Introducción a la configuración WPA

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de WPA (Wi-Fi Protected Access), el estándar de seguridad interina que utilizan los miembros de Wi-Fi Alliance.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento completo de las redes inalámbricas y de los problemas de seguridad inalámbrica
- Conocimiento de los métodos de seguridad del protocolo de autenticación extensible (EAP)

Componentes Utilizados

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

- Puntos de acceso (AP) basados en el software Cisco IOS®
- Versión 12.2(15)JA o posterior del software del IOS de Cisco**Nota:** Preferiblemente, use la

última versión del software Cisco IOS, aunque WPA sea compatible con la versión 12.2(11)JA y posteriores del software Cisco IOS. Para obtener la última versión de Cisco IOS Software, consulte Descargas (sólo clientes registrados) .
- Tarjeta de interfaz de red (NIC) compatible con WPA y software cliente compatible con WPA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Teoría Precedente

Las funciones de seguridad en una red inalámbrica, como WEP, son vulnerables. El grupo industrial Wi-Fi Alliance (o WECA) elaboró un estándar de seguridad provisional de última generación para las redes inalámbricas. El estándar proporciona defensa contra las debilidades hasta que la organización IEEE ratifique el estándar 802.11i.

Este nuevo esquema se basa en la autenticación actual EAP/802.1x y la administración de claves dinámicas y agrega un encripción de cifras más fuerte. Después de que el dispositivo cliente y el servidor de autenticación hagan una asociación EAP/802.1x, se negocia la administración de claves WPA entre el AP y el dispositivo cliente compatible con WPA.

Los productos de punto de acceso de Cisco también proporcionan una configuración híbrida en la que los clientes EAP basados en WEP heredados (con administración de claves antigua o sin ella) funcionan conjuntamente con los clientes WPA. Esta configuración se denomina modo de migración. El modo de migración permite un enfoque por fases para migrar a WPA. Este documento no cubre el modo de migración. Este documento proporciona un esquema para una red segura WPA pura.

Además de los problemas de seguridad a nivel empresarial o corporativo, WPA también proporciona una versión de clave precompartida (WPA-PSK) destinada a redes inalámbricas domésticas, de oficinas pequeñas o de oficinas domésticas. Cisco Aironet Client Utility (ACU) no admite WPA-PSK. La utilidad Wireless Zero Configuration de Microsoft Windows admite WPA-PSK para la mayoría de las tarjetas inalámbricas, al igual que estas utilidades:

- Cliente AEGIS de Meetinghouse Communications**Nota:** Consulte Anuncio EOS y EOL para la Línea de Productos AEGIS de Meetinghouse.
- Cliente Odyssey de Funk Software**Nota:** Consulte Centro de Atención al Cliente de Juniper Networks.
- Utilidades de cliente del fabricante de equipos originales (OEM) de algunos fabricantes

Puede configurar WPA-PSK cuando:

- El modo de cifrado se define como protocolo de integridad de clave temporal (TKIP) del cifrado en la ficha Administrador de cifrado.
- El tipo de autenticación, el uso de la gestión de claves autenticadas y la clave previamente compartida se definen en la ficha Service Set Identifier (SSID) Manager de la GUI.
- No se necesita configuración en la ficha Server Manager (Administrador de servidor).

Para habilitar WPA-PSK a través de la interfaz de línea de comandos (CLI), introduzca estos comandos. Inicie desde el modo de configuración:

```
AP(config)#interface dot11Radio 0
AP(config-if)#encryption mode ciphers tkip
```

```
AP(config-if)#ssid ssid_name
AP(config-if-ssid)#authentication open
AP(config-if-ssid)#authentication key-management wpa
AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

Nota: Esta sección proporciona solamente la configuración relevante para WPA-PSK. La configuración de esta sección es sólo para proporcionarle un entendimiento sobre cómo habilitar WPA-PSK y no es el foco de este documento. Este documento explica cómo configurar WPA.

Convenciones

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

Configurar

WPA se basa en los métodos de EAP/802.1x. Este documento asume que tiene una configuración EAP ligero (LEAP), EAP o EAP protegido (PEAP) que funciona antes de agregar la configuración para utilizar WPA.

Esta sección presenta los datos para configurar las características descritas en este documento.

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

Red EAP (Protocolo de autenticación extensible) o autenticación abierta con EAP.

En cualquier método de autenticación basado en EAP/802.1x, puede preguntarse cuáles son las diferencias entre la autenticación de red EAP y la autenticación abierta con EAP. Estos ítems se refieren a valores en el campo de autenticación de algoritmos en los encabezados de paquetes de administración y asociación. La mayoría de los fabricantes de clientes inalámbricos configuran este campo en el valor 0 (autenticación abierta) y luego señalan su deseo de realizar la autenticación EAP más adelante en el proceso de asociación. Cisco establece un valor distinto, desde el comienzo de la asociación con el indicador de red EAP.

Utilice el método de autenticación que indica esta lista si su red tiene clientes que son:

- Los clientes de Cisco—usan EAP de red.
- Clientes de terceros (que incluyen productos compatibles con Cisco Compatible Extensions [CCX]): utilice la autenticación abierta con EAP.
- Una combinación de clientes de Cisco y de terceros: elija tanto la autenticación de red EAP como la autenticación abierta con EAP.

Configuración de CLI

En este documento, se utilizan estas configuraciones:

- Una configuración LEAP que existe y funciona
- Versión 12.2(15)JA del software del IOS de Cisco para los AP basados en el software del IOS de Cisco

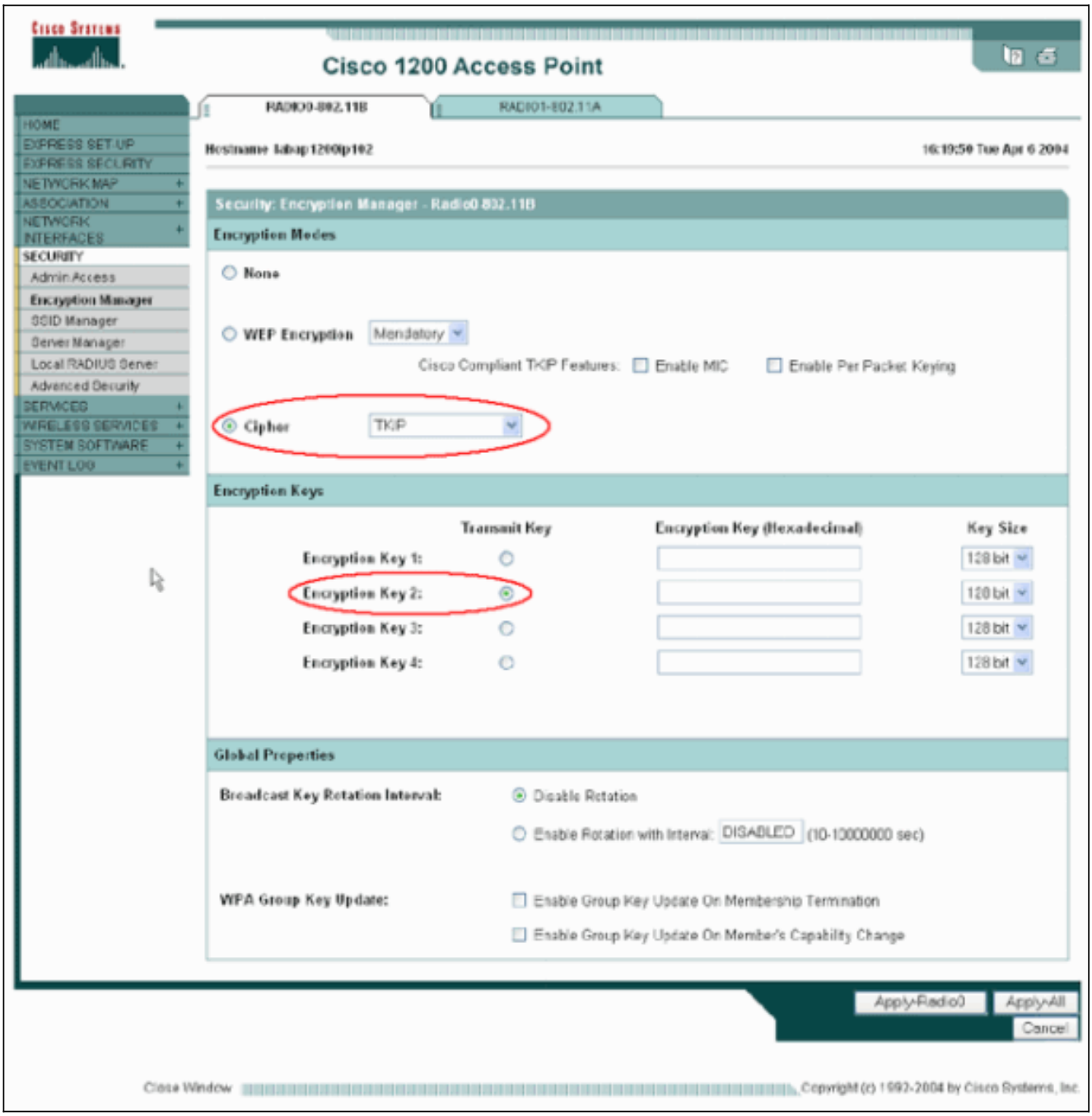
AP

```
ap1#show running-config
 Building configuration...
 .
 .
 .
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip
!--- This defines the cipher method that WPA uses. The
TKIP !--- method is the most secure, with use of the Wi-
Fi-defined version of TKIP. ! ssid WPAlabap1200
authentication open eap eap_methods
!--- This defines the method for the underlying EAP when
third-party clients !--- are in use.     authentication
network-eap eap_methods
!--- This defines the method for the underlying EAP when
Cisco clients are in use.     authentication key-
management wpa
!--- This engages WPA key management. ! speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 rts threshold 2312
channel 2437 station-role root bridge-group 1 bridge-
group 1 subscriber-loop-control bridge-group 1 block-
unknown-source no bridge-group 1 source-learning no
bridge-group 1 unicast-flooding bridge-group 1 spanning-
disabled . . . interface FastEthernet0 no ip address no
ip route-cache duplex auto speed auto bridge-group 1 no
bridge-group 1 source-learning bridge-group 1 spanning-
disabled ! interface BVI1 ip address 192.168.2.108
255.255.255.0 !--- This is the address of this unit. no
ip route-cache ! ip default-gateway 192.168.2.1 ip http
server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server host 192.168.2.100 auth-port 1645 acct-
port 1646 key shared_secret !--- This defines where the
RADIUS server is and the key between the AP and server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end ! end
```

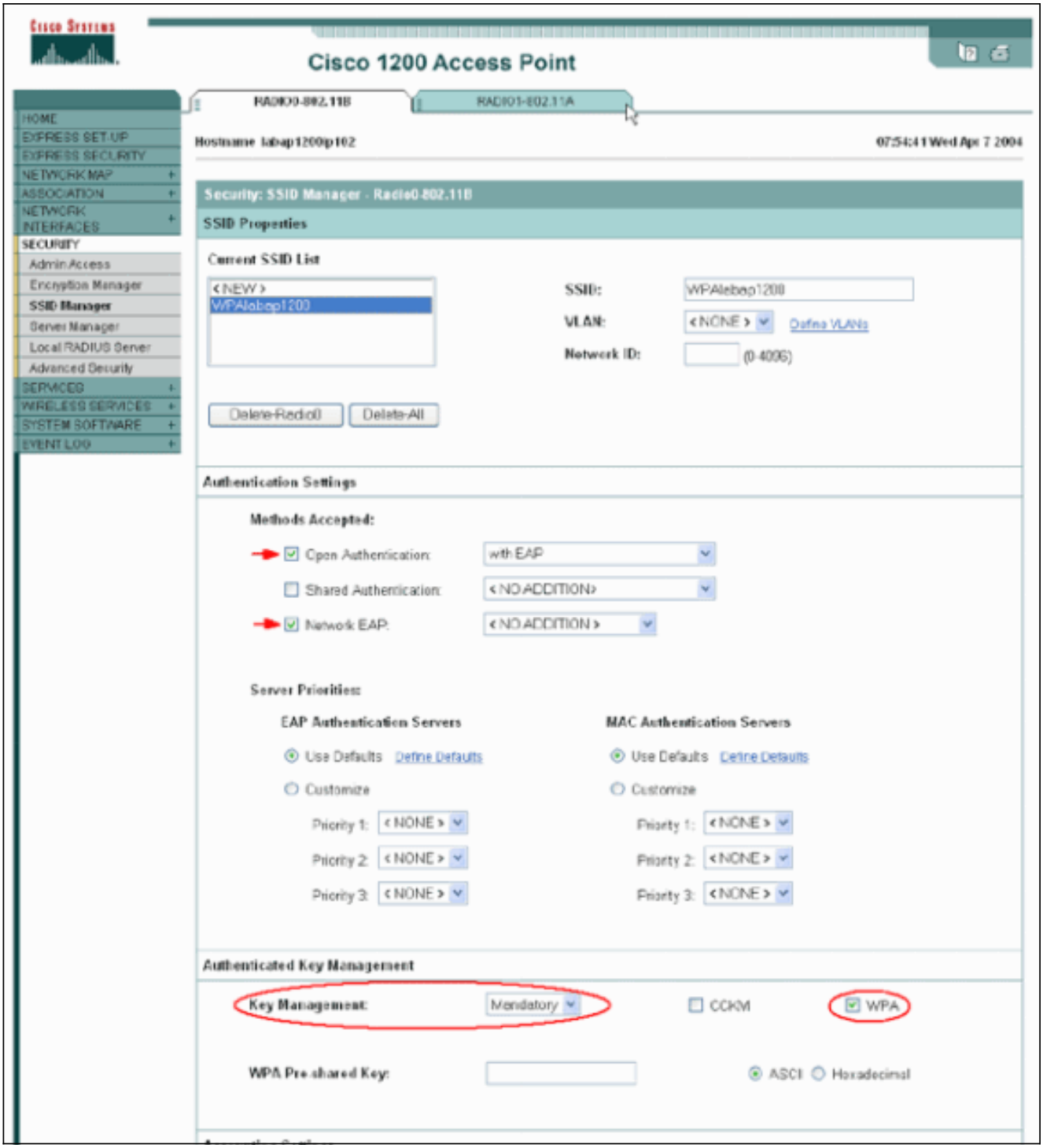
Configuración de la interfaz gráfica para el usuario

Complete estos pasos para configurar el AP para WPA:

1. Complete estos pasos para configurar el Encryption Manager:Active el encripción para TKIP.Borre el valor de la clave de cifrado 1.Establezca Encryption Key 2 (Clave de cifrado 2) como Transmit Key (Clave de transmisión).Haga clic en **Apply-Radio#**
   .



2. Complete estos pasos para configurar el Administrador SSID:Seleccione el SSID deseado de la lista SSID actual.Elija un método de autenticación adecuado.Base esta decisión en el tipo de tarjetas de cliente que utiliza. Vea la sección Red EAP o Autenticación Abierta con EAP de este documento para obtener más información. Si EAP funcionó antes de la adición de WPA, es probable que no sea necesario realizar un cambio.Complete estos pasos para habilitar la administración de claves:Elija **Obligatorio** en el menú desplegable Administración de claves.Marque la casilla de verificación WPA.Haga clic en **Apply-Radio#**
   .

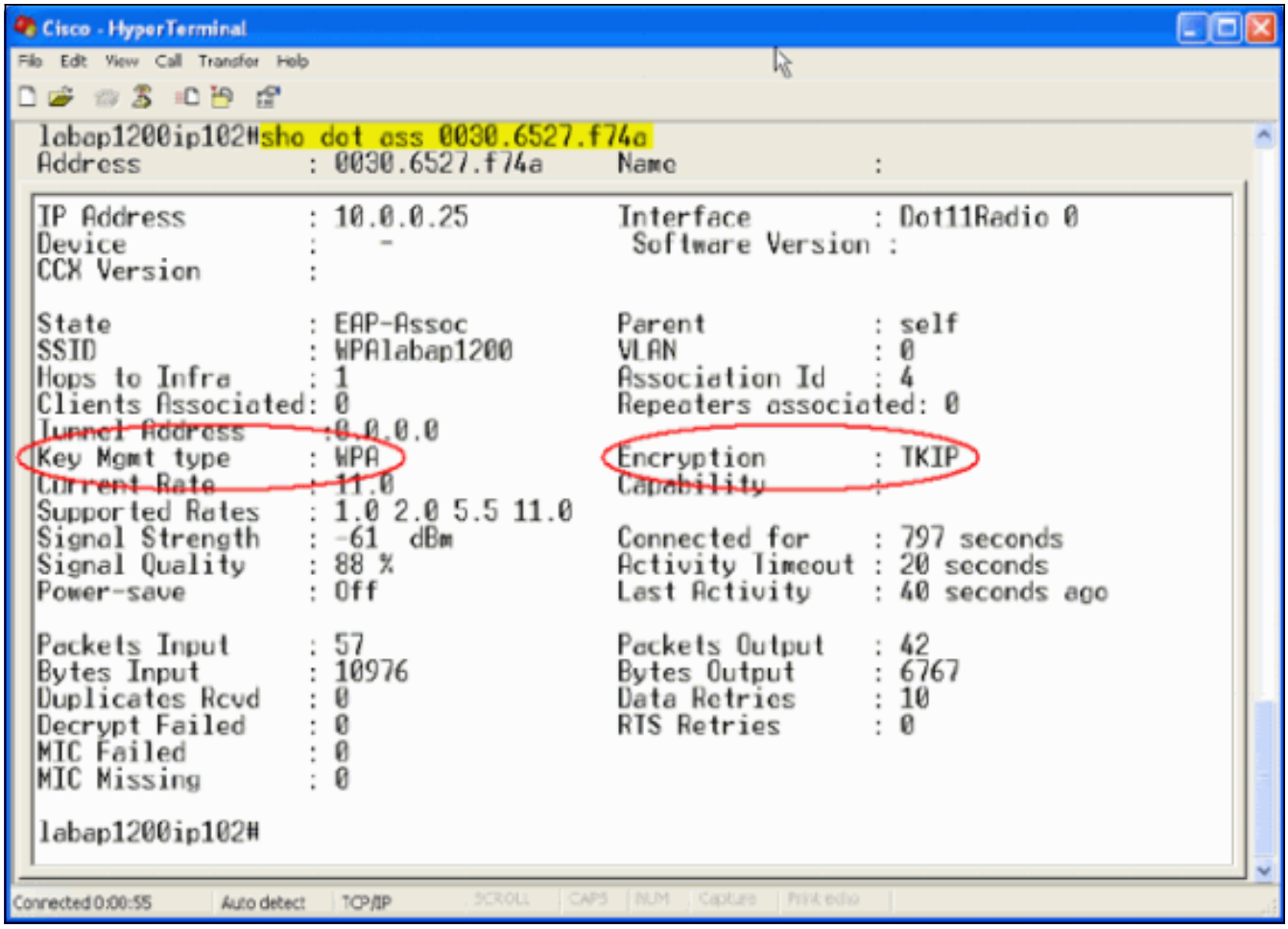


Verificación

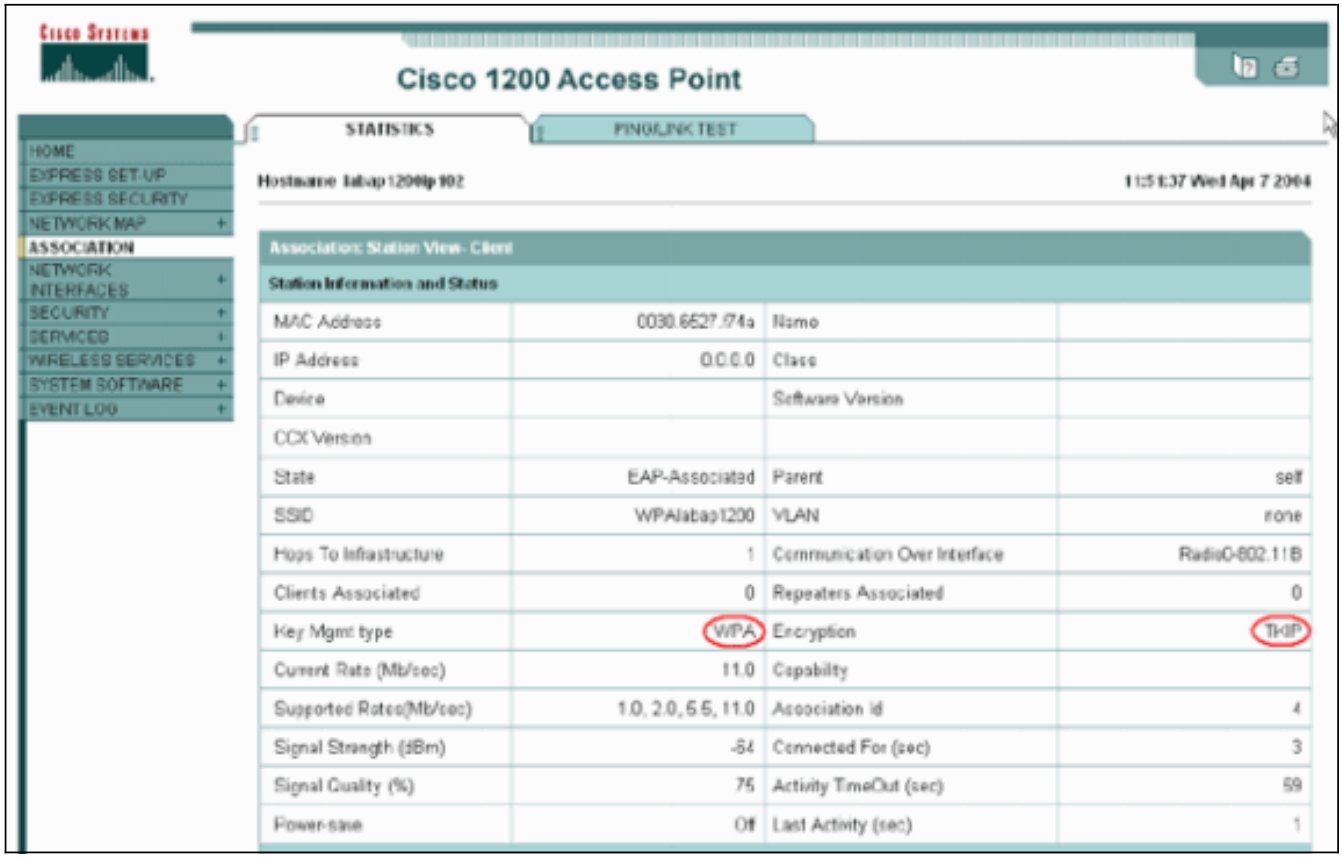
Use esta sección para confirmar que su configuración funciona correctamente.

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.

- **show dot11 association** *mac_address* —Este comando muestra información sobre un cliente asociado identificado específicamente. Verifique que el cliente negocie Key Management como **WPA** y Encryption como **TKIP**.



- La entrada de la tabla Association para un cliente determinado también debe indicar Key Management como **WPA** y Encryption as **TKIP**. En la tabla Asociación, haga clic en una dirección MAC específica para un cliente para ver los detalles de la asociación para ese cliente.



Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Procedimiento de resolución de problemas

Esta información es importante para esta configuración. Siga estos pasos para resolver problemas con su configuración:

1. Si esta configuración de LEAP, EAP o PEAP no se ha probado a fondo antes de la implementación de WPA, debe completar estos pasos:Inhabilite temporalmente el modo de encriptación WPA.Vuelva a habilitar el EAP adecuado.Confirme que la autenticación funcione.
2. Verifique que la configuración del cliente coincida con la del AP.Por ejemplo, cuando el AP esté configurado para WPA y TKIP, confirme que los ajustes coincidan con los ajustes configurados en el cliente.

Comandos para Troubleshooting

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

La administración de claves WPA implica un intercambio de señales en cuatro direcciones después de que la autenticación EAP se complete correctamente. Puede ver estos cuatro mensajes en depuraciones. Si EAP no autentica correctamente el cliente o si no ve los mensajes, complete estos pasos:

1. Desactive temporalmente WPA.
2. Vuelva a habilitar el EAP adecuado.
3. Confirme que la autenticación funcione.

Esta lista describe las depuraciones:

- **debug dot11 aaa manager keys**: Esta depuración muestra el intercambio de señales que se produce entre el AP y el cliente WPA como negociación de la clave transitoria par (PTK) y la clave transitoria de grupo (GTK). Esta depuración se introdujo en la versión 12.2(15)JA del software Cisco IOS.Si no aparece ningún resultado de depuración, verifique estos elementos:El **término mon del monitor de terminal** está habilitado (si utiliza una sesión Telnet).Las depuraciones están habilitadas.El cliente está configurado correctamente para WPA.Si la depuración muestra que los apretones de manos PTK y/o GTK están generados pero no verificados, verifique el software del suplicante WPA para la configuración correcta y la versión actualizada.
- **debug dot11 aaa authenticator state-machine**: Esta depuración muestra los diversos estados de negociaciones por los que pasa un cliente mientras asocia y autentica. Los nombres de estado indican estos estados. Esta depuración se introdujo en la versión 12.2(15)JA del software Cisco IOS. La depuración anula el comando **debug dot11 aaa dot1x state-machine** en Cisco IOS Software Release 12.2(15)JA y versiones posteriores.
- **debug dot11 aaa dot1x state-machine**: Esta depuración muestra los diversos estados de

negociaciones por los que pasa un cliente mientras asocia y autentica. Los nombres de estado indican estos estados. En las versiones del software Cisco IOS anteriores a la versión 12.2(15)JA del software Cisco IOS, esta depuración también muestra la negociación de administración de claves WPA.

- **debug dot11 aaa authenticator process—Este comando de depuración es muy útil para diagnosticar problemas con comunicaciones negociadas.** La información detallada muestra lo que cada participante en la negociación envía y muestra la respuesta del otro participante. También puede utilizar esta depuración junto con el comando **debug radius authentication**. Esta depuración se introdujo en la versión 12.2(15)JA del software Cisco IOS. La depuración anula el comando **debug dot11 aaa dot1x process** en Cisco IOS Software Release 12.2(15)JA y versiones posteriores.
- **debug dot11 aaa dot1x process—Este comando de depuración es útil para diagnosticar problemas con comunicaciones negociadas.** La información detallada muestra lo que cada participante en la negociación envía y muestra la respuesta del otro participante. También puede utilizar esta depuración junto con el comando **debug radius authentication**. En las versiones del software Cisco IOS anteriores a la versión 12.2(15)JA del software Cisco IOS, esta depuración muestra la negociación de administración de claves WPA.

Información Relacionada

- Configuración de conjuntos Cipher y WEP
- Configuración de los tipos de autenticación
- WPA2: acceso Wi-Fi protegido 2
- Configuración de acceso Wi-Fi protegido 2 (WPA 2)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).