости передачи данных. Более подробно о характеристиках консольного кабеля см. в разделе *Локальное подключение к точкам доступа серии 1200 and 1230AG* документа Первичная настройка точки доступа.

В данном документе описывается процедура настройки при помощи графического интерфейса пользователя.

Существует два способа подключения к точке доступа при помощи GUI:

- Перед подключением посредством GUI назначить устройству IP-адрес.
- Получить IP-адрес воспользовавшись протоколом динамического конфигурирования хоста (DHCP).

Различные модели точек доступа Aironet по-разному работают с IP-адресами. При подключении к LAN таких точек доступа, как Aironet 350, 1130AG, 1200 и 1240AG, имеющих настройки по умолчанию, точка доступа запрашивает IP-адрес на DHCP-сервере. Если точка доступа не получит IP-адрес, то она будет постоянно отправлять запросы на сервер.

При подключении к LAN точки доступа Aironet 1100, имеющей настройки по умолчанию, эта точка доступа предпринимает несколько попыток получить IP-адрес от DHCP-сервера. Если точка доступа не получит IP-адрес, тогда будет назначен IP-адрес 10.0.0.1, который будет действовать в течение 5 минут. В течение 5-минутного периода можно найти IP-адрес, используемый по умолчанию, и настроить статический адрес. Если точка доступа не будет настроена в течение 5 минут, тогда точка доступа отвергает адрес 10.0.0.1 и запрашивает адрес на DHCP-сервере. Если точка доступа не получит IP-адрес, то она будет постоянно отправлять запросы на сервер. Если вы не успеете за 5 минут определить адрес по умолчанию, тогда точку доступа можно выключить и снова повторить всю процедуру.

В этом документе для сети используется точка доступа Aironet 1200. При выполнении входа на точку доступа через консоль на точке доступа будет настроен адрес 10.0.0.1. О том, как назначить точке доступа IP-адрес, см. раздел *Получение и назначение IP-адресов* документа Первичная настройка точки доступа.

Пошаговые инструкции

После настройки IP-адреса к точке доступа можно подключиться через браузер, чтобы настроить ее на прием клиентских запросов на ассоциирование, поступающих от клиентского адаптера.

Выполните следующие действия:

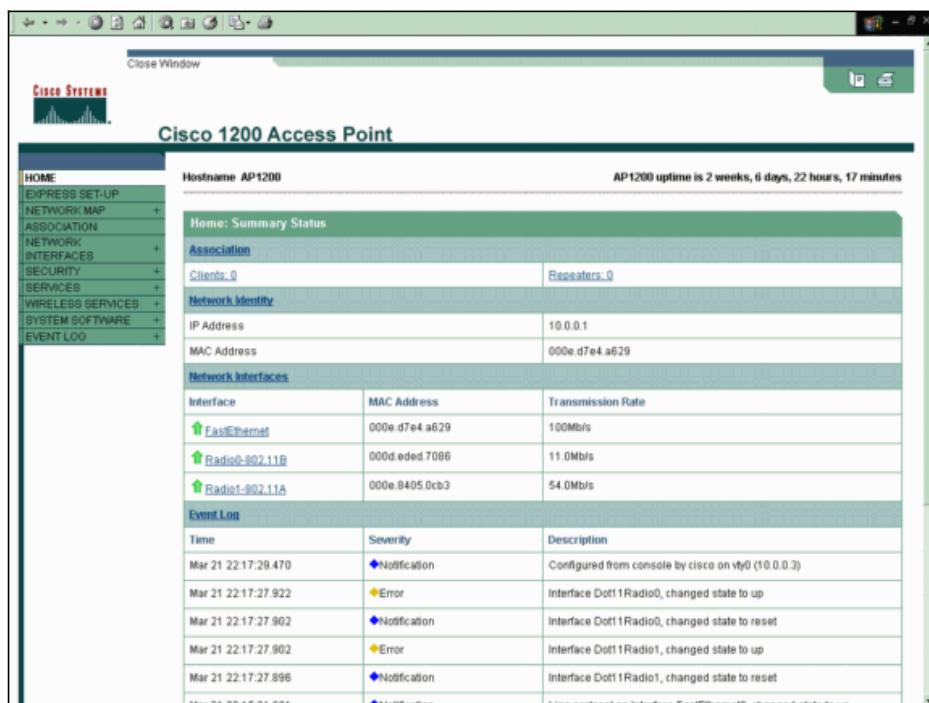
1. Чтобы посредством GUI получить доступ к точке доступа и чтобы вывести окно Summary Status, необходимо выполнить следующие действия:

1. Откройте веб-браузер и в адресной строке введите **10.0.0.1**.
2. Чтобы пропустить поле Username и перейти к полю Password нажмите клавишу **Tab**.

Появится окно "Enter Network Password".

3. Введите пароль **Cisco** с учетом регистра и затем нажмите **Enter**.

В окне "Summary Status" будет отображена следующая информация:



The screenshot shows the Cisco 1200 Access Point web interface. The main heading is "Cisco 1200 Access Point" and the hostname is "AP1200". The uptime is "2 weeks, 6 days, 22 hours, 17 minutes". The page is titled "Home: Summary Status".

Association

Clients: 0	Repeaters: 0
------------	--------------

Network Identity

IP Address	10.0.0.1
MAC Address	000e.d7e4.a629

Network Interfaces

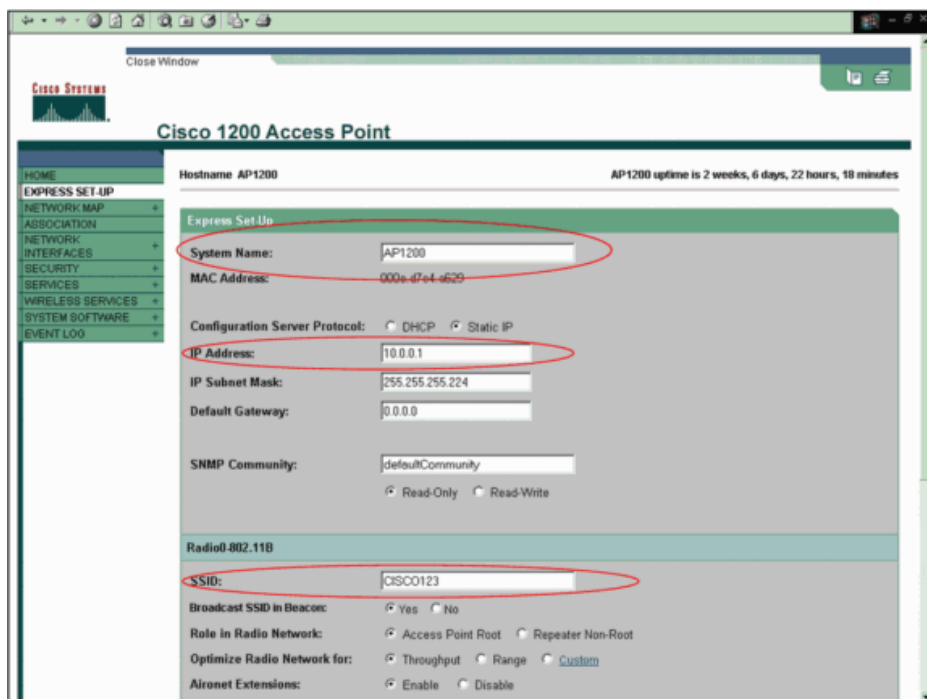
Interface	MAC Address	Transmission Rate
FastEthernet0	000e.d7e4.a629	100Mbps
Radio0-902.11B	000d.eded.7086	11.0Mbps
Radio1-902.11A	000e.8405.0cb3	54.0Mbps

Event Log

Time	Severity	Description
Mar 21 22:17:28.470	Notification	Configured from console by cisco on vty0 (10.0.0.3)
Mar 21 22:17:27.922	Error	Interface Dot11Radio0, changed state to up
Mar 21 22:17:27.902	Notification	Interface Dot11Radio0, changed state to reset
Mar 21 22:17:27.902	Error	Interface Dot11Radio1, changed state to up
Mar 21 22:17:27.896	Notification	Interface Dot11Radio1, changed state to reset
Mar 21 22:15:31.891	Notification	Line protocol on interface FastEthernet0, changed state to up

2. В меню слева щелкните опцию **Express Setup**.

Появится окно "Express Setup". Воспользуйтесь данным окном, чтобы настроить часть базовых параметров, которые необходимы для установления беспроводного подключения. Используйте окно "Express Setup" при работе с точкой доступа AP 1200 для того, чтобы настроить получение ассоциаций от беспроводных клиентов. Ниже представлен пример настройки:



3. В окне "Express Setup" в соответствующих полях укажите необходимые значения.

К настраиваемым параметрам относятся следующие:

- Имя точки доступа
- Настройка IP-адреса точки доступа (при использовании статического IP-адреса)
- Шлюз по умолчанию
- Строка сообщества протокола Simple Network Management Protocol (SNMP)
- Роль, выполняемая в беспроводной сети
- SSID

В нашем примере настраиваются следующие параметры:

- IP address: **10.0.0.1**
- Host name: **AP1200**
- SSID: **CISCO123**

Примечание: идентификаторы SSID являются уникальными идентификаторами сети WLAN. Беспроводные устройства используют идентификаторы SSID для установления и поддержания беспроводных соединений. Идентификаторы SSID различают регистр ввода и могут содержать до 32 буквенно-цифровых символов. Не используйте пробелы или специальные символы в SSID.

Примечание: все другие параметры сохраняют значения, заданные по умолчанию.

4. Чтобы сохранить изменения, нажмите **Apply**.

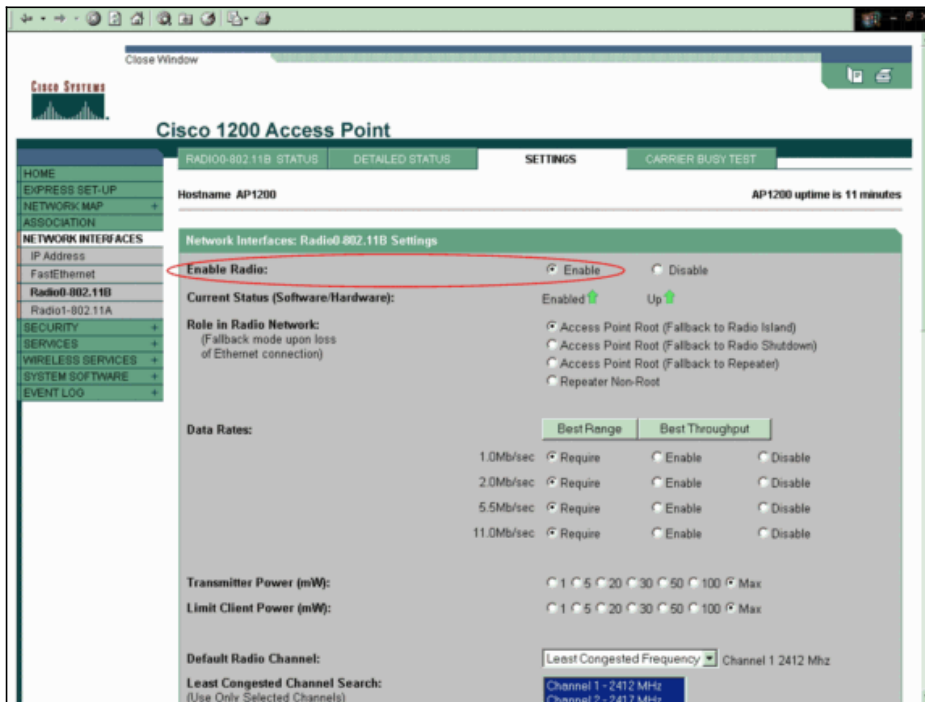
5. Для настройки параметров радиосвязи, необходимо выполнить следующие действия:

1. Чтобы перейти к странице "Network Interfaces Summary", в меню слева щелкните **Network Interfaces**.
2. Выберите необходимый радио-интерфейс.

В данном примере используется интерфейс Radio0-802.11B. После выбора интерфейса Radio0-802.11B станет доступной страница "Radio Status".

3. Чтобы перейти к странице "Settings" для настройки радио-интерфейса, щелкните вкладку **Settings**.
4. Чтобы включить радио-интерфейс, выберите **Enable**.

5. Все остальные настройки, имеющиеся на данной странице, сохраняют значения, заданные по умолчанию.
6. Чтобы сохранить внесенные изменения, в нижней части страницы нажмите **Apply**.



6. Для настройки идентификатора SSID и открытой аутентификации с шифрованием WEP выполните следующие действия:

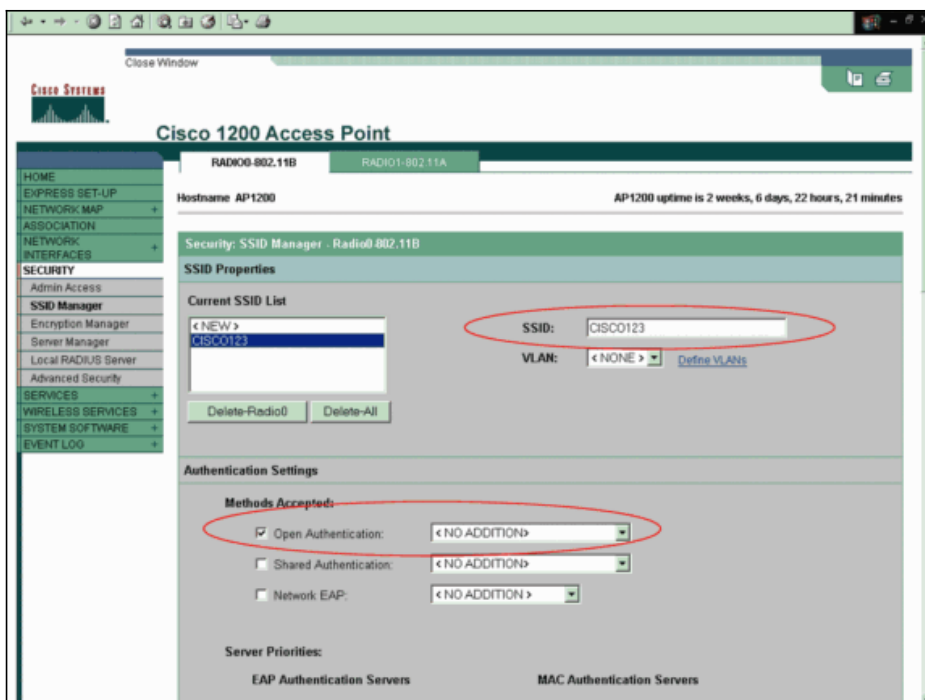
1. В меню слева последовательно выберите **Security > SSID Manager**.

Появится страница "SSID Manager".

2. В списке Current SSID выберите идентификатор SSID, который был создан при выполнении шага 3.

В этом примере в качестве идентификатора SSID используется идентификатор "CISCO123".

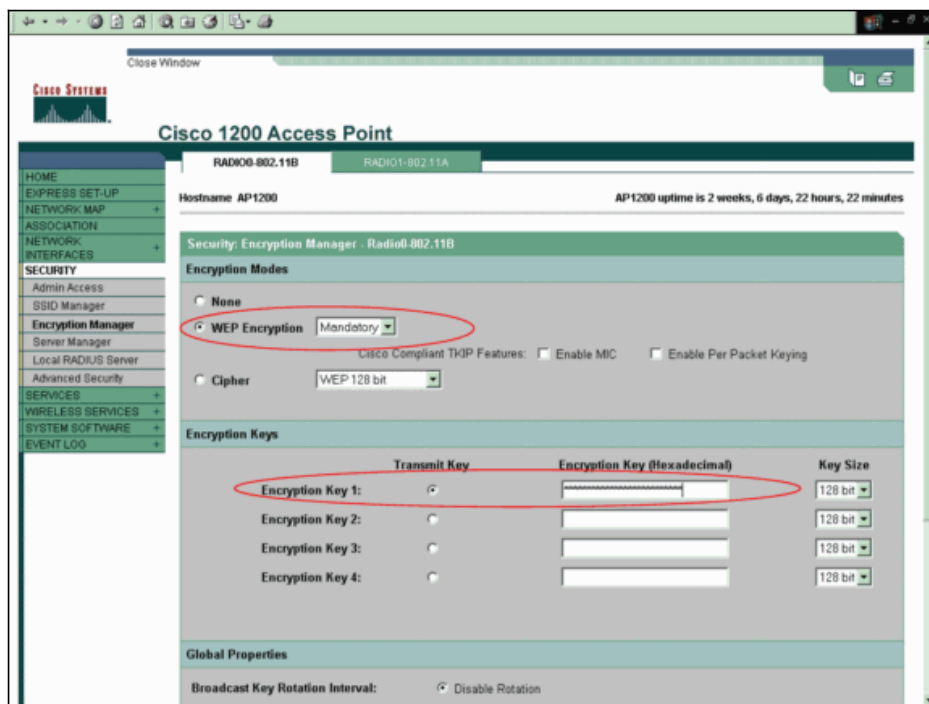
3. В разделе "Authentication Settings" ("Параметры аутентификации") выберите **Open Authentication** (Открытая аутентификация).
4. Для всех остальных параметров сохраняются значения, заданные по умолчанию.
5. Внизу страницы нажмите **Apply**.



7. Чтобы настроить ключи WEP, выполните следующие действия:

1. Выберите последовательно **Security > Encryption Manager**.
2. В разделе "Encryption Modes" ("Режимы шифрования") щелкните **WEP Encryption** (шифрование WEP) и в раскрывающемся списке выберите **Mandatory** ("Обязательное").
3. В области "Encryption Keys" ("Ключи шифрования") введите ключ для WEP-шифрования.

Ключи шифрования WEP могут иметь 40- или 128-битную длину. В нашем примере используется 128-битный ключ WEP-шифрования – **1234567890abcdef1234567890**.



4. Чтобы сохранить изменения, нажмите **Apply**.

Настройка адаптера беспроводного клиента

Прежде чем приступить к настройке адаптера беспроводного клиента, на ПК или портативном компьютере необходимо установить собственно адаптер и его программные компоненты. Указания по установке драйверов и утилит клиентского адаптера см. в документе "Установка клиентского адаптера".

Пошаговые инструкции

По завершении установки клиентского адаптера можно приступить к его настройке. В этом разделе описывается процедура настройки клиентского адаптера.

Выполните следующие действия:

1. В Aironet Desktop Utility (ADU) создайте профиль клиентского адаптера.

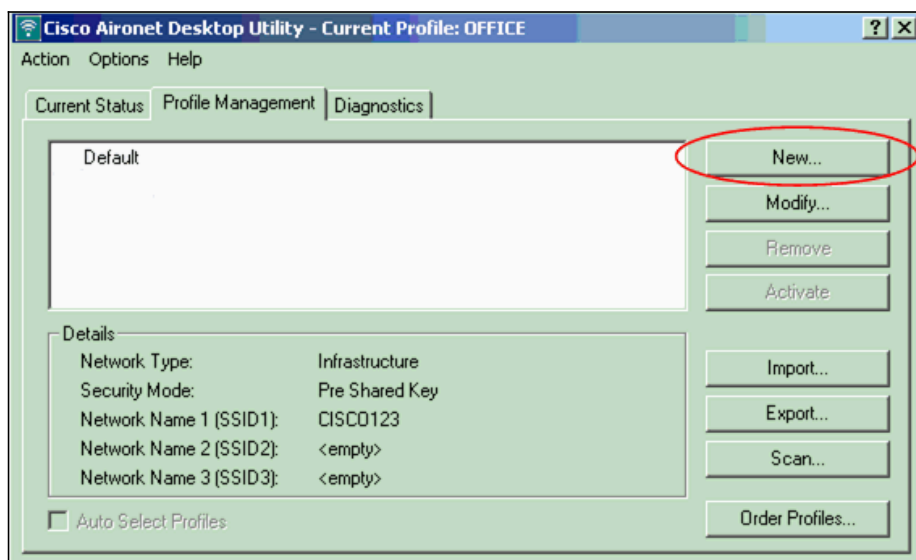
В профиле задаются параметры, которые будут использоваться клиентским адаптером для подключения к беспроводной сети. ADU позволяет настроить до 16 различных профилей. В зависимости от имеющихся требований можно включать тот или иной профиль. Профили позволяют использовать клиентский адаптер в различных местах, для чего требуются различные настройки. Например, можно настроить профили для использования клиентского адаптера в офисе, дома и в общественных местах (аэропорты и зоны WI-FI).

Чтобы создать новый профиль, выполните следующие действия:

1. В ADU щелкните вкладку **Profile Management** ("Управление профилями").

2. Щелкните **New**.

Ниже приведен пример:



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:

1. В поле "Profile Name" введите имя профиля.

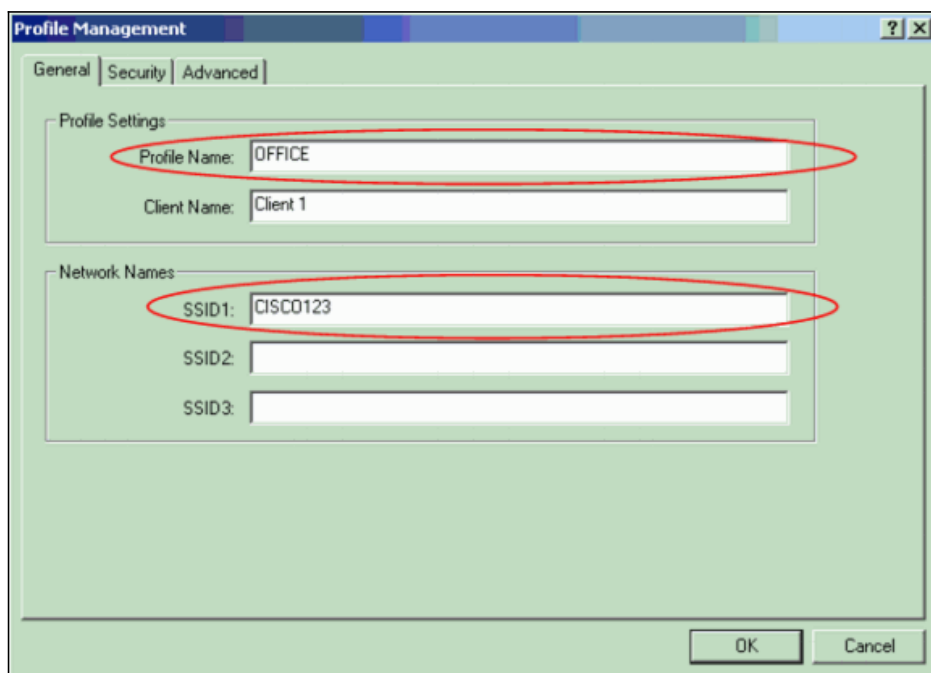
В данном примере в качестве имени профиля используется используется имя **OFFICE**.

2. В поле "Client Name" введите имя клиента.

Имя клиента используется для идентификации беспроводного клиента в сети WLAN. В данном случае для первого клиента используется имя **Client 1**.

3. В области "Network Names" укажите идентификатор SSID, который будет использоваться в этом профиле.

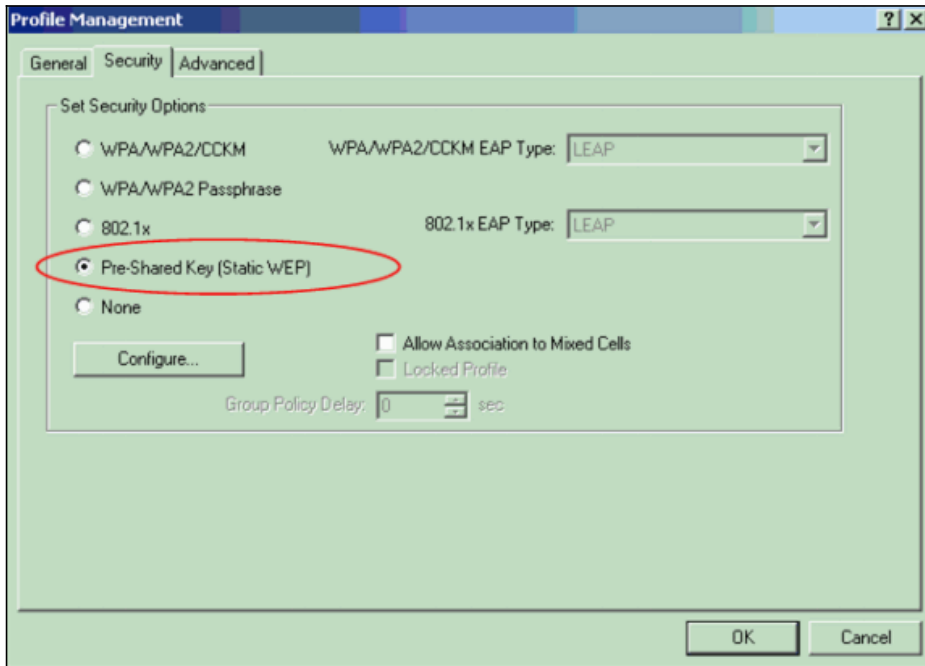
Здесь указывается тот же идентификатор SSID, что был настроен для точки доступа. В данном примере используется идентификатор SSID **CISCO123**.



3. Для настройки параметров безопасности необходимо выполнить следующие действия:

1. В верхней части окна щелкните вкладку **Security** ("Безопасность").
2. В области "Set Security Options" щелкните **Pre-Shared Key (Static WEP)**.

Ниже приведен пример:

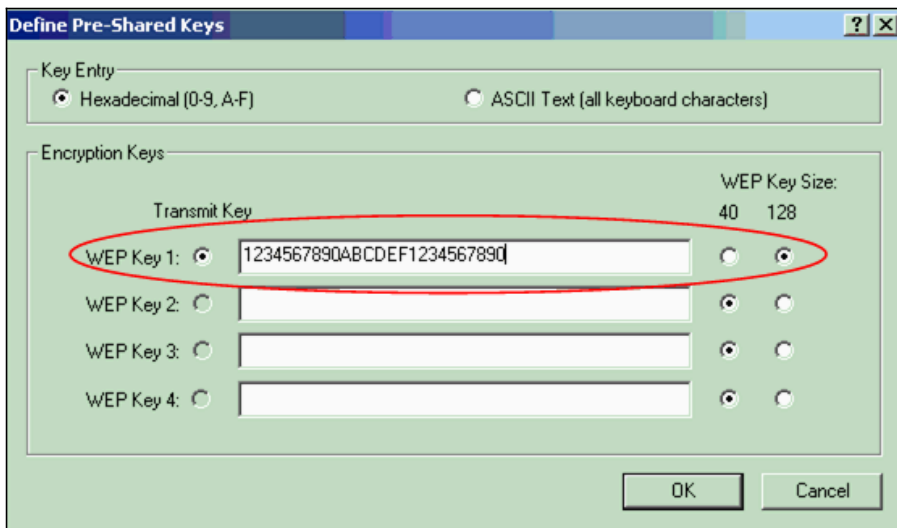


3. Нажмите **Configure**.

Появится окно "Define Pre-Shared Keys" ("Предварительные совместно используемые ключи").

4. В области "Key Entry" ("Числовое представление ключа") выберите тип числового представления.

В данном примере используется **шестнадцатиричное представление ключа (0-9, A-F)**.



5. В области "Encryption Keys" введите ключ WEP, который будет использоваться для шифрования пакетов с данными.

В данном примере используется ключ WEP – **1234567890abcdef1234567890**. См. пример в пункте d.

Примечание: используйте тот же самый ключ WEP, который был настроен для точки доступа.

4. Чтобы сохранить ключ WEP, нажмите **ОК**.

5. Для установки открытого метода аутентификации выполните следующие действия:

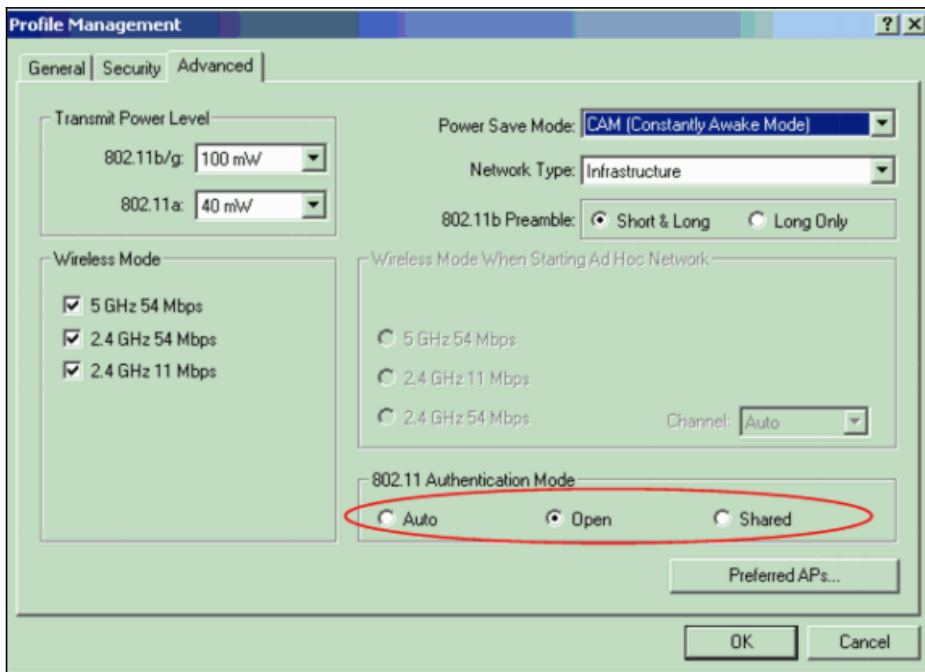
1. В верхней части окна "Profile Management" щелкните вкладку **Advanced**.

2. Убедитесь, что в области "802.11 Authentication Mode" выбрана опция **Open**.

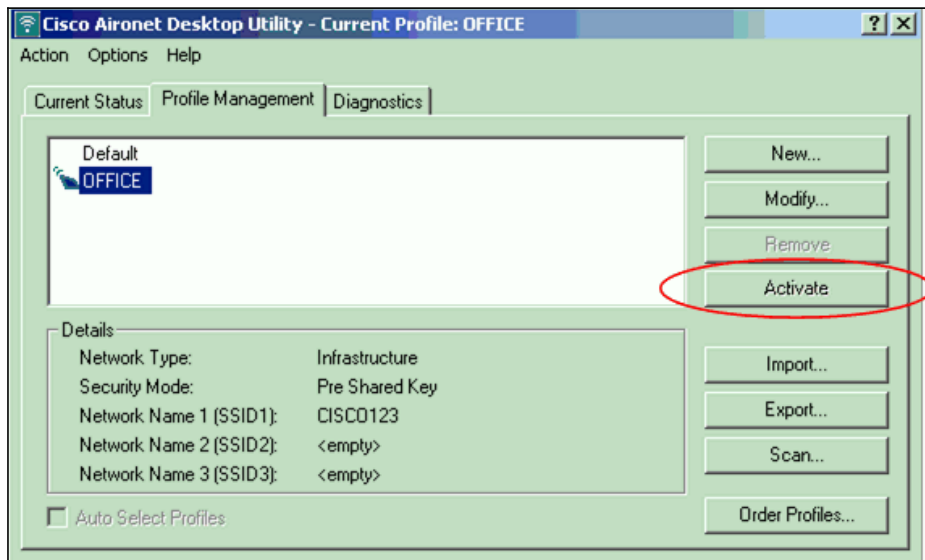
Примечание: обычно открытая аутентификация выбрана по умолчанию.

3. Для всех остальных параметров сохраняются значения, заданные по умолчанию.

4. Нажмите **ОК**.



6. Чтобы сделать активным данный профиль, нажмите **Activate**.



Примечание: для создания нового профиля можно воспользоваться теми же самыми Пошаговыми инструкциями. Для создания профиля можно использовать и другой метод, в котором клиентский адаптер выполняет сканирование радио-окружения и определяет имеющиеся сети, а затем по результатам сканирования создается профиль. Более подробно об этом методе см. в разделе "Создание нового профиля" документа "Использование Менеджера профилей".

Для настройки двух других клиентских адаптеров можно использовать ту же самую процедуру настройки. Для других адаптеров можно использовать тот же самый идентификатор SSID. В этом случае различаться будут только имена клиентов и IP-адреса, которые статически назначаются каждому из адаптеров.

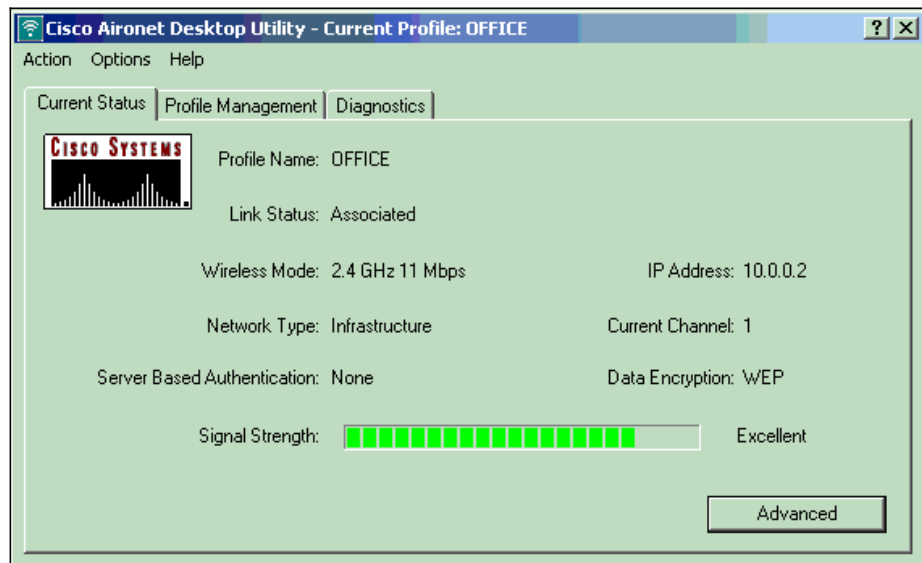
Примечание: в нашем примере предполагается, что IP-адрес клиентского адаптера настраивается вручную и что этот адрес находится в той же подсети, что и точка доступа.

Проверка

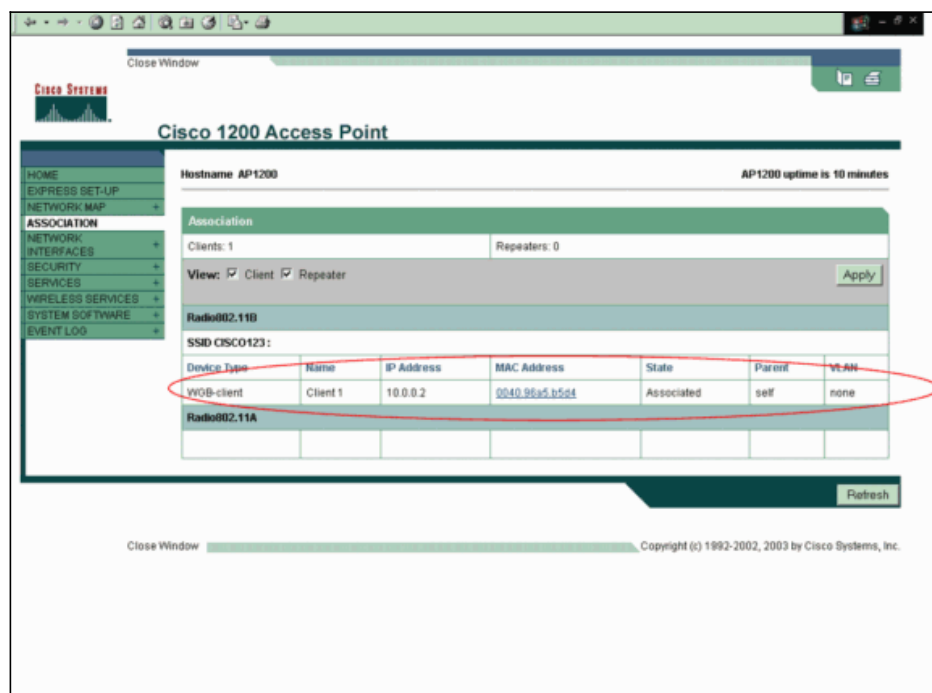
Воспользуйтесь данным разделом, чтобы проверить правильность функционирования вашей конфигурации.

После того как были произведены настройки и активирован профиль, клиентский адаптер подключается к точке доступа. Чтобы проверить статус клиентского соединения, в верхней части окна ADU щелкните вкладку **Current Status** ("Текущий статус").

В данном примере показано, что клиент успешно подключился к точке доступа. Так же можно видеть, что для связи с точкой доступа клиент использует канал 1 и шифрование WEP. При этом в поле "Server Based Authentication" ("Серверная аутентификация") указано "None", поскольку используется открытая аутентификация:



Для проверки подключения к точке доступа можно использовать другой метод. На домашней странице точки доступа в меню, расположенном слева, нажмите **Association**. Ниже приведен пример:



Устранение неполадок

Если используется аутентификация 802.1x и если в сети присутствуют коммутатор Cisco Catalyst 2950 или 3750 Switch, то тогда клиент 802.1X может не выполнить аутентификацию. В этом случае будет выводиться следующее сообщение об ошибке:

```
Jul 21 14:14:52.782 EDT: %RADIUS-3-ALLDEADSERVER: Group rad_eap: No active radius servers found. Id 254
```

Такая ошибка возникает на коммутаторах Catalyst 2950 и 3750 в том случае, если значения, указанные в поле RADIUS State(24), меняются между "Access Challenge" и "Access Request". Это связано с ошибкой Cisco с идентификатором CSCef50742. Данная неполадка устранена в Cisco IOS версии 12.3(4)JA При использовании версии 12.3(4)JA клиенты успешно выполняют аутентификацию 802.1X через коммутаторы Cisco Catalyst 2950 и 3750 (т.е. сбой, возникающий из-за изменения значений в поле "State (24)", был устранен).

Дополнительные сведения

- **Руководство по настройке ПО Cisco IOS версии 12.3(7)JA для точек доступа Cisco Aironet**
- **Руководство по установке и настройке клиентских WLAN-адаптеров Cisco Aironet 802.11a/b/g (CB21AG и PI21AG) (OL-4211-04)**
- **Первичная настройка точки доступа**
- **Страница поддержки беспроводных сетей LAN**
- **Техническая поддержка и документация – Cisco Systems**

© 1992-2010 Cisco Systems, Inc. Все права защищены.

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92125/wlan_connect.shtml
