Identificación de clientes desconocidos en una red inalámbrica empresarial de Cisco

Objetivo

El objetivo de este artículo es mostrarle cómo identificar puntos de acceso (AP) desconocidos y clientes inalámbricos desconocidos en una red de malla o tradicional Cisco Business Wireless (CBW).

Dispositivos aplicables | Versión de firmware

- 140AC (hoja de datos) | 10.0.1.0 (Descargar la última versión)
- 141ACM (hoja de datos) | 10.0.1.0 (Descargar la última versión) - los extensores sólo se utilizan en una red de malla
- 142ACM (hoja de datos) | 10.0.1.0 (Descargar la última versión) - los extensores sólo se utilizan en una red de malla
- 143ACM (hoja de datos) | 10.0.1.0 (Descargar la última versión) - los extensores sólo se utilizan en una red de malla
- 145AC (hoja de datos) | 10.0.1.0 (Descargar la última versión)
- 240AC (hoja de datos) | 10.0.1.0 (Descargar la última versión)
- 150AX (hoja de datos) | 10.3.2.0 (Descargar la última versión)
- 151AXM (hoja de datos) | 10.3.2.0 (Descargar la última versión)

Los dispositivos de la serie CBW 15x no son compatibles con los dispositivos de la serie CBW 14x/240 y no se admite la coexistencia en la misma LAN.

Introducción

Los puntos de acceso (AP) CBW se basan en 802.11 a/b/g/n/ac (onda 2), con antenas internas. Se pueden utilizar como dispositivos independientes tradicionales o como parte de una red de malla.

En un mundo perfecto, todo el mundo sería respetuoso y honesto al utilizar la red inalámbrica. Desafortunadamente, no vivimos en un mundo perfecto. Como administrador, su trabajo consiste en ser consciente de cualquier problema potencial.

Los AP rogue son AP que se han instalado en una red sin su permiso. Los clientes no autorizados son cualquier otro dispositivo detectado que no pertenezca a su empresa.

Estas conexiones pueden ser totalmente inocentes, pero siempre existe el riesgo de que estos piratas intenten atacar su red o robar información confidencial. Para mantenerse al tanto de esto, puede ver los AP rogue y los clientes rogue. Una vez detectados, estos rogues no pueden ser bloqueados a través del AP, pero le da información para investigar más a fondo.

Los AP CBW solo detectarán los canales no autorizados en los canales que esté utilizando actualmente o los canales que se superpongan.

Ver puntos de acceso desconocidos

Esta sección alterna resalta las sugerencias para principiantes.

Inicio de sesión

Inicie sesión en la interfaz de usuario Web del punto de acceso principal. Para ello, abra un navegador web e introduzca https://ciscobusiness.cisco. Es posible que reciba una advertencia antes de continuar. Introduzca sus credenciales.También puede acceder al AP principal introduciendo https://[dirección IP] (del AP principal) en un navegador web.

Sugerencias de herramientas

Si tiene preguntas sobre un campo de la interfaz de usuario, busque una sugerencia de herramienta similar a la siguiente:

¿Tiene problemas para localizar el icono Expandir menú principal?

Desplácese hasta el menú situado en el lado izquierdo de la pantalla. Si no ve el botón de menú, haga clic en este icono para abrir el menú de la barra lateral.

Aplicación empresarial de Cisco

Estos dispositivos tienen aplicaciones complementarias que comparten algunas funciones de gestión con la interfaz de usuario web. No todas las funciones de la interfaz de usuario Web estarán disponibles en la aplicación.

Descargar la aplicación para iOS Descargar aplicación para Android

Preguntas Frecuentes

Si aún tiene preguntas sin responder, puede consultar nuestro documento de preguntas frecuentes. Preguntas frecuentes

Paso 1

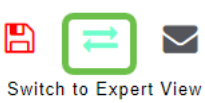
Inicie sesión en la interfaz de usuario Web del punto de acceso principal. Para ello, abra un navegador web y escriba *https://ciscobusiness.cisco*. Es posible que reciba una advertencia antes de continuar. Introduzca sus credenciales.

También puede acceder al AP primario ingresando *https://<ipaddress>* (del AP primario) en un navegador web.

Si no está familiarizado con los términos utilizados, consulte Cisco Business: Glossary of New Terms (Glosario de términos nuevos de Cisco Business:).

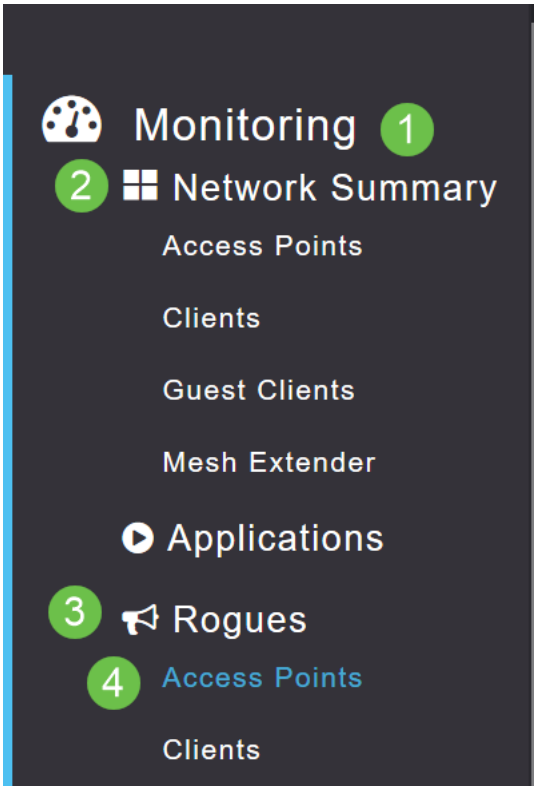
Paso 2

Para realizar estas configuraciones, debe estar en la *vista Experto*. Haga clic en el **icono de flecha** en el menú superior derecho de la interfaz de usuario web para cambiar a la *vista Experto*.



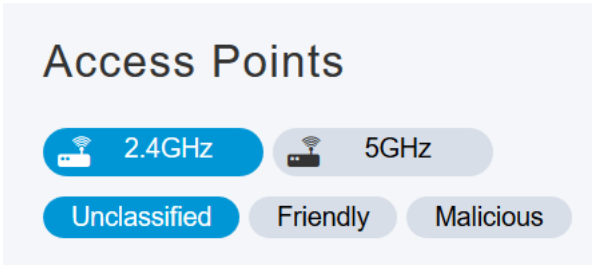
Paso 3

Vaya a **Monitoring > Network Summary > Rogues > Access Points.**



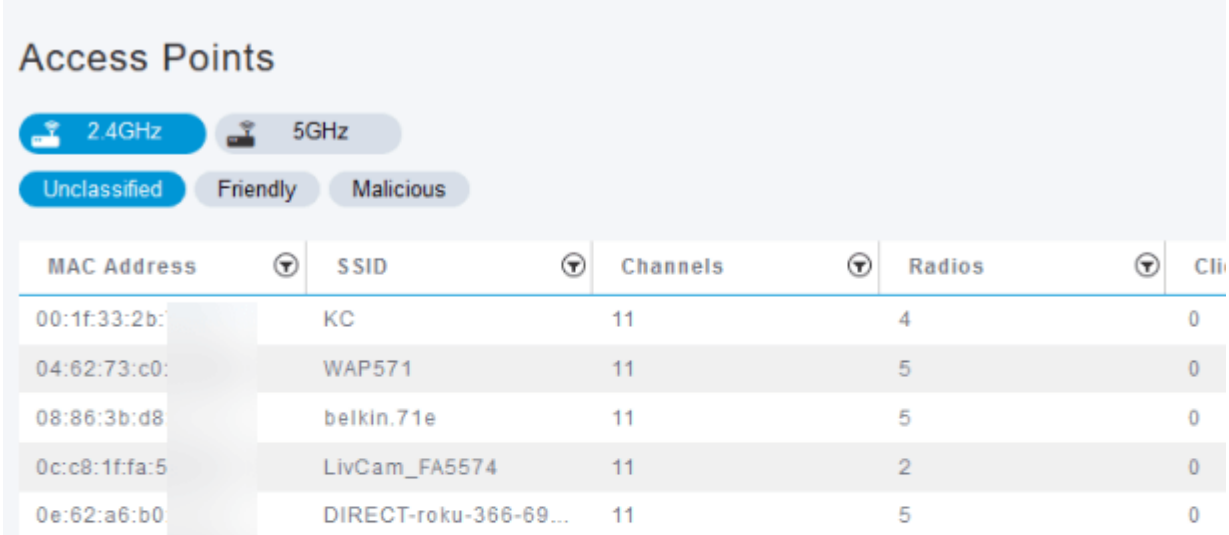
Paso 4

Una vez que se abra esta página, haga clic en la ficha para ver 2,4 GHz o 5 GHz. De forma predeterminada, todos los AP no autorizados se etiquetan como Sin clasificar. El AP no cambia las etiquetas para los AP rogue, eso es algo que haría manualmente.



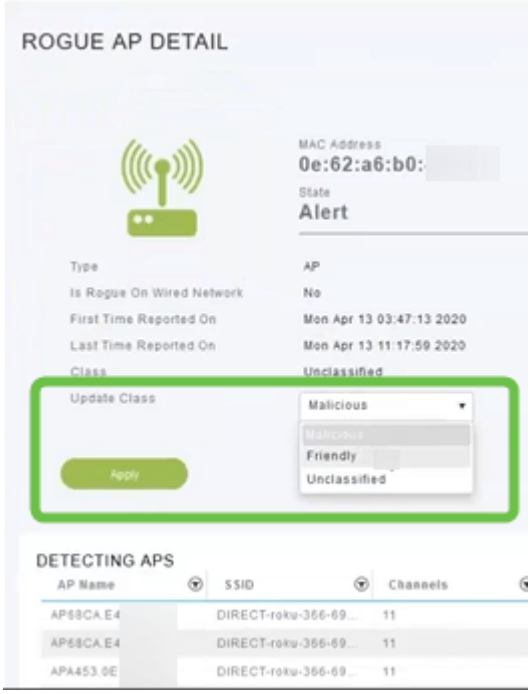
Paso 5

Los AP rogue se enumeran, puede hacer clic en cualquiera de ellos para investigar más.



Paso 6 (opcional)

Si desea clasificar cualquiera de los AP como *Amigable* o *Malicioso*, puede seleccionar cualquiera de las opciones del menú desplegable bajo *Actualizar Clase*. Puede que desee hacer esto para que cuando vea los puntos de acceso no clasificados en el futuro, no tenga que ordenar por una lista completa. Asegúrese de hacer clic en **Aplicar** cuando haya terminado.



Paso 7 (opcional)

Si desea etiquetar un AP como *Interno* (en la red) o *Externo* (posiblemente una compañía vecina), puede hacerlo en la sección *Estado de actualización*. Haga clic en **Aplicar** cuando haya terminado.

Ver clientes desconocidos

Paso 1

Inicie sesión en la interfaz de usuario web del punto de acceso principal. Para ello, abra un navegador web y escriba *https://ciscobusiness.cisco*. Es posible que reciba una advertencia antes de continuar. Introduzca sus credenciales.

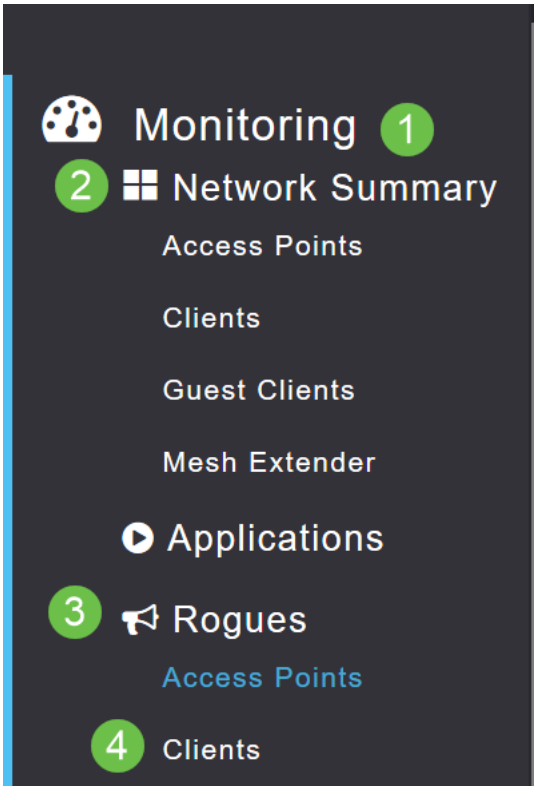
También puede acceder al AP primario ingresando *https://<ipaddress>* (del AP primario) en un navegador web. Para algunas acciones, puede utilizar la aplicación Cisco Business Mobile.

Paso 2

Para realizar estas configuraciones, debe estar en la *vista Experto*. Haga clic en el **icono de flecha** en el menú superior derecho de la interfaz de usuario web para cambiar a la *vista Experto*. Para obtener más información sobre la configuración de un servidor RADIUS, consulte Radius

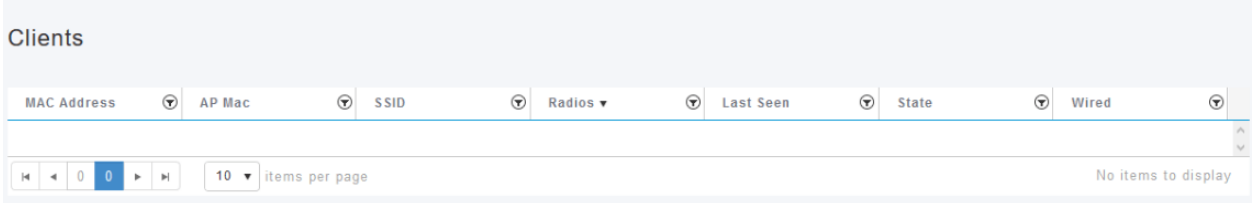
Paso 3

Vaya a **Monitoring > Network Summary > Rogues > Clients.**



Paso 4

Si hay algún cliente no autorizado, aparecerá en la lista. En este ejemplo, no se ha detectado ningún cliente no autorizado.



Conclusión

Ahora tiene la posibilidad de ver los sistemas no fiables en la red. Si ve muchos sistemas no fiables en un canal que está utilizando, puede cambiar el canal. Hay consideraciones que debe tener en cuenta, por lo que consulte el artículo sobre el cambio de canal de RF (enlace cuando

esté disponible).

Preguntas Frecuentes Radius Actualización del firmware RLAN Perfiles de aplicación Perfiles de clientes Herramientas de AP principal Umbrella Usuarios de WLAN Registro Modelado de tráfico Pícaros Interferentes Administración de la Configuración Modo de malla de configuración de puerto Bienvenido a CBW Mesh Networking Red de invitados mediante autenticación de correo electrónico y cuentas RADIUS Resolución de problemas Uso de un router Draytek con CBW

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).