Lightweight Access Point de la configuración como supplicant del 802.1x

Contenido

Introducción

Este documento describe cómo configurar un Lightweight Access Point como supplicant del 802.1x para autenticar contra un servidor de RADIUS.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Cisco Aironet 1130, 1240, o Punto de acceso de las 1250 Series
- WLC que funciona con la versión 5.1 IOS®
- Cisco Catalyst 3560 Series Switch con el Cisco IOS Release 12.2(35)SE5
- Cisco Catalyst 3750 Series Switch con el Cisco IOS Release 12.2(40)SE
- Cisco Catalyst 4500 Series Switch con el Cisco IOS Release 12.2(40)SG
- Cisco Catalyst 6500 Series Switch con el Supervisor Engine 32 que funciona con el Cisco IOS Release 12.2(33)SXH

Componentes Utilizados

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Los revestimientos factory installed los Certificados X.509, firmados por una clave privada, que se queman en el dispositivo a la hora de la fabricación. Los revestimientos utilizan este certificado para autenticar con el WLC en el proceso del unido. Para más información, refiera a asegurar el avión del control del LWAPP de los reguladores del Wireless LAN de las Cisco 440X Series del documento que despliegan. Este método describe otra manera de autenticar los revestimientos. Con la versión 5.1 del WLC, usted puede configurar la autenticación del 802.1x entre un Punto de acceso del Cisco Aironet y un switch Cisco. El Punto de acceso actúa como el supplicant del 802.1x y es autenticado por el Switch contra un servidor de RADIUS (ACS) ese EAP-FAST de las aplicaciones con el aprovisionamiento anónimo PAC. Una vez que se configura para la autenticación del 802.1x, el Switch no permite que ningún tráfico con excepción del tráfico del 802.1x pase a través del puerto hasta que el dispositivo conectado con el puerto autentique con éxito. Un Punto de acceso se puede autenticar o antes de que se una a un WLC o después de que se ha unido a un WLC, en este caso usted configura el 802.1x en el Switch después de que el REVESTIMIENTO se una al WLC.

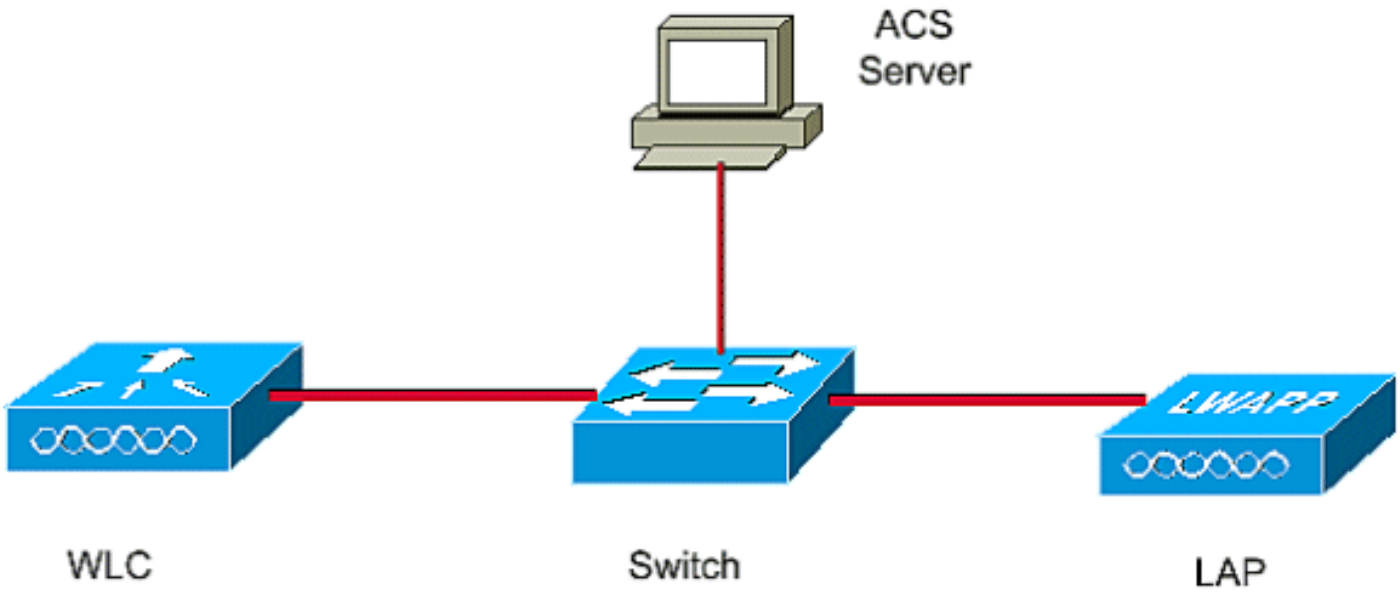
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento utiliza estos IP Addresses:

- La dirección IP del Switch es 10.77.244.210
- La dirección IP del servidor ACS es 10.77.244.196
- La dirección IP del WLC es 10.77.244.204

Configure el REVESTIMIENTO

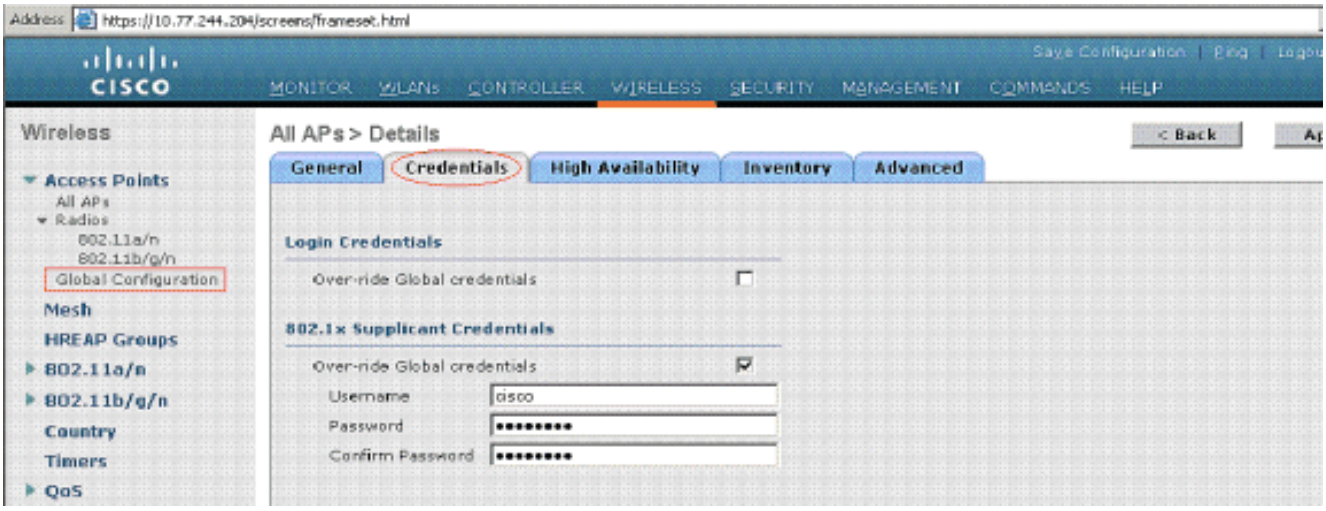
En esta sección, le presentan con la información para configurar el REVESTIMIENTO como supplicant del 802.1x.

Complete estos pasos:

1. Aseegurese que el Punto de acceso está cargado con una imagen de recuperación ligera.
2. Conecte el REVESTIMIENTO con el Switch.
3. El REVESTIMIENTO pasa con el proceso del unido y se registra con el WLC. Esto se puede marcar del menú inalámbrico del WLC tal y como se muestra en del cuadro 1.**Figura 1**

4. Haga clic el **Punto de acceso**, y haga clic la lengueta de las **credenciales**.
5. Bajo las credenciales del supplicant del 802.1x que dirigen, marque el cuadro **global de las credenciales de la invalidación** para fijar el nombre de usuario y contraseña del 802.1x para este Punto de acceso. Usted puede también fijar el nombre de usuario y contraseña en el campo común a todos los Puntos de acceso que se unen a un WLC con el menú de la

configuración global. El cuadro 2 muestra cómo fijar las credenciales del 802.1x para un Punto de acceso.**Figura 2**



Nota: Usted puede también fijar el nombre de usuario y contraseña del 802.1x para un Punto de acceso con el comando CLI del WLC que los **config ap dot1xuser agregan el <password> Cisco_AP (nombre de la contraseña del <user> del nombre de usuario AP)**.

6. El tecleo **se aplica** para confiar sus cambios.
7. **Configuración de la salvaguardia del** tecleo para salvar las credenciales.**Nota:** Una vez que están guardadas, estas credenciales se conservan a través de las reinicializaciones del WLC y AP. Cambian solamente cuando el REVESTIMIENTO se une a un nuevo WLC. El REVESTIMIENTO asume el nombre de usuario y contraseña que fue configurado en el nuevo WLC.
8. Si el Punto de acceso no se ha unido a un WLC todavía, usted debe consolar en el REVESTIMIENTO para fijar las credenciales y para utilizar este comando CLI en el enable mode:`LAP#lwapp ap dot1x username <username> password <password>` **Nota:** Este comando está disponible solamente para los Puntos de acceso que funcionan con la imagen de recuperación 5.1.

Configure el Switch

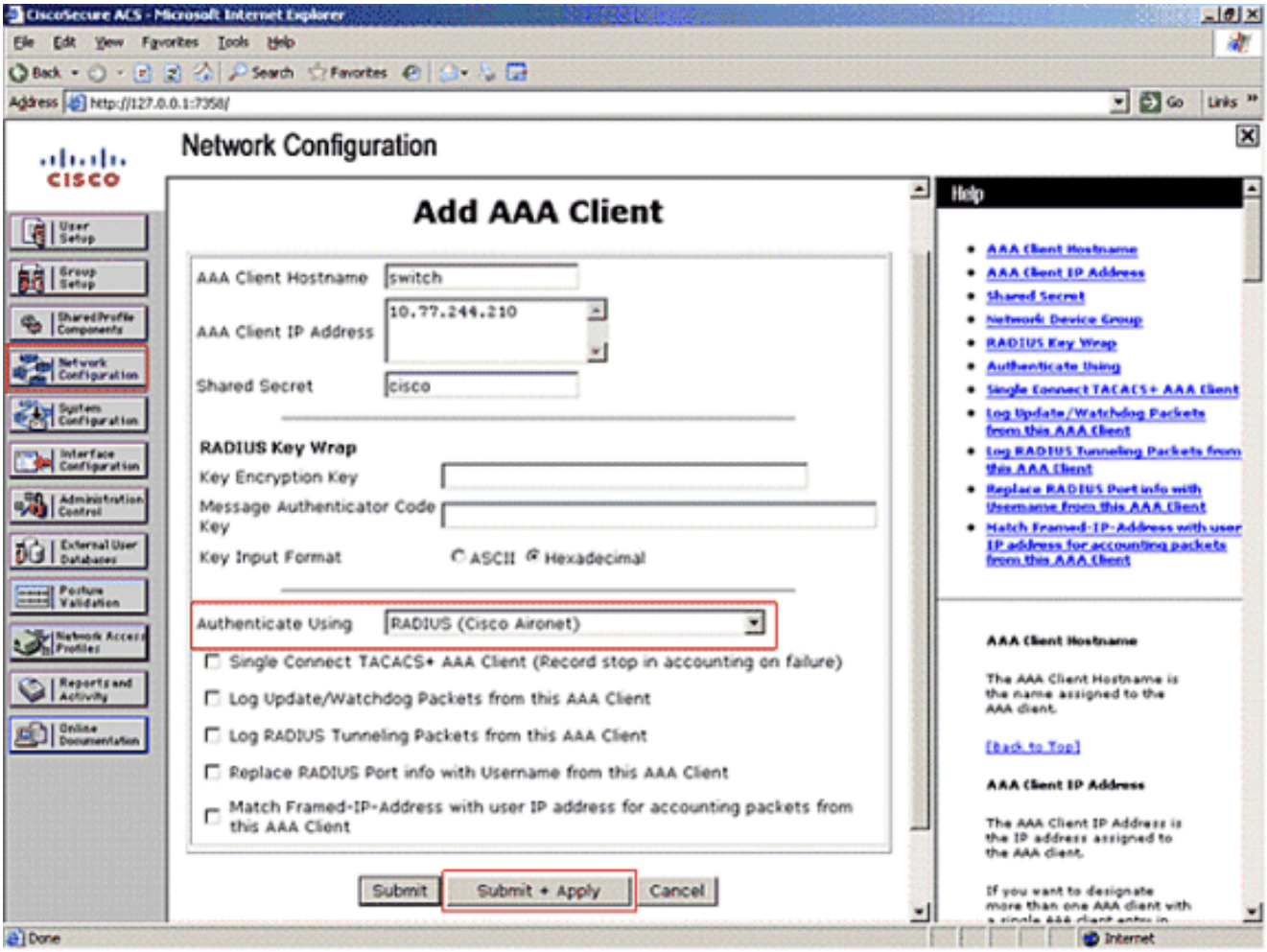
El Switch actúa como authenticator para el REVESTIMIENTO y autentica el REVESTIMIENTO contra un servidor de RADIUS. Si el Switch no tiene el software obediente, actualice el Switch. En el Switch CLI, ingrese estos comandos de habilitar la autenticación del 802.1x en un puerto del switch:

```
switch#configure terminal                    switch(config)dot1x system-auth-control
switch(config)aaa new-model                    switch(config)aaa authentication dot1x default
group radius                    switch(config)radius server host 10.77.244.196 key cisco!---
configures the radius server with shared secret switch(config)interface gigabitEthernet 1/0/43!-
-- 43 is the port number on which the access point is connected. switch(config-if)switchport
mode access switch(config-if)dot1x pae authenticator!--- configures dot1x authentication
switch(config-if)dot1x port-control auto!--- With this command switch initiates the 802.1x
authentication.
```

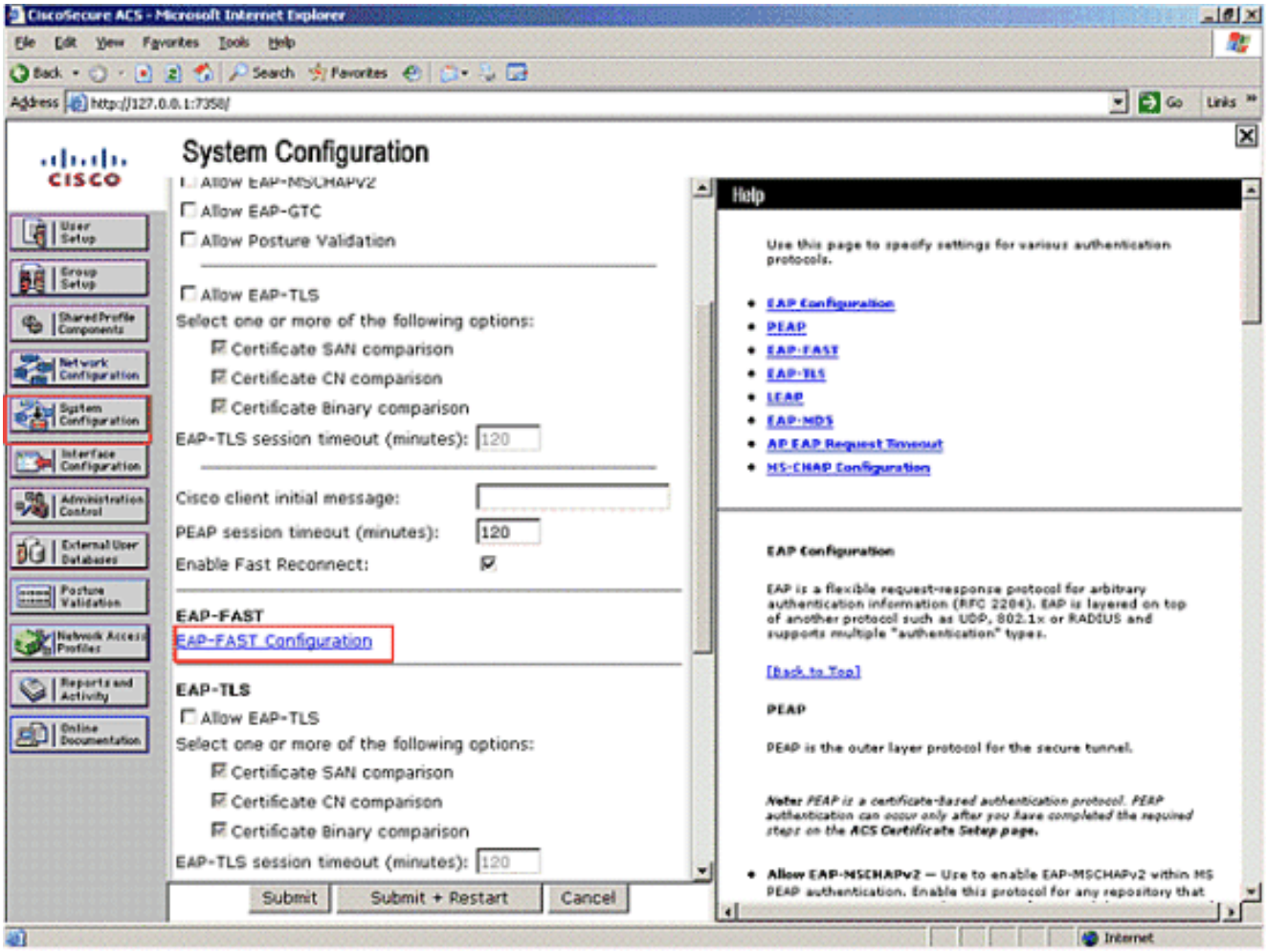
Configure al servidor de RADIUS

El REVESTIMIENTO se autentica con el EAP-FAST. Aseegurese que el servidor de RADIUS usted utiliza los soportes este método EAP. En este ejemplo, utilizan al servidor ACS para la autenticación. Complete estos pasos en el servidor ACS:

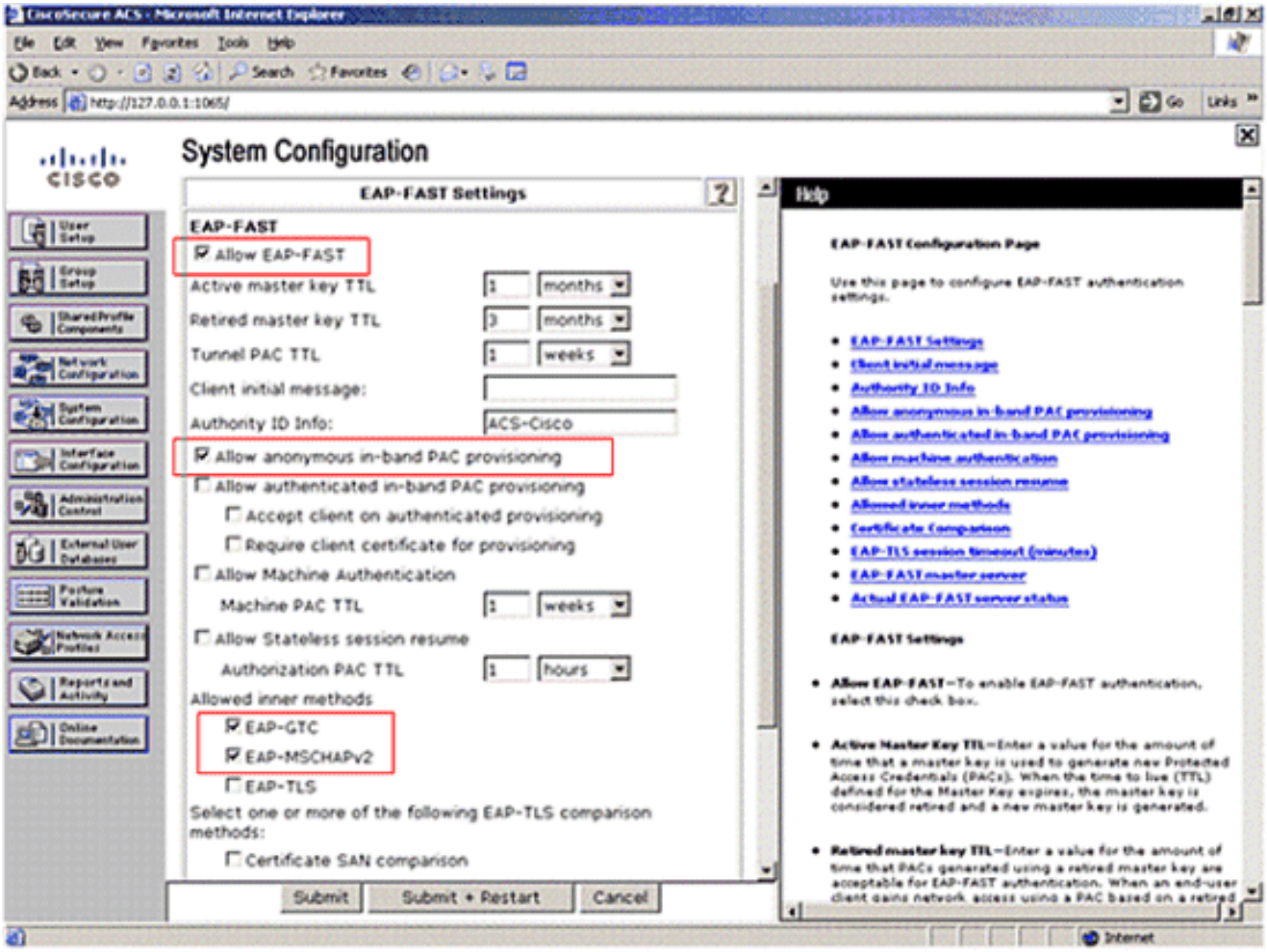
1. Inicie la pantalla ACS admin.
2. Configure el nombre de usuario y contraseña del REVESTIMIENTO en la base de datos ACS. Para agregar una cuenta de usuario en el ACS, refiera User Management (Administración de usuario) a la sección del guía del usuario del documento para el Cisco Secure Access Control Server 4.2.
3. Configure el Switch como cliente AAA al servidor ACS. En la pantalla ACS admin, haga clic el menú de la **configuración de red**.
4. Bajo sección del **cliente AAA**, el tecleo **agrega la nueva entrada**. Ingrese estos parámetros:Ingrese el IP Address del Switch en el campo del *IP Address del cliente AAA*.Ingrese el secreto compartido del Switch. Éste debe ser exactamente lo mismo en el Switch y el servidor ACS.Elija un **protocolo RADIUS** en la *autenticidad usando el* campo. Por abandono, es TACACS+.**Nota:** Marque al servidor ACS para una descripción de los protocolos RADIUS.Vea la figura 3.**Figura 3**



5. El tecleo **somete + se aplica** para salvar al cliente AAA.
6. El EAP-FAST tiene que ser habilitado en el servidor de RADIUS. Haga clic el menú de la **configuración del sistema** en el lado izquierdo. Haga clic la opción de la **configuración de la autenticación global**.**'Figura 4'**



7. **Configuración del EAP-FAST del** tecleo tal y como se muestra en del cuadro 4.
8. En la página Configuración del EAP-FAST, marque el cuadro del **EAP-FAST de la permit**. El REVESTIMIENTO utiliza el EAP-FAST con el aprovisionamiento anónimo PAC. Marque el cuadro **anónimo del aprovisionamiento de la en-banda PAC de la permit**. Para más información, refiera a la autenticación del EAP-FAST del documento con el ejemplo de configuración de los reguladores y del servidor RADIUS externo del Wireless LAN.**Figura 5**



9. Aseegurese que el **EAP-GTC** y el **EAP MSCHAPv2** están marcados debajo *permiten los métodos internos*. El cuadro 5 muestra una configuración de muestra de los pasos 8 y 9.

Verificación

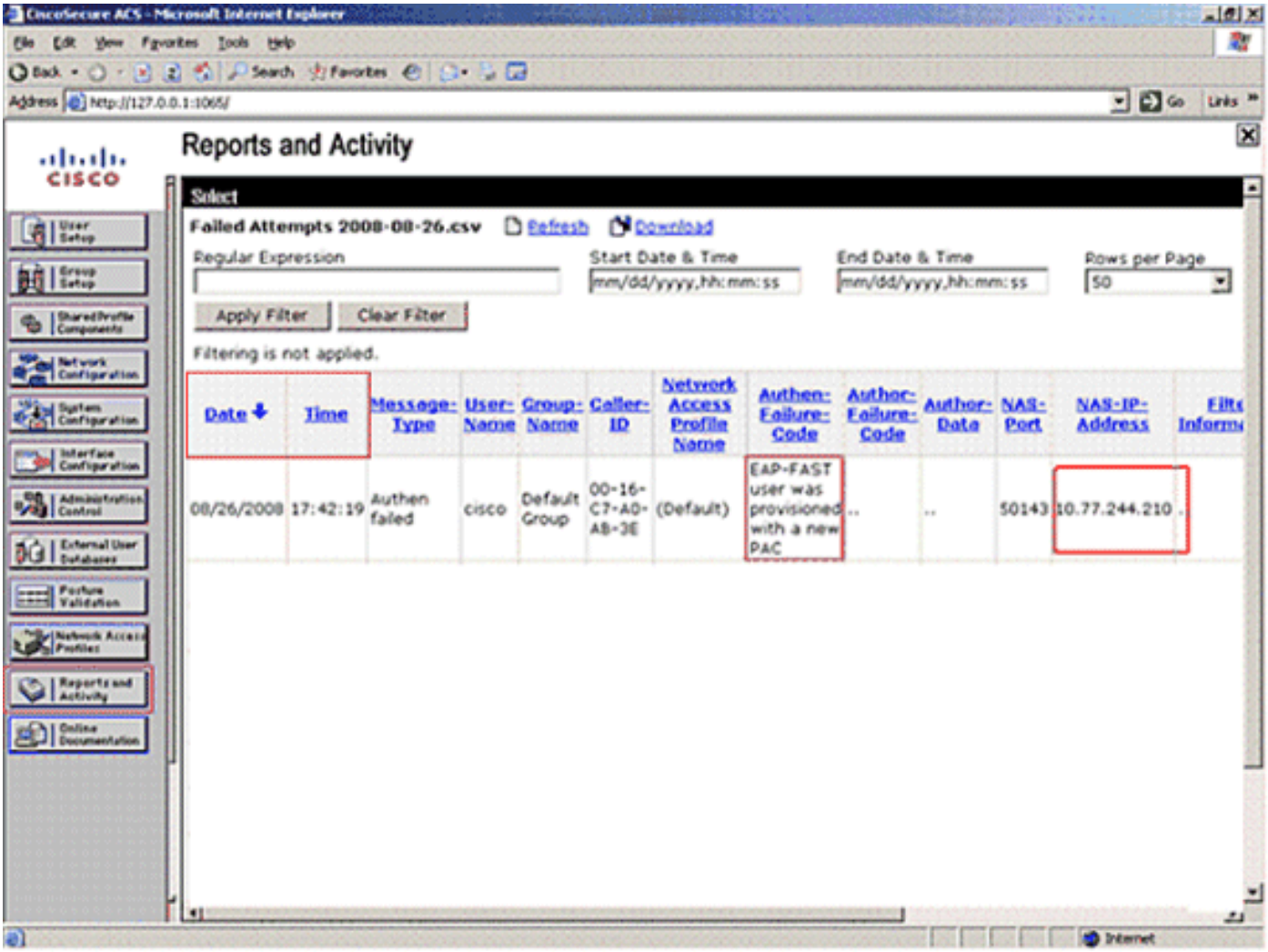
Use esta sección para confirmar que su configuración funciona correctamente.

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.

Una vez que el 802.1x se habilita en el puerto del switch, todo el tráfico a menos que el tráfico del 802.1x se bloquee a través del puerto. El REVESTIMIENTO, que se registra ya al WLC, consigue desasociado. Solamente después que una autenticación acertada del 802.1x es el otro tráfico permitido pasar a través. El registro exitoso del REVESTIMIENTO al WLC después de que el 802.1x se habilite en el Switch indica que la autenticación del REVESTIMIENTO es acertada.

Usted puede también marcar esto del ACS. De la pantalla principal ACS, haga clic el menú de los **informes y de la autenticación**. Haga clic la opción de los **intentos fallidos**. Si la autenticación es acertada, usted encuentra que un *mensaje fallido de la autenticación* con el *usuario del EAP-FAST del* código *era aprovisionado con un nuevo PAC con la dirección IP del Switch* en el campo del Nas-ip-address tal y como se muestra en del cuadro 6. Usted puede también confirmar con la fecha y hora de la autenticación.

'Figura 6'



Troubleshooting

Use esta sección para resolver problemas de configuración.

1. Utilice el **comando ping** y el control si el servidor ACS es accesible del Switch.
2. Aseegurese que el Switch está configurado como cliente AAA en el servidor ACS.
3. Asegúrese de que el secreto compartido sea lo mismo entre el Switch y el servidor ACS.
4. Marque si el EAP-FAST se habilita en el servidor ACS.
5. Marque para saber si hay la conformidad del software en los dispositivos.
6. Marque si las credenciales del 802.1x se configuran para el REVESTIMIENTO y son lo mismo en el servidor ACS.**Nota:** El nombre de usuario y contraseña es con diferenciación entre mayúsculas y minúsculas.

Comandos para resolución de problemas

Hay actualmente comandos no debug disponibles para esta característica.

Información Relacionada

- Control de Puntos de Acceso Ligeros
- Configurar la autenticación del acceso basado del IEEE 802.1X

- Soporte Técnico y Documentación - Cisco Systems