Detección rogue bajo redes inalámbricas unificadas

Contenido

[Introducción](#)
[Descripción general de características](#)
[Detección rogue de la infraestructura](#)
[Detalles rogue](#)
[Determine a los granujas activos](#)
[Contención rogue del Active](#)
[Detección rogue – Pasos para la configuración](#)
[Comandos para resolución de problemas](#)
[Conclusión](#)
[Información Relacionada](#)

Introducción

Las redes inalámbricas amplían las redes alámbricas y aumentan la productividad de los trabajadores y el acceso a la información. Sin embargo, una red inalámbrica no autorizada representa un problema de seguridad añadido. Se pone menos cuidado en la seguridad de los puertos de las redes alámbricas, y las redes inalámbricas son una extensión fácil de las redes alámbricas. Por lo tanto, un empleado que traiga su propio punto de acceso de Cisco (AP) a una red inalámbrica o una infraestructura cableada bien protegida y permita el acceso de usuarios no autorizados a esta en principio red protegida puede comprometer fácilmente una red segura.

La detección rogue permite que el administrador de la red monitoree y elimine estos problemas de seguridad. Cisco unificó la arquitectura de red proporciona dos métodos de detección rogue que habilitan una solución rogue completa de la identificación y de la contención sin la necesidad de costoso y duro-a-alinean las redes y las herramientas de recubrimiento.

Descripción general de características

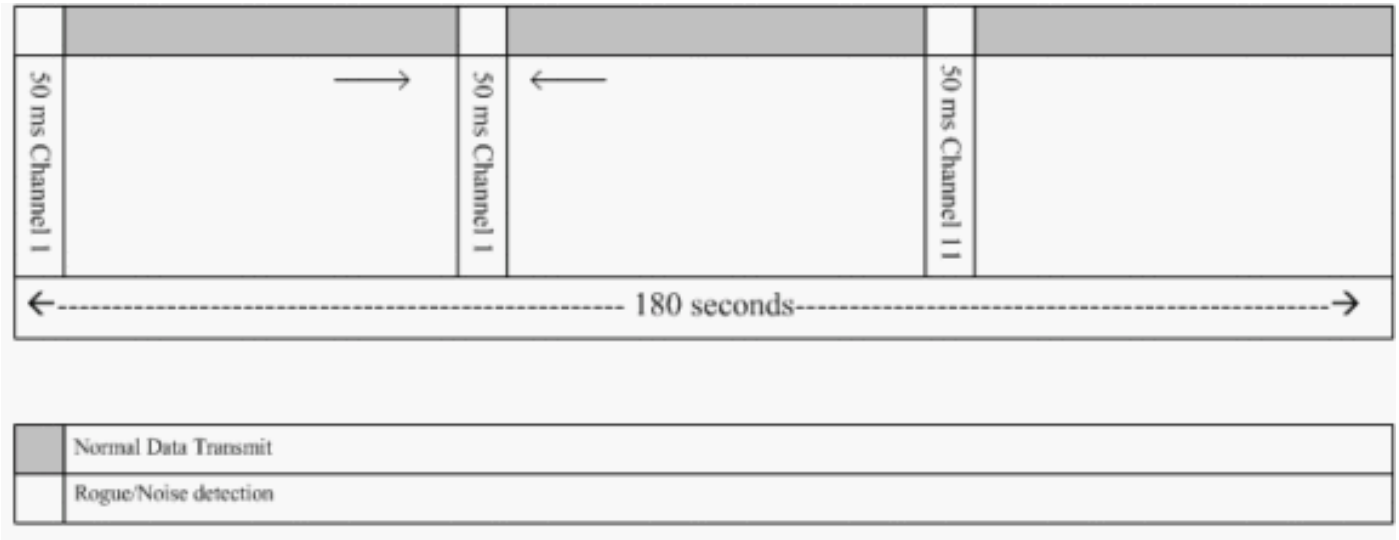
La detección rogue no es limitada por ninguna regulaciones y no se requiere ninguna adherencia legal para su operación. Sin embargo, la contención rogue introduce generalmente las cuestiones legales que pueden poner el proveedor de la infraestructura en una posición incómoda si están idas para actuar automáticamente. Cisco es extremadamente sensible a tales problemas y proporciona estas soluciones. Cada regulador se configura con un nombre del grupo RF. Una vez que un AP ligero se registra con un regulador, integra un **elemento de información de autenticación (IE)** que sea específico al grupo RF configurado en el regulador en todos sus faros/tramas de respuesta de la sonda. Cuando el AP ligero oye los faros sondar las tramas de respuesta de un AP sin este **IE** o con el **IE incorrecto**, después el AP ligero señala que el AP como granuja, registra su BSSID en una tabla rogue, y envía la tabla al regulador. Hay dos

métodos, a saber el Discovery Protocol rogue de la ubicación (RLDP) y la operación pasiva, que se explican detalladamente; vea la sección activa de los granujas del determinar.

Detección rogue de la infraestructura

La detección rogue en un entorno de red inalámbrica activo puede ser costosa. Este proceso pide el AP en el servicio (o el modo local) para cesar el servicio, para estar atento el ruido, y para realizar la detección rogue. El administrador de la red configura los canales para analizar, y configura el período de tiempo en el cual se analizan todas las estaciones. El AP está atento al ms 50 para los faros rogue del cliente, después vuelve al canal configurado para mantener a los clientes otra vez. Esta exploración activa, combinada con los mensajes vecinos, identifica qué AP son granujas y qué AP son válidos y parte de la red. Para configurar los canales analizados y el período de tiempo de la exploración, hojear a la **Tecnología inalámbrica > a la red 802.11b/g** (“**b/g**” o “**a**” dependiendo del requisito de la red) y seleccionar el botón **auto RF** en la esquina derecha superior de la ventana del buscador.

Usted puede navegar hacia abajo **divulgar/los canales de supervisión de interferencia/del granuja** para configurar los canales que se explorarán para los granujas y el ruido. Las opciones disponibles son: Todo el) de los canales (1 a 14, canales del país (1 a 11) o canales dinámicos de la asociación del canal (DCA) (por abandono 1, 6 y 11). El período de tiempo de la exploración a través de estos canales se puede configurar en la misma ventana, bajo **intervalos del monitor (60 a 3600 secs)** junto con el intervalo de la medida de ruido. Por abandono, el intervalo que escucha para el ruido del apagado-canal y los granujas es 180 segundos. Esto significa que cada canal está analizado cada 180 segundos. Éste es un ejemplo de los canales DCA que se analizan cada 180 segundos:



Según lo ilustrado, un número alto de canales configurados para ser analizado combinó con los intervalos cortos de la exploración, deja menos hora para el AP realmente a los clientes de los datos de servicio.

Las esperas ligeras AP para etiquetar los clientes y los AP como granujas porque otro AP no señalan estos granujas posiblemente hasta que se complete otro ciclo. El mismo AP se mueve al mismo canal otra vez para monitorear para el granuja AP y los clientes, así como ruido e interferencia. Si detectan a los mismos clientes y/o AP, los enumeran como granujas en el regulador otra vez. El regulador ahora comienza a determinar si asocian a estos granujas a la red local o simplemente a un AP vecino. En ambos casos, un AP que no es parte de la red inalámbrica local manejada se considera un granuja.

Detalles rogue

Un AP ligero va apagado-canal para el ms 50 para estar atenta los clientes rogue, el monitor para el ruido, e interferencia del canal. Envían cualesquiera clientes o AP rogue detectados al regulador, que recopila esta información:

- La dirección MAC del granuja AP
- El nombre del granuja AP
- La dirección MAC rogue del cliente conectado
- Si las tramas están protegidas con el WPA o el WEP
- El preámbulo
- El relación señal-ruido (SNR)
- El indicador de la potencia de la señal del receptor (RSSI)

Punto de acceso rogue del detector

Usted puede hacer un AP actúa como detector rogue, que permite que sea colocado en un puerto troncal de modo que pueda oír todos los VLA N conectados atar con alambre-lado. Procede a encontrar al cliente en la subred atada con alambre en todos los VLA N. El detector rogue AP está atentos los paquetes del Address Resolution Protocol (ARP) para determinar los direccionamientos de la capa 2 de los clientes o del granuja rogue identificados AP enviados por el regulador. Si se encuentra un direccionamiento de la capa 2 que hace juego, el regulador genera una alarma que identifique el granuja AP o al cliente como amenaza. Esta alarma indica que vieron al granuja en la red alámbrica.

Determine a los granujas activos

Los AP rogue se deben “ver” dos veces antes de que sean agregados como granuja por el regulador. Los AP rogue no se consideran ser una amenaza si no están conectados con el segmento cableado de la red corporativa. Para determinar si el granuja es acercamientos activos, diversos se utilizan. Esos acercamientos incluyen RLDP.

Discovery Protocol rogue de la ubicación (RLDP)

RLDP es un acercamiento activo, se utiliza que cuando el AP rogue no tiene ninguna autenticación (autenticación abierta) configurada. Este modo, que se inhabilita por abandono, da instrucciones un AP activo para moverse al canal rogue y para conectar con el granuja como cliente. Durante este tiempo, el AP activo envía los mensajes del deauthentication a todos los clientes conectados y después apaga la interfaz radio. Entonces, se asociará al granuja AP como cliente.

El AP entonces intenta obtener una dirección IP del granuja AP y adelante de un paquete del User Datagram Protocol (UDP) (puerto 6352) que contenga el AP local y la información de conexión rogue al regulador a través del granuja AP. Si el regulador recibe este paquete, la alarma se fija para notificar al administrador de la red que descubrieron a un granuja AP en la red alámbrica con la característica RLDP.

Nota: Utilice el **comando enable del rldp del dot11 del debug** para marcar si el AP ligero asocia y recibe un DHCP Address del granuja AP. Este comando también visualiza el paquete UDP enviado por el AP ligero al regulador.

Una muestra de un paquete UDP (puerto destino 6352) enviado por el AP ligero se muestra aquí:

```
0020 0a 01 01 0d 0a 01 ....... (. * ..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
..... x ......... 0040 00 00 00 00 00 00 00 00 00 00
```

Los primeros 5 bytes de los datos contienen el DHCP Address dado al modo local AP por el granuja AP. Los 5 bytes siguientes son la dirección IP del regulador, seguida por 6 bytes que representen la dirección MAC del granuja AP. Entonces, hay 18 bytes de los ceros.

Operación pasiva:

Se utiliza este acercamiento cuando el AP rogue tiene un poco de forma de autenticación, WEP o WPA. Cuando una forma de autenticación se configura en el granuja AP, el AP ligero no puede asociarse porque no conoce la clave configurada en el granuja AP. El proceso comienza con el regulador cuando pasa encendido la lista de MAC Address del cliente rogue a un AP que se configure como detector rogue. El detector rogue analiza todas las subredes conectadas y configuradas para los pedidos ARP, y el ARP busca para un direccionamiento de la capa que corresponde con 2. Si se descubre una coincidencia, el regulador notifica al administrador de la red que detectan a un granuja en la subred atada con alambre.

Contención rogue del Active

Detectan una vez a un cliente rogue en la red alámbrica, el administrador de la red puede contener el granuja AP y a los clientes rogue. Esto puede ser alcanzada porque los paquetes de la de-autenticación del 802.11 se envían a los clientes que se asocian para eliminar las plantas débiles los AP para atenuar la amenaza que tal agujero crea. Cada vez que hay una tentativa de contener al granuja AP, el casi 15% del recurso AP ligero se utiliza. Por lo tanto, se sugiere para localizar y para quitar físicamente al granuja AP una vez que se contiene.

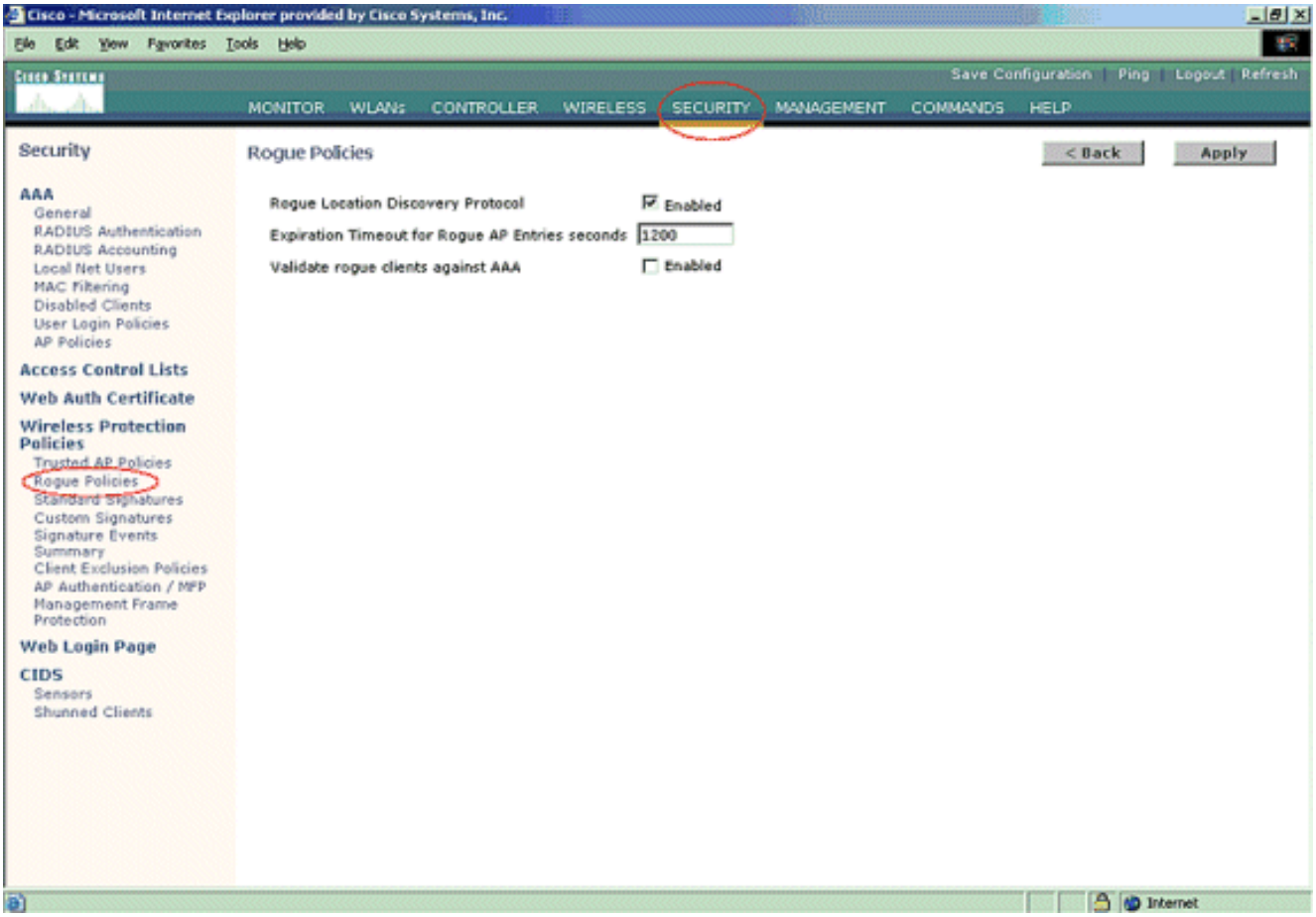
Nota: De la versión 5.2.157.0 del WLC, una vez que se detecta el colorete usted puede ahora elegir contener a manualmente o automáticamente al granuja detectado. En las versiones de software del regulador antes de 5.2.157.0, la contención manual es la única opción.

Detección rogue – Pasos para la configuración

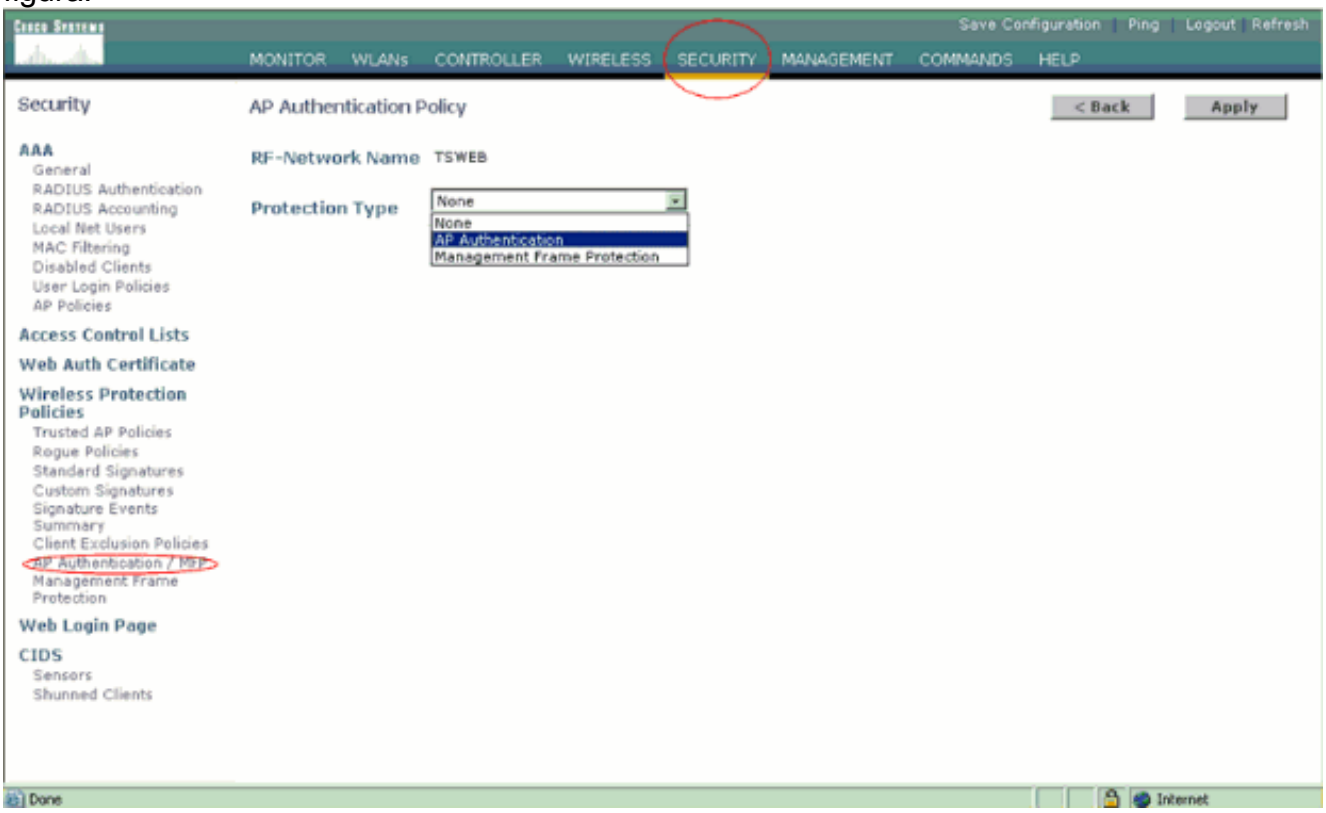
Casi la configuración rogue entera de la detección se habilita por abandono para permitir maximizado, seguridad de la red del hacia fuera-de--cuadro. Estos pasos para la configuración asumen que no se configura ninguna detección rogue en el regulador para aclarar la información rogue importante de la detección.

Para configurar la detección rogue, complete estos pasos:

1. Asegúrese de que el Discovery Protocol de la ubicación del granuja esté girado. Para girarlo, elegir la **Seguridad > las directivas del granuja** y hacer clic **habilitado** en el **Discovery Protocol rogue de la ubicación** tal y como se muestra en de la figura.**Nota:** Si no oyen a un granuja AP por una determinada cantidad de hora, es forma quitada el regulador. Éste es el **descanso de la expiración** para un granuja AP, que se configura debajo de la opción RLDP.

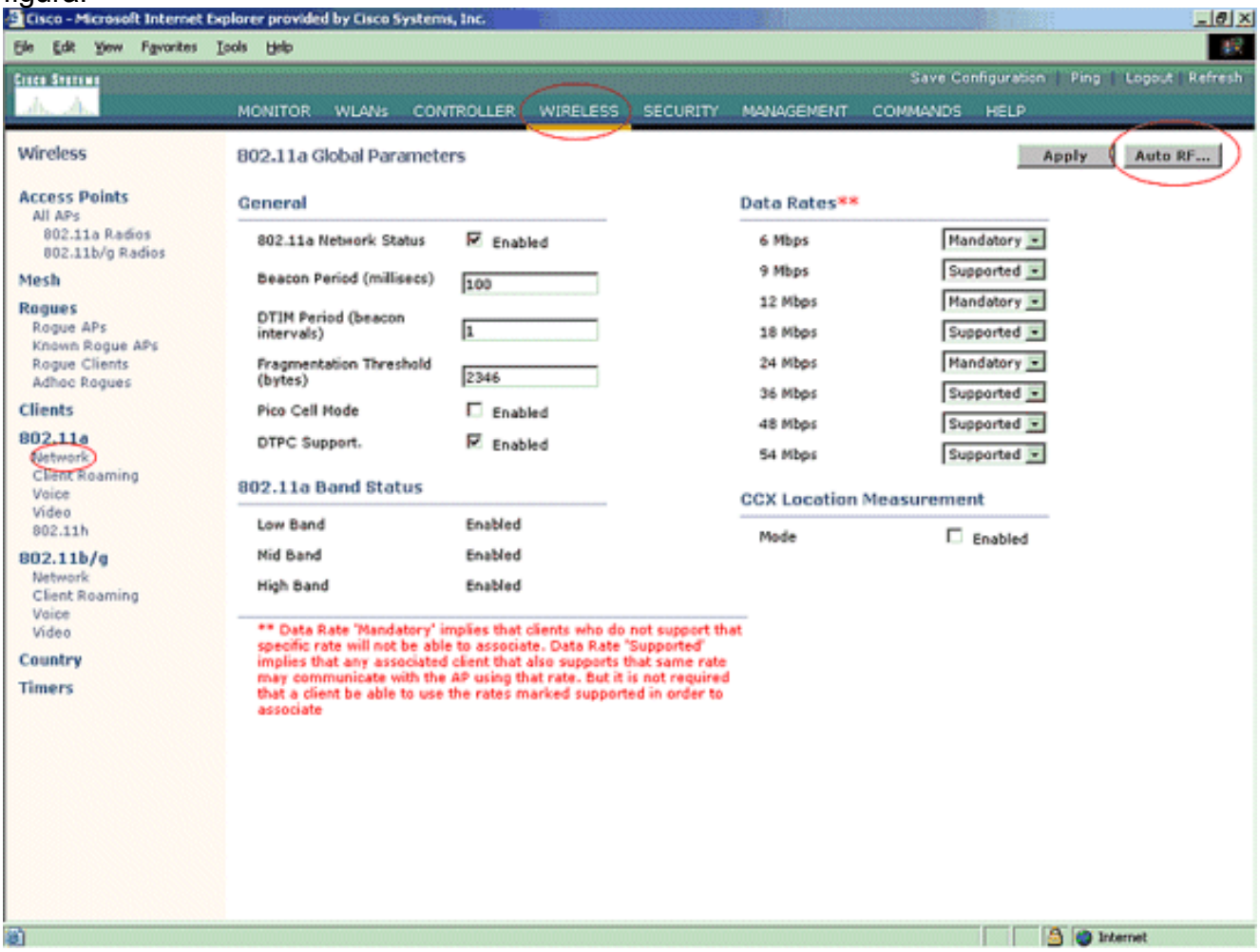


2. Esto es un paso opcional. Cuando se habilita esta característica, los AP que envían los paquetes RRM vecinos con diversos **nombres del grupo RF** están señalados como granujas. Esto será útil en estudiar su entorno RF. Para habilitarlo, elija la **autenticación de Security-> AP**. Entonces, elija la **autenticación AP** como el tipo de protección tal y como se muestra en de la
figura.

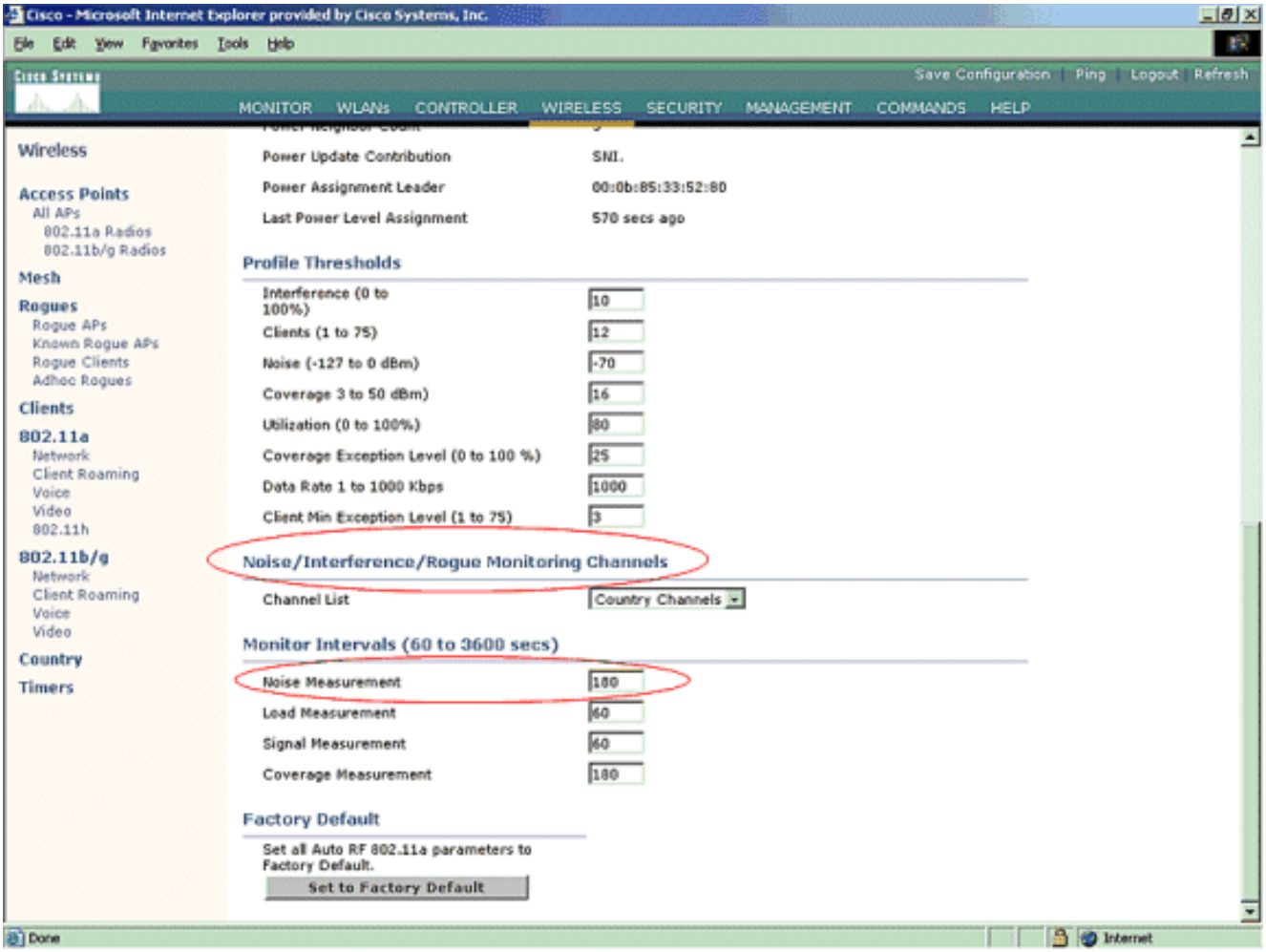


3. Verifique los canales que se analizarán en estos pasos:Seleccione la **red de la Tecnología**

inalámbrica > del 802.11a, entonces **RF auto** en el Lado derecho tal y como se muestra en de la
figura.



En la página **auto RF**, navegue hacia abajo y elija los **canales de supervisión del ruido/de interferencia/del granuja**.



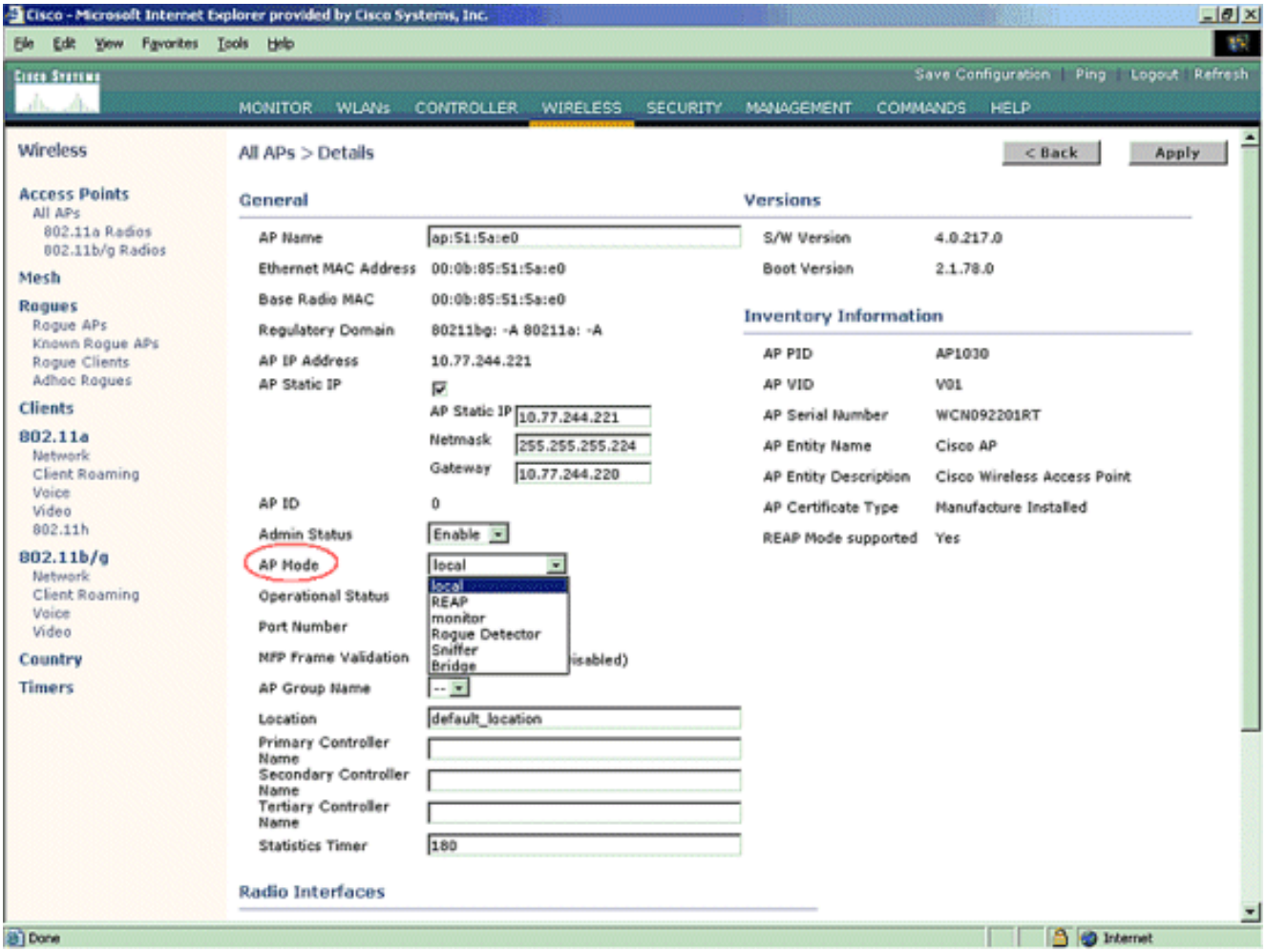
La lista del canal detalla los canales que se analizarán para la supervisión rogue, además del otro regulador y de las funciones AP. Refiera al Lightweight Access Point FAQ para más información sobre los AP ligeros, y al Troubleshooting FAQ del regulador del Wireless LAN (WLC) para más información sobre los reguladores inalámbricos.

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. Fije el período de tiempo para analizar los canales seleccionados:La duración de la exploración del grupo definido de canales se configura conforme a los **intervalos > a la medida de ruido del monitor**, y el rango permisible es a partir 60 a 3600 segundos. Si están idos en el valor por defecto de 180 segundos, los AP analizan cada canal en el grupo de canal una vez, para el ms 50, cada 180 segundos. Durante este período, los cambios de la radio AP de su canal del servicio al canal especificado, escuchan y registran los valores por un período del ms 50, y después vuelven al canal original. El tiempo del salto más la época de detención del ms 50 toma el apagado-canal AP para el ms aproximadamente 60 cada vez. Esto significa que cada AP pasa el total de los de aproximadamente 840 ms 180

segundos que están atentos a los granujas.“Escuche” o el tiempo de la “detención” no se puede modificar y no se cambia con un ajuste del valor de la medida de ruido. Si se baja el temporizador de la medida de ruido, el proceso de detección rogue es probable encontrar a más granujas y encontrarlos más rápidamente. Sin embargo, esta mejora viene a expensas de la integridad de los datos y del Servicio al cliente. Un valor más alto, por otra parte, permite una mejor integridad de los datos pero baja la capacidad de encontrar a los granujas rápidamente.

5. Configure el modo de operación AP:Un modo de operación ligero AP define el papel del AP. Los modos relacionados con la Información presentada en este documento son:**Local** — Éste es el funcionamiento normal de un AP. Este modo permite que mantengan a los clientes de los datos mientras que los canales configurados se analizan para el ruido y los granujas. En este modo de operación, el AP va apagado-canal para el ms 50 y está atentos a los granujas. Completa un ciclo a través de cada canal, uno a la vez, para el período especificado bajo configuración auto RF.**Monitor** — Éste es modo RO de radio, y permite que el AP analice todo el configurado canaliza cada 12 segundos. Solamente los paquetes de la de-autenticación se envían en el aire con un AP configuraron esta manera. Un modo monitor AP puede detectar a los granujas, pero no puede conectar con un granuja sospechoso pues un cliente para enviar los paquetes RLDP.**Nota:** El DCA refiere a los canales sin traslapo que son configurables con los modos predeterminados.**Detector rogue** — En este modo, se apaga la radio AP, y el AP escucha el tráfico atado con alambre solamente. El regulador pasa los AP configurados como los detectores rogue así como listas de clientes rogue sospechosos y de direcciones MAC AP. El detector rogue está atentos los paquetes ARP solamente, y se puede conectar con todos los dominios de broadcast a través de un link de troncal si está deseado.Usted puede configurar a un individuo modo AP simplemente, una vez que el AP ligero está conectado con el regulador. Para cambiar modo AP, conecte con la interfaz Web del regulador y navegue a la **Tecnología inalámbrica**. Haga clic en los **detalles** al lado del AP deseado a para visualizar una pantalla similar ésta:



Utilice modo AP el menú desplegable para seleccionar el modo de operación deseado AP.

Comandos para resolución de problemas

Usted puede también utilizar estos comandos para resolver problemas su configuración en el AP:

- **muestre el resumen rogue ap** — Este comando visualiza la lista del granuja AP detectado por los AP ligeros.
- **muestre el ap rogue detallado** *< dirección MAC del ap> rogue* — utilice este comando para ver los detalles sobre un granuja individual AP. Éste es el comando que las ayudas de determinar si el granuja AP está conectado sobre la red alámbrica.

Conclusión

La detección rogue y la contención dentro de la solución centralizada Cisco del regulador es método más eficaz y el menos más intruso de la industria. La flexibilidad proporcionada al administrador de la red permite un más ajuste personalizado que pueda acomodar cualquier requisito de la red.

Información Relacionada

- Descripción de los grupos RF
- Soporte Técnico y Documentación - Cisco Systems