Wireless LAN Connectivity using an ISR with WEP Encryption and LEAP Authentication Configuration Example

Document ID: 69011

Introduction

This document explains how to configure a Cisco 870 Series Integrated Services Router (ISR) for Wireless LAN connectivity with WEP encryption and LEAP authentication.

The same configuration applies to any other Cisco ISR Wireless Series models.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure the basic parameters of the Cisco 870 Series ISR.
- Knowledge of how to configure the 802.11a/b/g Wireless Client Adapter using the Aironet Desktop Utility (ADU).

Refer to Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide, Release 2.5 for information on how to configure the 802.11a/b/g Client Adapter.

Components Used

The information in this document is based on these software and hardware versions:

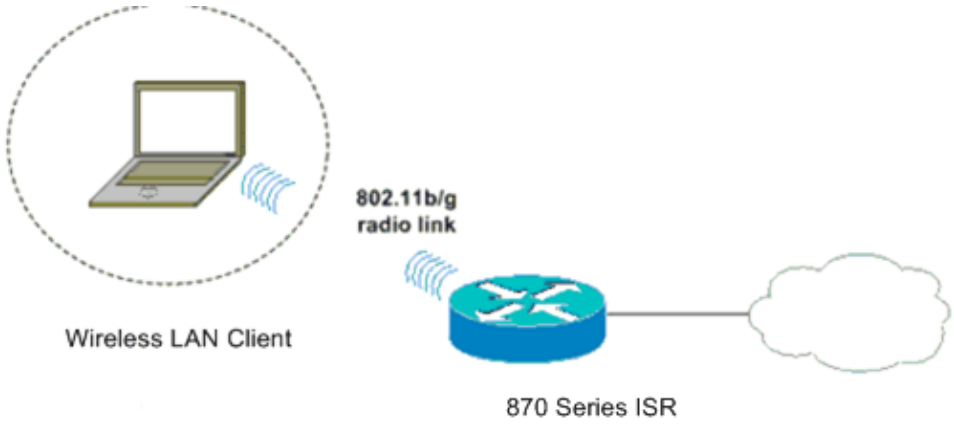
- Cisco 871W ISR that runs Cisco IOS® Software Release 12.3(8)YI1
- Laptop with Aironet Desktop Utility version 2.5
- 802.11 a/b/g Client Adapter that runs firmware version 2.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup.

In this setup, the wireless LAN client associates with the 870 router. The internal Dynamic Host Configuration Protocol (DHCP) server on the 870 router is used to provide an IP address to the wireless clients. WEP encryption is enabled on the 870 ISR and the WLAN client. LEAP authentication is used to authenticate the wireless users and the local RADIUS server feature on the 870 router is used to validate the credentials.



Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

871W Router Configuration

Complete these steps to configure the 871W ISR as an access point to accept association requests from the wireless clients.

1. Configure Integrated Routing and Bridging (IRB) and setup the bridge group.

   Type these commands from global configuration mode in order to enable IRB.

```
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. Configure the bridged virtual interface (BVI).

Assign an IP address to the BVI. Type these commands from global configuration mode.

```
WirelessRouter<config>#interface bvi1

!--- Enter interface configuration mode for the BVI.

WirelessRouter<config-if>#ip address 172.16.1.100 255.255.0.0
```

Refer to the *Bridge Group Configuration on Access Points and Bridges* section of Using VLANs with Cisco Aironet Wireless Equipment for more information about the functionality of Bridge Groups in access points.

3. Configure the internal DHCP server feature on the 871W ISR.

The internal DHCP server feature on the router can be used to assign IP addresses to wireless clients that associate to the router. Complete these commands in global configuration mode.

```
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
```

Note: The client adapter should also be configured to accept IP addresses from a DHCP server.

4. Configure the 871W ISR as a local RADIUS server.

In global configuration mode, type these commands to configure the 871W ISR as a local RADIUS server.

```
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

!--- Specifies the RADIUS server host.
```

Note: Use ports 1812 and 1813 for authentication and accounting for the local RADIUS server.

```
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. Configure the radio interface.

   The configuration of the radio interface involves the configuration of various wireless parameters on the router including the SSID, the encryption mode, the authentication type, speed, and the role of the wireless router. This example uses the SSID called **Test**.

   Type these commands to configure the radio interface in global configuration mode.

```
WirelessRouter<config>#interface dot11radio0

!--- Enter radio interface configuration mode.

WirelessRouter<config-if>#ssid Test

!--- Configure an SSID test.

irelessRouter<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.
```

The 870 router accepts association requests from the wireless clients once this procedure is done.

When you configure EAP authentication type on the router, it is recommended to choose both **Network−EAP and Open with EAP** as authentication types in order to avoid any authentication issues.

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

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

Note: This document assumes that the network has only Cisco Wireless clients.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

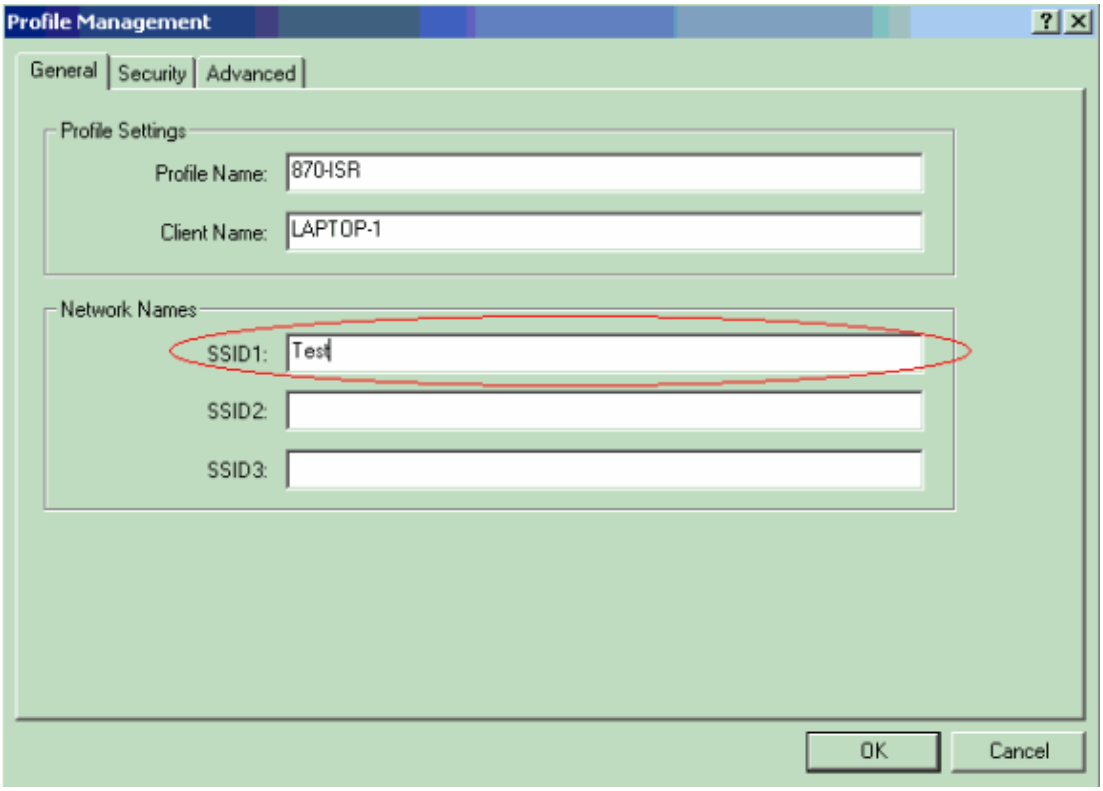
Client Adapter Configuration

Complete these steps in order to configure the client adapter. This procedure creates a new profile called **870−ISR** on the ADU, as an example. This procedure also uses Test as the SSID and enables LEAP authentication on the client adapter.

1. Click **New** to create a new profile in the Profile Management window on the ADU. Enter the Profile Name and the SSID that the client adapter uses under the General tab.

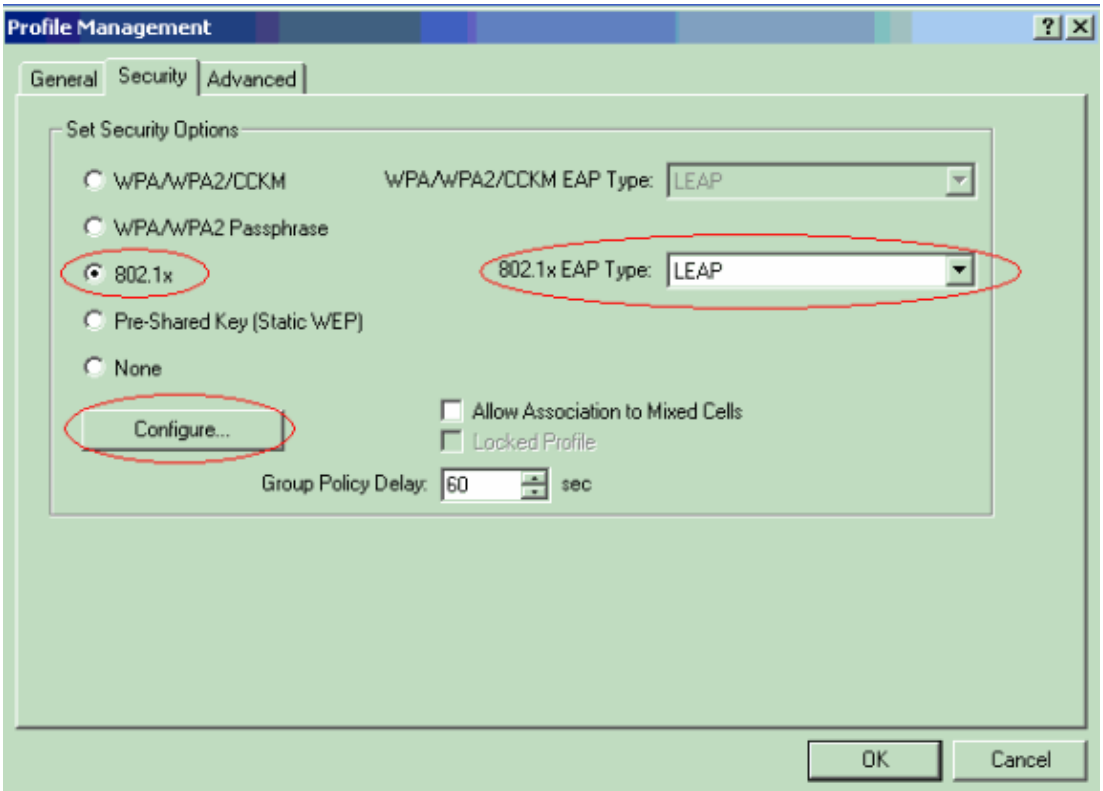
   In this example, the profile name is **870−ISR** and the SSID is **Test**.

   Note: The SSID must exactly match the SSID that you configured on the 871W ISR. SSID is case sensitive.



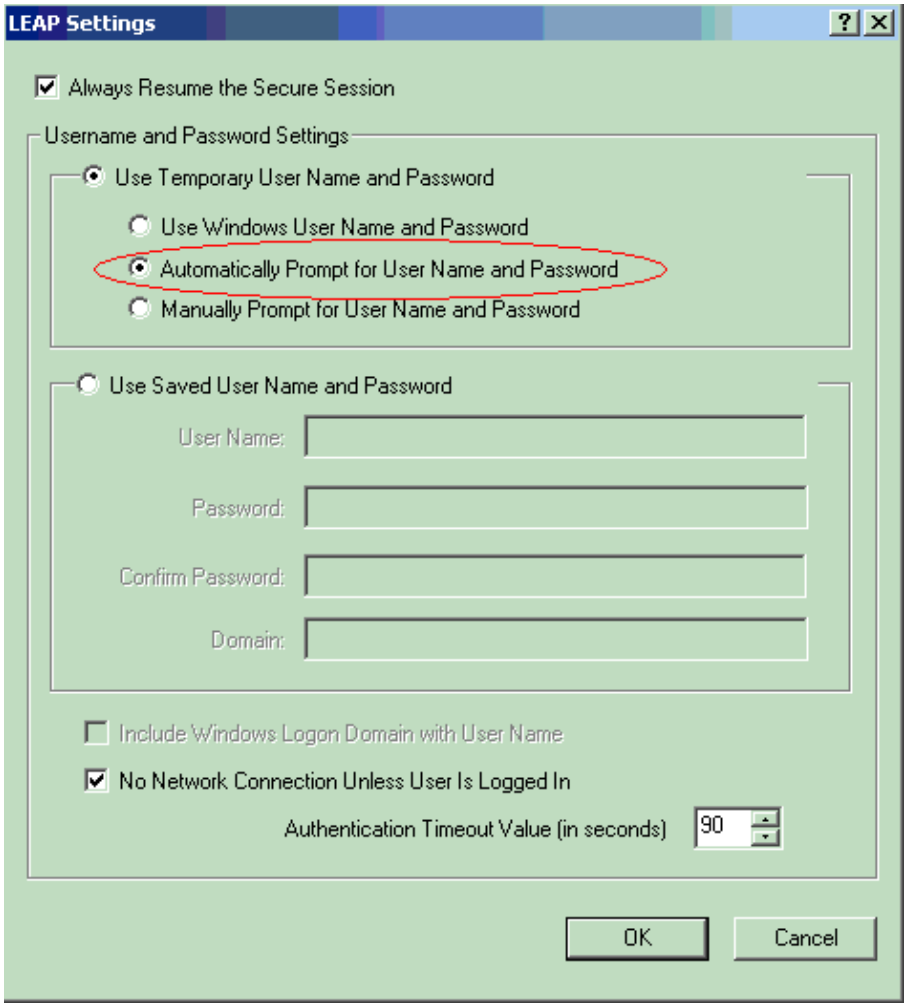
2. Go to the Security tab, select **802.1x** and choose **LEAP** from the 802.1x EAP Type menu.

   This action enables LEAP authentication on the client adapter.

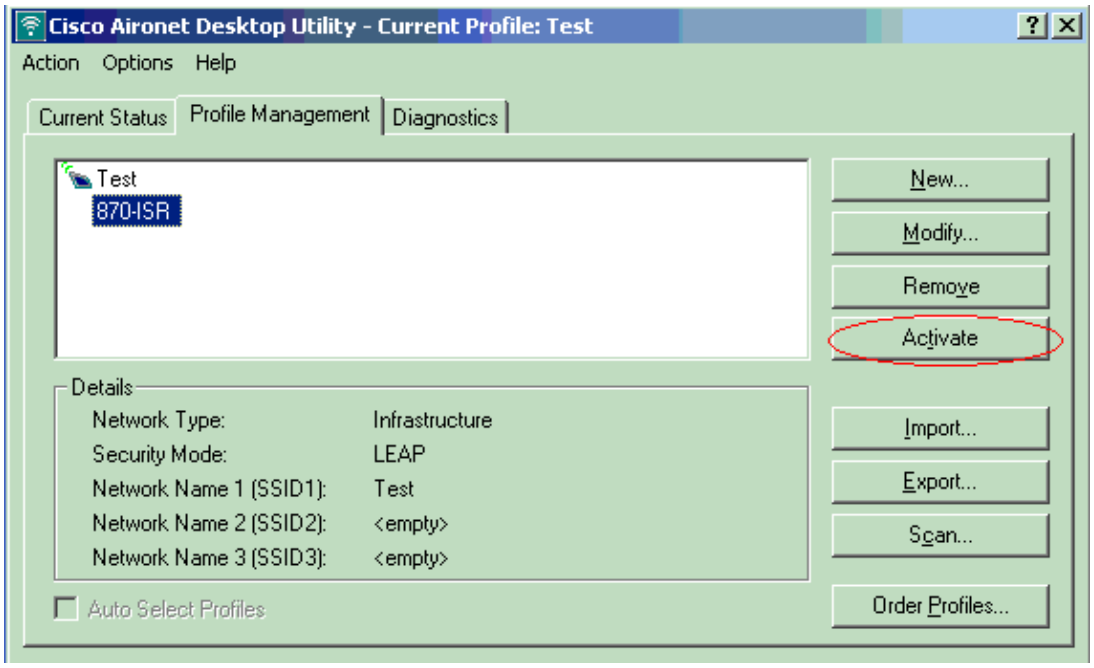


3. Click **Configure** to define LEAP settings.

   This configuration chooses the option **Automatically Prompt for Username and Password**. This option enables you to manually enter the user name and password when LEAP authentication takes place.



4. Click **OK** to exit the Profile Management window.
5. Click **Activate** to enable this profile on the client adapter.

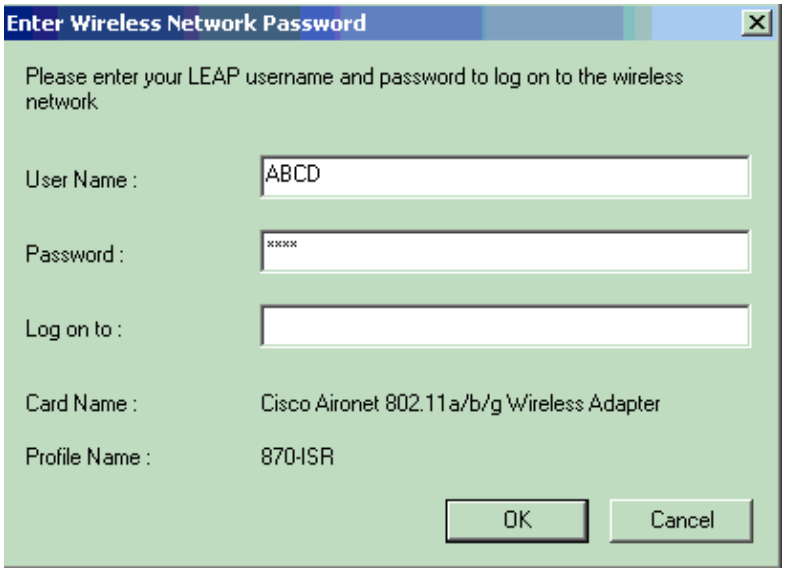


Verify

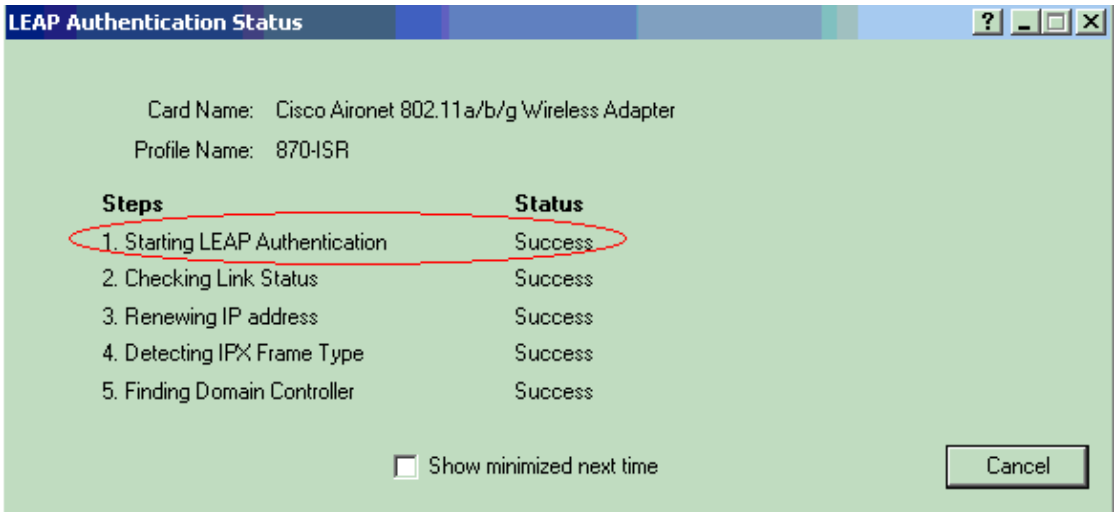
Use this section to confirm that your configuration works properly.

Once the client adapter and the 870 router is configured, activate the profile 870−ISR on the client adapter to verify the configuration.

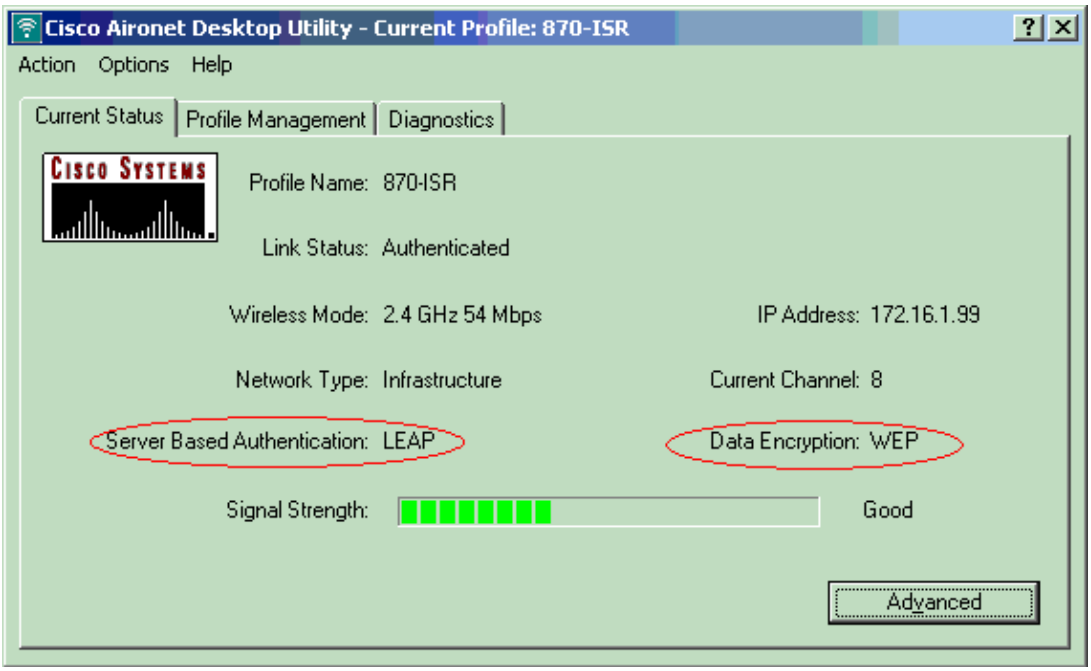
Enter the user name and password when the Enter Wireless Network Password window displays. These should correspond to the ones configured in the 871W ISR. One of the profiles used in this example is User Name **ABCD** and Password **ABCD**.



The LEAP Authentication Status window appears. This window verifies the user credentials against the local RADIUS server.



Check the ADU Current Status in order to verify that the client uses WEP encryption and LEAP authentication.



The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show dot11 association** Verifies the configuration on the 870 router.

```
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** Verifies that the client has an IP address through the DHCP server.

```
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
```

Troubleshoot

This section provides troubleshooting information relevant to this configuration.

1. Set the method on the SSID to **Open** in order to temporarily disable authentication.

   This eliminates the possibility of radio frequency (RF) issues preventing successful authentication.

   - Use the **no authentication open eap eap_methods**, **no authentication network-eap eap_methods** and **authentication open** commands from the CLI.

   If the client successfully associates, then RF does not contribute to the association problem
2. Check if the the WEP keys configured on the wireless router match with the WEP keys configured on the clients.

If there is a mismatch in the WEP keys, the clients are not able to communicate with the wireless router.

3. Verify that shared secret passwords are synchronized between the wireless router and the authentication server.

You can also use these debug commands to troubleshoot your configuration.

- **debug dot11 aaa authenticator all** Activates the debugging of MAC and EAP authentication packets.
- **debug radius authentication** Displays the RADIUS negotiations between the server and client.
- **debug radius local−server packets** Displays the content of the RADIUS packets that are sent and received.
- **debug radius local−server client** Displays error messages about failed client authentications.

Related Information

- **Encryption Algorithms and Authentication Types**
- **Wireless Authentication Types on Fixed ISR Through SDM Configuration Example**
- **Wireless Authentication Types on a Fixed ISR Configuration Example**
- **Cisco Access Router Wireless Configuration Guide**
- **1800 ISR Wireless Router with Internal DHCP and Open Authentication Configuration Example**
- **Wireless Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Apr 07, 2008 Document ID: 69011