PEAP bajo Redes Inalámbricas Unificadas con Microsoft Internet Authentication Service (IAS)

Contenido

Introducción

Este documento proporciona un ejemplo de configuración para configurar Protected Extensible Authentication Protocol (PEAP) mediante la autenticación MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) versión 2 en una red Cisco Unified Wireless con el Servicio de autenticación de Internet de Microsoft (IAS) como servidor RADIUS.

prerrequisitos

Requisitos

Hay una suposición que el lector tiene la instalación de Windows 2003 del conocimietno básico y instalación del controlador de Cisco puesto que este documento cubre solamente las configuraciones específicas para facilitar las pruebas.

Nota: Este documento se piensa para dar a los lectores un ejemplo en la configuración requerida en el servidor MS para el PEAP – autenticación CHAP MS. La configuración de servidor de Microsoft presentada en esta sección se ha probado en el laboratorio y se ha encontrado para trabajar como se esperaba. Si usted tiene problema que configura al servidor de Microsoft, entre en contacto Microsoft para la ayuda. El TAC de Cisco no soporta la configuración del Microsoft Windows server.

Para la instalación inicial y la información de la configuración para los reguladores de las Cisco 4400 Series, refiera a la guía de inicio rápido: Cisco Wireless LAN Controllers de la serie 4400.

Microsoft Windows 2003 guías de instalación y configuración se puede encontrar en instalar el r2 2003 del Servidor Windows .

Antes de que usted comience, instale el Microsoft Windows server 2003 con el sistema operativo SP1 en cada uno de los servidores en el laboratorio de prueba y ponga al día todo el Service Packs. Instale los reguladores y los Puntos de acceso ligeros (revestimientos) y asegúrese de que las actualizaciones de último software están configuradas.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Regulador de las Cisco 4400 Series que funciona con la versión de firmware 4.0
- Cisco protocolo de 1131 Lightweight Access Point (LWAPP) AP
- Servidor de Enterprise de Windows 2003 (SP1) con el Internet Authentication Service (IAS), el Certificate Authority (CA), el DHCP, y los servicios del Domain Name System (DNS) instalados
- Profesional de Windows XP con el SP2 (y el Service Packs actualizado) y el Wireless Network Interface Card del Cisco Aironet 802.11a/b/g (NIC)
- Utilidad Aironet Desktop versión 4.0
- Cisco 3560 Switch

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Descripción PEAP

Seguridad del nivel del transporte de las aplicaciones PEAP (TLS) para crear un canal cifrado entre un cliente PEAP de autenticidad, tal como una laptop inalámbrica, y un authenticator PEAP, tal como Internet Authentication Service de Microsoft (IAS) o cualquier servidor de RADIUS. El PEAP no especifica un método de autentificación, sino proporciona la seguridad complementaria para otros protocolos de autenticación EAP, tales como EAP MSCHAPv2, que puede actuar a través del canal cifrado TLS proporcionado por el PEAP. El proceso de autenticación PEAP consiste en dos fases principales:

Fase uno PEAP: TLS cifró el canal

Los socios del cliente de red inalámbrica con el AP. Una asociación de IEEE 802.11-based proporciona un sistema operativo o la clave de autenticación compartida antes de una asociación segura se crea entre el cliente y el Punto de acceso (REVESTIMIENTO). Después de que la asociación de IEEE 802.11-based se establezca con éxito entre el cliente y el Punto de acceso, la sesión de TLS se negocia con el AP. Después de que la autenticación se complete con éxito entre el cliente de red inalámbrica y el servidor IAS, la sesión de TLS se negocia entre ellos. La clave que se deriva dentro de esta negociación se utiliza para cifrar toda la comunicación subsiguiente.

Fase dos PEAP: comunicación EAP-autenticada

La comunicación EAP, que incluye la negociación EAP, ocurre dentro del canal de TLS creado por el PEAP dentro de la primera fase del proceso de autenticación PEAP. El servidor IAS autentica al cliente de red inalámbrica con el v2 EAP-MS-CHAP. El REVESTIMIENTO y los mensajes delanteros del regulador solamente entre el cliente de red inalámbrica y el servidor de RADIUS. El WLC y el REVESTIMIENTO no pueden desencriptar estos mensajes porque no es el punto extremo de TLS.

Después de que ocurra la etapa una PEAP, y el canal de TLS se crea entre el servidor IAS y el cliente de red inalámbrica del 802.1x, porque una tentativa de la autenticación satisfactoria donde el usuario ha suministrado las credenciales basadas en la contraseña válidas el v2 PEAP-MS-CHAP, la secuencia del mensaje de RADIUS es ésta:

1. El servidor IAS envía un mensaje request de la identidad al cliente: EAP-petición/identidad.
2. El cliente responde con un mensaje de respuesta de la identidad: EAP-respuesta/identidad.
3. El servidor IAS envía un mensaje de impugnación del v2 MS-CHAP: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (desafío).
4. El cliente responde con un desafío y una respuesta del v2 MS-CHAP: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (respuesta).
5. El servidor IAS devuelve un paquete del éxito del v2 MS-CHAP cuando el servidor ha autenticado con éxito al cliente: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (éxito).
6. El cliente responde con un paquete del éxito del v2 MS-CHAP cuando el cliente ha autenticado con éxito el servidor: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (éxito).
7. El servidor IAS envía un EAP-TLV que indique la autenticación satisfactoria.
8. El cliente responde con un Mensaje de éxito del estatus EAP-TLV.
9. El servidor completa la autenticación y envía un mensaje del EAP-éxito usando el texto simple. Si los VLA N se despliegan para el aislamiento del cliente, los atributos del VLA N se incluyen en este mensaje.

Configurar

Este documento proporciona un ejemplo para la configuración del v2 PEAP MS-CHAP.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

En esta configuración, un servidor de Microsoft Windows 2003 realiza estos papeles:

- Controlador de dominio para el dominio **Wireless.com**
- Servidor DHCP/DNS
- Servidor del Certificate Authority (CA)
- Active Directory – mantener la base de datos de usuarios
- Internet Authentication Service (IAS) – autenticar a los usuarios de red inalámbrica

Este servidor conecta con la red alámbrica a través de un 2 Switch de la capa como se muestra.

El regulador del Wireless LAN (WLC) y el REVESTIMIENTO registrado también conectan con la red a través del 2 Switch de la capa.

El c1 de los clientes de red inalámbrica y el C2 utilizarán el acceso protegido Wi-Fi 2 (WPA2) - autenticación del v2 PEAP MSCHAP para conectar con la red inalámbrica.

El objetivo es configurar el servidor de Microsoft 2003, el regulador del Wireless LAN, y el AP ligero para autenticar a los clientes de red inalámbrica con la autenticación del v2 PEAP MSCHAP.

La siguiente sección explica cómo configurar los dispositivos para esta configuración.

Configuraciones

Esta sección mira la configuración requerida poner la autenticación del v2 PEAP MS-CHAP en esta red inalámbrica (WLAN):

- Configure el servidor de Microsoft Windows 2003
- Configure el regulador del Wireless LAN (WLC) y los AP ligeros
- Configure a los clientes de red inalámbrica

Comience con la configuración del servidor de Microsoft Windows 2003.

Configure el servidor de Microsoft Windows 2003

Configure el servidor de Microsoft Windows 2003

Como se menciona en la sección de la configuración de la red, utilice el servidor de Microsoft Windows 2003 en la red para realizar estas funciones.

- **Controlador de dominio** – para la **Tecnología inalámbrica del** dominio
- **Servidor DHCP/DNS**

- **Servidor del Certificate Authority (CA)**
- **Internet Authentication Service (IAS)** – autenticar a los usuarios de red inalámbrica
- **Active Directory** – mantener la base de datos de usuarios

Configure el servidor de Microsoft Windows 2003 para estos servicios. Comience con la configuración del servidor de Microsoft Windows 2003 como controlador de dominio.

Configure el servidor de Microsoft Windows 2003 como controlador de dominio

Para configurar el servidor de Microsoft Windows 2003 como controlador de dominio, complete estos pasos:

1. Haga clic el **comienzo**, haga clic el **funcionamiento**, teclee **dcpromo.exe, y** después haga clic el comienzo OKTO el Asisitente de instalación de Active Directory.
2. Haga clic **al lado de** funcionan con al Asisitente de instalación de Active Directory.
3. Para crear un nuevo dominio, elija el **controlador de dominio de la** opción para un nuevo dominio.
4. El tecleo **al lado de** crea un nuevo bosque de los árboles de dominio.
5. Si el DNS no está instalado en el sistema, el Asisitente le proporciona las opciones con las cuales configurar el DNS. Elija **ningún, apenas instale y configure el DNS** en este ordenador. Haga clic en Next (Siguiente).
6. Teclee el nombre DNS completo para el nuevo dominio. En este ejemplo **Wireless.com** se utiliza y tecleo **después**.
7. Ingrese el nombre de NETBIOS para el dominio y haga clic **después**. Este ejemplo utiliza la **TECNOLOGÍA INALÁMBRICA**.
8. Elija las ubicaciones de la base de datos y del registro para el dominio. Haga clic en Next (Siguiente).
9. Elija una ubicación para la carpeta de Sysvol. Haga clic en Next (Siguiente).
10. Elija los permisos predeterminados para los usuarios y los grupos. Haga clic en Next (Siguiente).
11. Fije la contraseña del administrador y el tecleo **después**.
12. El tecleo **al lado de** valida las opciones de dominio fijadas previamente.
13. Clic en Finalizar para cerrar al Asisitente de instalación de Active Directory.
14. Recomience el servidor para que los cambios tomen el efecto.

Con este paso, usted ha configurado el servidor de Microsoft Windows 2003 como controlador de dominio y ha creado un nuevo dominio **Wireless.com**. Servicios siguientes del DHCP de la configuración en el servidor.

Instale y configure los servicios del DHCP en el servidor de Microsoft Windows 2003

El servicio del DHCP en el servidor de Microsoft 2003 se utiliza para proporcionar los IP Addresses a los clientes de red inalámbrica. Para instalar y configurar los servicios del DHCP en este servidor, complete estos pasos:

1. El tecleo **agrega o quita los programas** en el panel de control.
2. El tecleo **agrega/quita a los componentes de Windows**.
3. Elija los **servicios de red** y haga clic los **detalles**.
4. Elija el **Protocolo de configuración dinámica de host (DHCP)** y haga clic la **AUTORIZACIÓN**.
5. El tecleo **al lado de** instala el servicio del DHCP.

6. Haga clic en **Finish** para completar la instalación.
7. Para configurar los servicios del DHCP, haga clic el **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas)** y haga clic el **DHCP broche-**en.
8. Elija al servidor DHCP - **tsweb-lapt.wireless.com** (en este ejemplo).
9. Haga clic la **acción** y después haga clic **autorizan** para autorizar el servicio del DHCP.
10. En el árbol de la consola, haga clic con el botón derecho del ratón **tsweb-lapt.wireless.com** y después haga clic el **nuevo alcance** para definir un alcance del IP Address para los clientes de red inalámbrica.
11. En la recepción a la nueva página del asistente de alcance del nuevo asistente de alcance, haga clic **después**.
12. En la página del nombre del alcance, teclee el nombre del alcance de DHCP. En este ejemplo, utilice a los **clientes DHCP** como el nombre del alcance. Haga clic en Next (Siguiente).
13. En la página del alcance del IP Address, ingrese el comienzo y los IP Addresses del final para el alcance, y haga clic **después**.
14. En el agregar las exclusiones paginan, mencionan que la dirección IP que usted quisiera reservar/excluya del alcance de DHCP. Haga clic en Next (Siguiente).
15. Mencione el tiempo de validez en la página del tiempo de validez, y haga clic **después**.
16. En la configuración las opciones DHCP paginan, eligen **sí, quiero ahora configurar la opción DHCP**, y hago clic **después**.
17. Si hay router del default gateway, mencione la dirección IP del router de gateway en la página del router (default gateway), y haga clic **después**.
18. En el Domain Name y los servidores DNS pagine, teclee el nombre del dominio que fue configurado previamente. En el ejemplo, utilice **Wireless.com**. Ingrese el IP Address del servidor. Haga clic en Add (Agregar).
19. Haga clic en Next (Siguiente).
20. En la página del servidor de los TRIUNFOS, haga clic **después**.
21. En la página del alcance del activar, elija **sí, quiero ahora activar el alcance**, y hago clic **después**.
22. Al completar al nuevo asistente de alcance, clic en Finalizar.
23. En la ventana Snapin del DHCP, verifique que el alcance de DHCP que fue creado sea activo.

Ahora que el DHCP DNS se habilita en el servidor, configure el servidor como servidor del Certificate Authority (CA) de la empresa.

Instale y configure el servidor de Microsoft Windows 2003 como servidor del Certificate Authority (CA)

El PEAP con EAP-MS-CHAPv2 valida al servidor de RADIUS basado en el certificado presente en el servidor. Además, el certificado de servidor se debe publicar por un Certification Authority (CA) público que es confiado en por la computadora cliente (es decir, el certificado de CA público existe ya en la carpeta del Trusted Root Certification Authority en el almacén de certificados de la computadora cliente). En este ejemplo, configure el servidor de Microsoft Windows 2003 como Certificate Authority (CA) que publica el certificado al Internet Authentication Service (IAS).

Para instalar y configurar los servicios de certificados en el servidor, complete estos pasos:

1. El tecleo **agrega o quita los programas en el panel de control**.

2. El tecleo **agrega/quita a los componentes de Windows**.
3. **Servicios de certificados del** tecleo.
4. El tecleo **sí al** mensaje de advertencia, **después de instalar los servicios de certificados, el ordenador no puede ser retitulado y el ordenador no se puede unir a o quitar de un dominio. ¿Usted quiere continuar?**
5. Conforme al tipo del Certificate Authority, elija la **empresa raíz CA**, y haga clic **después**.
6. Ingrese un nombre para identificar el CA. Este ejemplo utiliza Tecnología inalámbrica-**CA**. Haga clic en Next (Siguiente).
7. "Un directorio del registro CERT" se crea para el almacenamiento de la base de datos del certificado. Haga clic en Next (Siguiente).
8. Si se habilita el IIS, debe ser parado antes de que usted proceda. Haga Click en OK al mensaje de advertencia que el IIS debe ser parado. Recomienza automáticamente después de que CA esté instalado.
9. Clic en Finalizar para completar la instalación de los servicios del Certificate Authority (CA).

El siguiente paso es instalar y configurar el Internet Authentication Service en el servidor de Microsoft Windows 2003.

Conecte a los clientes con el dominio

El siguiente paso es conectar a los clientes con la red alámbrica y descargar la información específica del dominio del nuevo dominio. Es decir conecte a los clientes con el dominio. A tal efecto, complete estos pasos:

1. Conecte a los clientes con la red alámbrica con un cable Ethernet directo recto.
2. Inicie encima del cliente y inicie sesión con la contraseña username del cliente.
3. Haga clic el **comienzo**; haga clic el **funcionamiento**; teclee el **cmd**; y **AUTORIZACIÓN del** tecleo.
4. En el comando prompt, el **ipconfig del** tipo, y el tecleo **ingresan** para verificar que el DHCP trabaja correctamente y el cliente recibió un IP Address del servidor DHCP.
5. Para unirse a al cliente al dominio, haga clic con el botón derecho del ratón el **mi PC**, y elija las **propiedades**.
6. Haga clic la lengueta del **nombre de computadora**.
7. Haga clic el **cambio**.
8. Haga clic el **dominio**; teclee **wireless.com**; y **AUTORIZACIÓN del** tecleo.
9. **Administrador del nombre de usuario del** tipo y el específico de la contraseña al dominio al cual el cliente se une a. (Ésta es la cuenta del administrador en el Active Directory en el servidor.)
10. Haga clic en OK.
11. Tecleo **sí** para recomenzar el ordenador.
12. Una vez que el ordenador recomienza, inicie sesión con esta información: Nombre de usuario = **administrador**; **Password> de la** contraseña = del <domain; Dominio = **Tecnología inalámbrica**.
13. **Mi PC del** click derecho, y **propiedades del** tecleo.
14. Haga clic la lengueta del **nombre de computadora** para verificar que usted está en el dominio de Wireless.com.
15. El siguiente paso es verificar que el cliente recibió el certificado de CA (confianza) del servidor.
16. **Comienzo del** tecleo; **funcionamiento del** tecleo; tipo **mmc**, y **AUTORIZACIÓN del** tecleo.

17. El clic en Archivo, y el tecleo **agregan/quitan broche-**en.
18. Haga clic en Add (Agregar).
19. Elija el **certificado**, y el haga click en Add
20. Elija la **cuenta de la Computadora**, y haga clic **después**.
21. Clic en Finalizar para validar la computadora local predeterminada.
22. **Cierre del** tecleo, y **AUTORIZACIÓN del** tecleo.
23. Amplíe los **Certificados (computadora local)**; amplíe los **Trusted Root Certification Authority**; y **Certificados del** tecleo. **Tecnología inalámbrica del** hallazgo en la lista.
24. Relance este procedimiento para agregar a más clientes al dominio.

Instale el Internet Authentication Service en el servidor de Microsoft Windows 2003 y pida un certificado

En esta configuración, el Internet Authentication Service (IAS) se utiliza como servidor de RADIUS para autenticar a los clientes de red inalámbrica con la autenticación PEAP.

Complete estos pasos para instalar y para configurar IAS en el servidor.

1. El tecleo **agrega o quita los programas** en el panel de control.
2. El tecleo **agrega/quita a los componentes de Windows**.
3. Elija los **servicios de red**, y haga clic los **detalles**.
4. Elija el **Internet Authentication Service**; haga clic la **AUTORIZACIÓN**; y tecleo **después**.
5. Clic en Finalizar para completar la instalación de IAS.
6. El siguiente paso es instalar el certificado del ordenador para el Internet Authentication Service (IAS).
7. **Comienzo del** tecleo; **funcionamiento del** tecleo; tipo **mmc**; y **AUTORIZACIÓN del** tecleo.
8. Haga clic la **consola** en el menú de archivos, y después elija **agregan/quitan broche-**en.
9. El tecleo **agrega** para agregar a broche-en.
10. Elija los **Certificados de la** lista de broche-INS, y el haga click en Add
11. Elija la **cuenta de la Computadora**, y haga clic **después**.
12. Elija la **computadora local**, y el clic en Finalizar.
13. Haga clic **cerca**, y haga clic la **AUTORIZACIÓN**.
14. Amplíe los **Certificados (computadora local)**; haga clic con el botón derecho del ratón la **carpeta personal**; elija **todas las tareas** y después **pida el nuevo certificado**.
15. Haga clic **después** en la *recepción al Asisitente del pedido de certificado*.
16. Elija el Certificate Template plantilla de certificado del **controlador de dominio** (si usted pide un certificado del ordenador en un servidor con excepción de DC, elija un Certificate Template plantilla de certificado de la **Computadora**), y haga clic **después**.
17. Teclee un nombre y una descripción para el certificado.
18. Clic en Finalizar para completar al Asisitente de la petición de la certificación.

Configure el Internet Authentication Service para la autenticación del v2 PEAP-MS-CHAP

Ahora que usted ha instalado y ha pedido un certificado para IAS, configure IAS para la autenticación.

Complete estos pasos:

1. Haga clic el **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas)**, y haga clic el **Internet Authentication Service broche-**en.
2. Haga clic con el botón derecho del ratón el **Internet Authentication Service (IAS)**, y después haga clic el **servicio del registro en el Active Directory**.
3. **El Internet Authentication Service del registro en el** cuadro de diálogo del **Active Directory** aparece; **AUTORIZACIÓN del** tecleo. Esto permite a IAS para autenticar a los usuarios en el Active Directory.
4. Haga Click en OK en el cuadro de diálogo siguiente.
5. Agregue el regulador del Wireless LAN como cliente AAA en el servidor IAS MS.
6. Haga clic con el botón derecho del ratón a los **clientes RADIUS**, y elija al **nuevo cliente RADIUS**.
7. Teclee el nombre del cliente (WLC en este caso), y ingrese el IP Address del WLC. Haga clic en Next (Siguiente).
8. En la página siguiente, bajo Client Vendedor, elija la **norma RADIUS**; ingrese el secreto compartido; y clic en Finalizar.
9. Note que el WLC está agregado como cliente AAA en IAS.
10. Cree una política de acceso remoto para los clientes.
11. Para hacer esto, haga clic con el botón derecho del ratón las **políticas de acceso remoto**, y elija la **nueva política de acceso remoto**.
12. Teclee un nombre para la política de acceso remoto. En este ejemplo, utilice el nombre **PEAP**. Luego haga clic en Next (Siguiente).
13. Elija los atributos de la política basados en sus requisitos. En este ejemplo, elija la **Tecnología inalámbrica**.
14. En la página siguiente, elija al **usuario** para aplicar esta política de acceso remoto para enumerar de los usuarios.
15. Bajo métodos de autentificación, elija **EAP protegido (PEAP)**, y haga clic la **configuración**.
16. En las **propiedades protegidas EAP** pagine, elija el certificado apropiado del menú desplegable publicado certificado, y haga clic la **AUTORIZACIÓN**.
17. Verifique los detalles de la política de acceso remoto, y del clic en Finalizar.
18. La política de acceso remoto se ha agregado a la lista.
19. Haga clic con el botón derecho del ratón la directiva, y haga clic las **propiedades**. Elija el "**Permiso de acceso remoto de Grant**" bajo "**si un pedido de conexión hace juego las condiciones especificadas**."

Agregan a los usuarios al Active Directory

En esta configuración, la base de datos de usuarios se mantiene en el Active Directory.

Para agregar a los usuarios a la base de datos del Active Directory, complete estos pasos:

1. En el árbol de la consola de los usuarios de directorio activo y computadora, haga clic con el botón derecho del ratón a los **usuarios**; haga clic **nuevo**; y entonces haga clic al **usuario**.
2. En el nuevo objeto – El cuadro de diálogo del usuario, teclea el nombre del usuario de red inalámbrica. Este ejemplo utiliza el nombre **WirelessUser** en el campo de primer nombre y **WirelessUser** en el campo de nombre de inicio de usuario. Haga clic en Next (Siguiente).
3. En el nuevo objeto – El cuadro de diálogo del usuario, teclea una contraseña de su opción en la contraseña y confirma los campos de contraseña. Borre al **usuario debe cambiar la contraseña en la** casilla de verificación **siguiente del inicio**, y hace clic **después**.

4. En el nuevo objeto – Cuadro de diálogo del usuario, clic en Finalizar.
5. Relance los pasos 2 a 4 para crear las cuentas de usuario adicionales.

Permita el acceso de red inalámbrica a los usuarios

Complete estos pasos:

1. En el árbol de la consola de los **usuarios de directorio activo y computadora**, haga clic la **carpeta del usuario**; haga clic con el botón derecho del ratón **WirelessUser**; haga clic las **propiedades**; y entonces vaya al **dial-in tab**.
2. Elija **permiten el acceso**, y hacen clic la **AUTORIZACIÓN**.

Configure el regulador del Wireless LAN y los AP ligeros

Ahora configure los dispositivos de red inalámbrica para esta configuración. Esto incluye la configuración de los reguladores del Wireless LAN, de los AP ligeros, y de los clientes de red inalámbrica.

Configure el WLC para la autenticación de RADIUS a través del servidor de RADIUS MS IAS

Primero configure el WLC para utilizar el MS IAS como el servidor de autenticación. El WLC necesita ser configurado para remitir los credenciales de usuario a un servidor RADIUS externo. El servidor RADIUS externo después valida los credenciales de usuario y proporciona el acceso a los clientes de red inalámbrica. Para hacer esto, agregue al servidor IAS MS como servidor de RADIUS en la página de la **Seguridad > de la autenticación de RADIUS**.

Complete estos pasos:

1. Elija la **Seguridad** y la **autenticación de RADIUS del** regulador GUI para visualizar la página de los servidores de autenticación de RADIUS. Entonces haga clic **nuevo** para definir a un servidor de RADIUS.
2. Defina los parámetros del servidor de RADIUS en los **servidores de autenticación de RADIUS > nueva** página. Estos parámetros incluyen la dirección IP, el secreto compartido, el número del puerto, y el estado del servidor del servidor de RADIUS. Las casillas de verificación del usuario de la red y de la Administración determinan si la autenticación basada en RADIUS solicita la Administración y los usuarios de la red. Este ejemplo utiliza el MS IAS como el servidor de RADIUS con la dirección IP 10.77.244.198.
3. Haga clic en Apply (Aplicar).
4. Han agregado al WLC como servidor de RADIUS y puede ser utilizado al servidor IAS MS para autenticar a los clientes de red inalámbrica.

Configure una red inalámbrica (WLAN) para los clientes

Configure el SSID (la red inalámbrica (WLAN)) con la cual los clientes de red inalámbrica conectan. En este ejemplo, cree el SSID, y nómbrelo **PEAP**.

Defina la autenticación de la capa 2 como WPA2 de modo que los clientes realicen la

autenticación basada EAP (PEAP-MSCHAPv2 en este caso) y el uso AES como el mecanismo de encripción. Deje el resto de los valores en sus valores por defecto.

Nota: Este documento ata la red inalámbrica (WLAN) con las interfaces de administración. Cuando usted tiene VLAN múltiples en su red, usted puede crear un VLAN distinto y atarlo al SSID. Para la información sobre cómo configurar los VLA N en el WLCs, refiera a los VLA N en el ejemplo de configuración de los reguladores del Wireless LAN.

Para configurar una red inalámbrica (WLAN) en el WLC complete estos pasos:

1. Haga clic los **WLAN del** GUI del regulador para visualizar la página WLAN. Esta página enumera los WLAN que existen en el regulador.
2. Elija **nuevo** para crear una nueva red inalámbrica (WLAN). Ingrese el ID DE WLAN y el WLAN SSID para el WLAN, y el tecleo **se aplica**.
3. Una vez que usted crea una nueva red inalámbrica (WLAN), la **red inalámbrica (WLAN) > edita la** página para la nueva red inalámbrica (WLAN) aparece. En esta página usted puede definir los diversos parámetros específicos a esta red inalámbrica (WLAN) que incluyen las políticas generales, los servidores de RADIUS, las políticas de seguridad, y los parámetros del 802.1x.
4. Marque el **estado del administrador** bajo políticas generales para habilitar la red inalámbrica (WLAN). Si usted quisiera que el AP transmitiera el SSID en sus tramas de recuperación de problemas, marque el **broadcast SSID**.
5. Bajo Seguridad de la capa 2, elija **WPA1+WPA2**. Esto habilita el WPA en la red inalámbrica (WLAN). Navegue hacia abajo la página y elija la directiva WPA. Este ejemplo utiliza el WPA2 y la encripción AES. Elija al servidor de RADIUS apropiado del menú desplegable bajo los servidores de RADIUS. En este ejemplo, utilice **10.77.244.198** (dirección IP del servidor IAS MS). Los otros parámetros se pueden modificar basaron en el requisito de la red WLAN.
6. Haga clic en Apply (Aplicar).

Configure a los clientes de red inalámbrica

Configure a los clientes de red inalámbrica para la autenticación PEAP-MS CHAPv2

Este ejemplo proporciona la información sobre cómo configurar al cliente de red inalámbrica con la utilidad de escritorio del Cisco Aironet. Antes de que usted configure el adaptador del cliente, asegure el que la última versión del firmware y la utilidad se utilicen. Encuentre la última versión del firmware y las utilidades en la página inalámbrica de las descargas en el cisco.com.

Para configurar el adaptador de red inalámbrica de cliente del a/b/g del 802.11 del Cisco Aironet con el ADU, complete estos pasos:

1. Abra utilidad Aironet Desktop.
2. Haga clic la **Administración del perfil**, y haga clic **nuevo** para definir un perfil.
3. Conforme a la ficha general, ingrese el nombre del perfil y el SSID. En este ejemplo, utilice el SSID que usted configuró en el WLC (PEAP).
4. Elija la ficha de seguridad; elija **WPA/WPA2/CCKM**; bajo WPA/WPA2/CCKM EL EAP, el tipo elige **PEAP [EAP-MSCHAPv2]**, y hace clic la **configuración**.

5. Elija **validan el certificado de servidor**, y eligen Tecnología inalámbrica-**CA** bajo menú desplegable de las autoridades de certificación de la Raíz confiable.
6. El Haga Click en OK, y activa el perfil.**Nota:** Cuando usted utiliza el Challenge Handshake Authentication Protocol protegido de EAP-Microsoft versión 2 (PEAP-MSCHAPv2) con Microsoft XP SP2, y la placa de red inalámbrica es manejada por la configuración de la Tecnología inalámbrica cero de Microsoft (WZC), usted debe aplicar el hotfix de Microsoft KB885453. Esto previene varios problemas en la autenticación relacionada con el PEAP rápidamente reanuda.

Verificación y resolución de problemas

Para verificar si la configuración trabaja como se esperaba, active el perfil PEAP-MSCHAPv2 en el client1 del cliente de red inalámbrica.

Una vez que el perfil PEAP-MSCHAPv2 se activa en el ADU, el cliente realiza la autenticación abierta del 802.11 y después realiza la autenticación PEAP-MSCHAPv2. Aquí está un ejemplo de la autenticación acertada PEAP-MSCHAPv2.

Utilice los comandos debug de entender la Secuencia de eventos que ocurren.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Estos comandos debug en el regulador del Wireless LAN son útiles.

- **permiso de los eventos del dot1x del debug** — Para configurar el debugging de los eventos del 802.1x
- **permiso de los eventos aaa del debug** — Para configurar el debugging de los eventos AAA
- **direcciones MAC < MAC address > del debug** — Para configurar el debugging MAC, utilice el comando mac del debug
- **haga el debug del permiso del mensaje DHCP** — Para configurar el debug de los mensajes de error del DHCP

Éstas son las salidas de ejemplo del **comando enable de los eventos del dot1x del debug** y **hacen el debug del** comando del **< MAC address > del cliente**.

permiso de los eventos del dot1x del debug:

```
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**

direcciones MAC < dirección MAC > del debug:

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**

Nota: Si usted utiliza al solicitante de Microsoft para autenticar con un Cisco Secure ACS para la autenticación PEAP, el cliente potencialmente no autentica con éxito. La conexión inicial puede autenticar a veces con éxito, pero subsiguiente rápido-conecte los intentos de autenticación no conectan con éxito. Esto es un problema conocido. Los detalles de este problema y del arreglo para lo mismo están disponibles aquí .

Información Relacionada

- PEAP bajo redes inalámbricas unificadas con ACS 4.0 y Windows 2003
- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Actualización del software del regulador del Wireless LAN (WLC) a las versiones 3.2, 4.0, y

4.1

- Guías de configuración del Cisco Wireless LAN Controllers de la serie 4400
- Soporte Técnico y Documentación - Cisco Systems