Пример конфигурации базового беспроводного подключения LAN

Содержание

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

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

- Знакомство с технологией радиочастот (RF) базового беспроводного подключения
- Основное понимание того, как обратиться к AP Cisco

Этот документ предполагает, что уже установлены драйверы клиентских беспроводных карт для PC или портативных ПК.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

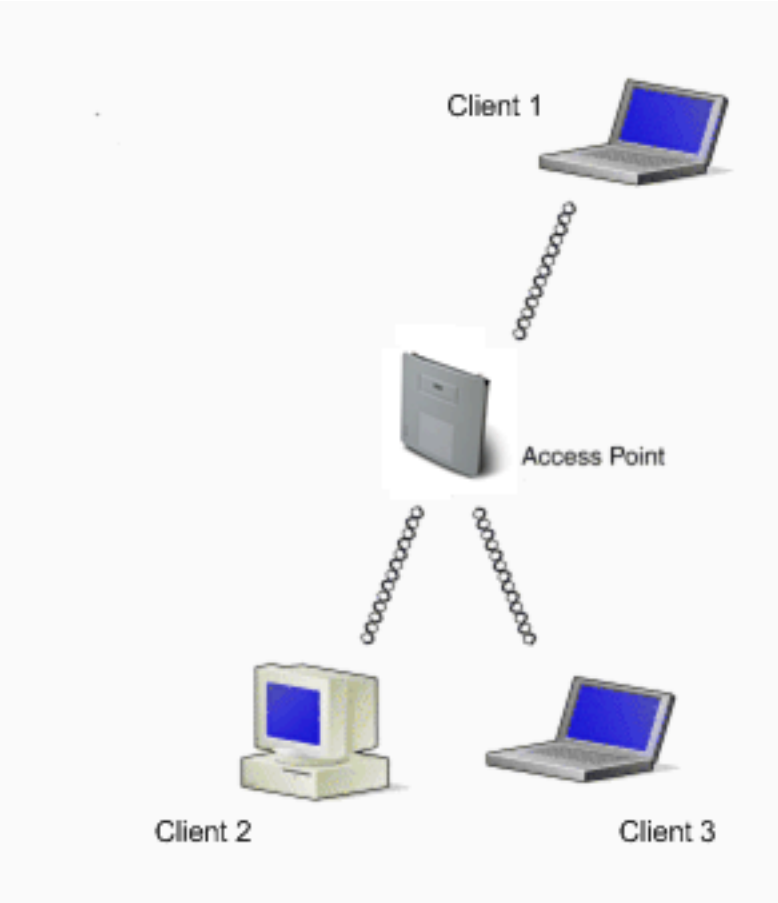
- AP одного Aironet серии 1200, который выполняет релиз 12.3 программного обеспечения Cisco IOS (7) JA
- Три Aironet 802.11a/b/g Клиентские адаптеры, которые выполняют микропрограммное обеспечение 2.5
- Набор программ Aironet Desktop Utility версии 2.5

Примечание: Этот документ использует AP, который имеет интегрированную антенну. 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.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в условиях реальной сети оператор должен понимать последствия использования любой команды или изменений, внесенных в графическом интерфейсе пользователя.

Схема сети

В настоящем 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 Протокола WEP

Этот документ объясняет конфигурацию на AP и клиентских адаптерах.

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

Условные обозначения

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

!--- конфигурацию

Настройка точки доступа Cisco

Можно настроить AP с использованием любого из них:

- GUI
- Интерфейс командной строки (CLI) после установления сеанса Telnet
- Консольный порт

Примечание: Для соединения с AP через консольный порт подключите девятиконтактный, сквозной кабель последовательного порта DB-9 с последовательным портом RS-232 на AP и к COM - порту на компьютере. Для установления соединения с точкой доступа необходимо настроить эмулятор терминала. Для настройки соединения через эмулятор терминала необходимо использовать следующие настройки:

- 9600 бод
- 8 информационных битов
- Без контроля четности
- 1 стоповый бит
- No flow control

Примечание: Эти параметры 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 разделеЛокальное 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 процедур.

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 конфигурации IP-адреса можно обратиться к AP через браузер для настройки AP для принятия запросов связывания клиента от клиентского адаптера.

Выполните следующие действия:

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

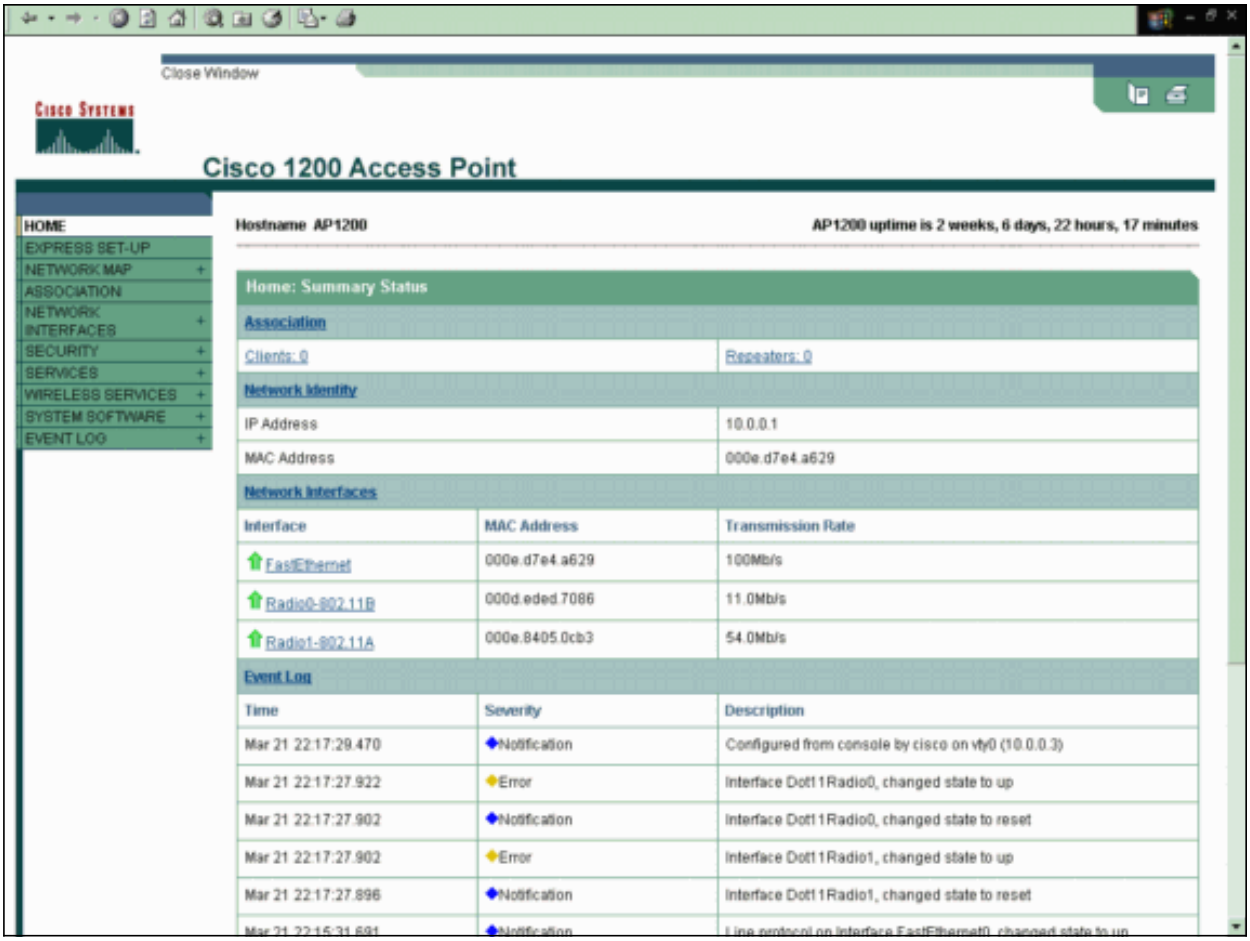
Откройте веб-браузер и в адресной строке введите 10.0.0.1.

Чтобы пропустить поле Username и перейти к полю Password нажмите клавишу Tab.

Появится окно "Enter Network Password".

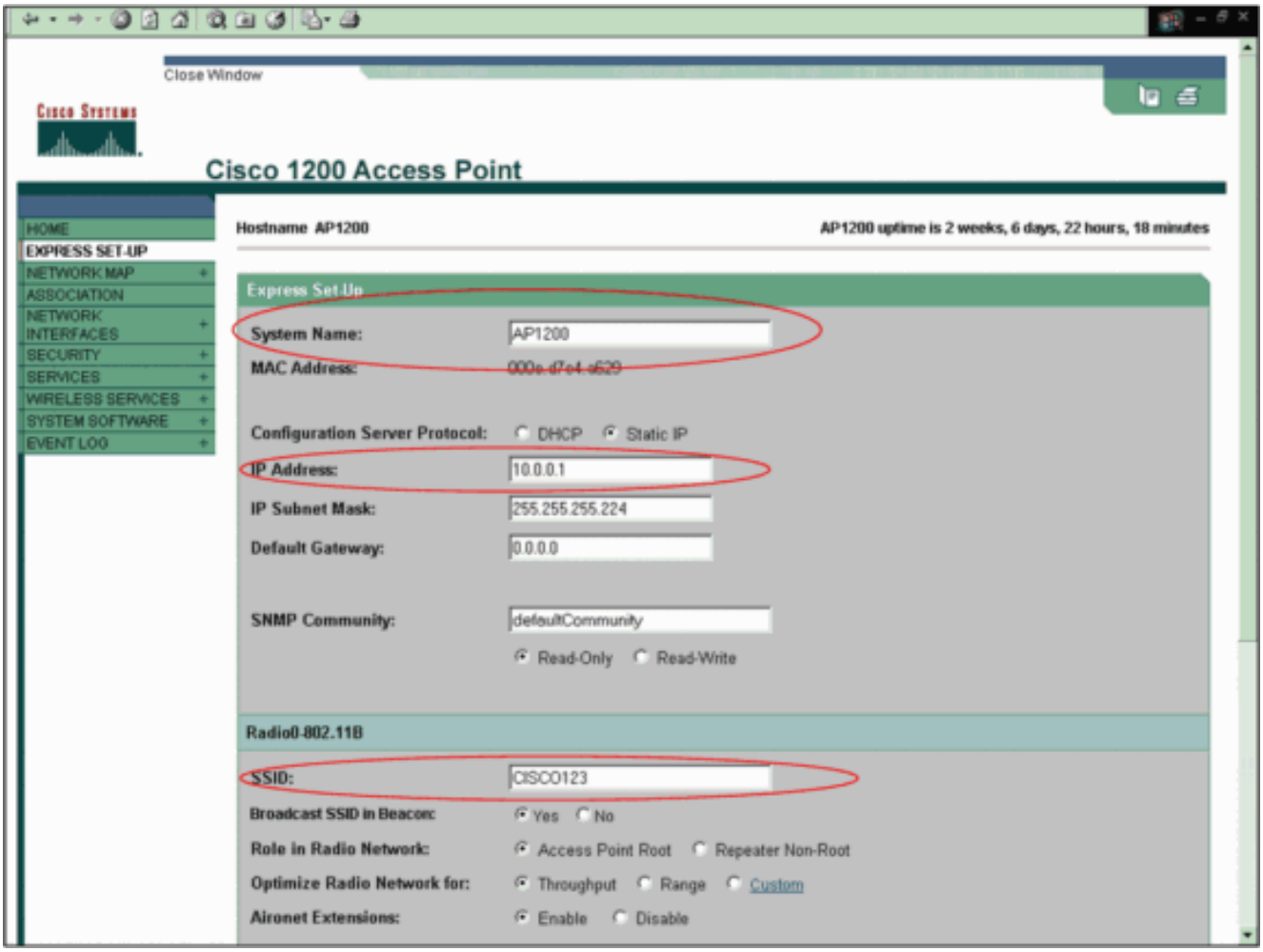
Введите пароль Cisco (чувствительный к регистру) и нажмите клавишу Enter.

В окне "Summary Status" будет отображена следующая информация:



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:



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

К настраиваемым параметрам относятся следующие:

Имя хоста AP

Настройка IP-адреса AP, если адрес является статическим ip

Шлюз по умолчанию

Строка имени и пароля Протокола SNMP

Роль в радиосети

SSID

Данный пример настраивает эти параметры:

IP-адрес: **10.0.0.1**

Host name: **AP1200**

SSID: **CISCO123**

Примечание: SSIDs являются уникальными идентификаторами, которые определяют сеть 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: Другие параметры оставляют со значениями по умолчанию.

Чтобы сохранить изменения, нажмите Apply.

Для настройки параметров радиосвязи, необходимо выполнить следующие действия:

Чтобы перейти к странице "Network Interfaces Summary", в меню слева щелкните Network Interfaces.

Выберите необходимый радио-интерфейс.

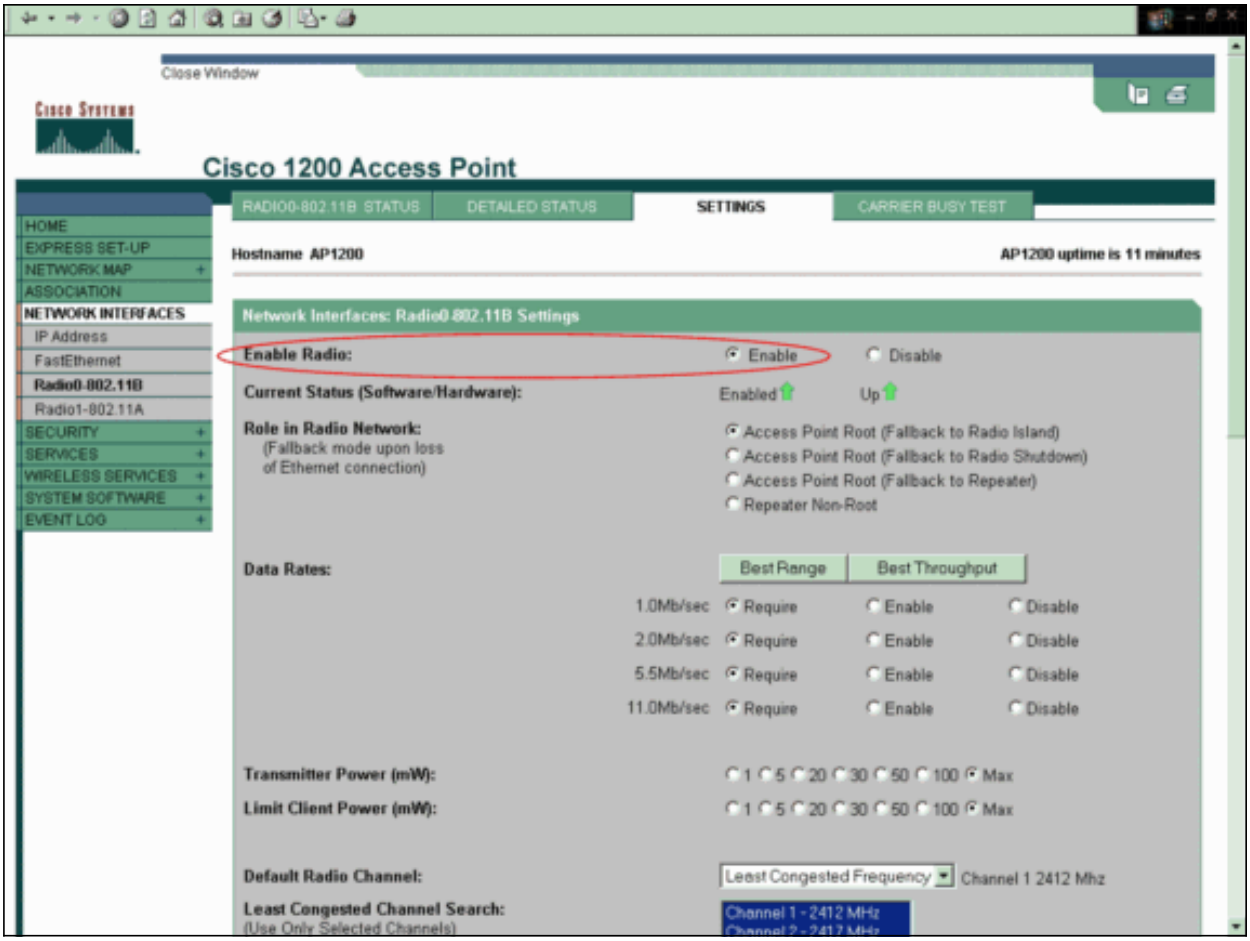
В данном примере используется интерфейс Radio0-802.11B. После выбора интерфейса Radio0-802.11B станет доступной страница "Radio Status".

Чтобы перейти к странице "Settings" для настройки радио-интерфейса, щелкните вкладку Settings.

Чтобы включить радио-интерфейс, выберите Enable.

Все остальные настройки, имеющиеся на данной странице, сохраняют значения, заданные по умолчанию.

Чтобы сохранить внесенные изменения, в нижней части страницы нажмите Apply.



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

Выберите **Security> SSID Manager** в меню слева.

Появится страница "SSID Manager".

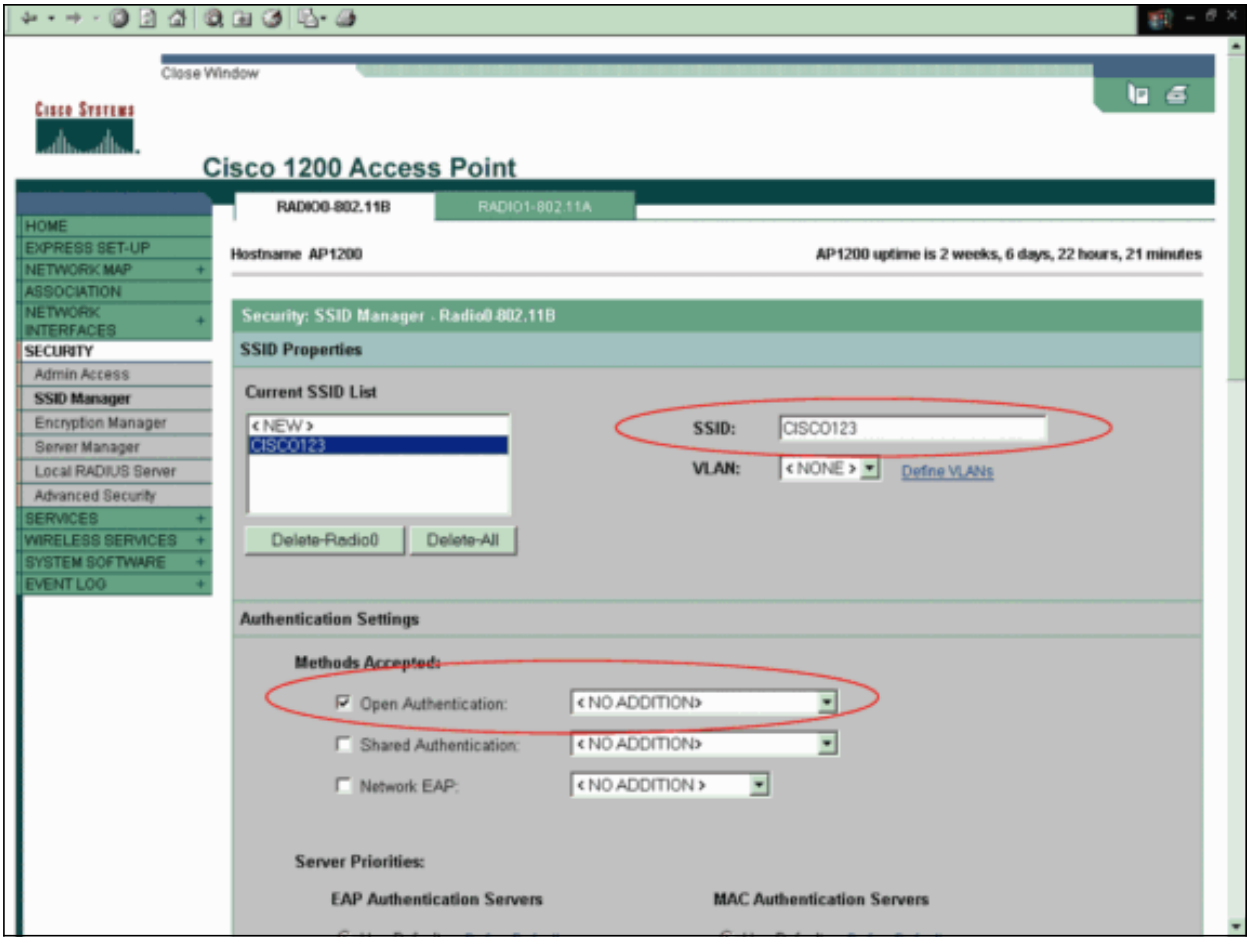
В списке Current SSID выберите идентификатор SSID, который был создан при выполнении шага 3.

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

В разделе "Authentication Settings" ("Параметры аутентификации") выберите Open Authentication (Открытая аутентификация).

Для всех остальных параметров сохраняются значения, заданные по умолчанию.

Внизу страницы нажмите Apply.



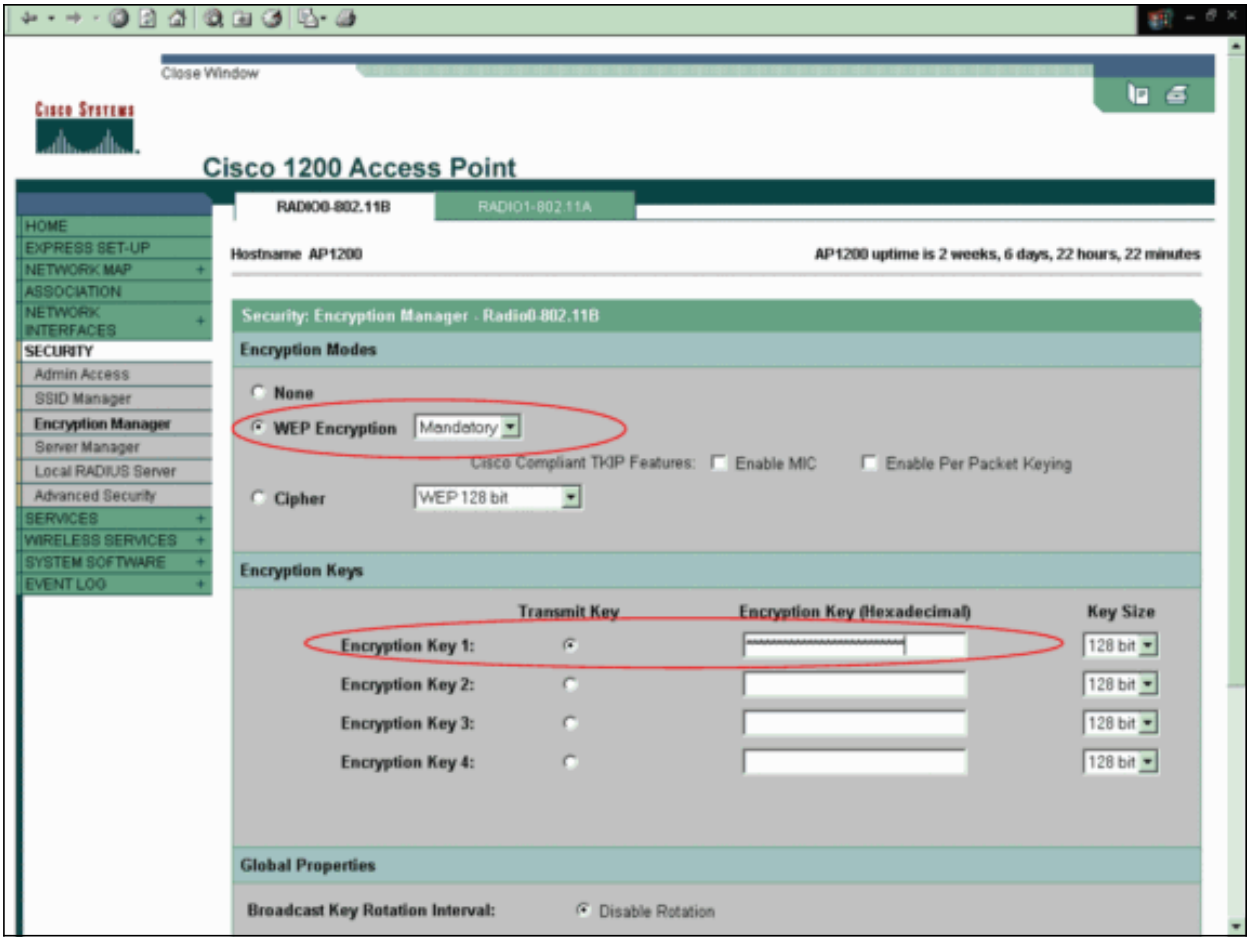
Чтобы настроить ключи WEP, выполните следующие действия:

Выберите Security > Encryption Manager.

В разделе "Encryption Modes" ("Режимы шифрования") щелкните WEP Encryption (шифрование WEP) и в раскрывающемся списке выберите Mandatory ("Обязательное").

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.**



Чтобы сохранить изменения, нажмите Apply.

Настройка адаптера беспроводного клиента

Перед конфигурацией клиентского адаптера необходимо установить клиентский адаптер и программные компоненты клиентского адаптера на ПК или портативном ПК. Указания по установке драйверов и утилит клиентского адаптера см. в документе "Установка клиентского адаптера".

Пошаговые инструкции

После установки клиентского адаптера на машине можно настроить его. В этом разделе описывается процедура настройки клиентского адаптера.

Выполните следующие действия:

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

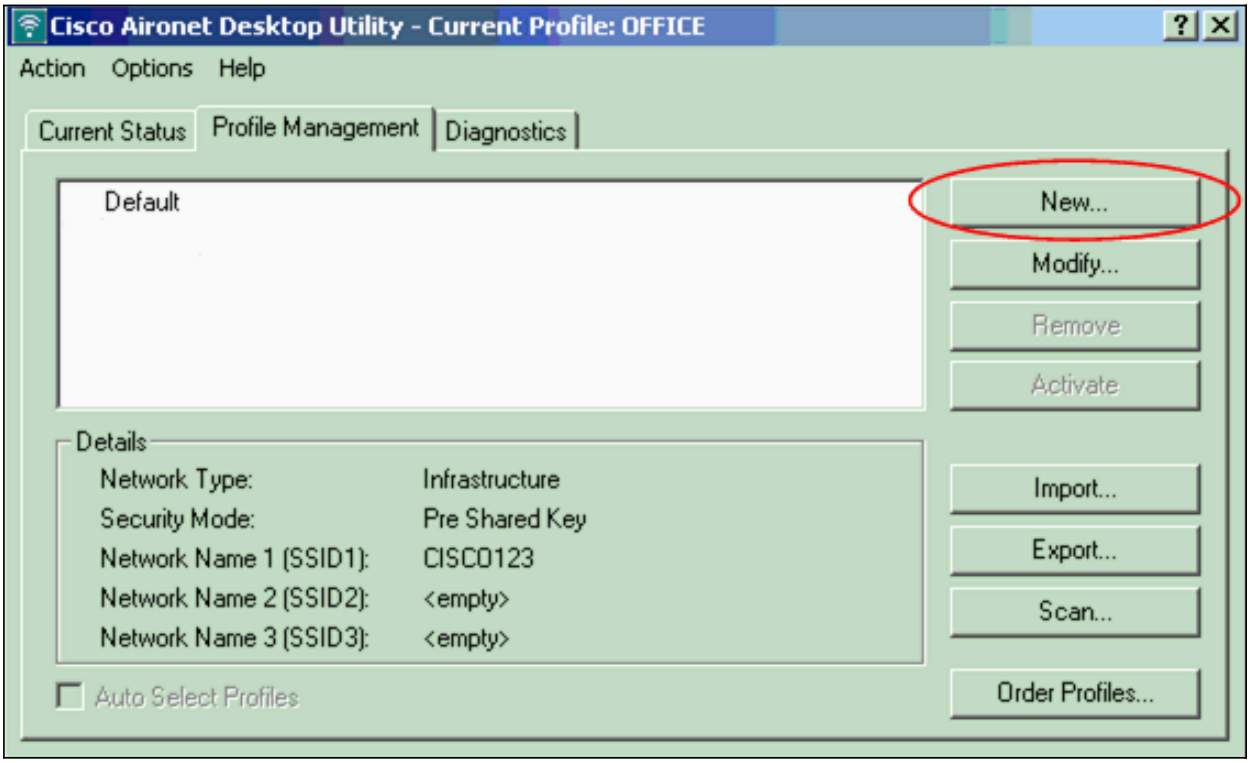
В профиле задаются параметры, которые будут использоваться клиентским адаптером для подключения к беспроводной сети. ADU позволяет настроить до 16 различных профилей. В зависимости от имеющихся требований можно включать тот или иной профиль. Профили позволяют использовать клиентский адаптер в различных 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:

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

Щелкните New.

Например:



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.

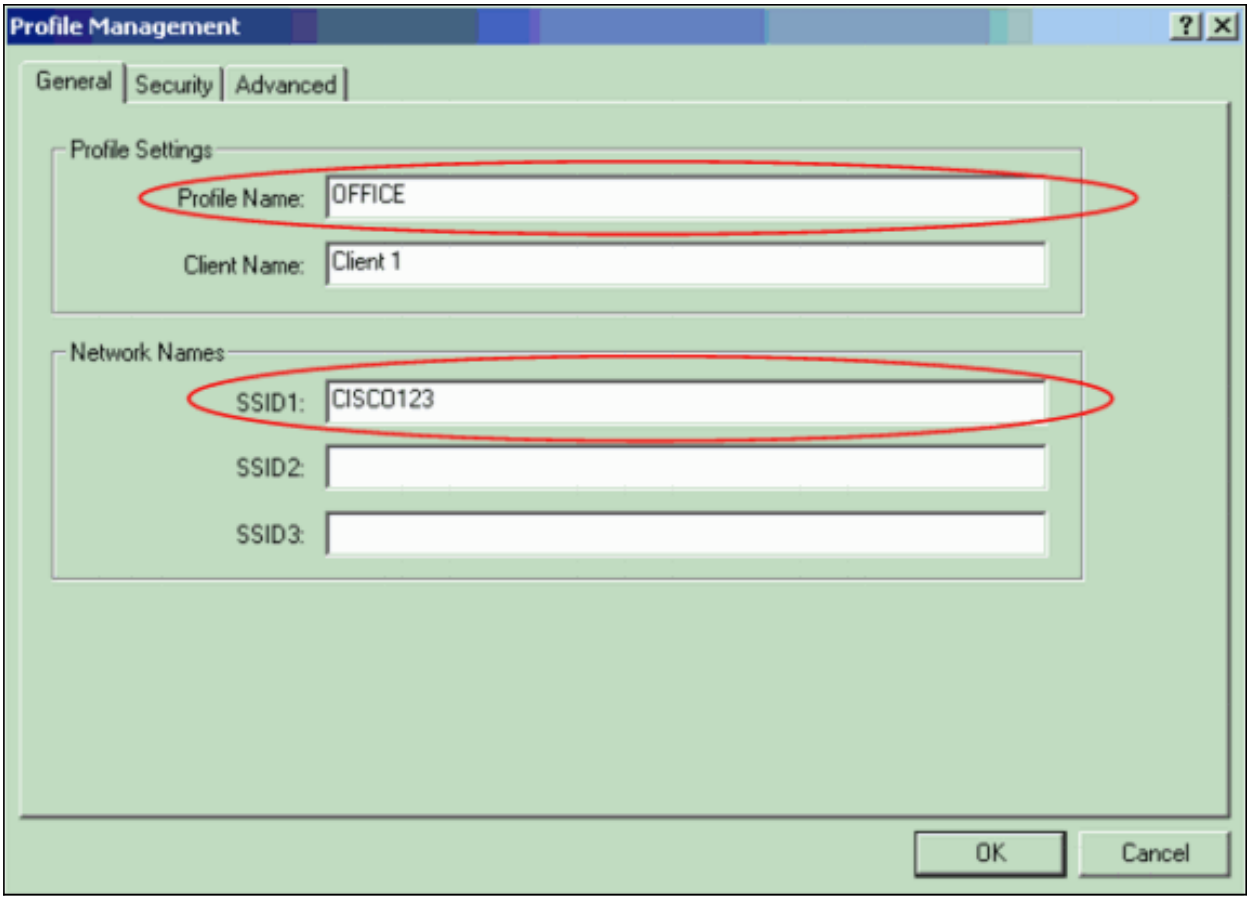
В данном примере в качестве имени профиля используется используется имя OFFICE.

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 .**

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.**

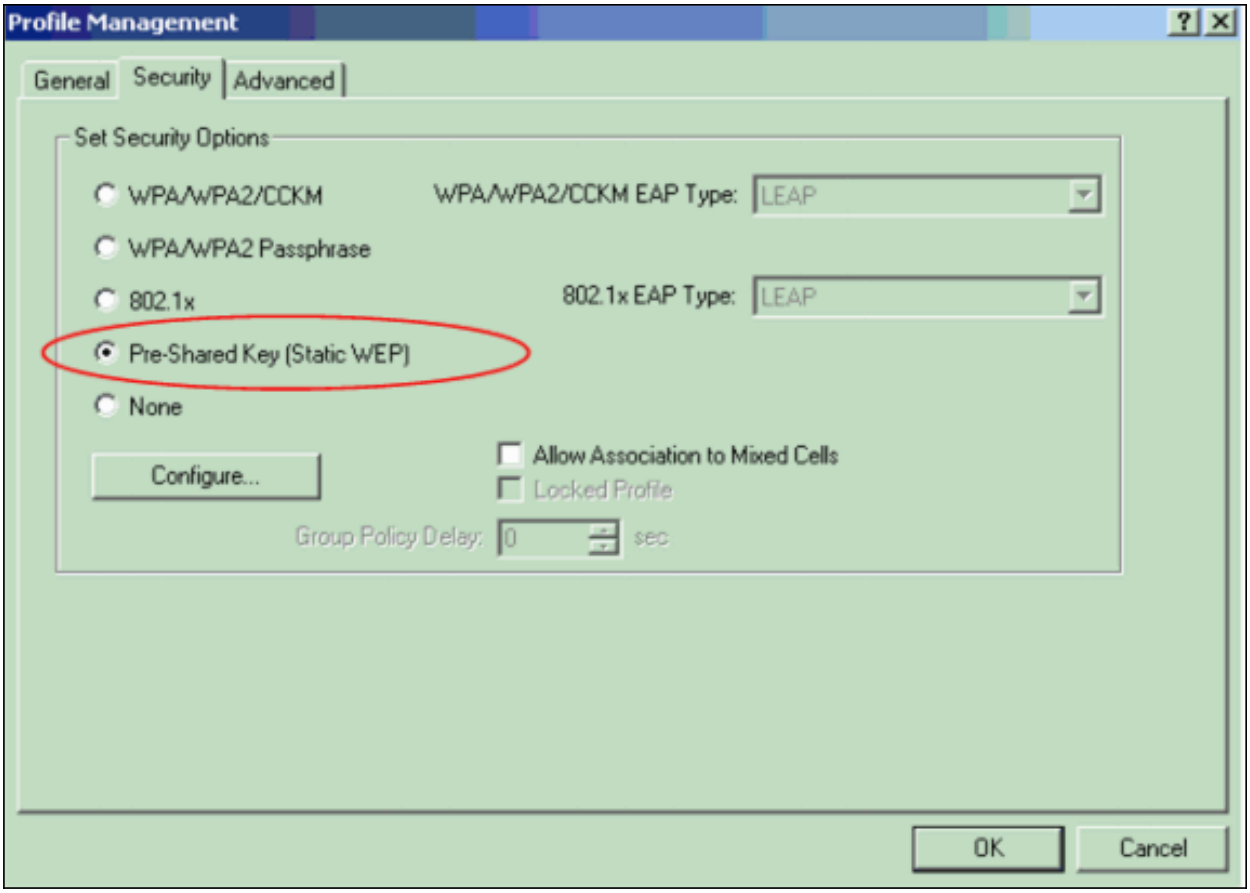


Для настройки параметров безопасности необходимо выполнить следующие действия:

В верхней части окна щелкните вкладку Security ("Безопасность").

В области "Set Security Options" щелкните Pre-Shared Key (Static WEP).

Например:

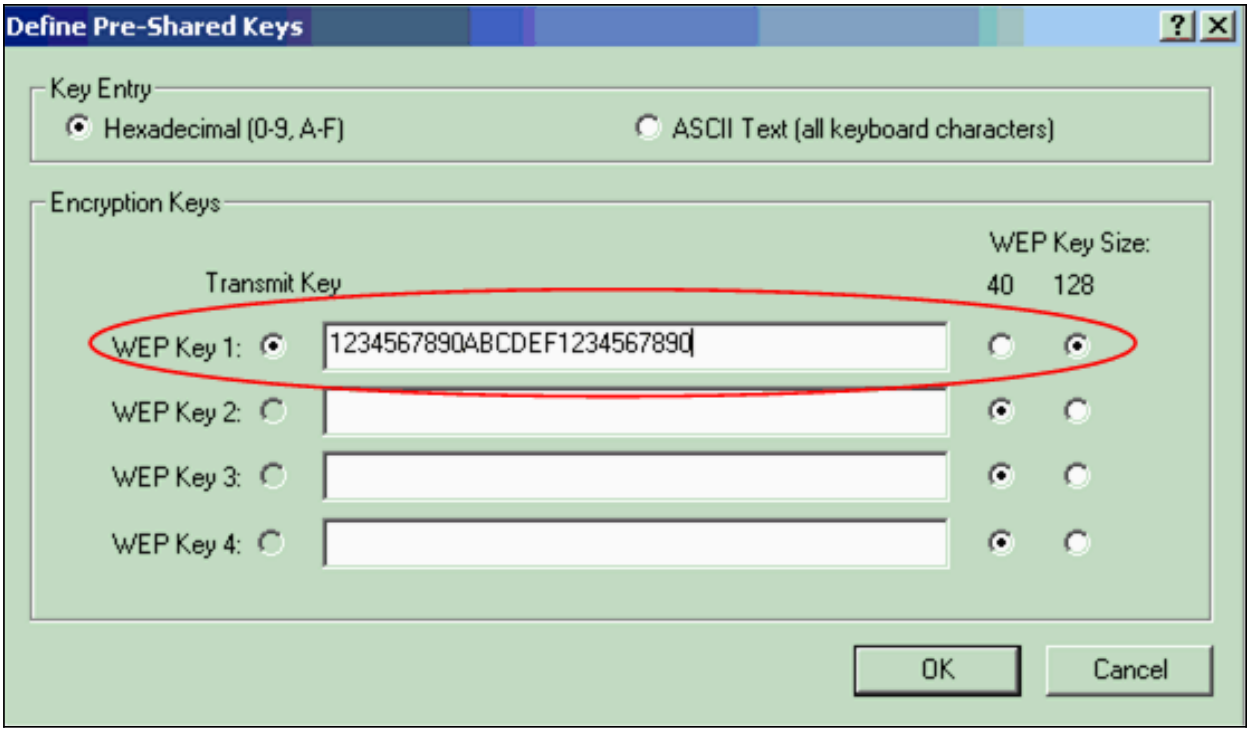


Нажмите кнопку Configure (Настроить).

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

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

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



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 Ключ WEP в качестве того, который вы настроили в AP.

Чтобы сохранить ключ WEP, нажмите OK.

Для установки открытого метода аутентификации выполните следующие действия:

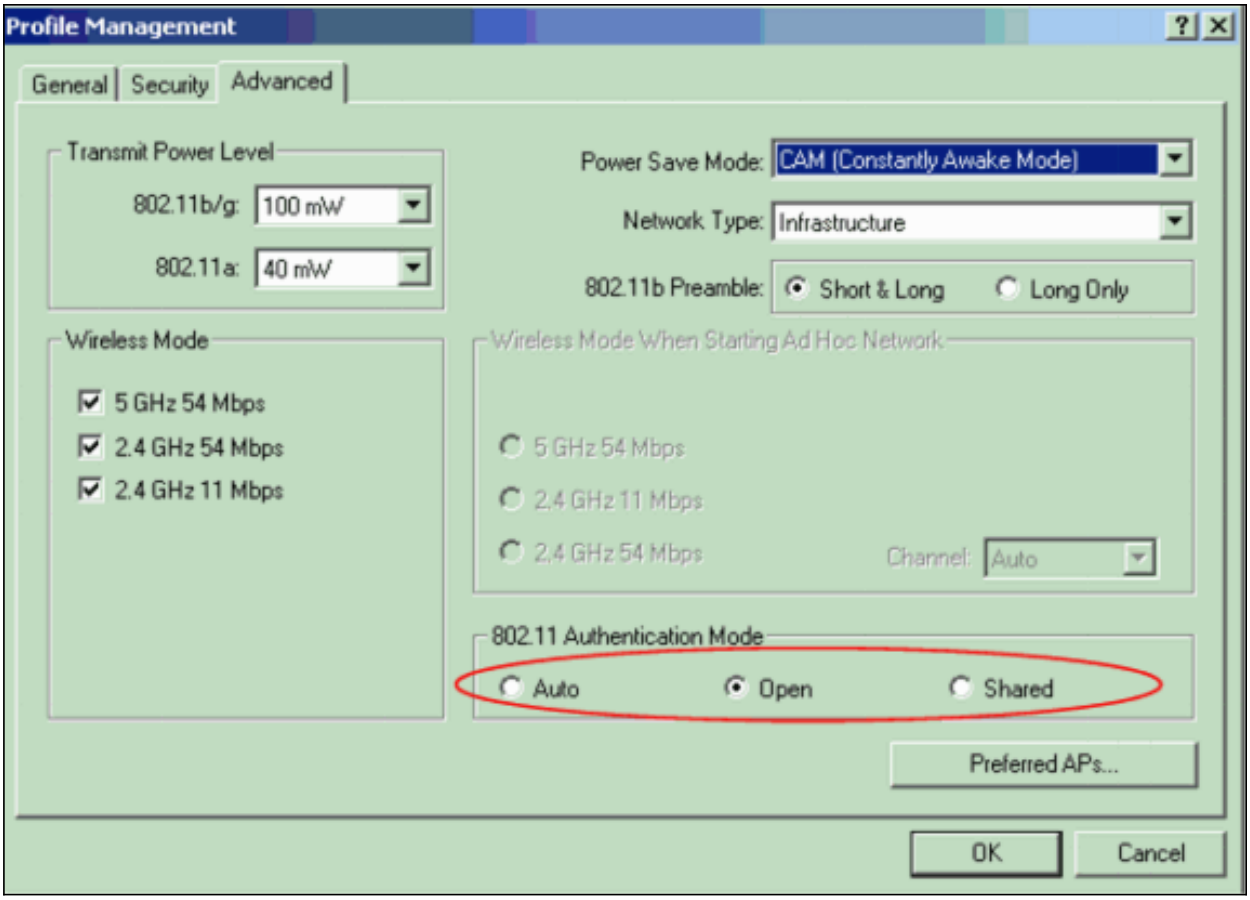
В верхней части окна "Profile Management" щелкните вкладку Advanced.

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

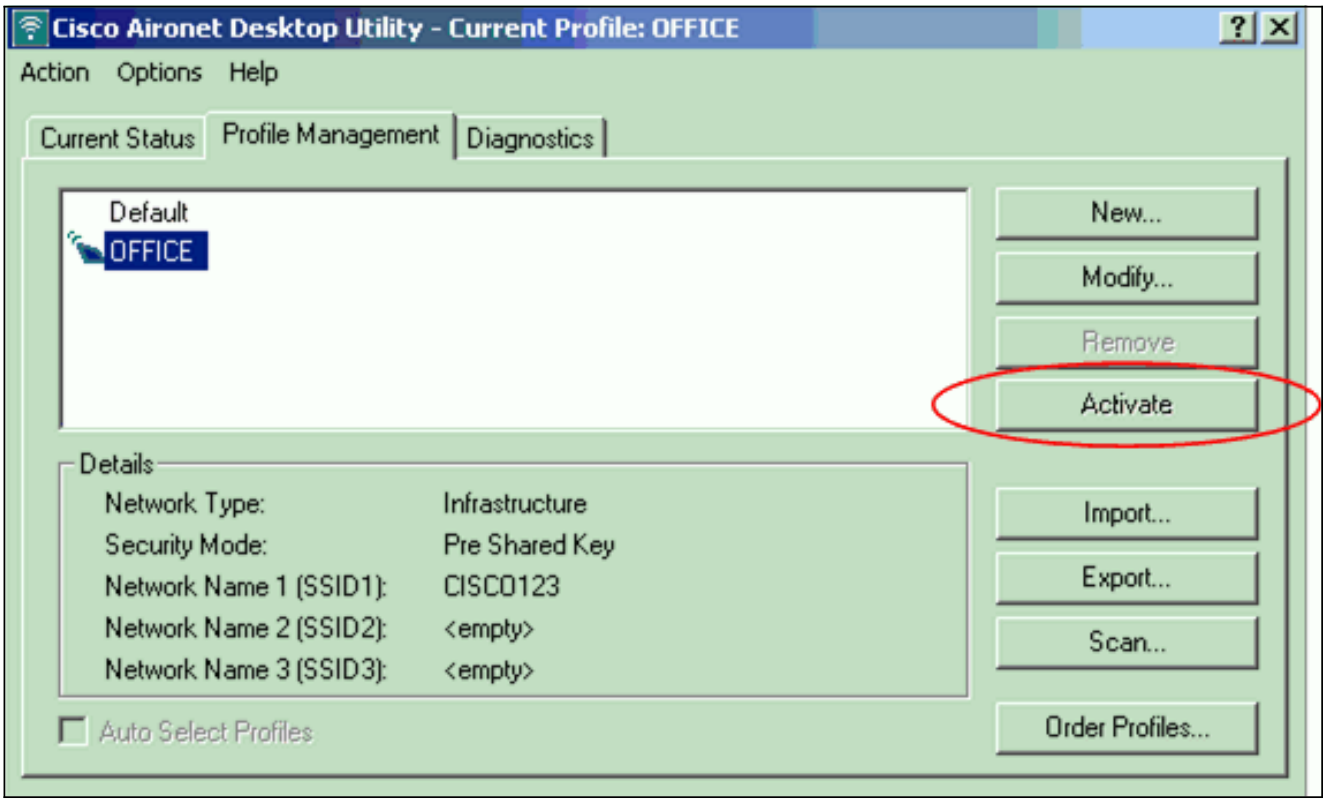
Примечание: Открытая аутентификация обычно включается по умолчанию.

Для всех остальных параметров сохраняются значения, заданные по умолчанию.

Нажмите кнопку OK.



Чтобы сделать активным данный профиль, нажмите Activate.



Примечание: Можно использовать эти те же Пошаговые инструкции для создания абсолютно нового профиля. 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 индентификатор SSID. В этом случае различаться будут только имена клиентов и IP-адреса, которые статически назначаются каждому из адаптеров.

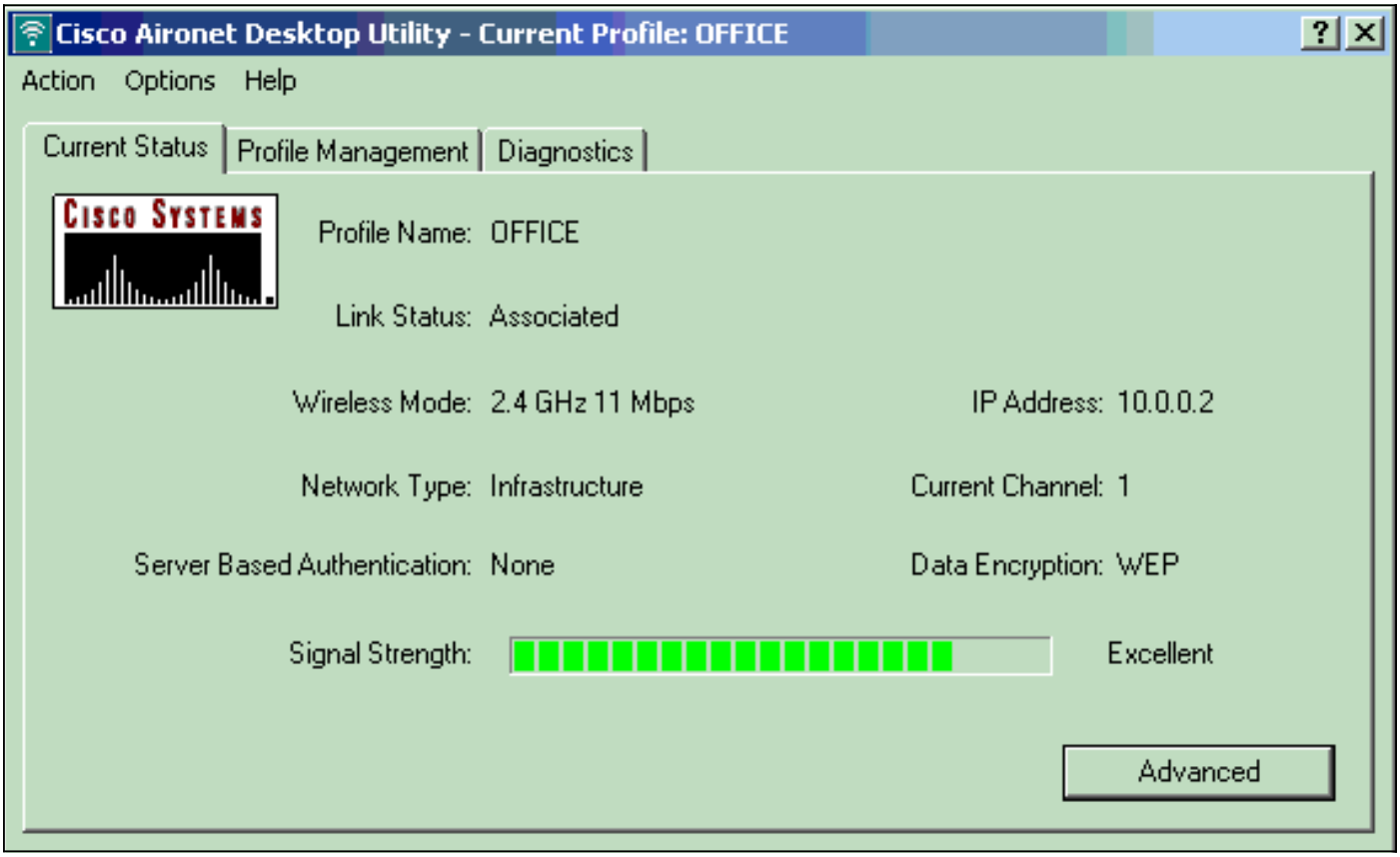
Примечание: Данный пример предполагает, что IP-адрес клиентского адаптера настроен вручную и находится в той же подсети как AP.

Проверка

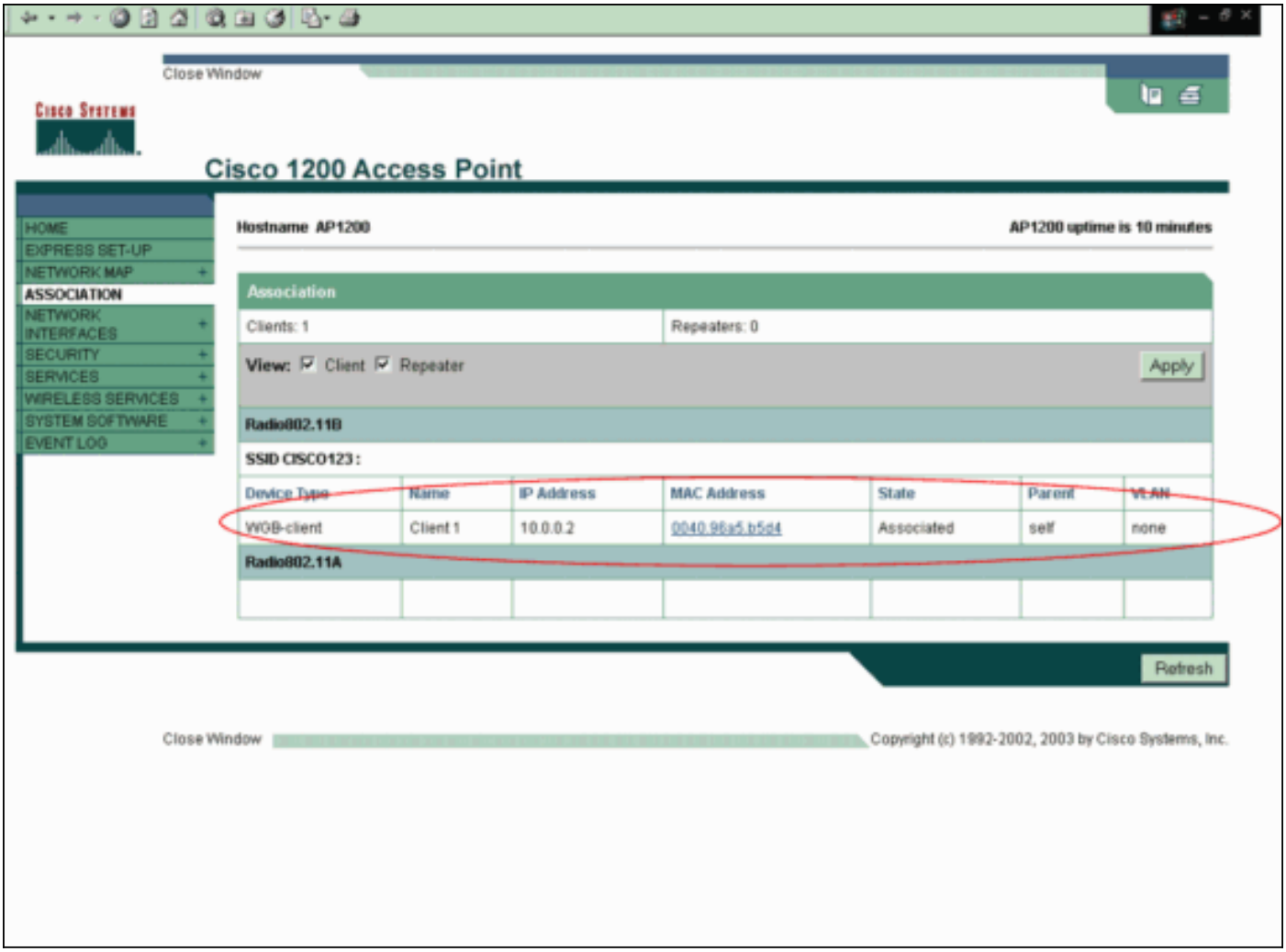
Воспользуйтесь данным разделом, чтобы проверить правильность функционирования вашей конфигурации.

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. Например:



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. Появляется 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 для точек доступа Cisco Aironet 12.3 (7) JA
- Cisco Aironet 802.11a/b/g Клиентские адаптеры беспроводной сети (CB21AG и PI21AG) Руководство по установке и конфигурированию, OL-4211-04
- Настройка точка доступа впервые
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация