Configuración de los servicios de dominio inalámbrico

Contenido

Introducción

Este documento introduce el concepto de Servicios de dominio inalámbrico (WDS). El documento también describe cómo configurar un punto de acceso o el Módulo de servicios del Wireless LAN (WLSM) como el WDS y por lo menos otro como infraestructura AP. El procedimiento que se describe en este documento ayuda en la configuración de un WDS que sea funcional y permita a los clientes asociarse ya sea al AP de WDS o a un AP de infraestructura. Este documento se prepone establecer una base de la cual usted pueda configurar rápidamente la itinerancia segura o introducir un motor de las soluciones de red inalámbrica LAN (WLSE) en la red, así que usted puede utilizar las características.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Tenga conocimiento completo de las redes inalámbricas LAN y de los problemas de seguridad de red inalámbrica.

- Tenga métodos de seguridad del Protocolo de Autenticación Extensible (EAP) del Conocimiento de actuales.

Componentes Utilizados

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

- AP con el software de Cisco IOS®
- Cisco IOS Software Release 12.3(2)JA2 o Posterior
- Módulo de servicios del Wireless LAN de las Catalyst 6500 Series

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos usados en este documento comenzado con una configuración despejada (predeterminada) y una dirección IP en la interfaz BVI1, así que la unidad es accesibles del Cisco IOS Software GUI o del comando line interface(cli). Si usted trabaja en una red en funcionamiento, asegúrese de que usted entienda el impacto potencial del comando any.

Convenciones

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

Servicios del dominio de red inalámbrica

El WDS es una nueva función para los AP en el Cisco IOS Software y la base de las Catalyst 6500 Series WLSM. El WDS es una función de la base que habilita las otras funciones como éstos:

- Rápido asegure la itinerancia
- Interacción WLSE
- Administración de radios

Usted debe establecer las relaciones entre los AP que participan en el WDS y el WLSM, antes de que cualquier otro WDS-basara el trabajo de las características. Uno de los propósitos de WDS es eliminar de la necesidad que tiene el servidor de autenticación de validar las credenciales de usuario y reducir el tiempo requerido para las autenticaciones de los clientes.

Para utilizar el WDS, usted debe señalar un AP o el WLSM como el WDS. UN WDS AP debe utilizar un nombre y una contraseña de usuario WDS para establecer una relación con un servidor de autenticación. El servidor de autenticación puede ser servidor RADIUS externo o la característica local del servidor de RADIUS en el WDS AP. El WLSM debe tener una relación con el servidor de autenticación, aunque el WLSM no necesita autenticar al servidor.

Otros AP, llamados la infraestructura AP, comunican con el WDS. Antes de que ocurra el registro, la infraestructura AP debe autenticarse al WDS. Un grupo de servidores de la infraestructura en el WDS define esta autenticación de infraestructura.

Uno o más grupos de servidor del cliente en el WDS definen la autenticación de cliente.

Cuando un cliente intenta asociarse a una infraestructura AP, la infraestructura AP pasa las

credenciales del usuario al WDS para la validación. Si el WDS ve las credenciales por primera vez, el WDS da vuelta al servidor de autenticación para validar las credenciales. El WDS entonces oculta las credenciales, para eliminar la necesidad de volver al servidor de autenticación cuando lo mismo usuario intenta autenticarse otra vez. Los ejemplos de la reautentificación incluyen:

- Reintroducción
- Itinerancia
- Cuando el usuario pone en marcha el dispositivo del cliente

Cualquier protocolo de autenticación EAP basado en RADIUS puede ser tunneled con el WDS tal como éstos:

- EAP ligero (SALTO)
- EAP protegido (PEAP)
- Seguridad de la capa del EAP-transporte (EAP-TLS)
- Autenticación adaptable de EAP con el Tunelización seguro (EAP-FAST)

La autenticación de la dirección MAC puede también hacer un túnel a un servidor de autenticación externa o contra una lista local a un WDS AP. El WLSM no soporta la autenticación de la dirección MAC.

El WDS y la infraestructura AP comunican sobre un Multicast Protocol llamado el Control Protocol del Contexto WLAN (WLCCP). Estos mensajes de multidifusión no pueden ser ruteados, así que un WDS y la infraestructura asociada AP deben estar en la misma subred IP y en el mismo segmento de LAN. Entre el WDS y las aplicaciones TCP WLSE, WLCCP y el User Datagram Protocol (UDP) en el puerto 2887. Cuando el WDS y el WLSE están en diversas subredes, un protocolo como el Network Address Translation (NAT) no puede traducir los paquetes.

Un AP configurado como el dispositivo WDS soporta hasta 60 AP participantes. Un router de los Servicios integrados (ISR) configurado como los dispositivos WDS soporta hasta 100 AP participantes. Y un Switch WLSM-equipado apoya hasta 600 AP participantes y a hasta 240 Grupos de movilidad. Un solo AP apoya a hasta 16 Grupos de movilidad.

Nota: Cisco recomienda que la infraestructura AP funciona con la misma versión del IOS que el dispositivo WDS. Si usted utiliza una versión anterior del IOS, los AP pudieron no poder autenticar al dispositivo WDS. Además, Cisco recomienda que usted utiliza la última versión del IOS. Usted puede encontrar la última versión del IOS de la página inalámbrica de las descargas.

Papel del dispositivo WDS

El dispositivo WDS realiza varias tareas en su Wireless LAN:

- Hace publicidad de su capacidad WDS y participa en la elección del mejor dispositivo WDS para su Wireless LAN. Cuando usted configura su Wireless LAN para el WDS, usted configura un dispositivo como el candidato WDS principal y uno o más dispositivos adicionales como candidatos WDS de respaldo. Si el dispositivo WDS principal va off-line, uno de los dispositivos WDS de reserva toma su lugar.
- Autentica todos los AP en la subred y establece un canal de la comunicación segura con cada uno de ellos.
- Recoge los datos de radio de los AP en la subred, agrega los datos, y adelante los al dispositivo WLSE en su red.

- Actúa como paso para todos los dispositivos del cliente 802.1x-authenticated asociados a los AP participantes.
- Registra todos los dispositivos del cliente en la subred que utilicen cerrar dinámico, establece las claves de la sesión para ellas, y oculta sus credenciales de seguridad. Cuando un cliente vaga por a otro AP, los credenciales de seguridad dispositivo WDS adelante del cliente al nuevo AP.

Papel de los Puntos de acceso usando el dispositivo WDS

Los AP en su Wireless LAN obran recíprocamente con el dispositivo WDS en estas actividades:

- Descubra y siga los anuncios actuales del dispositivo WDS y de la retransmisión WDS al Wireless LAN.
- Autentique con el dispositivo WDS y establezca un canal de la comunicación segura al dispositivo WDS.
- Registre los dispositivos del cliente asociados con el dispositivo WDS.
- Señale los datos de radio al dispositivo WDS.

Configuración

El WDS presenta la configuración en una moda pedida, modular. Emplear de cada concepto el concepto que precede. El WDS omite otros elementos de configuración tales como contraseñas, Acceso Remoto, y las Configuraciones de radio para mayor clareza y foco en el tema de la base.

Esta sección presenta la información necesaria configurar las características descritas en este documento.

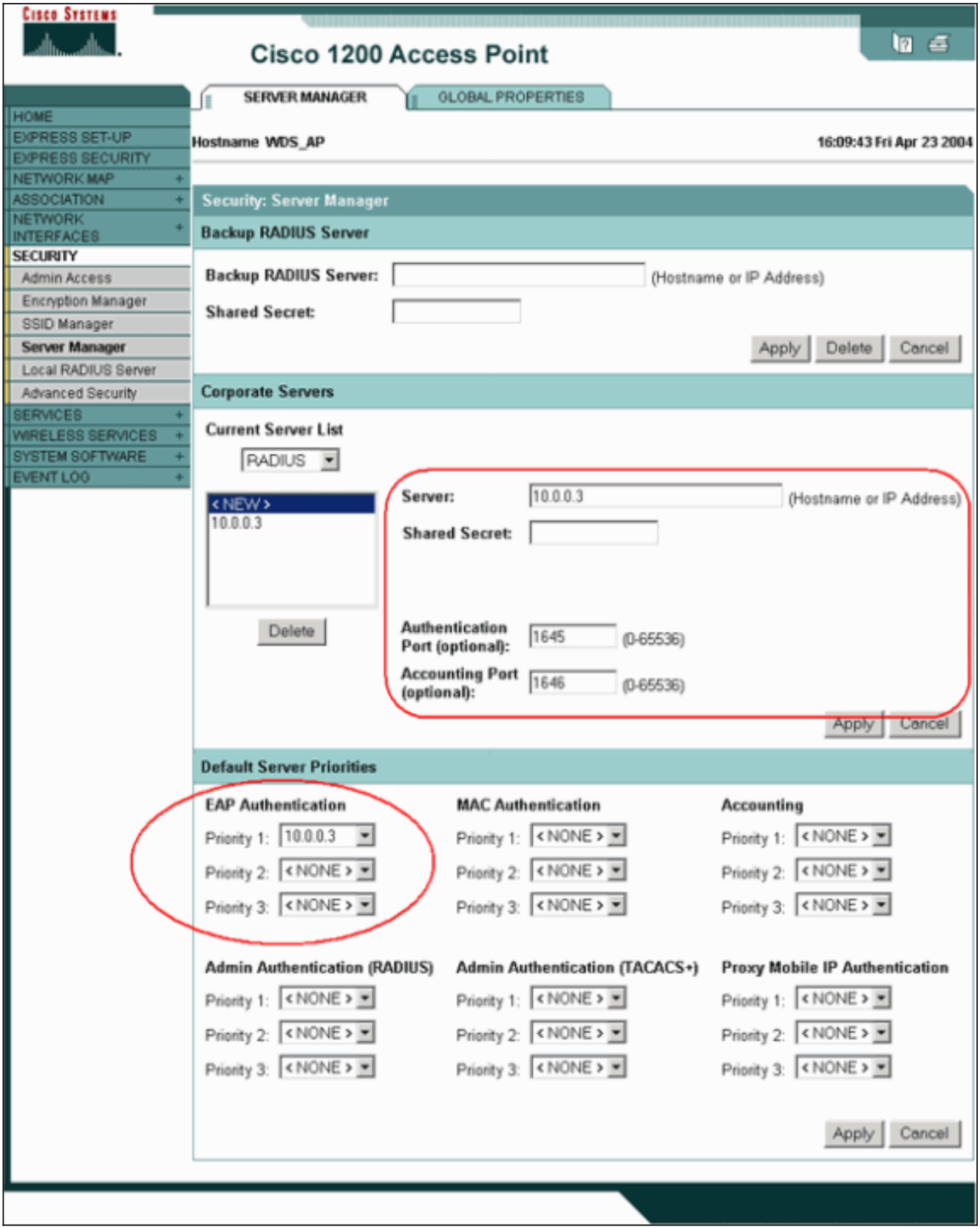
Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Señale un AP como WDS

El primer paso es señalar un AP como el WDS. El WDS AP es el único que comunica con el servidor de autenticación.

Complete estos pasos para señalar un AP como WDS:

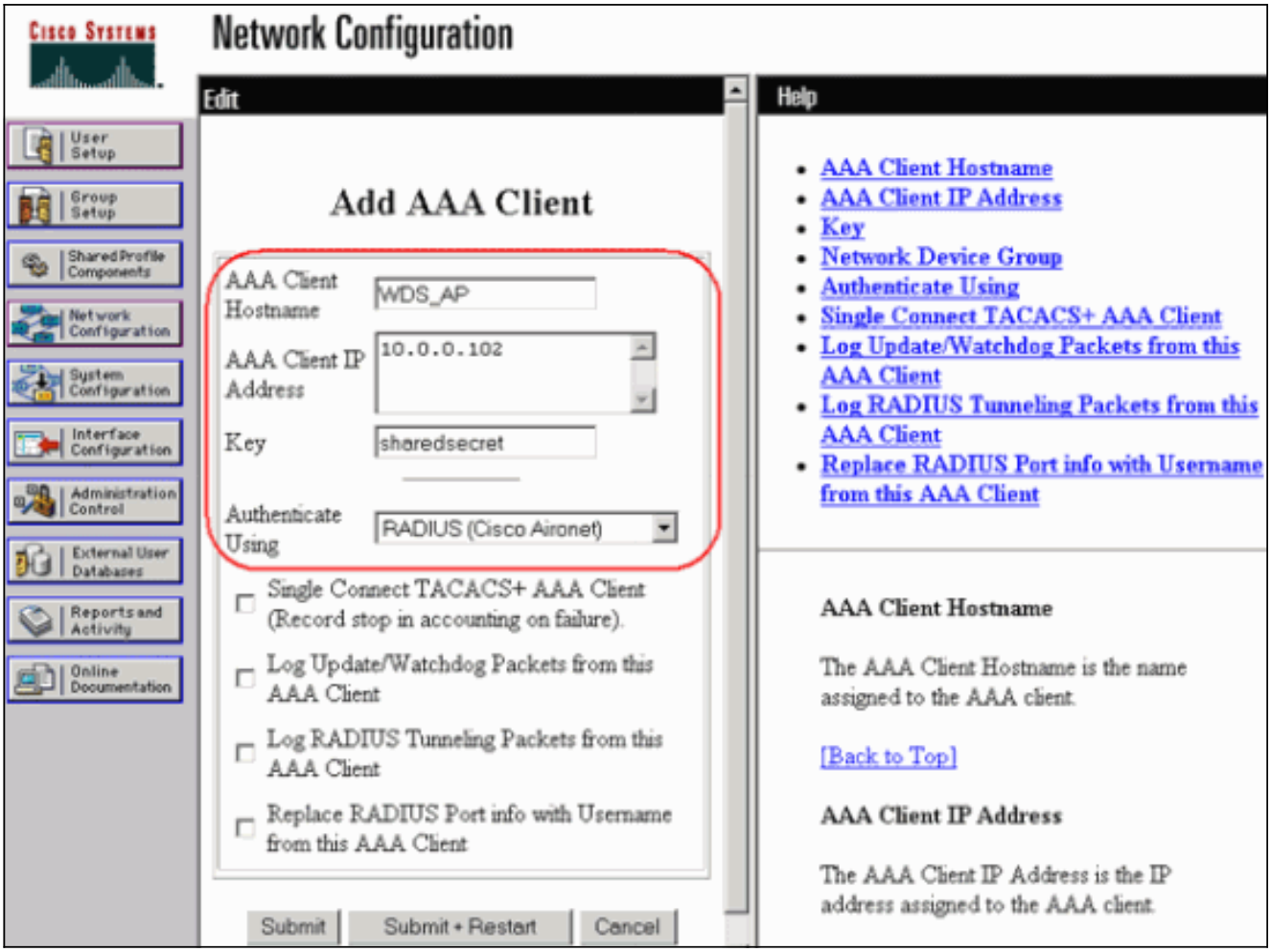
1. Para configurar al servidor de autenticación en el WDS AP, elija la **Seguridad > al administrador de servidor** a ir a la lengueta del administrador de servidor:Bajo los servidores corporativos, teclee la dirección IP del servidor de autenticación en el campo del servidor.Especifique el secreto compartido y los puertos.Bajo prioridades predeterminadas del servidor, fije el campo de la prioridad 1 a ese dirección IP del servidor conforme al tipo de autenticación
apropiado.



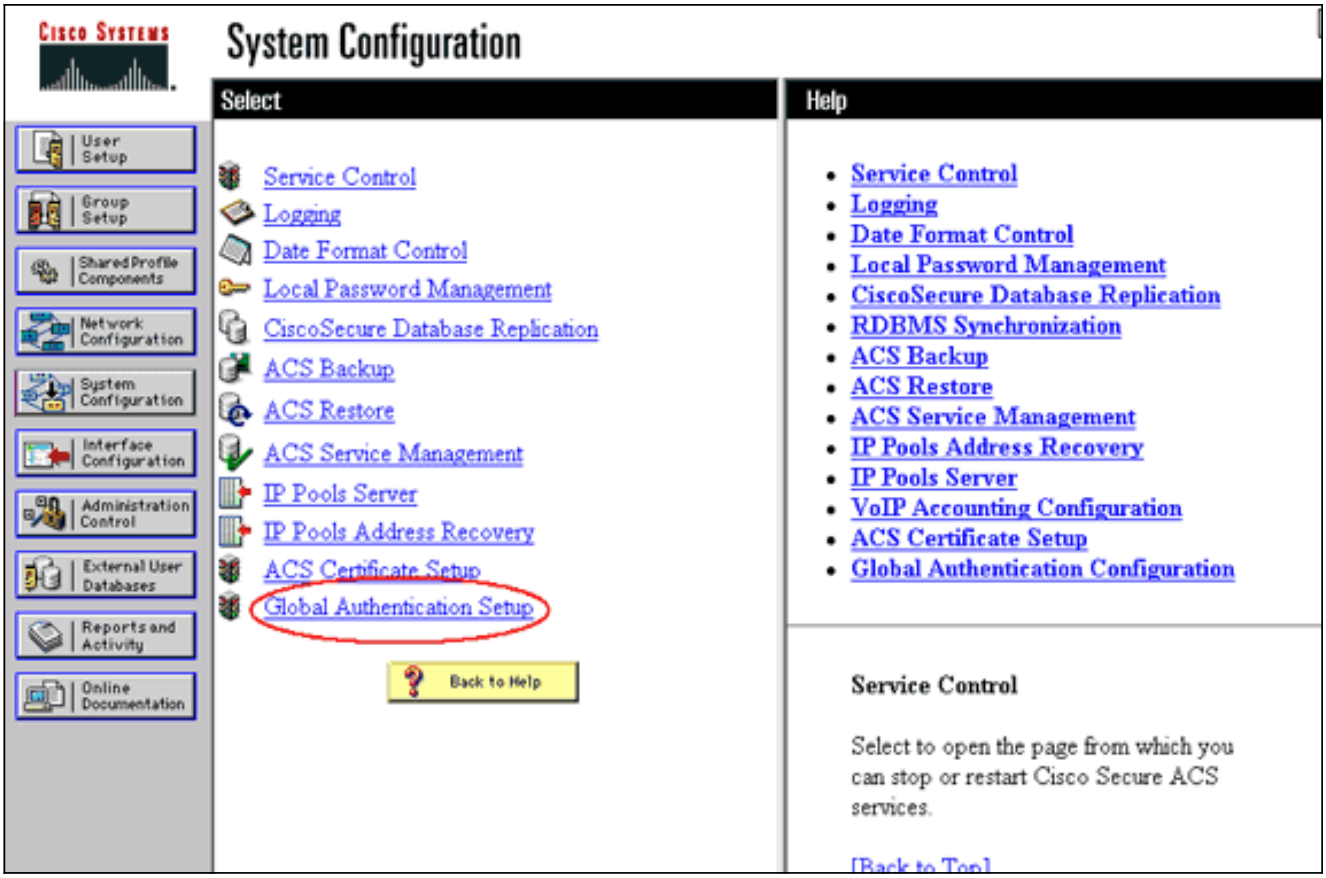
Alternativamente, publique estos comandos del CLI:

2. El siguiente paso es configurar el WDS AP en el servidor de autenticación como cliente del Authentication, Authorization, and Accounting (AAA). Para esto, usted necesita agregar el WDS AP como cliente AAA. Complete estos pasos:**Nota:** Este documento utiliza el servidor del Cisco Secure ACS como el servidor de autenticación.En el Cisco Secure Access Control Server (ACS), esto ocurre en la página de la configuración de red donde usted define estos atributos para el WDS AP:NombreDIRECCIÓN IPSecreto compartidoMétodo de autentificaciónRADIUS Cisco AironetGrupo de trabajo en ingeniería de Internet [IETF] RADIUSHaga clic en **someten**.Para otros servidores de autenticación NON-ACS, refiera a la

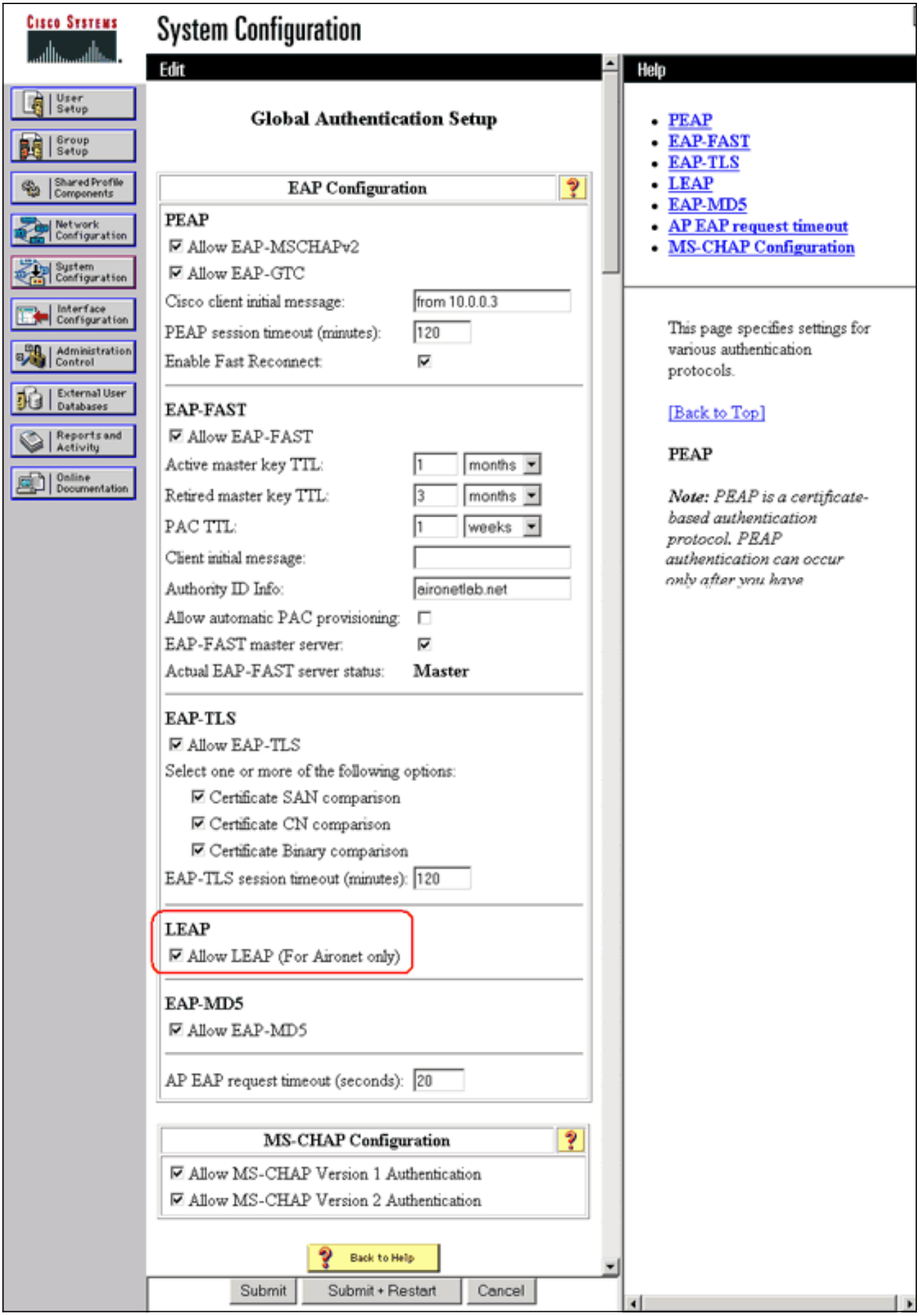
documentación del
fabricante.



También, en el Cisco Secure ACS, asegúrese de que usted configure el ACS para realizar la autenticación LEAP en la configuración del sistema - página de configuración de la autenticación global. Primero, la **configuración del sistema del** tecleo, entonces hace clic la **configuración de la autenticación global**.

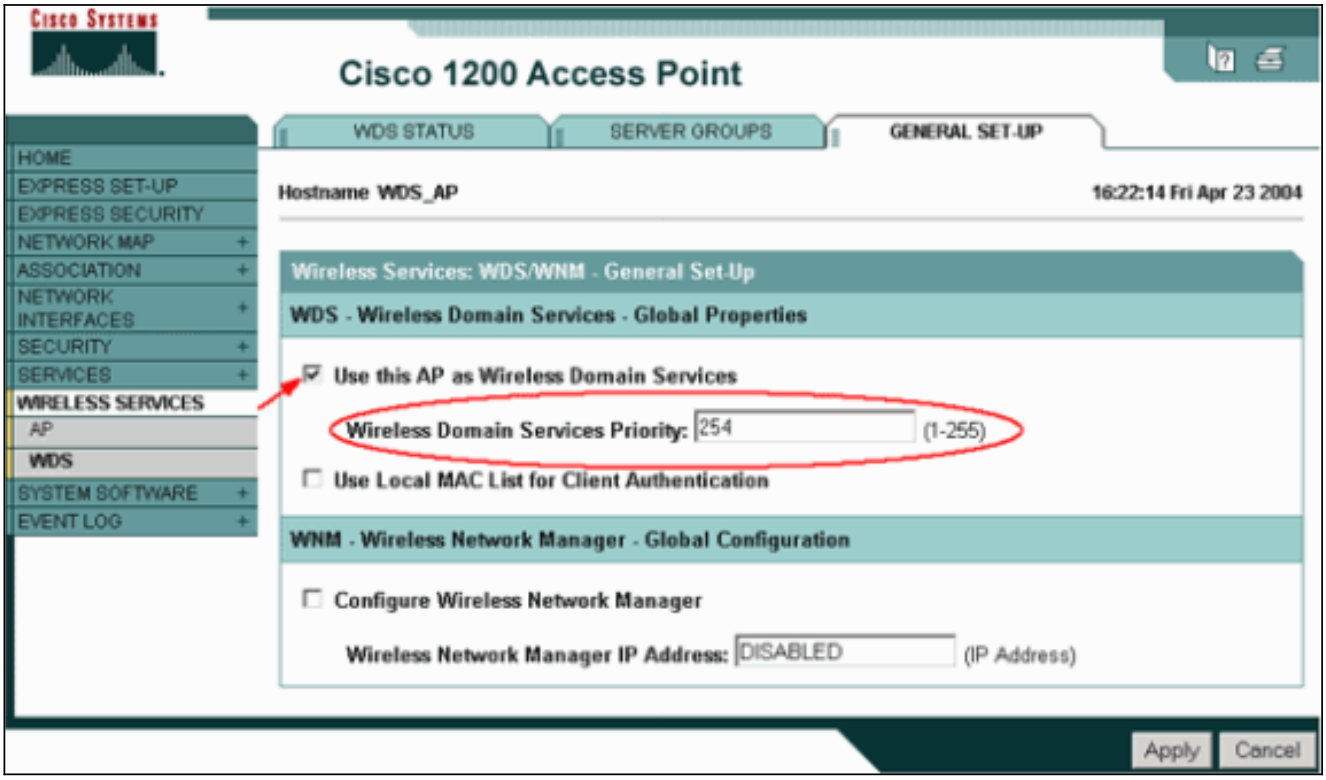


Navegue hacia abajo la página a la configuración del SALTO. Cuando usted examina la caja, ACS autentica
LEAP.



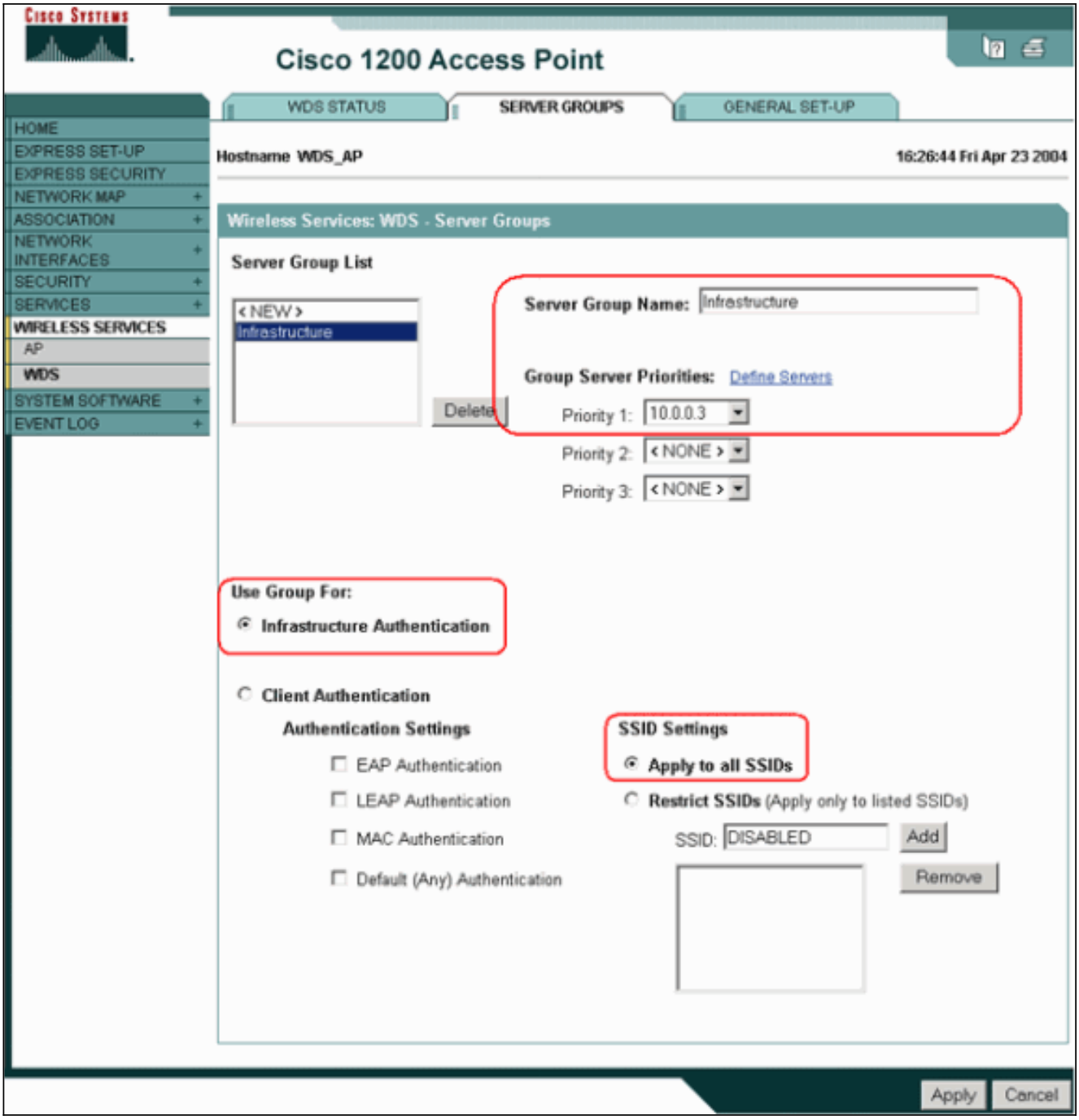
3. Para configurar los setttings WDS en el WDS AP, elegir los **Servicios inalámbricos > el WDS** en el WDS AP, y hacer clic en la **configuración general** cuadro realiza estos pasos:Bajo servicios del dominio de la WDS-Tecnología inalámbrica - Propiedades Globales, **uso del**

control **este AP como servicios del dominio de red inalámbrica**.Fije el valor para el campo de prioridad de los servicios del dominio de red inalámbrica a un valor de aproximadamente **254**, porque éste es primer. Usted puede configurar uno o más AP o Switches como candidatos para proporcionar el WDS. El dispositivo con la prioridad más alta proporciona el WDS.



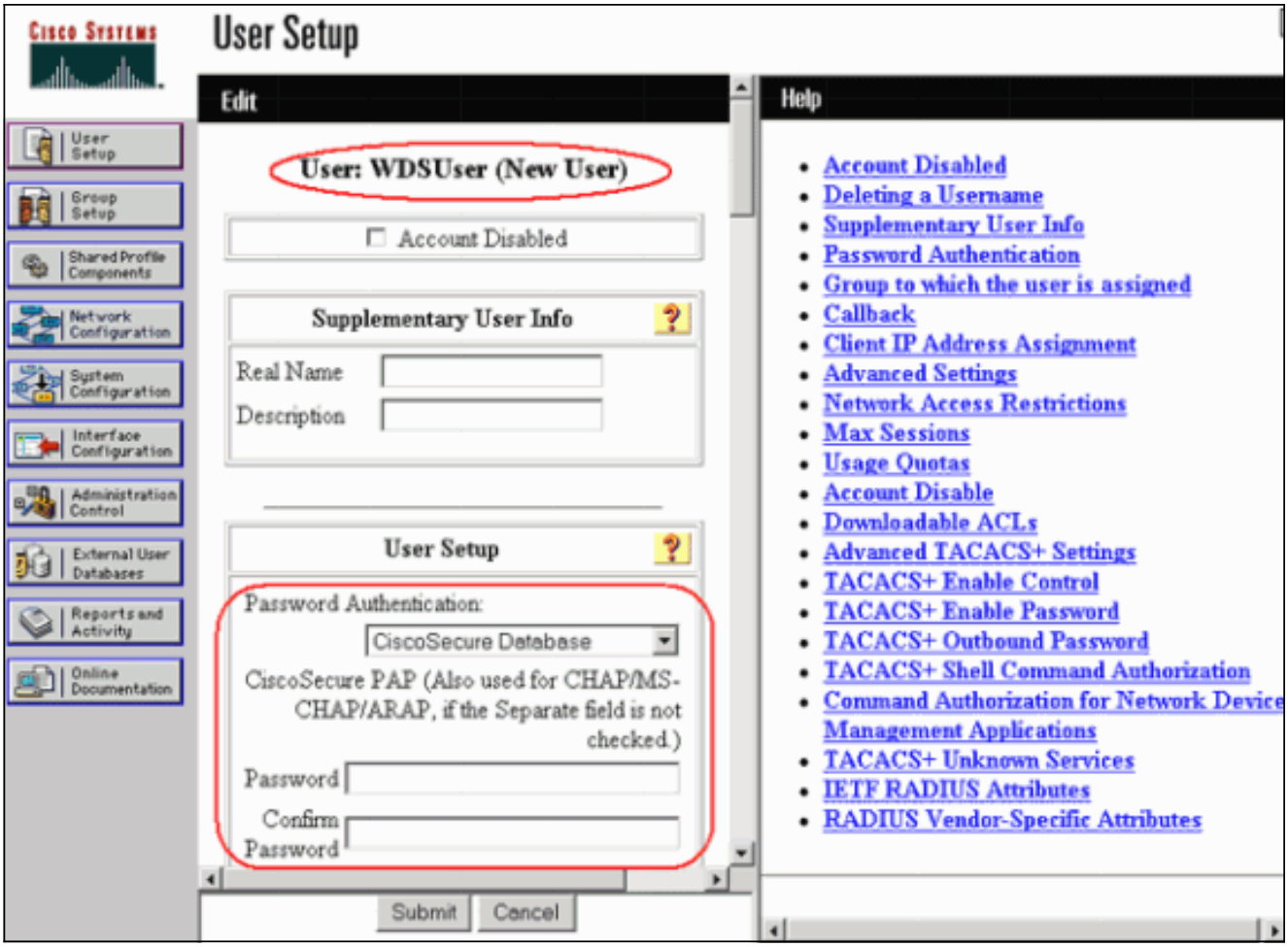
Alternativamente, publique estos comandos del CLI:

4. Elija los **Servicios inalámbricos > el WDS**, y vaya a la lengueta de los **grupos de servidores**:Defina un nombre de grupo de servidores que autentique los otros AP, un grupo de la infraestructura.Establezca Prioridad 1 para el servidor de autenticación configurado previamente.Haga clic al **grupo del uso para:** Botón de radio de la **autenticación de infraestructura**.Aplique las configuraciones a los identificadores relevantes del conjunto de servicio
(SSID).



Alternativamente, publique estos comandos del CLI:

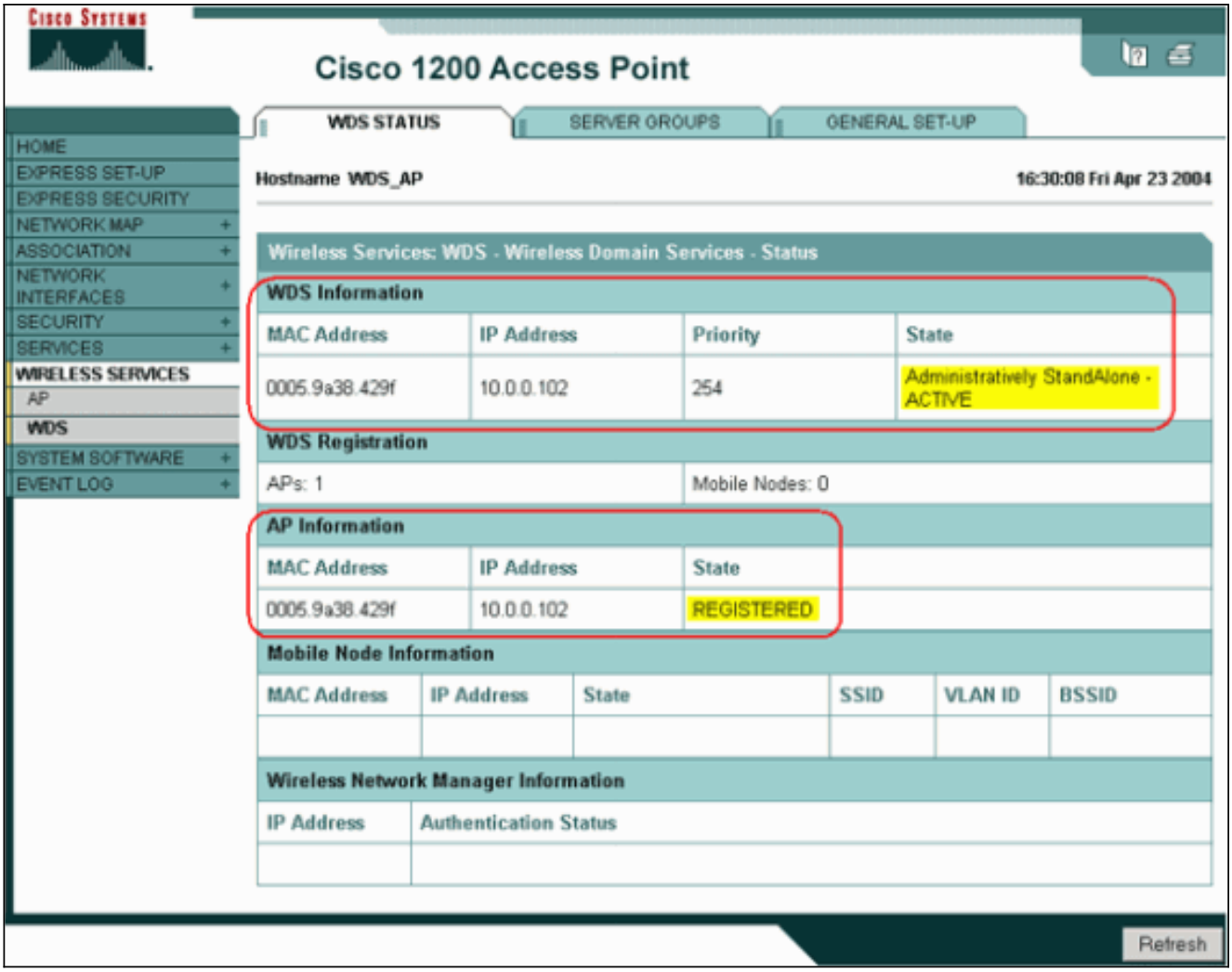
5. Configure el nombre y la contraseña de usuario WDS como usuario en su servidor de autenticación.En el Cisco Secure ACS, esto ocurre en la página de la configuración de usuario, donde usted define el nombre y la contraseña de usuario WDS. Para otros servidores de autenticación NON-ACS, refiera a la documentación del fabricante.**Nota:** No ponga al usuario WDS en un grupo que se asigne las muchas derechas y privilegios — el WDS requiere solamente la autenticación
limitada.



6. Elija los **Servicios inalámbricos > el AP**, y haga clic el **permiso** para el participar en la opción de la infraestructura swan. Entonces teclee el nombre de usuario y contraseña WDS.Debe definir un nombre de usuario y una contraseña de WDS en el servidor de autenticación para todos los dispositivos que sean designados miembros del WDS.

Alternativamente, publique estos comandos del CLI:

7. Elija los **Servicios inalámbricos > el WDS**. En la lengueta del estado WDS WDS AP, control si el WDS AP aparece en la área de información del WDS, en el estado ACTIVO. El AP debe también aparecer en la área de información AP, con el estado según lo REGISTRADO.Si el AP no aparece REGISTRADO o ACTIVO, marque al servidor de autenticación para cualquier error o la autenticación fallida intenta.Cuando el AP se registra apropiadamente, agregue una infraestructura AP para utilizar los servicios del WDS.



Alternativamente, publique estos comandos del CLI:**Nota:** Usted no puede las asociaciones del probar cliente porque la autenticación de cliente no tiene disposiciones todavía.

Señale un WLSM como WDS

Esta sección explica cómo configurar un WLSM como WDS. El WDS es el único dispositivo que comunica con el servidor de autenticación.

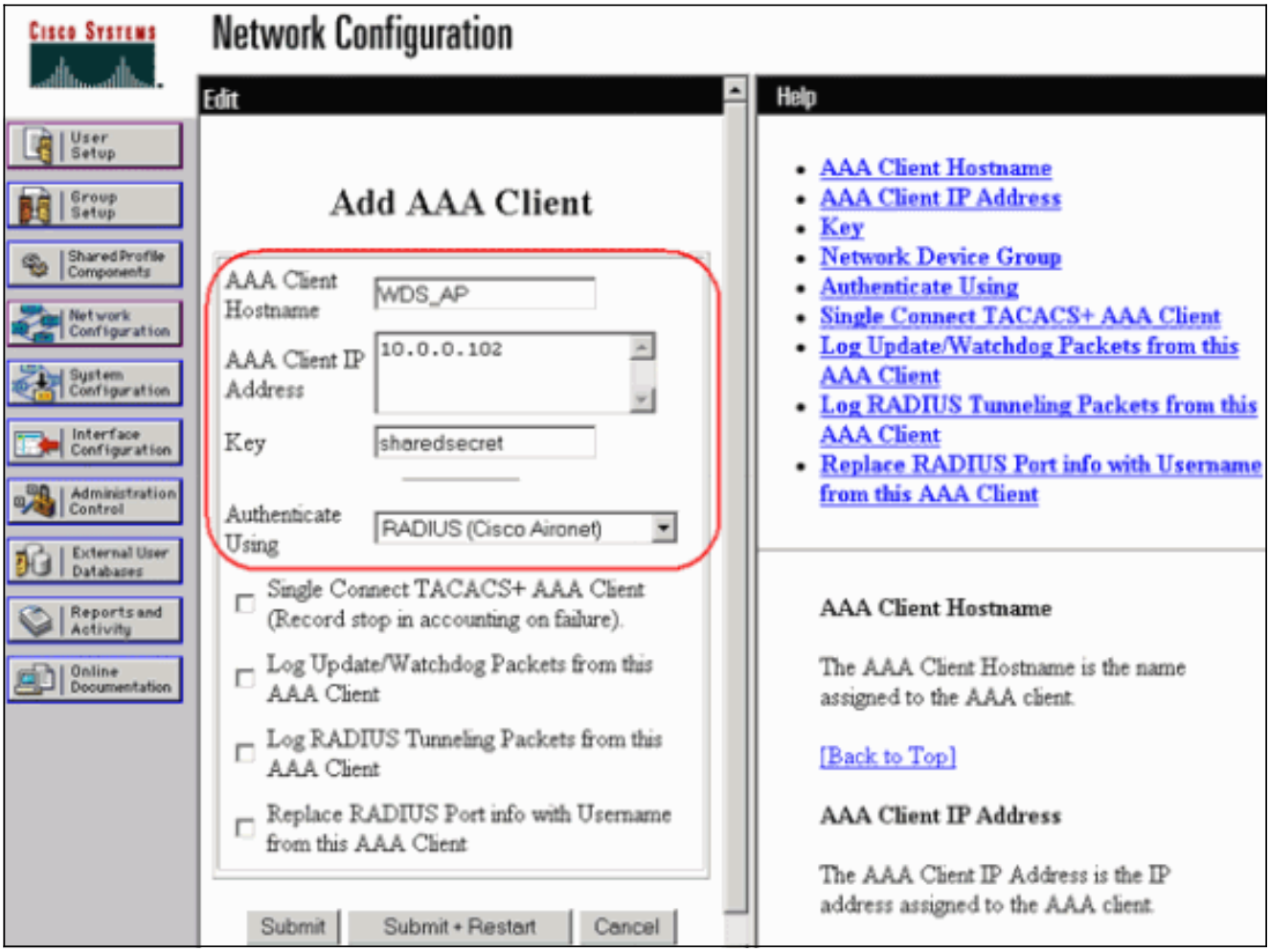
Nota: Publique estos comandos en el prompt de `comando enable del` WLSM, no del Supervisor Engine 720. Para conseguir al comando prompt del WLSM, publique estos comandos en un prompt de `comando enable` en el Supervisor Engine 720:

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

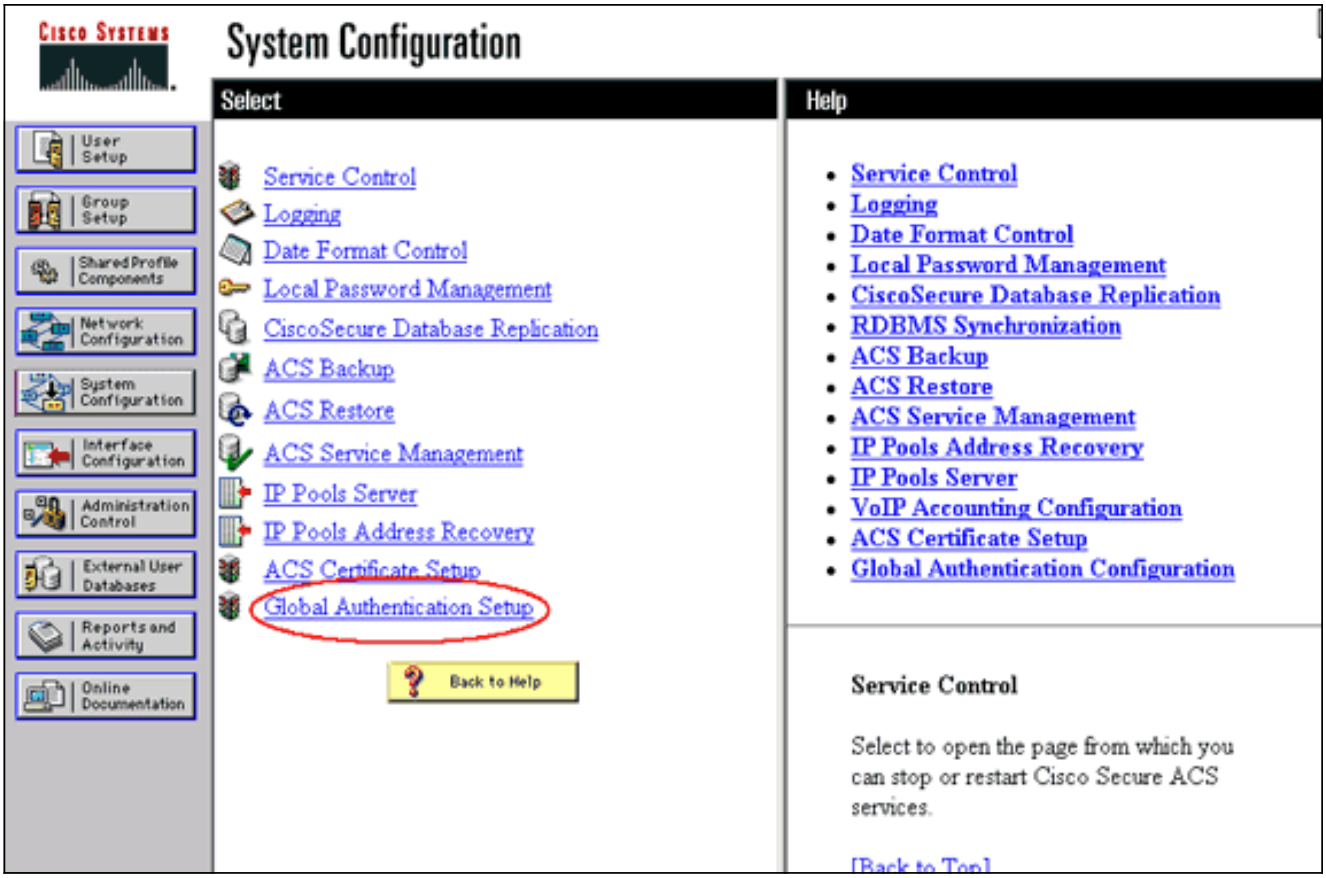
Nota: Para resolver problemas y mantener su WLSM más fácilmente, Acceso Remoto de Telnet de la configuración al WLSM. Consulte Configuración de acceso remoto de Telnet.

Para señalar un WLSM como WDS:

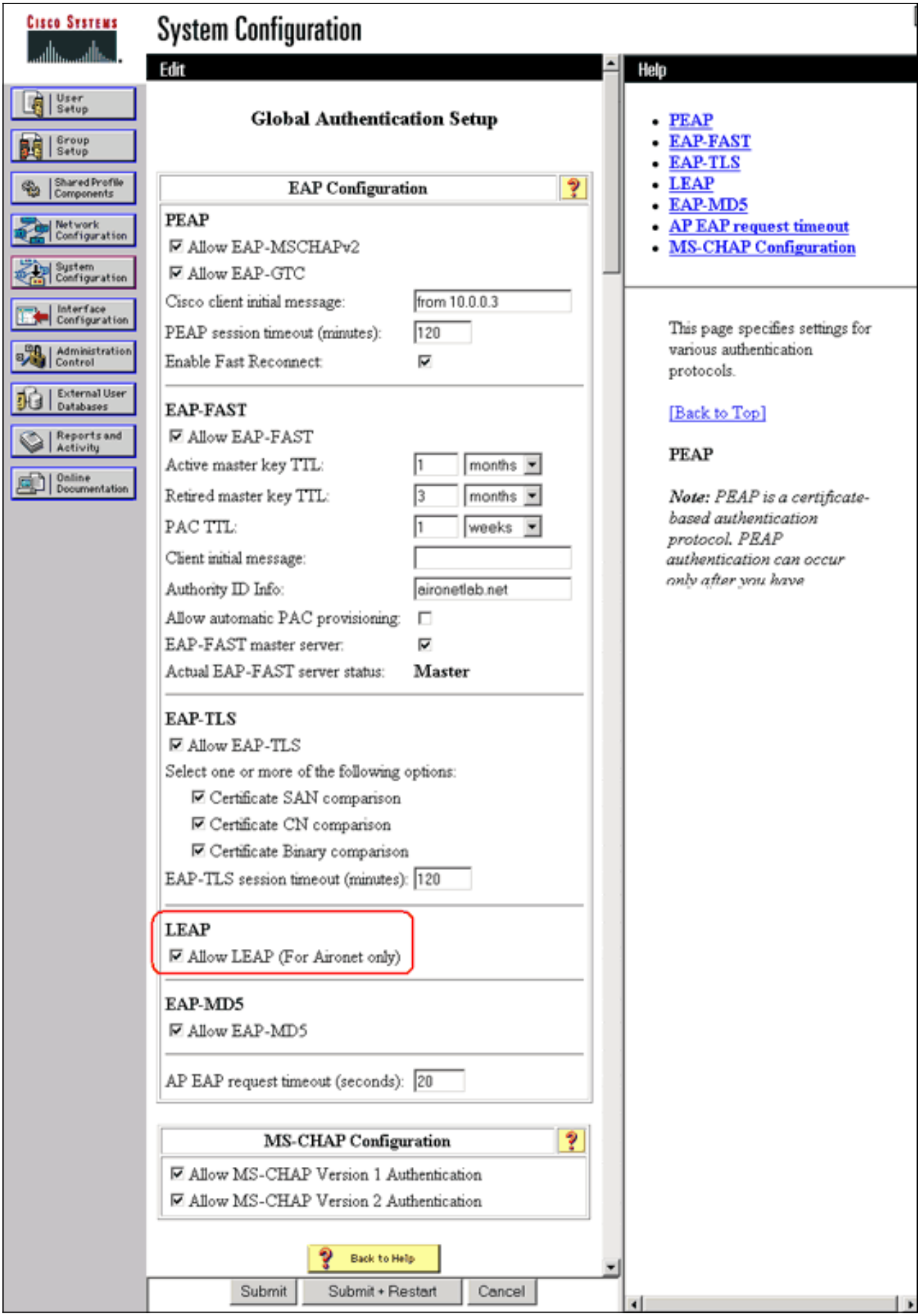
1. Del CLI del WLSM, publique estos comandos, y establezca una relación con el servidor de autenticación:**Nota:** No hay control de prioridad en WLSM. Si la red contiene los varios módulos WLSM, el WLSM utiliza la configuración de redundancia para determinar el módulo primario.
2. Configure el WLSM en el servidor de autenticación como cliente AAA.En el Cisco Secure ACS, esto ocurre en la página de la configuración de red donde usted define estos atributos para el WLSM:NombreDIRECCIÓN IPSecreto compartidoMétodo de autentificaciónRADIUS Cisco AironetRADIUS IETFPara otros servidores de autenticación NON-ACS, refiera a la documentación del
fabricante.



También, en el Cisco Secure ACS, configuración ACS para realizar la autenticación LEAP en la configuración del sistema - página de configuración de la autenticación global. Primero, la **configuración del sistema del** tecleo, entonces hace clic la **configuración de la autenticación**
global.



Navegue hacia abajo la página a la configuración del SALTO. Cuando usted examina la caja, ACS autentica
LEAP.



3. En el WLSM, defina un método que autentique los otros AP (grupo de servidores de la infraestructura).
4. En el WLSM, defina un método que autentique los dispositivos del cliente (grupo de servidor

del cliente) y qué EAP teclea el uso de esos clientes.**Nota:** Este paso elimina la necesidad del proceso del método de autenticación de cliente de la definición.

5. Defina un VLA N único entre el Supervisor Engine 720 y el WLSM para permitir que el WLSM comunique con las entidades exteriores como los AP y los servidores de autenticación. Esta VLAN no se utiliza en ningún otro lugar ni para ningún otro propósito en la red. Cree el VLA N en el Supervisor Engine 720 primero, después publique estos comandos:En el Supervisor Engine 720:En WLSM:
6. Verifique la función del WLSM con estos comandos:En WLSM:En el Supervisor Engine 720:

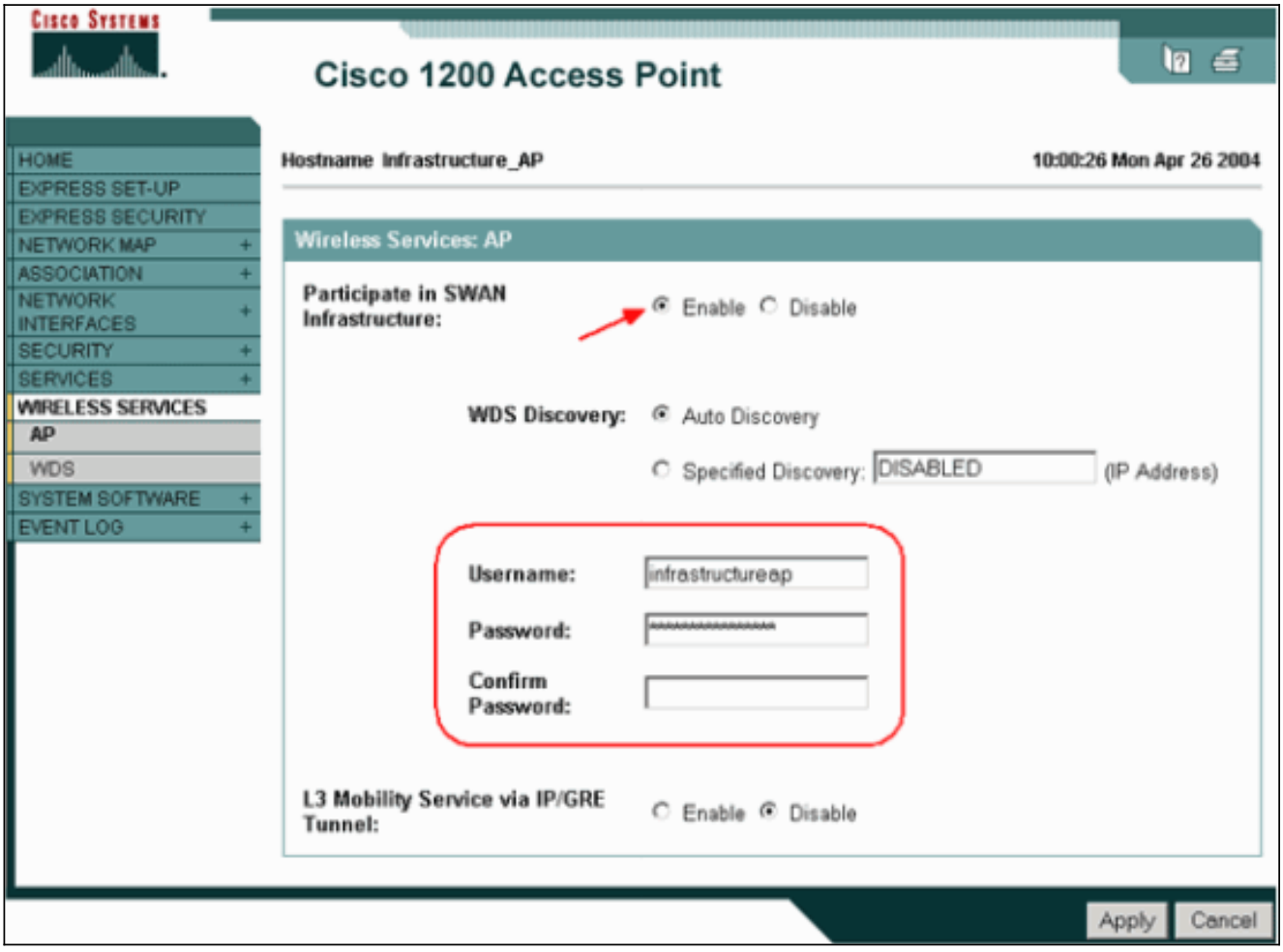
Señale un AP como dispositivo de infraestructura

Después, usted debe señalar por lo menos una infraestructura AP y relacionarse el AP con el WDS. Los clientes se asocian a la infraestructura AP. La infraestructura AP solicita el WDS AP o WLSM para realizar la autenticación para ellos.

Complete estos pasos para agregar una infraestructura AP que utilice los servicios del WDS:

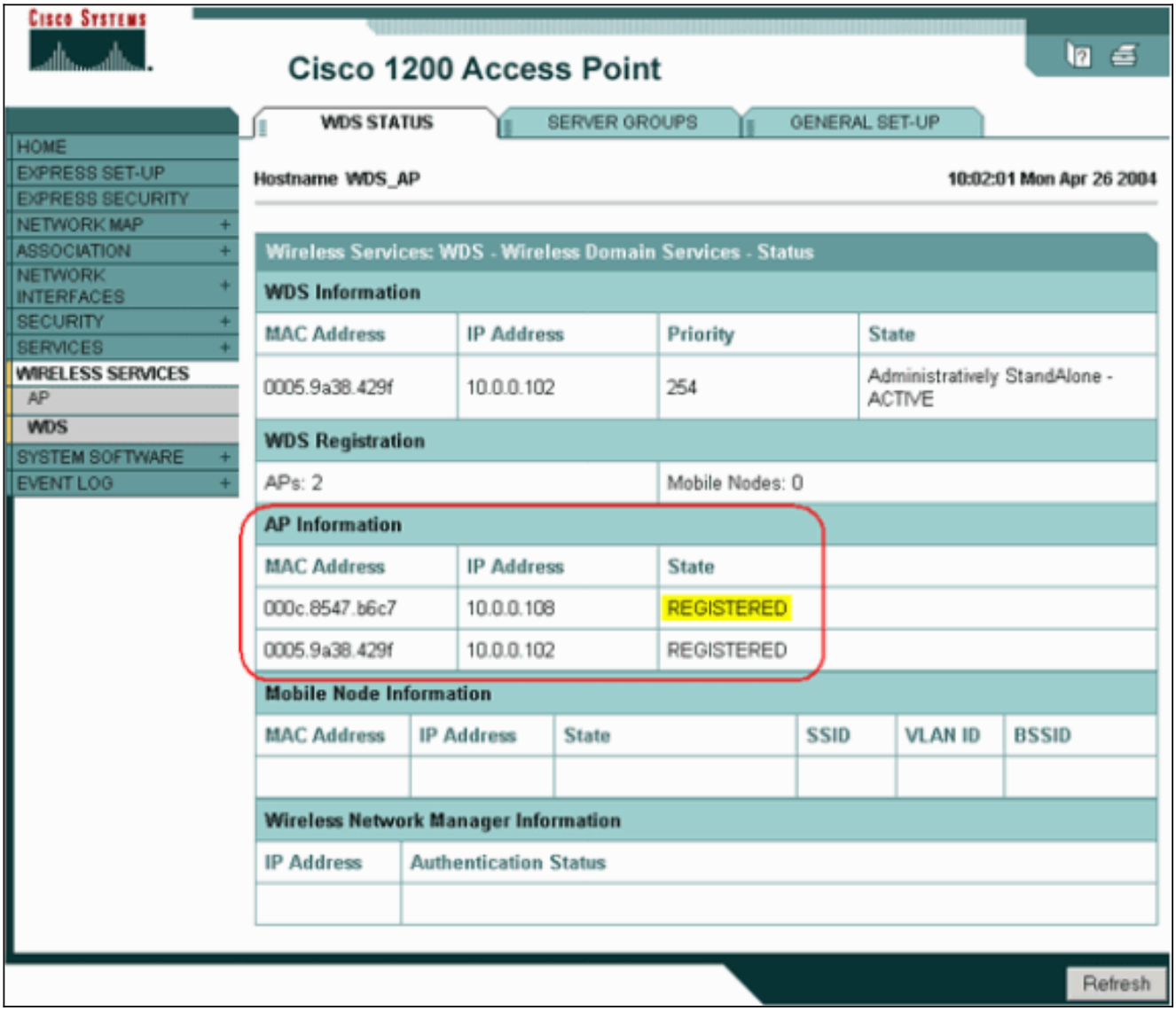
Nota: Esta configuración se aplica solamente a la infraestructura AP y no el WDS AP.

1. Elija los **Servicios inalámbricos > el AP**. En la infraestructura AP, seleccione el **permiso** para la opción de Servicios inalámbricos. Entonces teclee el nombre de usuario y contraseña WDS.Debe definir un nombre de usuario y contraseña WDS en el servidor de autenticación para todos los dispositivos que serán miembros de WDS.



Alternativamente, publique estos comandos del CLI:

2. Elija los **Servicios inalámbricos > el WDS**. En la lengueta del estado WDS WDS AP, la nueva infraestructura AP aparece en la área de información del WDS, con el estado como ACTIVE, y en la área de información AP, con el estado según lo REGISTRADO.Si el AP no aparece ACTIVO y/o REGISTRADO, marque al servidor de autenticación para cualquier error o la autenticación fallida intenta.Después de que el AP aparezca ACTIVO y/o REGISTRADO, agregue un método de autenticación de cliente al
WDS.



Alternativamente, publique este comando del CLI:Alternativamente, publique este comando del WLSM:Entonces, publique este comando en la infraestructura AP:**Nota:** Usted no puede las asociaciones del probar cliente porque la autenticación de cliente no tiene disposiciones todavía.

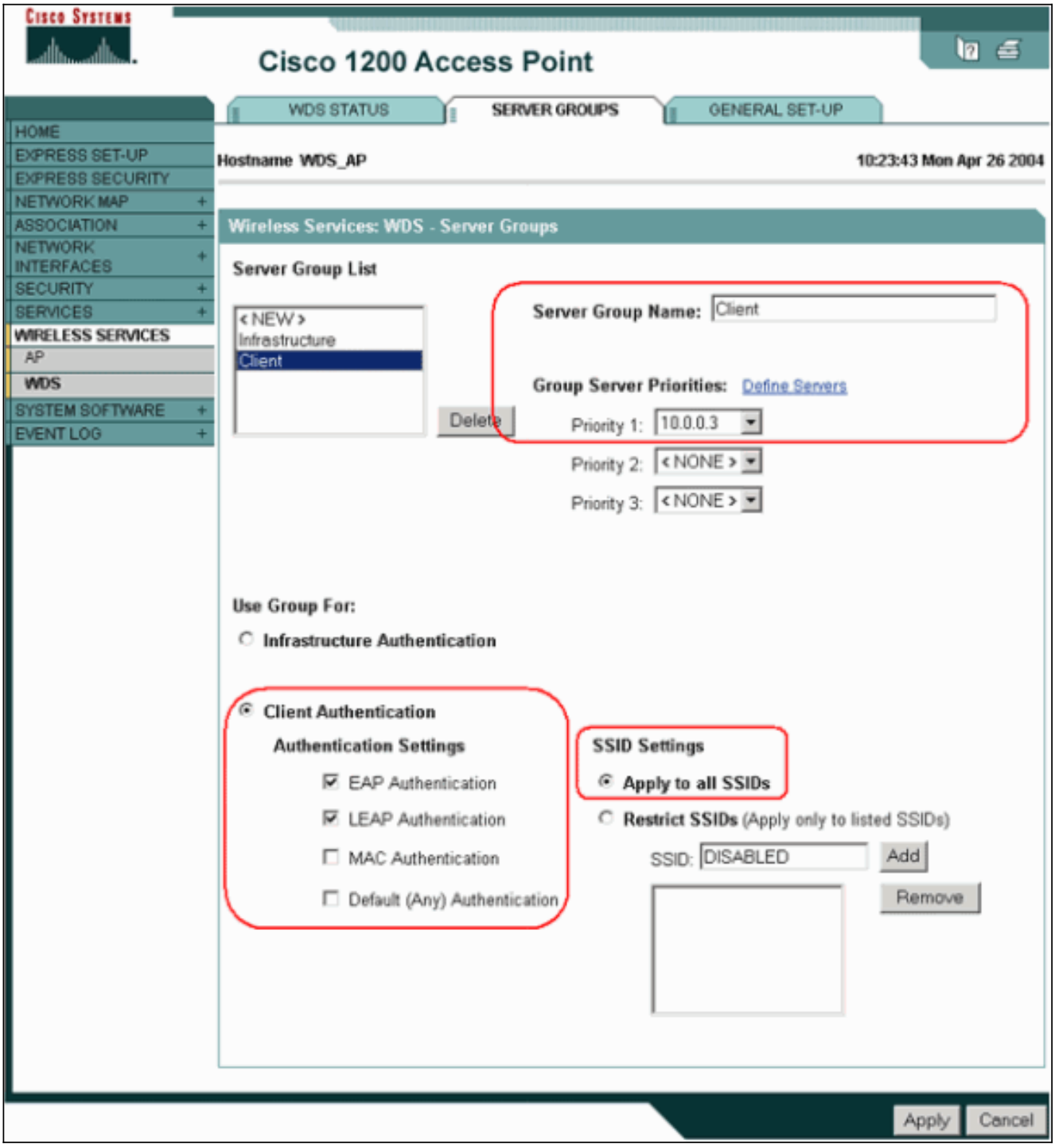
Defina el método de autenticación de cliente

Finalmente, defina un método de autenticación de cliente.

Complete estos pasos para agregar un método de autenticación de cliente:

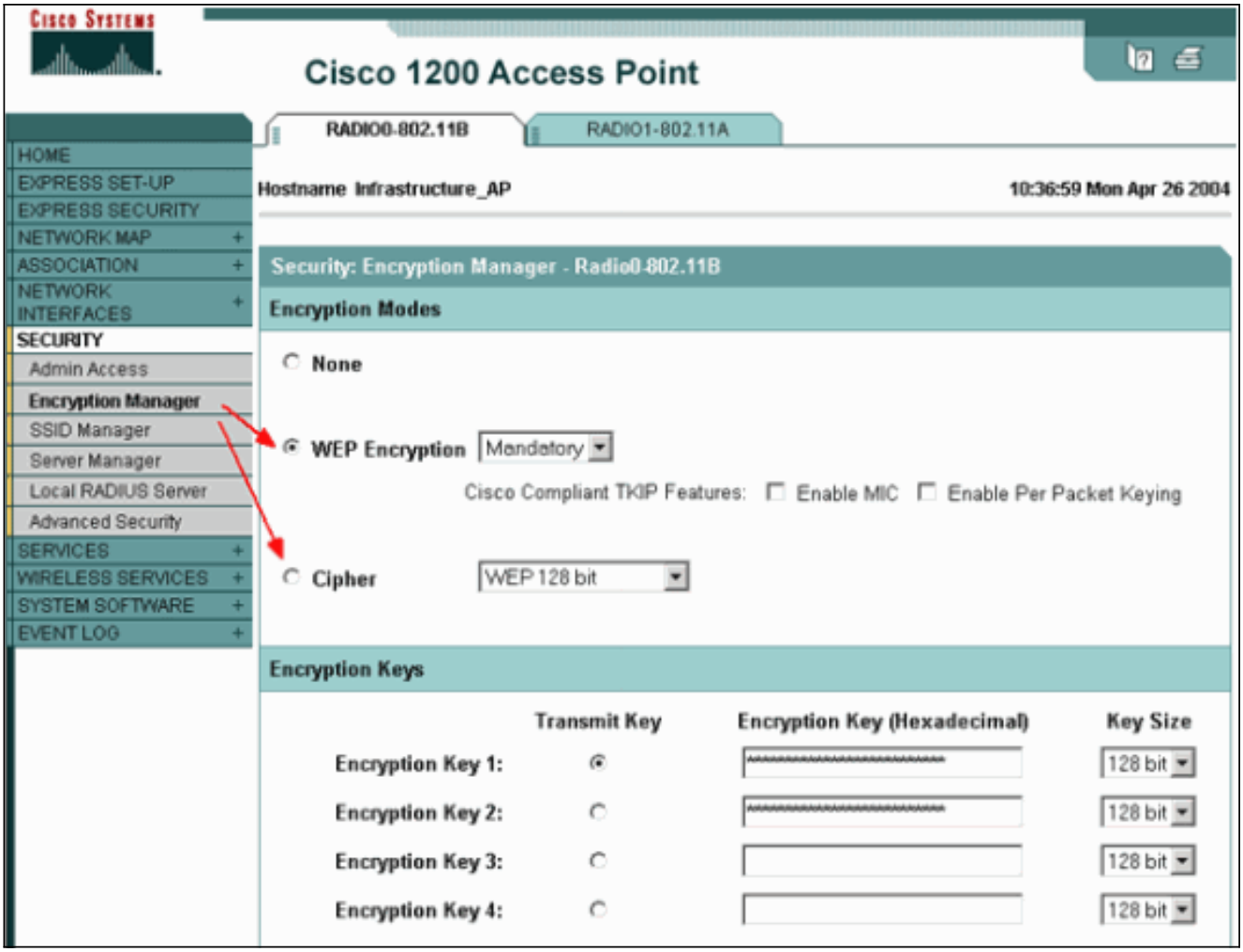
1. Elija los **Servicios inalámbricos > el WDS**. Realice estos pasos en la lengueta de los grupos de servidores WDS AP:Defina a un grupo de servidores que autentique a los clientes (Grupo de clientes).Establezca Prioridad 1 para el servidor de autenticación configurado

previamente.Fije el tipo de autenticación correspondiente (SALTO, EAP, MAC, y así sucesivamente).Aplique las configuraciones a los SSID relevantes.

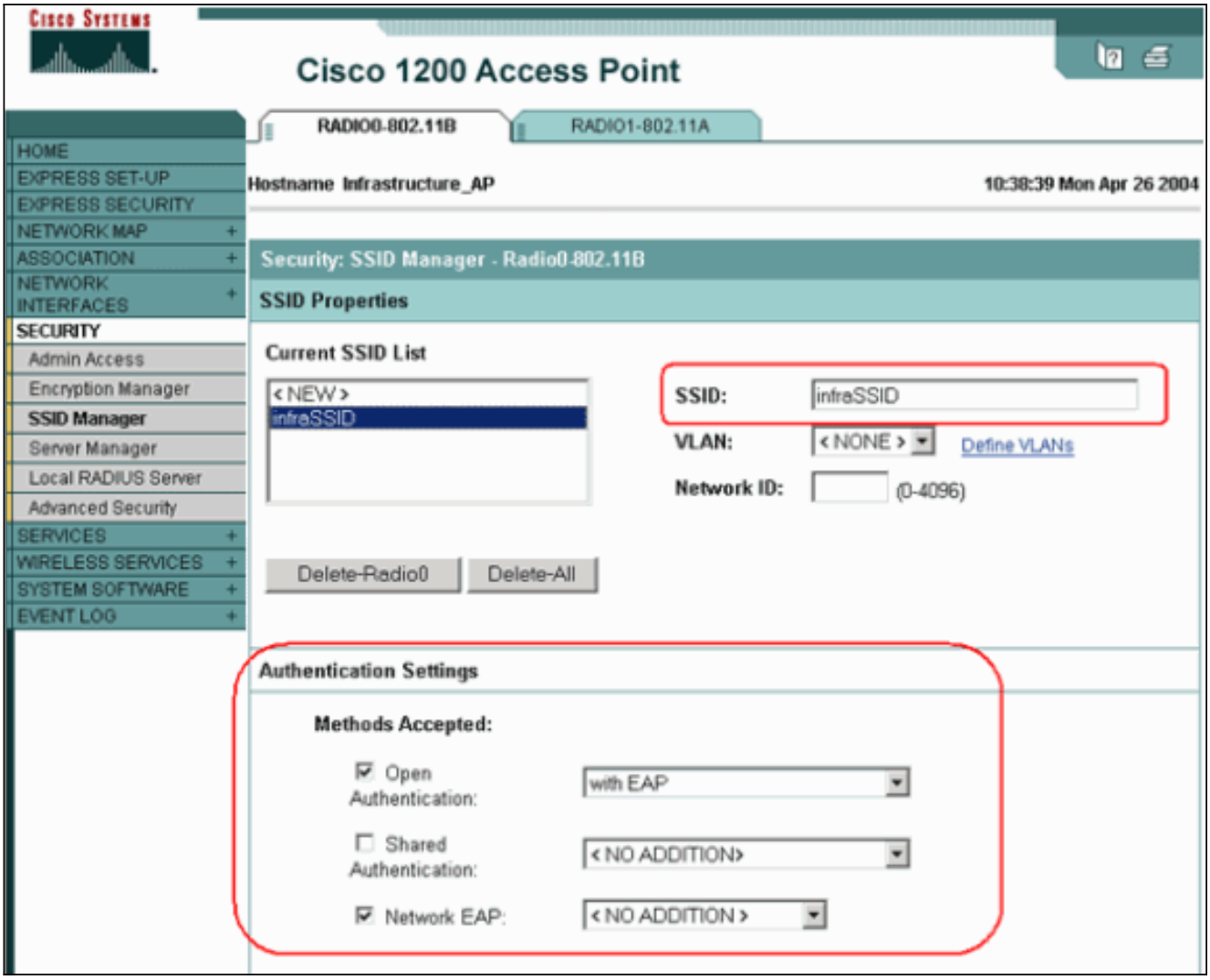


Alternativamente, publique estos comandos del CLI:**Nota:** El ejemplo WDS AP es dedicado y no valida las asociaciones del cliente.**Nota:** No configure en la infraestructura AP para los grupos de servidores porque la infraestructura AP transmite a cualquier petición el WDS de ser procesado.

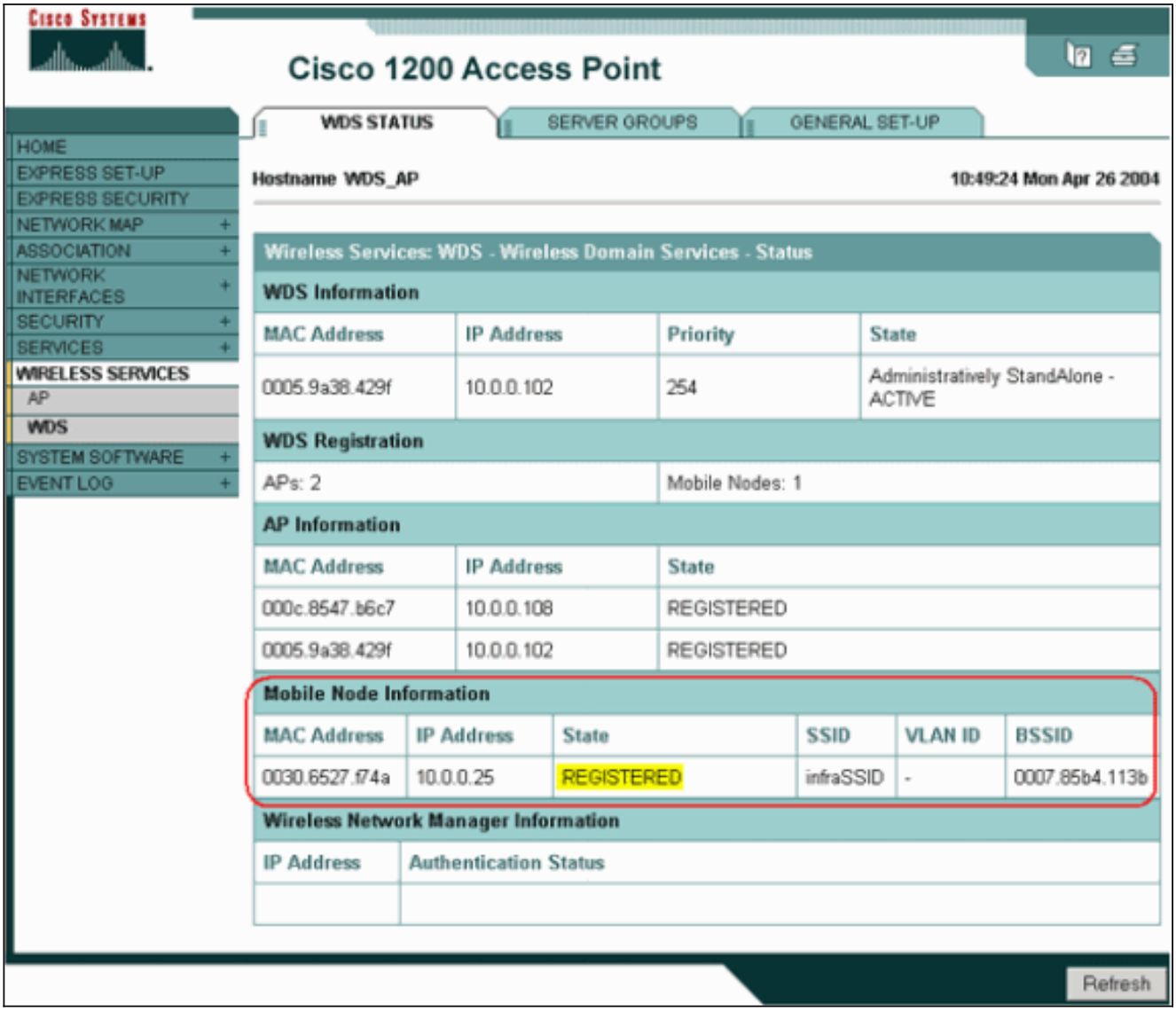
2. En la infraestructura AP o AP:Bajo la **Seguridad > el** elemento de menú del **administrador del cifrado**, la **encripción WEP** o **cifra del** tecleo, de acuerdo con del protocolo de autenticación usted utiliza.



Conforme al elemento de menú de la **Seguridad > del administrador SSID**, métodos de autentificación selectos de acuerdo con del protocolo de autenticación que usted utiliza.



3. Usted puede ahora probar con éxito si los clientes autentican a la infraestructura AP. El AP del WDS en la lengueta del estado WDS (conforme a los **Servicios inalámbricos > al** elemento de menú **WDS**) indica que el cliente aparece en la área de información del nodo móvil y tiene un estado REGISTRADO.Si no aparece el cliente, marque al servidor de autenticación para cualquier error o la autenticación fallida intenta por los clientes.



Alternativamente, publique estos comandos del CLI:**Nota:** Si usted necesita el debug authentication, asegúrese de que usted haga el debug de en el WDS AP, porque el WDS AP es el dispositivo que comunica con el servidor de autenticación.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de la configuración. Esta lista muestra algunas de las preguntas comunes relacionadas con el comando WDS para aclarar más lejos la utilidad de estos comandos:

- **Pregunta: ¿En el WDS AP, cuáles son las configuraciones recomendadas para estos elementos?descanso del radio-servidordeadtime del radio-servidorTiempo del holdoff del error del Message Integrity Check del Temporal Key Integrity Protocol (TKIP) (MIC)Tiempo del rechazo de clienteIntervalo del Reauthentication EAP o MACDescanso de los clientes EAP (opcional)Respuesta:** Se sugiere que usted guarda la configuración con las configuraciones predeterminadas con respecto a estas configuraciones especiales, y las

utiliza solamente cuando hay un problema con respecto a la sincronización.Éstas son las configuraciones recomendadas para el WDS AP:**Descanso del radio-servidor de la** neutralización. Éste es el número de segundos las esperas AP para una contestación a un pedido de RADIUS antes de que vuelva a enviar la petición. El valor por defecto es 5 segundos.**Deadtime del radio-servidor de la** neutralización. El RADIUS es saltado por los pedidos adicionales la duración de los minutos a menos que todos los servidores sean muertos marcados.El tiempo del holdoff del error TKIP MIC se habilita por abandono a 60 segundos. Si usted habilita el tiempo del holdoff, usted puede ingresar el intervalo en los segundos. Si el AP detecta dos errores MIC en el plazo de 60 segundos, bloquea a todos los clientes TKIP en esa interfaz para el período de tiempo del holdoff especificado aquí.El tiempo del rechazo de cliente se debe inhabilitar por abandono. Si usted habilita el holdoff, ingrese el número de segundos que el AP deba esperar después de que procesen a una falla de autenticación antes de una petición de la autenticación subsiguiente.El intervalo del Reauthentication EAP o MAC se inhabilita por abandono. Si usted habilita el reauthentication, usted puede especificar el intervalo o validar el intervalo dado por el servidor de autenticación. Si usted elige especificar el intervalo, ingrese el intervalo en los segundos que el AP espera antes de que fuerce a un cliente autenticado a reauthenticate.El descanso de los clientes EAP (opcional) es 120 segundos por abandono. Ingrese la cantidad de tiempo que el AP debe esperar a los clientes de red inalámbrica para responder a las peticiones de la autenticación EAP.

- **Pregunta: Con respecto al tiempo del holdoff TKIP, leí que esto se debe fijar al ms 100 y a no 60 segundos. ¿Asumo que está fijada al segundo del navegador porque ése es el número más bajo que usted puede selecto?Respuesta:** No hay recomendación específica de fijarla al ms 100 a menos que haya un error señalado donde está aumentar la única solución este vez. El segundo es la configuración más baja.
- **Pregunta: ¿Hace la autenticación de cliente de estos dos comandos help de manera y son necesarios en el WDS o la infraestructura AP?en-para-login-auth del atributo 6 del radio-servidoratributo 6 del radio-servidor soporte-múltipleRespuesta:** Estos comandos no ayudan al proceso de autenticación y no se necesitan en el WDS o el AP.
- **Pregunta: En la infraestructura AP, asumo que ningunas de las configuraciones del administrador de servidor y de las Propiedades Globales son necesarias porque el AP recibe la información del WDS. ¿Ninguno de estos comandos del específico se necesitan para la infraestructura AP?en-para-login-auth del atributo 6 del radio-servidoratributo 6 del radio-servidor soporte-múltipledescanso del radio-servidordeadtime del radio-servidorRespuesta:** No hay necesidad de tener el administrador de servidor y Propiedades Globales para la infraestructura AP. El WDS toma el cuidado de esa tarea y no hay necesidad de tener estas configuraciones:**en-para-login-auth del atributo 6 del radio-servidoratributo 6 del radio-servidor soporte-múltipledescanso del radio-servidordeadtime del radio-servidor**Sigue habiendo por abandono y se requiere la configuración del **formato %h del incluir-en-acceso-req del atributo 32 del radio-servidor**.

Un AP es un dispositivo de la capa 2. Por lo tanto, el AP no soporta la movilidad de la capa 3 cuando el AP se configura para actuar como dispositivo WDS. Usted puede alcanzar la movilidad de la capa 3 solamente cuando usted configura el WLSM como el dispositivo WDS. Refiera a la sección de la *arquitectura de la movilidad de la capa 3 del* Módulo de servicios del Wireless LAN de las Cisco Catalyst 6500 Series: White Paper para más información.

Por lo tanto, cuando usted configura un AP como dispositivo WDS, no utilice el **comando mobility network-id**. Este comando se aplica para acodar 3 movilidad y usted necesita tener un WLSM

mientras que su dispositivo WDS para configurar correctamente la movilidad de la capa 3. Si usted utiliza el **comando mobility network-id** incorrectamente, usted puede ver algunos de estos síntomas:

- Los clientes de red inalámbrica no pueden asociarse al AP.
- Los clientes de red inalámbrica pueden asociarse al AP, pero no reciben una dirección IP del servidor DHCP.
- Un teléfono inalámbrico no se autentica cuando usted tiene una Voz sobre el despliegue de WLAN.
- La autenticación EAP no ocurre. Con la red-**identificación de la movilidad** configurada, el AP intenta construir un túnel del Generic Routing Encapsulation (GRE) para remitir los paquetes EAP. Si no se establece ningún túnel, los paquetes no van dondequiera.
- Un AP configurado como dispositivo WDS no funciona como se esperaba, y la configuración WDS no trabaja.**Nota:** Usted no puede configurar el AP/bridge del Cisco Aironet 1300 como master WDS. Los 1300 AP/bridge no soportan estas funciones. Los 1300 AP/bridge pueden participar en una red WDS mientras que un dispositivo de infraestructura en el cual algún otro AP o WLSM se configure como master WDS.

Comandos para resolución de problemas

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.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **haga el debug del authenticator todo aaa del dot11** — Muestra a diversas negociaciones que va un cliente a través mientras que el cliente se asocia y autentica con el 802.1x o el proceso EAP. Este debug fue introducido en el Cisco IOS Software Release 12.2(15)JA. Este comando toma obsoleto el comando debug dot11 aaa dot1x en esa versión y en las posteriores.
- **autenticación aaa del debug** — Muestra el proceso de autenticación de una perspectiva genérica AAA.
- **wlccp ap del debug** — Muestra que las negociaciones WLCCP implicadas como AP se unen a un WDS.
- **paquete del wlccp del debug** — Muestra la información detallada sobre las negociaciones WLCCP.
- **salto-cliente del wlccp del debug** — Muestra los detalles mientras que un dispositivo de infraestructura se une a un WDS.

Información Relacionada

- Configurando el WDS, ayune itinerancia segura, y Administración de la radio
- Nota de configuración del Módulo de servicios del Wireless LAN de las Catalyst 6500 Series
- Configuración de conjuntos Cipher y WEP
- Configuración de los tipos de autenticación
- Páginas de soporte de LAN inalámbrica
- Soporte Técnico y Documentación - Cisco Systems