Autenticación en los ejemplos de configuración de los reguladores del Wireless LAN

Contenido

Introducción

Este documento proporciona los ejemplos de configuración que explican cómo configurar diversos tipos de Layer 1, la capa 2, y acodan 3 métodos de autentificación en los reguladores del Wireless LAN (WLCs).

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de la configuración de los Puntos de acceso ligeros (revestimientos) y del WLCs de Cisco
- Conocimiento de los estándares de seguridad 802.11i

Componentes Utilizados

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

hardware.

- WLC de Cisco 4400 que funciona con la versión de firmware 6.0.182.0
- Cisco 1000 Series LAP
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con la versión de firmware 2.6
- Versión del servidor 3.2 del Cisco Secure ACS

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.

Autenticación en el WLCs

La solución acerca de la seguridad de la red del Cisco Unified Wireless (UWN) lía el Layer 1 potencialmente complicado, la capa 2, y acoda 3 componentes de la Seguridad del punto de acceso del 802.11 en un administrador simple de la directiva que personalice las políticas de seguridad sistema-anchas sobre una base de la por-Tecnología inalámbrica LAN (red inalámbrica (WLAN)). La solución acerca de la seguridad de Cisco UWN proporciona las herramientas de Administración de seguridad simples, unificadas, y sistemáticas.

Estos mecanismos de seguridad se pueden implementar en el WLCs.

Soluciones del Layer 1

Restrinja el acceso al cliente basado en el número de intentos fallidos consecutivos.

Acode 2 soluciones

Ninguno autenticación — Cuando esta opción se selecciona de la lista desplegable de la Seguridad de la capa 2, no se realiza ninguna autenticación de la capa 2 en la red inalámbrica (WLAN). Éste es lo mismo que la autenticación abierta del estándar del 802.11.

WEP estático — Con el Wired Equivalent Privacy (WEP) estático, todos los AP y radio cliente NIC en una red inalámbrica (WLAN) determinada deben utilizar la misma clave de encripción. Cada estación remitente cifra el cuerpo de cada bastidor con una clave WEP antes de la transmisión, y la estación receptora la desencripta usando una clave idéntica sobre la recepción.

802.1x — Configura la red inalámbrica (WLAN) para utilizar la autenticación basada 802.1x. El uso del IEEE 802.1X ofrece un marco eficaz para autenticar y controlar el tráfico de usuarios a una red protegida, así como varía dinámicamente las claves de encripción. el 802.1x ata un protocolo llamado Protocolo de Autenticación Extensible (EAP) a los media atada con alambre y de la red inalámbrica (WLAN) y soporta los métodos de autenticación múltiple.

WEP estático + 802.1x — Este ajuste de seguridad de la capa 2 habilita el 802.1x y el WEP

estático. Los clientes pueden utilizar la autenticación del WEP estático o del 802.1x para conectar con la red.

Acceso protegido de Wi-Fi (WPA) — El WPA o WPA1 y el WPA2 son las soluciones acerca de la seguridad estándar basadas del Wi-Fi Alliance que proporcionan la protección de datos y el control de acceso para los sistemas WLAN. WPA1 es compatible con el estándar de IEEE 802.11i pero fue implementado antes de la ratificación del estándar. El WPA2 es la implementación de Alliance del Wi-Fi del estándar ratificado de IEEE 802.11i.

Por abandono, WPA1 utiliza el Temporal Key Integrity Protocol (TKIP) y el Message Integrity Check (MIC) para la protección de datos. El WPA2 utiliza el algoritmo de encripción más fuerte del Advanced Encryption Standard usando el modo contrario con el protocolo del Message Authentication Code del Cipher Block Chaining (AES-CCMP). WPA1 y el WPA2 utilizan el 802.1x para la administración de claves autenticada por abandono. Sin embargo, estas opciones están también disponibles: PSK, CCKM, y CCKM+802.1x. Si usted selecciona el CCKM, Cisco permite solamente a los clientes que soportan el CCKM. Si usted selecciona CCKM+802.1x, Cisco permite a los clientes del NON-CCKM también.

CKIP — El Protocolo de integridad de clave Cisco (CKIP) es un Security Protocol del patentado Cisco para los media del 802.11 que cifran. CKIP mejora la Seguridad del 802.11 en el modo de infraestructura que usa la permutación dominante, el MIC, y el número de la secuencia de mensaje. Soportes del Software Release 4.0 CKIP con la clave estática. Para que esta característica actúe correctamente, usted debe habilitar los elementos de información del Aironet (IE) para la red inalámbrica (WLAN). CKIP las configuraciones especificadas en una red inalámbrica (WLAN) son obligatorias para cualquier cliente que intente asociarse. Si la red inalámbrica (WLAN) se configura para ambos CKIP cierre la permutación y MMH MIC, el cliente debe soportar ambos. Si la red inalámbrica (WLAN) se configura para solamente una de estas características, el cliente debe soportar solamente esto CKIP característica. Parásitos atmosféricos del soporte del WLCs solamente CKIP (como el WEP estático). El WLCs no soporta CKIP con el 802.1x (dinámico CKIP).

Soluciones de la capa 3

Ninguno — Cuando esta opción se selecciona de la lista desplegable de la Seguridad de la capa 3, no se realiza ninguna autenticación de la capa 3 en la red inalámbrica (WLAN).

Nota: El ejemplo de configuración para ninguna autenticación de la capa 3 y ninguna autenticación de la capa 2 se explica en el ningunos sección de la autenticación.

La directiva de la red (passthrough de la autenticación Web y de la red) — autenticación Web es utilizada típicamente por los clientes que quieren desplegar una red del acceso de invitado. En una red del acceso de invitado, hay autenticación inicial del nombre de usuario y contraseña, pero la Seguridad no se requiere para el tráfico subsiguiente. Las instalaciones típicas pueden incluir “hot spot” las ubicaciones, tales como T-Mobile o Starbucks.

La autenticación Web para el WLC de Cisco se hace localmente. Usted crea una interfaz y después asocia un identificador del conjunto WLAN/service (SSID) a esa interfaz.

La autenticación Web proporciona la autenticación simple sin un supplicant o un cliente. Considere que la autenticación Web no proporciona la cifrado de datos. La autenticación Web se utiliza típicamente como acceso simple de invitados para “hot spot” o ambiente de campus donde la conectividad es la única preocupación.

El passthrough de la red es una solución a través de la cual reorientan a los usuarios de red inalámbrica a una página aceptable de la política de uso sin tener que autenticar cuando conectan con Internet. Este cambio de dirección es tomado el cuidado de por el WLC sí mismo. El único requisito es configurar el WLC para el passthrough de la red, que es básicamente autenticación Web sin tener que ingresar cualquier credencial.

Passthrough VPN — El passthrough VPN es una característica que permite que un cliente establezca un túnel solamente con un servidor VPN específico. Por lo tanto, si usted necesita acceder con seguridad al servidor VPN configurado así como otro servidor VPN o Internet, esto no es posible con el passthrough VPN habilitado en el regulador.

En las siguientes secciones, los ejemplos de configuración se proporcionan para cada uno de los mecanismos de autenticación.

Ejemplos de Configuración

Antes de que usted configure los WLAN y los tipos de autenticación, usted debe configurar el WLC para la operación básica y registrar los revestimientos al WLC. Este documento asume que el WLC está configurado para la operación básica y que los revestimientos están registrados al WLC. Si usted es usuario nuevo que intenta poner el WLC para la operación básica con los revestimientos, refiera al registro ligero AP (REVESTIMIENTO) a un regulador del Wireless LAN (WLC).

Soluciones acerca de la seguridad del Layer 1

Los clientes de red inalámbrica pueden ser acceso restringido basado en el número de intentos fallidos consecutivos de acceder la red WLAN. La exclusión del cliente ocurre en estas condiciones por abandono. Estos valores no pueden ser cambiados.

- Falla de autenticación consecutiva del 802.11 (5 veces consecutivas, el 6to intento se excluye)
- Errores consecutivos de la asociación del 802.11 (5 veces consecutivas, el 6to intento se excluye)
- Fallas de autenticación consecutivas del 802.1x (3 veces consecutivas, el 4to intento se excluye)
- Error externo del servidor de políticas
- Tentativa de utilizar la dirección IP asignada ya a otro dispositivo (hurto IP o reutilización IP)
- Autenticación Web consecutiva (3 veces consecutivas, el 4to intento se excluye)

Para localizar las directivas de la exclusión del cliente, la **Seguridad del** tecleo en el menú superior, y después elegir las **directivas inalámbricas de la protección > las directivas de la exclusión del cliente la** navegación en el lado izquierdo de la página.

El temporizador de la exclusión puede ser configurado. Las opciones de la exclusión se pueden habilitar o inhabilitar por el regulador. El temporizador de la exclusión se puede habilitar o inhabilitar por la red inalámbrica (WLAN).

El número máximo de logines simultáneos para un nombre de único usuario por abandono es 0. Usted puede ingresar cualquier valor entre 0 y 8. Este parámetro se puede fijar en la **SEGURIDAD >AAA > las directivas del ingreso del usuario al sistema** y permite que usted especifique el número máximo de logines simultáneos para un solo Nombre del cliente, entre uno

y ocho, o 0 = ilimitado. Aquí tiene un ejemplo:

Soluciones acerca de la seguridad de la capa 2

Ningunos autenticación

Este ejemplo muestra una red inalámbrica (WLAN) configurada sin la autenticación.

Nota: Este ejemplo también trabaja para ninguna autenticación de la capa 3.

WLC de la configuración para ninguna autenticación

Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN).La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.
2. El tecleo **va** para configurar una nueva red inalámbrica (WLAN).
3. Ingrese los parámetros para el WLAN. Este ejemplo muestra la configuración para esta red inalámbrica (WLAN).
4. Haga clic en Apply (Aplicar).
5. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).
6. Haga clic la **ficha de seguridad**, y no elija **ninguno** para la Seguridad de la capa 2 y de la capa 3.**Nota:** Para que una red inalámbrica (WLAN) llegue a ser activa, el estatus debe ser habilitado. Para habilitarlo, marque el cuadro de **revisión de estado** conforme a la ficha general.Esto no habilita ninguna autenticación para esta red inalámbrica (WLAN).
7. Elija otros parámetros basados en sus requisitos de diseño. Este ejemplo utiliza los valores predeterminados.
8. Haga clic en Apply (Aplicar).

Cliente de red inalámbrica de la configuración para ninguna autenticación

Complete estos pasos para configurar al cliente del Wireless LAN para esta configuración:

Nota: Este documento utiliza un adaptador del cliente del Aironet 802.11a/b/g que funcione con el firmware 3.5 y explique la configuración del adaptador del cliente con la versión de ADU 3.5.

1. Para crear un nuevo perfil, haga clic la lengueta de la **Administración del perfil** en el ADU.
2. Haga clic en **New**.
3. Cuando las visualizaciones (generales) de la ventana de la Administración del perfil, completan estos pasos para fijar el nombre del perfil, el Nombre del cliente, y el SSID:Ingrese el nombre del perfil en el campo de nombre del perfil.Este ejemplo utiliza *NoAuthentication* como el nombre del perfil.Ingrese el nombre del cliente en el campo de Nombre del cliente.El Nombre del cliente se utiliza para identificar al cliente de red inalámbrica en la red WLAN. Esta configuración utiliza el *client1* para el Nombre del cliente.Bajo nombres de red, ingrese el SSID que debe ser utilizado para este perfil.El SSID es lo mismo que el SSID que usted configuró en el WLC. El SSID en este ejemplo es *NullAuthentication.*

4. Haga clic en la ficha Security (Seguridad).
5. No haga clic el **ninguno** botón de radio bajo opciones de seguridad del conjunto, y después haga clic la **AUTORIZACIÓN**.Cuando se activa el SSID, el cliente de red inalámbrica conecta con la red inalámbrica (WLAN) sin ninguna autenticación.

WEP estático

Este ejemplo muestra una red inalámbrica (WLAN) configurada con el WEP estático.

WLC de la configuración para el WEP estático

Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN).La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.
2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).
3. Ingrese el ID DE WLAN y el WLAN SSID.En este ejemplo, la red inalámbrica (WLAN) se nombra *StaticWEP* y el ID DE WLAN es *2.*
4. Haga clic en Apply (Aplicar).
5. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).De la lista desplegable de la capa 2, elija el **WEP estático**.Esto habilita el WEP estático para esta red inalámbrica (WLAN).Bajo parámetros del WEP estático, elija el índice del tamaño de la clave WEP y dominante, y ingrese la clave de encripción del WEP estático.El tamaño de clave puede ser 40 bits o 104 bits. El índice dominante puede estar entre 1 y 4. Un índice de clave WEP único se puede aplicar a cada red inalámbrica (WLAN). Porque hay solamente cuatro índices de clave WEP, sólo cuatro WLAN se pueden configurar para el cifrado de la capa 2 del WEP estático. En este ejemplo, 104 se utiliza el bit WEP y la clave WEP usada es 1234567890abcdef.Marque si configuran al servidor de RADIUS para la autenticación. El servidor de RADIUS puede ser configurado en la **ficha de seguridad** localizada en **AAA > radio > autenticación**. Una vez que está configurado, el servidor de RADIUS debe ser asignado a la red inalámbrica (WLAN) para la autenticación. Vaya a los **servidores del > Security (Seguridad) WLAN >AAA** para asignar al servidor de RADIUS a la red inalámbrica (WLAN) para la autenticación.En este ejemplo, 10.77.244.196 es el servidor de RADIUS.
6. Elija otros parámetros basados en sus requisitos de diseño.Este ejemplo utiliza los valores predeterminados.
7. Haga clic en Apply (Aplicar).**Nota:** El WEP se representa siempre en el hexadecimal (maleficio). Cuando usted ingresa la clave WEP en el ASCII, la cadena ASCII WEP se convierte al maleficio, que se utiliza para cifrar el paquete. No hay método estándar que los vendedores se realizan para convertir el maleficio al ASCII, pues algunos harán completar mientras que otros no. Por lo tanto, para la compatibilidad máxima del inter-vendedor, maleficio del uso para sus claves WEP.**Nota:** Si usted quiere habilitar la clave de autenticación compartida para la red inalámbrica (WLAN), marque la casilla de verificación de la **clave de autenticación compartida de la permit** bajo parámetros del WEP estático. Esta manera, si configuran al cliente también para la clave de autenticación compartida, clave de autenticación compartida seguida por la encripción WEP de los paquetes ocurrirá en la red inalámbrica (WLAN).

Cliente de red inalámbrica de la configuración para el WEP estático

Complete estos pasos para configurar al cliente del Wireless LAN para esta configuración:

1. Para crear un nuevo perfil, haga clic la lengueta de la **Administración del perfil** en el ADU.
2. Haga clic en **New**.
3. Cuando las visualizaciones (generales) de la ventana de la Administración del perfil, completan estos pasos para fijar el nombre del perfil, el Nombre del cliente, y el SSID:Ingrese el nombre del perfil en el campo de nombre del perfil.Este ejemplo utiliza *StaticWEP* como el nombre del perfil.Ingrese el nombre del cliente en el campo de Nombre del cliente.El Nombre del cliente se utiliza para identificar al cliente de red inalámbrica en la red WLAN. Esta configuración utiliza al *cliente 2* para el Nombre del cliente.Bajo nombres de red, ingrese el SSID que debe ser utilizado para este perfil.El SSID es lo mismo que el SSID que usted configuró en el WLC. El SSID en este ejemplo es *StaticWEP*.
4. Haga clic en la ficha Security (Seguridad).
5. Elija la **clave previamente compartida (WEP estático)** bajo opciones de seguridad del conjunto.
6. Haga clic la **configuración**, y defina el tamaño de la clave WEP y la clave WEP.Esto debe hacer juego con la clave WEP configurada en el WLC para esta red inalámbrica (WLAN).
7. Haga clic en Apply (Aplicar).Cuando se activa el SSID, el cliente de red inalámbrica conecta con la red inalámbrica (WLAN) y los paquetes se cifran usando la clave de WEP estático.

autenticación del 802.1x

Este ejemplo muestra una red inalámbrica (WLAN) configurada con la autenticación del 802.1x.

WLC de la configuración para la autenticación del 802.1x

Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN).La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.
2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).En este ejemplo, la red inalámbrica (WLAN) se nombra *802.1x*, y el ID DE WLAN es *3*. Un nombre del perfil debe también ser agregado.
3. Haga clic en Apply (Aplicar).
4. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).De la lista desplegable de la capa 2, elija el **802.1x**.**Nota:** Solamente la encripción WEP está disponible con el 802.1x. Elija 40 bits o 104 bits para el cifrado, y aseegurese la Seguridad de la capa 3 se fija a ningunos.Esto habilita la autenticación del 802.1x para esta red inalámbrica (WLAN).Bajo parámetros del servidor de RADIUS, seleccione al servidor de RADIUS que será utilizado para autenticar las credenciales del cliente.Elija otros parámetros basados en sus requisitos de diseño.Este ejemplo utiliza los valores predeterminados.
5. Haga clic en Apply (Aplicar).**Notas:**Si usted elige el *802.1x* para la Seguridad de la capa 2, el CCKM no puede ser utilizado.Si usted elige *WPA 1* o el *WPA2* para la Seguridad de la capa 2, estas opciones aparecen bajo administración de claves del auth:*802.1x+CCKM* — Si usted elige esta opción, soportan a los clientes del CCKM o del NON-CCKM (CCKM

opcional).*802.1x* — Si usted elige esta opción, sólo soportan a los clientes del 802.1x.*CCKM* — Si usted elige esta opción, sólo soportan a los clientes del CCKM, donde dirigen a los clientes a un servidor externo para la autenticación.*PSK* — Si usted elige esta opción, una clave previamente compartida se utiliza para el WLC y el cliente. También, todos los estándares se fijan para ser utilizados antes de los PRE-estándares; por ejemplo, WPA/WPA2 toma el precedente sobre el CCKM cuando está utilizado simultáneamente.El tipo de autenticación EAP usado para validar a los clientes es dependiente en el tipo EAP configurado en el servidor de RADIUS y los clientes de red inalámbrica. Una vez que el 802.1x se habilita en el WLC, el WLC permite que todos los tipos de paquetes EAP fluyan entre el REVESTIMIENTO, el cliente de red inalámbrica y el servidor de RADIUS.Estos documentos proporcionan los ejemplos de configuración en algunos de los tipos de la autenticación EAP:PEAP bajo redes inalámbricas unificadas con ACS 4.0 y Windows 2003EAP-TLS bajo red inalámbrica unificada con ACS 4.0 y Windows 2003Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)

Cliente de red inalámbrica de la configuración para la autenticación del 802.1x

Complete estos pasos para configurar al cliente del Wireless LAN para esta configuración:

1. Para crear un nuevo perfil, haga clic la lengueta de la **Administración del perfil** en el ADU.
2. Haga clic en **New**.
3. Cuando las visualizaciones (generales) de la ventana de la Administración del perfil, completan estos pasos para fijar el nombre del perfil, el Nombre del cliente, y el SSID:Ingrese el nombre del perfil en el campo de nombre del perfil.Este ejemplo utiliza *EAPAuth* como el nombre del perfil.Ingrese el nombre del cliente en el campo de Nombre del cliente.El Nombre del cliente se utiliza para identificar al cliente de red inalámbrica en la red WLAN. Esta configuración utiliza al *cliente 3* para el Nombre del cliente.Bajo nombres de red, ingrese el SSID que debe ser utilizado para este perfil.El SSID es lo mismo que el SSID que usted configuró en el WLC. El SSID en este ejemplo es *802.1x*.
4. Haga clic en la ficha Security (Seguridad).
5. Haga clic el botón de radio del **802.1x**.
6. De la lista desplegable del tipo del 802.1x EAP, elija el tipo EAP usado.
7. Haga clic la **configuración** para configurar los parámetros específicos al tipo seleccionado EAP.
8. Haga clic en Apply (Aplicar).Cuando se activa el SSID, el cliente de red inalámbrica conecta con la red inalámbrica (WLAN) usando la autenticación del 802.1x. Las claves WEP dinámicas se utilizan para las sesiones.

Autenticación del WEP estático + del 802.1x

Este ejemplo muestra una red inalámbrica (WLAN) configurada con la autenticación del WEP estático + del 802.1x.

Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN).La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.
2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).

3. Ingrese el ID DE WLAN y el WLAN SSID.En este ejemplo, la red inalámbrica (WLAN) se nombra *WEP+802.1x*, y el ID DE WLAN es *4.*
4. Haga clic en Apply (Aplicar).
5. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).De la lista desplegable de la capa 2, elija **Static-WEP+802.1x**.Esto habilita el WEP estático y la autenticación del 802.1x para esta red inalámbrica (WLAN).Bajo parámetros del servidor de RADIUS, seleccione al servidor de RADIUS que será utilizado para autenticar las credenciales del cliente usando el 802.1x, y configure al servidor de RADIUS tal y como se muestra en del ejemplo anterior.Bajo parámetros del WEP estático, seleccione el índice del tamaño de la clave WEP y dominante, y ingrese la clave de encripción del WEP estático tal y como se muestra en de la imagen anterior.Elija otros parámetros basados en sus requisitos de diseño.Este ejemplo utiliza los valores predeterminados.

Configure al cliente de red inalámbrica para el WEP estático y el 802.1x

Vea al cliente de red inalámbrica de la configuración para el cliente de red inalámbrica de la autenticación y de la configuración del 802.1x para las secciones del WEP estático para la información sobre cómo configurar al cliente de red inalámbrica.

Una vez que se crean los perfiles del cliente, los clientes que se configuran para el socio del WEP estático con el REVESTIMIENTO. Utilice el SSID WEP+802.1x para conectar con la red.

Semejantemente, autentican a los clientes de red inalámbrica que se configuran para utilizar la autenticación del 802.1x usando el EAP y acceder la red con el mismo SSID WEP+802.1x.

Acceso protegido Wi-Fi

Este ejemplo muestra a red inalámbrica (WLAN) cuál se configura con el WPA con el 802.1x.

Configure el WLC para el WPA

Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN).La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.
2. El tecleo **va** para configurar una nueva red inalámbrica (WLAN).Elija el tipo y el nombre del perfil. En este ejemplo, la red inalámbrica (WLAN) se nombra *WPA*, y el ID DE WLAN es *5.*
3. Haga clic en Apply (Aplicar).
4. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).Haga clic la **ficha de seguridad**, haga clic la lengueta de la **capa 2**, y elija **WPA1+WPA2 de la** lista desplegable de la Seguridad de la capa 2.Bajo parámetros WPA1+WPA2, marque la casilla de verificación de la **directiva WPA1** para habilitar WPA1, marcar la casilla de verificación de la **directiva WPA2** para habilitar el WPA2, o marcar ambas casillas de verificación para habilitar WPA1 y el WPA2.El valor predeterminado se inhabilita para WPA1 y el WPA2. Si usted deja WPA1 y el WPA2 inhabilitados, los Puntos de acceso hacen publicidad en sus faros y elementos de información de respuesta de la sonda solamente para el método de Administración de clave de autenticación que usted

elige.Marque la casilla de verificación **AES** para permitir a la encripción de datos AES o a la casilla de verificación **TKIP** para habilitar la encripción de datos TKIP para WPA1, el WPA2, o ambos.Los valores predeterminados son TKIP para WPA1 y AES para el WPA2.Elija uno de estos métodos de administración de claves de la lista desplegable del mgmt de la clave del auth:*802.1x* — Si usted elige esta opción, sólo soportan a los clientes del 802.1x.*CCKM* — Si usted elige esta opción, sólo soportan a los clientes del CCKM, donde dirigen a los clientes a un servidor externo para la autenticación.*PSK* — Si usted elige esta opción, una clave previamente compartida se utiliza para el WLC y el cliente. También, todos los estándares se fijan para ser utilizados antes de los PRE-estándares; por ejemplo, WPA/WPA2 toma el precedente sobre el CCKM cuando está utilizado simultáneamente.*802.1X+CCKM* — Si usted elige esta opción, soportan a los clientes del CCKM o del NON-CCKM (CCKM opcional).Este ejemplo utiliza el 802.1x.**Nota:** Si usted elige el PSK, elija el **ASCII** o el **maleficio de la** lista desplegable del formato del PSK, y después ingrese una clave previamente compartida en el campo vacío. Las claves previamente compartidas WPA deben contener 8 a 63 caracteres del texto ASCII o 64 caracteres hexadecimales.
5. El tecleo **se aplica** para aplicar sus cambios.

Configure al cliente de red inalámbrica para el WPA

Complete estos pasos para configurar al cliente del Wireless LAN para esta configuración:

1. En la ventana de administración del perfil en el ADU, haga clic **nuevo** para crear un nuevo perfil.
2. Haga clic la **ficha general**, y 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*. El SSID debe hacer juego el SSID que usted configuró en el WLC para el WPA.
3. En la ficha de seguridad, haga clic **WPA/WPA2/CCKM el** botón de radio, y elija el tipo apropiado EAP WPA/WPA2/CCKM de la lista desplegable del tipo EAP. Este paso habilita el WPA.
4. Haga clic la **configuración** para definir las configuraciones EAP específicas al tipo de EAP seleccionado.
5. Haga clic en OK.**Nota:** Cuando se activa este perfil, autentican al cliente usando el 802.1x y cuando la autenticación es acertada, el cliente conecta con la red inalámbrica (WLAN). Marque el estado actual ADU para verificar que el cliente utiliza el cifrado TKIP (cifrado predeterminado usado por WPA1) y la autenticación EAP.

CKIP

Este ejemplo muestra una red inalámbrica (WLAN) configurada con CKIP.

Configure el WLC para CKIP

Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN).La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.

2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).Elija el tipo y el nombre del perfil. En este ejemplo, la red inalámbrica (WLAN) se nombra *CKIP* y el ID DE WLAN es *6.*
3. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).De la lista desplegable de la capa 2, elija **CKIP**.Este paso habilita CKIP para esta red inalámbrica (WLAN).Bajo CKIP parámetros, seleccione el índice del tamaño de clave y dominante, y ingrese la clave de encripción estática.El tamaño de clave puede ser 40 bits, 104 bits, o los bits 128. El índice dominante puede estar entre 1 y 4. Un índice de clave WEP único se puede aplicar a cada red inalámbrica (WLAN). Porque hay solamente cuatro índices de clave WEP, sólo cuatro WLAN se pueden configurar para el cifrado de la capa 2 del WEP estático.Para CKIP, elija la **opción de modo MMH**, o la opción **dominante de la permutación**, o ambas.**Nota:** Uno de estos parámetros o ambos se debe seleccionar para que CKIP trabaje como se esperaba. Si estos parámetros no se seleccionan, la red inalámbrica (WLAN) permanece en el estado inhabilitado.En este ejemplo, el bit 104 dominante se utiliza, y la clave es 1234567890abc.
4. Elija otros parámetros basados en sus requisitos de diseño.Este ejemplo utiliza los valores predeterminados.
5. Haga clic en Apply (Aplicar).**Nota:** CKIP es funcional en los 1100, 1130, y 1200 AP, pero no AP 1000. El Aironet IE necesita ser habilitado para que esta característica trabaje. CKIP amplía las claves de encripción a 16 bytes.

Configure al cliente de red inalámbrica para CKIP

Complete estos pasos para configurar al cliente del Wireless LAN para esta configuración:

1. Para crear un nuevo perfil, haga clic la lengueta de la **Administración del perfil** en el ADU, y después haga clic **nuevo**.
2. Cuando las visualizaciones (generales) de la ventana de la Administración del perfil, completan estos pasos para fijar el nombre del perfil, el Nombre del cliente, y el SSID:Ingrese el nombre del perfil en el campo de nombre del perfil.Este ejemplo utiliza *CKIP* como el nombre del perfil.Ingrese el nombre del cliente en el campo de Nombre del cliente.El Nombre del cliente se utiliza para identificar al cliente de red inalámbrica en la red WLAN. Esta configuración utiliza *Client6* para el Nombre del cliente.En Nombres de Red, ingrese el SSID que debe ser utilizado para este perfil.El SSID es lo mismo que el SSID que usted configuró en el WLC. El SSID en este ejemplo está *CKIP*.
3. Haga clic en la ficha Security (Seguridad).
4. Elija la **clave previamente compartida (WEP estático)** bajo opciones de seguridad del conjunto, haga clic la **configuración**, y defina el tamaño de la clave WEP y la clave WEP.Estos valores deben hacer juego con la clave WEP configurada en el WLC para esta red inalámbrica (WLAN).
5. Haga clic en OK.Cuando se activa el SSID, el cliente de red inalámbrica negocia con el REVESTIMIENTO y el WLC para utilizar CKIP para el cifrado los paquetes.

Soluciones acerca de la seguridad de la capa 3

Directiva de la red (passthrough de la autenticación Web y de la red)

Refiera al ejemplo de configuración de la autenticación Web del regulador del Wireless LAN para

la información sobre cómo habilitar la autenticación Web en una red WLAN.

Refiera a la autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN para la información sobre cómo configurar la autenticación del Web externa y la autenticación del passthrough de la red en una red inalámbrica (WLAN).

Refiera al ejemplo de configuración del passthrough de la red del regulador del Wireless LAN para más información sobre cómo habilitar el passthrough de la red en una red WLAN.

El mecanismo de la página del chapoteo es un mecanismo de seguridad de la capa 3 introducido en la versión 5.0 del WLC usada para la autenticación de cliente. Refiera al regulador del Wireless LAN que la página del chapoteo reorienta el ejemplo de configuración para más información.

Passthrough VPN

Refiera al cliente VPN sobre el Wireless LAN con el ejemplo de configuración del WLC para la información sobre cómo configurar el passthrough VPN en una red inalámbrica (WLAN).

Troubleshooting

Comandos para resolución de problemas

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

Debugs para la autenticación Web:

- *<client-MAC-direccionamiento xx de las* **direcciones MAC del debug***: xx: xx: xx: xx: xx>* — Debugging de la dirección MAC de las configuraciones para el cliente.
- **el debug aaa todo habilita** — Configura el debugging de todos los mensajes AAA.
- **permiso del estado PEM del debug** — Debug de las configuraciones de la máquina de estado del administrador de la directiva
- **permiso de los eventos PEM del debug** — Debug de las configuraciones de los eventos del administrador de la directiva.
- **permiso del mensaje DHCP del debug** — Utilice este comando para visualizar la información de debugging sobre las actividades del cliente del Protocolo de configuración dinámica de host (DHCP) y monitorear el estatus de los paquetes DHCP.
- **haga el debug del permiso del paquete DHCP** — Utilice este comando para visualizar la información llana del paquete DHCP.
- **haga el debug del permiso P.M. SSH-appgw** — Debug de las configuraciones de los gatewayes de aplicación.
- **permiso del debug P.M. SSH-TCP** — Debug de las configuraciones de la dirección tcp del administrador de la directiva

Debugs para el WEP: Ningún debug para el WEP porque se realiza en el AP, gira el **dot11 del debug todo el permiso**.

Debugs para ocultar 802.1X/WPA/RSN/PMK:

- **<client-MAC-direccionamiento** *xx de las* **direcciones MAC del debug***: xx: xx: xx: xx: xx* **>** — Debugging de la dirección MAC de las configuraciones para el cliente.

- **el dot1x todo del debug habilita** — Utilice este comando para visualizar la información de debugging del 802.1x.
- **haga el debug del dot11 todo el permiso** — Utilice este comando para habilitar el debugging de las funciones de radio.
- **haga el debug del permiso de los eventos PEM** — Debug de las configuraciones de los eventos del administrador de la directiva.
- **permiso del estado PEM del debug** — Debug de las configuraciones de la máquina de estado del administrador de la directiva.
- **permiso del mensaje DHCP del debug** — Utilice este comando para visualizar la información de debugging sobre las actividades del cliente del Protocolo de configuración dinámica de host (DHCP) y monitorear el estatus de los paquetes DHCP.
- **haga el debug del permiso del paquete DHCP** — Utilice este comando para visualizar la información llana del paquete DHCP.
- **haga el debug del** debug de las configuraciones del **permiso de las manos de la movilidad (para el intra-Switch que vaga por)** — de los paquetes de la movilidad.
- **muestre el <mac del detalle del cliente >** — Visualiza la información detallada para un cliente por el MAC address. Marque configuración del tiempo de espera de la sesión de la red inalámbrica (WLAN) y RADIUS.

Información Relacionada

- Restrinja el acceso de la red inalámbrica (WLAN) basado en el SSID con el WLC y el ejemplo de configuración del Cisco Secure ACS
- ACL en el ejemplo de la configuración de controlador del Wireless LAN
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems