Tipos de autenticación inalámbricos en un ejemplo de configuración fijo ISR

Contenido

Introducción

Este documento proporciona el ejemplo de configuración que explica cómo configurar los diversos tipos de autenticación de la capa 2 en un router integrado tecnología inalámbrica de Cisco de la Configuración fija para la conectividad de red inalámbrica con los comandos CLI.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar los parámetros básicos del router de los Servicios integrados de Cisco (ISR)
- Conocimiento de cómo configurar el adaptador de red inalámbrica de cliente 802.11a/b/g con utilidad Aironet Desktop (ADU)

Componentes Utilizados

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

- Cisco 877W ISR que funciona con la versión 12.3(8)YI1 del Cisco IOS ® Software
- Laptop con utilidad Aironet Desktop la versión 3.6
- adaptador del cliente del a/b/g del 802.11 que funciona con la versión de firmware 3.6

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

Antecedentes

El Routers de la Configuración fija de los Servicios integrados de Cisco soporta una solución de red inalámbrica LAN segura, asequible, y fácil de usar que combine la movilidad y la flexibilidad con las características de la empresa-clase requeridas por los profesionales de redes. Con un sistema de administración basado en el Cisco IOS Software, los routeres Cisco actúan como Puntos de acceso y son con certificación Wi-Fi, los transmisores-receptores del Wireless LAN de IEEE 802.11a/b/g-compliant.

Usted puede configurar y monitorear al Routers con el comando line interface(cli), el sistema de administración basado en buscador, o el Simple Network Management Protocol (SNMP). Este documento describe cómo configurar el ISR para la conectividad de red inalámbrica con los comandos CLI.

Configurar

Este ejemplo muestra cómo configurar estos tipos de autenticación en un router integrado tecnología inalámbrica de Cisco de la Configuración fija con los comandos CLI.

- Autenticación abierta
- autenticación 802.1x/EAP (protocolo extensible authentication)
- Autenticación protegida Wi-Fi de la clave previamente compartida del acceso (WPA-PSK)
- Autenticación WPA (con el EAP)

Nota: Este documento no se centra en la autenticación compartida puesto que es un tipo de autenticación menos asegurado.

En esta sección encontrará la información para configurar las funciones 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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Esta configuración utiliza al servidor de RADIUS local en la Tecnología inalámbrica ISR para autenticar a los clientes de red inalámbrica con la autenticación del 802.1x.

Autenticación abierta de la configuración

La autenticación abierta es un algoritmo de la autenticación nula. El Punto de acceso concede cualquier pedido la autenticación. La autenticación abierta permite cualquier acceso a la red del dispositivo. Si el no encryption se habilita en la red, cualquier dispositivo que conozca el SSID del Punto de acceso puede acceder a la red. Con la encripción WEP habilitada en un Punto de acceso, la clave WEP sí mismo llega a ser los medios del control de acceso. Si un dispositivo no tiene la clave WEP correcta, aunque la autenticación es acertada, el dispositivo no puede transmitir los datos a través del Punto de acceso. Ningunos pueden él desencriptar los datos enviados del Punto de acceso.

Este ejemplo de configuración apenas explica una autenticación abierta simple. La clave WEP se puede hacer obligatoria u opcional. Este ejemplo configura la clave WEP como opcional de modo que cualquier dispositivo que no utilice el WEP pueda también autenticar y asociarse a este AP.

Refiera a la autenticación abierta para más información.

Este ejemplo utiliza esta configuración de la configuración para configurar la autenticación abierta en el ISR.

- Nombre SSID: “**ábrase**”
- VLAN 1
- Rango interno del servidor DHCP: **10.1.0.0/16**

Nota: Por la simplicidad, este ejemplo no utiliza ninguna técnica del cifrado para los clientes autenticados.

Complete estas acciones en el router:

1. Configure el Integrated Routing and Bridging (IRB) y configure al Grupo de Bridge
2. Configure el (BVI) de la Interfaz Virtual Interconectada
3. Configure el SSID para la autenticación abierta
4. Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N

Configure el Integrated Routing and Bridging (IRB) y configure al Grupo de Bridge

Complete estas acciones:

1. **Habilite el IRB en el router.irb del** router<configure>#bridge**Nota:** Si se van todos los tipos de la Seguridad a ser configurados en un único router, es bastante para habilitar el IRB solamente una vez global en el router. No necesita ser habilitado para cada tipo de autenticación individual.
2. **Defina a un Grupo de Bridge.**Este ejemplo utiliza el bridge-group number **1.**router<configure>#bridge *1*
3. **Elija el Spanning Tree Protocol para el Grupo de Bridge.**Aquí, el IEEE Spanning-Tree Protocol se configura para este Grupo de Bridge.**protocolo IEEE del** router<configure>#bridge *1*
4. **Permita a un BVI para validar y para rutear los paquetes enrutables recibidos de su Grupo de Bridge correspondiente.**Este ejemplo permite al BVI para validar y para rutear el paquete del IP.*IP de la* **ruta del** router<configure>#bridge *1*

Configure el (BVI) de la Interfaz Virtual Interconectada

Complete estas acciones:

1. **Configure el BVI.**Configure el BVI cuando usted asigna el número correspondiente del Grupo de Bridge al BVI. Cada Grupo de Bridge puede solamente tener un BVI correspondiente. Este ejemplo asigna el Grupo de Bridge número 1 al BVI.router<configure>#interface **BVI** *<1>*
2. **Asigne una dirección IP al BVI.router<config-if>#ip address** *10.1.1.1 255.255.0.0*router<config-if>#no **cerrado**

Refiera al bridging de la configuración para información detallada sobre el bridging.

Configure el SSID para la autenticación abierta

Complete estas acciones:

1. **Habilite la interfaz radio**Para habilitar la interfaz radio, ir al modo de configuración de la interfaz radio del DOT11 y asignar un SSID a la interfaz.router<config>#interface

dot11radio0el router<config-if>#no **apaga**router<config-if>#ssid *abierto*El tipo de la autenticación abierta puede ser configurado conjuntamente con la autenticación de la dirección MAC. En este caso, el Punto de acceso fuerza todos los dispositivos del cliente para realizar la autenticación del MAC address antes de que se permitan unirse a la red.La autenticación abierta se puede también configurar junto con la autenticación EAP. El Punto de acceso fuerza todos los dispositivos del cliente para realizar la autenticación EAP antes de que se permitan unirse a la red. Para el nombre de la lista, especifique la lista del método de autentificación.Un Punto de acceso configurado para la autenticación EAP fuerza todos los dispositivos del cliente que se asocien para realizar la autenticación EAP. Los dispositivos del cliente que no utilizan el EAP no pueden utilizar el Punto de acceso.

2. **Lazo SSID a un VLA N.**Para habilitar el SSID en esta interfaz, ate el SSID al VLA N en el modo de configuración SSID.*1* router<config-ssid>vlan
3. **Configure el SSID con la autenticación abierta.**router<config-ssid>#authentication **abierto**
4. **Configure la interfaz radio para la clave WEP opcional.modo WEP del vlan1 del** router<config>#encryption **opcional**
5. **VLA N del permiso en la interfaz radio.**router<config>#interface **Dot11Radio 0.1dot1q** *1 del* router<config-subif>#encapsulationrouter<config-subif>#bridge-group *1*

Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N

Teclee estos comandos en el modo de configuración global de configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N:

- **excluir-direccionamiento 10.1.1.1 10.1.1.5 DHCP del IP**
- **pool DHCP del IP** *abierto*

En el modo de la configuración de agrupamiento DHCP, teclee estos comandos:

- **red** *10.1.0.0 255.255.0.0*
- **valor por defecto-router** *10.1.1.1*

Autenticación de la configuración 802.1x/EAP

Este tipo de autenticación proporciona el del más alto nivel de la Seguridad para su red inalámbrica. Con el Protocolo de Autenticación Extensible (EAP) usado para obrar recíprocamente con un servidor de RADIUS EAP-compatible, el Punto de acceso ayuda a un dispositivo de red inalámbrica de cliente y al servidor de RADIUS a realizar la autenticación recíproca y a derivar una clave WEP dinámica del unicast. El servidor de RADIUS envía la clave WEP al Punto de acceso, que la utiliza para todas las señales de datos de unidifusión que envíe a o reciba del cliente.

Refiera a la autenticación EAP para más información.

Este ejemplo utiliza esta configuración puesta:

- Nombre SSID: **salto**
- VLAN2
- Rango interno del servidor DHCP: **10.2.0.0/16**

Este ejemplo utiliza la autenticación LEAP como el mecanismo para autenticar al cliente de red inalámbrica.

Nota: Refiera al v3.2 del Cisco Secure ACS for Windows con la autenticación de la máquina del EAP-TLS para configurar el EAP-TLS.

Nota: Refiera a configurar el v3.2 del Cisco Secure ACS for Windows con la autenticación de la máquina PEAP-MS-CHAPv2 para configurar PEAP-MS-CHAPv2.

Nota: Entienda que toda la configuración de estos tipos EAP implica principalmente los cambios de configuración en el lado del cliente y en el lado del servidor de autenticación. La configuración en el router inalámbrico o el Punto de acceso más o menos sigue siendo lo mismo para todos estos tipos de autenticación.

Nota: Según lo mencionado inicialmente, esta configuración utiliza al servidor de RADIUS local en la Tecnología inalámbrica ISR para autenticar a los clientes de red inalámbrica con la autenticación del 802.1x.

Complete estas acciones en el router:

1. Configure el Integrated Routing and Bridging (IRB) y configure al Grupo de Bridge
2. Configure el (BVI) de la Interfaz Virtual Interconectada
3. Configure al servidor de RADIUS local para la autenticación EAP
4. Configure el SSID para la autenticación 802.1x/EAP
5. Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N

Configure el Integrated Routing and Bridging (IRB) y configure al Grupo de Bridge

Complete estas acciones:

1. **Habilite el IRB en el router.irb del** router<configure>#bridge**Nota:** Si se van todos los tipos de la Seguridad a ser configurados en un único router, es bastante para habilitar el IRB solamente una vez global en el router. No necesita ser habilitado para cada tipo de autenticación individual.
2. **Defina a un Grupo de Bridge.**Este ejemplo utiliza el bridge-group number 2.router<configure>#bridge *2*
3. **Elija el Spanning Tree Protocol para el Grupo de Bridge.**Aquí, el IEEE Spanning-Tree Protocol se configura para este Grupo de Bridge.**protocolo IEEE del** router<configure>#bridge *2*
4. **Elija el Spanning Tree Protocol para el Grupo de Bridge.**Aquí, el IEEE Spanning-Tree Protocol se configura para este Grupo de Bridge.**protocolo IEEE del** router<configure>#bridge *2*
5. **Permita a un BVI para validar y para rutear los paquetes enrutables que se reciben de su Grupo de Bridge correspondiente.**Este ejemplo permite al BVI para validar y para rutear los paquetes del IP.*IP de la* **ruta del** router<configure>#bridge *2*

Configure el (BVI) de la Interfaz Virtual Interconectada

Complete estas acciones:

1. **Configure el BVI.**Configure el BVI cuando usted asigna el número correspondiente del Grupo de Bridge al BVI. Cada Grupo de Bridge puede solamente tener un BVI correspondiente. Este ejemplo asigna el Grupo de Bridge número 2 al BVI.router<configure>#interface **BVI** *<2>*
2. **Asigne una dirección IP al BVI.router<config-if>#ip address** *10.2.1.1 255.255.0.0*router<config-if>#no **cerrado**

Configure al servidor de RADIUS local para la autenticación EAP

Como se mencionó antes, este documento utiliza al servidor de RADIUS local en el router enterado inalámbrico para la autenticación EAP.

1. **Habilite el modelo del control de acceso del Authentication, Authorization, and Accounting (AAA).**router<configure>#aaa **de modelo nuevo**
2. **Cree un grupo de servidores rad-EAP para el servidor de RADIUS.acct-puerto** *1813 del auténtico*-**puerto** *1812 de 10.2.1.1 del* **servidor del radio rad-***EAP del* **servidor del grupo del** router<configure>#aaa
3. **Cree los eap_methods de una lista de métodos que enumera hacia fuera el método de autentificación usado para autenticar al usuario que ingresa al sistema AAA. Asigne la lista de métodos a este grupo de servidores.***los eap_methods de la* **conexión con el sistema de autenticación del** router<configure>#aaa **agrupan el rad-***EAP*
4. **Habilite al router como servidor de autenticación local y ingrese en el modo de configuración para el authenticator.local del** router<configure>#radius-server
5. **En el modo de la configuración de servidor de RADIUS, agregue al router como cliente AAA del servidor de autenticación local.clave** *Cisco de 10.2.1.1 de los* router<config-radsrv>#nas
6. ***User1 del* usuario de la configuración en el servidor de RADIUS local.grupo rad-***EAP del user1 de la* **contraseña del** *user1 del* router<config-radsrv>#user
7. **Especifique el host del servidor de RADIUS.acct-puerto** *1813 Cisco* **dominante del auténtico-puerto** *1812 de 10.2.1.1 del* **host del** router<config-radsrv>#radius-server**Nota:** Esta clave debe ser lo mismo que la especificada en el comando **NAS** bajo modo de la configuración de servidor de RADIUS.

Configure el SSID para la autenticación 802.1x/EAP

La configuración de la interfaz radio y del SSID asociado para 802.1x/EAP implica la configuración de los diversos parámetros de red inalámbrica en el router, que incluye el SSID, el modo de encripción, y el tipo de autenticación. Este ejemplo utiliza el *salto* llamado SSID.

1. **Habilite la interfaz radio.**Para habilitar la interfaz radio, ir al modo de configuración de la interfaz radio del DOT11 y asignar un SSID a la interfaz.router<config>#interface **dot11radio0**el router<config-if>#no **apaga***salto del* router<config-if>#ssid
2. **Lazo SSID a un VLA N.**Para habilitar el SSID en esta interfaz, ate el SSID al VLA N en el modo de configuración SSID.*2* router<config-ssid>#vlan
3. **Configure el SSID con la autenticación 802.1x/LEAP.***eap_methods del* router<config-ssid>#authentication red-**EAP**
4. **Configure la interfaz radio para la Administración de clave dinámica.el modo del VLAN 2 del** router<config>#encryption **cifra wep40**
5. **VLA N del permiso en la interfaz radio.**router<config>#interface **Dot11Radio 0.2dot1q** *2 del*

router<config-subif>#encapsulationrouter<config-subif>#bridge-group *2*

Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N

Teclee estos comandos en el modo de configuración global de configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N:

- **excluir-direccionamiento 10.2.1.1 10.2.1.5 DHCP del IP**
- *leapauth del* **pool DHCP del IP**

En el modo de la configuración de agrupamiento DHCP, teclee estos comandos:

- **red** *10.2.0.0 255.255.0.0*
- **valor por defecto-router** *10.2.1.1*

Administración de claves WPA

El acceso protegido Wi-Fi es una mejora de la seguridad basada en estándares, interoperable que aumenta fuertemente el nivel de protección de datos y de control de acceso para los sistemas actuales y futuros del Wireless LAN.

Refiera a la administración de claves WPA para más información.

Soportes de administración de claves WPA dos mutuamente - la Administración exclusiva teclea: El WPA-PRE-Sshared cierra (WPA-PSK) y WPA (con el EAP).

Configurar el WPA-PSK

El WPA-PSK se utiliza como tipo de la administración de claves en un Wireless LAN donde no está disponible la autenticación 802.1x-based. En tales redes, usted debe configurar una clave previamente compartida en el Punto de acceso. Usted puede ingresar la clave previamente compartida como el ASCII o caracteres hexadecimales. Si usted ingresa la clave como caracteres ASCII, usted ingresa entre 8 y 63 caracteres, y el Punto de acceso amplía la clave con el proceso descrito en el estándar basado en la contraseña de la criptografía (RFC2898). Si usted ingresa la clave como caracteres hexadecimales, usted debe ingresar 64 caracteres hexadecimales.

Este ejemplo utiliza esta configuración puesta:

- Nombre SSID: **WPA-compartido**
- VLAN3
- Rango interno del servidor DHCP: **10.3.0.0/16**

Complete estas acciones en el router:

1. Configure el Integrated Routing and Bridging (IRB) y configure al Grupo de Bridge
2. Configure el (BVI) de la Interfaz Virtual Interconectada
3. Configure el SSID para la autenticación WPA-PSK
4. Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N

Configure el Integrated Routing and Bridging (IRB) y configure al Grupo de Bridge

Complete estas acciones:

1. **Habilite el IRB en el router.irb del** router<configure>#bridge**Nota:** Si se van todos los tipos de la Seguridad a ser configurados en un único router, es bastante para habilitar el IRB solamente una vez global en el router. No necesita ser habilitado para cada tipo de autenticación individual.
2. **Defina a un Grupo de Bridge.**Este ejemplo utiliza el bridge-group number **3.**router<configure>#bridge *3*
3. **Elija el Spanning Tree Protocol para el Grupo de Bridge.**El IEEE Spanning-Tree Protocol se configura para este Grupo de Bridge.**protocolo IEEE del** router<configure>#bridge *3*
4. **Permita a un BVI para validar y para rutear los paquetes enrutables recibidos de su Grupo de Bridge correspondiente.**Este ejemplo permite al BVI para validar y para rutear los paquetes del IP.*IP de la* **ruta del** router<configure>#bridge *3*

Configure el (BVI) de la Interfaz Virtual Interconectada

Complete estas acciones:

1. **Configure el BVI.**Configure el BVI cuando usted asigna el número correspondiente del Grupo de Bridge al BVI. Cada Grupo de Bridge puede solamente tener un BVI correspondiente. Este ejemplo asigna el Grupo de Bridge número 3 al BVI.router<configure>#interface **BVI** *<2>*
2. **Asigne una dirección IP al BVI.router<config-if>#ip address** *10.3.1.1 255.255.0.0*router<config-if>#no **cerrado**

Configure el SSID para la autenticación WPA-PSK

Complete estas acciones:

1. **Habilite la interfaz radio.**Para habilitar la interfaz radio, ir al modo de configuración de la interfaz radio del DOT11 y asignar un SSID a la interfaz.router<config>#interface **dot11radio0**el router<config-if>#no **apaga**router<config-if>#ssid WPA-*compartido*
2. **Para habilitar la administración de claves WPA, primero configure la cifra del cifrado WPA para la interfaz VLAN. Este ejemplo utiliza el tkip como la cifra del cifrado**.Teclee este comando de especificar el tipo de la administración de claves WPA en la interfaz radio.router<config>#interface **dot11radio0***tkip* **vlan de** *3* **cifras del modo del** #encryption del router (config-if)
3. **Lazo SSID a un VLA N.**Para habilitar el SSID en esta interfaz, ate el SSID al VLA N en el modo de configuración SSID.*3* router<config-ssid>vlan
4. **Configure el SSID con la autenticación WPA-PSK.Usted necesita configurar la autenticación EAP abierta o de la red primero en el modo de configuración SSID para habilitar la administración de claves WPA. Este ejemplo configura la autenticación abierta.**router<config>#interface **dot11radio0**router<config-if>#ssid WPA-*compartido*router<config-ssid>#authentication **abiertoAhora, administración de claves del permiso WPA en el SSID. El tkip de la cifra de la administración de claves se configura ya para este VLA N.wpa de la administración de claves del** #authentication del router (config-si-

SSID)**Configure la autenticación WPA-PSK en el SSID.** *¡*#wpa-PSK **ASCII** *1234567890 del* router (config-si-SSID)*! --- 1234567890 es el valor de clave previamente compartida para este SSID. Asegúrese de que la misma clave esté especificada para este SSID en el lado del cliente.*

5. **Habilite el VLA N en la interfaz radio.**router<config>#interface **Dot11Radio 0.3dot1q** *3 del* router<config-subif>#encapsulationrouter<config-subif>#bridge-group *3*

Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N

Teclee estos comandos en el modo de configuración global de configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N:

- **excluir-direccionamiento 10.3.1.1 10.3.1.5 DHCP del IP**
- *WPA-PSK del* **pool DHCP del IP**

En el modo de la configuración de agrupamiento DHCP, teclee estos comandos:

- **red** *10.3.0.0 255.255.0.0*
- **valor por defecto-router** *10.3.1.1*

Autenticación de la configuración WPA (con el EAP)

Éste es otro tipo de la administración de claves WPA. Aquí, los clientes y el servidor de autenticación autentican el uno al otro con un método de autenticación EAP, y el cliente y servidor genera en parejas una clave principal (PMK). Con el WPA, el servidor genera el PMK dinámicamente y lo pasa al Punto de acceso, pero, con el WPA-PSK, usted configura una clave previamente compartida en el cliente y el Punto de acceso, y esa clave previamente compartida se utiliza como el PMK.

Refiera al WPA con la autenticación EAP para más información.

Este ejemplo utiliza esta configuración puesta:

- Nombre SSID: **wpa-dot1x**
- VLA N 4
- Rango interno del servidor DHCP: **10.4.0.0/16**

Complete estas acciones en el router:

1. Configure el Integrated Routing and Bridging (IRB) y configure al Grupo de Bridge
2. Configure el (BVI) de la Interfaz Virtual Interconectada
3. Configure al servidor de RADIUS local para la autenticación WPA.
4. Configure el SSID para el WPA con la autenticación EAP
5. Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N

Configure el Integrated Routing and Bridging (IRB) y configure al Grupo de Bridge

Complete estas acciones:

1. **Habilite el IRB en el router.irb del** router<configure>#bridge**Nota:** Si se van todos los tipos de la Seguridad a ser configurados en un único router, es bastante para habilitar el IRB solamente una vez global en el router. No necesita ser habilitado para cada tipo de autenticación individual.
2. **Defina a un Grupo de Bridge.**Este ejemplo utiliza el bridge-group number **4.**router<configure>#bridge *4*
3. **Seleccione el Spanning Tree Protocol para el Grupo de Bridge.**Aquí, el IEEE Spanning-Tree Protocol se configura para este Grupo de Bridge.**protocolo IEEE del** router<configure>#bridge *4*
4. **Permita a un BVI para validar y para rutear los paquetes enrutables recibidos de su Grupo de Bridge correspondiente.**Este ejemplo permite al BVI para validar y para rutear los paquetes del IP.*IP de la* **ruta del** router<configure>#bridge *4*

Configure el (BVI) de la Interfaz Virtual Interconectada

Complete estas acciones:

1. **Configure el BVI.**Configure el BVI cuando usted asigna el número correspondiente del Grupo de Bridge al BVI. Cada Grupo de Bridge puede solamente tener un BVI correspondiente. Este ejemplo asigna el Grupo de Bridge número 4 al BVI.router<configure>#interface **BVI** *<4>*
2. **Asigne una dirección IP al BVI.router<config-if>#ip address** *10.4.1.1 255.255.0.0*router<config-if>#no **cerrado**

Configure al servidor de RADIUS local para la autenticación WPA

Refiera a la sección bajo autenticación 802.1x/EAP para el procedimiento detallado.

Configure el SSID para el WPA con la autenticación EAP

Complete estas acciones:

1. **Habilite la interfaz radio.**Para habilitar la interfaz radio, ir al modo de configuración de la interfaz radio del DOT11 y asignar un SSID a la interfaz.router<config>#interface **dot11radio0**el router<config-if>#no **apaga**router<config-if>#ssid *wpa-dot1x*
2. **Para habilitar la administración de claves WPA, primero configure la cifra del cifrado WPA para la interfaz VLAN. Este ejemplo utiliza el tkip como la cifra del cifrado**.Teclee este comando de especificar el tipo de la administración de claves WPA en la interfaz radio.router<config>#interface **dot11radio0***tkip* **vlan de** *4* **cifras del modo del** #encryption del router (config-if)
3. **Lazo SSID a un VLA N.**Para habilitar el SSID en esta interfaz, ate el SSID al VLA N en el modo de configuración SSID.*4* **vlan**
4. **Configure el SSID con la autenticación WPA-PSK.**Para configurar la interfaz radio para el WPA con la autenticación EAP, primero configure el SSID asociado para la red EAP.router<config>#interface **dot11radio0**router<config-if>#ssid WPA-*compartidoeap_methods del* **eap de la red del** router<config-ssid>#authentication
5. **Ahora, habilite la administración de claves WPA en el SSID. El tkip de la cifra de la administración de claves se configura ya para este VLA N.wpa de la administración de**

claves del #authentication del router (config-si-SSID)

6. **VLA N del permiso en la interfaz radio.**router<config>#interface **Dot11Radio 0.4dot1q** *4 del* router<config-subif>#encapsulationrouter<config-subif>#bridge-group *4*

Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N

Teclee estos comandos en el modo de configuración global de configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N:

- **excluir-direccionamiento 10.4.1.1 10.4.1.5 DHCP del IP**
- **pool** *wpa-dot1shared* **DHCP del IP**

En el modo de la configuración de agrupamiento DHCP, teclee estos comandos:

- **red** *10.4.0.0 255.255.0.0*
- **valor por defecto-router** *10.4.1.1*

Cliente de red inalámbrica de la configuración para la autenticación

Después de que usted configure el ISR, configure al cliente de red inalámbrica para diversos tipos de autenticación según lo explicado de modo que el router pueda autenticar a estos clientes de red inalámbrica y proporcionar el acceso a la red WLAN. Este documento utiliza la utilidad de escritorio del Cisco Aironet (ADU) para la configuración del client cara.

Configure al cliente de red inalámbrica para la autenticación abierta

Complete estos pasos:

1. En la ventana de administración del perfil en el ADU, haga clic **nuevo** para crear un nuevo perfil.Visualizaciones de una nueva ventana donde usted puede fijar la configuración para la autenticación abierta. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utiliza.En este ejemplo, el nombre del perfil y el SSID están **abiertos**.**Nota:** El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación abierta.
2. Haga clic la **ficha de seguridad** y deje la opción de seguridad como **ningunos** para la encripción WEP. Puesto que este ejemplo utiliza el WEP como opcional, la determinación de esta opción a ningunos permitirá que el cliente se asocie y comunique con éxito con la red WLAN.Haga clic en OK (Aceptar).
3. **Ventana avanzada** selecta de la lengueta de la **Administración del perfil** y del modo de autenticación del 802.11 del conjunto como **abierto** para la autenticación abierta.

Use esta sección para confirmar que su configuración funciona correctamente.

1. Después de que se cree el perfil del cliente, el tecleo **activa** bajo lengueta de la Administración del perfil para activar el perfil.
2. Marque el estatus ADU para una autenticación satisfactoria.

Configure al cliente de red inalámbrica para la autenticación 802.1x/EAP

Complete estos pasos:

1. En la ventana de administración del perfil en el ADU, haga clic **nuevo** para crear un nuevo perfil.Visualizaciones de una nueva ventana donde usted puede fijar la configuración para la autenticación abierta. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utiliza.En este ejemplo, el nombre del perfil y el SSID son **salto**.
2. Bajo **Administración del perfil**, haga clic la **ficha de seguridad**, fije la opción de seguridad como 802.1x, y elija el tipo apropiado EAP. Este documento utiliza el SALTO como el tipo EAP para la autenticación. Ahora, **configuración del** tecleo para configurar las configuraciones del nombre de usuario y contraseña del SALTO.**Nota:** Nota: El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación 802.1x/EAP.
3. Bajo configuraciones del nombre de usuario y contraseña, este ejemplo elige **indicar manualmente para el Nombre de usuario y la contraseña** para indicar al cliente que ingrese el Nombre de usuario y la contraseña correctos mientras que el cliente intenta conectar con la red. Haga clic en OK.

Use esta sección para confirmar que su configuración funciona correctamente.

- Después de que se cree el perfil del cliente, el tecleo **activa** bajo lengueta de la **Administración del perfil** para activar el **salto del** perfil. Le indican para el nombre y la contraseña de **usuario LEAP**. Este ejemplo utiliza el **user1 del** nombre de usuario y contraseña. Haga clic en OK.
- Usted puede mirar al cliente autenticar con éxito y ser asignado una dirección IP del servidor DHCP configurado en el router.

Configure al cliente de red inalámbrica para la autenticación WPA-PSK

Complete estos pasos:

1. En la ventana de administración del perfil en el ADU, haga clic **nuevo** para crear un nuevo perfil.Visualizaciones de una nueva ventana donde usted puede fijar la configuración para la autenticación abierta. Conforme a la **ficha general**, ingrese el **nombre del perfil** y el **SSID** que el adaptador del cliente utiliza.En este ejemplo, WPA-**se comparten el** nombre del perfil y el SSID.**Nota:** El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación WPA-PSK.
2. Bajo **Administración del perfil**, haga clic la **ficha de seguridad** y fije la opción de seguridad como **WPA/WPA2 passphrase**. Ahora, **configuración del** tecleo para configurar el passphrase WPA.
3. Defina una clave previamente compartida WPA. La clave debe ser 8 a 63 caracteres ASCII de largo. Haga clic en OK.

Use esta sección para confirmar que su configuración funciona correctamente.

- Después de que se cree el perfil del cliente, el tecleo **activa** bajo lengueta de la **Administración del perfil** para activar el perfil WPA-**compartido**.
- Marque el ADU para una autenticación satisfactoria.

Configure al cliente de red inalámbrica para la autenticación WPA (con el EAP)

Complete estos pasos:

1. En la ventana de administración del perfil en el ADU, haga clic **nuevo** para crear un nuevo perfil.Visualizaciones de una nueva ventana donde usted puede fijar la configuración para la autenticación abierta. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utiliza.En este ejemplo, el nombre del perfil y el SSID son **wpa-dot1x**.**Nota:** El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación WPA (con el EAP).
2. Bajo **Administración del perfil**, haga clic la **ficha de seguridad**, fije la opción de seguridad como **WPA/WPA2/CCKM**, y y elija WPA/WPA2/CCKM el tipo apropiado EAP. Este documento utiliza el SALTO como el tipo EAP para la autenticación. Ahora, **configuración del** tecleo para configurar las configuraciones del nombre de usuario y contraseña del SALTO.
3. Bajo área de las configuraciones del nombre de usuario y contraseña, este ejemplo elige **indicar manualmente para el Nombre de usuario y la contraseña** para indicar al cliente que ingrese el Nombre de usuario y la contraseña correctos mientras que el cliente intenta conectar con la red. Haga clic en OK.

Use esta sección para confirmar que su configuración funciona correctamente.

1. Después de que se cree el perfil del cliente, el tecleo **activa** bajo lengueta de la Administración del perfil para activar el perfil **wpa-dot1x**. Le indican para el nombre y la contraseña de usuario LEAP. Este ejemplo utiliza el nombre de usuario y contraseña como **user1**. Haga clic en OK.
2. Usted puede mirar al cliente autenticar con éxito.

El comando show dot11 associations del router CLI visualiza a las profundidades totales en el estatus de la asociación del cliente. Aquí está un ejemplo.

Asociaciones del dot11 de Router#show

```
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address IP address Device Name Parent State 0040.96ac.e657 10.3.0.2 CB21AG/PI21AG WCS self EAP-Assoc SSID [open] : SSID [pre-shared] : DISABLED, not associated with a configured VLAN SSID [wpa-dot1x] : SSID [wpa-shared] : Others: (not related to any ssid)
```

Troubleshooting

Comandos para resolución de problemas

Usted puede utilizar estos comandos debug de resolver problemas su configuración.

- **authenticator todo aaa del dot11 del debug** — Activa el debugging del MAC y de los paquetes de la autenticación EAP.
- **autenticación de RADIUS del debug** — Visualiza las negociaciones RADIUS entre el servidor y el cliente.
- **paquetes del servidor local del radio del debug** — Visualiza el contenido de los paquetes RADIUS se envían y se reciben que.
- **cliente del servidor local del radio del debug** — Visualiza los mensajes de error sobre las autenticaciones de cliente falladas.

Información Relacionada

- Autenticación en los ejemplos de configuración de los reguladores del Wireless LAN
- Configurar los VLA N en los Puntos de acceso
- Router inalámbrico de 1800 ISR con el DHCP y el ejemplo de configuración internos de la autenticación abierta
- Tecnología inalámbrica de Cisco ISR y guía de Configuración de punto de acceso HWIC
- Conectividad del Wireless LAN usando un ISR con el ejemplo de configuración de la encripción WEP y de la autenticación LEAP
- Soporte Técnico y Documentación - Cisco Systems
- Configuración de los tipos de autenticación
- Conectividad del Wireless LAN usando un ISR con el ejemplo de configuración de la encripción WEP y de la autenticación LEAP