Unified Wireless Network: Troubleshoot Client Issues

Document ID: 107585

Contents

Introduction

The radio frequency (RF) environment is complex and dynamic. Various factors need to be considered to create a good wireless environment. This document explains various issues that you can encounter when you connect a wireless client in a Cisco Unified Wireless environment, as well as the steps to be taken to troubleshoot and resolve these issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Wireless solution
- Cisco Wireless LAN Controllers (WLC) GUI basic configurations

Components Used

This document is applicable to all devices that participate in the Cisco unified environment but is not restricted to specific software and hardware versions.

Conventions

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

Background Information

In a Cisco Unified environment, the WLC assumes a central role. It manages the entire wireless network. Lightweight access points (LAPs), which serve the wireless clients, register themselves to the WLC and download the entire configuration from WLC. The initial step is to check if the LAP is registered to the WLC. Click the wireless menu from WLC GUI, and check if the LAP is listed on the page.

Configuration Issues

For a successful wireless connection, it is essential that configuration on the WLC is done correctly. This section describes some of the most commonly seen configuration issues.

SSID Mismatch

The client uses its SSID to identify and associate to the wireless network, so ensure that the SSID is configured identically on the WLC and the client. In order to check the SSID configured on the WLC, click the **WLANs** page. Click the appropriate *WLAN*, and check the *SSID* configured under the *General* tab.

Note: *SSID* is case sensitive. It might help the wireless client to associate to the WLAN if you delete and recreate the WLAN.

Security Mismatch

Security configurations must match between the WLC and the client. If the authentication type is Static WEP, check if the appropriate encryption key/key index on the WLC matches that of the client. If the authentication type is 802.1x or WPA, ensure that the authentication type/encryption key size matches between the client and the WLC. For more information on how to configure the WLC and the client for various security solutions, refer to Authentication on Wireless LAN Controllers Configuration Examples.

Note: Layer 2 security solutions, such as WPA or 802.1x, cannot be used for a WLAN configured with Layer 3 security solutions, such as web authentication or passthrough. For more information on compatible security solutions refer to Wireless LAN Controller Layer 2 and Layer 3 Security Compatibility Matrix.

Disabled WLAN

For a successful wireless connection, the corresponding WLAN must be active on the WLC. By default, the status of the WLAN is not enabled on the WLC. In order to activate the WLAN, click the **WLANs** menu in the WLC. A list of WLANs configured on the WLC displays. Click the WLAN that is configured with the SSID to which the client wants to associate. Under the General tab of the **WLANs > Edit** page, check the status box.

Unsupported Data–Rates

For a particular standard, either 802.11b/g or 802.11a, you can optionally set certain data rates as mandatory and other data rates as supported or disabled on the WLC. For a successful association, a wireless client must support the data rates that are configured as mandatory on the WLC. In order to check the data rates configured on the WLC, click the **Wireless** menu on the WLC GUI, and check the data rates configured under the **802.11b/g/n > Network or 802.11a/n > Network** option that appears on the left–hand side of the page. Check the support page of the client vendor to determine this. If you upgrade the client driver, it can help the client to support the required data rates.

Note: For better connectivity, set the lowest data rate to **mandatory** on the WLC and other data rates to **supported**.

Disabled Clients

On the WLC, there is an option to manually disable the clients. This feature helps to prevent rogue clients from trying to access the network. Check whether the MAC address of the client that is unable to associate is found in the Disabled Clients list, and, if so, remove it. You can find the list of disabled clients when you click the **Disabled Clients** option under the **Security** menu in the GUI.

Note: Clients can be denied association to the network if they do not abide by the default Client Exclusion policies configured on the WLC. For more information on the Client Exclusion policy, refer to the Configuring Client Exclusion Policies section of the Cisco Wireless LAN Controller Configuration Guide, Release 4.2.

Radio Preambles

The radio preamble (sometimes called a header) is a section of data at the head of a packet, which contains information that wireless devices need when they send and receive packets.

Some clients do not support **short preamble**, so they cannot connect to the WLAN that has **short preamble** enabled. Short preambles improve throughput performance, so they are enabled by default on the WLC. In order to disable the **short preamble**, click the **Wireless** menu of the WLC GUI. Then click the **802.11b/g > network** menu on the left–hand side. *Uncheck* the **short preamble** box.

Cisco Properietary Features – Issues with Third Party Clients

If the client devices that are unable to connect to the network are non–Cisco devices, disabling some of the Cisco proprietary features results in a successful connection. For a list of features that the client supports, contact the vendor of the third–party client device.

These are some of the important proprietary features:

- **Aironet IE** Aironet IE contains information, such as the access point name, load, number of associated clients, and so on sent out by the access point in the beacon and probe responses of the WLAN. CCX clients use this information to choose the best access point with which to associate.
- **MFP** Management Frame Protection is a feature introduced to ensure the integrity of the management frames, such as de–authentication, disassociation, beacons, and probes wherein the access point protects the management frames that it transmits when it adds a Message Integrity Check Information Element (MIC IE) to each frame. Any attempt made by the intruders to copy, alter, or replay the frame invalidates the MIC, which causes any receiving access point, which is configured to detect MFP frames, to report the discrepancy.

These features are enabled by default for any WLAN that is created on the WLC. In order to disable these features, click the **WLANs** menu in the WLC. A list of WLANs configured on the WLC displays. Click the WLAN to which the client wants to associate. Under the **Advanced Tab of WLANs > Edit page**, uncheck the boxes that correspond to **Aironet IE and MFP**.

- **Radio Preambles** The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that the wireless device and client devices need to send and receive packets. You can set the radio preamble to long or short depending on which setting is supported on the wireless client.
- **Ethernet Encapsulation Transformation** When the wireless device receives data packets that are not 802.3 packets, the wireless device must use an encapsulation transformation method to format the packets to 802.3. Here are the two transformation methods:

  - 802.1H: This method provides optimum performance for Cisco Aironet wireless products. 802.1H is the default setting.
  - RFC1042: Use this setting to ensure interoperability with non−Cisco Aironet wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H, but is used by other manufacturers of wireless equipment.

- **wpa handshake timeout** Some vendors need longer wpa handshake timeouts. You can use the **dot11 wpa handshake timeout** command in order to change the wpa handshake timeout.
- **ssid** Some vendors require the ssid to be broadcast. In order to broadcast the ssid, enable *guest−mode* under the ssid configuration.

IP Address Issues

Wireless clients need valid IP addresses to communicate with the rest of the network.

The controller behaves like a router with an IP helper address. That is, it fills in the gateway IP address and unicasts it to the DHCP server via the dynamic interface on which the client is installed. So be aware that DHCP snooping on switches will, by default, block these DHCP packets on untrusted ports.

When the DHCP offer comes back to the controller, it changes the DHCP server IP address to its virtual IP address. The reason it does this is because when Windows roams between APs, the first thing it does is try to contact the DHCP server and renew its address.

With the DHCP server address of 1.1.1.1 (which is the typical virtual IP address on a controller), the controller can intercept that packet and fake out Windows. That is also why the virtual IP address is the same on all controllers. If a Windows laptop roams to an AP on another controller, it will try to contact the virtual interface on the controller. Due to the mobility event and context transfer, the new controller to which the Windows client roamed already has all the information to fake out Windows again.

If you want to use the internal DHCP server, all you have to do is put the management IP address as the DHCP server on the dynamic interface you create for the subnet. Then assign that interface to the WLAN. The reason the controller needs an IP address on each subnet is so it can fill in the DHCP gateway address in the DHCP request.

We see a lot of DHCP/ IP address problems. Here are the reasons and steps to resolve these issues:

1. If the type of authentication configured is one of Layer 2 security solutions, such as 802.1x or WPA, the client must successfully authenticate to obtain a valid IP address. First check if the client is successfully authenticated.

   Note: An exception is if the client is configured for Layer 3 security solutions, such as web authentication, or the web passthrough client is assigned an IP address before authentication.

2. Each WLAN defined on the WLC is mapped to a dynamic interface of the WLC, which is configured with a VLAN that belongs to a unique subnet. Clients that associate to this WLAN are assigned IP addresses from the interface subnet of the VLAN. Check if the IP subnet and gateway of this WLAN are defined on the DHCP server for the client to obtain an IP address on this subnet. Refer to the documentation of the appropriate vendor to configure the DHCP server.

   Note: As a prerequisite, check whether the DHCP server is reachable from the WLC and if the DHCP service is turned on.
3. Make sure that the IP address of the DHCP server is defined correctly in the interface of the WLC that is mapped to the WLAN. In order to check this, click the **Controller** menu in the GUI. Click the **Interfaces** menu on the left−hand side, and check the **DHCP** server field. On the same page, check that the interface is mapped to a *physical port* that is up and active. In order to troubleshoot DHCP related issues, use the commands **debug dhcp packet enable** and **debug dhcp message enable** on the WLC.

   Note: You can also configure WLC as a DHCP server. For more information on how to configure the DHCP sever on the WLC, refer to the Using the GUI to Configure DHCP section of the document Cisco Wireless LAN Controller Configuration Guide, Release 5.0.
4. DHCP proxy is enabled by default on the WLC. WLC unicasts the packet to the DHCP server configured on the WLAN's interface or the WLAN itself. If the DHCP server does not support the Cisco DHCP proxy behaviour, disable DHCP proxy on the WLC. For more information on how to disable DHCP Proxy on the WLC, refer to Configuring DHCP Proxy section of Cisco Wireless LAN Controller Configuration Guide, Release 5.2 .
5. WLC usually connects to the wired network through a switch. Check if switch ports that are connected to the WLC and the DHCP server are configured as trunk and that the appropriate VLANs are allowed on those ports. For more information on how to configure the Cisco switches, refer to the Configure the Layer 2 Switch Port that Connects to the WLC as Trunk Port section of the document Guest WLAN and Internal WLAN using WLCs Configuration Example.
6. Static clients are not allowed to associate to the WLAN if the **DHCP Addr. Assignment field** is enabled for the WLAN. This option necessitates that all clients that associate to this WLAN must obtain IP addresses through DHCP. In order to check if this option is enabled, click the WLANs menu in the WLC GUI. A list of WLANs configured on the WLC displays. Click the appropriate WLAN. Go to the **Advanced** tab and locate the **DHCP Address Assignment** field.
7. Some DHCP servers, such as a Cisco PIX firewall, do not support DHCP relay services. They accept only broadcast DHCP packets, not any unicast packets from a DHCP relay agent, so ensure that the DHCP clients are directly connected to the interface on which the server is enabled.

   Note: Check the appropriate vendor document for DHCP relay support.

Client Issues

It is equally important that things are in place on the client side. Perform these checks on the client side:

1. Sometimes, the client card is not recognized by the computer. In that case, try the card on a different slot. If it does not work, try it on a different computer. For more information on issues within installation, refer to the Troubleshooting section of the document Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows.

   Note: Make sure that the wireless card is compatible with the operating system that is installed on the machine. This can be checked from the data sheet of the client card.
2. Check if the client is installed properly on the machine. The status of the client card can be checked from the **Windows Device Manager** screen. Look for the message that reads, *"This device is working properly."* If it is not, it indicates that the drivers are not installed properly. Try to uninstall the driver

and reinstall the drivers on the machine. In order to uninstall the drivers, right−click the wireless adapter from the Device Manager screen and click **Uninstall**. For more information on how to reinstall the client adapter, refer to the Installing the Client Adapter section of the document Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows.

Note: If you use ACU to configure the client card, make sure that the radio is not disabled on the ACU. In addition, check if the status of the card is enabled under **Network Connection** on the Windows Control Panel.

Note: Use only one supplicant software for the wireless card. It is always recommended to use the vendor−provided supplicant for the card. As a secondary option, you can either use the one provided by the PC vendor or the WZC provided by Windows.

Note: Complete these steps in order to debug WZC:

  a. Use the **netsh ras set tracing * enabled** command in order to turn on WZC debugging.
  b. Use the **netsh ras set tracing * disabled** command in order to turn off WZC debugging.

  Logs are written to *C:\Windows\tracing*. *eapol.log*, *rastls.log*, and *wzctrace.log* are the most important logs.

Note: Refer to Wireless Diagnostics and Troubleshooting for more information.

3. Configuration on the client must match that of WLC. This mainly refers to the SSID and security configuration on the client. If you use the Cisco utility to configure the client, refer to the Using the Profile Manager section of the document Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows.
4. If you are unable to transfer data, even after a successful wireless association, try to disable all other adapters as well as those of VPN and wired adapters. If there is more than one wireless adapter in the machine, disable other adapters to avoid conflicts between them.
5. If you find connectivity issues only with a single client, try to upgrade the drivers and firmware of that client. If you find connectivity issues with a majority of the clients and you have ruled out other issues, choose to upgrade the WLC.
6. Ensure that the devices, that is, client and the WLC, are Wi−Fi certified to avoid any interoperability issues related to security and operations.
7. If you use a Windows machine, make sure that you have installed all the latest security patches or hotfixes available from Microsoft. If you use Windows client utility, make sure that you have installed the latest patch available from Microsoft.
8. Some clients respond slowly to EAP authentication. This results in time−outs on the WLC, and you can receive this error message on the WLC:

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>
```

In response to this message, increase the EAP time−out values on the WLC to provide sufficient time for the client to authenticate. Use these commands to adjust the EAP timers on the WLC:

```
config advanced eap identity-request-timeout <1-120 secs>
config advanced eap identity-request-retries    <1-20>

!--- Specifies the amount of time and the maximum number of
   times the WLC attempts to send an EAP identity request to wireless clients.


config advanced eap request-timeout <1-120>
config advanced eap request-retries <1-20>
```

```
!--- Specifies the amount of time and the maximum number of t
   imes the WLC attempts to send  EAP request to the Radius Server .


config advanced eap eapol-key-timeout <1-5>
config advanced eap eapol-key-retries <0-4>

!--- Specifies the amount of time and the maximum number of
   times the WLC attempts to negotiate the encryption key.
```

RF Issues

RF interference is one of the main causes for poor connection. Interference can be caused by adjacent 802.11 networks or other sources, such as Microwave ovens or cordless phones that operate in the same frequency. Interference caused by adjacent 802.11 networks is of two types:

- **Co−channel interference:** When access points, whose coverage area overlaps,, are configured in the same channel or channels with overlapping frequencies, it causes connectivity issues for clients in the overlapping coverage area. In order to avoid this issue, either change the channel number to a non−overlapping channel, or move the access point farther away so that their coverage areas do not overlap. For example, in 802.11b/g, network channels 1, 6, and 11 are non−overlapping channels.
- **Adjacent Channel interference:** When access points are placed too close to each other or use high output power levels, it causes interference, even when the access points are configured on the non−overlapping channels. Decrease the power of the access point to fix this issue.

  Note: Non−overlapping channels are also called adjacent channels, which explains the name *adjacent channel interference*.

Use spectrum analyzers to locate interference sources, such as microwave ovens or cordless phones that operate in the 2.4 GHz range, or devices that operate in the 5 GHz range. Remove the interference sources once they are identified. Alternatively, you can change the standard on which your wireless networking operates, for example, from 802.11b/g to 802.11a to avoid interference.

Another important aspect for effective RF communication is signal strength. Poor signal strength leads to intermittent connection. Obstacles, such as walls, metals, absorb and reflect RF energy, which reduces the signal strength. Increase the power to the required level on the access point to provide the adequate coverage. You can also use high gain antennas to extend the range and the signal strength, but ensure that it is FCC approved to operate with the device.

Note: Signal to Noise Ratio (SNR), which is the difference between the signal strength and the RF noise (RF signal or energy from other sources that operates in the same frequency as the wireless network), is a key factor to measure the quality of the link. Higher SNR indicates a good link quality, which results in faster data transfer. A lower value indicates poor quality, which leads to intermittent connectivity or poor performance. Wireless Packet analyzers/site survey software can show you the SNR and throughput at a particular location.

In the Cisco unified environment, there is a concept called Radio Resource Management (RRM) implemented on the WLCs. The RRM is a software embedded in the controller, which acts as a built−in RF engineer to consistently provide real−time RF management of your wireless network. It automatically takes care of all the mentioned RF issues. For more information on RRM, refer to the Configuring Radio Resource Management section of the document Cisco Wireless LAN Controller Configuration Guide, Release 5.0.

Error Messages

Amid the course of client connectivity, you can receive multiple error messages, both on the WLC and client sides.

- **The client is either unable to get an IP address or encounter delay in getting the IP address through DHCP. The debug dhcp on the controller indicates this:**

```
Sun Nov 9 22:09:05 2008: <mac address of the client> DHCP processing DHCP NAK
```

DHCP NAK is usually sent by the DHCP server to indicate an attempt by the client to obtain an IP address from the subnet to which it does not belong. This usually occurs when a client roams from one WLC to another, where the same WLAN is assigned a different VLAN.

Configure the DHCP proxy on the WLC to provide a fix for this.

Troubleshooting Client Issues with WCS

WCS can be used to troubleshoot client–related issues in a wireless environment. It does this with the help of the Troubleshooting tool built into WCS. In order to troubleshoot a client through the WCS, users need to perform these steps

1. From the WCS Dashboard page, click the **Monitor** menu and choose **Clients** from the list.
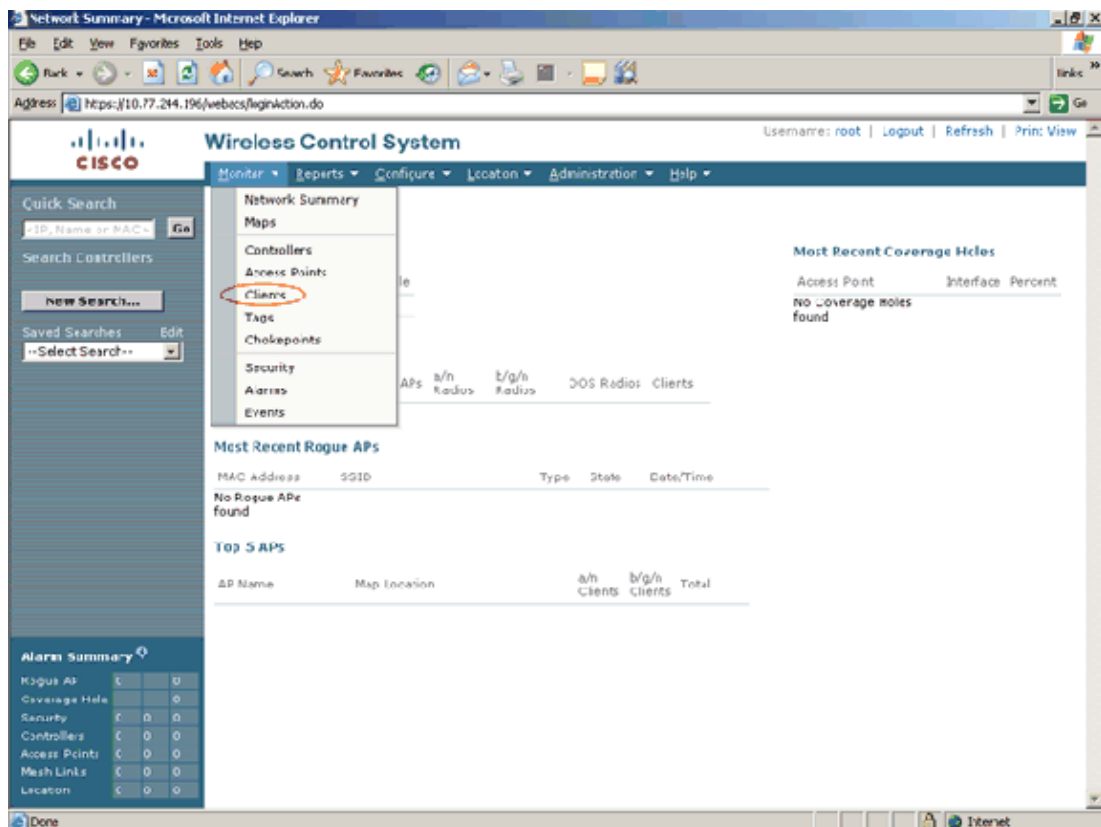
2. This brings up the Client Summary page as shown in Figure 1, which displays the list of clients in the wireless network.

Figure 1
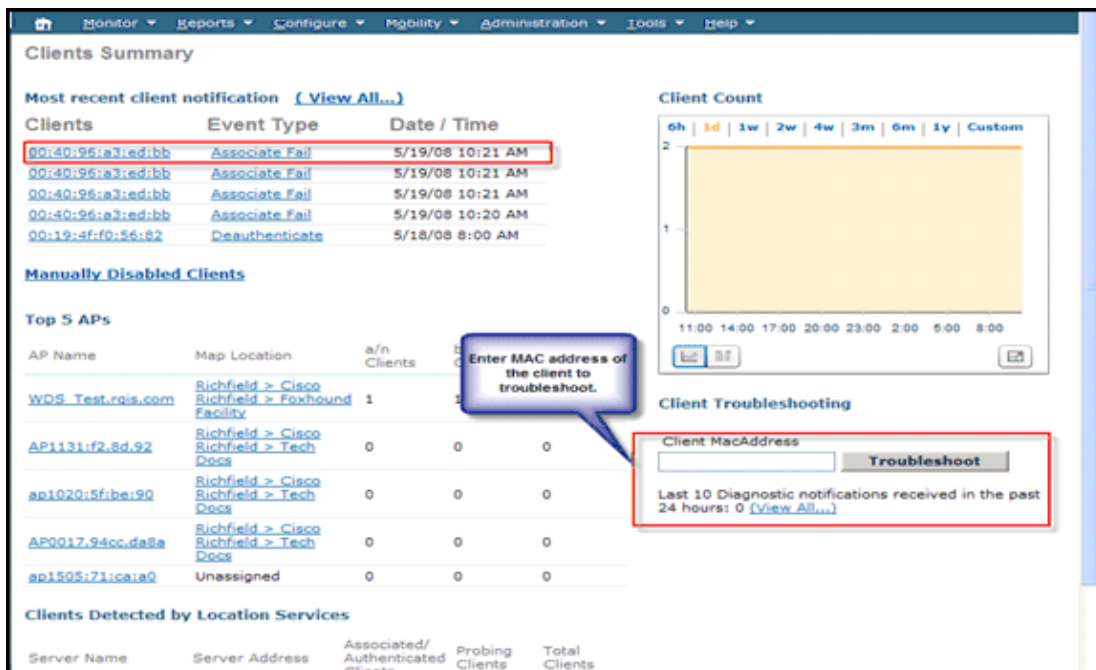
3. Click a client to get details such as the SSID or authentication method of a particular client. Figure 2 shows an example of this. The **Troubleshoot** dialogue box at the bottom right–hand side of the Client Summary page shown in Figure 1 allows users to enter in the MAC address of the device to troubleshoot. This brings you to the Troubleshooting Tool page as shown in Figure 3. Upon identification and selection of the client to troubleshoot, users are presented with the Client Details page:

Figure 2
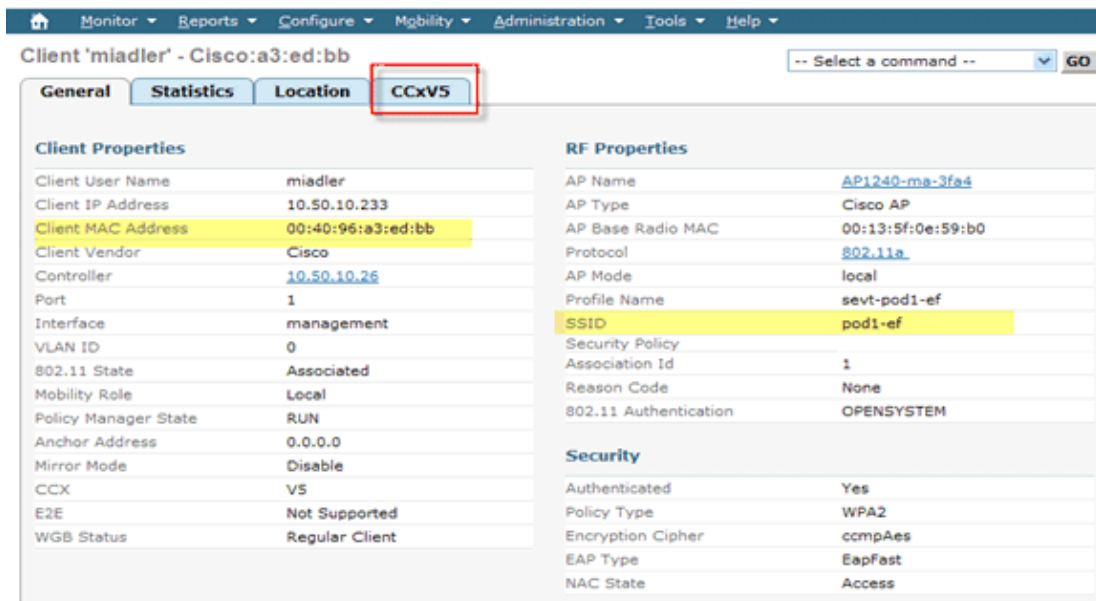
Troubleshooting WEP

Legacy wireless clients that still use the WEP security mechanisms are often hard to troubleshoot. Perform these checks on the client and AP:

- WEP key length (and key mismatches)
- WEP key index (and configuration mismatches)
- Configured authentication method (open versus shared key)

Authentication Mismatch

Although the capture of packets can be a tedious process, the WCS client troubleshooting tool can easily help point out where the problem exists. Often, this little tip is what reduces troubleshooting time. Figure 2 shows the **WCS troubleshooting tool**. As presented in the figure, the problematic stage is identified and visualized, which sets the stage for detailed analysis.

Figure 3
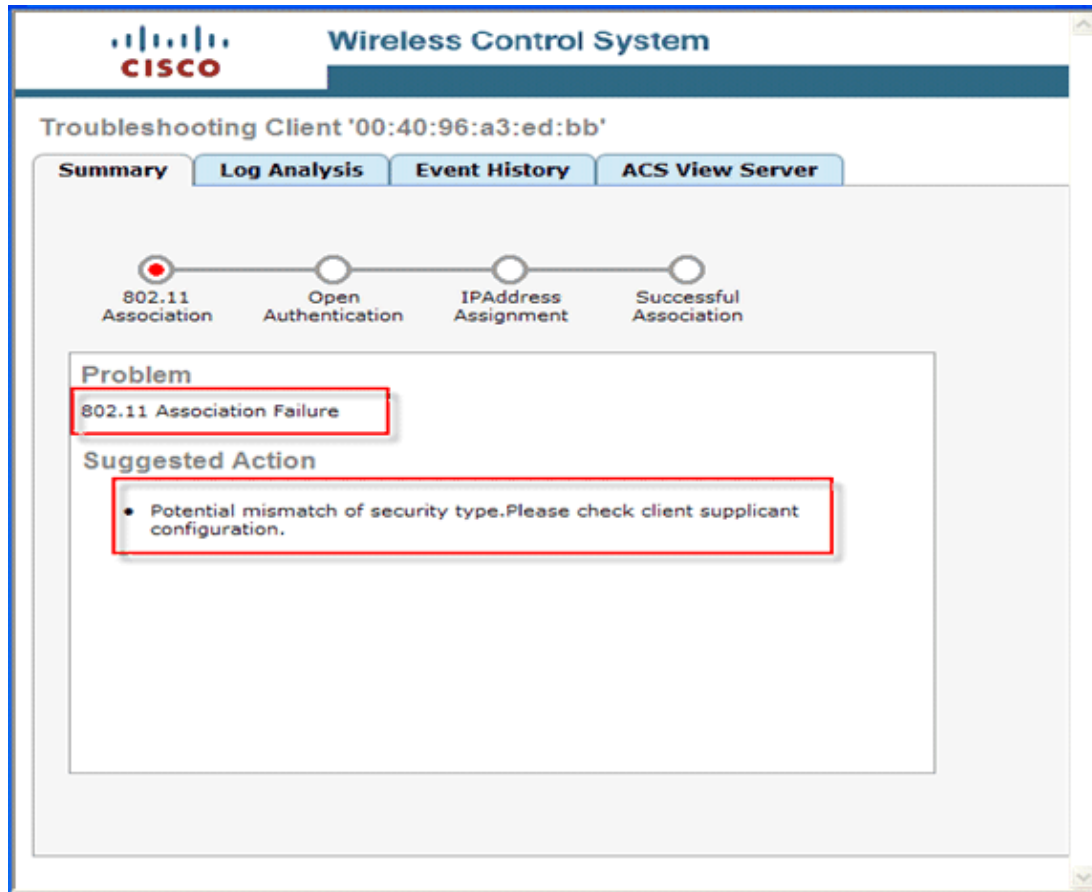
WEP Key Index Mismatch

In general, you can configure up to 4 WEP keys on the client and AP. One of the keys is chosen as the transmit key. This must match between the client and the AP. For example, if Key 2 is chosen as the transmit key on the client, this must match with the Key 2 on the AP, but AP can have a different key than the transmit key. Another issue is often this: client and infrastructure vendors interpret the specifications differently, which causes different implementations in the product. One common example is the usage of key indexes from 0 through 3 versus key indexes from 1 through 4. This can result in mismatched configuration and failed connection attempts. At that point, pay close attention to the Key ID filed in the packet decode, which tells if that is the root cause of the problem.

Troubleshooting WPA−PSK

WPA−PSK troubleshooting is similar to WEP in many ways. Most failed attempts are due to misconfigurations in the key. With the WCS Client troubleshooting tool, administrators can collect the logs of the WPA transaction. The logs, as highlighted below, display where the potential problem can be *(incorrect pre−shared key configuration on the client in this particular example)* and are derived from the **Log Analysis** tab of the client troubleshooting tool of WCS. Set up a WLAN with WPA−PSK as Layer 2 security policy and

configure the client supplicant with an incorrect PSK. These are logs of misconfigured PSK keys in the events:

```
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received.
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client.
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting requires 802 1x authentication.
<TIMESTAMP> INFO 10.10.10.2
   Client moved to associated state successfully.
<TIMESTAMP> ERROR 10.10.10.2
   802.1x authentication message received, static dynamic wep supported.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Client 802.1x authentication failure exceeded the limit.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key has possible incorrect psk configuration.
```
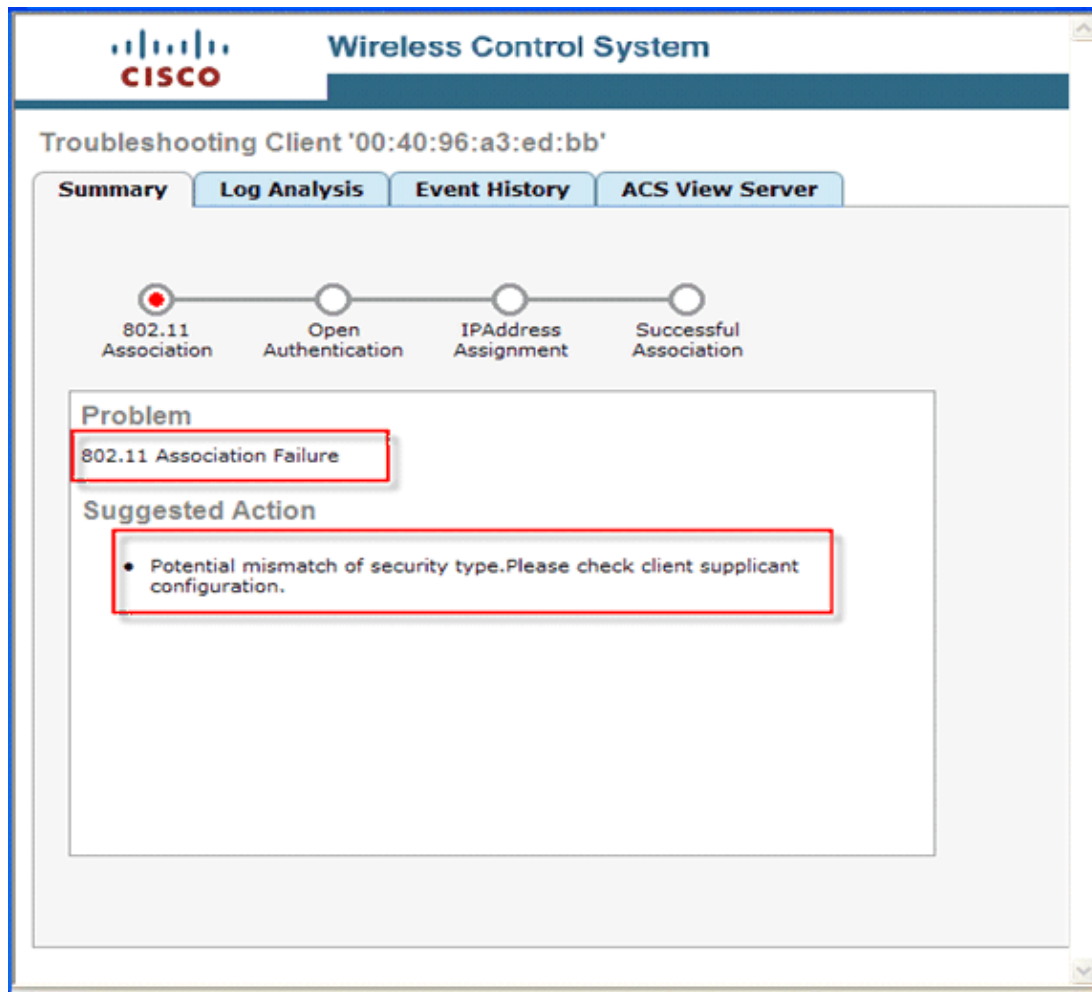
Troubleshooting 802.1X

As WLAN adoption becomes pervasive, legacy clients phase out; 802.1x is the direction for most future deployments. There can be a variety of misconfiguration–related issues in the chain (client <> AP <> WLC <> L2/L3 network <> AAA server). Here it is assumed that things are in place between the WLC and the AAA server. Issues that arise between the supplicant (client) and the AAA server generally are these:

- Wrong EAP type
- Wrong credentials/ expired certificates
- Wrong EAP inner method

On the client side, modify the credentials of the user under security settings; for example, enter the wrong password and rerun the same test. The troubleshooting tool exactly points out where the problem lies, as well as the suggested action.
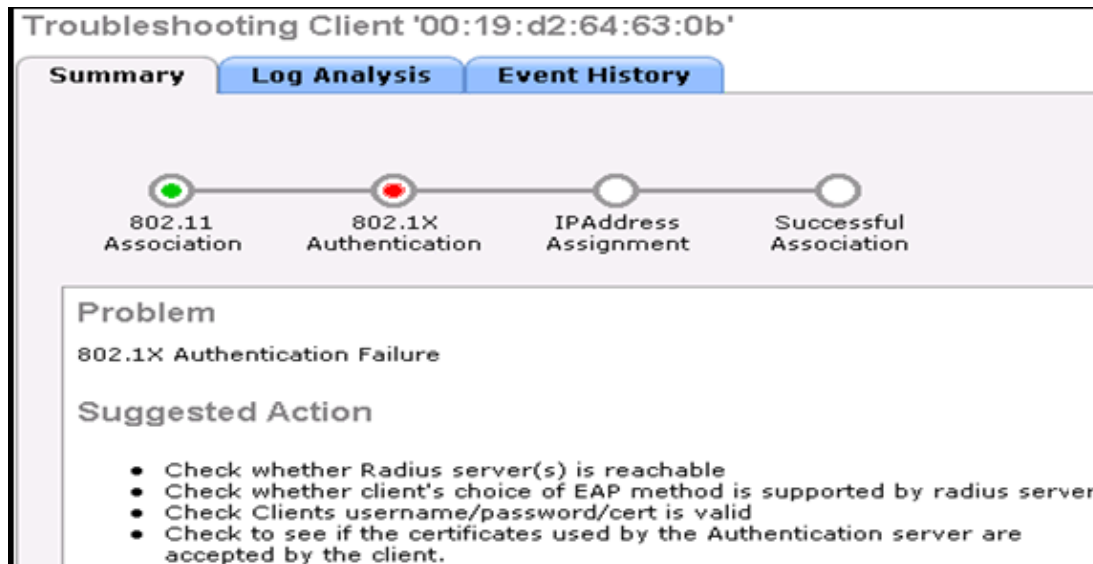
Click the **Log Analysis** tab in the figure shown above and check the logs for any indication of an unsuccessful 802.1x authentication.

```
<TIMESTAMP> INFO 10.10.10.2
   Received EAP Response from the client.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> INFO 10.10.10.2
   Received Access-Challenge from the RADIUS server for the client
<TIMESTAMP> INFO 10.10.10.2
   Sending EAP request to client from radius server.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> ERROR 10.10.10.2
   Received Access-Reject from the RADIUS server for the client.
<TIMESTAMP> ERROR 10.10.10.2
   Received eap failurefrom the client.
```

Troubleshooting Web–Auth

In general, good troubleshooting practice must include a checkup of the Policy Manager State of the client that has issues. As it is confirmed in the WCS screen shot below, the client in question is stuck at the *WEBAUTH_REQD* state. This means that the 802.11 process is complete without any errors, and these possible issues can occur:

- Incorrect username/password
- Incorrect ACL implementation (to reach external web–auth server, if any)
- DNS not configured properly and more

  Note: For more information on troubleshooting web authentication, refer to the document Controller Web Authentication Configuration Example.

The logs collected from WCS display that the web–auth process has not been successful. Such a situation can be simulated in the lab if you set the WLAN Layer 3 policy to web–auth and do not complete the web–auth process or enter incorrect/non–existent login credentials. Check the client troubleshooting tool summary section to know where the problem occurred. You see these logs on WCS:

```
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting does not require 802 1x authentication
<TIMESTAMP> INFO 10.10.10.2
   Client web authentication is required
<TIMESTAMP> INFO 10.10.10.2
   Client moved to associated state successfully
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received
```

Troubleshooting DHCP and IP Addressing

Often, the client devices are used in more than one wireless network. An example can be employee usage of a corporate device on a home or public network. An employee can have an assigned a static IP address in the home network. He/she connects to the corporate network with a previously assigned static IP address without his/her knowledge. This leads to a connectivity issue, which can be easily pointed out with the aid of the WCS Client Troubleshooting suite (as displayed below). The majority of the issues in this realm lies on the wireless client, but this can also point towards a potential problem on the wired infrastructure, such as an exhausted scope, incorrect scope, etc. Attempt to create this scenario when you assign an incorrect static IP address on the client or change the DHCP scope parameters on the switch.

Troubleshooting Client '00:19:d2:64:63:0b'

Summary | **Log Analysis** | **Event History**

802.11
Association | 802.1X
Authentication | IPAddress
Assignment | Successful
Association

Problem

Client could not complete the dhcp interaction.

Suggested Action

- Check whether the DHCP server is reachable.
- Check whether dhcp server is configured to serve the wlan.
- Check whether dhcp scope is exhausted.
- Check whether multiple dhcp servers are configured with overlapping scopes.
- Check local dhcp server is present if dhcp bridging mode enabled (move it to second) client is configured to get address from dhcp server
- Check if client has static ip configured and ensure client generates ip traffic * if ipsec wlan, ensure that client is configured to do dhcp exchanges in open (safenet/netscreen default config does not include it)

Related Information

- **Cisco Wireless LAN Controller Configuration Guide, Release 5.1**
- **Radio Resource Management under Unified Wireless Networks**
- **Troubleshooting and Routine Procedures**
- **Technical Support & Documentation – Cisco Systems**