Introducción a la configuración de 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.

prerrequisitos

Requisitos

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 basados en programas de Cisco IOS® (APs)
- Cisco IOS Software Release 12.2(15)JA o Posterior**Nota:** Preferiblemente, utilice la última

versión de software del Cisco IOS, aunque el WPA se utiliza en el Cisco IOS Software Release 12.2(11)JA y Posterior. Para obtener el último Cisco IOS versión de software, refiera a las transferencias directas (clientes registrados solamente).
- Un indicador luminoso LED amarillo de la placa muestra gravedad menor de interfaz WPA-obediente de red (NIC) y su software cliente WPA-obediente

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.

Teoría previa

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

Emplear de este los nuevos esquema la autenticación actual EAP/802.1x y la administración de claves dinámica, y agregan un cifrado más fuerte de la cifra. Después del dispositivo cliente y de la autenticación el servidor hace una asociación EAP/802.1x, negocian a la administración de claves WPA entre el AP y el dispositivo cliente WPA-obediente.

Los Productos de Cisco AP también preven una Configuración de Híbrido en la cual ambos clientes EAP basados en WEP de la herencia (con la herencia o ninguna administración de claves) trabajen conjuntamente con los clientes WPA. Esta configuración se refiere como modo de migración. El modo de migración tiene en cuenta un acercamiento organizado emigrar al WPA. Este documento no cubre al modo de migración. Este documento proporciona a un esquema para una red WPA-asegurada pura.

Además de los problemas de seguridad de la empresa o del nivel corporativo, el WPA también proporciona a una versión de la clave previamente compartida (WPA-PSK) que se piense para el uso en la oficina pequeña, la oficina en el hogar (SOHO) o las redes inalámbricas caseras. La utilidad de cliente de Cisco Aironet (ACU) no utiliza el WPA-PSK. La utilidad de configuración de la Tecnología inalámbrica cero de Microsoft Windows utiliza el WPA-PSK para la mayoría de las placas de red inalámbrica, al igual que estas utilidades:

- AEGIS Client de las comunicaciones de Meetinghouse**Nota:** Refiera al aviso FOE y EOL para la línea de producto de la TUTELA de Meetinghouse.
- Cliente Odyssey del software Funk**Nota:** Refiera al centro de atención al cliente de las redes Juniper .
- Utilidades de cliente del fabricante del equipo original (OEM) de algunos fabricantes

Usted puede configurar el WPA-PSK cuando:

- Usted define al modo de encripción como Temporal Key Integrity Protocol (TKIP) de la cifra en la ficha Manager del cifrado.
- Usted define el tipo de la autenticación, el uso de la administración de claves autenticada, y la clave previamente compartida en la ficha Manager del Service Set Identifier (SSID) del GUI.
- No se requiere ninguna configuración en el administrador de servidor cuadro.

Para activar el WPA-PSK a través del comando line interface(cli), ingrese estos comandos. Salga del modo de la 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 a la configuración que es relevante al WPA-PSK. La configuración en esta sección es solamente darle una comprensión en cómo activar el WPA-PSK y no es el foco de este documento. Este documento explica cómo configurar el WPA.

Convenciones

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

Configurar

Emplear WPA los métodos actuales EAP/802.1x. Este documento asume que usted tiene una luz EAP (SALTO), EAP, o la configuración protegida EAP (PEAP) que trabaja antes de que usted agregue la configuración para dedicar el WPA.

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

Nota: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

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

En cualquier método de autenticación EAP/802.1x-based, usted puede preguntar cuáles están las diferencias entre la 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 conjunto de los clientes de red inalámbrica este campo en el valor 0 (autenticación abierta), y entonces señalan su deseo de hacer la autenticación EAP más adelante en el proceso de asociación. Cisco fija el valor diferentemente, desde el principio de la asociación con el indicador de la red EAP.

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

- Clientes de Cisco — Utilice la red-EAP.
- Clientes de tercera persona (que incluyen las Extensiones compatibles de Cisco que el [CCX] - los Productos obedientes) — utiliza la autenticación abierta con EAP.
- Una combinación de ambo Cisco y clientes de tercera persona — elija la red-EAP y la autenticación abierta con EAP.

Configuración de CLI

Este documento utiliza estas configuraciones:

- Una configuración LEAP que existe y trabaja

- Cisco IOS Software Release 12.2(15)JA para el Cisco IOS APs basados en programas

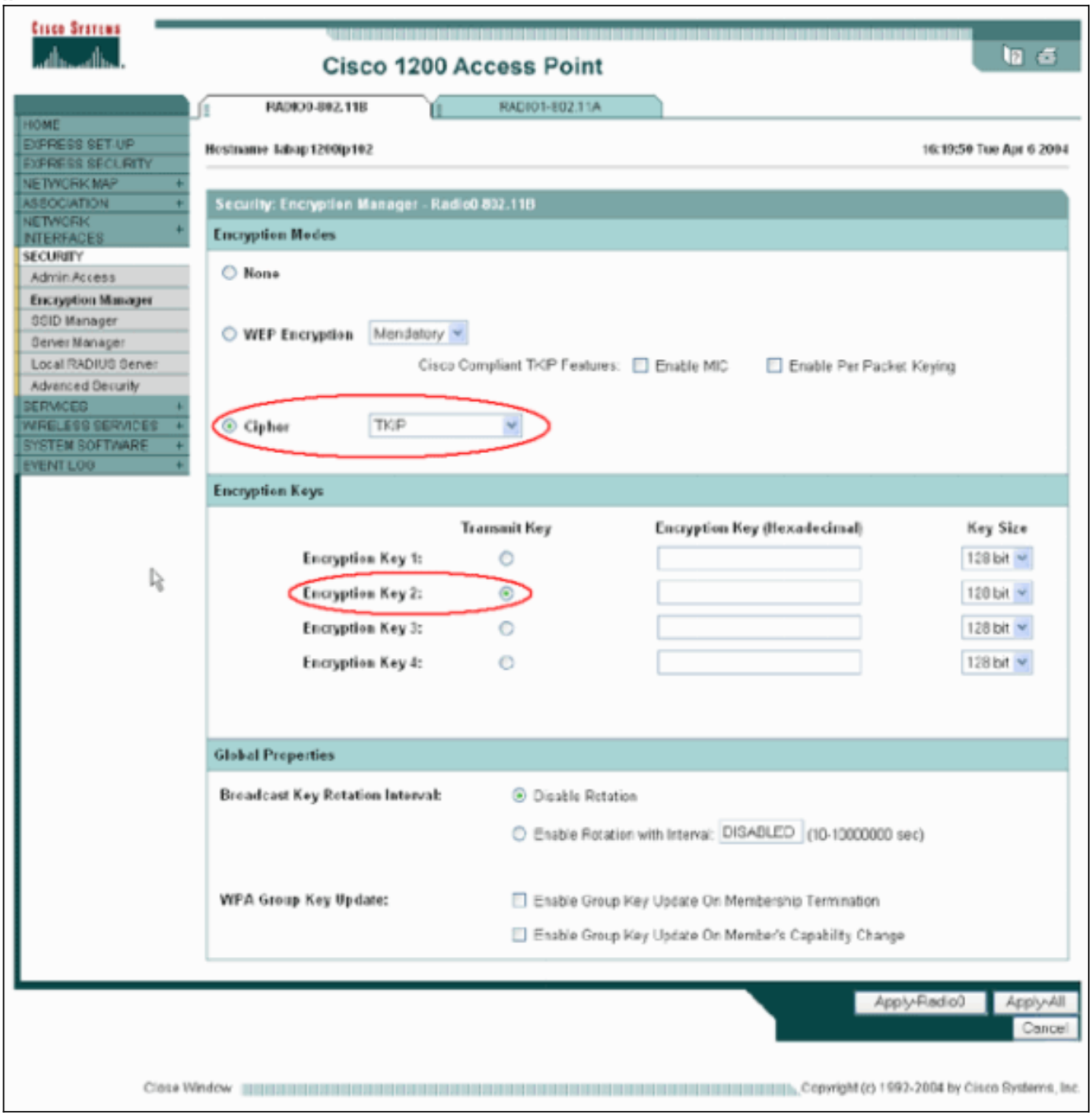
AP

```
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

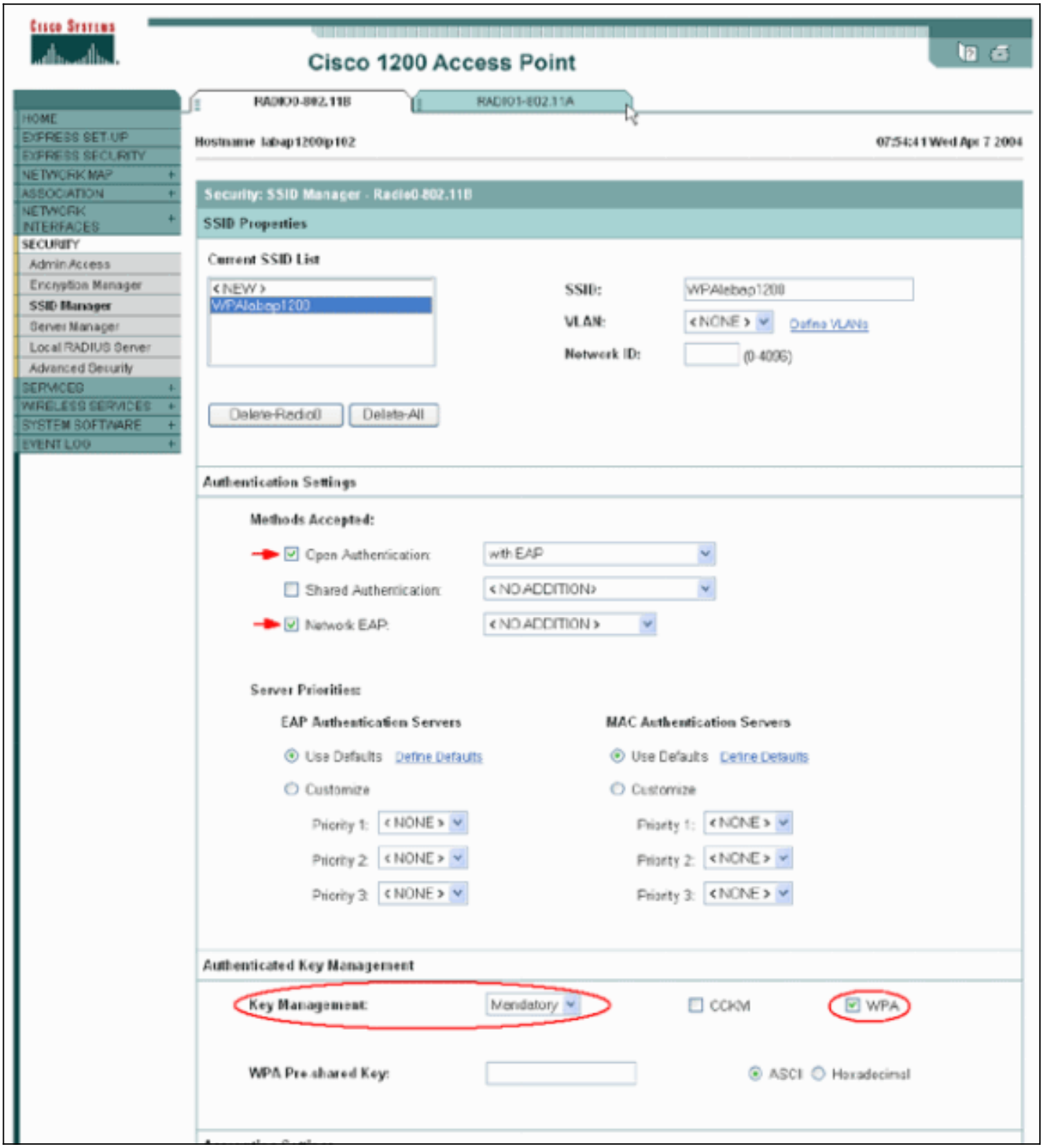
Complete estos pasos para configurar el AP para el WPA:

1. Complete estos pasos para poner al encargado del cifrado:Active la cifra para el TKIP.Borre el valor en la clave de encripción 1.Fije la clave de encripción 2 como la clave de transmitir.Haga clic la Aplicar-**radio**
#.



2. Complete estos pasos para poner al administrador SSID:Seleccione el SSID deseado de la lista actual SSID.Elija un método de autenticación apropiado.Base esta decisión en el tipo de indicadores luminosos LED amarillo de la placa muestra gravedad menor del cliente que usted utilice. Vea la red EAP o la autenticación abierta con la sección EAP de este documento para más información. Si EAP trabajó antes de la adición de WPA, un cambio no es probablemente necesario.Complete estos pasos para activar la administración de claves:Elija **obligatorio del** menú desplegable de la administración de claves.Controle la casilla de verificación WPA.Haga clic la Aplicar-**radio**

#.

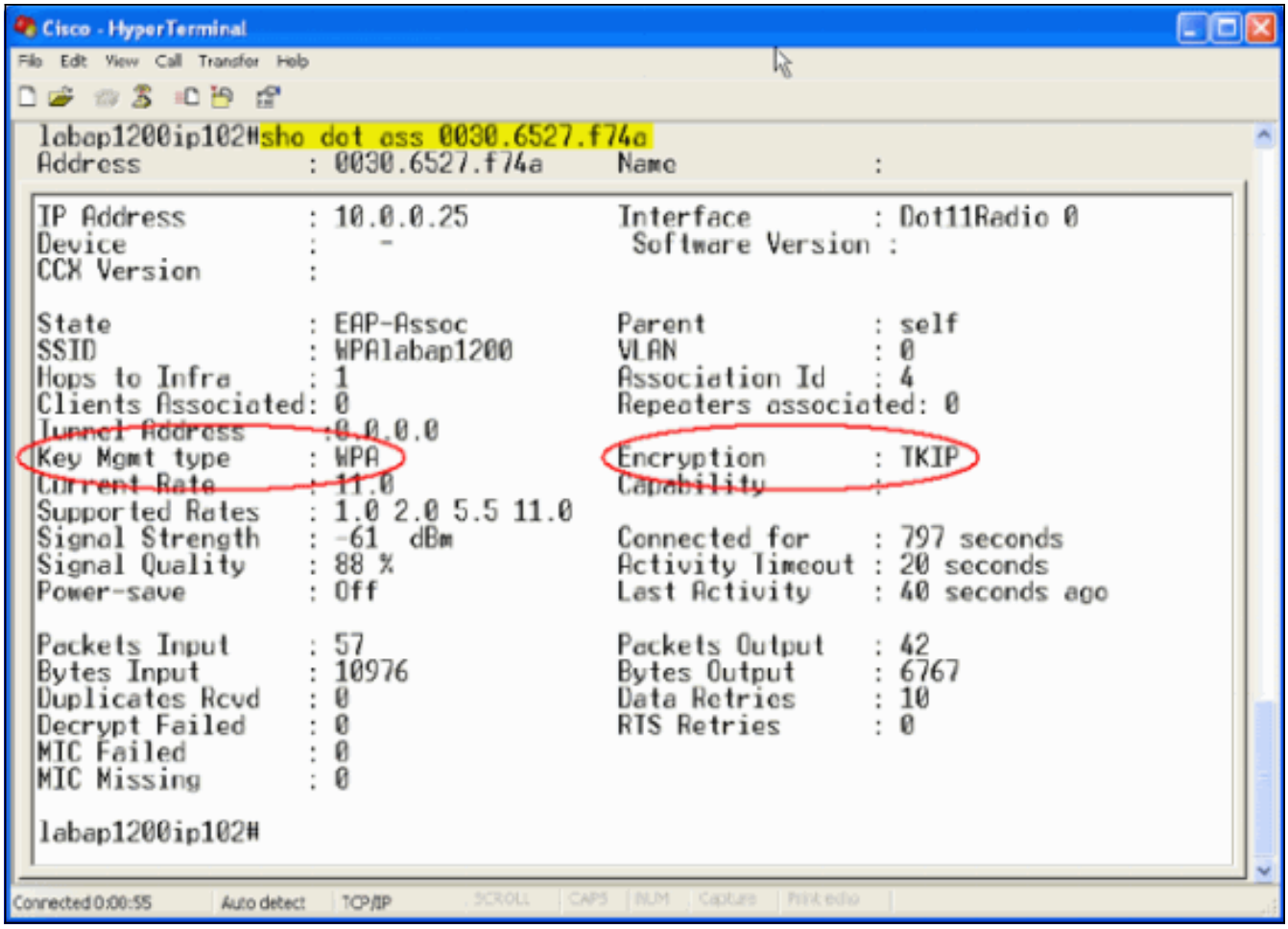


Verificación

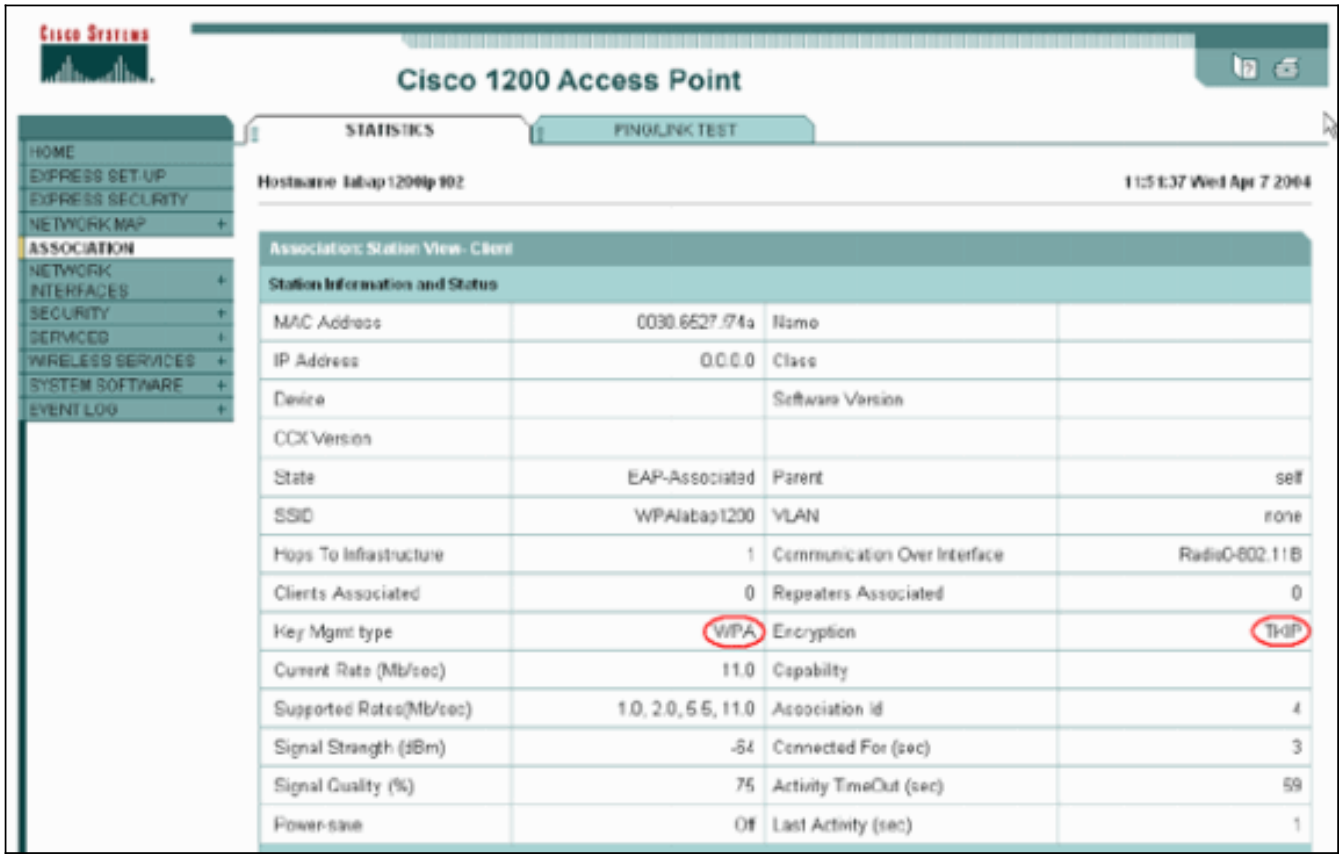
Use esta sección para confirmar que su configuración funciona correctamente.

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

- **muestre los *mac_address de la* asociación dot11** — Este comando visualiza la información sobre un cliente asociado específicamente identificado. Verifique que el cliente negocie la administración de claves como **WPA** y el cifrado como **TKIP**.



- La entrada de tabla de la asociación para un cliente particular debe también indicar la administración de claves como **WPA** y el cifrado como **TKIP**. En la tabla de asociación, haga clic una dirección MAC determinada para un cliente para ver los detalles de la asociación para ese
cliente.



Troubleshooting

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

Procedimiento de resolución de problemas

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

1. Si este SALTO, EAP, o configuración de PEAP no se ha probado a conciencia antes de la implementación de WPA, usted debe completar estos pasos:Inhabilite temporalmente al modo de encripción WPA.Vuelva a permitir el EAP apropiado.Confirme que la autenticación trabaja.
2. Verifique que la configuración del cliente haga juego el del AP.Por ejemplo, cuando el AP se configura para el WPA y el TKIP, confirme que las configuraciones hacen juego las configuraciones que se configuran en el cliente.

Resuelva problemas los comandos

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

La administración de claves WPA implica un apretón de manos de cuatro terminales después de que la autenticación EAP complete con éxito. Usted puede ver estos cuatro mensajes en las depuraciones. Si EAP no autentica con éxito al cliente o si usted no ve los mensajes, complete estos pasos:

1. Inhabilite temporalmente el WPA.
2. Vuelva a permitir el EAP apropiado.
3. Confirme que la autenticación trabaja.

Esta lista describe las depuraciones:

- **claves del encargado de la depuración dot11 aaa** — Esta depuración muestra que el apretón de manos que sucede entre el AP y el cliente WPA como la clave en parejas transitoria (PTK) y la clave transitoria del grupo (GTK) negocian. Esta depuración fue introducida en el Cisco IOS Software Release 12.2(15)JA.Si aparecen ningunas salidas de la depuración, verifique estos items:Se activa el **término** terminal **lunes del** monitor (si usted utiliza una sesión de Telnet).Se activan las depuraciones.Configuran al cliente apropiadamente para el WPA.Si la depuración muestra que el PTK y/o las entradas en contacto GTK están construidos pero no verificados, controle el software del solicitante de WPA para saber si hay la configuración correcta y la versión actualizada.
- **ponga a punto la estado-máquina del authenticator dot11 aaa** — Esta depuración muestra los diversos estados de las negociaciones a que va un cliente a través mientras que se asocian y autentican. Los nombres del estado indican estos estados. Esta depuración fue introducida en el Cisco IOS Software Release 12.2(15)JA. Los obsoletes de la depuración el **comando debug dot11 aaa dot1x state-machine** en el Cisco IOS Software Release 12.2(15)JA y Posterior.

- **estado-máquina de la depuración dot11 aaa dot1x** — Esta depuración muestra los diversos estados de las negociaciones a que va un cliente a través mientras que se asocian y autentican. Los nombres del estado indican estos estados. En las versiones de software del Cisco IOS que son anteriores que el Cisco IOS Software Release 12.2(15)JA, esta depuración también muestra la negociación de la administración de claves WPA.
- **proceso del authenticator de la depuración dot11 aaa** — Esta depuración es la más útil diagnosticar los problemas con las comunicaciones negociadas. La información detallada muestra lo que envía cada participante en la negociación y muestra la respuesta del otro participante. Usted puede también utilizar esta depuración conjuntamente con el **comando debug radius authentication**. Esta depuración fue introducida en el Cisco IOS Software Release 12.2(15)JA. Los obsoletes de la depuración el **comando debug dot11 aaa dot1x process** en el Cisco IOS Software Release 12.2(15)JA y Posterior.
- **proceso de la depuración dot11 aaa dot1x** — Esta depuración es útil diagnosticar los problemas con las comunicaciones negociadas. La información detallada muestra lo que envía cada participante en la negociación y muestra la respuesta del otro participante. Usted puede también utilizar esta depuración conjuntamente con el **comando debug radius authentication**. En las versiones de software del Cisco IOS que son anteriores que el Cisco IOS Software Release 12.2(15)JA, esta depuración muestra la negociación de la administración de claves WPA.

Información Relacionada

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