PEAP Under Unified Wireless Networks with Microsoft Internet Authentication Service (IAS)

Contents

Introduction

This document provides a configuration example for setting up Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 2 authentication in a Cisco Unified Wireless network with the Microsoft Internet Authentication Service (IAS) as the RADIUS server.

Prerequisites

Requirements

There is an assumption that the reader has knowledge of basic Windows 2003 installation and Cisco controller installation since this document only covers the specific configurations to facilitate the tests.

Note: This document is intended to give the readers an example on the configuration required on MS server for PEAP – MS CHAP Authentication. The Microsoft server configuration presented in this section has been tested in the lab and found to be working as expected. If you have trouble configuring the Microsoft server, contact Microsoft for help. Cisco TAC does not support Microsoft Windows server configuration.

For initial installation and configuration information for the Cisco 4400 Series Controllers, refer to the Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers.

Microsoft Windows 2003 installation and configuration guides can be found at Installing Windows Server 2003 R2 .

Before you begin, install the Microsoft Windows Server 2003 with SP1 operating system on each of the servers in the test lab and update all Service Packs. Install the controllers and lightweight access points (LAPs) and ensure that the latest software updates are configured.

Components Used

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

- Cisco 4400 Series Controller that runs firmware Version 4.0
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise server (SP1) with Internet Authentication Service (IAS), Certificate Authority (CA), DHCP, and Domain Name System (DNS) services installed
- Windows XP Professional with SP 2 (and updated Service Packs) and Cisco Aironet 802.11a/b/g Wireless network interface card (NIC)
- Aironet Desktop Utility Version 4.0
- Cisco 3560 Switch

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.

Conventions

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

PEAP Overview

PEAP uses Transport Level Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a Wireless laptop, and a PEAP authenticator, such as Microsoft Internet Authentication Service (IAS) or any RADIUS server. PEAP does not specify an

authentication method, but provides additional security for other EAP authentication protocols, such as EAP-MSCHAPv2, that can operate through the TLS encrypted channel provided by PEAP. The PEAP authentication process consists of two main phases:

PEAP phase one: TLS encrypted channel

The Wireless client associates with the AP. An IEEE 802.11-based association provides an Open System or Shared Key authentication before a secure association is created between the client and Access Point (LAP). After the IEEE 802.11-based association is successfully established between the client and the Access Point, the TLS session is negotiated with the AP. After authentication is successfully completed between the Wireless client and IAS server, the TLS session is negotiated between them. The key that is derived within this negotiation is used to encrypt all subsequent communication.

PEAP phase two: EAP-authenticated communication

EAP communication, which includes EAP negotiation, occurs inside the TLS channel created by PEAP within the first stage of the PEAP authentication process. The IAS server authenticates the Wireless client with EAP-MS-CHAP v2. The LAP and the Controller only forward messages between the Wireless client and RADIUS server. The WLC and the LAP cannot decrypt these messages because it is not the TLS end point.

After PEAP stage one occurs, and the TLS channel is created between the IAS server and the 802.1X Wireless client, for a successful authentication attempt where the user has supplied valid password-based credentials with PEAP-MS-CHAP v2, the RADIUS message sequence is this:

1. The IAS server sends an identity request message to the client: EAP-Request/Identity.
2. The client responds with an identity response message: EAP-Response/Identity.
3. The IAS server sends an MS-CHAP v2 challenge message: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
4. The client responds with an MS-CHAP v2 challenge and response: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. The IAS server sends back an MS-CHAP v2 success packet when the server has successfully authenticated the client: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success).
6. The client responds with an MS-CHAP v2 success packet when the client has successfully authenticated the server: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success).
7. The IAS server sends an EAP-TLV that indicates successful authentication.
8. The client responds with an EAP-TLV status success message.
9. The server completes authentication and sends an EAP-Success message using plaintext. If VLANs are deployed for client isolation, the VLAN attributes are included in this message.

Configure

This document provides an example for the configuration of PEAP MS-CHAP v2.

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

Network Diagram

This document uses this network setup:

In this setup, a Microsoft Windows 2003 server performs these roles:

- Domain controller for the domain **Wireless.com**
- DHCP/DNS server
- Certificate Authority (CA) server
- Active Directory – to maintain the user database
- Internet Authentication Service (IAS) – to authenticate the Wireless users

This server connects to the wired network through a Layer 2 switch as shown.

The Wireless LAN Controller (WLC) and the registered LAP also connect to the network through the Layer 2 switch.

Wireless clients C1 and C2 will use Wi-Fi Protected Access 2 (WPA2) - PEAP MSCHAP v2 authentication to connect to the Wireless network.

The objective is to configure the Microsoft 2003 server, Wireless LAN Controller, and Light Weight AP to authenticate the Wireless clients with PEAP MSCHAP v2 authentication.

The next section explains how to configure the devices for this setup.

Configurations

This section looks at the configuration required to setup PEAP MS-CHAP v2 Authentication in this WLAN:

- Configure the Microsoft Windows 2003 Server
- Configure the Wireless LAN Controller (WLC) and the Light Weight APs
- Configure the Wireless Clients

Start with the configuration of the Microsoft Windows 2003 server.

Configure the Microsoft Windows 2003 Server

Configure the Microsoft Windows 2003 Server

As mentioned in the Network setup section, use the Microsoft Windows 2003 server in the network to perform these functions.

- **Domain controller** – for the domain **Wireless**
- **DHCP/DNS server**
- **Certificate Authority (CA) server**
- **Internet Authentication Service (IAS)** – to authenticate the Wireless users
- **Active Directory** – to maintain the user database

Configure the Microsoft Windows 2003 server for these services. Begin with the configuration of the Microsoft Windows 2003 server as a Domain Controller.

Configure the Microsoft Windows 2003 server as a Domain Controller

In order to configure the Microsoft Windows 2003 server as a Domain Controller, complete these steps:

1. Click **Start**, click **Run**, type **dcpromo.exe**, and then click **OK** to start the Active Directory Installation Wizard.
2. Click **Next** to run the Active Directory Installation Wizard.
3. In order to create a new domain, choose the option **Domain Controller** for a new domain.
4. Click **Next** to create a new forest of domain trees.
5. If DNS is not installed on the system, the wizard provides you options with which to configure DNS. Choose **No, Just Install and Configure DNS** on this computer. Click **Next**.
6. Type the full DNS name for the new domain. In this example **Wireless.com** is used and click **Next**.
7. Enter the NETBIOS name for the domain and click **Next**. This example uses **WIRELESS**.
8. Choose the database and log locations for the domain. Click **Next**.
9. Choose a location for the Sysvol folder. Click **Next**.
10. Choose the default permissions for the users and groups. Click **Next**.
11. Set the Administrator Password and click **Next**.
12. Click **Next** to accept the Domain Options set previously.
13. Click **Finish** to close the Active Directory Installation Wizard.
14. Restart the server for the changes to take effect.

With this step, you have configured the Microsoft Windows 2003 server as a Domain controller and created a new domain **Wireless.com**. Next configure DHCP services on the server.

Install and Configure DHCP Services on the Microsoft Windows 2003 Server

The DHCP service on the Microsoft 2003 server is used to provide IP addresses to the Wireless clients. In order to install and configure DHCP services on this server, complete these steps:

1. Click **Add or Remove Programs** in the Control Panel.
2. Click **Add/Remove Windows Components**.
3. Choose **Networking Services** and click **Details**.
4. Choose **Dynamic Host Configuration Protocol (DHCP)** and click **OK**.
5. Click **Next** to install the DHCP service.
6. Click **Finish** to complete the installation.
7. In order to configure DHCP services, click **Start > Programs > Administrative tools** and click the **DHCP** snap-in.
8. Choose the DHCP server - **tsweb-lapt.wireless.com** (in this example).
9. Click **Action** and then click **Authorize** to authorize DHCP service.
10. In the Console tree, right-click **tsweb-lapt.wireless.com** and then click **New Scope** to define an IP address range for the Wireless clients.
11. On the Welcome to the New Scope Wizard page of the New Scope Wizard, click **Next**.
12. On the Scope Name page, type the name of the DHCP scope. In this example, use **DHCP-Clients** as the scope name. Click **Next**.
13. On the IP Address Range page, enter the start and end IP addresses for the scope, and click **Next**.
14. On the Add Exclusions page, mention the IP address that you would like to reserve/exclude from the DHCP scope. Click **Next**.
15. Mention the lease duration in the Lease Duration page, and click **Next**.

16. On the Configure DHCP options page, choose **Yes, I want to configure DHCP Option now**, and click **Next**.
17. If there is default gateway router, mention the IP address of the gateway router in the Router (Default Gateway) page, and click **Next**.
18. On the Domain Name and DNS servers page, type the name of the domain that was configured previously. In the example, use **Wireless.com**. Enter the IP address of the server. Click **Add**.
19. Click **Next**.
20. On the WINS Server page, click **Next**.
21. On the Activate Scope page, choose **Yes, I want to activate the scope now**, and click **Next**.
22. On completing the New Scope Wizard, click **Finish**.
23. In the DHCP Snapin window, verify that the DHCP scope that was created is active.

Now that the DHCP/ DNS is enabled on the server, configure the server as an enterprise Certificate Authority (CA) server.

Install and Configure the Microsoft Windows 2003 Server as a Certificate Authority (CA) Server

PEAP with EAP-MS-CHAPv2 validates the RADIUS server based on the certificate present on the server. Additionally, the server certificate must be issued by a public certification authority (CA) that is trusted by the client computer (that is, the public CA certificate already exists in the Trusted Root Certification Authority folder on the client computer certificate store). In this example, configure the Microsoft Windows 2003 server as a Certificate Authority (CA) that issues the certificate to the Internet Authentication Service (IAS).

In order to install and configure the certificate services on the server, complete these steps:

1. Click **Add or Remove programs in Control Panel**.
2. Click **Add/Remove Windows components**.
3. Click **Certificate Services**.
4. Click **Yes** to the warning message, **After Installing Certificate Services, the computer cannot be renamed and the computer cannot join or be removed from a domain. Do you want to continue?**
5. Under Certificate Authority Type, choose **Enterprise root CA**, and click **Next**.
6. Enter a name to identify the CA. This example uses **Wireless-CA**. Click **Next**.
7. A “Cert Log” directory is created for certificate database storage. Click **Next**.
8. If IIS is enabled, it must be stopped before you proceed. Click **OK** to the warning message that IIS must be stopped. It restarts automatically after CA is installed.
9. Click **Finish** to complete the installation of Certificate Authority (CA) services.

The next step is to install and configure the Internet Authentication Service on the Microsoft Windows 2003 server.

Connect Clients to the Domain

The next step is to connect the clients to the wired network and download the domain specific information from the new domain. In other words, connect the clients to the domain. In order to do this, complete these steps:

1. Connect the clients to the wired network with a straight through Ethernet cable.
2. Boot up the client and login with the username/ password of the client.
3. Click **Start**; click **Run**; type **cmd**; and click **OK**.
4. At the command prompt, type **ipconfig**, and click **Enter** to verify that DHCP works correctly and the client received an IP address from the DHCP server.
5. In order to join the client to the domain, right click **My Computer**, and choose **Properties**.
6. Click the **Computer Name** tab.
7. Click **Change**.
8. Click **Domain**; type **wireless.com**; and click **OK**.
9. Type **Username Administrator** and the password specific to the domain to which the client joins. (This is the administrator account in the Active Directory on the server.)
10. Click **OK**.
11. Click **Yes** to restart the computer.
12. Once the computer restarts, login with this information: Username = **Administrator**; Password = <**domain password**>; Domain = **Wireless**.
13. Right click **My Computer**, and click **Properties**.
14. Click the **Computer Name** tab to verify that you are on the Wireless.com domain.
15. The next step is to verify that the client received the CA certificate (trust) from the server.
16. Click **Start**; click **Run**; type **mmc**, and click **OK**.
17. Click **File**, and click **Add/Remove** snap-in.
18. Click **Add**.
19. Choose **Certificate**, and click **Add**.
20. Choose **Computer Account**, and click **Next**.
21. Click **Finish** to accept the default local computer.
22. Click **Close**, and click **OK**.
23. Expand **Certificates (Local Computer)**; expand **Trusted Root Certification Authorities**; and click **Certificates**. Find **Wireless** in the list.
24. Repeat this procedure to add more clients to the domain.

Install the Internet Authentication Service on the Microsoft Windows 2003 Server and Request a Certificate

In this setup, the Internet Authentication Service (IAS) is used as a RADIUS server to authenticate Wireless clients with PEAP authentication.

Complete these steps to install and configure IAS on the server.

1. Click **Add or Remove Programs** in the Control Panel.
2. Click **Add/Remove Windows Components**.
3. Choose **Networking Services**, and click **Details**.
4. Choose **Internet Authentication Service**; click **OK**; and click **Next**.
5. Click **Finish** to complete the IAS installation.
6. The next step is to install the computer certificate for the Internet Authentication Service (IAS).
7. Click **Start**; click **Run**; type **mmc**; and click **OK**.
8. Click **Console** in the file menu, and then choose **Add/Remove** snap-in.
9. Click **Add** to add a snap-in.
10. Choose **Certificates** from the list of snap-ins, and click **Add**.

11. Choose **Computer account**, and click **Next**.
12. Choose **Local computer**, and click **Finish**.
13. Click **Close**, and click **OK**.
14. Expand **Certificates (Local Computer)**; right click **Personal folder**; choose **All tasks** and then **Request New Certificate**.
15. Click **Next** on the ***Welcome to the Certificate Request Wizard*** .
16. Choose the **Domain Controller** certificate template (if you request a computer certificate on a server other than the DC, choose a **Computer** certificate template), and click **Next**.
17. Type a name and description for the certificate.
18. Click **Finish** to complete the certification request wizard.

Configure the Internet Authentication Service for PEAP-MS-CHAP v2 Authentication

Now that you have installed and requested a certificate for the IAS, configure the IAS for authentication.

Complete these steps:

1. Click **Start > Programs > Administrative Tools**, and click **Internet Authentication Service** snap-in.
2. Right-click **Internet Authentication Service (IAS)**, and then click **Register Service in Active Directory**.
3. The **Register Internet Authentication Service in Active Directory** dialog box appears; click **OK**. This enables IAS to authenticate users in the Active Directory.
4. Click **OK** in the next dialog box.
5. Add the Wireless LAN Controller as an AAA client on the MS IAS server.
6. Right-click **RADIUS Clients**, and choose **New RADIUS Client**.
7. Type the name of the client (WLC in this case), and enter the IP address of the WLC. Click **Next**.
8. On the next page, under Client-Vendor, choose **RADIUS Standard**; enter the shared secret; and click **Finish**.
9. Notice that the WLC is added as an AAA client on the IAS.
10. Create a remote access policy for the clients.
11. In order to do this, right-click **Remote Access Policies**, and choose **New Remote Access Policy**.
12. Type a name for the remote access policy. In this example, use the name **PEAP**. Then click **Next**.
13. Choose the policy attributes based on your requirements. In this example, choose **Wireless**.
14. On the next page, choose **User** to apply this remote access policy to list of users.
15. Under Authentication Methods, choose **Protected EAP (PEAP)**, and click **Configure**.
16. On the **Protected EAP Properties** page, choose the appropriate certificate from the Certificate Issued drop-down menu, and click **OK**.
17. Verify the details of the remote access policy, and click **Finish**.
18. The remote access policy has been added to the list.
19. Right-click the policy, and click **Properties**. Choose “**Grant remote access permission**” under “**If a connection request matches the specified conditions**.”

Add Users to the Active Directory

In this setup, the User database is maintained on the Active Directory.

In order to add users to the Active directory database, complete these steps:

1. In the Active Directory Users and Computers console tree, right-click **Users**; click **New**; and then click **User**.
2. In the New Object – User dialog box, type the name of the Wireless user. This example uses the name **WirelessUser** in the First name field and **WirelessUser** in the User logon name field. Click **Next**.
3. In the New Object – User dialog box, type a password of your choice in the Password and Confirm password fields. Clear the **User must change password at next logon** check box, and click **Next**.
4. In the New Object – User dialog box, click **Finish**.
5. Repeat steps 2 through 4 in order to create additional user accounts.

Allow Wireless Access to Users

Complete these steps:

1. In the **Active Directory Users and Computers** console tree, click the **Users** folder; right-click **WirelessUser**; click **Properties**; and then go to the **Dial-in** tab.
2. Choose **Allow access**, and click **OK**.

Configure the Wireless LAN Controller and Lightweight APs

Now configure the Wireless devices for this setup. This includes the configuration of the Wireless LAN Controllers, Lightweight APs, and Wireless clients.

Configure the WLC for RADIUS Authentication through MS IAS RADIUS Server

First configure the WLC to use the MS IAS as the authentication server. The WLC needs to be configured in order to forward the user credentials to an external RADIUS server. The external RADIUS server then validates the user credentials and provides access to the Wireless clients. In order to do this, add the MS IAS server as a RADIUS server in the **Security > RADIUS Authentication** page.

Complete these steps:

1. Choose **Security** and **RADIUS Authentication** from the controller GUI to display the RADIUS Authentication Servers page. Then click **New** in order to define a RADIUS server.
2. Define the RADIUS server parameters in the **RADIUS Authentication Servers > New** page. These parameters include the RADIUS Server IP Address, Shared Secret, Port Number, and Server Status. The Network User and Management check boxes determine if the RADIUS-based authentication applies for management and network users. This example uses the MS IAS as the RADIUS server with IP address 10.77.244.198.

3. Click **Apply**.
4. MS IAS server has been added to the WLC as a Radius server and can be used to authenticate Wireless Clients.

Configure a WLAN for the Clients

Configure the SSID (WLAN) to which the Wireless clients connects. In this example, create the SSID, and name it **PEAP**.

Define the Layer 2 Authentication as WPA2 so that the clients perform EAP based authentication (PEAP-MSCHAPv2 in this case) and use AES as the encryption mechanism. Leave all other values at their defaults.

Note: This document binds the WLAN with the management interfaces. When you have multiple VLANs in your network, you can create a separate VLAN and bind it to the SSID. For information on how to configure VLANs on WLCs, refer to VLANs on Wireless LAN Controllers Configuration Example.

In order to configure a WLAN on the WLC complete these steps:

1. Click **WLANs** from the GUI of the controller in order to display the WLANs page. This page lists the WLANs that exist on the controller.
2. Choose **New** in order to create a new WLAN. Enter the WLAN ID and the WLAN SSID for the WLAN, and click **Apply**.
3. Once you create a new WLAN, the **WLAN > Edit** page for the new WLAN appears. On this page you can define various parameters specific to this WLAN that include General Policies, RADIUS Servers, Security Policies, and 802.1x Parameters.
4. Check **Admin Status** under General Policies in order to enable the WLAN. If you want the AP to broadcast the SSID in its beacon frames, check **Broadcast SSID**.
5. Under Layer 2 Security, choose **WPA1+WPA2**. This enables WPA on the WLAN. Scroll down the page and choose the WPA policy. This example uses WPA2 and AES encryption. Choose the appropriate RADIUS server from the pull-down menu under RADIUS Servers. In this example, use **10.77.244.198** (IP address of the MS IAS server). The other parameters can be modified based on the requirement of the WLAN network.
6. Click **Apply**.

Configure the Wireless Clients

Configure the Wireless Clients for PEAP-MS CHAPv2 Authentication

This example provides information on how to configure the Wireless client with Cisco Aironet Desktop Utility. Before you configure the client adapter, ensure that that latest version of the firmware and utility are used. Find the latest version of the firmware and utilities in the Wireless downloads page on Cisco.com.

In order to configure the Cisco Aironet 802.11 a/b/g Wireless client adapter with the ADU, complete these steps:

1. Open the Aironet Desktop Utility.

2. Click **Profile Management**, and click **New** to define a profile.
3. Under the General tab, enter the Profile name and SSID. In this example, use the SSID that you configured on the WLC (PEAP).
4. Choose the Security tab; choose **WPA/WPA2/CCKM**; under WPA/WPA2/CCKM EAP, type choose **PEAP [EAP-MSCHAPv2]**, and click **Configure**.
5. Choose **Validate Server Certificate**, and choose **Wireless-CA** under the Trusted Root Certificate Authorities drop-down menu.
6. Click **OK**, and activate the profile.**Note:** When you use Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2 (PEAP-MSCHAPv2) with Microsoft XP SP2, and the Wireless card is managed by the Microsoft Wireless Zero Configuration (WZC), you must apply the Microsoft hotfix KB885453. This prevents several issues on authentication related to PEAP Fast Resume.

Verify and Troubleshoot

In order to verify if the configuration works as expected, activate the profile PEAP-MSCHAPv2 on the Wireless client Client1.

Once the profile PEAP-MSCHAPv2 is activated on the ADU, the client performs 802.11 open authentication and then performs PEAP-MSCHAPv2 authentication. Here is an example of successful PEAP-MSCHAPv2 authentication.

Use the debug commands to understand the sequence of events that occur.

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

These debug commands on the Wireless LAN Controller are useful.

- **debug dot1x events enable** —In order to configure the debugging of 802.1x events
- **debug aaa events enable** —In order to configure the debugging of AAA events
- **debug mac addr <mac address>** —In order to configure MAC debugging, use the debug mac command
- **debug dhcp message enable** —In order to configure debug of DHCP error messages

These are the example outputs from the **debug dot1x events enable** command and **debug client <mac address>** command.

debug dot1x events enable:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
   mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 3)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)
```

```
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 4)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 5)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 6)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 7)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 8)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 9)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 10)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 11)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 12)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from
   mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Accept for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Creating a new PMK Cache
   Entry for station 00:40:96:ac:e6:57 (RSN 0)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP-Success to
   mobile 00:40:96:ac:e6:57 (EAP Id 13)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending default RC4 key to
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending Key-Mapping RC4 key to
   mobile 00:40:96:ac:e6:57
```

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57**

debug mac addr <MAC Address>:

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 - rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20) Change state to START (0)**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Initializing policy**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Change state to AUTHCHECK (2)**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2) Change state to 8021X_REQD (3)**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)** Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from mobile 00:40:96:ac:e6:57**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Authenticating state**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

```
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Accept for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending default RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   8021X_REQD (3) Change state to L2AUTHCOMPLETE (4)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Change state to RUN (20)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Reached PLUMBFASTPATH: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Replacing Fast Path rule
  type = Airespace AP Client
  on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
  Card = 0 (slot 0), InHandle = 0x00000000,
```

```
   OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
   Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
   while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
   moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

Note: If you use the Microsoft Supplicant to authenticate with a Cisco Secure ACS for PEAP authentication, the client potentially does not authenticate successfully. Sometimes the initial connection can authenticate successfully, but subsequent fast-connect authentication attempts do not connect successfully. This is a known issue. The details of this issue and the fix for the same are available here .

Related Information

- **PEAP under Unified Wireless Networks with ACS 4.0 and Windows 2003**
- **EAP Authentication with WLAN Controllers (WLC) Configuration Example**
- **Wireless LAN Controller (WLC) Software Upgrade to Versions 3.2, 4.0, and 4.1**
- **Cisco 4400 Series Wireless LAN Controllers Configuration Guides**
- **Technical Support & Documentation - Cisco Systems**