

# Пример конфигурации подключения к беспроводной локальной сети с использованием маршрутизатора ISR с WEP-шифрованием и LEAP-аутентификацией

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Схема сети](#)

[Условные обозначения](#)

[Конфигурация маршрутизатора 871W](#)

[Конфигурация клиентского адаптера](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

## Введение

В данном документе описывается конфигурация маршрутизатора Integrated Services Router (ISR) Cisco серии 870 для подключения к беспроводной сети с WEP-шифрованием и LEAP-аутентификацией.

Одинаковая конфигурация применяется к любым другим Моделям серии беспроводных сетей ISR Cisco.

## Предварительные условия

### Требования

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

- Общие сведения по настройке основных параметров маршрутизатора ISR Cisco серии 870.
- Общие сведения по настройке клиентского адаптера 802.11a/b/g Wireless Client Adapter с использованием программного обеспечения Aironet Desktop Utility (ADU).

[Дополнительные сведения по настройке 802.11a/b/g Client Adapter см. в документе](#)

## Используемые компоненты

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

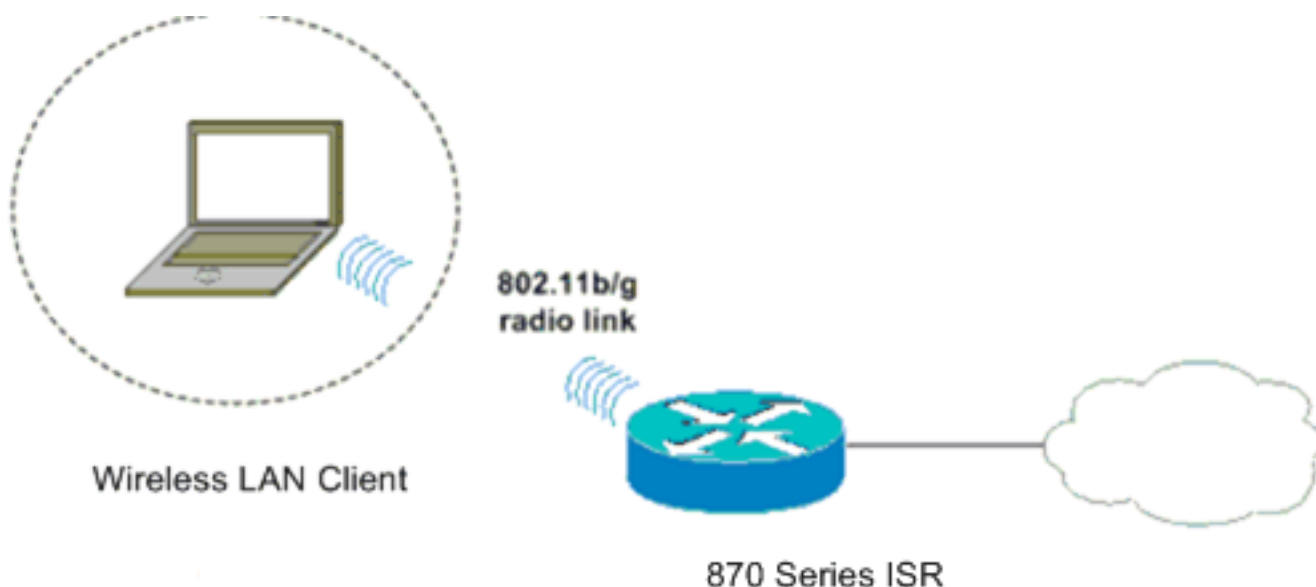
- Маршрутизатор Cisco 871W ISR, использующий программное обеспечение Cisco IOS® Software версии 12.3(8)Y11
- Ноутбук с программным обеспечением Aironet Desktop Utility версии 2.5
- Клиентский адаптер 802.11 a/b/g с микропрограммным обеспечением версии 2.5

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.

## Схема сети

В настоящем документе используется следующая схема сети.

В этой настройке клиент беспроводной локальной сети связывается с 870 маршрутизаторами. Внутренний сервер протокола динамической конфигурации хоста (DHCP) маршрутизатора 870 используется для предоставления IP-адресов беспроводным клиентам. WEP-шифрование включено на маршрутизаторе 870 ISR и клиенте беспроводной сети. LEAP-аутентификация используется для проверки подлинности клиентов беспроводной сети и локальный RADIUS сервер маршрутизатора 870 используется для проверки учетных записей.



## Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

## Конфигурация маршрутизатора 871W

Для конфигурации маршрутизатора 871W ISR в качестве точки доступа для принятия запросов ассоциации беспроводных клиентов выполните следующие действия.

1. Настройте встроенную систему маршрутизации и режима моста (IRB) и группу соединений моста. Для включения IRB введите в режиме глобальной конфигурации данные команды.  

```
WirelessRouter<config>#bridge irb !--- Enables IRB.
WirelessRouter<config>#bridge 1 protocol ieee !--- Defines the type of Spanning Tree Protocol as ieee.
WirelessRouter<config>#bridge 1 route ip !--- Enables the routing of the specified protocol in a bridge group.
```
2. Настройте виртуальный интерфейс моста (BVI). Присвойте IP-адрес BVI. Введите в глобальном режиме конфигурации данные команды.  

```
WirelessRouter<config>#interface bvi1 !--- Enter interface configuration mode for the BVI.
WirelessRouter<config-if>#ip address 172.16.1.100 255.255.0.0
```

[Дополнительные сведения по функционированию групп соединений моста в точках доступа см. в разделе Конфигурация групп моста на точках доступа и мостах документа Использование VLAN с беспроводным оборудованием Cisco Aironet Wireless.](#)
3. Настройте внутренний DHCP-сервер маршрутизатора 871W ISR. Внутренний DHCP-сервер маршрутизатора может быть использован для присвоения IP-адресов беспроводным клиентам, ассоциированным с маршрутизатором. Выполните в глобальном режиме конфигурации данные команды.  

```
WirelessRouter<config>#ip dhcp excluded-address 172.16.1.100 172.16.1.100 !--- Excludes IP addresses from the DHCP pool.
!--- This address is used on the BVI interface, so it is excluded.
WirelessRouter<config>#ip dhcp pool 870-ISR
WirelessRouter<dhcp-config>#network 172.16.1.0 255.255.0.0
```

**Примечание:** Клиентский адаптер должен также быть настроен для принятия IP-адресов от сервера DHCP.
4. Настройте маршрутизатор 871W ISR в качестве локального RADIUS сервера. Для настройки маршрутизатора 871W ISR в качестве локального RADIUS сервера введите данные команды в глобальном режиме конфигурации.  

```
WirelessRouter<config>#aaa new-model !--- Enable the authentication, authorization, and accounting !--- (AAA) access control model.
WirelessRouter<config>#radius-server local !--- Enables the 871 wireless-aware router as a local !--- authentication server and enters into configuration !--- mode for the authenticator.
WirelessRouter<config-radsrv>#nas 172.16.1.100 key Cisco !--- Adds the 871 router to the list of devices that use !--- the local authentication server.
WirelessRouter<config-radsrv>#user ABCD password ABCD
WirelessRouter<config-radsrv>#user XYZ password XYZ !--- Configure two users ABCD and XYZ on the local RADIUS server.
WirelessRouter<config-radsrv>#exit
WirelessRouter<config>#radius-server host 172.16.1.100 auth-port 1812 acct-port 1813 key Cisco !--- Specifies the RADIUS server host.
```

**Примечание:** Используйте порты 1812 и 1813 для аутентификации и составления локального сервера RADIUS.  

```
WirelessRouter<config>#aaa group server radius rad_eap !--- Maps the RADIUS server to the group rad_eap .
WirelessRouter<config-sg-radius>#server 172.16.1.100 auth-port 1812 acct-port 1813 !--- Define the server that falls in the group rad_eap.
WirelessRouter<config>#aaa authentication login eap_methods group rad_eap !--- Enable AAA login authentication.
```
5. Настройте радиоинтерфейс. Конфигурация радиоинтерфейса включает в себя настройку различных параметров беспроводной связи маршрутизатора, включая SSID, режим шифрования, тип аутентификации, скорость и роль беспроводного маршрутизатора. В данном примере используется SSID под именем Test. Введите данные команды для настройки радиоинтерфейса в глобальном режиме

```
конфигурации.WirelessRouter<config>#interface dot11radio0 !--- Enter radio interface
configuration mode. WirelessRouter<config-if>#ssid Test !--- Configure an SSID test.
WirelessRouter<config-ssid>#authentication open eap eap_methods WirelessRouter<config-
ssid>#authentication network-eap eap_methods !--- Expect that users who attach to SSID
'Test' !--- are requesting authentication with the type 128 !--- Network Extensible
Authentication Protocol (EAP) !--- authentication bit set in the headers of those requests.
!--- Group these users into a group called 'eap_methods'. WirelessRouter<config-ssid>#exit
!--- Exit interface configuration mode. WirelessRouter<config-if>#encryption mode wep
mandatory !--- Enable WEP encryption. WirelessRouter<config-if>#encryption key 1 size 128
1234567890ABCDEF1234567890 !--- Define the 128-bit WEP encryption key.
WirelessRouter<config-if>#bridge-group 1 WirelessRouter<config-if>#no shut !--- Enables the
radio interface.
```

По завершении данной операции маршрутизатор 870 принимает запросы ассоциации от беспроводных клиентов. При настройке типа EAP-аутентификации на маршрутизаторе рекомендуется выбирать оба типа Network-EAP и Open with EAP во избежание каких-либо аутентификационных проблем.

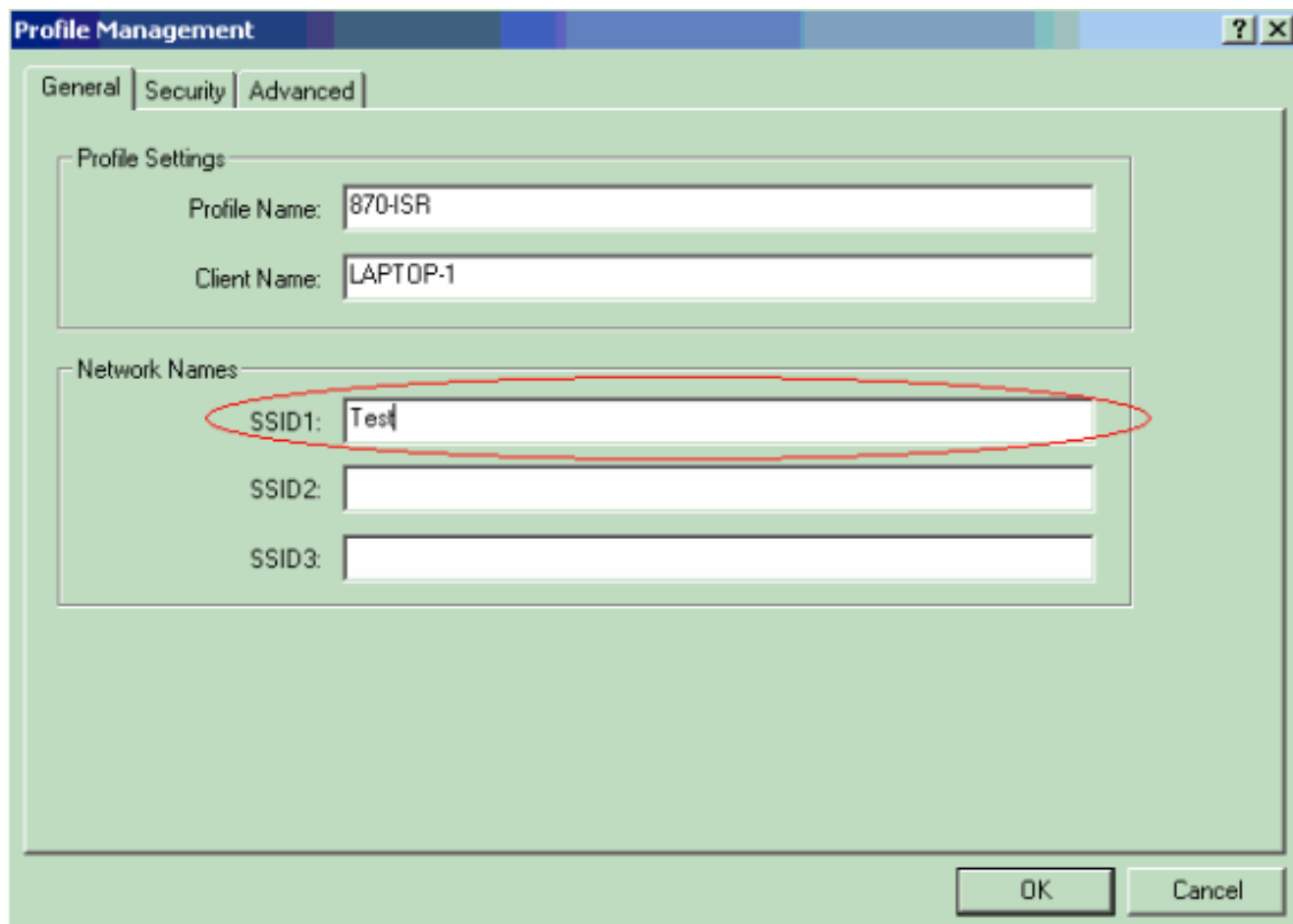
```
WirelessRouter<config-ssid>#authentication network-eap eap_methods
WirelessRouter<config-ssid>#authentication open eap eap_methods
```

**Примечание:** Этот документ предполагает, что сеть имеет только клиентов беспроводной связи Cisco. **Примечание:** [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

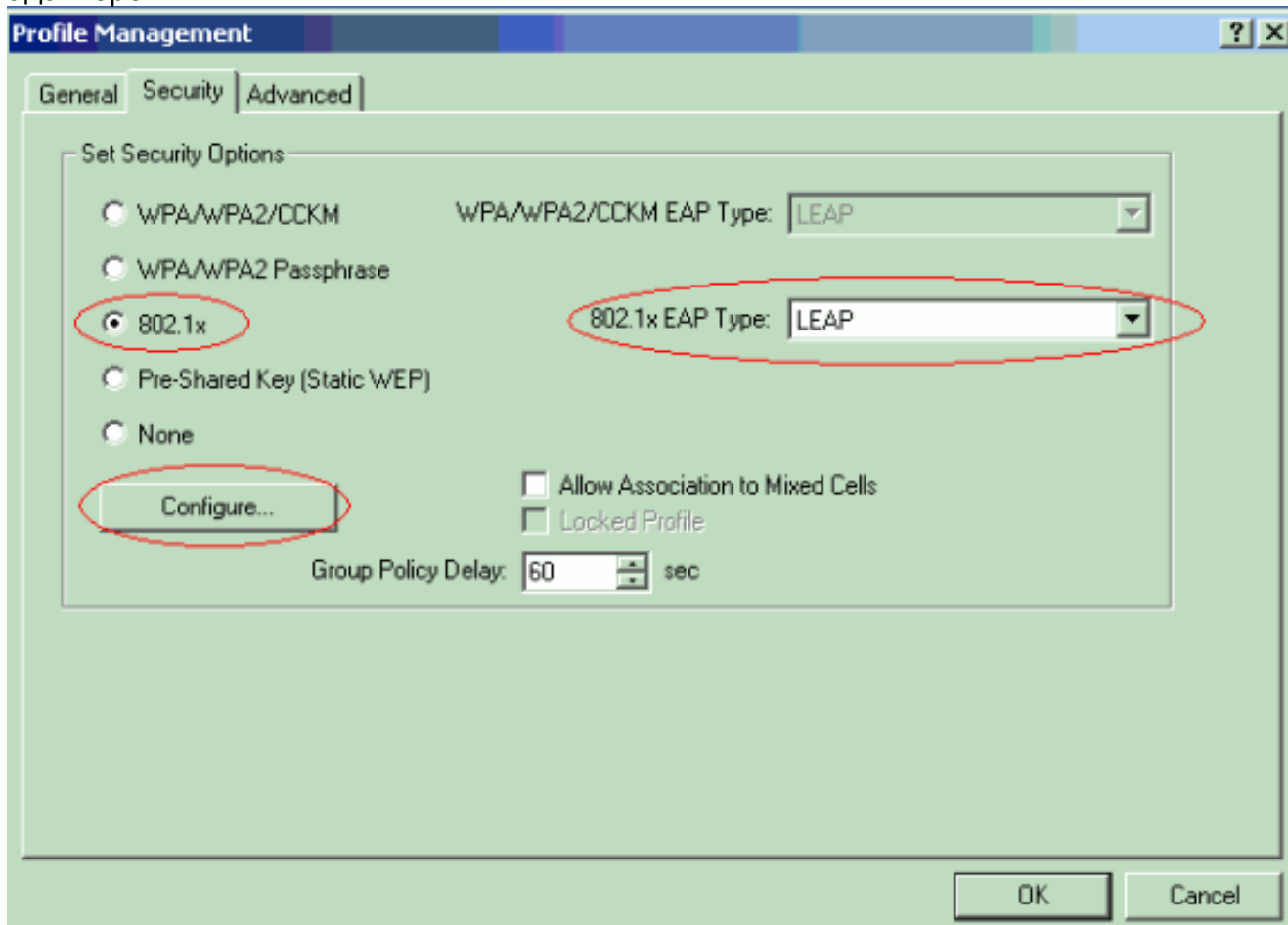
## Конфигурация клиентского адаптера

Для настройки клиентского адаптера выполните данные действия. Данное действие создает новый профиль 870-ISR в ADU в качестве примера. Данное действие также использует Test в качестве сетевого имени и включает LEAP-аутентификацию на клиентском адаптере.

1. Нажмите **New** для создания нового профиля в окне **Profile Management** в ADU. Введите название профиля и сетевое имя, используемое клиентским адаптером и указанное во вкладке **General**. В данном примере названием профиля является **870-ISR**, а сетевым именем (SSID) является **Test**. **Примечание:** SSID должен точно совпасть с SSID, который вы настроили на ISR на 871 Вт. При сравнении сетевых имен учитывается регистр символов.



2. Перейдите на вкладку Security, выберите 802.1x и LEAP в меню 802.1x EAP Type. Данное действие включает LEAP-аутентификацию на клиентском адаптере.



3. Нажмите **Configure** для настройки LEAP-аутентификации. Данная конфигурация выбирает опцию **Automatically Prompt** для имени пользователя и пароля. Данный параметр позволяет вводить имя и пароль вручную при прохождении LEAP-аутентификации.

**LEAP Settings** [?] [X]

Always Resume the Secure Session

Username and Password Settings

Use Temporary User Name and Password

Use Windows User Name and Password

Automatically Prompt for User Name and Password

Manually Prompt for User Name and Password

Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

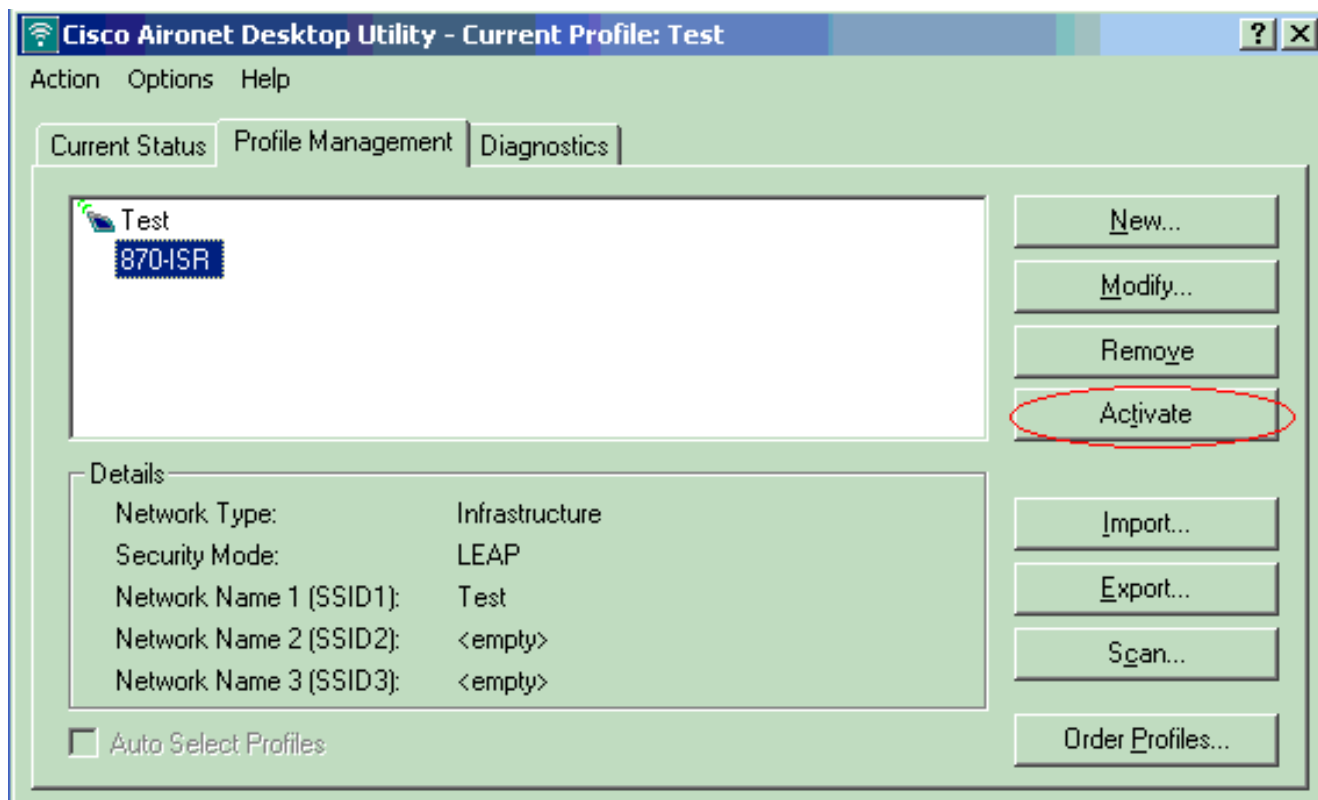
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

4. Нажмите **OK** для закрытия окна **Profile Management**.
5. Нажмите **Activate** для применения данного профиля на клиентском адаптере.



## Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

По завершении настройки клиентского адаптера и маршрутизатора 870 активируйте профиль 870-ISR на клиентском адаптере для проверки конфигурации.

Введите имя пользователя и пароль в окне Enter Wireless Network Password. Имя пользователя и пароль должны соответствовать указанным в настройках маршрутизатора 871W-ISR. **Один из профилей, используемых в данном примере, имеет имя пользователя ABCD и пароль ABCD.**

**Enter Wireless Network Password** [X]

Please enter your LEAP username and password to log on to the wireless network

User Name : ABCD

Password : \*\*\*\*

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : 870-ISR

OK Cancel

Откроется окно LEAP Authentication Status. В данном окне сверяются учетные записи пользователей с локальным RADIUS сервером.

**LEAP Authentication Status** [?] [-] [X]

Card Name: Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name: 870-ISR

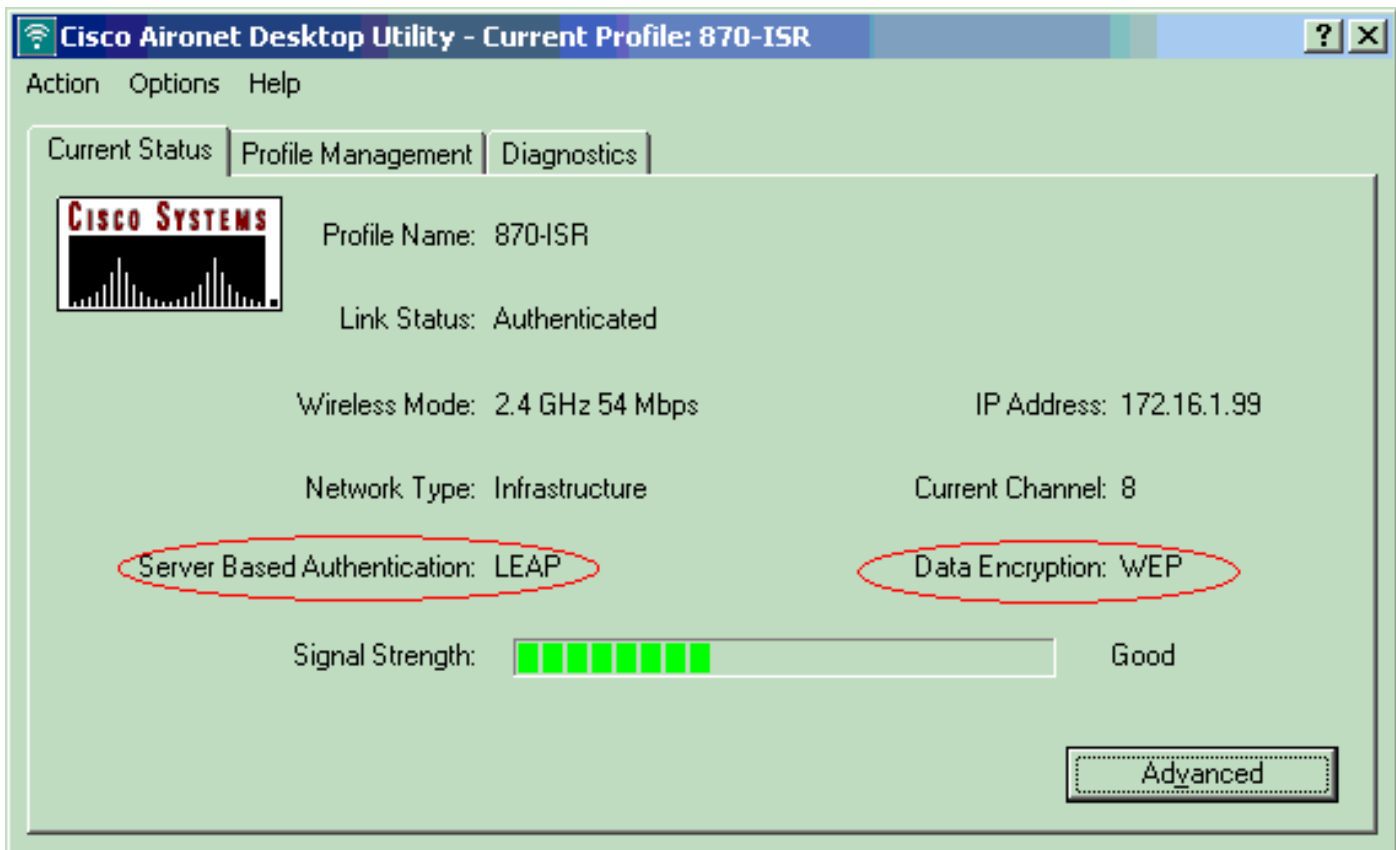
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

Show minimized next time

Cancel

На вкладке Current Status приложения ADU удостоверьтесь, что клиент использует WEP-шифрование и LEAP-аутентификацию.





[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Посредством OIT можно анализировать выходные данные команд show.

- **show dot11 association** — проверяет конфигурацию маршрутизатора

```
870.WirelessRouter#show dot11 association 802.11 Client Stations on Dot11Radio0: SSID
[Test]: MAC Address IP Address Device Name Parent State 0040.96ac.dd05 172.16.1.99
CB21AG/PI21AG LAPTOP-1 self EAP-Associated Others: (not related to any ssid)
```

- **show ip dhcp binding** — проверяет, что IP-адрес клиента присвоен DHCP-

```
сервером.WirelessRouter#show ip dhcp binding Bindings from all pools not associated with
VRF: IP address Client-ID/ Lease expiration Type Hardware address/ User name 172.16.1.99
0040.96ac.dd05 Feb 6 2006 10:11 PM Automatic
```

## Устранение неполадок

В данном разделе представлена информация по устранению проблем, касающихся данной конфигурации.

1. Установите способ Open в настройках SSID для временного отключения аутентификации. Это исключает возможность влияния проблем с радиосвязью на успешное прохождение аутентификации. Введите команды `no authentication open eap eap_methods`, `no authentication network-eap eap_methods` и `authentication open` в интерфейсе командной строки (CLI). Если клиент будет успешно сопоставлен, то радиочастота не вызовет проблем сопоставления
2. Убедитесь, что WEP-ключи, указанные в настройках маршрутизатора, совпадают с WEP-ключами клиентов. Если несовпадение присутствует, связь с маршрутизатором для клиентов будет недоступна.
3. Убедитесь, что общие секретные пароли синхронизированы между маршрутизатором и

сервером аутентификации.

Для устранения неполадок в вашей конфигурации вы также можете использовать данные команды отладки.

- `debug dot11 aaa authenticator all` — включает процесс отладки аутентификационных пакетов MAC и EAP.
- `debug radius authentication` — отображает связь RADIUS между сервером и клиентом.
- `debug radius local-server packets` — отображает содержание полученных и отправленных пакетов RADIUS.
- `debug radius local-server client` — отображает сообщения об ошибках при неудачных аутентификациях клиентов.

## [Дополнительные сведения](#)

- [Алгоритмы шифрования и типы аутентификации](#)
- [Пример настройки типов аутентификации на фиксированном ISR с помощью SDM](#)
- [Пример настройки типов аутентификации беспроводной связи на фиксированном ISR](#)
- [Руководство по настройке Cisco Access Router Wireless](#)
- [Пример настройки беспроводного маршрутизатора 1800 ISR с внутренним DHCP-сервером и открытой аутентификацией](#)
- [Страница поддержки беспроводных технологий](#)
- [Cisco Systems – техническая поддержка и документация](#)