

El dominio de red inalámbrica mantiene el AP como ejemplo de configuración del servidor AAA

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Configure el WDS AP](#)

[Configure la infraestructura AP](#)

[Configure el método de autenticación de cliente](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento suministra una configuración de ejemplo para configurar un Punto de Acceso (AP) para:

- Proporcione al Wireless Domain Services (WDS).
- Realice el papel de un servidor del Authentication, Authorization, and Accounting (AAA).

Usted puede utilizar esta clase de disposición cuando usted no tienen un servidor de RADIUS externo para autenticar la infraestructura APs y los dispositivos cliente que participan en WDS.

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de WDS
- 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.

- Cisco Aironet de la serie 1200 APs que funciona con el Software Release 12.3(7)JA1 de Cisco IOS®

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

WDS es una parte de la red Tecnología inalámbrica-enterada estructurada Cisco (CISNE). WDS es una colección de Características del Software Cisco IOS que aumenten la movilidad del cliente LAN de la Tecnología inalámbrica (red inalámbrica (WLAN)) y simplifiquen el despliegue y la Administración de la red inalámbrica (WLAN).

WDS es la base para muchas características tales como rápido asegura la itinerancia, acoda la movilidad 3, y la Administración de la radio.

Refiera a [configurar WDS, rápido aseguran la itinerancia, la Administración de radio, y los servicios inalámbricos de la detección de intrusos](#) para más información sobre estas características.

Uno de los propósitos principales de WDS es ocultar los credenciales de usuario en la primera autenticación del cliente por el servidor de la autenticación. En los intentos subsiguientes, WDS autentica al cliente en base de la información ocultada. Para lograr esto:

- Uno de los APs se debe configurar como WDS AP.
- Otros APs se deben configurar como infraestructura APs que comunican al WDS AP.
- WDS AP debe establecer una relación con el servidor de la autenticación autenticando a él con un nombre de usuario y contraseña WDS.

Este servidor de la autenticación valida las credenciales de la infraestructura APs y los clientes cuando estos dispositivos autentican por primera vez. El servidor de la autenticación puede ser servidor de RADIUS externo o el servidor de RADIUS local en el WDS AP.

Los WDS y la infraestructura APs comunican sobre un protocolo del Multicast llamado el protocolo del control del contexto LAN de la Tecnología inalámbrica (WLCCP). Estos mensajes de multidifusión no pueden ser encaminados. Por lo tanto, un WDS y una infraestructura asociada APs deben estar en el mismo red secundario IP y en el mismo segmento de LAN.

Este documento explica cómo utilizar la característica local del servidor de RADIUS en el WDS AP para realizar la validación de las credenciales.

Configurar

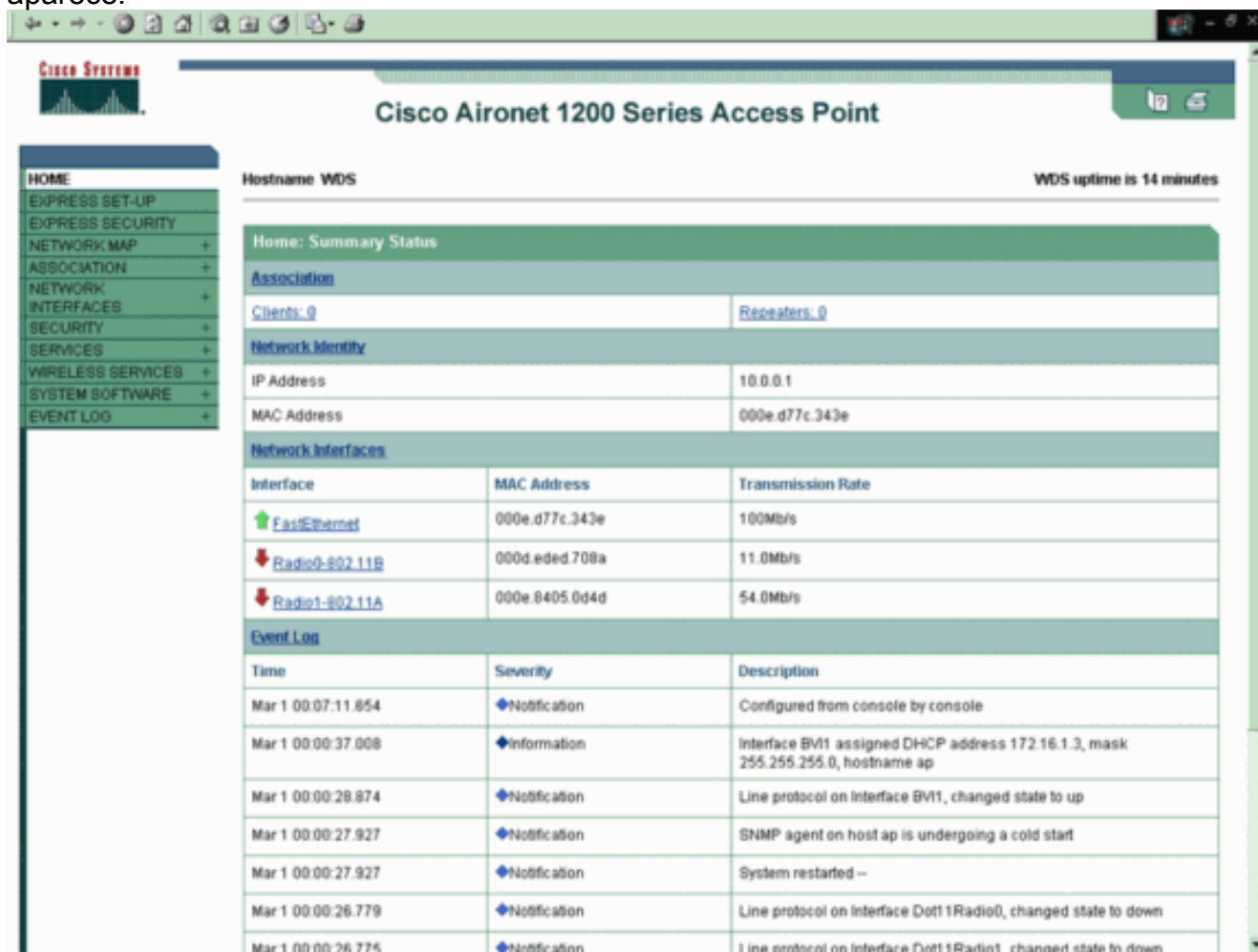
[Configure el WDS AP](#)

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

Para configurar el AP para servir como WDS AP con la funcionalidad de servidor AAA, usted debe primero activar la característica local del servidor de RADIUS en el AP.

Complete estos pasos:

1. Ábrase una sesión al AP a través del GUI. La página sumaria del estatus aparece.



The screenshot shows the Cisco Aironet 1200 Series Access Point GUI. The main title is "Cisco Aironet 1200 Series Access Point". The hostname is "WDS" and the WDS uptime is "14 minutes". The page is titled "Home: Summary Status".

Association

Clients: 0	Repeaters: 0
------------	--------------

Network Identity

IP Address	10.0.0.1
MAC Address	000e.d77c.343e

Network Interfaces

Interface	MAC Address	Transmission Rate
FastEthernet	000e.d77c.343e	100Mb/s
Radio0-802.11B	000d.eded.708a	11.0Mb/s
Radio1-802.11A	000e.8405.0d4d	54.0Mb/s

Event Log

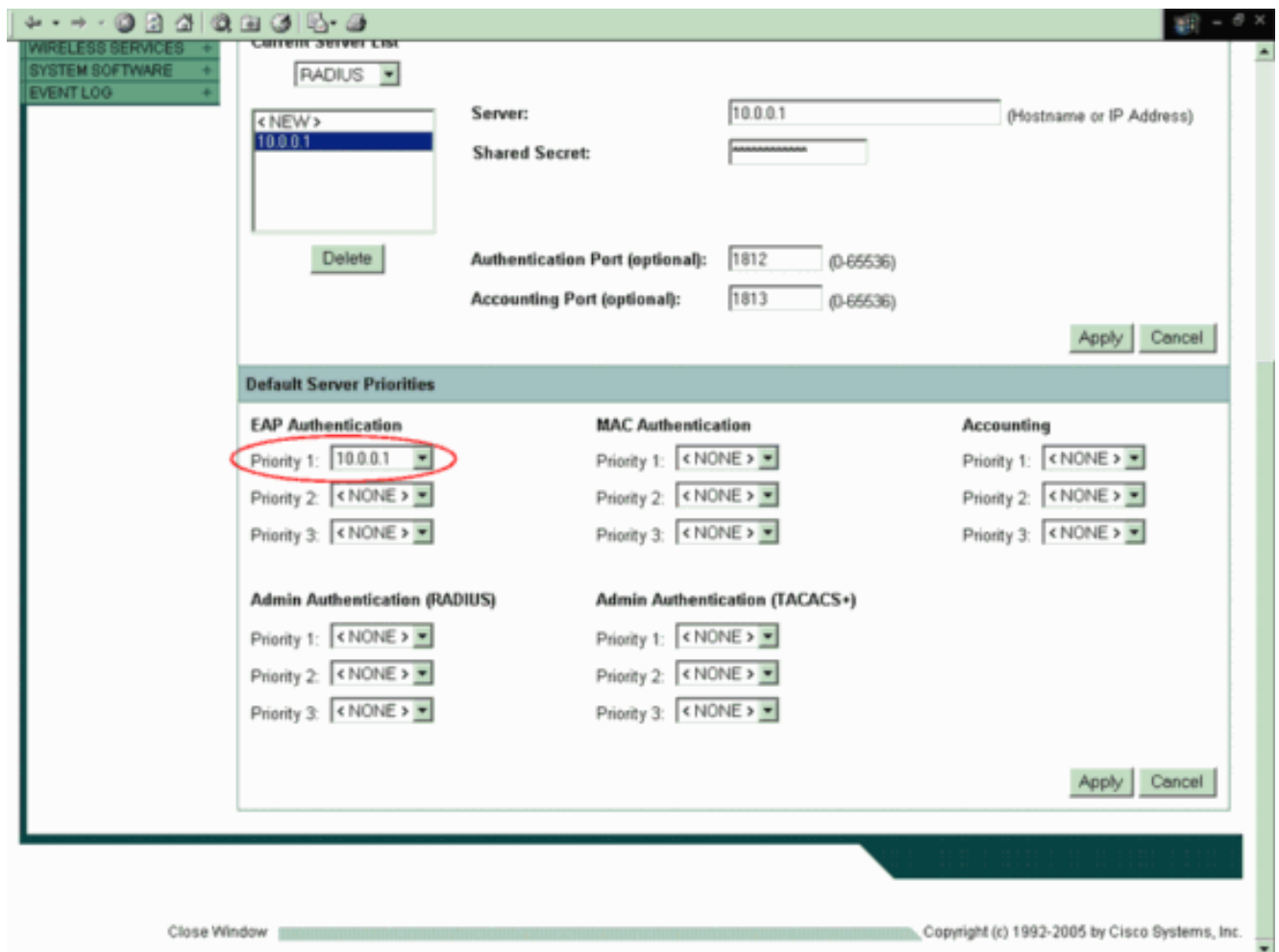
Time	Severity	Description
Mar 1 00:07:11.854	Notification	Configured from console by console
Mar 1 00:00:37.008	Information	Interface BVI1 assigned DHCP address 172.16.1.3, mask 255.255.255.0, hostname ap
Mar 1 00:00:28.874	Notification	Line protocol on interface BVI1, changed state to up
Mar 1 00:00:27.927	Notification	SNMP agent on host ap is undergoing a cold start
Mar 1 00:00:27.927	Notification	System restarted --
Mar 1 00:00:26.779	Notification	Line protocol on interface Dot11Radio0, changed state to down
Mar 1 00:00:26.775	Notification	Line protocol on interface Dot11Radio1, changed state to down

2. Seleccione la **Seguridad > al administrador de servidor del** menú del lado izquierdo en el AP.
3. Ingrese el IP address y el secreto compartido del AP que actúa como el servidor de RADIUS bajo los servidores corporativos. En este caso ingrese el IP address del WDS AP puesto que el WDS AP va a actuar como el servidor de RADIUS. El ejemplo utiliza a la dirección IP 10.0.0.1. Puesto que esto es servidor de RADIUS local usted debe utilizar 1812 y 1813 mientras que los puertos de la autenticación y el considerar como este ejemplo muestran.
4. Haga clic en Apply (Aplicar).

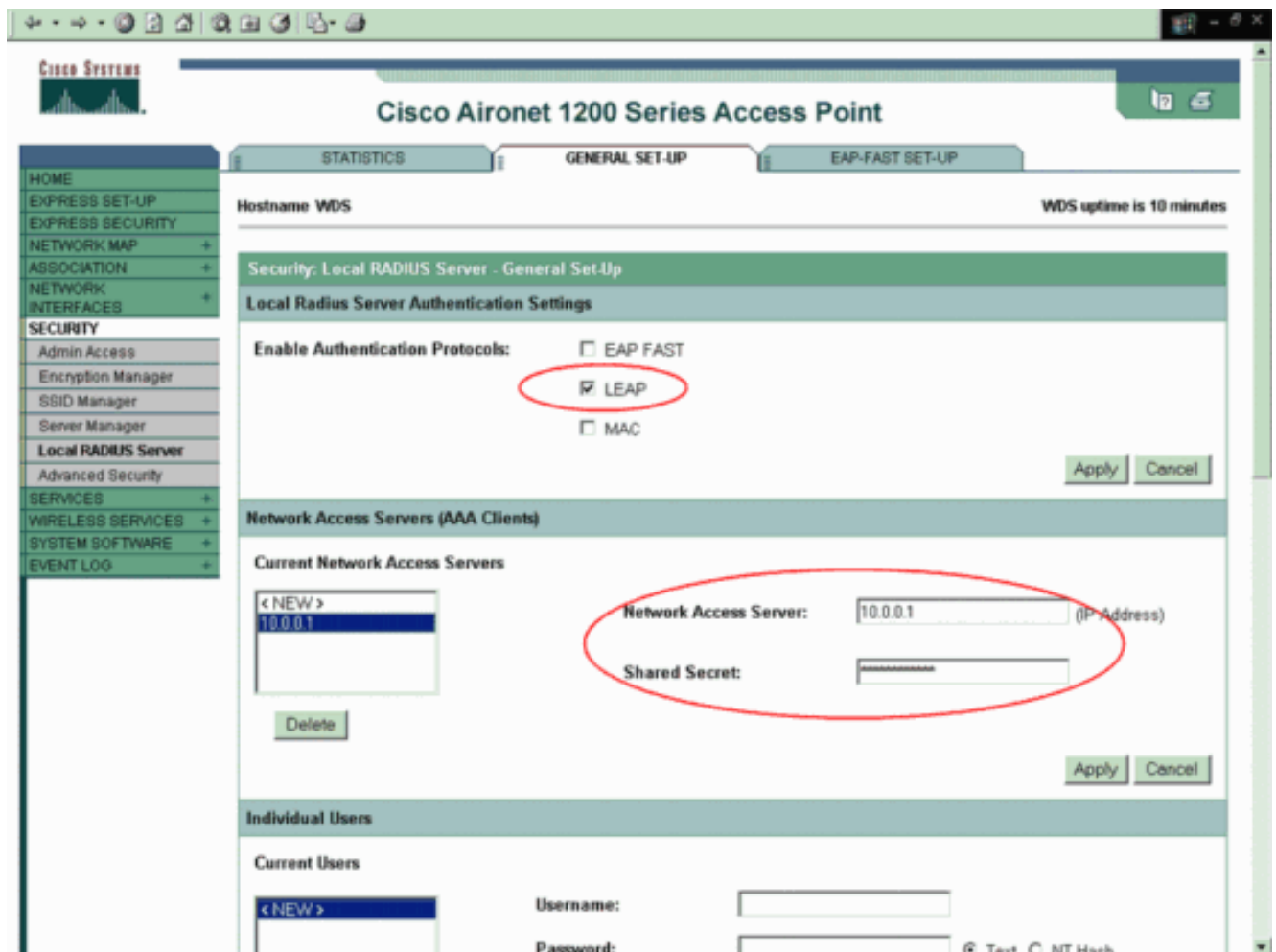
The screenshot displays the configuration interface for a Cisco Aironet 1200 Series Access Point. The main title is "Cisco Aironet 1200 Series Access Point". The left sidebar contains a navigation menu with categories like HOME, EXPRESS SET-UP, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The "Server Manager" section is active, showing "SERVER MANAGER" and "GLOBAL PROPERTIES" tabs. The hostname is "WDS" and the uptime is "8 minutes".

The "Security: Server Manager" section includes a "Backup RADIUS Server" configuration with fields for "Backup RADIUS Server" (Hostname or IP Address) and "Shared Secret". Below this is the "Corporate Servers" section, which has a "Current Server List" dropdown set to "RADIUS". A table lists a server with IP "10.0.0.1". The "Server" and "Shared Secret" fields for this server are circled in red. Below the table, the "Authentication Port (optional)" is set to "1812" and the "Accounting Port (optional)" is set to "1813", both also circled in red. At the bottom, the "Default Server Priorities" section shows "EAP Authentication", "MAC Authentication", and "Accounting" with "Priority 1" set to "< NONE >".

5. Seleccione la dirección IP WDS APs como **prioridad 1** bajo prioridades del servidor del valor por defecto para la autenticación EAP. Haga clic en Apply (Aplicar). Esto permite que el servidor de RADIUS local sea la primera opción para la infraestructura de autenticación APs y los clientes.



6. Seleccione la **Seguridad > servidor de RADIUS local** del menú del lado izquierdo. Haga clic la **disposición general** para configurar los parámetros locales del servidor de RADIUS. Seleccione el **SALTO** bajo configuraciones locales de la autenticación de servidor de RADIUS y el tecleo **se aplica**. Ingrese el IP address del WDS AP y una contraseña secreta compartida bajo los servidores del acceso a la red. Este ejemplo utiliza la contraseña del secreto compartido como **test123**. Haga clic en **Apply** (Aplicar).



- Ingrese el nombre de usuario y contraseña de toda la infraestructura APs y de los clientes que comuniquen con el WDS AP bajo los usuarios individuales. Haga clic en Apply (Aplicar). Este ejemplo incluye el nombre de usuario y contraseña de la infraestructura AP que usted configura para registrar con el WDS AP. Este ejemplo utiliza el username como **infrastructureAP1** y la contraseña como **Cisco**. El mismo nombre de usuario y la contraseña necesita ser configurado en el Punto de acceso de la infraestructura.

The screenshot shows a web-based configuration interface for a network device. It is divided into two main sections: 'Individual Users' and 'User Groups'.

Individual Users Section:

- Current Users:** A list on the left contains '<NEW>' and 'infrastructureAPI'. A 'Delete' button is below the list.
- Form Fields:**
 - Username:** 'infrastructureAPI' (highlighted with a red circle).
 - Password:** A masked password field (highlighted with a red circle). Radio buttons for 'Text' and 'NT Hash' are to its right.
 - Confirm Password:** An empty text field.
 - Group Name:** A dropdown menu showing '<NONE >'.
 - MAC Authentication Only
- Buttons:** 'Apply' and 'Cancel' buttons are at the bottom right.

User Groups Section:

- Current User Groups:** A list on the left contains '<NEW>'. A 'Delete' button is below the list.
- Form Fields:**
 - Group Name:** An empty text field.
 - Session Timeout (optional):** A text field with '(1-4294967295 sec)' to its right.
 - Failed Authentications before Lockout (optional):** A text field with '(1-4294967295)' to its right.
 - Lockout (optional):** Radio buttons for 'Infinite' and 'Interval'. The 'Interval' option is selected, with a text field and '(1-4294967295 sec)' to its right.
 - VLAN ID (optional):** An empty text field.
 - SSID (optional):** A text field with an 'Add' button to its right.
- Buttons:** A 'Delete' button is at the bottom right.

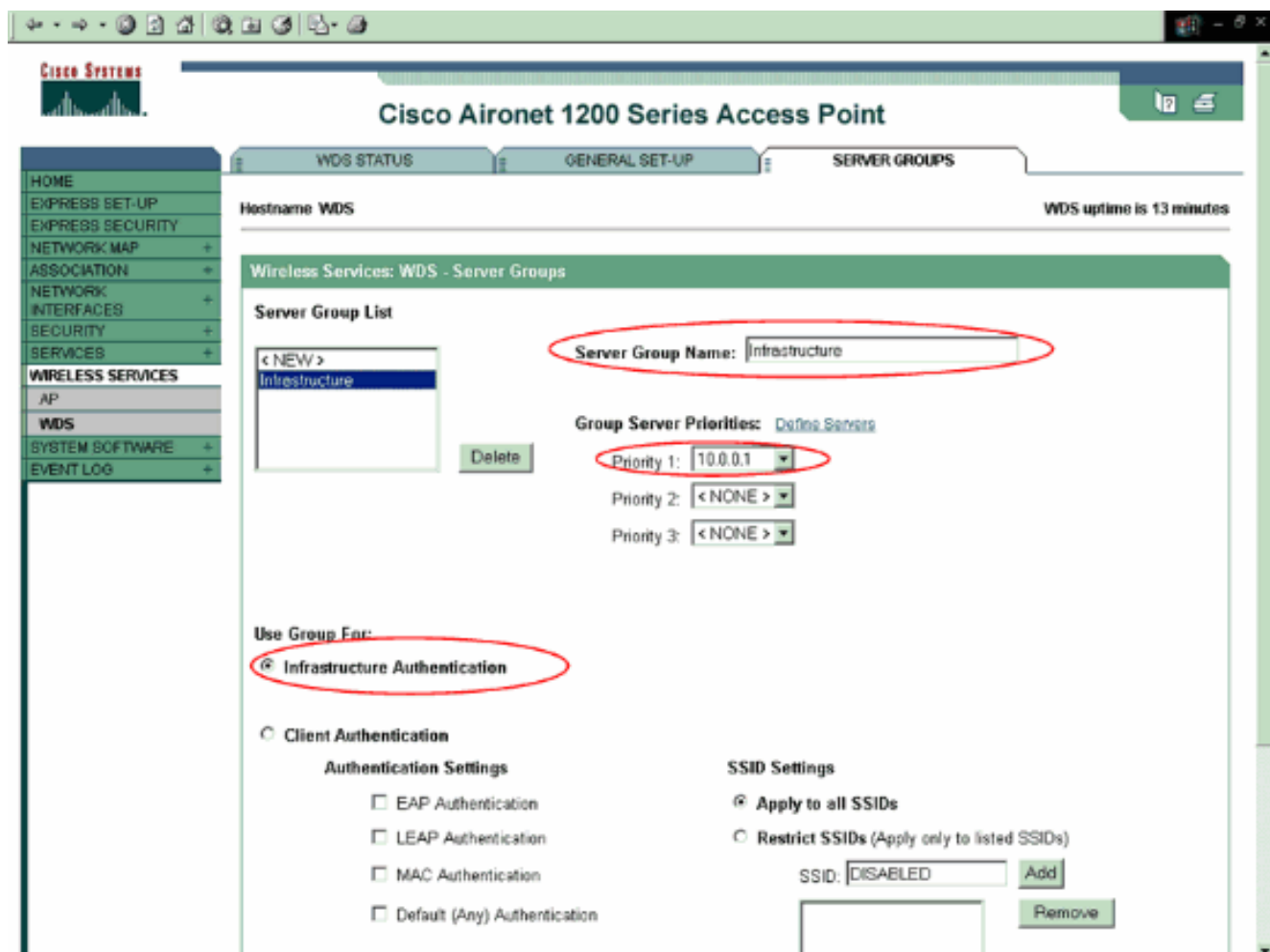
Después de que usted configure la característica local del servidor de RADIUS en el AP, usted necesita activar la funcionalidad WDS en el AP.

Complete estos pasos:

1. Seleccione los **Servicios inalámbricos > WDS** del menú del lado izquierdo en el AP.
2. Haga clic la **disposición general**.



3. Controle el uso este AP como servicios del dominio de red inalámbrica en la página de configuración general. Ingrese 254 en el campo de prioridad de los servicios del dominio de red inalámbrica. Haga clic en Apply (Aplicar).
4. Autenticación de infraestructura del permiso. **Grupos de servidores del teclado** en la página WDS. Ingrese un nombre en el campo de nombre del grupo de servidores para autenticar la infraestructura APs. Este ejemplo utiliza el nombre de grupo de servidores como **infraestructura**. Seleccione la dirección IP del servidor de RADIUS local de la lista desplegable de las prioridades del servidor del grupo. El WDS AP utiliza este servidor para autenticar la infraestructura APs. Seleccione la **autenticación de infraestructura** bajo grupo del uso para. Haga clic en Apply (Aplicar).



El WDS AP ahora actúa como servidor AAA. Configure uno de la infraestructura APs para registrarse con el WDS AP.

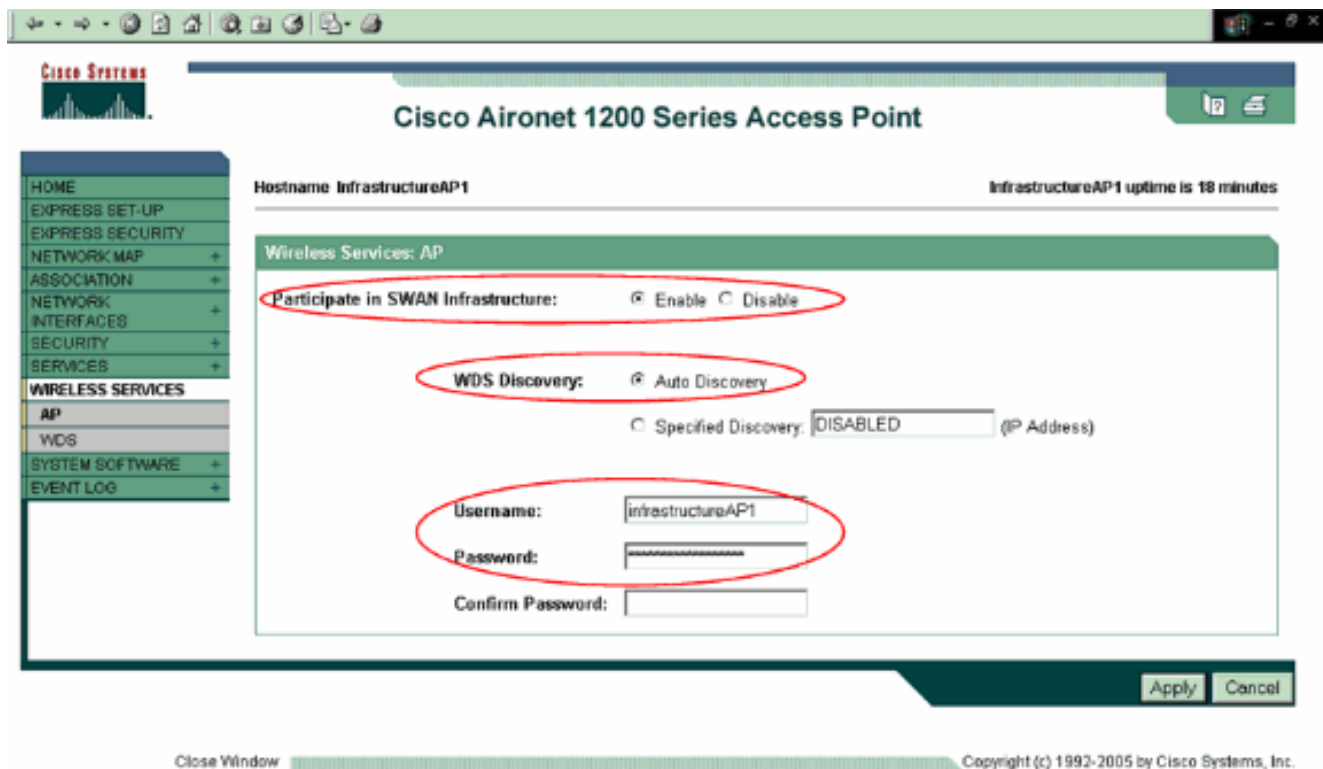
Nota: Use la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para encontrar más información sobre los comandos usados en este documento.

[Configure la infraestructura AP](#)

Esta sección explica la configuración requerida en la infraestructura AP para registrarse con el WDS AP. Los clientes se asocian a la infraestructura APs. La infraestructura APs solicita el WDS AP para realizar la autenticación para él.

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

1. Seleccione los **Servicios inalámbricos > el AP** del menú del lado izquierdo.
2. Seleccione el **permiso** debajo participan en la infraestructura del CISNE.
3. Seleccione la **detección automática** bajo descubrimiento WDS.



4. Ingrese el nombre de usuario y contraseña WDS en los campos adecuados. Haga clic en Apply (Aplicar). El nombre de usuario y contraseña debe existir en el servidor de RADIUS local. Usted debe definir un nombre de usuario y contraseña WDS en el servidor de la autenticación para todos los dispositivos que sean miembros del WDS.

La infraestructura AP aparece en la área de información AP con el estado según lo REGISTRADO una vez que usted configura el WDS AP y la infraestructura AP en el WDS AP, estado WDS cuadro. Esto está conforme a los Servicios inalámbricos > al elemento de menú WDS.

Close Window Copyright (c) 1992-2005 by Cisco Systems, Inc.

Las configuraciones incorrectas de la autenticación en el WDS AP o la infraestructura AP pueden hacer el AP no aparecer como ACTIVE y/o SE REGISTRARON. Controle las estadísticas del servidor de la autenticación para saber si hay cualesquiera errores o intento de autenticación fallado. Seleccione la **Seguridad > servidor de RADIUS local > las estadísticas** para las estadísticas del servidor de la autenticación.

Usted puede también utilizar el comando `show wlccp wds ap` del CLI en el WDS AP de verificar la configuración. En el registro acertado con el WDS AP, la salida después de un registro acertado con el WDS AP parece este ejemplo:

```
WDS#show wlccp wds ap
MAC-ADDR      IP-ADDR      STATE      LIFETIME      CDP-NEIGHBOR
000e.d7e4.a629 10.0.0.2     REGISTERED  97            10.77.241.161
```

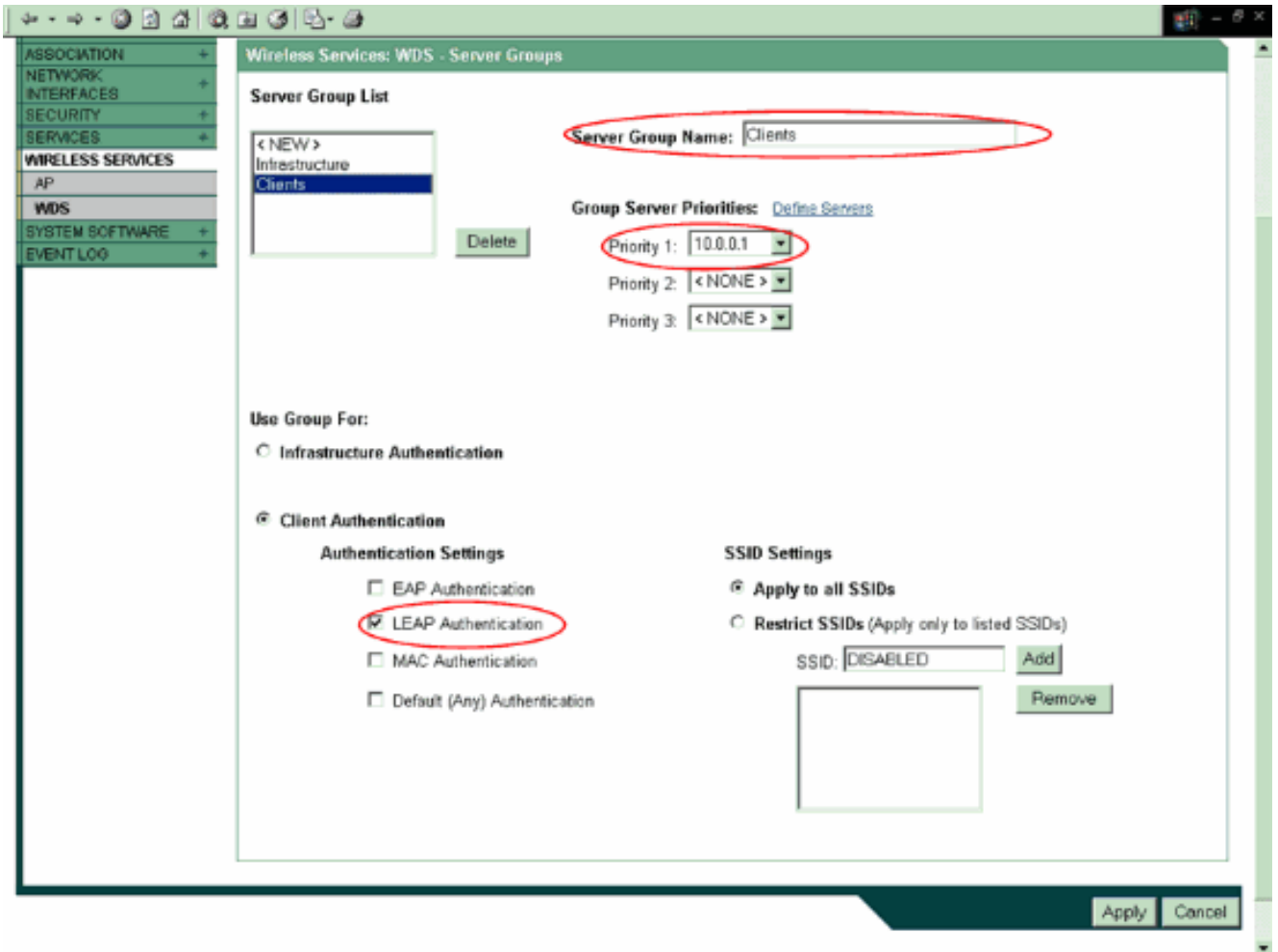
[Configure el método de autenticación de cliente](#)

Agregue un método de autenticación de cliente al WDS.

Complete estos pasos:

1. Seleccione los **Servicios inalámbricos > WDS > a los grupos de servidores** en el WDS AP. Defina a un grupo de servidores que autentique a los clientes (Grupo de clientes). Esto debe ser diferente previamente del grupo de servidor configurado para la autenticación de infraestructura. Este ejemplo utiliza el nombre de grupo de servidores como

clientes. Establezca la prioridad 1 al servidor de RADIUS local. Seleccione el tipo de autenticación (SALTO, EAP, MAC, y así sucesivamente) para utilizar para la autenticación de cliente. Este ejemplo utiliza la autenticación LEAP. Aplique las configuraciones a los SSID relevantes.



- Complete estos pasos en la infraestructura AP: Seleccione al **encargado de la Seguridad > del cifrado** y haga clic la **encriptación WEP** y elija **obligatorio** del menú desplegable. Bajo las claves de encriptación, ingrese la clave de encriptación WEP del 128-bit. Este ejemplo utiliza la clave de encriptación como **1234567890abcdef1234567890**.

Cisco Systems

Cisco Aironet 1200 Series Access Point

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
Admin Access
Encryption Manager
SSID Manager
Server Manager
Local RADIUS Server
Advanced Security
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG

RADIO0-802.11B | RADIO1-802.11B

Hostname InfrastructureAP1 | InfrastructureAP1 uptime is 22 minutes

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

None

WEP Encryption | Mandatory

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

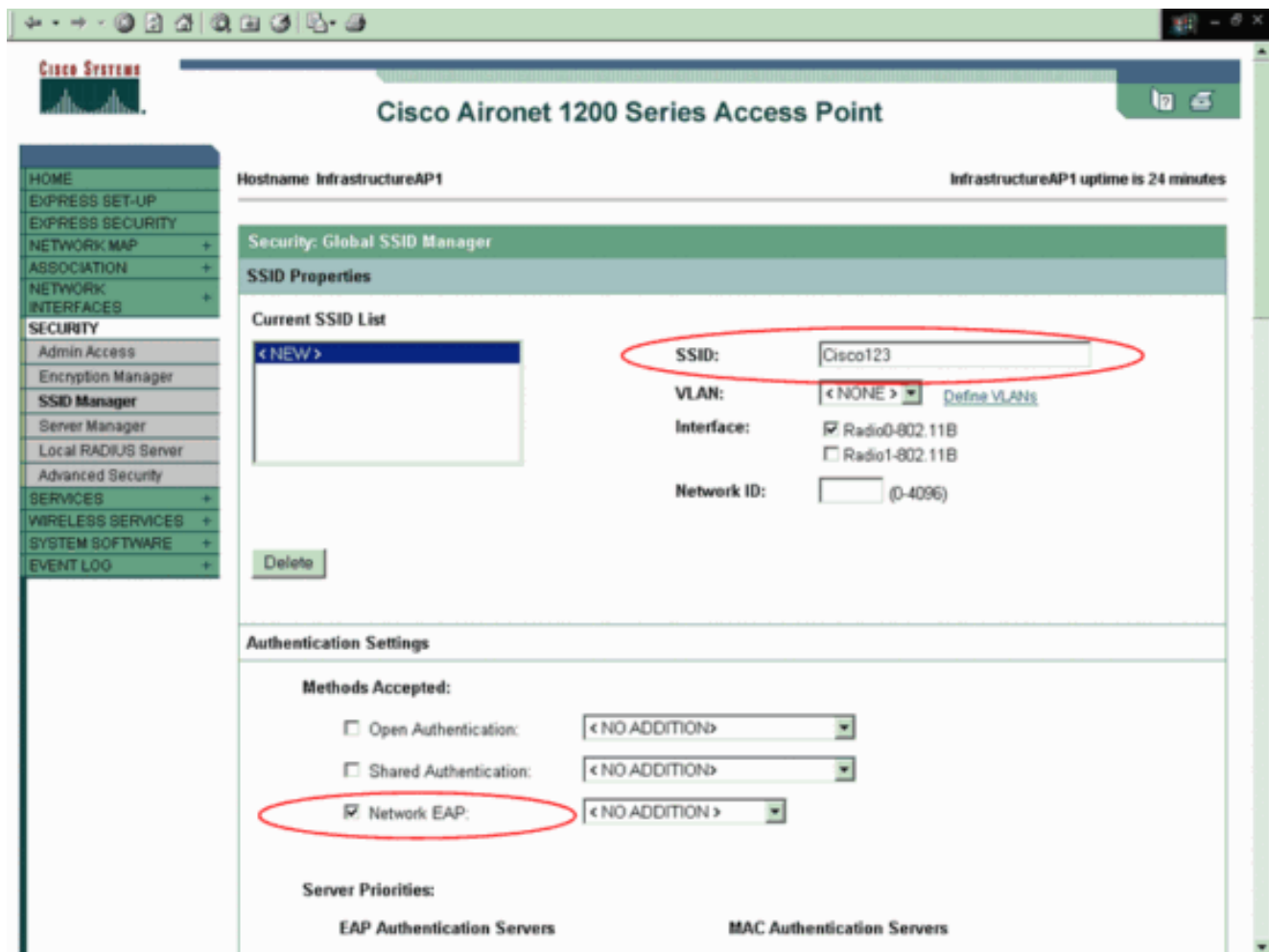
Cipher | WEP128 bit

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Global Properties

Seleccione la Seguridad > al administrador SSID y cree un nuevo SSID. Este ejemplo utiliza el SSID como Cisco123. Después, elija el método de autenticación. Seleccione la red EAP en la infraestructura AP.



Pruebe que los clientes autentican con éxito y asóciense a la infraestructura APs. El cliente pasa encendido sus credenciales a la infraestructura AP cuando sube por primera vez. La infraestructura AP entonces adelante lo mismo al WDS AP, que valida las credenciales.

Nota: Este documento no explica cómo configurar el adaptador del cliente. Refiera al [Cisco Aironet Wireless LAN Client Adapters](#) para la información sobre cómo configurar el adaptador del cliente.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

- **show wlccp wds mn** - Utilice este comando del CLI en el WDS AP de verificar la autenticación y la asociación acertadas de cliente con el WDS AP.

```
WDS#show wlccp wds mn
  MAC-ADDR      IP-ADDR      Curr-AP      STATE
0040.96a5.b5d4  10.0.0.15    000e.d7e4.a629  REGISTERED
```

Los comandos debug siguientes son también útiles.

- **wlccp ap {manganeso de la depuración | wds-descubrimiento | estado}** - utilice este comando de girar la visualización de los mensajes de la depuración relacionados con los dispositivos cliente (**manganeso**), el **proceso de descubrimiento WDS**, y la autenticación del Punto de acceso al Punto de acceso WDS (**estado**).
- **ponga a punto el paquete del wlccp** - Utilice este comando de girar la visualización de los

paquetes a y desde el Punto de acceso WDS.

- **ponga a punto al servidor local del radio** - Activa la visualización de los mensajes de error relacionados con las autenticaciones de cliente falladas al autenticador local

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Configuración de los servicios de dominio de red inalámbrica](#)
- [Adaptadores del cliente de Cisco Aironet](#)
- [El dominio de red inalámbrica mantiene el FAQ](#)
- [Ejemplos de configuración y lista de notas técnicas de la red inalámbrica \(WLAN\)](#)
- [Ejemplos de configuración y lista de notas técnicas del Cisco Aironet de la serie 1200](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)