Tipos de autenticación inalámbricos en el ISR fijo con el ejemplo de la configuración de SDM

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Antecedentes
Configurar
Diagrama de la red
Configure al router para el acceso del SDM
Ponga en marcha la aplicación inalámbrica del SDM en el router
Configure la autenticación abierta con la encripción WEP
Configure al servidor DHCP interno para los clientes de red inalámbrica de este VLA N
Configure abierto con la autenticación de MAC
Configure la autenticación 802.1x/EAP
Configure la autenticación compartida
Configure la autenticación WPA
Configure la autenticación WPA-PSK
Configuración de cliente de red inalámbrica
Cliente de red inalámbrica de la configuración para la autenticación abierta con la encripción WEP
Cliente de red inalámbrica de la configuración para abierto con la autenticación de MAC
Cliente de red inalámbrica de la configuración para la autenticación 802.1x/EAP
Cliente de red inalámbrica de la configuración para la autenticación compartida
Cliente de red inalámbrica de la configuración para la autenticación WPA
Cliente de red inalámbrica de la configuración para la autenticación WPA-PSK
Troubleshooting
Comandos para resolución de problemas
Información Relacionada

Introducción

Este documento proporciona los ejemplos de configuración que explican 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 el (SDM) del Administrador de dispositivos de seguridad.

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) con el SDM
- 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 el Software Release 12.3(8)YI1 de Cisco IOS®
- Versión 2.4.1 del SDM de Cisco instalada en el ISR
- 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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

El SDM de Cisco es una herramienta de Administración de dispositivos intuitiva, basada en web para los routeres basados en software del Cisco IOS. El SDM de Cisco simplifica el router y la Configuración de seguridad a través de los Asisitente elegantes, que ayudan a los clientes de manera rápida y fácil a desplegar, a configurar, y a monitorear al Routers del ® de Cisco Systems sin requerir el conocimiento del comando line interface(cli) del Cisco IOS Software.

El SDM se puede descargar gratuitamente del centro de software en el cisco.com.

El SDM puede ser instalado independientemente mientras que una copia separada en cada los routeres individuales, o él se puede también instalar en un PC. El SDM de Cisco instalado en un PC permite que usted utilice el SDM para manejar al otro Routers que funciona con las imágenes del IOS apropiadas en la red. Sin embargo, el SDM en un PC no soporta la restauración de la configuración del router para fabricar el valor por defecto.

Este documento utiliza el SDM instalado en el router inalámbrico para configurar al router para la autenticación inalámbrica.

El SDM de Cisco comunica con el Routers para dos propósitos:

- Acceda los archivos de aplicación del SDM de Cisco para la descarga al PC
- Lea y escriba la configuración del router y el estatus

El SDM de Cisco utiliza el HTTP para descargar los archivos de aplicación (sdm.tar, home.tar) al PC. Una combinación de HTTP y de telnet/SSH se utiliza para leer y para escribir la configuración del router.

Refiera al Q&A de Router de Cisco y Administrador de dispositivo de seguridad para información de última hora sobre el Routers y las versiones de software IOS que soportan el SDM.

Refiera a la configuración su router para soportar el SDM para más información sobre cómo utilizar el SDM de Cisco en un router.

Refiérase instalan los archivos del SDM para que las instrucciones instalen y descarguen los archivos del SDM en el router o en el PC.

Configurar

El documento explica cómo configurar estos tipos de autenticación con el SDM:

- Autenticación abierta con la encripción WEP
- Ábrase con la autenticación de MAC
- Autenticación compartida
- autenticación del protocolo de autenticación 802.1x/Extensible (EAP)
- Acceso protegido de Wi-Fi (WPA) - Pre autenticación de la clave compartida (PSK)
- Autenticación WPA

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 que usan la autenticación del 802.1x.

Configure al router para el acceso del SDM

Complete estos pasos para permitir que accedan al router con el SDM:

1. Configure al router para el HTTP/el acceso del https usando el procedimiento explicado adentro configuran a su router para soportar el SDM.
2. Asigne una dirección IP al router con estos pasos:`Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#interface fastEthernet 0 Router(config-if)#ip address 10.77.244.197 255.255.255.224 % IP addresses cannot be configured on L2 links.` En el 871W Router, usted puede ser que encuentre tal mensaje de error. Este mensaje de error muestra que el fast ethernet 0 es un link de la capa

2 en el cual usted no puede configurar ninguna dirección IP.

3. Para superar este problema, cree una interfaz de la capa 3 (VLA N) y asigne una dirección IP en lo mismo con estos pasos:`Router(config)#interface Vlan1 Router(config-if)#ip address 10.77.244.197 255.255.255.224`
4. No prohiba a este VLA N en los fast ethernet de la capa 2 0 interfaces con estos pasos. Este documento configura la interfaz Fast Ethernet como interfaz de tronco para permitir el VLAN1. Usted puede también configurarlo como interfaz de acceso y permitir el VLAN1 en la interfaz por su configuración de la red.`Router(config)#interface fastEthernet 0 Router(config-if)#switchport trunk encapsulation dot1q Router(config-if)#switchport trunk allowed vlan add vlan1 !--- This command allows VLAN1 through the fast ethernet interface. !--- In order to allow all VLANs through this interface, issue the !--- switchport trunk allowed vlan add all command on this interface.` **Nota:** Este ejemplo asume que realizan al router básico y las configuraciones de red inalámbrica ya en el router. Por lo tanto, el siguiente paso es inmediatamente poner en marcha la aplicación inalámbrica en el router para configurar los parámetros de autenticación.

Ponga en marcha la aplicación inalámbrica del SDM en el router

Complete estos pasos para poner en marcha la aplicación inalámbrica:

1. Comience el SDM abriendo un hojeador y ingresando el IP Address de su router.A le indican que valide o disminuya una ventana de la alerta de seguridad del buscador Web que parezca esto:
2. Haga clic **sí** para proceder.
3. En la ventana que aparece, ingrese el nombre de usuario y contraseña del privilegio level_15 para acceder al router.Este ejemplo utiliza el **admin** como el nombre de usuario y contraseña:
4. Para continuar, haga clic en OK (Aceptar). Ingrese la misma información dondequiera que se requiera.
5. Tecleo **sí** y **OK** como apropiado en las páginas resultantes para poner en marcha la aplicación del SDM.Mientras que la aplicación del SDM se abre, una ventana de la alerta de seguridad a le indica que valide un Security Certificate firmado.
6. Haga clic **sí** para validar el certificado firmado.El router Cisco y la página principal resultantes del SDM parecen esto:
7. En esta página, **configuración del** tecleo en el superior para iniciar la ventana del modo de la configuración del router.
8. En la ventana del modo de la configuración, seleccione las **interfaces y las conexiones de la** columna de las tareas que aparece en el lado izquierdo de esta página.
9. En la ventana de las interfaces y de las conexiones, haga clic la lengueta de la **conexión del crear**.Esto enumera todas las interfaces disponibles para ser configurada en el router.
10. Para poner en marcha la aplicación inalámbrica, elija la **Tecnología inalámbrica de la** lista de interfaces. Entonces, **aplicación de la Tecnología inalámbrica del lanzamiento del** tecleo.Este tiro de pantalla explica los pasos 8, 9 y 10:Esto pone en marcha la aplicación inalámbrica del SDM en una ventana separada donde los diversos tipos de autenticación pueden ser configurados.El Home Page inalámbrico de la aplicación del SDM parece esto:Observe que **inhabilitan al** estado del software y el estado del hardware de la interfaz de radio (de la Tecnología inalámbrica) está **abajo** porque no se configura ningún SSID en la interfaz. Después, usted configura los SSID y los tipos de autenticación en esta interfaz radio de modo que los clientes de red inalámbrica puedan comunicar a través de esta

interfaz.

Autenticación abierta de la configuración con la encripción WEP

La autenticación abierta es un algoritmo de la autenticación nula. El punto de acceso concederá 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 AP puede acceder a la red. Con la encripción WEP habilitada en un AP, 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 podrá transmitir los datos con el AP. También, no puede desencriptar los datos enviados del AP.

Refiera a la autenticación abierta al Punto de acceso para más información.

Este ejemplo utiliza estos parámetros de la configuración para la autenticación abierta con la encripción WEP:

- Nombre SSID: **openwep**
- Identificación de VLAN: **1**
- Dirección IP del VLA N: **10.1.1.1/16**
- Rango de DHCP Address para los clientes de red inalámbrica de este VLAN/SSID: **10.1.1.5/16 - 10.1.1.10/16**

Complete estos pasos para configurar la autenticación abierta con el WEP:

1. En el Home Page inalámbrico de la aplicación, haga clic los **Servicios inalámbricos** > el **VLA N** para configurar un VLA N.
2. Seleccione la **encaminamiento de los** servicios: Página del VLA N.
3. En los servicios: La página del routing VLAN, crea el VLA N y lo asigna a la interfaz radio.Ésta es la ventana de configuración de VLAN1 en la interfaz radio. El VLAN1 es el VLAN nativo aquí:
4. En el Home Page inalámbrico de la aplicación, seleccione la **seguridad de red inalámbrica** > al **administrador SSID** para configurar el SSID y el tipo de autenticación.
5. En la Seguridad: La página del administrador SSID, configura el SSID y asigna el SSID al VLA N creado en step1 para habilitar el SSID en la interfaz radio.
6. Bajo sección de las configuraciones de la autenticación de esta página, elija la **autenticación abierta**.Aquí está la ventana de configuración que explica estos pasos:
7. Haga clic en Apply (Aplicar).**Nota:** La casilla desplegable que corresponde al casilla “Abrir autenticación” implica que la autenticación abierta se puede configurar además con varios tipos de autenticación adicionales, tales como EAP o autenticación de MAC. Esta sección discute solamente la autenticación abierta sin la ADICIÓN (sin el tipo de autenticación adicional).
8. Encripción WEP de la configuración para este SSID/VLAN. En el Home Page inalámbrico, seleccione al **administrador de la seguridad de red inalámbrica** > del **cifrado** para configurar las configuraciones de encripción.En la Seguridad: La página del administrador del cifrado, fijó el modo de encripción y las claves para el **VLAN1**.Elija la **encripción WEP: Obligatorio** como el modo de encripción.Fije la clave de encripción para este VLA N.Esta sección utiliza estas configuraciones de la clave de encripción:Slot1 de la clave de encripción: utilizado como la clave de transmitirTamaño de la clave de encripción: bit 40Clave de encripción en el valor hexadecimal: 1234567890**Nota:** El mismo slot de la clave de encripción (1, en este

caso) se debe utilizar como la clave de transmitir en el cliente de red inalámbrica. También, el cliente de red inalámbrica debe ser configurado con el mismo valor de la clave (1234567890 en este caso) para que el cliente de red inalámbrica comunique con esta red WLAN.Esta ventana de configuración explica estos pasos:Esta página de la seguridad de red inalámbrica representa la configuración completa:

Servidor DHCP interno de la configuración para los clientes de red inalámbrica de este VLA N

Complete estos pasos para configurar a un servidor DHCP interno en el router. Éste es un opcional, aunque recomendado, método para asignar la dirección IP a los clientes de red inalámbrica.

1. En la ventana del modo de la configuración del SDM, seleccione las **tareas adicionales** bajo la columna de las tareas que está en el lado izquierdo de la ventana.
2. En las **tareas adicionales** pagine, amplíe el árbol del **DHCP** y elija a los **agrupamientos DHCP** tal y como se muestra en de este ejemplo. En la columna de los agrupamientos DHCP mostrada a la derecha de esta página, el tecleo **agrega** para crear a un nuevo agrupamiento DHCP.
3. En la página del agrupamiento DHCP del agregar, especifique el nombre del agrupamiento DHCP, red del agrupamiento DHCP, máscara de subred, comenzando la dirección IP, terminando los parámetros de la dirección IP y del router predeterminado tal y como se muestra en de este ejemplo:
4. Haga clic en OK.Configuran al servidor DHCP interno en el router.

Configuración abierta con la autenticación de MAC

En este tipo de autenticación, se permitirá al cliente de red inalámbrica acceder la red WLAN solamente si la dirección MAC del cliente está conforme a la lista de direcciones MAC permitidas en el servidor de autenticación. El AP retransmite la dirección MAC del dispositivo de red inalámbrica de cliente a un servidor de autenticación de RADIUS en su red, y el servidor marca el direccionamiento contra una lista de direcciones MAC permitidas. La autenticación MAC basada proporciona un método de autentificación alterno para los dispositivos del cliente que no tienen capacidad EAP.

Refiera a la autenticación de la dirección MAC a la red para más información.

Nota: El documento entero utiliza al servidor de RADIUS local para la autenticación de MAC, 802.1x/EAP, así como la autenticación WPA.

Este ejemplo utiliza estos parámetros de la configuración para abierto con la autenticación de MAC:

- Nombre SSID: **openmac**
- Identificación de VLAN: **2**
- Dirección IP del VLA N: **10.2.1.1/16**
- Rango de DHCP Address para los clientes de red inalámbrica de este VLAN/SSID: **10.2.1.5/16 - 10.2.1.10/16**

Complete estos pasos para configurar abierto con la autenticación de MAC:

1. En el Home Page inalámbrico de la aplicación, haga clic los **Servicios inalámbricos** > el **VLA N** para configurar un VLA N.
2. Seleccione la **encaminamiento de los** servicios: Página del VLA N. En los servicios: La página del routing VLAN, crea el VLA N y lo asigna a la interfaz radio.Aquí está la ventana de configuración de **VLAN2** en la interfaz radio:
3. Configure al servidor de RADIUS local para la autenticación de MAC. Este servidor de RADIUS local llevará a cabo la dirección MAC del cliente de red inalámbrica en su base de datos y permitirá o negará al cliente en la red WLAN según el resultado de la autenticación.En el Home Page inalámbrico, seleccione la **seguridad de red inalámbrica** > al **administrador de servidor** para configurar al servidor de RADIUS local.En la página del administrador de servidor, configure la dirección IP, secreto compartido, y la autenticación y los puertos de contabilidad del servidor de RADIUS.Porque es servidor de RADIUS local, la dirección IP especificada es el direccionamiento de esta interfaz inalámbrica. La clave secreta compartida usada debe ser lo mismo en la configuración de cliente AAA.En este ejemplo, el secreto compartido es **Cisco**.Haga clic en Apply (Aplicar).Navegue hacia abajo la página para buscar la sección de prioridades predeterminada del servidor. En esta sección, elija a este servidor de RADIUS (**10.2.1.1**) como el servidor de la prioridad predeterminada para la autenticación de MAC tal y como se muestra en de este ejemplo:Para configurar el cliente AAA y los credenciales de usuario, seleccione la **seguridad de red inalámbrica** > **servidor de RADIUS local del** Home Page inalámbrico.En la página del servidor RADIUS local, haga clic la **CONFIGURACIÓN GENERAL**.En la página de configuración GENERAL, configure el cliente AAA y la clave secreta compartida como se muestra.Con una configuración de servidor de RADIUS local, la dirección IP del servidor y el cliente AAA serán lo mismo.Navegue hacia abajo la página de configuración GENERAL para buscar la sección de configuración de los **usuarios individuales**. En los usuarios individuales seccione, configure la dirección MAC del cliente de red inalámbrica como nombre de usuario y contraseña.Habilite la casilla de verificación de la **autenticación de MAC solamente**, después haga clic **se aplican**.Para evitar al cliente de la falla de autenticación a veces, especifique la dirección MAC del cliente en un formato continuo sin ninguna separación tal y como se muestra en de este ejemplo.
4. En el Home Page inalámbrico de la aplicación, seleccione la **seguridad de red inalámbrica** > al **administrador SSID** para configurar el SSID y el tipo de autenticación.En la Seguridad: La página del administrador SSID, configura el SSID y asigna el SSID al VLA N creado en step1 para habilitar el SSID en la interfaz radio.Bajo sección de las configuraciones de la autenticación de esta página, elija la **autenticación abierta** y de la casilla desplegable correspondiente, eligen **con la autenticación de MAC**.Para configurar las prioridades del servidor, elija **personalizan** bajo el MAC autentican los servidores y eligen la dirección IP del servidor de RADIUS local **10.2.1.1**.Éste es un ejemplo que explica este paso:
5. Para configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N, complete los mismos pasos explicados en el servidor DHCP interno de la configuración para los clientes de red inalámbrica de esta sección del VLA N de este documento con estos parámetros de la configuración:Nombre del agrupamiento DHCP: VLAN2Red del agrupamiento DHCP: 10.2.0.0Máscara de subred: 255.255.0.0Comenzar el IP: 10.2.1.5Terminación del IP: 10.2.1.10Router predeterminado: 10.2.1.1

Autenticación de la configuración 802.1x/EAP

Este tipo de autenticación proporciona el del más alto nivel de la Seguridad para su red

inalámbrica. Usando el EAP a obrar recíprocamente con un servidor de RADIUS EAP-compatible, el AP 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 AP que la utiliza para todas las señales de datos de unidifusión a las cuales envíe, o la recibe, del cliente.

Refiera a la autenticación EAP a la red para más información.

Nota: Hay varios métodos de autenticación EAP disponibles. En este documento, explica cómo configurar el protocolo lightweight extensible authentication (SALTO) como la autenticación EAP. El SALTO utiliza el nombre de usuario y contraseña como credenciales de usuario para la autenticación.

Nota: Para configurar la autenticación adaptable de EAP vía el Tunelización seguro (EAP-FAST) como el tipo de la autenticación EAP, refiera a la guía de configuración de la versión 1.02 del EAP-FAST para el procedimiento.

Este ejemplo utiliza estos parámetros de la configuración para la autenticación EAP:

- Nombre SSID: **salto**
- Identificación de VLAN: **3**
- Dirección IP del VLA N: **10.3.1.1/16**
- Rango de DHCP Address para los clientes de red inalámbrica de este VLAN/SSID: **10.3.1.5/16 - 10.3.1.10/16**

Complete estos pasos para configurar la autenticación EAP:

1. Relance los pasos 1 y 2 de configuración abierta con la autenticación de MAC para crear y configurar el VLA N con estos parámetros de la configuración:Identificación de VLAN: 3Dirección IP de la interfaz radio: 10.3.1.1máscara de subred: 255.255.0.0
2. Entonces, configure al servidor de RADIUS local para la autenticación de cliente. Para realizar esto, relance los pasos 3a a 3c de la configuración abierto con la autenticación de MAC con estos parámetros de la configuración:Dirección IP del servidor de RADIUS: 10.3.1.1Secreto compartido: CiscoAquí está la pantalla de configuración que explica el paso 2 de la autenticación EAP:
3. Navegue hacia abajo la página para buscar la sección de prioridades predeterminada del servidor. En esta sección, elija a este servidor de RADIUS (**10.3.1.1**) como el servidor de la prioridad predeterminada para la autenticación EAP tal y como se muestra en de este ejemplo.
4. Relance los pasos 3e y 3f de la configuración se abren con la autenticación de MAC.
5. Relance los pasos 3g y 3h de la configuración se abren con la autenticación de MAC con estos parámetros de la configuración para la autenticación EAP:Dirección IP del cliente AAA: 10.3.1.1Secreto compartido: CiscoBajo sección de los usuarios individuales, configure el nombre de usuario y contraseña como **user1**.
6. En el Home Page inalámbrico de la aplicación, seleccione la **seguridad de red inalámbrica** > al **administrador SSID** para configurar el SSID y el tipo de autenticación.En la Seguridad: La página del administrador SSID, configura el SSID y asigna el SSID al VLA N creado en el paso 1 para habilitar el SSID en la interfaz radio.Bajo sección de las configuraciones de la autenticación de esta página, elija la **autenticación abierta** y de la casilla desplegable correspondiente, eligen la **autenticación EAP**. También, seleccione el tipo de la **autenticación EAP de la red**.Para configurar las prioridades del servidor, elija **personalizan** bajo el EAP

autentican los servidores y eligen la dirección IP del servidor de RADIUS local **10.3.1.1**.Aquí está un ejemplo que explica estos pasos:

7. Para configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N, complete los mismos pasos explicados en el servidor DHCP interno de la configuración para los clientes de red inalámbrica de esta sección del VLA N de este documento con estos parámetros de la configuración:Nombre del agrupamiento DHCP: VLAN3Red del agrupamiento DHCP: 10.3.0.0Máscara de subred: 255.255.0.0Comenzar el IP: 10.3.1.5Terminación del IP: 10.3.1.10Router predeterminado: 10.3.1.1
8. Configure la cifra que se utilizará para la Administración de clave dinámica sobre la autenticación satisfactoria del cliente de red inalámbrica.En el Home Page inalámbrico, seleccione al **administrador de la seguridad de red inalámbrica** > del **cifrado** para configurar las configuraciones de encripción.En la pantalla del administrador de la seguridad de red inalámbrica > del cifrado en la Seguridad: La página del administrador del cifrado, ingresa **3** para el modo de encripción y las claves del conjunto para el VLA N.Elija la **cifra** como el modo de encripción, y elija un algoritmo de encripción de la cifra de la casilla desplegable.Este ejemplo utiliza el **TKIP** como el algoritmo de la cifra:**Nota:** Mientras que configura la autenticación múltiple teclea en un router inalámbrico con el SDM, a veces él no pudo ser posible configurar dos diversos tipos de autenticación ambos usando el modo de encripción de la cifra en el mismo router. En estos casos, la configuración de encripción configurada con el SDM no se pudo aplicar en el router. Para superar esto, configure esos tipos de autenticación con el CLI.

Configure la autenticación compartida

Cisco proporciona la clave de autenticación compartida para cumplir con el estándar del IEEE 802.11B.

Durante la clave de autenticación compartida, el AP envía una cadena de texto de impugnación unencrypted a cualquier dispositivo que intente comunicar con el AP. El dispositivo que pide la autenticación cifra el texto de impugnación y lo envía de nuevo al AP. Si el texto de impugnación se cifra correctamente, el AP permite que el dispositivo solicitante autentique. El desafío unencrypted y el desafío cifrado pueden ser monitoreados. Sin embargo, esto sale del AP abierto para atacar de un intruso que calcule la clave WEP comparando las cadenas de texto unencrypted y cifradas.

Refiera a la clave de autenticación compartida al Punto de acceso para más información.

Este ejemplo utiliza estos parámetros de la configuración para la autenticación compartida:

- Nombre SSID: **compartido**
- Identificación de VLAN: **4**
- Dirección IP del VLA N: **10.4.1.1/16**
- Rango de DHCP Address para los clientes de red inalámbrica de este VLAN/SSID: **10.4.1.5/16 - 10.4.1.10/16**

Complete estos pasos para configurar la autenticación compartida:

1. Relance los pasos 1 y 2 de configuración abierta con la autenticación de MAC para crear y configurar el VLA N con estos parámetros de la configuración:Identificación de VLAN: 4Dirección IP de la interfaz radio: 10.4.1.1máscara de subred: 255.255.0.0

2. En el Home Page inalámbrico de la aplicación, seleccione la **seguridad de red inalámbrica >** al **administrador SSID** para configurar el SSID y el tipo de autenticación.En la Seguridad: La página del administrador SSID, configura el SSID y asigna el SSID al VLA N creado en step1 para habilitar el SSID en la interfaz radio.Bajo sección de las configuraciones de la autenticación de esta página, elija la **autenticación compartida**.Aquí está la pantalla de configuración que explica estos pasos:Haga clic en Apply (Aplicar).
3. Encripción WEP de la configuración para este SSID/VLAN. Porque es la clave de autenticación compartida, la misma clave se utiliza para la autenticación también. En el Home Page inalámbrico, seleccione al **administrador de la seguridad de red inalámbrica >** del **cifrado** para configurar las configuraciones de encripción.En la Seguridad: La página del administrador del cifrado, ingresa **4** para el modo de encripción y las claves del conjunto para el VLA N.Elija la **encripción WEP: Obligatorio** como el modo de encripción.Fije la clave de encripción para este VLA N.Esta sección utiliza estas configuraciones de la clave de encripción:Slot1 de la clave de encripción: utilizado como la clave de transmitirTamaño de la clave de encripción: bit 40Clave de encripción en el valor hexadecimal: 1234567890**Nota:** El mismo slot de la clave de encripción (1, en este caso) se debe utilizar como la clave de transmitir en el cliente de red inalámbrica. También, el cliente de red inalámbrica debe ser configurado con el mismo valor de la clave (1234567890 en este caso) para que el cliente de red inalámbrica comunique con esta red WLAN.Esta pantalla de configuración explica estos pasos:
4. Para configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N, complete los mismos pasos explicados en el servidor DHCP interno de la configuración para los clientes de red inalámbrica de esta sección del VLA N de este documento con estos parámetros de la configuración:Nombre del agrupamiento DHCP: VLA N 4Red del agrupamiento DHCP: 10.4.0.0Máscara de subred: 255.255.0.0Comenzar el IP: 10.4.1.5Terminación del IP: 10.4.1.10Router predeterminado: 10.4.1.1

Autenticación de la configuración WPA

El WPA 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 existir y los sistemas futuros del Wireless LAN. Soportes de administración de claves WPA dos mutuamente - la Administración exclusiva teclea: WPA y WPA-PSK.

Refiérase con la administración de claves WPA para más información.

Usando la administración de claves WPA, los clientes y el servidor de autenticación autentican el uno al otro usando un método de autenticación EAP, y el cliente y servidor genera en parejas una clave principal (PMK). Usando el WPA, el servidor genera el PMK dinámicamente y lo pasa al AP.

Este ejemplo utiliza estos parámetros de la configuración para la autenticación WPA:

- Nombre SSID: **wpa**
- Identificación de VLAN: **5**
- Dirección IP del VLA N: **10.5.1.1/16**
- Rango de DHCP Address para los clientes de red inalámbrica de este VLAN/SSID: **10.5.1.5/16 - 10.5.1.10/16**

Complete estos pasos para configurar la autenticación WPA:

1. Relance los pasos 1 y 2 de configuración abierta con la autenticación de MAC para crear y configurar el VLA N con estos parámetros de la configuración:Identificación de VLAN: 5Dirección IP de la interfaz radio: 10.5.1.1máscara de subred: 255.255.0.0
2. Porque el WPA es un estándar de la administración de claves, configure la cifra que se utilizará para la administración de claves WPA.En el Home Page inalámbrico, seleccione al **administrador de la seguridad de red inalámbrica** > del **cifrado** para configurar las configuraciones de encripción.En la pantalla del administrador de la seguridad de red inalámbrica > del cifrado en la Seguridad: La página del administrador del cifrado, ingresa **5** para el modo de encripción y las claves del conjunto para el VLA N.Elija la **cifra** como modo de encripción, y elija un algoritmo de encripción de la cifra de la casilla desplegable.Este ejemplo utiliza el **TKIP** como el algoritmo de la cifra:**Nota:** Mientras que configura la autenticación múltiple teclea en un router inalámbrico con el SDM, a veces él no pudo ser posible configurar dos diversos tipos de autenticación ambos usando el modo de encripción de la cifra en el mismo router. En estos casos, la configuración de encripción configurada con el SDM no se pudo aplicar en el router. Para superar esto, configure esos tipos de autenticación con el CLI.
3. El siguiente paso es configurar al servidor de RADIUS local para la autenticación de cliente. Para realizar esto, relance los pasos 3a a 3c de la configuración abierto con la autenticación de MAC con estos parámetros de la configuración:Dirección IP del servidor de RADIUS: 10.5.1.1Secreto compartido: CiscoNavegue hacia abajo la página del **administrador de servidor** para buscar la sección de prioridades predeterminada del servidor. En esta sección, elija a este servidor de RADIUS (**10.5.1.1**) como el servidor de la prioridad predeterminada para la autenticación EAP tal y como se muestra en de este ejemplo:Relance los pasos 3e y 3f de la configuración se abren con la autenticación de MAC.Relance los pasos 3g y 3h de la configuración se abren con la autenticación de MAC con estos parámetros de la configuración para la autenticación EAP:Dirección IP del cliente AAA: 10.5.1.1Secreto compartido: CiscoBajo sección de los usuarios individuales, configure el nombre de usuario y contraseña como **user2**.
4. Para habilitar el WPA para un SSID, usted necesita habilitar abierto con el EAP o la red EAP en el SSID. Para habilitar la red EAP, en el Home Page inalámbrico de la aplicación, selecciona la **seguridad de red inalámbrica** > al **administrador SSID** para configurar el SSID y el tipo de autenticación.En la Seguridad: La página del administrador SSID, configura el SSID y asigna el SSID al VLA N creado en step1 para habilitar el SSID en la interfaz radio.Bajo sección de las configuraciones de la autenticación de esta página, elija la **autenticación abierta** y de la casilla desplegable correspondiente, eligen la **autenticación EAP**. También, seleccione el tipo de la **autenticación EAP de la red**.Para configurar las prioridades del servidor, elija **personalizan** bajo el EAP autentican los servidores y eligen la dirección IP del servidor de RADIUS local **10.5.1.1**.Aquí está un ejemplo que explica estos pasos:
5. Navegue hacia abajo la página del administrador SSID para buscar la sección de **administración de claves autenticada**.
6. En esta sección, elija **obligatorio de la** casilla desplegable de la administración de claves, y habilite la **casilla de verificación WPA**.Aquí está la ventana de configuración que explica estos pasos:
7. Haga clic en Apply (Aplicar).
8. Para configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N, complete los mismos pasos explicados en el servidor DHCP interno de la configuración para los clientes de red inalámbrica de esta sección del VLA N de este documento con estos

parámetros de la configuración:Nombre del agrupamiento DHCP: VLA N 5Red del agrupamiento DHCP: 10.5.0.0Máscara de subred: 255.255.0.0Comenzar el IP: 10.5.1.5Terminación del IP: 10.5.1.10Router predeterminado: 10.5.1.1

Autenticación de la configuración WPA-PSK

Llaman el otro tipo de la administración de claves WPA el WPA-PSK. El WPA-PSK se utiliza para soportar el WPA en un Wireless LAN donde no está disponible la autenticación 802.1x-based. Con este tipo, usted debe configurar una clave previamente compartida en el AP. 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 AP amplía la clave usando 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 estos parámetros de la configuración para la autenticación WPA-PSK:

- Nombre SSID: **WPA-PSK**
- Identificación de VLAN: **6**
- Dirección IP del VLA N: **10.6.1.1/16**
- Intervalo de direcciones HCP para los clientes de red inalámbrica de este VLAN/SSID: **10.6.1.5/16 - 10.6.1.10/16**

Complete estos pasos para configurar el WPA-PSK:

1. Relance los pasos 1 y 2 de configuración abierta con la autenticación de MAC para crear y configurar el VLA N con estos parámetros de la configuración:Identificación de VLAN: 6Dirección IP de la interfaz radio: 10.6.1.1máscara de subred: 255.255.0.0
2. Porque el WPA-PSK es un estándar de la administración de claves, configure la cifra que se utilizará para la administración de claves WPA.En el Home Page inalámbrico, seleccione al **administrador de la seguridad de red inalámbrica** > del **cifrado** para configurar las configuraciones de encripción.En la **ventana de administrador de la seguridad de red inalámbrica** > del **cifrado** en la Seguridad: La página del administrador del cifrado, ingresa **6** para el modo de encripción y las claves del conjunto para el VLA N.Elija la **cifra** como modo de encripción, y elija un algoritmo de encripción de la cifra de la casilla desplegable.Este ejemplo utiliza **TKIP+WEP 128bit** como el algoritmo de la cifra.**Nota:** Mientras que configura la autenticación múltiple teclea en un router inalámbrico con el SDM, a veces él no pudo ser posible configurar dos diversos tipos de autenticación ambos usando el modo de encripción de la cifra en el mismo router. En estos casos, la configuración de encripción configurada con el SDM no se pudo aplicar en el router. Para superar esto, configure esos tipos de autenticación con el CLI.
3. Para habilitar el WPA-PSK para un SSID, usted necesita habilitar la autenticación abierta en el SSID. Para habilitar la autenticación abierta, relance el paso 6 de la autenticación abierta de la configuración con la encripción WEP.Aquí está la ventana de configuración de WPA-PSK:
4. Navegue hacia abajo la página del administrador SSID para buscar la sección de **administración de claves autenticada**.
5. En esta sección, elija **obligatorio de la** casilla desplegable de la administración de claves, habilite la **casilla de verificación WPA** y ingrese la clave previamente compartida WPA en el ASCII o el formato hexadecimal.Este ejemplo utiliza el formato ASCII. El mismo formato se

debe utilizar en la configuración del lado del cliente. Aquí está la ventana de configuración que explica el paso 5:La clave previamente compartida WPA usada en esta configuración es 1234567890.
6. Haga clic en Apply (Aplicar).
7. Para configurar al servidor DHCP interno para los clientes de red inalámbrica de este VLA N, complete los mismos pasos explicados en el servidor DHCP interno de la configuración para los clientes de red inalámbrica de esta sección del VLA N de este documento con estos parámetros de la configuración:Nombre del agrupamiento DHCP: VLA N 6Red del agrupamiento DHCP: 10.6.0.0Máscara de subred: 255.255.0.0Comenzar el IP: 10.6.1.5Terminación del IP: 10.6.1.10Router predeterminado: 10.6.1.1

Configuración de cliente de red inalámbrica

Después de que usted configure el ISR con el SDM, usted necesita configurar al cliente de red inalámbrica para los diversos tipos de autenticación de modo que el router pueda autenticar a estos clientes de red inalámbrica y proporcionar el acceso a la red WLAN. Este documento utiliza el ADU para la configuración del lado del cliente.

Cliente de red inalámbrica de la configuración para la autenticación abierta con la encripción WEP

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.
2. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utilizará.En este ejemplo, el nombre del perfil y el SSID son **openwep**.**Nota:** El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación abierta.
3. Haga clic la **ficha de seguridad** y deje la opción de seguridad como clave previamente compartida (WEP estático) para la encripción WEP.
4. Haga clic la **configuración** y defina la clave previamente compartida tal y como se muestra en de este ejemplo:
5. Haga clic la **ficha Avanzadas** en la página de la Administración del perfil y fije al modo de autenticación del 802.11 como **abierto** para la autenticación abierta.
6. Para verificar abierto con la autenticación WEP, active el **openwep** SSID configurado.
7. Verifique al cliente de red inalámbrica se asocia con éxito al router. Esto se puede verificar detalladamente del router inalámbrico que usa el **comando show dot11 associations**.Aquí tiene un ejemplo:`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [openwep] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.1.1.5 CB21AG/PI21AG client self Assoc Others: (not related to any ssid)`

Cliente de red inalámbrica de la configuración para abierto con la autenticación de MAC

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.
2. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utilizará.En este ejemplo, el nombre del perfil y el SSID son **openmac**.**Nota:** El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación abierta.
3. Haga clic la **ficha de seguridad** y deje la opción de seguridad como **ningunos** para abierto con la autenticación de MAC. Entonces, **AUTORIZACIÓN del** tecleo.
4. Para verificar abierto con la autenticación de MAC, active el **openmac** SSID configurado.
5. Verifique al cliente de red inalámbrica se asocia con éxito al router. Esto se puede verificar detalladamente del router inalámbrico que usa el **comando show dot11 associations**.Aquí tiene un ejemplo:`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [openmac] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.2.1.5 CB21AG/PI21AG client1 self MAC-Assoc SSID [openwep] : Others: (not related to any ssid)`

Cliente de red inalámbrica de la configuración 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.
2. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utilizará.En este ejemplo, el nombre del perfil y el SSID son **salto**.**Nota:** El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación 802.1x/EAP.
3. 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.
4. Haga clic la **configuración** para configurar las configuraciones del nombre de usuario y contraseña del SALTO.Bajo configuraciones del nombre de usuario y contraseña, este ejemplo elige **indicar manualmente para el Nombre de usuario y la contraseña** de modo que se indique al cliente que ingrese el nombre de usuario y contraseña correcto mientras que intente conectar con la red.
5. Haga clic en OK.
6. Para verificar la autenticación EAP, active el **salto** SSID configurado. A le indican que ingrese un nombre de usuario y contraseña del SALTO. Ingrese ambas las credenciales como **user1** y haga clic la **AUTORIZACIÓN**.
7. Verifique al cliente de red inalámbrica se autentica con éxito y se asigna con una dirección IP. Esto se puede verificar claramente de la ventana de estado ADU.Aquí está la salida equivalente del CLI del router:`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [leap] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.3.1.5 CB21AG/PI21AG client2 self EAP-Assoc SSID [openmac] : SSID [openwep] : Others: (not related to any ssid)`

Cliente de red inalámbrica de la configuración para la autenticación compartida

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.
2. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utilizará.En este ejemplo, **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 abierta.
3. Haga clic la **ficha de seguridad** y deje la opción de seguridad como clave previamente compartida (WEP estático) para la encripción WEP. Entonces, **configuración del** tecleo.
4. Defina la clave previamente compartida tal y como se muestra en de este ejemplo:
5. Haga clic en OK.
6. Bajo Administración del perfil, haga clic la **ficha Avanzadas** y al modo de autenticación del 802.11 del conjunto según lo **compartido** para la autenticación compartida.
7. Para verificar compartió la autenticación, activa el SSID **compartido** configurado.
8. Verifique al cliente de red inalámbrica se asocia con éxito al router. Esto se puede verificar detalladamente del router inalámbrico que usa el **comando show dot11 associations**.Aquí tiene un ejemplo:`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [shared] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.4.1.5 CB21AG/PI21AG WCS self Assoc`

Cliente de red inalámbrica de la configuración para la autenticación WPA

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.
2. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utilizará.En este ejemplo, el nombre del perfil y el SSID son **wpa**.**Nota:** El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación WPA (con el EAP).
3. Bajo Administración del perfil, haga clic la **ficha de seguridad**, fije la opción de seguridad como **WPA/WPA2/CCKM** y elija WPA/WPA2/CCKM el tipo apropiado EAP.Este documento utiliza el **SALTO** como el tipo EAP para la autenticación.
4. Haga clic la **configuración** para configurar las configuraciones del nombre de usuario y contraseña del SALTO.Bajo configuraciones del nombre de usuario y contraseña, este ejemplo elige **indicar manualmente para el Nombre de usuario y la contraseña** de modo que se indique al cliente que ingrese el nombre de usuario y contraseña correcto mientras que intente conectar con la red.
5. Haga clic en OK.
6. Para verificar la autenticación EAP, active el salto SSID configurado. A le indican que ingrese un nombre de usuario y contraseña del SALTO. Ingrese ambas las credenciales como **user2**, después haga clic la **AUTORIZACIÓN**.
7. Verifique al cliente de red inalámbrica se autentica con éxito y se asigna con una dirección IP. Esto se puede verificar claramente de la ventana de estado ADU.

Cliente de red inalámbrica de la configuración 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.
2. Conforme a la **ficha general**, ingrese el nombre del perfil y el SSID que el adaptador del cliente utilizará.En este ejemplo, el nombre del perfil y el SSID son WPA-**PSK**.**Nota:** El SSID debe hacer juego el SSID que usted configuró en el ISR para la autenticación WPA-PSK.
3. Bajo Administración del perfil, haga clic la **ficha de seguridad** y fije la opción de seguridad como **WPA/WPA2 passphrase**. Entonces, **configuración del** tecleo para configurar el passphrase WPA.
4. Defina una clave previamente compartida WPA. La clave debe ser 8 a 63 caracteres ASCII de largo. Entonces, **AUTORIZACIÓN del** tecleo.
5. Para verificar el WPA-PSK, active el WPA-**PSK** SSID configurado.
6. Verifique al cliente de red inalámbrica se asocia con éxito al router. Esto se puede verificar detalladamente del router inalámbrico que usa el **comando show dot11 associations**.

Troubleshooting

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

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
- Configuración de VLAN
- 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
- 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
- Soporte Técnico y Documentación - Cisco Systems