Resolución de problemas de detección y mitigación de acceso no deseado en una red inalámbrica unificada

Contenido

Introducción

Este documento describe la detección y mitigación de acceso no autorizado en redes inalámbricas de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controladores De Lan Inalámbrica De Cisco.
- Infraestructura Cisco Prime.

Componentes Utilizados

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

- Cisco Unified Wireless Lan Controllers (series 5520, 8540 y 3504) que ejecuta la versión 8.8.120.0.
- Series de AP 1832, 1852, 2802 y 3802 de Wave 2.
- APs 3700, 2700 y 1700 Series de Wave 1.

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 tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

Descripción general de Rogue

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 introduzca su propio punto de acceso (Cisco o no Cisco) en una infraestructura inalámbrica o por cable bien protegida y permita el acceso de usuarios no autorizados a esta red, que de lo contrario estaría protegida, puede poner en peligro fácilmente una red segura.

La detección de acceso no deseado permite al administrador de red supervisar y eliminar este problema de seguridad. La arquitectura Cisco Unified Network proporciona métodos para la detección de elementos no fiables que permiten una identificación completa de elementos no fiables y una solución de contención sin necesidad de herramientas y redes superpuestas caras y difíciles de justificar.

Cualquier dispositivo que comparta su espectro y no esté gestionado por usted puede considerarse un dispositivo no autorizado. Un pícaro se vuelve peligroso en estos escenarios:

- Cuando se configura para utilizar el mismo identificador de conjunto de servicios (SSID) que la red (honeypot)
- Cuando se detecta en la red con cables
- Desconocidos ad-hoc
- Cuando lo configura un extraño, la mayoría de las veces, con intención maliciosa

La mejor práctica es utilizar la detección de elementos no deseados para minimizar los riesgos de seguridad, por ejemplo, en un entorno corporativo.

Sin embargo, hay ciertos escenarios en los que no se necesita la detección de elementos no deseados, por ejemplo, en la implementación de Office Extend Access Point (OEAP), en toda la ciudad o en exteriores.

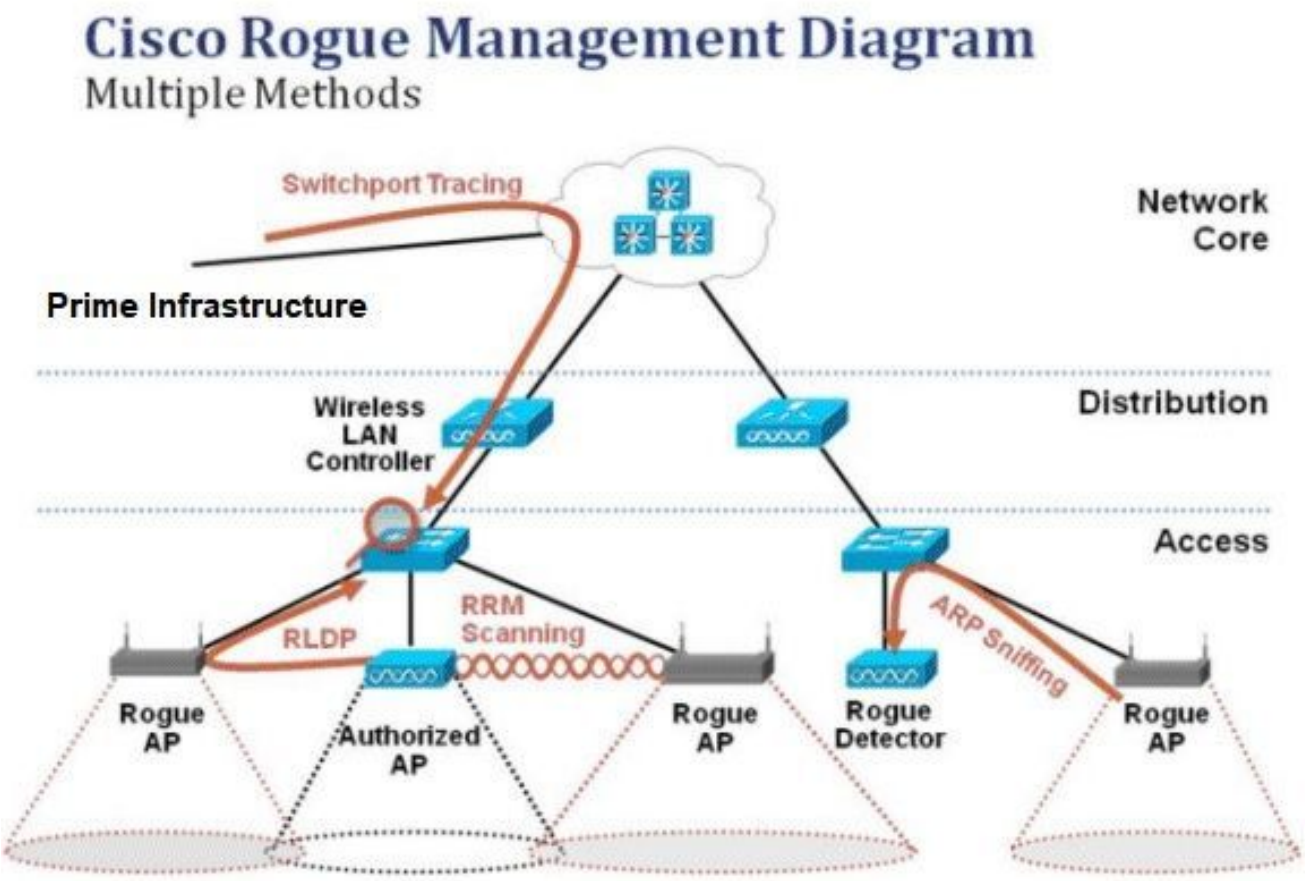
El uso de AP de malla al aire libre para detectar a los pícaros proporcionaría poco valor mientras que utilizaría recursos para analizar.

Por último, es fundamental evaluar (o evitar por completo) la autocontención maliciosa, ya que existen posibles problemas legales y responsabilidades si se deja que funcione automáticamente.

La solución Cisco Unified Wireless Network (UWN) consta de tres fases principales de gestión de dispositivos no fiables:

- Detección: se utiliza un análisis de gestión de recursos de radio (RRM) para detectar la presencia de dispositivos no fiables.

- Clasificación: se utilizan el protocolo de detección de ubicación desconocida (RLDP), los detectores de acceso no autorizado (solo PA de onda 1) y los seguimientos de puertos de switch para identificar si el dispositivo no autorizado está conectado a la red con cables. Las normas de clasificación de delincuentes también ayudan a filtrar los delincuentes en categorías específicas en función de sus características.
- Mitigación: el cierre de los puertos del switch, la ubicación y la contención de elementos no fiables se utilizan para rastrear su ubicación física y anular la amenaza del dispositivo no fiable.



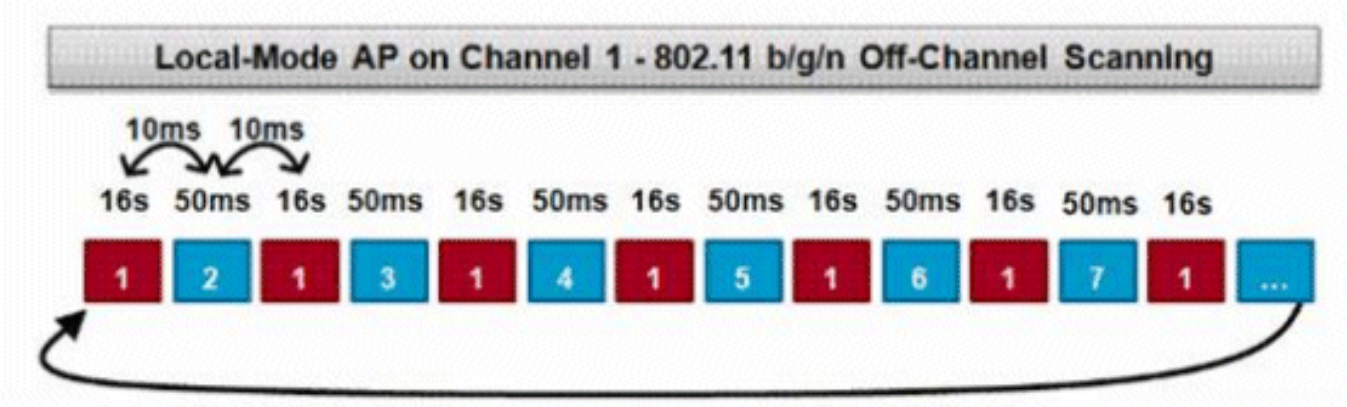
Detección de acceso no autorizado

Un pícaro es básicamente cualquier dispositivo que comparta su espectro, pero que no esté bajo su control. Esto incluye los puntos de acceso desconocidos, el router inalámbrico, los clientes desconocidos y las redes ad-hoc desconocidas. Cisco UWN utiliza una serie de métodos para detectar dispositivos no autorizados basados en Wi-Fi, como un análisis fuera de canal y funciones de modo de monitor dedicado. Cisco Spectrum Expert también se puede utilizar para identificar dispositivos no autorizados que no estén basados en el protocolo 802.11, como los puentes Bluetooth.

Análisis fuera del canal

Esta operación es realizada por los AP de modo Local y Flex-Connect (en modo conectado) y

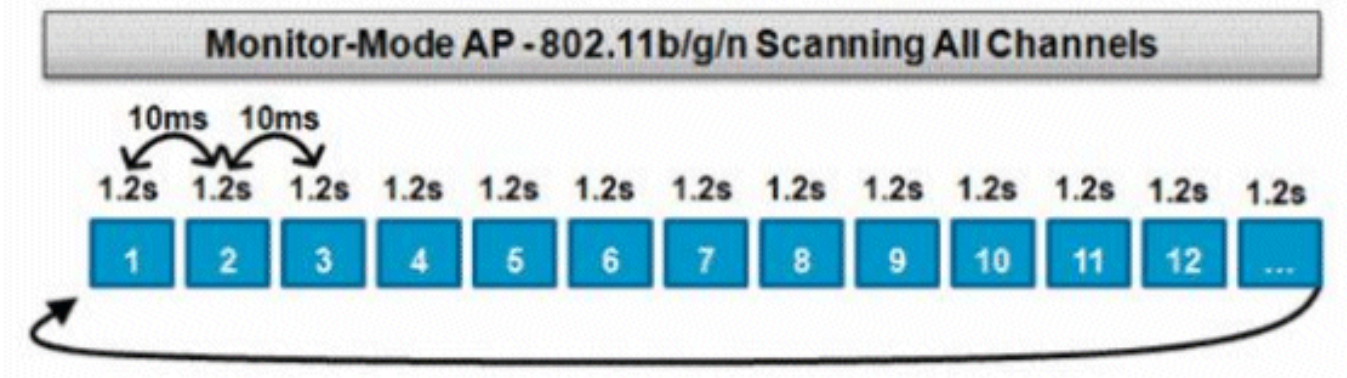
utiliza una técnica de división de tiempo que permite el servicio al cliente y el análisis de canal con el uso de la misma radio. Con el paso a fuera del canal por un período de 50ms cada 16 segundos, el AP, de forma predeterminada, sólo pasa un pequeño porcentaje de su tiempo para no servir a los clientes. Además, tenga en cuenta que se produce un intervalo de cambio de canal de 10 ms. En el intervalo de escaneo predeterminado de 180 segundos, cada canal FCC de 2,4 Ghz (1−11) se escanea al menos una vez. Para otros dominios normativos, como ETSI, el AP está fuera del canal durante un porcentaje de tiempo ligeramente mayor. Tanto la lista de canales como el intervalo de escaneo se pueden ajustar en la configuración RRM. Esto limita el impacto en el rendimiento a un máximo del 1,5% y el algoritmo incorpora inteligencia para suspender el escaneo cuando es necesario entregar tramas de QoS de alta prioridad, como la voz.



Este gráfico es una representación del algoritmo de escaneo fuera de canal para un AP de modo local en la banda de frecuencia de 2.4GHz. Una operación similar se realiza en paralelo en la radio de 5 GHz si el AP tiene uno presente. Cada cuadrado rojo representa el tiempo empleado en el canal de inicio de los AP, mientras que cada cuadrado azul representa el tiempo empleado en los canales adyacentes para fines de escaneo.

Análisis del modo de supervisión

Esta operación es realizada por el Modo Monitor y los APs Adaptive wIPS monitor mode que utilizan el 100% del tiempo de radio para escanear todos los canales en cada banda de frecuencia respectiva. Esto permite una mayor velocidad de detección y permite dedicar más tiempo a cada canal individual. Los AP en modo Monitor también son superiores en la detección de clientes no autorizados ya que tienen una visión más completa de la actividad que ocurre en cada canal.



Este gráfico es una representación del algoritmo de escaneo fuera de canal para un AP en modo monitor en la banda de frecuencia de 2.4GHz. Una operación similar se realiza en paralelo en la radio de 5 GHz si el AP tiene uno presente.

Comparación de los modos local y de supervisión

Un AP de modo local divide sus ciclos entre el servicio de los clientes WLAN y el análisis de los canales en busca de amenazas. Como resultado, un AP de modo local tarda más en recorrer todos los canales y pasa menos tiempo en la recolección de datos en cualquier canal en particular para que las operaciones del cliente no se interrumpan. En consecuencia, los tiempos de detección de ataques y ataques no autorizados son más largos (de 3 a 60 minutos) y se puede detectar un intervalo menor de ataques por aire que con un punto de acceso en modo de supervisión.

Además, la detección de tráfico en ráfagas, como clientes desconocidos, es mucho menos determinista porque el AP tiene que estar en el canal del tráfico al mismo tiempo que se transmite o recibe el tráfico. Esto se convierte en un ejercicio de probabilidades. Un AP de modo de monitor gasta todos sus ciclos en el escaneo de canales para buscar pícaros y ataques por aire. Un AP en modo monitor se puede utilizar simultáneamente para wIPS adaptable, servicios de ubicación (sensibles al contexto) y otros servicios en modo monitor.

Cuando se implementan los AP en modo de supervisión, las ventajas son un menor tiempo de detección. Cuando los AP en modo de supervisión se configuran adicionalmente con wIPS adaptable, se puede detectar una gama más amplia de amenazas y ataques aéreos.

AP de modo local	AP de modo de supervisión
Sirve a los clientes con análisis fuera de canal de división de tiempo	Análisis dedicado
Escucha 50 ms en cada canal	Escucha 1,2 segundos en cada canal
Configurable para escanear: • Todos los canales • Canales de país (predeterminado) • Canales DCA	Analiza todos los canales

Identificación de acceso no autorizado

Si la respuesta de sondeo o las balizas de un dispositivo no autorizado son escuchadas por los AP de modo local, flex-connect o monitor, esta información se comunica a través de CAPWAP al controlador de LAN inalámbrica (WLC) para el proceso. Para evitar falsos positivos, se utilizan

varios métodos para garantizar que otros AP gestionados basados en Cisco no se identifiquen como un dispositivo no fiable. Estos métodos incluyen actualizaciones de grupos de movilidad, paquetes vecinos de RF y APs fáciles de enumerar permitidos a través de Prime Infrastructure (PI).

Registros sospechosos

Mientras que la base de datos de dispositivos no fiables del controlador contiene solo el conjunto actual de no fiables detectados, la PI también incluye un historial de eventos y registra no fiables que ya no se ven.

Detalles de acceso no deseado

Un AP CAPWAP se desconecta del canal durante 50ms para escuchar a los clientes rogue, monitorear el ruido y la interferencia del canal. Cualquier cliente o AP rogue detectado se envía al controlador, que recopila esta información:

- La dirección MAC del punto de acceso no autorizado
- Nombre del punto de acceso no autorizado detectado
- La dirección MAC de los clientes desconocidos conectados
- Política de seguridad
- El preámbulo
- La relación señal-ruido (SNR)
- Luz testigo de intensidad de la señal del receptor (RSSI)
- Canal de detección de acceso no deseado
- Radio en la que se detecta el acceso no deseado
- SSID dudoso (si se transmite el SSID dudoso)
- Dirección IP no autorizada
- Primera y última vez que se informa del delincuente
- Ancho de canal

Para exportar eventos no fiables

Para exportar eventos no deseados a un sistema de administración de red (NMS) de terceros para su archivo, el WLC permite que se agreguen receptores de trampas SNMP adicionales. Cuando el controlador detecta o elimina un no fiable, se comunica una trampa que contiene esta información a todos los receptores de capturas SNMP. Una advertencia con la exportación de

eventos a través de SNMP es que si varios controladores detectan el mismo no autorizado, el NMS ve los eventos duplicados ya que la correlación se realiza solamente en PI.

Tiempo de espera de registro desconocido

Una vez que un AP no autorizado se ha agregado a los registros del WLC, permanece allí hasta que ya no se ve. Después de un tiempo de espera configurable por el usuario (valor predeterminado de 1200 segundos), un no fiable de la categoría_unclassified_se desactualiza.

Los sistemas no fiables de otros estados como_Contained_and_Friendly_ persisten para que se les aplique la clasificación adecuada si vuelven a aparecer.

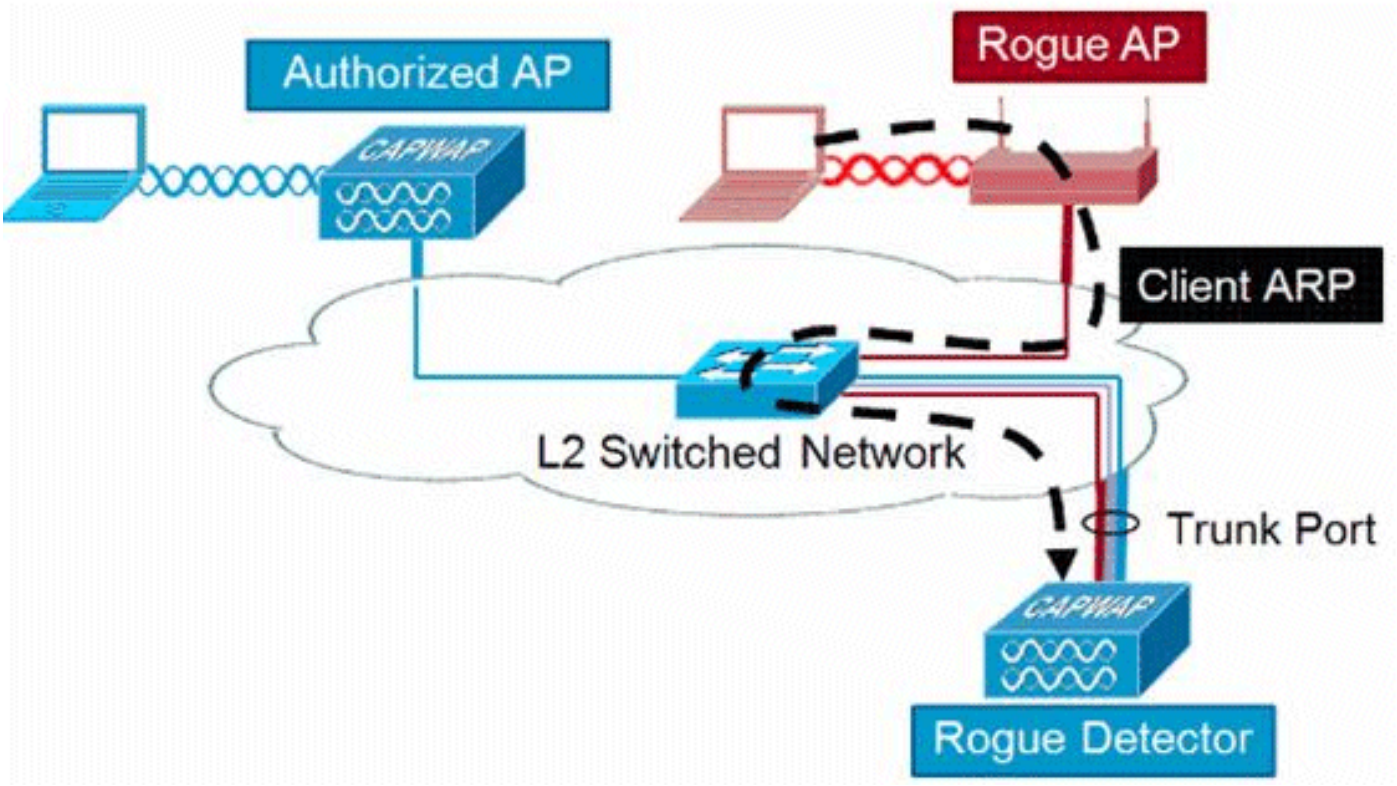
Existe un tamaño máximo de base de datos para los registros no autorizados que es variable entre las plataformas de controlador:

- 3504 - Detección y contención de hasta 600 puntos de acceso desconocidos y 1500 clientes desconocidos
- 5520 - Detección y contención de hasta 24000 puntos de acceso desconocidos y 32000 clientes desconocidos
- 8540 - Detección y contención de hasta 24000 puntos de acceso desconocidos y 32000 clientes desconocidos

AP de detector de acceso no autorizado

Un punto de acceso de detector de acceso no autorizado tiene como objetivo correlacionar la información no autorizada que se escucha por el aire con la información ARP obtenida de la red por cable. Si una dirección MAC se escucha por el aire como un AP o cliente no autorizado y también se escucha en la red cableada, se determina que el no autorizado está en la red cableada. Si se detecta que el punto de acceso no autorizado está en la red con cables, la gravedad de la alarma para ese punto de acceso no autorizado se eleva a_critical_. Un AP de detector no autorizado no es exitoso en la identificación de clientes no autorizados detrás de un dispositivo que utiliza NAT.

Este enfoque se utiliza cuando el AP no autorizado tiene alguna forma de autenticación, ya sea WEP o WPA. Cuando se configura una forma de autenticación en un AP no autorizado, el AP ligero no puede asociarse porque no conoce el método de autenticación y las credenciales configuradas en el AP no autorizado.



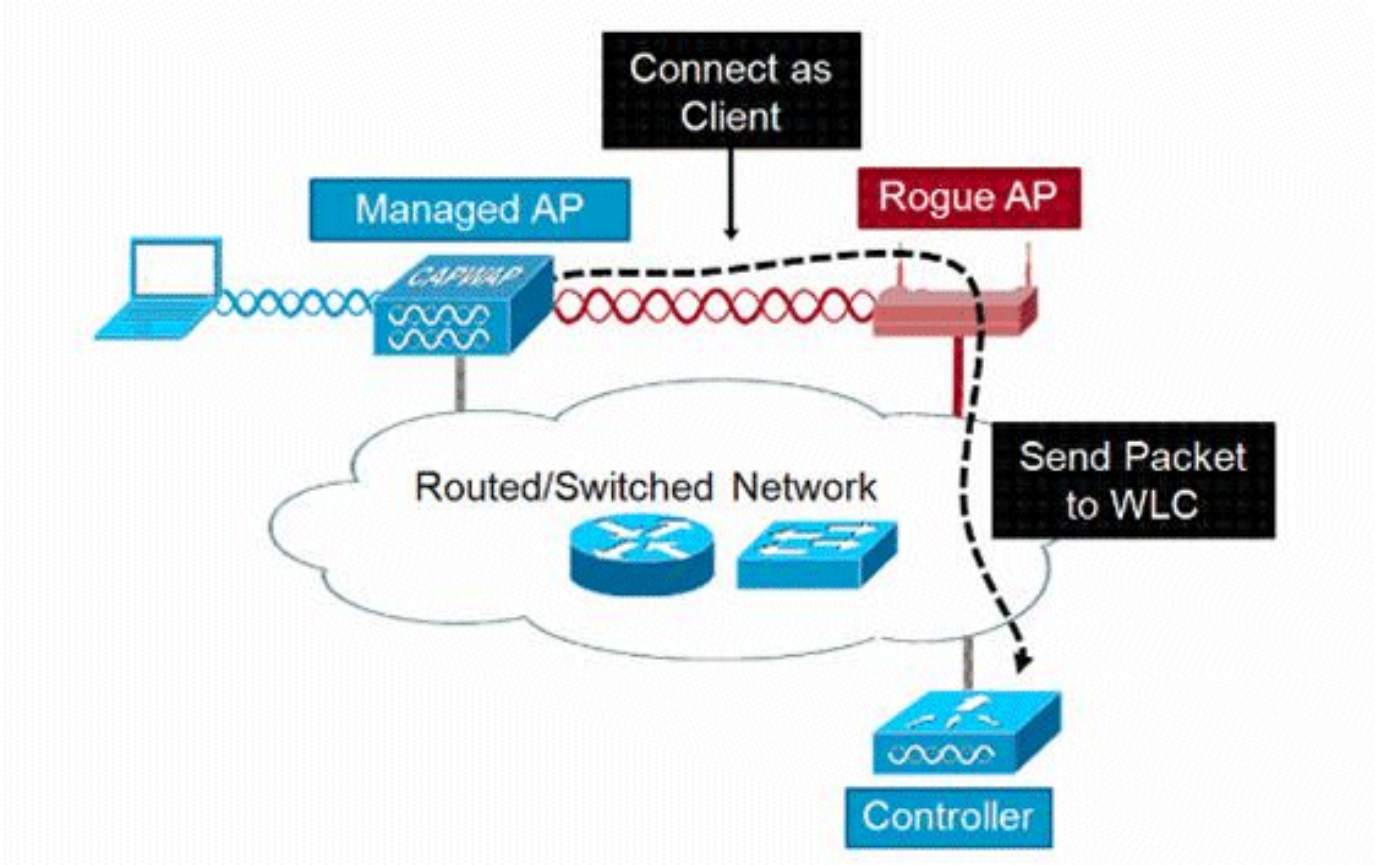
Nota: Solo los AP de la onda 1 se pueden configurar como detectores no fiables.

Consideraciones sobre escalabilidad

Un AP de detector de acceso no autorizado puede detectar hasta 500 clientes no autorizados y 500 clientes no autorizados. Si el detector de acceso no autorizado se coloca en un tronco con demasiados dispositivos no fiables, se superan estos límites, lo que provoca problemas. Para evitar que esto ocurra, mantenga los APs de detector de acceso no autorizados en la capa de distribución o acceso de su red.

RLDP

El objetivo de RLDP es identificar si un punto de acceso no autorizado específico está conectado a la infraestructura cableada. Esta función esencialmente utiliza el AP más cercano para conectar con el dispositivo rogue como cliente inalámbrico. Después de la conexión como cliente, se envía un paquete con la dirección de destino del WLC para evaluar si el AP está conectado a la red cableada. Si se detecta que el punto de acceso no autorizado está en la red con cables, la gravedad de la alarma para ese punto de acceso no autorizado se eleva a crítica.



El algoritmo de RLDP se enumera aquí:

1. Identifique el punto de acceso unificado más cercano al no fiable mediante el uso de valores de potencia de la señal.
2. El AP entonces se conecta con el rogue como cliente WLAN, intenta tres asociaciones antes de que se agote el tiempo de espera.
3. Si la asociación es exitosa, el AP entonces utiliza DHCP para obtener una dirección IP.
4. Si se obtuvo una dirección IP, el AP (que actúa como cliente WLAN) envía un paquete UDP a cada una de las direcciones IP del controlador.
5. Si el controlador recibe incluso uno de los paquetes RLDP del cliente, ese rogue se marca como en el cable con una gravedad de crítico.

Nota: Los paquetes RLDP no pueden alcanzar el controlador si las reglas de filtro están en su lugar entre la red del controlador y la red donde se encuentra el dispositivo no autorizado.

Advertencias de RLDP

- RLDP sólo funciona con AP rogue abiertos que difunden su SSID con la autenticación y el cifrado inhabilitados.

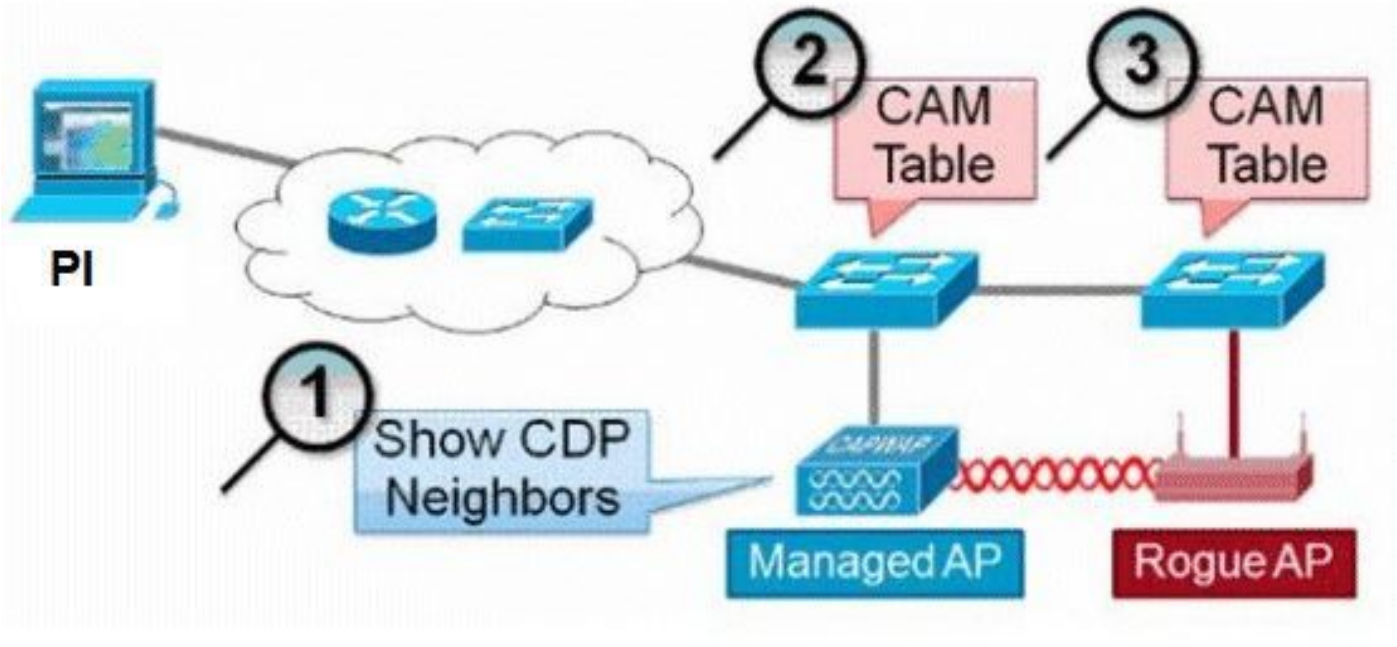
- RLDP requiere que el AP administrado que actúa como cliente pueda obtener una dirección IP a través de DHCP en la red no autorizada
- RLDP manual se puede utilizar para intentar y rastrear RLDP en un rogue varias veces.
- En el proceso RLDP, el AP no puede servir a los clientes. Esto afecta negativamente el rendimiento y la conectividad de los AP de modo local.
- RLDP no intenta conectarse a un AP no autorizado que opera en un canal DFS de 5 GHz.

Rastreos de puertos de switch

El seguimiento del puerto del switch es una técnica de mitigación de AP dudosa. Aunque el seguimiento del puerto del switch se inicia en el PI, utiliza la información CDP y SNMP para rastrear a un rogue hacia un puerto específico en la red.

Para que se ejecute el seguimiento del puerto del switch, todos los switches de la red deben agregarse al PI con credenciales SNMP. Aunque las credenciales de solo lectura funcionan para identificar el puerto en el que se encuentra el no fiable, las credenciales de lectura y escritura permiten que el PI también apague el puerto, por lo que contiene la amenaza.

En este momento, esta función funciona solamente con los switches de Cisco que ejecutan Cisco IOS® con CDP habilitado, y CDP también se debe habilitar en los AP administrados.

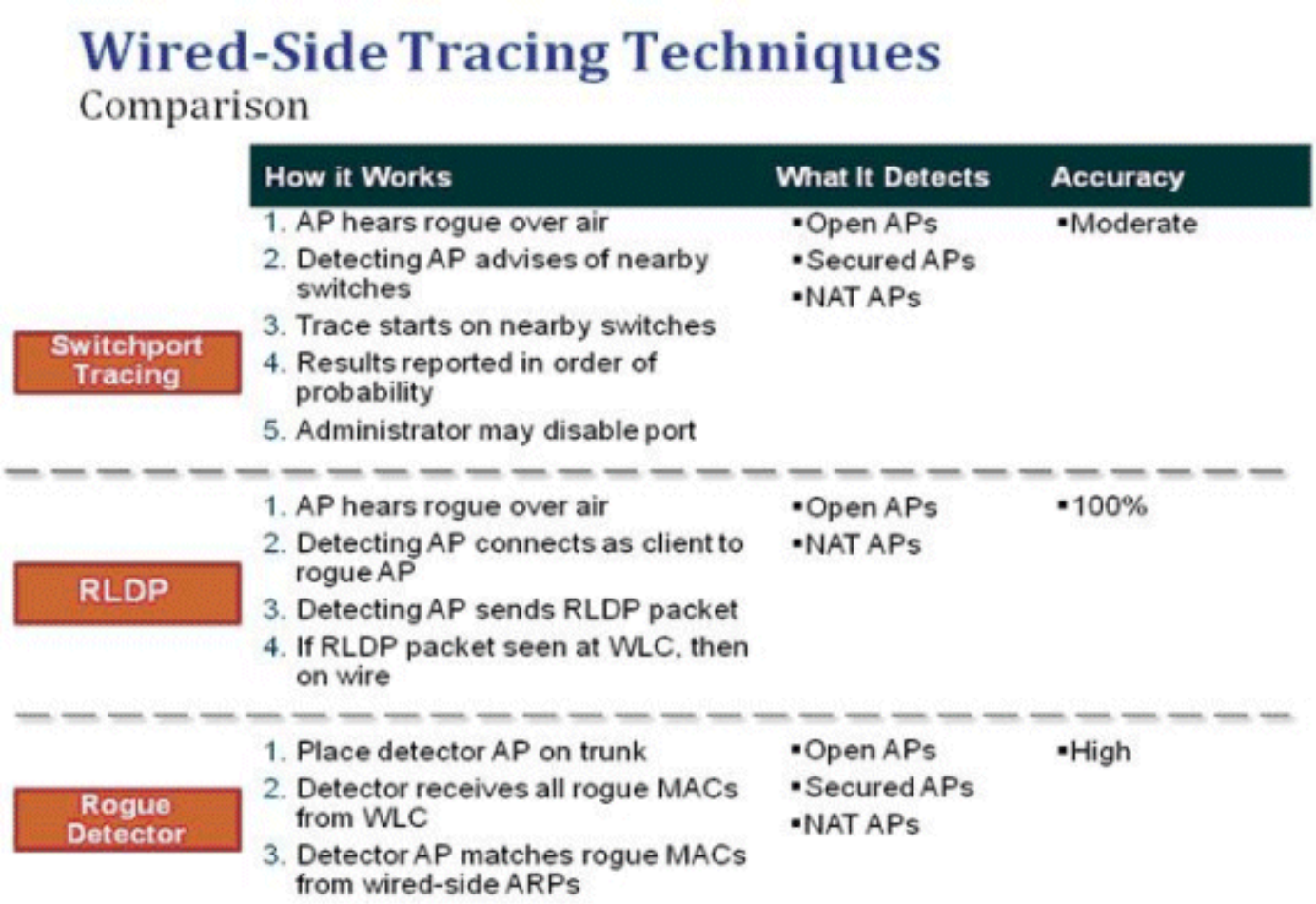


El algoritmo para el seguimiento del puerto del switch se enumera aquí:

1. El PI encuentra el AP más cercano, que detecta el AP no autorizado por el aire, y recupera sus vecinos CDP.
2. El IP entonces utiliza SNMP para examinar la tabla CAM dentro del switch vecino, busca una coincidencia positiva para identificar la ubicación de los rogues.

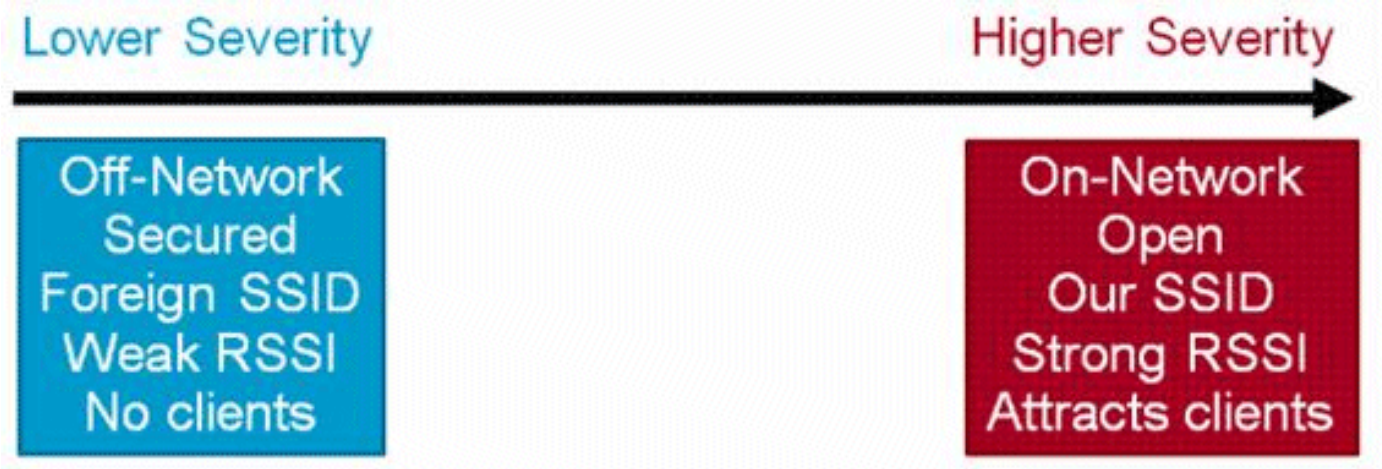
3. Una coincidencia positiva se basa en la dirección MAC no autorizada exacta, +1/−1 la dirección MAC no autorizada, cualquier dirección MAC de cliente no autorizada o una coincidencia de OUI basada en la información del proveedor inherente a una dirección MAC.

4. Si no se encuentra una coincidencia positiva en el switch más cercano, el PI continúa la búsqueda en los switches vecinos hasta a dos saltos de distancia (de forma predeterminada).



Clasificación de acceso no deseado

De forma predeterminada, todos los sistemas no fiables detectados por Cisco UWN se consideran no clasificados. Como se muestra en este gráfico, los clientes no autorizados se pueden clasificar según una serie de criterios que incluyen RSSI, SSID, tipo de seguridad, red de conexión/desconexión y número de clientes:



Reglas de clasificación de no fiables

Las reglas de clasificación de acceso no deseado permiten definir un conjunto de condiciones que marcan un acceso no deseado como malintencionado o no deseado. Estas reglas se configuran en el PI o en el WLC, pero siempre se realizan en el controlador a medida que se descubren nuevos rogues.

Lea el documentoRule Based Rogue Classification in Wireless LAN Controllers (WLC) and Prime Infrastructure (PI) para obtener más información sobre las reglas no autorizadas en los WLC.

Hechos de HA

Si mueve manualmente cualquier dispositivo no autorizado al estado contenido (cualquier clase) o al estado descriptivo, esta información se almacena en la memoria flash del WLC de Cisco en espera; sin embargo, la base de datos no se actualiza. Cuando ocurre el switchover HA, se carga la lista de rogue de la memoria flash del WLC de Cisco previamente en espera.

En un escenario de alta disponibilidad, si el nivel de seguridad de detección no autorizada se establece en Alta o Crítica, el temporizador no autorizado en el controlador en espera se inicia sólo después de que la detección no autorizada pase el tiempo de estabilización, que es de 300 segundos. Por lo tanto, las configuraciones activas en el controlador en espera se reflejan solamente después de 300 segundos.

Datos de Flex-Connect

Un punto de acceso FlexConnect (con la detección de elementos no fiables activada) en el modo conectado toma la lista de contención del controlador. Si se configuran SSID de contención automática y ad hoc de autocontención en el controlador, estas configuraciones se establecen en todos los AP de FlexConnect en el modo conectado y el AP lo almacena en su memoria.

Cuando el punto de acceso de FlexConnect pasa a un modo independiente, se realizan las siguientes tareas:

- La contención establecida por el controlador continúa.

- Si el AP de FlexConnect detecta cualquier AP no autorizado que tenga el mismo SSID que el de SSID infra (SSID configurado en el controlador al que está conectado el AP de FlexConnect), se inicia la contención si se activó la contención automática de SSID desde el controlador antes de que se mueva al modo independiente.
- Si el AP de FlexConnect detecta cualquier rogue ad hoc, se inicia la contención si se habilitó la contención automática ad hoc desde el controlador cuando estaba en el modo conectado.

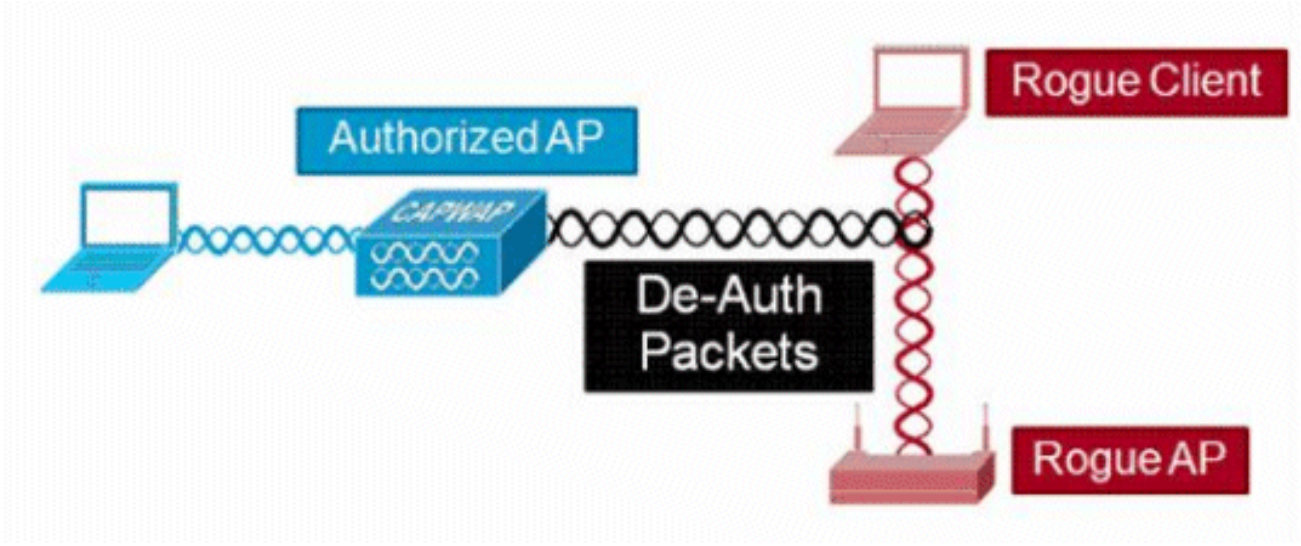
Cuando el punto de acceso de FlexConnect independiente vuelve al modo conectado, se realizan estas tareas:

- Toda la contención se borra.
- La contención iniciada desde el controlador toma el control.

Mitigación de acceso no deseado

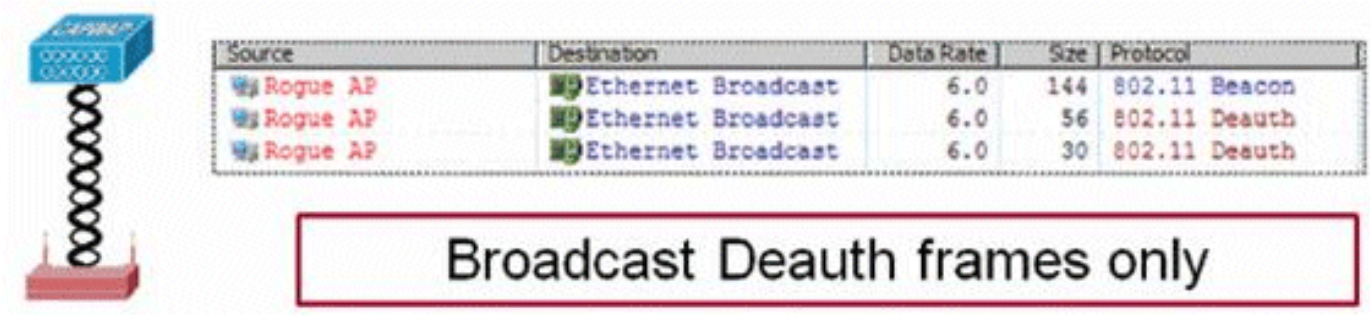
Contención de acceso no deseado

La contención es un método que utiliza paquetes por aire para interrumpir temporalmente el servicio en un dispositivo no autorizado hasta que se pueda eliminar físicamente. La contención funciona con la suplantación de paquetes de desautenticación con la dirección de origen suplantada del AP no autorizado para que cualquier cliente asociado sea expulsado.

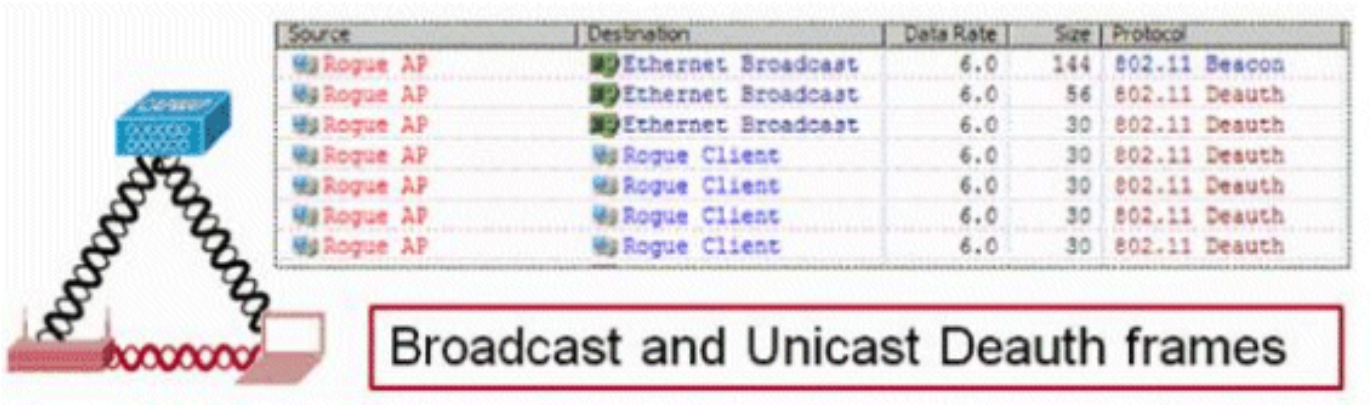


Detalles de contención de acceso no autorizado

Una contención iniciada en un AP no autorizado sin clientes sólo utiliza tramas de desautenticación enviadas a la dirección de difusión:

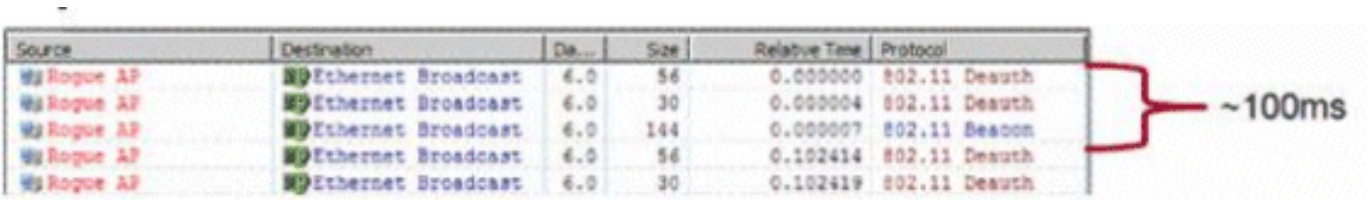


Una contención iniciada en un AP no autorizado con los clientes que utilizan tramas de desautenticación enviadas a la dirección de difusión y a la dirección del cliente:



Los paquetes de contención se envían al nivel de potencia del AP administrado y a la velocidad de datos habilitada más baja.

La contención envía un mínimo de 2 paquetes cada 100 ms:



Nota: Una contención realizada por los AP en modo no monitor se envía en un intervalo de 500 ms en lugar del intervalo de 100 ms utilizado por los AP en modo monitor.

- Un dispositivo no autorizado individual puede estar contenido por 1 o 4 puntos de acceso administrados que funcionan conjuntamente para mitigar la amenaza temporalmente.
- La contención se puede realizar mediante el uso del modo local, el modo monitor y los AP en modo flex-connect (conectado). Para el modo local de los AP flex-connect, se puede contener un máximo de tres dispositivos no autorizados por radio. Para los AP en modo monitor, se puede contener un máximo de seis dispositivos no autorizados por radio.

Contención automática

Además de la iniciación manual de la contención en un dispositivo no autorizado vía PI o la GUI del WLC, hay también la capacidad de lanzar automáticamente la contención bajo ciertos escenarios. Esta configuración se encuentra debajo de Generalen la sección Políticas no fiables de la interfaz de controlador o IP. Cada una de estas funciones está desactivada de forma predeterminada y solo se deben activar para anular las amenazas que causan más daños.

- Rogue on Wire: si se identifica que un dispositivo no fiable está conectado a la red con cables, se lo pone automáticamente bajo contención.
- Uso de nuestro SSID: Si un dispositivo no autorizado utiliza un SSID que es el mismo que el configurado en el controlador, se incluye automáticamente. Esta función tiene como objetivo hacer frente a un ataque de tiesto de miel antes de que cause daños.
- Cliente válido en punto de acceso no autorizado: si se descubre que un cliente enumerado en el servidor Radius/AAA está asociado con un dispositivo no autorizado, la contención se inicia únicamente contra ese cliente, lo que impide la asociación a cualquier punto de acceso no administrado.
- AdHoc Rogue AP - Si se descubre una red ad-hoc, se la contiene automáticamente.

Advertencias de contención dudosas

- Debido a que la contención utiliza una parte del tiempo de radio del AP administrado para enviar las tramas de desautenticación, el rendimiento de los clientes de datos y voz se ve afectado negativamente hasta en un 20%. En el caso de los clientes de datos, el impacto se reduce en rendimiento. Para los clientes de voz, la contención puede causar interrupciones en las conversaciones y reducir la calidad de la voz.
- La contención puede tener implicaciones legales cuando se lanza contra redes vecinas. Asegúrese de que el dispositivo no autorizado se encuentre dentro de la red y de que suponga un riesgo para la seguridad antes de iniciar la contención.

Cierre del puerto del switch

Una vez que se rastrea un puerto de switch mediante el uso de SPT, existe una opción para inhabilitar ese puerto en PI. El administrador debe realizar este ejercicio manualmente. Hay una opción disponible para activar el puerto del switch a través de PI si se elimina físicamente el acceso no deseado de la red.

Configurar

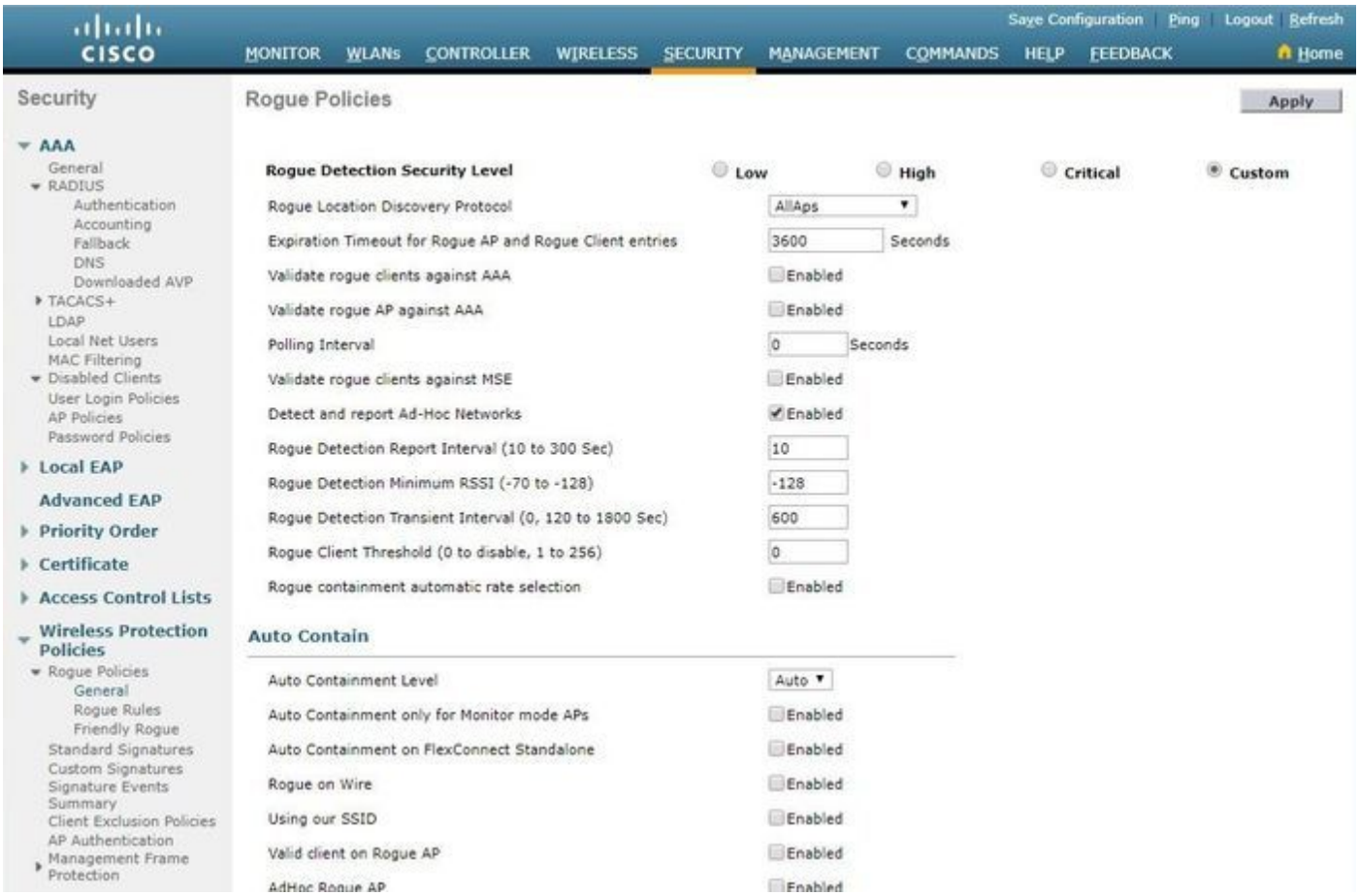
Configuración de Detección de acceso no autorizado

La detección de acceso no deseado está habilitada en el controlador de forma predeterminada.

Para configurar varias opciones, navegue hastaSeguridad > Políticas de protección inalámbrica > Políticas de acceso no autorizado > General. Como ejemplo:

Paso 1. Cambie el tiempo de espera para los AP rogue.

Paso 2. Habilitar la detección de redes no autorizadas ad-hoc.



Desde la CLI:

<#root>

```
(Cisco Controller) >
```

config rogue ap timeout ?

```
<seconds>      The number of seconds<240 - 3600> before rogue entries are flushed

(Cisco Controller) >
```

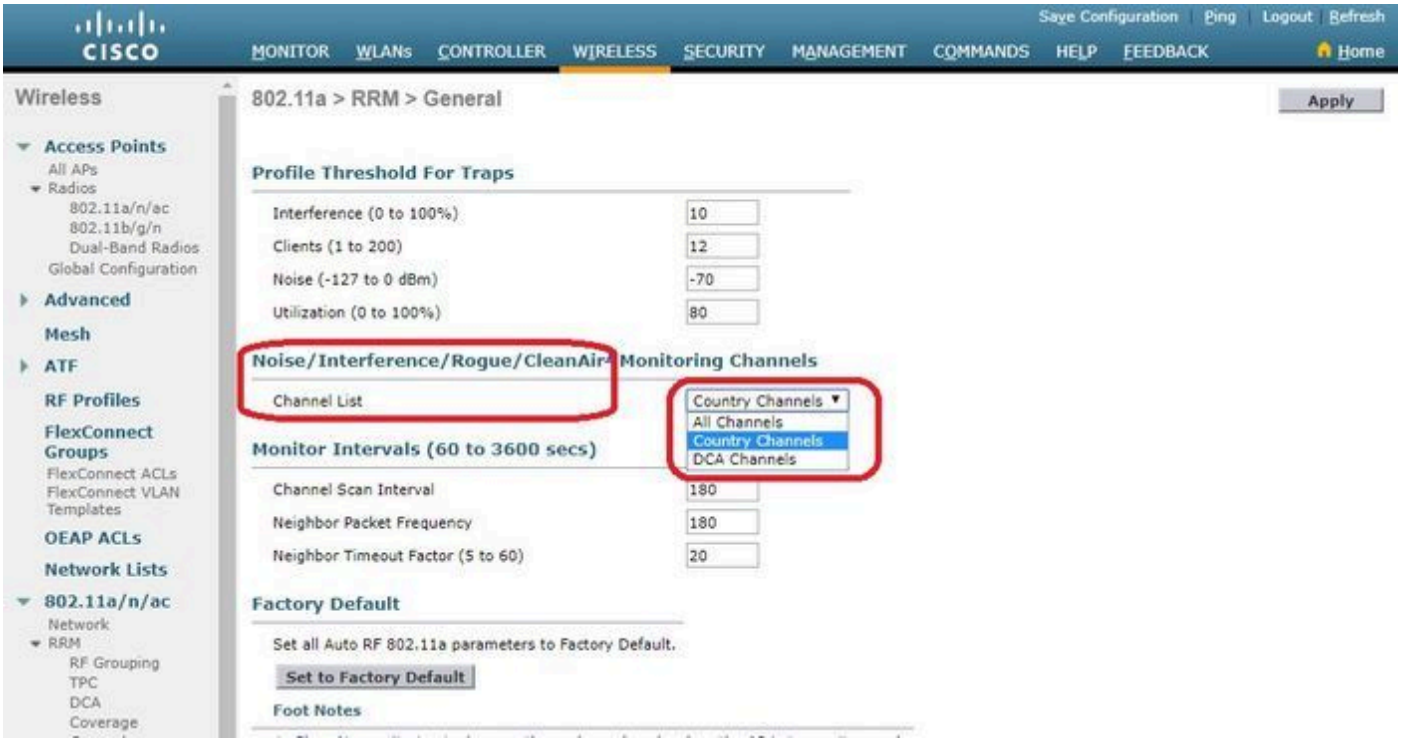
config rogue adhoc enable/disable

Configuración del análisis de canales para la detección de acceso no autorizado

Para un AP de modo local/Flex-Connect/Monitor, hay una opción en la configuración RRM que permite al usuario elegir qué canales se analizan en busca de canales no fiables. Depende de la

configuración, el AP explora todos los canales/país/canal DCA para los rogues.

Para configurar esto desde la GUI, navegue hasta Wireless > 802.11a/802.11b > RRM > General, como se muestra en la imagen.



Desde la CLI:

<#root>

```
(Cisco Controller) >
```

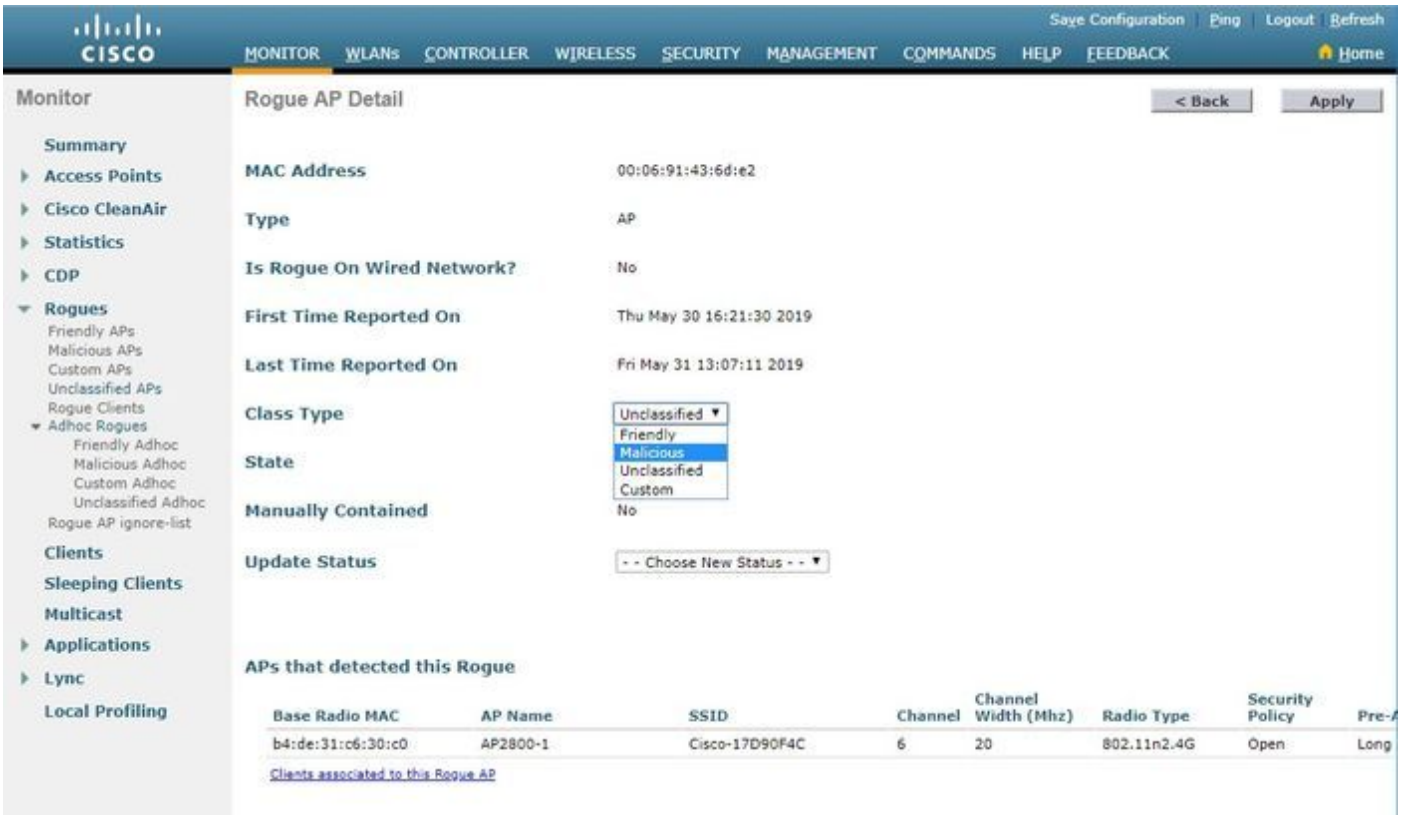
config advanced 802.11a monitor channel-list ?

```
all             Monitor all channels
country         Monitor channels used in configured country code
dca             Monitor channels used by automatic channel assignment
```

Configurar clasificación de no fiables

Clasificación manual de un punto de acceso no autorizado

Para clasificar un rogue AP como amistoso, malicioso, o no clasificado, navegue a Monitor > Rogue > Unclassified AP, y haga clic en el nombre del rogue AP particular. Elija la opción de la lista desplegable, como se muestra en la imagen.



Desde la CLI:

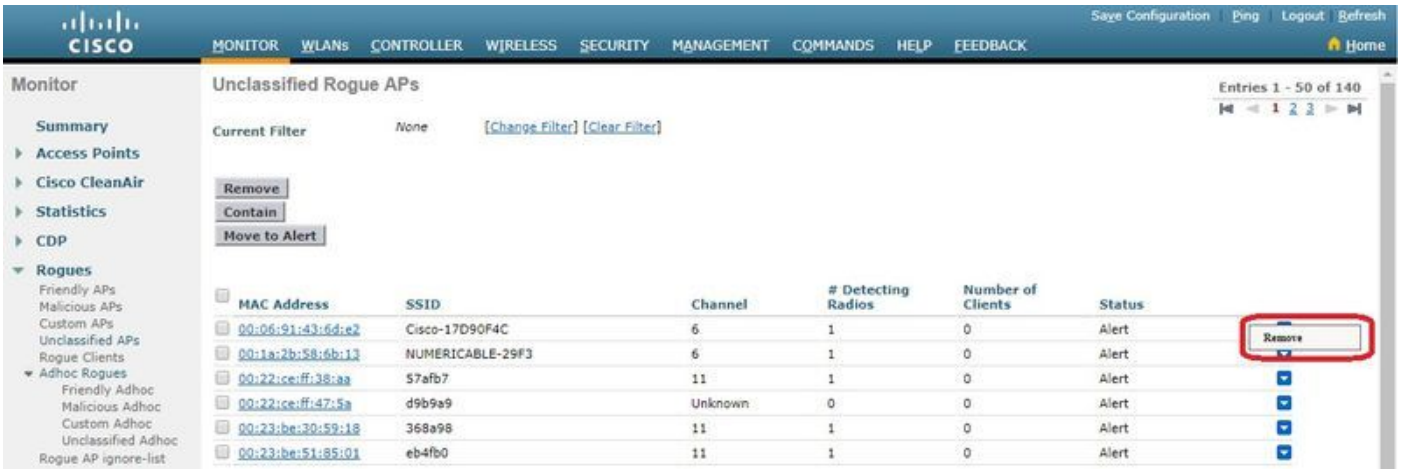
<#root>

```
(Cisco Controller) >
```

config rogue ap ?

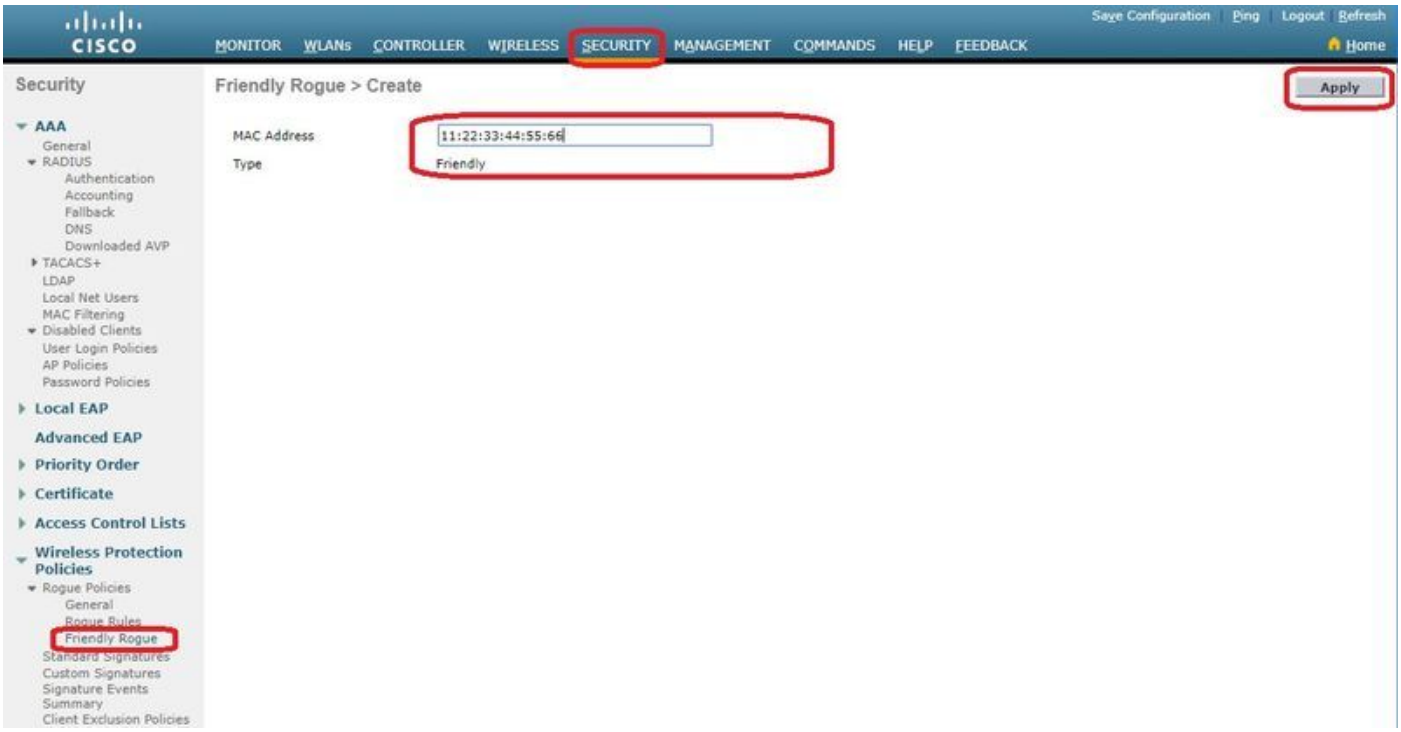
```
classify       Configures rogue access points classification.
friendly       Configures friendly AP devices.
rldp           Configures Rogue Location Discovery Protocol.
ssid           Configures policy for rogue APs advertsing our SSID.
timeout        Configures the expiration time for rogue entries, in seconds.
valid-client   Configures policy for valid clients which use rogue APs.
```

Para eliminar una entrada no autorizada manualmente de la lista de no fiables, navegue hastaMonitor > No fiable > APs no clasificados y haga clic en Remove, como se muestra en la imagen.



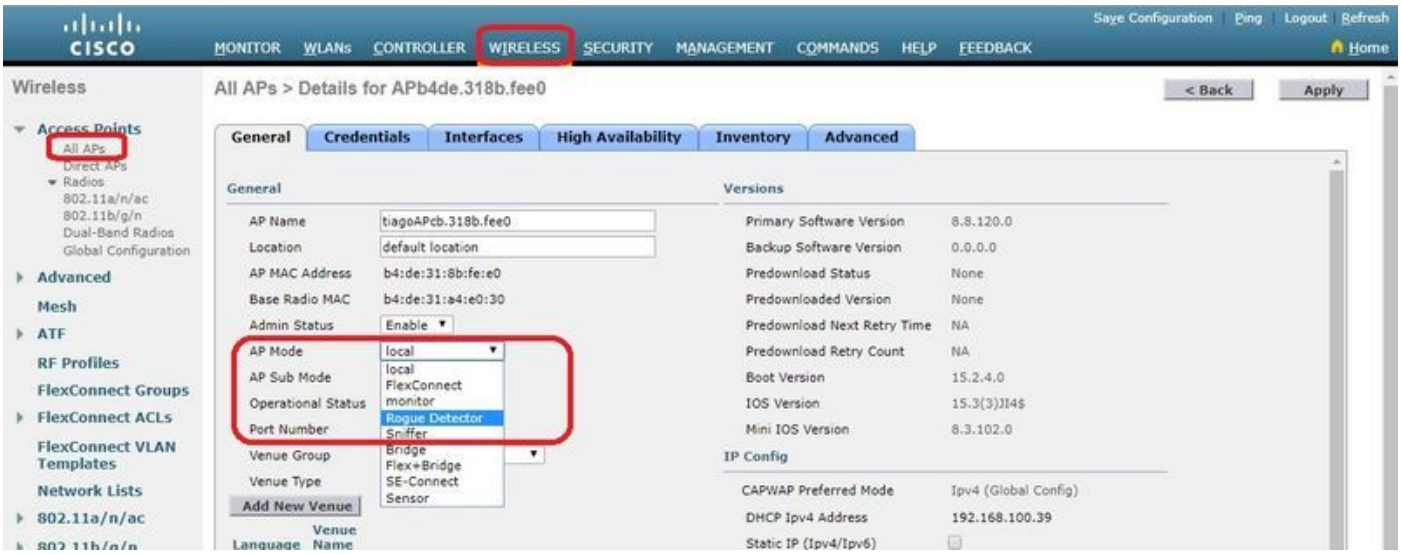
Para configurar un Rogue AP como un AP amistoso, navegue hastaSeguridad > Wireless Protection Policies > Rogue Policies > Friendly Rogue y agregue la dirección MAC del rogue.

Las entradas de rogue amistoso agregadas se pueden verificar desdeMonitor > Rogues > Friendly Rogue page, como se muestra en la imagen.



Configuración de un punto de acceso de detector no autorizado

Para configurar el AP como un detector rogue a través de la GUI, navegue hasta Wireless > All APs. Elija el nombre del AP y cambie el modo AP como se muestra en la imagen.



Desde la CLI:

<#root>

```
(Cisco Controller) >
```

config ap mode rogue AP_Managed

```
Changing the AP's mode cause the AP to reboot.
Are you sure you want to continue? (y/n) y
```

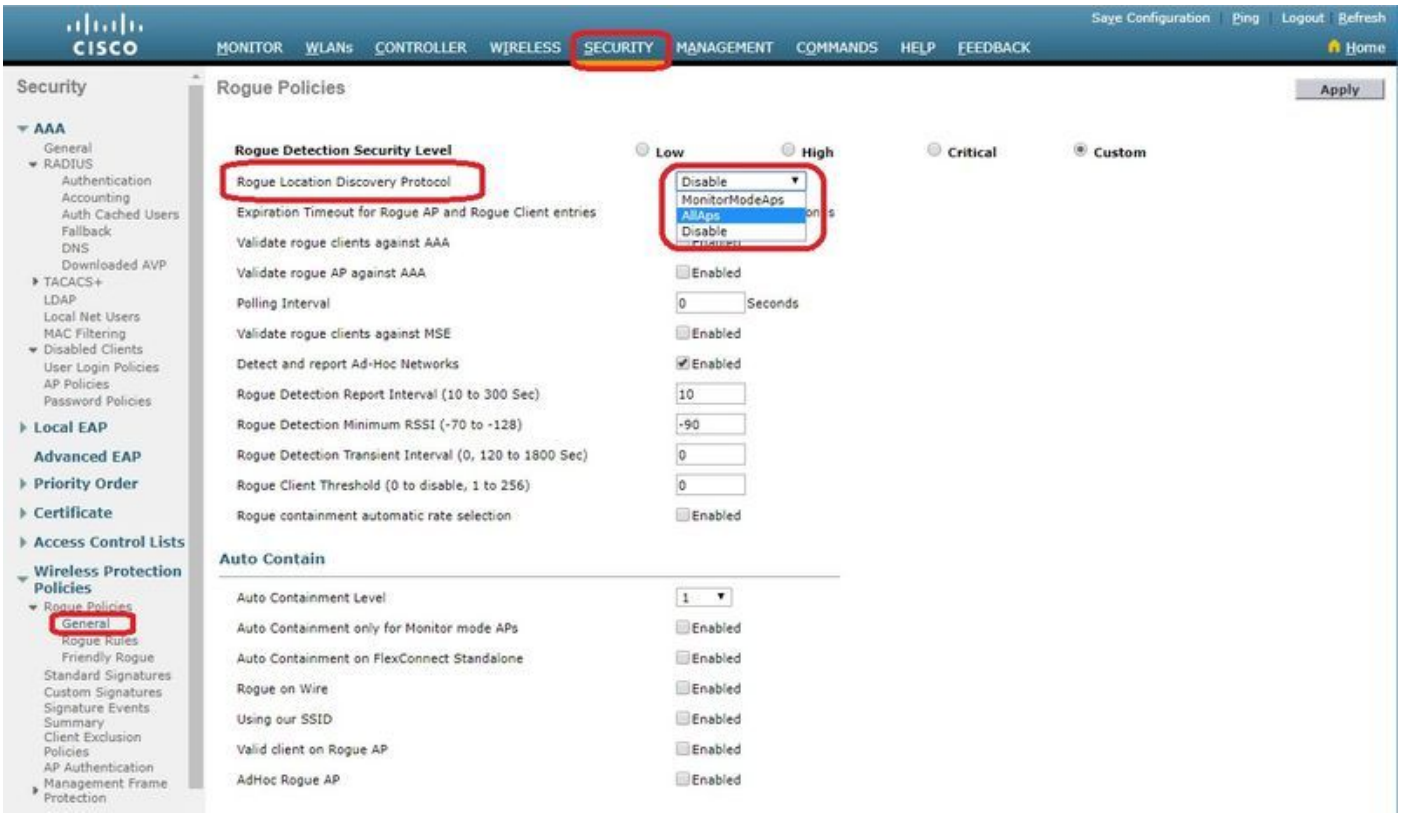
Configuración del puerto de switch para un AP de detector de acceso no autorizado

```
interface GigabitEthernet1/0/5
description Rogue Detector
switchport trunk native vlan 100
switchport mode trunk
```

Nota: La VLAN nativa en esta configuración es una que tiene conectividad IP al WLC.

Configurar RLDP

Para configurar RLDP en la GUI del controlador, navegue hastaSeguridad > Políticas de protección inalámbrica > Políticas de acceso no autorizado > General.



AP en modo Monitor: Permite que solamente los AP en modo monitor participen en RLDP.

Todos los APs- los APs de modo Local/Flex-Connect/Monitor participan en el proceso RLDP.

Desactivado: RLDP no se activa automáticamente. Sin embargo, el usuario puede activar RLDP manualmente para una dirección MAC determinada a través de la CLI.

Nota: El AP en modo Monitor obtiene preferencia sobre el AP Flex-Connect local para realizar RLDP si ambos detectan un rogue particular que excede los -85dbm RSSI.

Desde la CLI:

<#root>

```
(Cisco Controller) >

config rogue ap rldp enable

 ?

alarm-only      Enables RLDP and alarm if rogue is detected
auto-contain    Enables RLDP, alarm and auto-contain if rogue is detected.

(Cisco Controller) >config rogue ap rldp enable alarm-only ?

monitor-ap-only Perform RLDP only on monitor AP
```

La programación RLDP y el disparador manual sólo se pueden configurar a través del símbolo del

sistema. Para iniciar RLDP manualmente:

<#root>

```
(Cisco Controller) >

config rogue ap rldp initiate

 ?

<MAC addr> Enter the MAC address of the rogue AP (e.g. 01:01:01:01:01:01).
```

Para el programa de RLDP:

<#root>

```
(Cisco Controller) >

config rogue ap rldp schedule ?


add             Enter the days when RLDP scheduling to be done.
delete          Enter the days when RLDP scheduling needs to be deleted.
enable          Configure to enable RLDP scheduling.
disable         Configure to disable RLDP scheduling.


(Cisco Controller) >

config rogue ap rldp schedule add ?


fri             Configure Friday for RLDP scheduling.
sat             Configure Saturday for RLDP scheduling.
sun             Configure Sunday for RLDP scheduling.
mon             Configure Monday for RLDP scheduling.
tue             Configure Tuesday for RLDP scheduling.
wed             Configure Wednesday for RLDP scheduling.
thu             Configure Thursday for RLDP scheduling.
```

Los reintentos RLDP se pueden configurar con el comando:

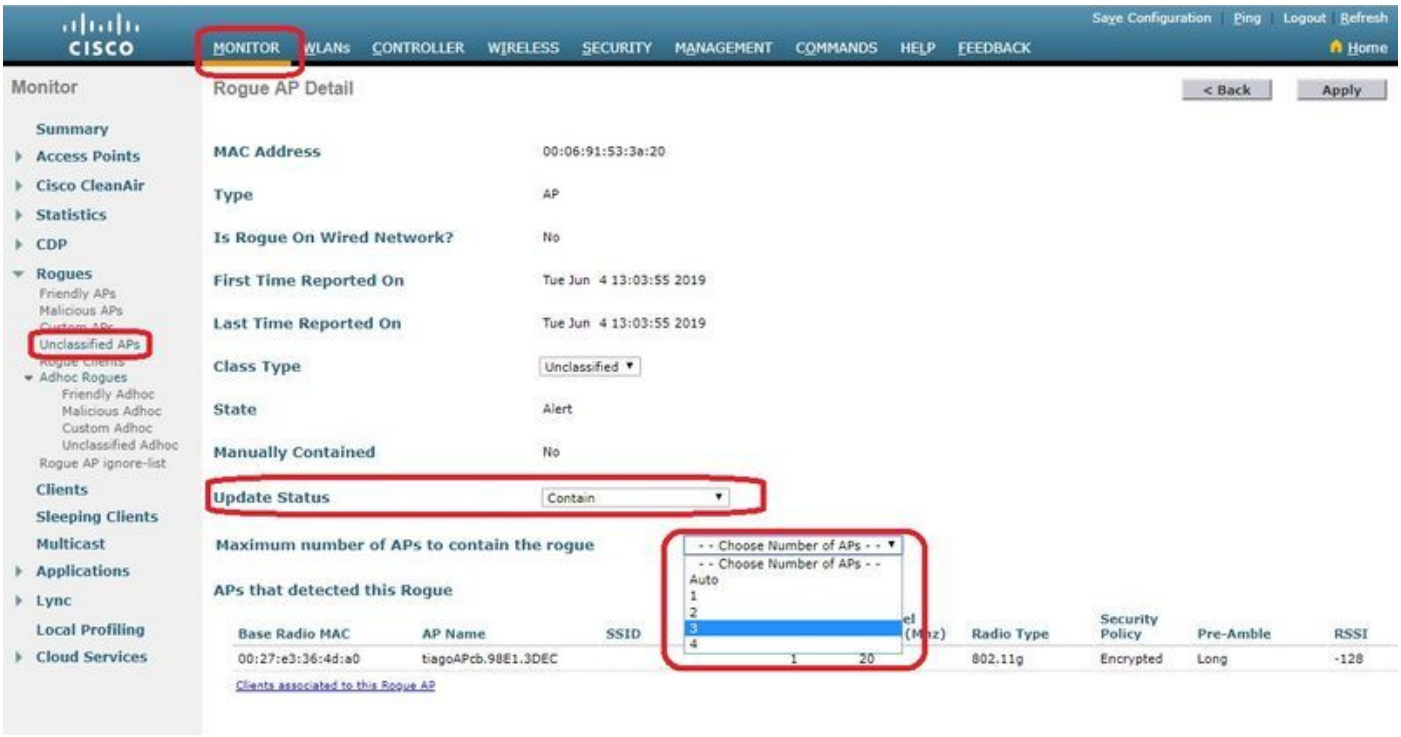
<#root>

```
(Cisco Controller) >

config rogue ap rldp retries ?


<count>         Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.
```

Configurar mitigación de acceso no deseado

Configuración de la contención manual

Para contener un AP no autorizado manualmente, navegue hasta Monitor > Rogues > Unclassified, como se muestra en la imagen.



Desde la CLI:

<#root>

```
(Cisco Controller) >
```

```
config rogue client
```

```
 ?

aaa             Configures to validate if a rogue client is a valid client which uses AAA/local databas
alert           Configure the rogue client to the alarm state.
contain         Start to contain a rogue client.
delete          Delete rogue Client
mse             Configures to validate if a rogue client is a valid client which uses MSE.

(Cisco Controller) >
```

```
config rogue client contain 11:22:33:44:55:66
```

```
 ?

<num of APs>    Enter the maximum number of Cisco APs to actively contain the rogue client [1-4].
```

Nota: Un punto de acceso no autorizado concreto puede estar contenido en 1-4 puntos de acceso. De forma predeterminada, el controlador utiliza un AP para contener un cliente. Si dos AP son capaces de detectar un rogue determinado, el AP con el RSSI más alto contiene el cliente independientemente del modo AP.

Contención automática

Para configurar la contención automática, vaya aSeguridad>Políticas de protección inalámbrica>Políticas no fiables>General y active todas las opciones aplicables para la red.

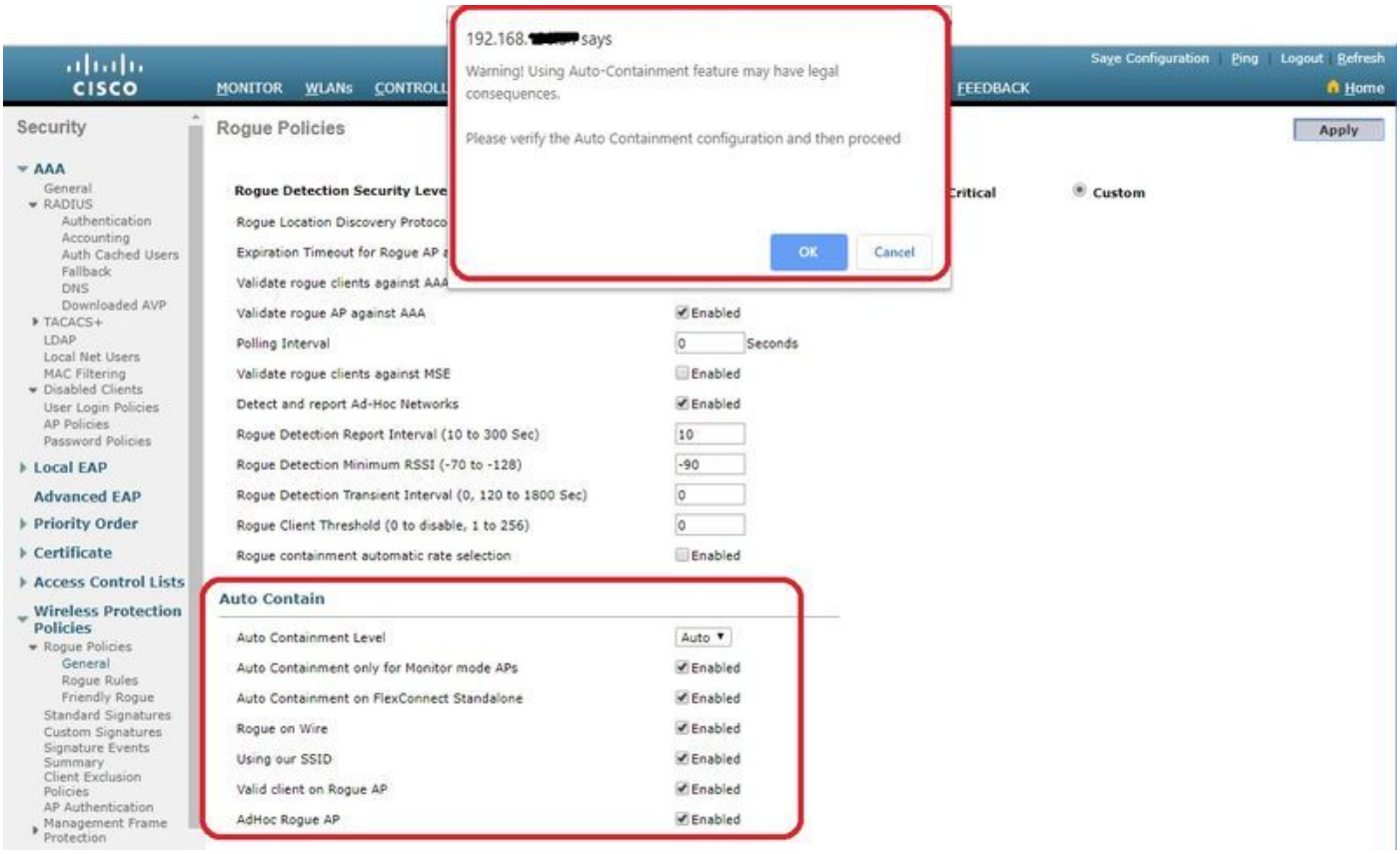
Si desea que el WLC de Cisco contenga automáticamente ciertos dispositivos rogue, marque esas casillas. De lo contrario, deje las casillas de verificación sin seleccionar, que es el valor predeterminado.

Advertencia: Cuando se habilita cualquiera de estos parámetros, aparece el mensaje:"El uso de esta función tiene consecuencias legales. ¿Desea continuar?" Las frecuencias de 2,4 y 5 GHz en las bandas Industrial, Scientific y Medical (ISM) están abiertas al público y se pueden utilizar sin licencia. Como tal, la contención de dispositivos en la red de otra parte podría tener consecuencias legales.

Estos son los parámetros de contención automática:

Parámetro	Descripción
Nivel de contención automático	Lista desplegable en la que puede elegir el nivel de contención automática no fiable de 1 a 4. Puede elegir hasta cuatro AP para la contención automática cuando un rogue se mueve a un estado contenido a través de cualquiera de las políticas de contención automática. También puede elegir Auto para la selección automática del número de AP utilizados para la contención automática. El WLC de Cisco elige el número requerido de AP basado en el RSSI para la contención eficaz. El valor RSSI asociado a cada nivel de contención es el siguiente: • 1 — 0 a -55 dBm • 2 — -75 a -55 dBm • 3 — -85 a -75 dBm • 4 — Menos de -85 dBm

Parámetro	Descripción
Contención automática sólo para puntos de acceso en modo Monitor	Marque la casilla que puede seleccionar para habilitar los AP del modo del monitor para la contención automática. El valor predeterminado es el estado deshabilitado.
Contención automática en FlexConnect independiente	Active la casilla de verificación que puede seleccionar para habilitar la contención automática en los puntos de acceso de FlexConnect en el modo independiente. El valor predeterminado es el estado deshabilitado. Cuando los AP de FlexConnect están en el modo autónomo, puede habilitar solamente las políticas de contención automática Use our SSID or AdHoc Rogue AP. La contención se detiene después de que el AP autónomo se conecta nuevamente al WLC de Cisco.
Rogue on Wire	Active la casilla de verificación que activa para contener automáticamente los sistemas no fiables detectados en la red con cables. El valor predeterminado es el estado deshabilitado.
Utilice nuestro SSID	Active la casilla de verificación que activa para contener automáticamente los dispositivos no fiables que anuncian el SSID de la red. Si deja este parámetro sin seleccionar, el WLC de Cisco solamente genera una alarma cuando se detecta tal rogue. El valor predeterminado es el estado deshabilitado.
Cliente válido en punto de acceso desconocido	Active esta casilla de verificación para que contenga automáticamente un punto de acceso no autorizado al que están asociados los clientes de confianza. Si deja este parámetro sin seleccionar, el WLC de Cisco solamente genera una alarma cuando se detecta tal rogue. El valor predeterminado es el estado deshabilitado.
Punto de acceso no autorizado ad hoc	Marque la casilla que usted habilita para contener automáticamente las redes ad-hoc que son detectadas por el WLC de Cisco. Si deja este parámetro sin seleccionar, el WLC de Cisco solamente genera una alarma cuando se detecta tal red. El valor predeterminado es el estado deshabilitado.



Haga clic en Aplicar para enviar los datos al WLC de Cisco, pero los datos no se conservan a través de un ciclo de energía; estos parámetros se almacenan temporalmente en la RAM volátil.

Desde la CLI:

<#root>

```
(Cisco Controller) >
```

config rogue adhoc ?

```
alert           Stop Auto-Containment, generate a trap upon detection of the
                    adhoc rogue.
auto-contain    Automatically contain adhoc rogue.
contain         Start to contain adhoc rogue.
disable         Disable detection and reporting of Ad-Hoc rogues.
enable          Enable detection and reporting of Ad-Hoc rogues.
external        Acknowledge presence of a adhoc rogue.

(Cisco Controller) >
```

config rogue adhoc auto-contain ?

```
(Cisco Controller) >
```

config rogue adhoc auto-contain

```
 Warning! Use of this feature has legal consequences
        Do you want to continue(y/n) :y
```

Con Prime Infrastructure

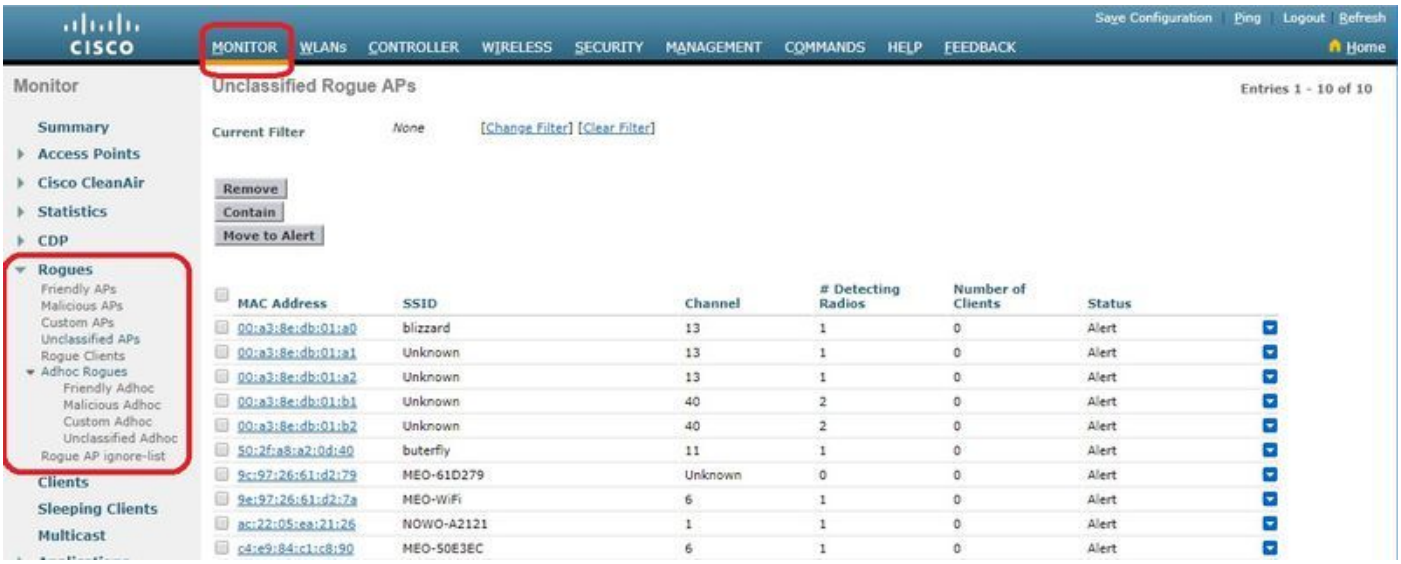
La infraestructura Cisco Prime se puede utilizar para configurar y supervisar uno o más controladores y puntos de acceso asociados. Cisco PI cuenta con herramientas para facilitar el control y la supervisión de sistemas de gran tamaño. Cuando utiliza Cisco PI en su solución inalámbrica de Cisco, los controladores determinan periódicamente el cliente, el punto de acceso no autorizado, el cliente de punto de acceso no autorizado, la ubicación de la etiqueta de ID de radiofrecuencia (RFID) y almacenan las ubicaciones en la base de datos de Cisco PI.

La infraestructura Cisco Prime admite la clasificación basada en reglas y utiliza las reglas de clasificación configuradas en el controlador. El controlador envía trampas a Cisco Prime Infrastructure después de estos eventos:

- Si un punto de acceso desconocido pasa al estado descriptivo por primera vez, el controlador envía una trampa a la infraestructura Cisco Prime sólo si el estado no autorizado es Alert (Alerta). No envía una trampa si el estado del argumento es Internal o External.
- Si se elimina una entrada arogueentry después de que venza el tiempo de espera, el controlador envía una trampa a los puntos de acceso roguede Cisco Prime Infrastructure que se categorizan como maliciosos (alerta, amenaza) o no clasificados (alerta). El controlador no removeverogueentries with theseroguestates: Contained, Conheld Pending, Internal y External.

Verificación

Para encontrar detalles de acceso no autorizado en un controlador en la interfaz gráfica, navegue hasta Monitor > Rogues, como se muestra en la imagen.



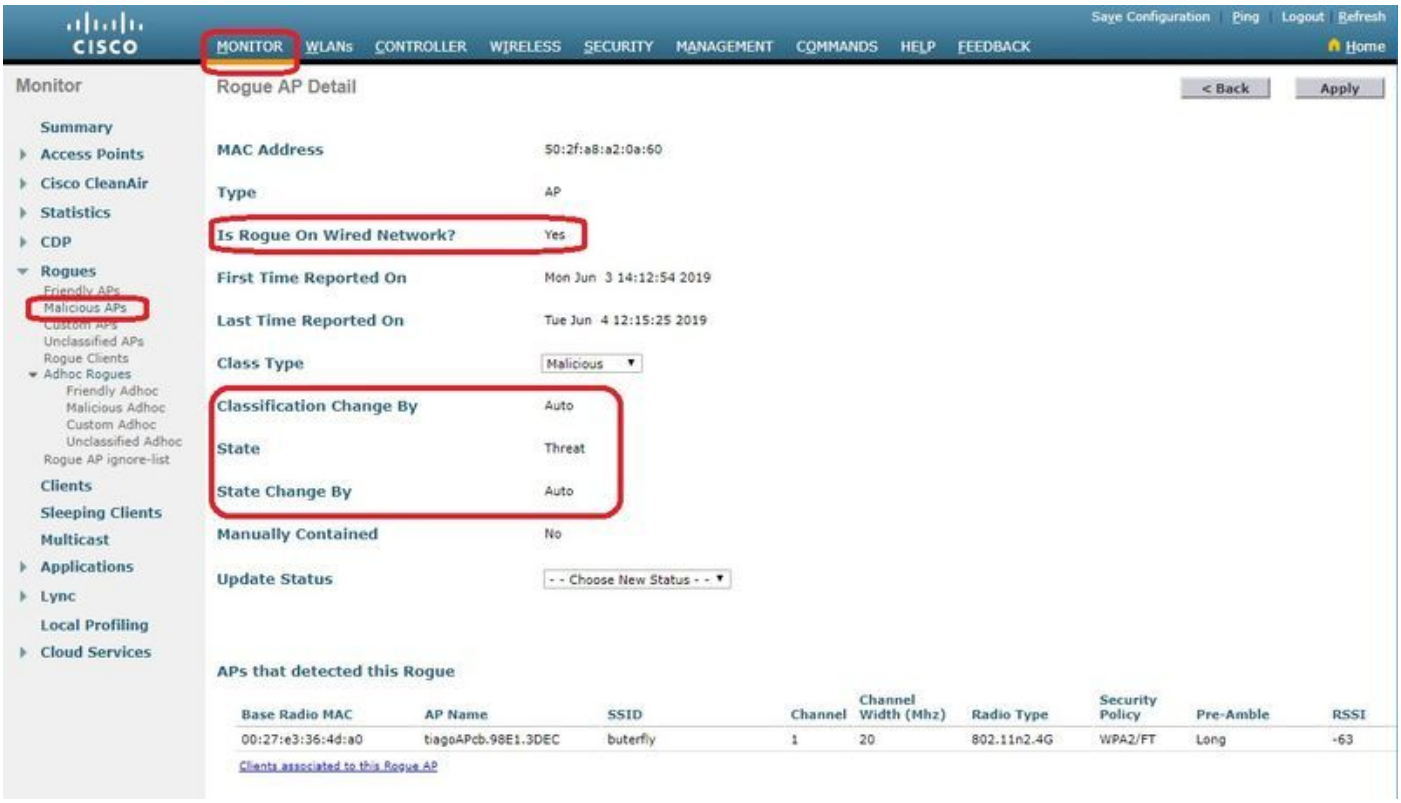
En esta página, hay disponible una clasificación diferente para los pícaros:

- AP amistosos - AP que son marcados como amistosos por el administrador.
- AP maliciosos - AP que se identifican como maliciosos vía RLDP o AP del detector Rogue.

- AP personalizados: AP clasificados como personalizados por reglas no fiables.
- AP no clasificados - De forma predeterminada, los AP no clasificados se muestran como una lista no clasificada en el controlador.
- Clientes Rogue - Clientes conectados a AP Rogue.
- No fiables ad hoc: clientes no fiables ad hoc.
- Lista de ignorados de puntos de acceso no autorizados: enumerados mediante PI.

Nota: Si el WLC y el AP autónomo es administrado por el mismo PI, el WLC enumera automáticamente este AP autónomo en la lista de ignorados del AP Rogue. No se requiere ninguna configuración adicional en el WLC para habilitar esta función.

Haga clic en una entrada no autorizada determinada para obtener los detalles de esa entrada no autorizada. A continuación se muestra un ejemplo de un acceso no autorizado detectado en una red con cables:



Desde la CLI:

<#root>

```
(Cisco Controller) >
```

show rogue ap summary

```
Rogue Detection Security Level................... custom
Rogue Pending Time............................... 180 secs
Rogue on wire Auto-Contain....................... Disabled
Rogue uses our SSID Auto-Contain................ Disabled
Valid client on rogue AP Auto-Contain............ Disabled
Rogue AP timeout................................. 1200
Rogue Detection Report Interval.................. 10
Rogue Detection Min Rssi......................... -90
Rogue Detection Transient Interval............... 0
Rogue Detection Client Num Threshold............. 0
Validate rogue AP against AAA.................... Enabled
Rogue AP AAA validation interval................. 0 secs
Total Rogues(AP+Ad-hoc) supported................ 600
Total Rogues classified.......................... 12

MAC Address       Class        State                #Det #Rogue  #Highest RSSI     #RSSI  #Channel
                                                    Aps  Clients  det-Ap
----------------- ------------ -------------------- ---- ------- ----------------- ------ -------------
00:a3:8e:db:01:a0 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -16    13
00:a3:8e:db:01:a1 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -16    13
00:a3:8e:db:01:a2 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -16    13
00:a3:8e:db:01:b0 Malicious    Threat               2    1       00:27:e3:36:4d:a0 -27    40
00:a3:8e:db:01:b1 Unclassified Alert                2    0       00:27:e3:36:4d:a0 -28    40
00:a3:8e:db:01:b2 Unclassified Alert                2    0       00:27:e3:36:4d:a0 -28    40
50:2f:a8:a2:0a:60 Malicious    Threat               1    2       00:27:e3:36:4d:a0 -66    1
50:2f:a8:a2:0d:40 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -65    11
9c:97:26:61:d2:79 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    6
ac:22:05:ea:21:26 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (1,5)
c4:e9:84:c1:c8:90 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (6,2)
d4:28:d5:da:e0:d4 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -85    13

(Cisco Controller) >
```

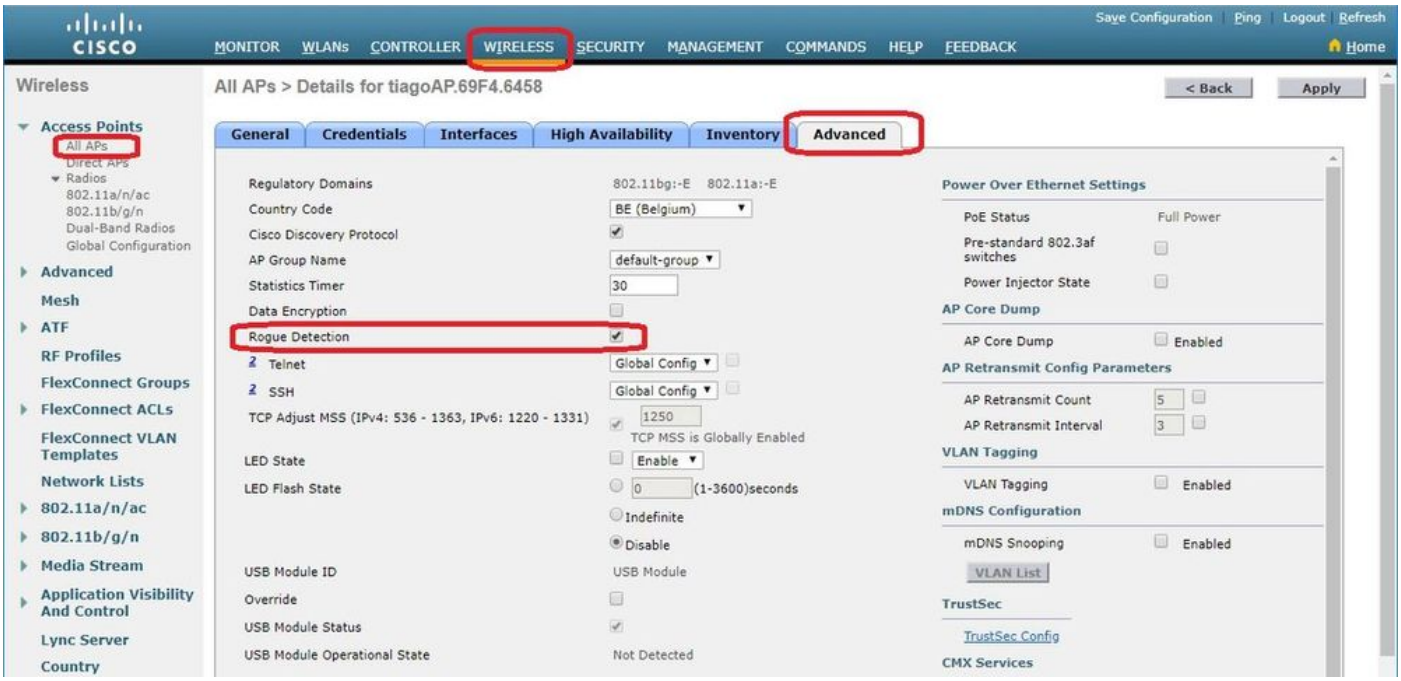
show rogue ap detailed 50:2f:a8:a2:0a:60

```
Rogue BSSID...................................... 50:2f:a8:a2:0a:60
Is Rogue on Wired Network........................ Yes
Classification................................... Malicious
Classification change by......................... Auto
Manual Contained................................. No
State............................................ Threat
State change by.................................. Auto
First Time Rogue was Reported.................... Tue Jun  4 13:06:55 2019
Last Time Rogue was Reported..................... Wed Jun  5 08:25:57 2019
Reported By
    AP 1
        MAC Address.............................. 00:27:e3:36:4d:a0
        Name..................................... tiagoAPcb.98E1.3DEC
        Radio Type............................... 802.11n2.4G
        SSID..................................... buterfly
        Channel.................................. 1
        RSSI..................................... -64 dBm
        SNR...................................... 29 dB
        Security Policy.......................... WPA2/FT
        ShortPreamble............................ Disabled
        Last reported by this AP................. Wed Jun  5 08:25:57 2019
```

Troubleshoot

Si No Se Detecta El Rogue

Verifique que la detección no autorizada esté habilitada en el AP. En la GUI:



En la CLI:

<#root>

```
(Cisco Controller) >show ap config general tiagoAPcb.98E1.3DEC

Cisco AP Identifier.............................. 13
Cisco AP Name.................................... tiagoAPcb.98E1.3DEC
[...]
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Disabled
AP SubMode ...................................... Not Configured

Rogue Detection ................................. Enabled

Remote AP Debug ................................. Disabled
Logging trap severity level ..................... informational
KPI not configured ..............................
Logging syslog facility ......................... kern
S/W  Version .................................... 8.8.120.0
Boot  Version ................................... 1.1.2.4
[...]
Power Type/Mode.................................. PoE/Full Power
Number Of Slots.................................. 3
AP Model......................................... AIR-AP3802I-I-K9
AP Image......................................... AP3G3-K9W8-M
Cisco IOS Version..................................... 8.8.120.0
```

```
Reset Button..................................... Enabled
AP Serial Number................................. FGL2114A4SU
[...]
```

La detección de acceso no autorizado se puede habilitar en un AP con este comando:

<#root>

```
(Cisco Controller) >
```

config rogue detection enable ?

```
all             Applies the configuration to all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

Un AP de modo local escanea solamente los canales de país/canales DCA y depende de la configuración. Si el rogue está en cualquier otro canal, el controlador no puede identificar al rogue si usted no tiene APs de modo de monitoreo en la red. Ejecute este comando para verificar:

<#root>

```
(Cisco Controller) >
```

show advanced 802.11a monitor

```
Default 802.11a AP monitoring
  802.11a Monitor Mode........................... enable
  802.11a Monitor Mode for Mesh AP Backhaul...... disable
```

802.11a Monitor Channels..... Country channels

```
  802.11a RRM Neighbor Discover Type............. Transparent
  802.11a RRM Neighbor RSSI Normalization........ Enabled
  802.11a AP Coverage Interval................... 90 seconds
  802.11a AP Load Interval....................... 60 seconds
  802.11a AP Monitor Measurement Interval........ 180 seconds
  802.11a AP Neighbor Timeout Factor............. 20
  802.11a AP Report Measurement Interval......... 180 seconds
```

- El AP no autorizado no se transmite por el SSID.
- Asegúrese de que la dirección MAC de AP no autorizada no esté agregada en la lista amistosa de no fiables o que esté permitida a través de PI.
- Las balizas del punto de acceso no autorizado no están disponibles para el punto de acceso que detectó sistemas no fiables. Esto se puede verificar mediante la captura de los paquetes con un sabueso cerca del detector de AP no autorizado.
- Un AP de modo local puede tardar hasta 9 minutos en detectar un rogue (3 ciclos 180x3).

- Los puntos de acceso de Cisco no pueden detectar puntos de acceso desconocidos en frecuencias como el canal de seguridad pública (4,9 GHz).
- Los AP de Cisco no pueden detectar a los pícaros que trabajan en FHSS (espectro de extensión del salto de frecuencia).

Depuraciones útiles

<#root>

```
(Cisco Controller) >
```

debug client

```
 (If rogue mac is known)
(Cisco Controller) >
```

debug client 50:2f:a8:a2:0a:60

```
(Cisco Controller) >*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Found Rogue AP: 50:2f:a8:a2

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417. Detecti
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or channel wi
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 rg changed rssi prev -64, new -55
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0  rssi -55,
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malici

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule classification :

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=but

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly
```

<#root>

```
(Cisco Controller) >
```

debug dot11 rogue enable

```
(Cisco Controller) >*emWeb: Jun 05 08:39:46.828:
Debugging session started on Jun 05 08:39:46.828  for WLC AIR-CT3504-K9   Version :8.8.120.0  SN :FCW224
*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for proces

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0, (Radio_upTi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid b0:72:bf:93:e0:d7 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 50:2f:a8:a2:0a:60 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:a1 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b0 src
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b2 src
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Found Rogue AP: 00:a3:8e:db:01:a1 on slot 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue SSID timestmap expired. last update at 0
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check:  knownApCount=0, totalNumOfRogueE
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check:  avgNumOfRogues[0]/10=4, rogueAla
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2  SYNC for Channel (new/old : 40/0) or channel w
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last update at 0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 rg changed rssi prev -28, new -28
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1  SYNC for Channel (new/old : 13/0) or channel w
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Updated AP report 00:27:e3:36:4d:a0  rssi -28,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Updated AP report 00:27:e3:36:4d:a0  rssi -16,
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class unclas

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP at 0xff

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue is Rule candidate for  : Class Change by

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Added Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclass

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Scheduled pending Time 184 and expiry time 1200
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 ssidLen = 0 min = 0 00:a3:8e:db:01:b2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 0 to 1 for rogue AP b0:72:bf:
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2  Rogue AP: 00:a3:8e:db:01:b2 autocontain = 2 Mo

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Checking Impersonation source 00:a3:8e:db:01:b2
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for  : Class Change by

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7  Send Rogue Info Notificaiton for AP report 00:
```

```
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg send new rssi -59
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue After Rule Classification : Class unclass

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0  rssi -59,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 ssidLen = 0 min = 0 00:a3:8e:db:01:a1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 This rogue does not use my ssid. Rogue ssid=



*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue before Rule Classification : Class unconf

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1  Rogue AP: 00:a3:8e:db:01:a1 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue state is pending or lrad, cannot apply ro

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule classification :

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source 00:a3:8e:db:01:a1
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Manual Contained Flag = 0, trustlevel = 1

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source b0:72:bf:93:e0:d7
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Found Rogue AP: 00:a3:8e:db:01:b0 on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg new Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0  SYNC for Channel (new/old : 40/0) or channel w
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 rg changed rssi prev -28, new -26
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or channel wi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Updated AP report 00:27:e3:36:4d:a0  rssi -26,
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 rg changed rssi prev -65, new -63
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0  rssi -63,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malici

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 ssidLen = 8 min = 8 00:a3:8e:db:01:b0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7
```

```
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 This rogue does not use my ssid. Rogue ssid=bli

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0  Rogue AP: 00:a3:8e:db:01:b0 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=but

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60  Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mo

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue Client ssid: blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 New AP report 00:27:e3:36:4d:a0  rssi -37, snr
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 rgc change from -38 RSSI -37
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 rgc change from -39 RSSI -39
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Updated AP report 00:27:e3:36:4d:a0 rssi -37, s
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Updated AP report 00:27:e3:36:4d:a0 rssi -39, s
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 APF processing Rogue Client: on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New AP report 00:27:e3:36:4d:a0  rssi -62, snr
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rgc change from -61 RSSI -62
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -62, s
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 1 to 2 for rogue AP b0:72:bf:
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Deleting Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Freed rogue client table for Rogue AP at 0xfff0

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg delete for Rogue AP: b0:72:bf:93:e0:d7
```

Registros de trampa esperados

Una vez que se ha detectado o eliminado un no fiable de la lista:

0	Miércoles 5 de junio de 2019 09:01:57 2019	Cliente no autorizado: b4:c0:f5:2b:4f:90 detectado por 1 APs Cliente no autorizado Bssid: a6:b1:e9:f0:e8:41, Estado: Alerta, Última detección de AP:00:27:e3:36:4d:a0 Gateway de cliente no autorizado mac 00:00:00:02:02:02.
1	Miércoles 5 de junio de 2019 09:00:39	Punto de acceso no autorizado: 9c:97:26:61:d2:79 eliminado de la radio base MAC: 00:27:e3:36:4d:a0 Interfaz no:0(802.11n(2,4 GHz))
2	Miércoles 5 de junio de 2019 08:53:39	Punto de acceso no autorizado: 7c:b7:33:c0:51:14 eliminado de la radio base MAC: 00:27:e3:36:4d:a0 Interfaz no:0(802.11n(2,4 GHz))
3	Miércoles 5 de junio de 2019 08:52:27	Cliente no autorizado: fc:3f:7c:5f:b1:1b es detectado por 1 APs Cliente no autorizado Bssid: 50:2f:a8:a2:0a:60, Estado: Alerta, Última detección de AP:00:27:e3:36:4d:a0 Gateway de cliente no autorizado mac 00:26:44:73:c5:1d.
4	Miércoles 5 de junio de 2019 08:52:17	Punto de acceso no autorizado: d4:28:d5:da:e0:d4 eliminado de la radio base MAC: 00:27:e3:36:4d:a0 Interfaz no:0(802.11n(2,4 GHz))

Recomendaciones

1. Configure el análisis de canales para todos los canales si sospecha que hay potenciales sistemas no fiables en la red.
2. El número y la ubicación de los puntos de acceso de los detectores de acceso no autorizados pueden variar de uno por planta a uno por edificio y depende de la disposición de la red por cable. Es recomendable tener al menos un AP de detector de acceso no autorizado en cada planta de un edificio. Debido a que un AP de detector de acceso no autorizado requiere un enlace troncal para todos los dominios de difusión de red de capa 2 que se van a supervisar, la ubicación depende del diseño lógico de la red.

Si el no fiable no está clasificado

Verifique que las reglas no autorizadas estén configuradas correctamente.

Depuraciones útiles

<#root>

```
(Cisco Controller) >
```

debug dot11 rogue rule enable

```
(Cisco Controller) >*emWeb: Jun 05 09:12:27.095:
Debugging session started on Jun 05 09:12:27.095 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW2245M0
```

```
(Cisco Controller) >
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr

*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr

*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40
```

Rogue Classification:malicious, RuleName:TestRule, Rogue State:Containment Pending

```
*apfRogueTask_3: Jun 05 09:13:27.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr

*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious, RuleName:TestRu

*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr
```

Recomendaciones

Si tiene entradas no autorizadas conocidas, agréguelas a la lista descriptiva o habilite la validación con AAA y asegúrese de que las entradas de cliente conocidas se encuentran en la base de datos de autenticación, autorización y contabilidad (AAA).

RLDP No Encuentra Rogues

- Si el no fiable está en el canal DFS, RLDP no funciona.
- RLDP funciona sólo si la WLAN no autorizada está abierta y DHCP está disponible.
- Si el AP de modo local sirve al cliente en el canal DFS, no participa en el proceso RLDP.
- RLDP no es compatible con AP modelo 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 y 3800 Series AP.

Depuraciones útiles

<#root>

```
(Cisco Controller) >
```

debug dot11 rldp enable

```
!--- RLDP not available when AP used to contain only has invalid channel for the AP country code

*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Rogue detected slot :0 Rogue contains SlotId :2
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61
```

Invalid channel 1 for the country IL for AP 00:27:e3:36:4d:a0

```
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Waiting for ARLDP request

!--- ROGUE detected on DFS channel

*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Received request to detect Rogue
*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Rogue detected slot :1 Rogue contains SlotId :1
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e
```

Our AP 00:27:e3:36:4d:a0 detected this rogue on a DFS Channel 100

```
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Waiting for ARLDP request

!--- RLDP is not supported on AP model 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series

*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Received request to detect Rogue
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a
```

Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP1852I-E-K9

```
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: Waiting for ARLDP request

!--- Association TO ROGUE AP

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP
*apfRLDP: Jun 05 15:02:49.602: Rogue detected slot :0 Rogue contains SlotId :0
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61
```

Monitor Mode AP found b4:de:31:a4:e0:30 with RSSI -61

```
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 found closest monitor AP b4:de:31:a4:e0:30 slot = 0, c

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Found RAD: 0xffd682b5b8, slotId = 0, Type=1

*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 AP b4:de:31:a4:e0:30 Client b4:de:31:a4:e0:31 Slot = 0
*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 WARNING!!!!! mscb already exists!

*apfRLDP: Jun 05 15:02:50.102: b4:de:31:a4:e0:31 In rldpSendAddMobile:724 setting Central switched to T
*apfRLDP: Jun 05 15:02:50.302: 50:2f:a8:a2:0a:61
```

rldp started association, attempt 1

```
*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP St

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 rldp started association, attempt 2
*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP St

*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 rldp started association, attempt 3
*apfOpenDtlSocket: Jun 05 15:03:00.608: apfRoguePreamble = 0 mobile b4:de:31:a4:e0:31.
*apfOpenDtlSocket: Jun 05 15:03:00.808:
```

50:2f:a8:a2:0a:61 RLDP state RLDP_ASSOC_DONE

(3).

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Successfully associated with rogue: 50:2F:A8:A2:0A:61

!--- Attempt to get ip from ROGUE

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Starting dhcp

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 htype: Ethernet

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hlen: 6

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hops: 1

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 secs: 0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 flags: 0x0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 options:

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:00.870: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:00.870: [0000] 02 40

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 host name: RLDP

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 htype: Ethernet

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 hlen: 6

```
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31         hops: 1

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31          xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31         secs: 0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31        flags: 0x0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31        hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31          my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31     gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31         DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:10.878: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:10.878:      [0000] 02 40

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31           host name: RLDP

*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        htype: Ethernet

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         hlen: 6

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         hops: 1

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         secs: 0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        flags: 0x0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31     gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:20.885: DHCP option: 39/57.2: (2)
```

```
*apfRLDP: Jun 05 15:03:20.885:      [0000] 02 40

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31           host name: RLDP

*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61

!--- RLDP DHCP fails as there is no DHCP server providing IP address

*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCP FAILED state for rogue  50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 DHCP failed
*apfRLDP: Jun 05 15:03:20.885: Waiting for ARLDP request
```

Recomendaciones

1. Inicie RLDP manualmente en entradas sospechosas no autorizadas.
2. Programe RLDP periódicamente.
3. RLDP se puede implementar en los AP de modo local o de monitoreo. Para la mayoría de las implementaciones escalables, y para eliminar cualquier impacto en el servicio al cliente, RLDP se debe implementar en los AP del modo de monitor cuando sea posible. Sin embargo, esta recomendación requiere que se implemente una superposición de AP en modo monitor con una proporción típica como 1 AP en modo monitor por cada 5 AP en modo local. Los AP en el modo de monitor wIPS adaptable también se pueden aprovechar para esta tarea.

AP de detector de acceso no autorizado

La entrada de acceso no autorizado en un detector de acceso no autorizado se puede ver con este comando en la consola AP. En el caso de los sistemas no fiables conectados por cable, el indicador se desplaza para establecer el estado.

<#root>

```
tiagoAP.6d09.eff0#

show capwap rm rogue detecto

r
 LWAPP Rogue Detector Mode
  Current Rogue Table:
  Rogue hindex = 0: MAC 502f.a8a2.0a61,

flag = 0

, unusedCount = 1
  Rogue hindex = 0: MAC 502f.a8a2.0a60,

flag = 0

, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d41,

flag = 0
```

```
, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d40,
```

flag = 0

```
, unusedCount = 1

!--- once rogue is detected on wire, the flag is set to 1
```

Comandos de depuración útiles en una consola AP

<#root>

```
Rogue_Detector#
```

debug capwap rm rogue detector

```
*Jun 05 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 05 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 05 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

Contención de acceso no deseado

Depuraciones esperadas

<#root>

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Updated AP report b4:de:31:a4:e0:30 rssi -33, s
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Looking for Rogue 00:a3:8e:db:01:b0 in known AP
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue AP 00:a3:8e:db:01:b0 is not found either
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6 ContainmentLe

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected by AP: b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RadioType: 2 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue before Rule Classification :

Class malicious, Change by Auto State Contained Change by Auto



*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue doesnt qualify for rule classification :

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 6

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0

Rogue AP: 00:a3:8e:db:01:b0 autocontain = 1 Mode = 6



*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 apfRogueMode : 6 apfRogueContainmentLevel : 4 l

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 1 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Skipping xor radio for 1 band and cont slotid 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 0 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 2 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected on detected slot 0 contains slot
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 1 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -28
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -31
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC b4:de:31:a4:e0:30 RSSI = -33
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -28 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -31 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC b4:de:31:a4:e0:30 RSSI = -33 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0

 Contains rogue with 3 container AP(s).Requested containment level : 4


*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Checking Impersonation source 00:a3:8e:db:01:b0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im
```

Recomendaciones

1. El AP de modo local/Flex-Connect puede contener 3 dispositivos a la vez por radio, y el AP de modo monitor puede contener 6 dispositivos por radio. Como resultado, asegúrese de que el AP no contenga ya el número máximo de dispositivos permitidos. En este escenario, el cliente está en un estado de contención pendiente.

2. Verifique las reglas de contención automática.

Conclusión

La detección y la contención de acceso no autorizado en la solución de controlador centralizado de Cisco es el método más eficaz y menos intrusivo del sector. La flexibilidad que se proporciona al administrador de la red permite un ajuste más personalizado que puede adaptarse a cualquier requisito de la red.

Información Relacionada

- Guía de configuración del controlador inalámbrico de Cisco, versión 8.8 - Rogue Management
- Prácticas recomendadas de configuración del controlador LAN inalámbrico (WLC) de Cisco
- Guía de implementación de WLC 3504 Versión 8.5
- Guía de implementación del controlador LAN inalámbrico Cisco 5520
- Notas de la versión de Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless versión 8.8.120.0

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).