Guía de diseño CX - Tecnología inalámbrica para redes públicas de gran tamaño

Contenido

Introducción

Este documento describe las pautas de diseño y configuración para redes Wi-Fi públicas de gran tamaño.

Guía de diseño de CX

Las guías de diseño de CX están escritas por especialistas de Cisco Technical Assistance Center (TAC) y Cisco Professional Services (PS) y revisadas por expertos de Cisco. Las guías se basan en las prácticas líderes de Cisco, así como en el conocimiento y la experiencia obtenidos de innumerables implementaciones de clientes a lo largo de muchos años. Las redes diseñadas y configuradas de acuerdo con las recomendaciones de este documento ayudan a evitar los obstáculos más comunes y a mejorar el funcionamiento de la red.

Ámbito de aplicación y definiciones

Este documento proporciona directrices de diseño y configuración para redes inalámbricas públicas de gran tamaño.

Definición: Grandes redes públicas. Implementaciones inalámbricas, a menudo de alta densidad, que proporcionan conectividad de red para miles de dispositivos cliente desconocidos o no gestionados.

Este documento a menudo asume que la red de destino está proporcionando servicios a eventos grandes y/o temporales. También se adapta a las redes estáticas permanentes para los lugares que reciben a muchos invitados. Por ejemplo, un centro comercial o un aeropuerto tienen similitudes con la red Wi-Fi de un estadio o de un recinto de conciertos, en el sentido de que no hay control sobre los usuarios finales, y estos existen en la red normalmente solo durante un par de horas, o como máximo durante el día.

La cobertura inalámbrica para grandes eventos o lugares tiene su propio conjunto de requisitos, que tiende a ser diferente de las redes empresariales, de fabricación o incluso de las grandes redes educativas. Las grandes redes públicas pueden tener miles de personas, concentradas en uno o pocos edificios. Pueden tener itinerancia de cliente muy frecuente, constantemente o durante picos, además de que la red debe ser lo más compatible posible con cualquier cosa en términos de dispositivos de cliente inalámbricos, sin control sobre la configuración o la seguridad de los dispositivos del cliente.

Esta guía presenta conceptos generales de RF para alta densidad, así como detalles de implementación. Muchos de los conceptos de radio de esta guía se aplican a todas las redes de alta densidad, incluida Cisco Meraki. Sin embargo, los detalles de implementación y las configuraciones se centran en Catalyst Wireless mediante el controlador inalámbrico Catalyst 9800, ya que esta es la solución más común implementada actualmente para grandes redes públicas.

Este documento utiliza los términos Wireless Controller y Wireless LAN Controller (WLC) indistintamente.

Grandes redes públicas

Las grandes redes públicas y de eventos son únicas en muchos aspectos. Este documento explora y proporciona orientación sobre estas áreas clave.

- Las redes públicas de gran tamaño son intensas; hay miles de dispositivos en un espacio de radiofrecuencia (RF) reducido y una itinerancia significativa a medida que la gente camina, algunos eventos y lugares pueden ser más estáticos con picos de ancho de banda en momentos muy específicos. La infraestructura debe gestionar todos estos cambios de estado de la forma más adecuada posible para los clientes que entran y se desplazan por el área.
- La prioridad principal es la facilidad de incorporación. Un cliente asociado es un cliente feliz. Esto significa que desea que la asociación del cliente a la red sea lo más rápida posible. Un cliente que no está conectado a Wi-Fi busca puntos de acceso disponibles que generen energía de RF no deseada, lo que se traduce en congestión adicional y pérdida de capacidad en el aire.
- La implementación de RF debe diseñarse con el mayor cuidado posible. Un diseño de RF adecuado usando antenas direccionales es imprescindible si se requiere una densidad muy alta, o si el lugar tiene grandes espacios abiertos y/o techos altos.
- Otro factor clave en el diseño es la compatibilidad. Algunas funciones son estándar en la especificación 802.11, mientras que otras son exclusivas, y ninguna de ellas plantea ningún problema a los clientes. Sin embargo, la realidad es diferente y hay muchos controladores

de cliente mal programados que se comportan mal cuando ven balizas complicadas o características/configuraciones que no entienden.
- La resolución de problemas es complicada debido a las restricciones de tiempo y escalabilidad. Si algo no funciona con un cliente específico, no podrá trabajar con ese usuario final para entender el problema. Los usuarios pueden ser difíciles de encontrar, pero también pueden no ser cooperativos debido a la naturaleza transitoria de su visita en el lugar.
- La seguridad es un factor importante. Hay menos control debido a la gran cantidad de visitantes invitados y a una superficie de ataque mucho mayor.

Referencias externas

Nombre del documento	Fuente	Ubicación
Prácticas recomendadas de configuración de Cisco Catalyst serie 9800	Cisco	Enlace
Resolución de problemas de CPU del controlador LAN inalámbrico	Cisco	Enlace
Validar el rendimiento de Wi-Fi: guía de pruebas y supervisión	Cisco	Enlace
Guía de implementación del punto de acceso Cisco Catalyst CW9166D1	Cisco	Enlace
Guía de implementación de la antena de estadio Catalyst 9104 (C-ANT9104)	Cisco	Enlace
Supervisar los KPI de Catalyst 9800 (indicadores de rendimiento clave)	Cisco	Enlace
Solución de problemas de conectividad del cliente Catalyst 9800 Flujo	Cisco	Enlace
Guía de configuración del software del controlador inalámbrico Cisco Catalyst serie 9800 (17.12)	Cisco	Enlace
Wi-Fi 6E: el siguiente gran capítulo del informe técnico sobre Wi-Fi	Cisco	Enlace

Descargo

Este documento ofrece recomendaciones basadas en ciertos escenarios, suposiciones y conocimientos adquiridos de numerosas implementaciones. Sin embargo, usted o el lector son responsables de determinar el diseño de la red, el negocio, el cumplimiento de las normas, la seguridad, la privacidad y otros requisitos, incluyendo si seguir las directrices o recomendaciones que se proporcionan en esta guía.

Diseño de la red

Consideraciones de RF

Tipos de lugares

Esta guía se centra en las redes de invitados de gran tamaño, generalmente abiertas al público, y con un control limitado sobre los usuarios finales y los tipos de dispositivos cliente. Estos tipos de redes se pueden implementar en diversas ubicaciones y pueden ser temporales o permanentes. El principal caso práctico suele ser proporcionar acceso a Internet a los visitantes, aunque rara vez es el único caso práctico.

Ubicaciones típicas:

- Estadios y estadios
- Lugares de conferencias
- Auditorios grandes

Desde el punto de vista de la radiofrecuencia, cada uno de estos tipos de ubicación tiene su propio conjunto de matices. La mayoría de estos ejemplos suelen ser instalaciones permanentes, aparte de los lugares de celebración de conferencias, ya que pueden ser permanentes o estar instalados para una feria comercial específica de forma temporal.

Otras ubicaciones:

- Crucero
- Aeropuerto
- Centro comercial/centro comercial

Los aeropuertos y los cruceros también son ejemplos de implementaciones que encajan en la categoría de grandes redes públicas; sin embargo, estas tienen consideraciones adicionales específicas para cada caso y a menudo hacen uso de AP omnidireccionales internos.

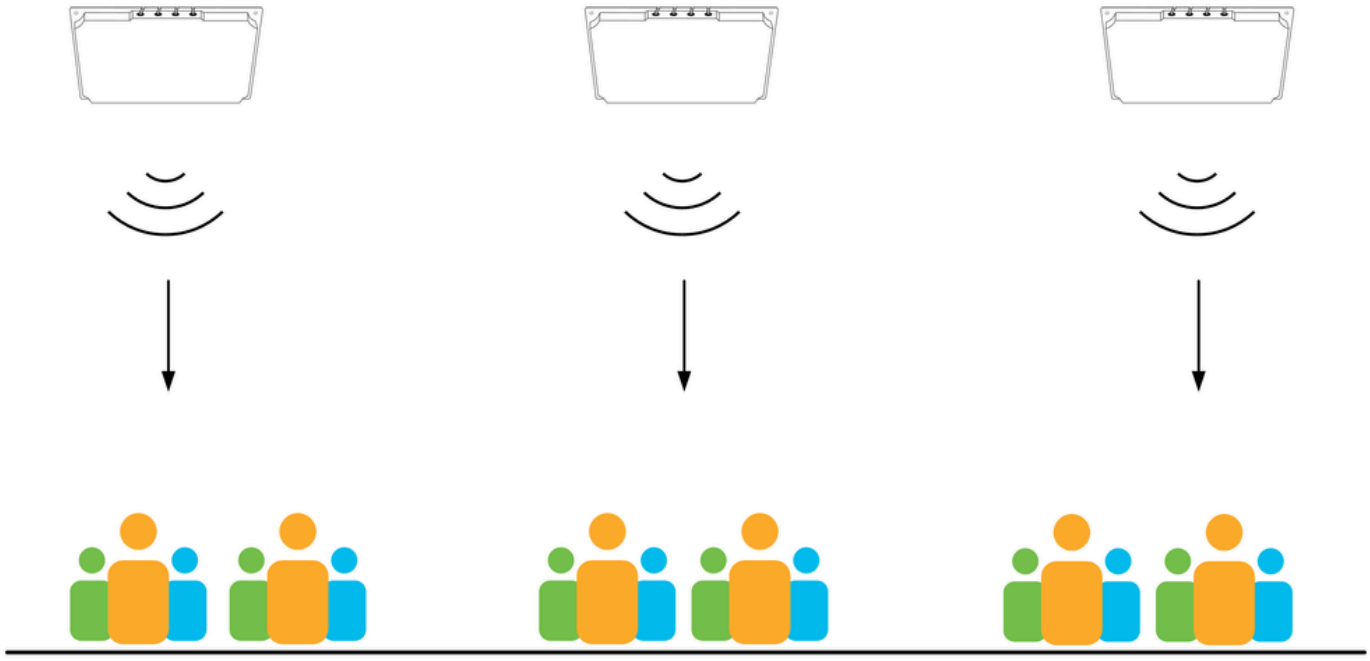
Estrategias de cobertura

Las estrategias de cobertura dependen en gran medida del tipo de emplazamiento, las antenas utilizadas y las ubicaciones de montaje de antena disponibles.

Sobrecarga

Siempre que sea posible, se prefiere la cobertura de gastos generales.

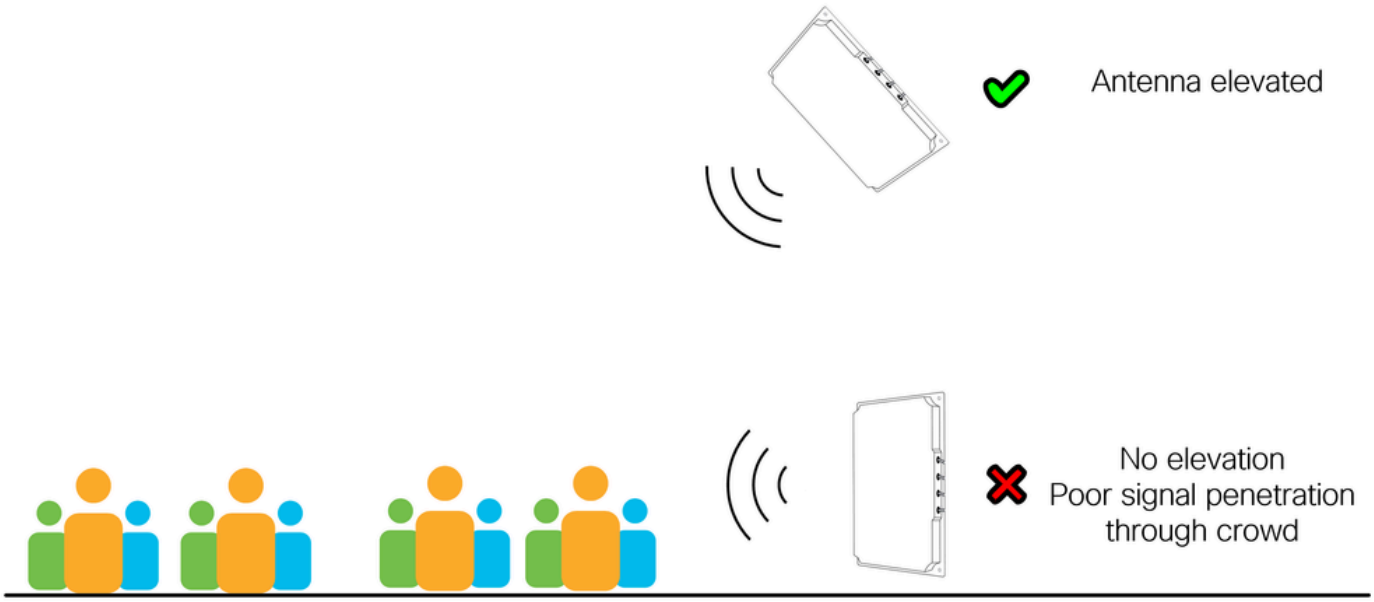
Las soluciones de sobrecarga tienen la clara ventaja de que todos los dispositivos cliente suelen tener una línea de visión directa con la sobrecarga de la antena, incluso en escenarios saturados. Las soluciones de sobrecarga que utilizan antenas direccionales proporcionan un área de cobertura más controlada y bien definida, lo que las hace menos complicadas desde el punto de vista de la sintonización de radio, a la vez que proporcionan un equilibrio de carga superior y características de itinerancia del cliente. Consulte la sección Power Balance para obtener más información.



AP sobre los clientes

Lado

Las antenas direccionales montadas en los laterales son una opción popular y funcionan bien en una variedad de escenarios, particularmente cuando el montaje en la parte superior no es posible debido a la altura o restricciones de montaje. Al utilizar el montaje lateral, es importante comprender el tipo de área que cubre la antena. Por ejemplo, ¿se trata de una zona exterior abierta o de una zona interior densa? Si el área de cobertura es un área de alta densidad con muchas personas, la antena debe elevarse tanto como sea posible, ya que la propagación de la señal a través de una multitud humana siempre es pobre. Recuerde que la mayoría de los dispositivos móviles se utilizan en la parte inferior de la cintura, no por encima de la cabeza del usuario. La altura de la antena es menos significativa si el área de cobertura es un área de menor densidad.



La elevación de la antena siempre es mejor

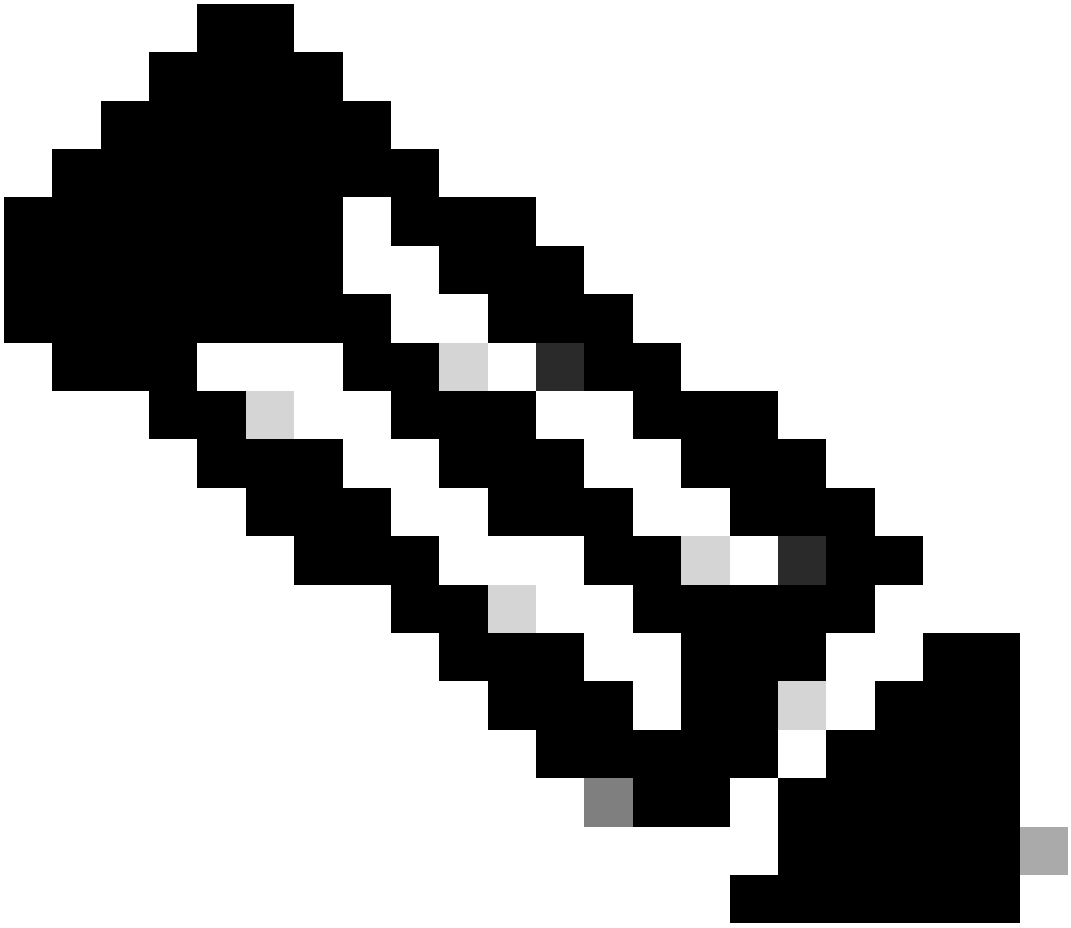
Omnidireccional

El uso de antenas omnidireccionales (internas o externas) debe evitarse generalmente en escenarios de muy alta densidad, esto se debe al área de impacto potencialmente alta para la interferencia de co-canal. Las antenas omnidireccionales no deben utilizarse a una altura superior a 6 m (no se aplica a las unidades exteriores de alta ganancia).

Debajo del asiento

En algunos estadios o arenas puede haber situaciones en las que no haya ubicaciones adecuadas para el montaje de la antena. La última alternativa que queda es proporcionar cobertura desde abajo colocando los AP debajo de los asientos donde los usuarios están sentados. Este tipo de solución es más difícil de implementar correctamente y suele ser más costosa, por lo que se requieren muchos más puntos de acceso y procedimientos de instalación específicos.

El principal reto de la implementación en emplazamientos inferiores a los previstos es la gran diferencia de cobertura entre un emplazamiento lleno y uno vacío. Un cuerpo humano es muy eficiente en atenuar la señal de radio, lo que significa que cuando hay una multitud de personas que rodean el AP, la cobertura resultante es significativamente menor en comparación con cuando esas personas no están allí. Este factor de atenuación de multitudes permite que se implementen más AP, lo que puede aumentar la capacidad general. Sin embargo, cuando el lugar está vacío no hay atenuación de los cuerpos humanos y la interferencia significativa, y esto conduce a complicaciones cuando el lugar está parcialmente lleno.



Nota: la implementación en ubicaciones inferiores es una solución válida pero poco frecuente, y debe evaluarse caso por caso. En este documento no se trata más a fondo la implementación en el asiento.

Estética

En algunas implementaciones entra en juego la cuestión de la estética. Pueden ser áreas con diseños arquitectónicos específicos, valor histórico o espacios donde la publicidad o la marca dicte dónde se pueden montar (o no) los equipos. Se pueden requerir soluciones específicas para solucionar cualquier limitación de ubicación. Algunas de estas soluciones alternativas incluyen ocultar el AP/antena, pintar el AP/antena, montar el equipo en una carcasa o simplemente usar una ubicación diferente. Si pinta la antena, anule la garantía. Si decide pintarla, utilice siempre pintura no metálica. Cisco generalmente no vende carcasas para antenas, pero muchas están disponibles fácilmente a través de varios proveedores.

Todas estas soluciones alternativas tienen un impacto en el rendimiento de la red. Los arquitectos inalámbricos siempre comienzan proponiendo posiciones de montaje óptimas para una mejor

cobertura de radio, y estas posiciones iniciales normalmente proporcionan el mejor rendimiento. Cualquier cambio en estas posiciones suele dar lugar a que las antenas se alejen de sus ubicaciones óptimas.

Las ubicaciones en las que se montan las antenas suelen ser elevadas; pueden ser techos, pasarelas, estructuras de techos, vigas, pasillos y cualquier ubicación que proporcione cierta elevación sobre el área de cobertura prevista. Estas ubicaciones suelen compartirse con otras instalaciones, como equipos de audio, aire acondicionado, iluminación y varios detectores/sensores. Por ejemplo, los equipos de audio e iluminación deben montarse en ubicaciones muy específicas, pero ¿por qué? Simplemente, es porque los equipos de audio e iluminación no funcionan correctamente cuando están ocultos en una caja o detrás de una pared, y todo el mundo reconoce esto.

Lo mismo se aplica a las antenas inalámbricas, que funcionan mejor cuando hay una línea de visión para el dispositivo cliente inalámbrico. Dar prioridad a la estética puede tener (y muy a menudo tiene) un efecto negativo en el rendimiento inalámbrico, lo que disminuye el valor de la inversión en infraestructura.

Redes no autorizadas

Las redes Wi-Fi no autorizadas son redes inalámbricas que comparten un espacio de RF común pero que no son gestionadas por el mismo operador. Estos pueden ser temporales o permanentes e incluyen dispositivos de infraestructura (AP) y dispositivos personales (como teléfonos móviles que comparten una zona Wi-Fi). Las redes Wi-Fi no autorizadas son una fuente de interferencias y, en algunos casos, también suponen un riesgo para la seguridad. No se debe subestimar el impacto de los sistemas no fiables en el rendimiento inalámbrico. Las transmisiones Wi-Fi se limitan a un espectro de radio relativamente pequeño que comparten todos los dispositivos Wi-Fi. Cualquier dispositivo que se comporte mal en las proximidades puede afectar al rendimiento de la red para muchos usuarios.

En el contexto de las grandes redes públicas, estas suelen diseñarse y sintonizarse cuidadosamente mediante antenas especializadas. Un buen diseño de RF cubre solo las áreas requeridas, a menudo usando antenas direccionales, y ajusta las características de envío y recepción para una eficiencia máxima.

En el otro extremo del espectro se encuentran los dispositivos de nivel de consumidor o los dispositivos suministrados por los proveedores de servicios de Internet. Estos dispositivos tienen opciones limitadas para el ajuste de RF fino o están configurados para un alcance máximo y un rendimiento percibido, a menudo con alta potencia, baja velocidad de datos y canales anchos. La introducción de estos dispositivos en una red de eventos de gran tamaño puede causar estragos.

¿Qué se puede hacer?

En el caso de los puntos de conexión personales, es muy poco lo que se puede hacer, ya que sería casi imposible supervisar a decenas de miles de personas que entran en un lugar. En el caso de la infraestructura, o de los dispositivos semipermanentes, existen algunas opciones. La posible remediación comienza con una educación sencilla, que incluye una señalización sencilla

para la sensibilización, a través de documentos de política de radio firmados, que termina con una aplicación activa y un análisis del espectro. En todos los casos, debe adoptarse una decisión empresarial sobre la protección del espectro radioeléctrico en el lugar de celebración de la reunión, junto con medidas concretas para hacer cumplir dicha decisión empresarial.

El aspecto de la seguridad de las redes no autorizadas entra en juego cuando los dispositivos controlados por un tercero anuncian el mismo SSID que la red gestionada. Esto equivale a un ataque de honeypot y se puede utilizar como método para robar credenciales de usuario. Siempre se recomienda crear una regla no autorizada para alertar sobre la detección de SSID de infraestructura anunciados por dispositivos no gestionados. En la sección de seguridad se tratan los sistemas no fiables con más detalle.

Único 5 GHz frente a dual 5 GHz

Dual 5GHz se refiere al uso de ambas radios de 5GHz en los AP soportados. Existe una diferencia clave entre los 5 GHz duales que utilizan antenas externas y los 5 GHz duales que utilizan antenas internas (celdas micro/macro en AP omnidireccionales). En el caso de las antenas externas, la dualidad de 5 GHz es a menudo un mecanismo útil, que proporciona cobertura y capacidad adicionales al tiempo que reduce el recuento total de puntos de acceso.

Micro/Macro/Meso

Los AP internos tienen ambas antenas juntas (dentro del AP) y hay restricciones relacionadas con la potencia Tx máxima cuando se utiliza 5 GHz dual. La segunda radio está limitada a una potencia Tx baja (esto es impuesto por el controlador inalámbrico) lo que conduce a un gran desequilibrio de potencia Tx entre las radios. Esto puede hacer que la radio principal (de mayor potencia) atraiga a muchos clientes mientras que la radio secundaria (de menor potencia) está infrautilizada. En este caso, el segundo radio es la adición de energía en el medio ambiente sin proporcionar beneficios a los clientes. Si se observa este escenario, puede ser mejor inhabilitar la segunda radio y simplemente agregar otro AP (único de 5 GHz) si se requiere capacidad adicional.

Los diferentes modelos de AP tienen diferentes opciones de configuración, la segunda radio de 5 GHz puede funcionar a niveles de energía más altos en los nuevos macro/meso AP como el 9130 y 9136, y algunos AP internos Wi-Fi 6E como la serie 9160 incluso pueden funcionar en macro/macro en algunos casos. Verifique siempre la capacidad de su modelo de AP exacto. La segunda ranura de 5 GHz también está limitada en el uso de canal; cuando una ranura funciona en una banda UNII, la otra ranura está restringida a una banda UNII diferente, lo que afecta a la planificación de canales y, posteriormente, a la potencia de transmisión disponible. Piense siempre en la diferencia de potencia Tx entre las radios duales de 5 GHz; esto es así en todos los casos, incluidos los puntos de acceso internos.

FRA

La asignación de radio flexible (FRA) se introdujo como tecnología para mejorar la cobertura de 5 GHz mediante el cambio de radios adicionales de 2,4 GHz al modo de 5 GHz o radios de 5 GHz potencialmente sin usar al modo de monitor (para los puntos de acceso que la admitían). Dado

que este documento cubre grandes redes públicas, se asume que las áreas de cobertura y el diseño de radio están bien definidos usando antenas direccionales, por lo que se prefiere una configuración determinista sobre una dinámica. No se recomienda el uso de FRA para redes públicas de gran tamaño.

Opcionalmente, FRA se podría utilizar cuando la red está configurada para ayudar a determinar qué radios convertir a 5 GHz, pero una vez que esté satisfecho con el resultado, se recomienda congelar FRA.

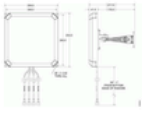
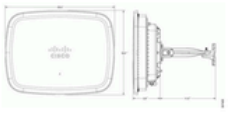
Normativa

Cada dominio de regulación define qué canales están disponibles para su uso y sus niveles máximos de potencia. También hay restricciones sobre qué canales se pueden utilizar en interiores en lugar de en exteriores. En función del dominio normativo, a veces no es posible utilizar una solución dual de 5 GHz de forma eficaz. Un ejemplo de esto es el dominio ETSI donde se permiten 30dBm en los canales UNII-2e, pero solamente 23dBm en UNII1/2. En este ejemplo, si el diseño requiere el uso de 30 dBm (normalmente debido a una mayor distancia a la antena), el uso de una única radio de 5 GHz puede ser la única solución factible.

Antenas

Las grandes redes públicas pueden utilizar cualquier tipo de antena y, normalmente, elegir la más adecuada para el trabajo. La mezcla de antenas dentro de la misma área de cobertura hace que el proceso de diseño de radio sea más difícil y debe evitarse si es posible. Sin embargo, las grandes redes públicas a menudo tienen grandes áreas de cobertura con diferentes opciones de montaje incluso dentro de la misma área, lo que hace necesario mezclar antenas en algunos casos. Las antenas omnidireccionales se entienden bien y funcionan igual que cualquier otra antena. En esta guía se tratan las antenas direccionales externas.

Esta tabla enumera las antenas externas más utilizadas.

	C-ANT9103 Patch antenna (8x8) 6 dBi	5GHz Beamwidth 70°x70° ~33ft (10m)
	ANT2566P4W-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 110°x55° (120°x60°) ~33ft (10m)
	ANT2566D4M-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 55°x60° (60°x60°) ~33ft (10m)
	ANT2513P4M-N/S HD “Stadium” antenna 13 dBi	5GHz Beamwidth 31°x27° (30°x30°) ~66ft (20m)
	C-ANT9104 HD “Stadium” antenna Narrow 10dBi / Wide 7dBi	5GHz Beamwidth Narrow 25°x25° Wide 80°x25°

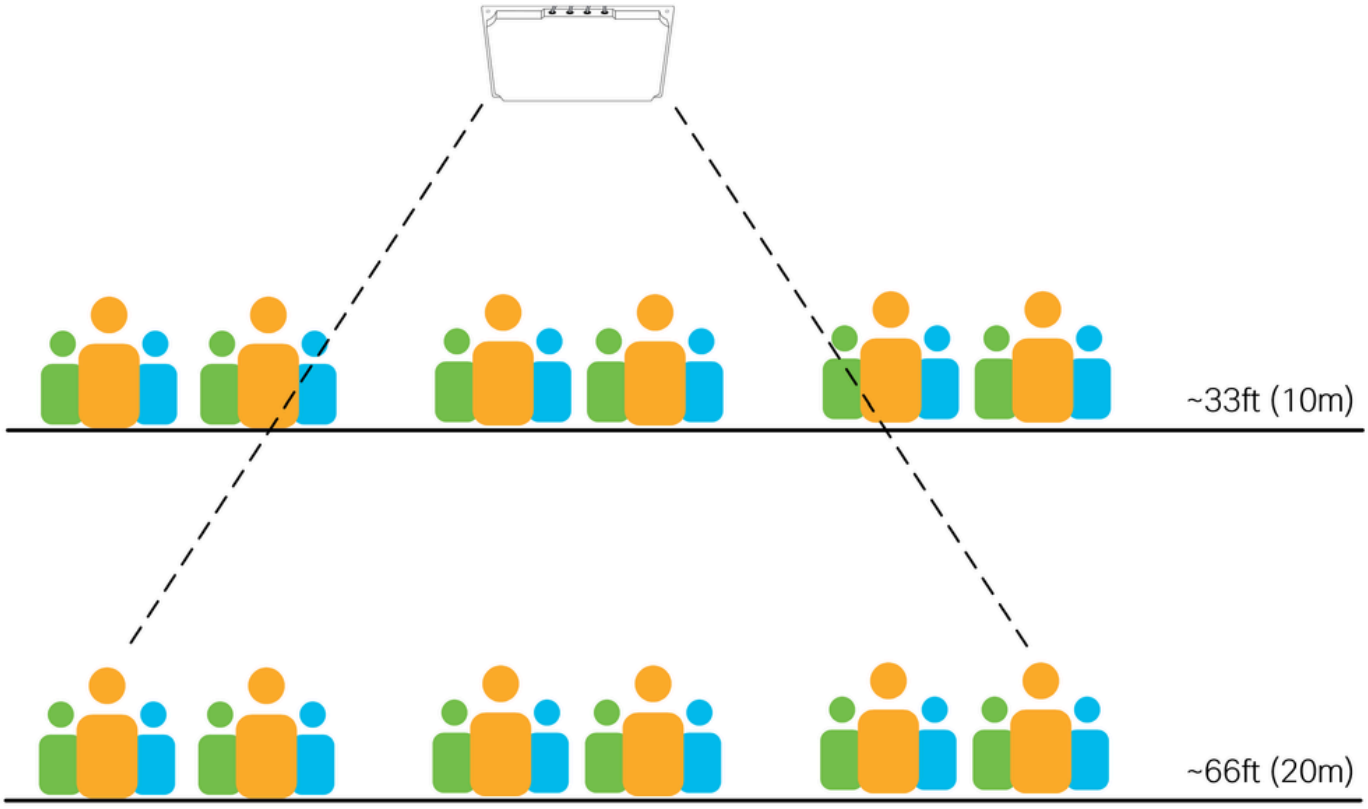
Lista de antenas

Los factores principales que se deben tener en cuenta al elegir una antena son la anchura de haz de la antena y la distancia/altura a la que se monta la antena. La tabla muestra el ancho de haz de 5 GHz para cada antena, con los números entre paréntesis que muestran valores redondeados (y más fáciles de recordar).

Las distancias sugeridas en la tabla no son reglas duras, solo pautas basadas en la experiencia. Las ondas de radio viajan a la velocidad de la luz y no se detienen simplemente después de alcanzar una distancia arbitraria. Todas las antenas funcionan más allá de la distancia sugerida; sin embargo, el rendimiento disminuye a medida que aumenta la distancia. La altura de la instalación es un factor clave durante la planificación.

El siguiente diagrama muestra dos posibles alturas de montaje para la misma antena a unos 10 m (33 pies) y 20 m (66 pies) en un área de alta densidad. Observe que el número de clientes que la antena puede ver (y aceptar conexiones desde) aumenta con la distancia. El mantenimiento de tamaños de células más pequeñas se vuelve más difícil con distancias más grandes.

La regla general es que cuanto mayor sea la densidad de usuarios, más importante será utilizar la antena correcta para la distancia dada.



Una antena de estadio

La antena de estadio C9104 es adecuada para cubrir áreas de alta densidad en distancias altas. Consulte la Guía de implementación de la antena de estadio Catalyst 9104 (C-ANT9104) para obtener más información.

Cambios a lo largo del tiempo

Los cambios en el entorno físico a lo largo del tiempo son comunes en casi todas las instalaciones inalámbricas (por ejemplo, el movimiento de paredes interiores). Las visitas periódicas al lugar y las inspecciones visuales siempre han sido una práctica recomendada. Para las redes de eventos existe la complejidad adicional de tratar con sistemas de audio e iluminación, y en muchos casos también otros sistemas de comunicación (como el 5G). Todos estos sistemas se suelen instalar en ubicaciones elevadas por encima de los usuarios, lo que a veces provoca una competencia por el mismo espacio. Una buena ubicación para una antena inalámbrica de un estadio suele ser también una buena ubicación para una antena 5G. Es más, a medida que estos sistemas se actualicen con el tiempo, se podrán reubicar en ubicaciones en las que obstruyan o interfieran activamente con el sistema inalámbrico. Es importante realizar un seguimiento de las otras instalaciones y comunicarse con los equipos que las instalan para garantizar que todos los sistemas se instalan en ubicaciones adecuadas sin interferir entre sí (física o electromagnéticamente).

Alta densidad y 6 GHz

En el momento de escribir este documento, hay una selección limitada de antenas externas compatibles con 6 GHz. Solo el AP/antena integrada CW9166D1 funciona a 6 GHz, las especificaciones detalladas de la antena están disponibles en la Guía de implementación del punto de acceso Cisco Catalyst CW9166D1. El CW9166D1 proporciona una cobertura de 6 GHz con una anchura de haz de 60°x60° y se puede utilizar de forma eficaz para cualquier implementación que cumpla las condiciones de este tipo de antena. Por ejemplo, los auditorios y almacenes son buenos candidatos para la implementación del CW9166D1, ya que la unidad integrada ofrece funcionalidad de antena direccional para uso en interiores.

	CW9166D1 6GHz (4x4) or XOR 5GHz	60° x 60° 8 dBi
	5GHz (4x4)	70° x 70° 6 dBi
	2.4GHz (4x4)	70° x 70° 6 dBi

9166D1

En el contexto de las grandes redes públicas, estas suelen tener varias áreas grandes y requieren el uso de una combinación de antenas a distintas alturas. La implementación de una red pública de gran tamaño de extremo a extremo con solo una antena de 60°x60° puede suponer un reto debido a las limitaciones de distancia. Por lo tanto, también puede resultar complicado proporcionar una cobertura integral a 6 GHz utilizando únicamente el CW9166D1 para una red pública de gran tamaño.

Un enfoque posible consiste en utilizar 5 GHz como banda de cobertura principal, mientras que utilizar 6 GHz solo en áreas específicas para descargar dispositivos cliente compatibles a la banda de 6 GHz más limpia. Este tipo de enfoque hace uso de antenas de 5 GHz únicamente en áreas más grandes, mientras que utiliza las antenas de 6 GHz donde sea posible y donde se requiera capacidad adicional.

Por ejemplo, si tenemos en cuenta un gran salón de eventos en una conferencia comercial, el salón principal utiliza antenas de estadio para proporcionar la cobertura principal a 5 GHz; la altura de la instalación exige el uso de antenas de estadio. El CW9166D1 no se puede utilizar en la sala principal de este ejemplo debido a limitaciones de distancia, pero se puede utilizar de forma eficaz en una sala VIP adyacente o en una zona de prensa donde se requiera una mayor densidad. El roaming del cliente entre las bandas de 5 GHz y 6 GHz se analiza más adelante en este documento.

Normativa

Al igual que ocurre con los 5 GHz, la potencia disponible y los canales para 6 GHz difieren significativamente entre los dominios normativos. En particular, existe una gran diferencia en el espectro disponible entre los dominios FCC y ETSI, así como estrictas directrices sobre la potencia Tx disponible para uso en interiores y exteriores, la potencia de bajo consumo en interiores (LPI) y la potencia estándar (SP), respectivamente. Con 6 GHz, las restricciones adicionales incluyen los límites de alimentación del cliente, el uso de antenas externas y la inclinación de la antena hacia abajo y (solo en EE. UU. por ahora) el requisito de coordinación de frecuencia automatizada (AFC) para implementaciones SP.

Para obtener más información sobre Wi-Fi 6E, consulte Wi-Fi 6E: The Next Great Chapter (Wi-Fi 6E: El siguiente gran capítulo del informe técnico sobre Wi-Fi).

Administración de Recursos de Radio

Radio Resource Management (RRM) es un conjunto de algoritmos responsables del control del funcionamiento de la radio. Esta guía hace referencia a dos algoritmos RRM clave, a saber, Dynamic Channel Assignment (DCA) y Transmit Power Control (TPC). RRM es una alternativa al canal estático y a la configuración de alimentación.

- DCA se ejecuta según una programación configurable (10 minutos de forma predeterminada).
- TPC se ejecuta según una programación automática (valor predeterminado: 10 minutos).

Cisco Event Driven RRM (ED-RRM) es una opción de DCA que permite tomar una decisión de cambio de canal fuera de la programación de DCA estándar, normalmente en respuesta a condiciones de RF severas. ED-RRM puede cambiar un canal inmediatamente cuando se detectan niveles excesivos de interferencia. En entornos ruidosos y/o inestables que permiten ED-RRM plantea un riesgo de cambios excesivos de canal, esto es un impacto negativo potencial en los dispositivos cliente.

Se recomienda el uso de RRM y se prefiere en general a la configuración estática; sin embargo, con ciertas advertencias y excepciones.

- El TPC debe limitarse a un intervalo estrecho de valores utilizando el ajuste TPC mín./máx., según sea necesario, y debe estar siempre alineado con el diseño de radiofrecuencia.
    - Habilite TPC Channel Aware en entornos de alta densidad.

- El ciclo de DCA se debe cambiar desde el valor predeterminado de 10 minutos.
    - No utilice ED-RM en entornos HD.
    - Inhabilite Evite la carga del AP de Cisco.
    - Las opciones de evitación de AP dudosos como Evitar la Interferencia de AP Externo pueden resultar en un entorno inestable si hay muchos dudosos. Siempre es mejor eliminar al pícaro que intentar responder a él.
- Las decisiones de RRM pueden verse afectadas por los AP/antenas que no se escuchan entre sí correctamente, como en el caso de las antenas direccionales que apuntan unas de otras.
- Algunas antenas (por ejemplo, C9104) no admiten RRM y siempre requieren una configuración estática.
- RRM no corrige un diseño de RF deficiente.

En todos los casos, RRM debe implementarse con un entendimiento del resultado esperado y ajustarse para operar dentro de límites que sean apropiados para el entorno de RF dado. En las secciones siguientes de este documento se analizan estos puntos con más detalle.

Configuración de RF

Canales

En general, cuantos más canales, mejor. En las implementaciones de alta densidad, puede haber órdenes de magnitud más de AP y radios implementados que los canales disponibles, lo que implica una gran proporción de reutilización de canales y, junto con eso, mayores niveles de interferencia de canal compartido. Se deben utilizar todos los canales disponibles y, por lo general, no se recomienda limitar la lista de canales disponibles.

Puede haber casos en los que un sistema inalámbrico específico (e independiente) deba coexistir en el mismo espacio físico y se le deban asignar canales dedicados, eliminando al mismo tiempo los canales asignados de la lista de DCA del sistema principal. Estos tipos de exclusiones de canales deben evaluarse con mucho cuidado y utilizarse sólo cuando sea necesario. Un ejemplo de esto puede ser un link punto a punto que funciona en un área abierta adyacente a la red principal, o un área de prensa dentro de un estadio. Si se excluyen más de uno o dos canales de la lista de DCA, es motivo para volver a evaluar la solución propuesta. En algunos casos, como estadios de muy alta densidad, excluir incluso un solo canal puede a veces no ser una opción factible.

La asignación dinámica de canales (DCA) se puede utilizar con RRM basada en WLC o RRM mejorada por IA.

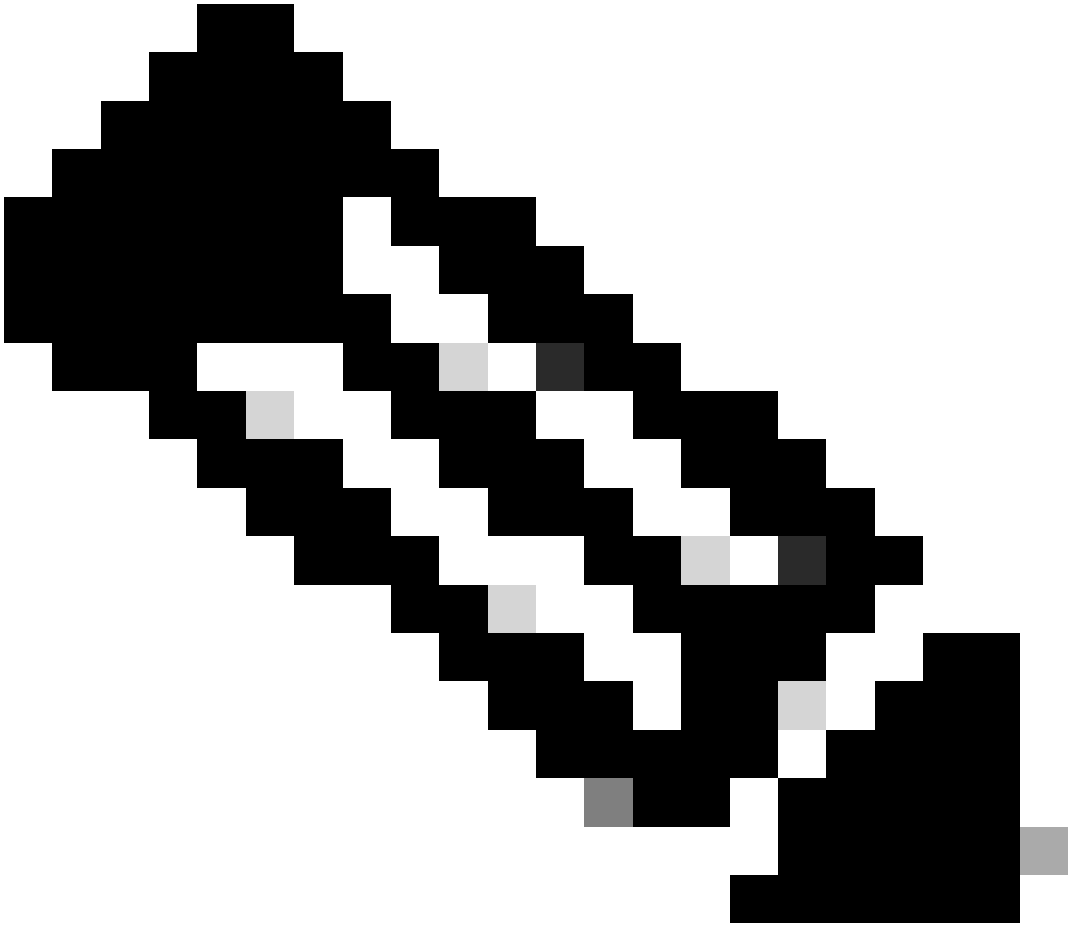
El intervalo DCA predeterminado es de 10 minutos, lo que puede provocar cambios frecuentes de canal en entornos de RF inestables. El temporizador DCA predeterminado debe aumentarse con respecto a los 10 minutos predeterminados en todos los casos, el intervalo DCA específico debe

estar alineado con los requisitos operativos de la red en cuestión. Un ejemplo de configuración puede ser: intervalo DCA 4 horas, tiempo de anclaje 8. Esto limita los cambios de canal a una vez cada 4 horas, a partir de las 8 am.

Dado que las interferencias están destinadas a producirse, adaptarse a ellas en cada ciclo de DCA no aporta necesariamente valor, ya que muchas de ellas son temporales. Una buena técnica es usar DCA automático durante las primeras horas y congelar el algoritmo y el plan de canal cuando tienes algo estable con lo que estás contento.

Cuando se reinicia el WLC, DCA se ejecuta en modo agresivo durante 100 minutos para encontrar un plan de canal adecuado. Es una buena idea reiniciar el proceso manualmente cuando se hacen cambios significativos en el diseño de RF (por ejemplo, agregar o quitar numerosos AP o cambiar el ancho del canal). Para iniciar este proceso manualmente, utilice este comando.

```
ap dot11 [24ghz | 5ghz | 6ghz] rrm dca restart
```



Nota: los cambios de canal pueden afectar a los dispositivos cliente.

2,4 GHz

La banda de 2,4 GHz ha sido criticada con frecuencia. Solo tiene tres canales que no se solapan y muchas otras tecnologías que no sean Wi-Fi lo utilizan, lo que crea interferencias indeseables. Algunas organizaciones insisten en proporcionar servicios en él, así que ¿cuál es una conclusión razonable? Es un hecho que la banda de 2,4 GHz no proporciona una experiencia satisfactoria para los usuarios finales. Peor aún, al intentar proporcionar el servicio a 2,4 GHz, afecta a otras tecnologías de 2,4 GHz, como Bluetooth. En grandes recintos o eventos, muchas personas siguen esperando que sus auriculares inalámbricos funcionen cuando realizan una llamada o que sus dispositivos inteligentes sigan funcionando de la forma habitual. Si su Wi-Fi denso funciona a 2,4 GHz, está afectando a los dispositivos que ni siquiera utilizan su Wi-Fi de 2,4 GHz.

Una cosa es segura: si realmente debe proporcionar un servicio Wi-Fi de 2,4 GHz, lo mejor es hacerlo en un SSID independiente (consérvelo a dispositivos de IoT o llámelo "heredado"). Esto significa que los dispositivos de doble banda no se conectan a 2,4 GHz involuntariamente y que

solo se conectan a ellos los dispositivos de 2,4 GHz de banda única.

Cisco no aconseja ni admite el uso de canales de 40 MHz en 2,4 GHz.

5 GHz

Implementación típica de tecnología inalámbrica de alta densidad. Utilice todos los canales disponibles siempre que sea posible.

El número de canales varía en función del dominio de regulación. Considere el impacto del radar en la ubicación específica, utilice los canales DFS (incluidos los canales TDWR) siempre que sea posible.

El ancho de canal de 20 MHz es muy recomendable para todas las implementaciones de alta densidad.

40 MHz se puede utilizar en la misma base que 2,4 GHz, es decir, solo cuando (y donde) sea absolutamente necesario.

Evalúe la necesidad y las ventajas reales de los canales de 40 MHz en el entorno específico. Los canales de 40 MHz requieren una relación señal-ruido (SNR) más alta para obtener cualquier mejora posible en el rendimiento. Si no es posible una SNR más alta, los canales de 40 MHz no sirven para nada. Las redes de alta densidad dan prioridad a la media de todos los usuarios sobre un rendimiento potencialmente mayor para cualquier usuario individual. Es mejor colocar más APs en los canales de 20MHz que tener APs usando 40MHz como el canal secundario se utiliza solamente para las tramas de datos y por lo tanto se utiliza mucho menos eficientemente que tener dos células de radio diferentes, cada una funcionando en 20MHz (en términos de capacidad total, no en términos de rendimiento de un solo cliente).

6 GHz

La banda de 6 GHz todavía no está disponible en todos los países. Además, algunos dispositivos tienen un adaptador Wi-Fi de 6 GHz, pero necesita una actualización de la BIOS para activarse en el país específico en el que está utilizando el dispositivo. La forma más popular en que los clientes descubren las radios de 6 GHz en este momento es a través del anuncio de RNR en la radio de 5 GHz. Esto significa que 6GHz no debe funcionar solo sin una radio 5GHz en el mismo AP. 6GHz está allí para descargar clientes y tráfico de la radio 5GHz y para proporcionar típicamente una mejor experiencia para los clientes capaces. Los canales de 6 GHz permiten utilizar anchos de banda de canal mayores, pero depende en gran medida del número de canales disponibles en el dominio regulador. Con los canales de 24,6 GHz disponibles en Europa, no es descabellado optar por los canales de 40 MHz para proporcionar un rendimiento máximo mejor en comparación con los canales de 20 MHz que probablemente utiliza en 5 GHz. En Estados Unidos, con casi el doble de canales, el uso de 40 MHz es una obviedad e incluso ir a 80 MHz no es irracional para un evento de gran densidad. Los anchos de banda más grandes no deben utilizarse en eventos o lugares de alta densidad.

Velocidades de datos

La velocidad de datos que un cliente negocia con un AP es en gran medida una función de la relación señal-ruido (SNR) de esa conexión, y lo contrario también es cierto, es decir, las velocidades de datos más altas requieren SNR más alto. De hecho, es principalmente SNR el que determina la máxima velocidad de link posible, pero ¿por qué es esto importante al configurar las velocidades de datos? Esto se debe a que algunas velocidades de datos tienen un significado especial.

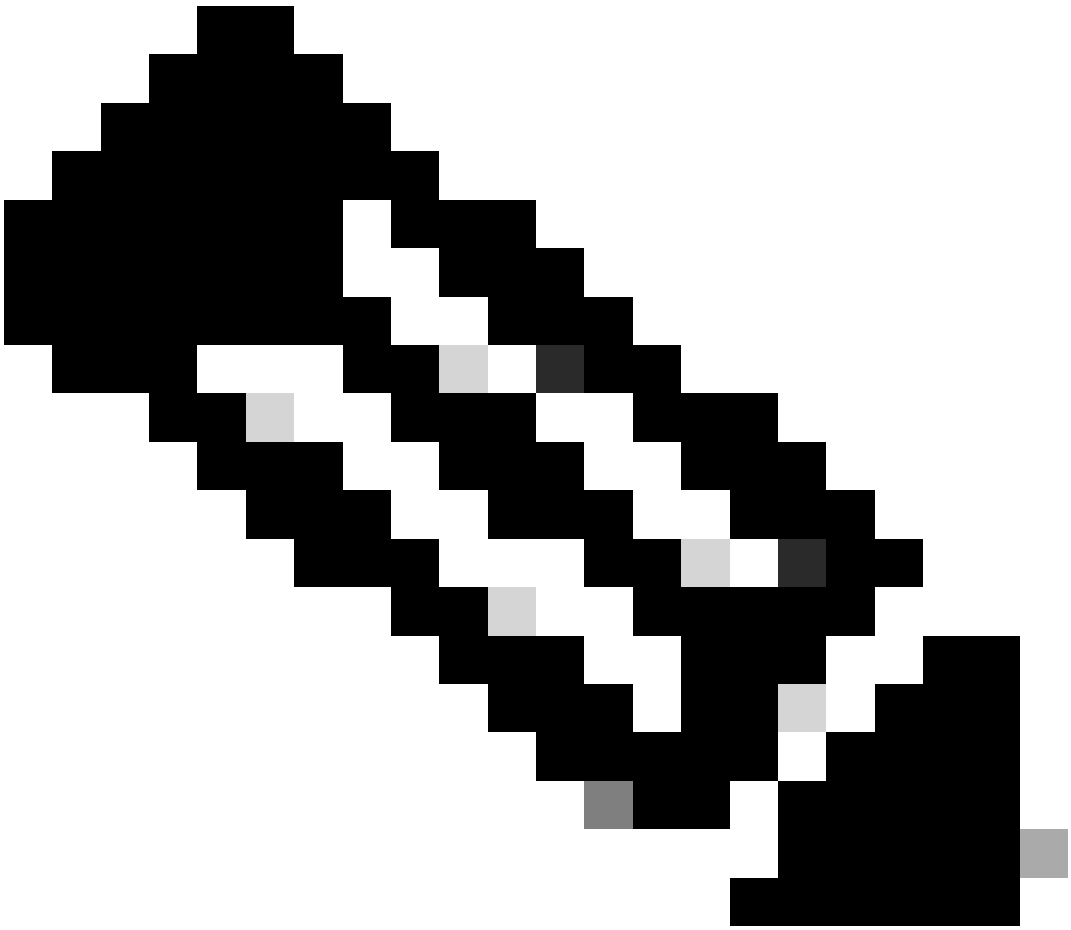
Las velocidades de datos clásicas de OFDM (802.11a) se pueden configurar en una de las tres opciones siguientes: Desactivado, Soportado o Obligatorio. Las velocidades OFDM son (en Mbps): 6, 9, 12, 18, 24, 36, 48, 54, y el cliente y el AP deben soportar una velocidad antes de que se pueda utilizar.

Soportado: el AP utilizará la velocidad

Obligatorio: el AP utilizará la velocidad y enviará tráfico de administración con esta velocidad

Deshabilitado: el AP no utilizará la velocidad, lo que forzará al cliente a utilizar otra velocidad

---



Nota: Las tarifas obligatorias también se denominan tarifas básicas

La importancia de la velocidad obligatoria es que todas las tramas de administración se envían usando esta velocidad, así como las tramas de difusión y multidifusión. Si hay varias velocidades obligatorias configuradas, las tramas de administración utilizan la velocidad obligatoria configurada más baja y las de difusión y multidifusión utilizan la velocidad obligatoria configurada más alta.

Las tramas de administración incluyen balizas que debe escuchar el cliente para poder asociarse al AP. Al aumentar la velocidad obligatoria también aumenta el requisito SNR para esa transmisión, recuerde que las velocidades de datos más altas requieren SNR más alto, y esto normalmente significa que el cliente necesita estar más cerca del AP para poder decodificar la baliza y asociarse. Por lo tanto, al manipular la velocidad de datos obligatoria también manipulamos el rango de asociación efectiva del AP, obligando a los clientes a acercarse más al AP o hacia una posible decisión de roaming. Los clientes que están cerca del AP utilizan velocidades de datos más altas, y las velocidades de datos más altas utilizan menos tiempo de transmisión - el efecto esperado es una celda más eficiente. Es importante recordar que el aumento de la velocidad de datos sólo afecta a la velocidad de transmisión de ciertas tramas, no afecta a la propagación de RF de la antena ni al rango de interferencia. Todavía se necesitan buenas prácticas de diseño de RF para minimizar la interferencia y el ruido en los canales compartidos.

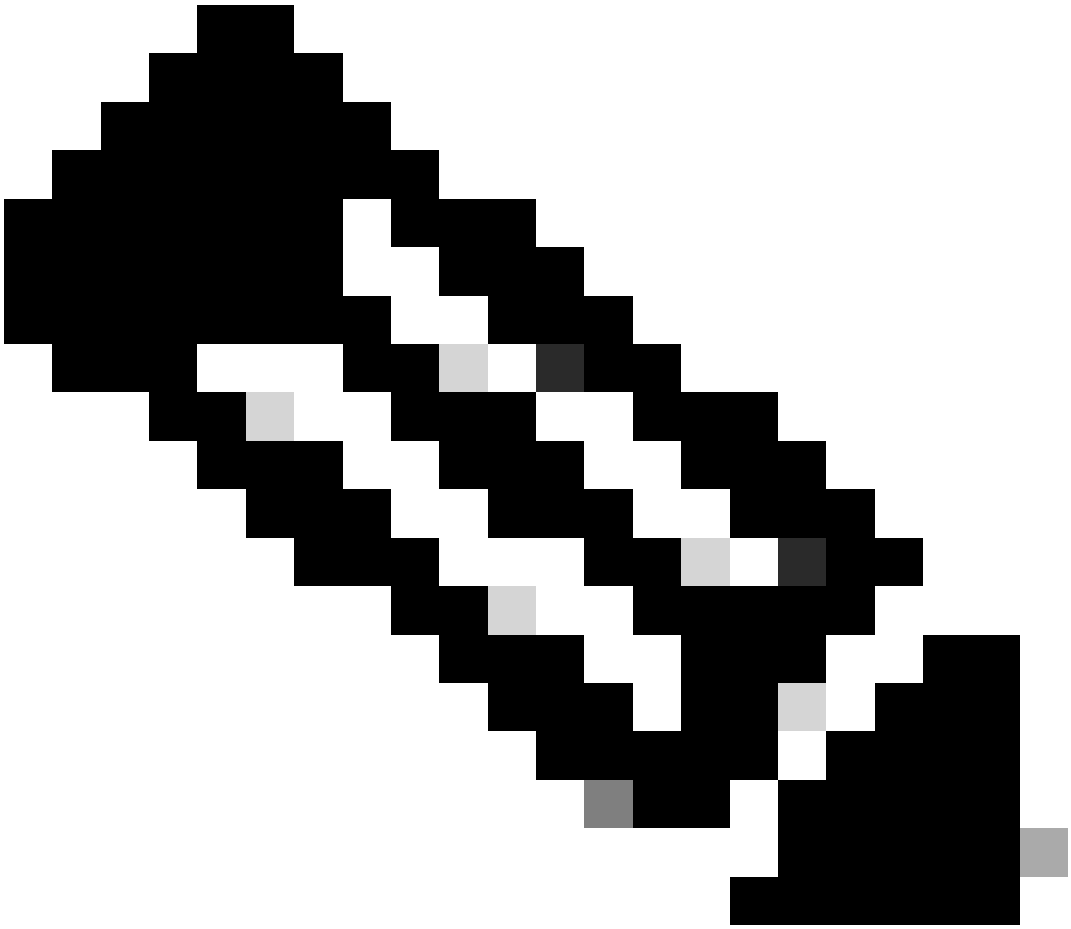
Por el contrario, dejar las velocidades más bajas como obligatorias significa normalmente que los clientes podrán asociarse desde una distancia mucho mayor, útil en escenarios de densidad de AP más baja, pero con potencial para causar estragos con el roaming en escenarios de densidad más alta. Cualquiera que haya intentado localizar un AP rogue que está transmitiendo un 6Mbps sabrá que usted puede detectar el AP muy lejos de su ubicación física!

En cuanto al tema de la difusión y multidifusión, en algunos casos se configura una segunda velocidad obligatoria (más alta) para aumentar la velocidad de entrega del tráfico de multidifusión. Esto rara vez es exitoso ya que la multidifusión nunca se reconoce y nunca se retransmite en caso de que se pierdan las tramas. Como parte de la pérdida es inherente a todos los sistemas inalámbricos, es inevitable que algunas tramas multicast se pierdan independientemente de la velocidad configurada. Un mejor enfoque para la entrega de multidifusión fiable son las técnicas de conversión de multidifusión a unidifusión que transmiten la multidifusión como un flujo de unidifusión, lo que tiene la ventaja de velocidades de datos más altas y entrega (reconocida) fiable.

Se recomienda utilizar una única tasa obligatoria, desactivar todas las tasas por debajo de la tasa obligatoria y dejar todas las tasas por encima de la tasa obligatoria como admitida. La velocidad específica a utilizar depende del caso de uso, como ya se mencionó, las tasas más bajas son útiles en escenarios de menor densidad y exteriores donde las distancias entre los AP son mayores. Para las redes de alta densidad y eventos, deben desactivarse las velocidades bajas.

Si no está seguro por dónde empezar, utilice una velocidad obligatoria de 12 Mbps para implementaciones de baja densidad y de 24 Mbps para implementaciones de alta densidad.

Muchos eventos a gran escala, estadios e incluso implementaciones de oficinas empresariales de alta densidad han demostrado funcionar de forma fiable con una configuración de velocidad obligatoria de 24 Mbps. Se recomienda realizar las pruebas adecuadas en casos prácticos específicos en los que se necesiten velocidades inferiores a 12 Mbps o superiores a 24 Mbps.



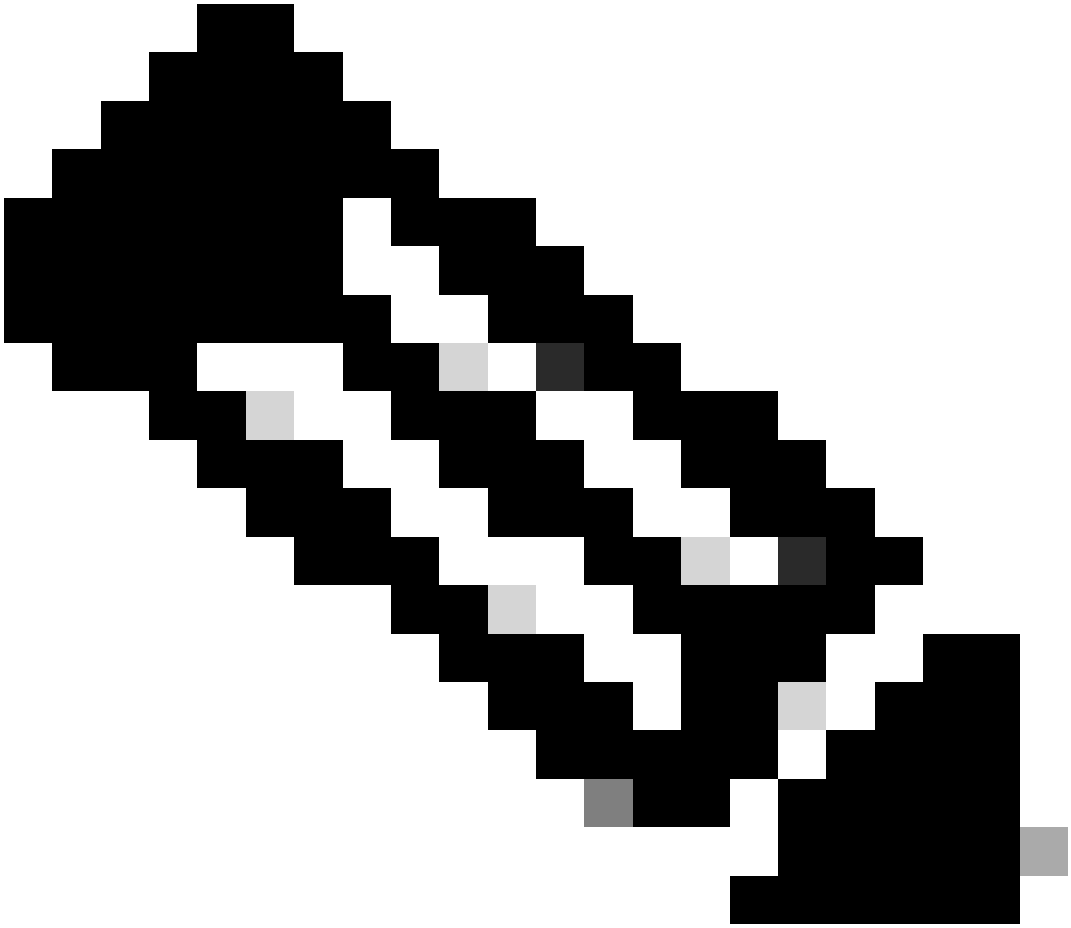
> Nota: Es mejor dejar todas las velocidades 802.11n/ac/ax habilitadas (todas las velocidades en la sección de alto rendimiento de la GUI del WLC), hay raramente una necesidad de inhabilitar cualquiera de estas.

Potencia de transmisión

Las recomendaciones de potencia de transmisión difieren según el tipo de implementación. Aquí diferenciamos las implementaciones interiores que utilizan antenas omnidireccionales de las que utilizan antenas direccionales. Ambos tipos de antenas pueden existir en una red pública de gran tamaño, aunque normalmente cubrirían diferentes tipos de áreas.

En el caso de las implementaciones omnidireccionales, es habitual utilizar el control automático

de potencia de transmisión (TPC) con un umbral mínimo configurado estáticamente y, en algunos casos, también un umbral máximo configurado estáticamente.



> Nota: Los umbrales TPC hacen referencia a la potencia de transmisión de radio y excluyen la ganancia de la antena. Asegúrese siempre de que la ganancia de la antena esté configurada correctamente para el modelo de antena utilizado; esto se realiza automáticamente en el caso de antenas internas y antenas autoidentificables.

Ejemplo 1

TPC mín.: 5 dBm, TPC máx.: máximo (30 dBm)

Esto haría que el algoritmo TPC determinara la potencia de transmisión automáticamente, pero nunca por debajo del umbral mínimo configurado de 5dBm.

Ejemplo 2

TPC mín.: 2 dBm, TPC máx.: 11 dBm

Esto haría que el algoritmo TPC determinara la potencia de transmisión automáticamente, pero siempre permaneciendo entre 2dBm y 11dBm.

Un buen enfoque consiste en crear varios perfiles de RF con diferentes umbrales, por ejemplo, baja potencia (2-5 dBm), potencia media (5-11 dbM) y alta potencia (11-17 dBM), y luego asignar puntos de acceso omnidireccionales a cada perfil de RF según sea necesario. Los valores de cada perfil de radiofrecuencia se pueden ajustar al caso de uso esperado y al área de cobertura. Esto permite que los algoritmos RRM operen dinámicamente mientras se mantienen dentro de límites predefinidos.

El enfoque para las antenas direccionales es muy similar, la única diferencia es el nivel de precisión requerido. La ubicación de la antena direccional debe diseñarse y verificarse durante un estudio de radiofrecuencia previo al despliegue, y los valores de configuración de radio específicos suelen ser el resultado de este proceso.

Por ejemplo, si se requiere una antena fija montada en el techo para cubrir un área determinada desde una altura de ~26ft (8m), el estudio de radiofrecuencia debe determinar la potencia Tx mínima necesaria para lograr esta cobertura prevista (esto determina el valor TPC mínimo para el perfil de radiofrecuencia). Del mismo modo, a partir del mismo estudio de radiofrecuencia entenderíamos el posible solapamiento necesario entre esta y la siguiente antena, o incluso el punto en el que queremos que finalice la cobertura; esto proporcionaría el valor máximo de TPC para el perfil de radiofrecuencia.

Los perfiles de radiofrecuencia para antenas direccionales se configuran normalmente con los mismos valores TPC mínimos y máximos o con un rango estrecho de valores posibles (normalmente <= 3 dBm).

Se recomiendan los perfiles de RF para garantizar la consistencia de la configuración; no se recomienda la configuración estática de AP individuales. Se recomienda asignar un nombre a los perfiles de RF en función del área de cobertura, el tipo de antena y el caso práctico, por ejemplo, RF-Auditorium-Patch-Ceiling.

La cantidad correcta de potencia Tx es cuando el valor SNR requerido es alcanzado por el cliente más débil en el área de cobertura deseada, y no más que eso. 30 dBm es un gran valor objetivo de SNR de cliente en condiciones reales (es decir, en un lugar lleno de personas).

CHD

La detección de agujeros de cobertura (CHD) es un algoritmo independiente para identificar y remediar los agujeros de cobertura. CHD se configura globalmente, así como por WLAN. Un posible efecto de CHD es el aumento de la potencia Tx para compensar los agujeros de cobertura (áreas con clientes detectados consistentemente con una señal deficiente), este efecto está en el nivel de radio y afecta a todas las WLAN, incluso cuando se activa por una sola WLAN configurada para CHD.

Las grandes redes públicas se configuran típicamente a niveles de energía específicos usando perfiles de RF, algunos pueden estar en áreas abiertas con clientes que entran y salen de las áreas, no hay necesidad de un algoritmo para ajustar dinámicamente la energía Tx AP en

respuesta a estos eventos del cliente.

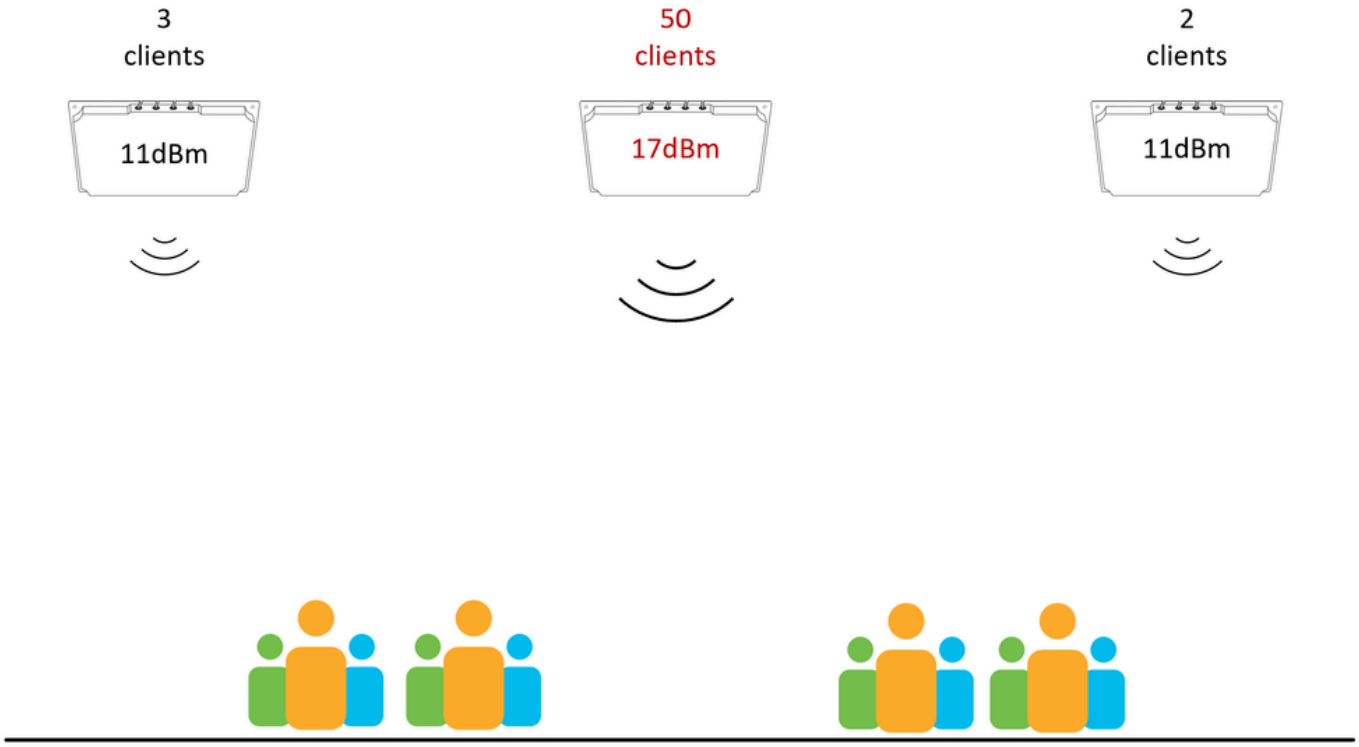
CHD debe estar deshabilitado globalmente para redes públicas de gran tamaño.

Balance de potencia

La mayoría de los dispositivos cliente prefieren una señal recibida más alta al elegir a qué AP asociarse. Se deben evitar situaciones donde un AP se configura con una potencia Tx significativamente más alta en comparación con otros AP circundantes. Los AP que funcionan con una mayor potencia Tx atraen a más clientes, lo que conduce a una distribución de clientes desigual entre los AP (por ejemplo, un solo AP/radio está sobrecargado de clientes mientras que los AP circundantes están infrautilizados). Esta situación es común en las implementaciones con una gran superposición de la cobertura de varias antenas, y en los casos en que un AP tiene varias antenas conectadas.

Las antenas de estadio, como la C9104, requieren un cuidado especial a la hora de seleccionar la potencia Tx, ya que los haces de antena se solapan según el diseño. Consulte la guía de implementación de la antena de estadio Catalyst 9104 (C-ANT9104) para obtener más información al respecto.

En el siguiente diagrama, la antena central está configurada con una potencia Tx mayor que las antenas circundantes. Es probable que esta configuración provoque que los clientes se "atasquen" en la antena central.

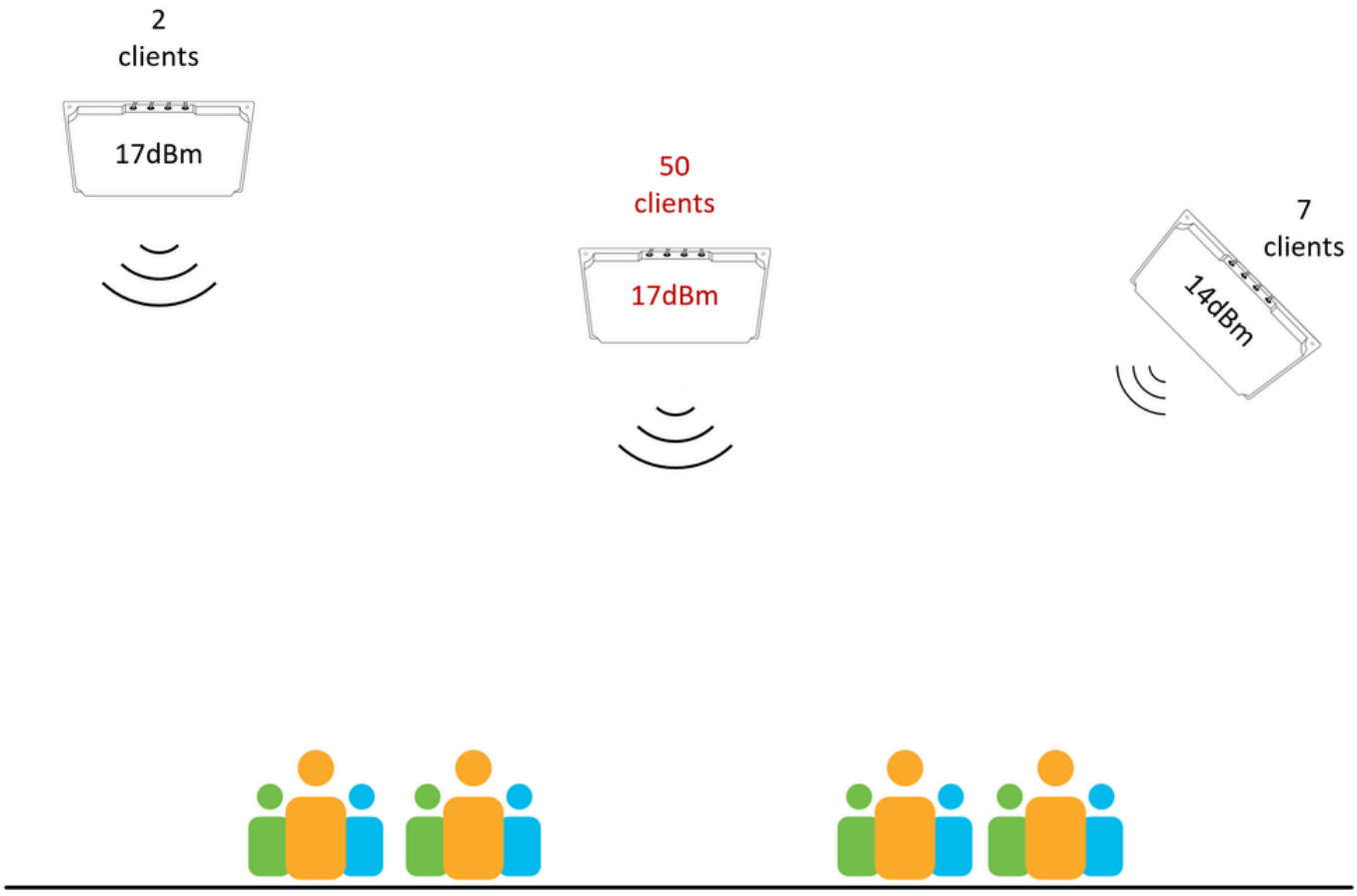


Un AP con más poder que sus AP vecinos atrae a todos los clientes alrededor

El siguiente diagrama muestra una situación más complicada, no todas las antenas están a la misma altura, y no todas las antenas están usando la misma inclinación/orientación. Lograr una potencia equilibrada es más complicado que simplemente configurar todas las radios con la

misma potencia Tx. En escenarios como este, puede ser necesario realizar un estudio del sitio posterior a la implementación, que proporciona una vista de la cobertura desde el punto de vista del dispositivo del cliente (sobre el terreno). Los datos de la encuesta se pueden utilizar para equilibrar la configuración con el fin de lograr una mejor cobertura y distribución entre los clientes.

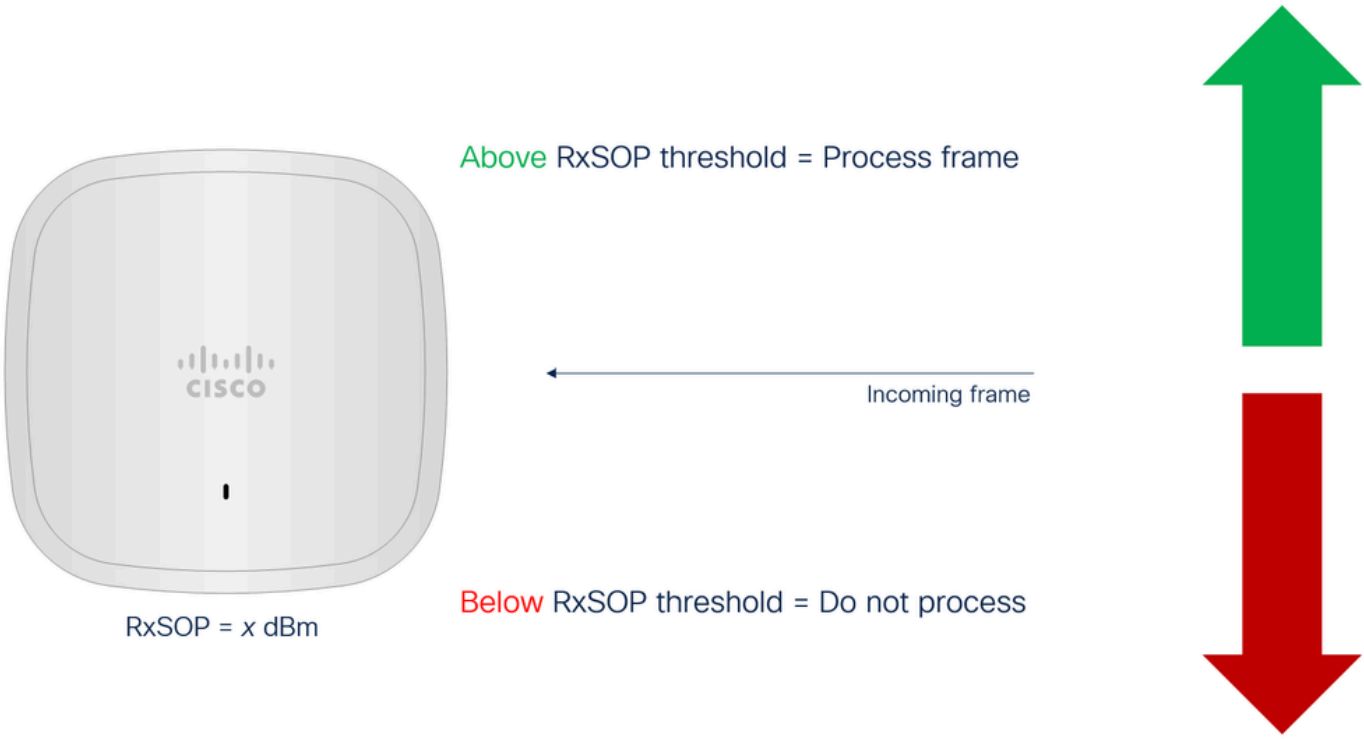
Diseñar ubicaciones de colocación de AP uniformes que eviten situaciones complicadas como esta es la mejor manera de evitar escenarios de ajuste de RF desafiantes (aunque a veces no hay otra opción).



Un AP está atrayendo a todos los clientes a pesar de que la potencia Tx es similar, pero la altura y los ángulos juegan un papel importante

RxSOP

A diferencia de mecanismos como la potencia Tx o las velocidades de datos que afectan a las características de la célula de transmisión, RxSOP (Inicio del Receptor de la Detección de Paquetes) tiene como objetivo influir en el tamaño de la célula de recepción. En esencia, RxSOP puede considerarse como un umbral de ruido, en el sentido de que define el nivel de señal recibida por debajo del cual el AP no intenta decodificar las transmisiones. Cualquier transmisión que llegue con un nivel de señal más débil que el umbral RxSOP configurado no es procesada por el AP y es tratada efectivamente como ruido.



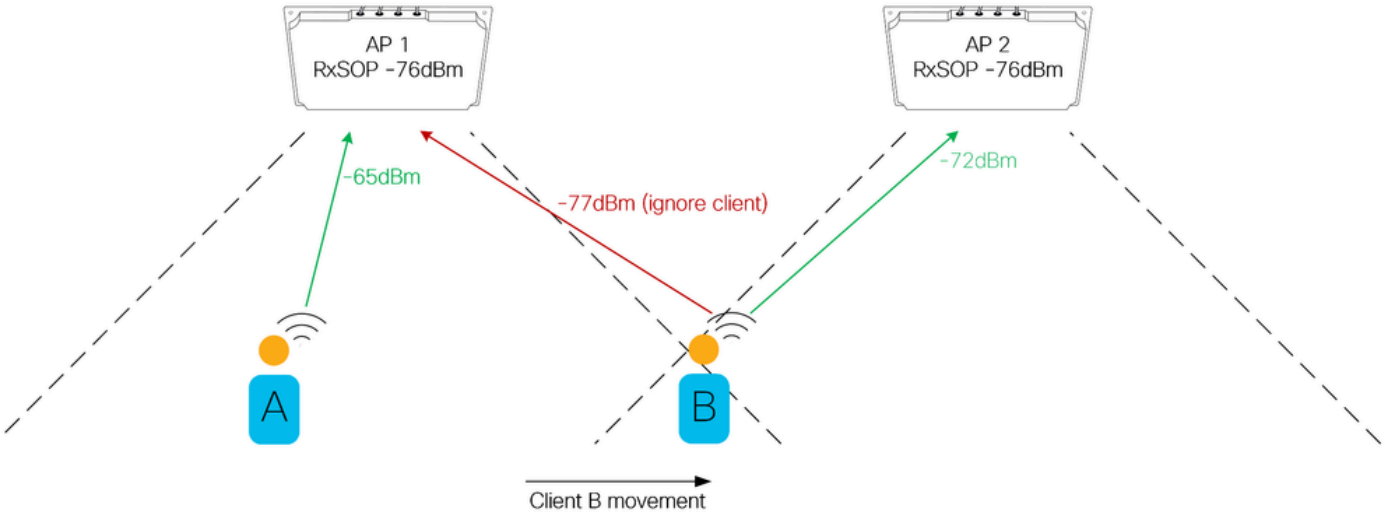
Concepto RxSOP explicado

La importancia de RxSOP

RxSOP tiene varios usos. Se puede utilizar para mejorar la capacidad de los AP para transmitir en entornos ruidosos, para controlar la distribución de clientes entre antenas, así como para optimizar para clientes más débiles y pegajosos.

En el caso de entornos ruidosos, recuerde que antes de transmitir una trama 802.11 la estación de transmisión (el AP en este caso) primero necesita evaluar la disponibilidad del medio, parte de este proceso es escuchar primero las transmisiones que ya están teniendo lugar. En entornos Wi-Fi densos, es común que muchos AP coexistan en un espacio relativamente limitado, a menudo utilizando los mismos canales. En tales entornos ocupados, el AP puede reportar la utilización del canal de los AP circundantes (incluyendo reflexiones) y retrasar su propia transmisión. Al establecer el umbral RxSOP apropiado, el AP puede ignorar esas transmisiones más débiles (reducción en la utilización del canal percibido) que conducen a una oportunidad de transmisión más frecuente y a un mejor rendimiento. Los entornos en los que los AP informan de una utilización significativa del canal (por ejemplo, > 10%) sin ninguna carga de cliente (por ejemplo, un lugar vacío) son buenos candidatos para el ajuste de RxSOP.

Para la optimización del cliente mediante RxSOP, considere este diagrama.



Roaming de clientes afectado por rxsop

En este ejemplo hay dos AP/antenas con áreas de cobertura bien definidas. El cliente B está pasando del área de cobertura del AP1 al área de cobertura del AP2. Hay un punto de cruce en el que AP2 escucha al cliente mejor que AP1, pero el cliente todavía no ha vagado a AP2. Este es un buen ejemplo de cómo configurar el umbral RxSOP puede forzar el límite del área de cobertura. Garantizar que los clientes estén siempre conectados al AP más cercano mejora el rendimiento al eliminar las conexiones de clientes distantes o débiles servidas a velocidades de datos más bajas. La configuración de los umbrales RxSOP de esta manera requiere una comprensión profunda de dónde comienza y termina el área de cobertura esperada de cada AP.

Los peligros de RxSOP.

Establecer el umbral RxSOP de manera demasiado agresiva resulta en agujeros de cobertura, ya que el AP no está decodificando transmisiones válidas de los dispositivos cliente válidos. Esto puede tener consecuencias adversas para el cliente ya que el AP no responde; después de todo, si la transmisión del cliente no fue escuchada no hay razón para responder. El ajuste de los umbrales RxSOP debe realizarse cuidadosamente, asegurándose siempre de que los valores configurados no excluyan a los clientes válidos dentro del área de cobertura. Tenga en cuenta que algunos clientes no pueden responder bien a ser ignorados de esta manera, las configuraciones RxSOP demasiado agresivas no le dan al cliente la oportunidad de vagar naturalmente, forzando efectivamente al cliente a encontrar otro AP. Un cliente que puede decodificar una baliza de un AP supone que puede transmitir a ese AP, por lo tanto, la intención del ajuste de RxSOP es hacer coincidir el tamaño de la celda de recepción con el rango de baliza del AP. Tenga en cuenta que un dispositivo cliente (válido) no siempre tiene una línea de visión directa hacia el AP, la señal es a menudo atenuada por los usuarios mirando hacia fuera de la antena o llevando sus dispositivos en bolsas o bolsillos.

Configuración de RxSOP

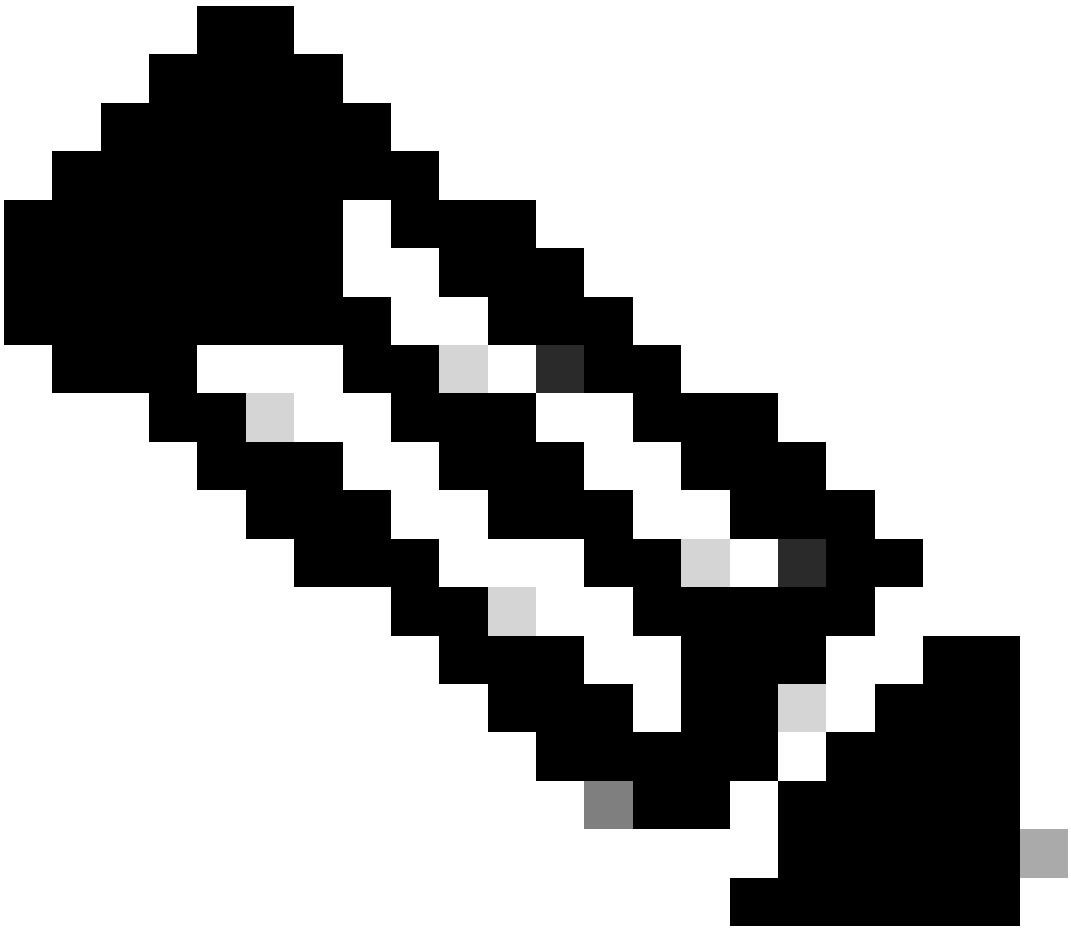
RxSOP está configurado por perfil de RF.

Para cada banda hay umbrales predefinidos (bajo/medio/alto) establecidos con un valor dBm predefinido. La recomendación aquí es utilizar siempre valores personalizados, incluso si el valor esperado es uno de los valores predefinidos disponibles, esto hace que la configuración sea más

legible.

Setting	Value
Auto	Not configured
Low	-80dBm
Medium	-78dBm
High	-76dBm
Custom	-60dBm to -85dBm

tabla de configuración de RxSop



Nota: Los cambios de RxSOP no requieren un reinicio de radio y se pueden realizar sobre la marcha.

Ampliación de la red

En general, utilizar un dispositivo al máximo de sus capacidades documentadas es una mala idea. Las hojas de datos informan la verdad, pero los números mencionados pueden estar en condiciones específicas de actividad. Los controladores inalámbricos se prueban y certifican para admitir un determinado número de clientes y puntos de acceso, y un cierto rendimiento, pero esto no supone que los clientes estén en roaming cada segundo, que pueda haber configurado ACL únicas extremadamente largas para cada cliente o habilitado todas las funciones de snooping disponibles. Por lo tanto, es importante tener en cuenta todos los aspectos con cuidado para garantizar que la red se amplíe durante las horas punta y también para mantener un margen de seguridad para el crecimiento futuro.

Número de puntos de acceso

Una de las primeras tareas a la hora de implementar cualquier red es presupuestar y solicitar la cantidad correcta de equipo, y el mayor factor variable es el número y el tipo de puntos de acceso y antenas. Las soluciones inalámbricas siempre deben basarse en un diseño de radiofrecuencia; sin embargo (y, por desgracia), a menudo este es el segundo paso en el ciclo de vida del proyecto. En el caso de las implementaciones sencillas de empresas en interiores, existen numerosas técnicas de estimación que pueden, con un nivel razonable de certeza, predecir cuántos puntos de acceso se pueden necesitar incluso antes de que un arquitecto inalámbrico examine los planos de planta. Los modelos predictivos también pueden ser muy útiles en este caso.

Para instalaciones más complejas, como redes industriales, exteriores, grandes redes públicas o cualquier lugar donde se necesiten antenas externas, las técnicas de estimación simple suelen ser inadecuadas. Se requiere cierto nivel de experiencia con instalaciones similares anteriores para estimar adecuadamente el tipo y la cantidad de equipo necesario. Una visita al sitio por parte de un arquitecto de tecnología inalámbrica es lo mínimo necesario para comprender el diseño de un lugar o instalación complejos.

Esta sección proporciona pautas sobre cómo determinar el número mínimo de APs y antenas para la implementación dada. Las cantidades finales y las ubicaciones de montaje específicas siempre se determinarán mediante un análisis de requisitos y un proceso de diseño de radio.

La lista de materiales inicial debe basarse en dos factores: el tipo de antenas y la cantidad de antenas.

Tipo de antenas

No hay atajos aquí. El tipo de antena viene determinado por el área que debe cubrirse y por las opciones de montaje disponibles en esa área. No es posible determinar esto sin comprender el espacio físico, lo que significa que alguien que conozca las antenas y sus patrones de cobertura

debe realizar una visita al sitio.

Cantidad de antenas

La cantidad de equipo necesario puede derivarse de la comprensión de la cantidad esperada de conexiones de cliente.

Dispositivos por persona

El número de usuarios humanos puede determinarse por el número de asientos de un lugar, o el número de entradas vendidas, o el número esperado de visitantes basado en estadísticas históricas. Cada usuario humano puede transportar varios dispositivos y es habitual suponer que hay más de un dispositivo por usuario, aunque la capacidad de un usuario humano para utilizar activamente varios dispositivos al mismo tiempo es cuestionable. El número de visitantes que se conectan activamente a la red también depende del tipo de evento o implementación.

Ejemplo 1: es normal que un estadio de 80 000 asientos no tenga 80 000 dispositivos conectados, este porcentaje suele ser significativamente inferior. Las proporciones de usuarios conectados del 20% no son infrecuentes durante los eventos deportivos, lo que significa que, para el ejemplo de un estadio con 80 000 asientos, el número esperado de dispositivos conectados puede ser de 16 000 (80 000 x 20% = 16 000). Este número también depende del mecanismo de onboarding utilizado; si se requiere que el usuario realice alguna acción (como hacer clic en un portal web), los números son menores que cuando la onboarding del dispositivo es automática. La incorporación automática puede ser tan sencilla como una PSK que se haya recordado de un evento anterior, o algo más avanzado como el uso de OpenRoaming que incorpora dispositivos sin interacción del usuario. Las redes de OpenRoaming pueden impulsar el índice de adopción de usuarios muy por encima del 50%, lo que puede tener un impacto significativo en la planificación de la capacidad.

Ejemplo 2: es razonable esperar que una conferencia tecnológica tenga una relación de conexiones de usuario alta. Los asistentes a la conferencia pasan más tiempo conectados a la red y esperan poder acceder a su correo electrónico y realizar tareas diarias a lo largo del día. También es más probable que este tipo de usuario conecte más de un dispositivo a la red, aunque su capacidad para utilizar varios dispositivos simultáneamente sigue siendo cuestionable. En el caso de las conferencias tecnológicas, se supone que el 100% de los visitantes se conectan a la red. Este número puede ser inferior en función del tipo de conferencia.

En ambos ejemplos, la clave está en comprender el número esperado de dispositivos conectados y no existe una solución única para cada red pública de gran tamaño. En cualquier caso, una antena se conecta a una radio y son los dispositivos cliente (no los usuarios humanos) los que se conectan a esa radio. Por lo tanto, los dispositivos cliente por radio son una métrica utilizable.

Dispositivos por radio

Los puntos de acceso de Cisco tienen un número máximo de clientes de 200 dispositivos conectados por radio para Wi-Fi 6 AP y 400 dispositivos por radio para Wi-Fi 6E AP. Sin embargo, no se recomienda diseñar para el número máximo de clientes. Para propósitos de planificación, se recomienda mantener el conteo de clientes por radio muy por debajo del 50% de la capacidad

máxima de AP. Además, el número de radios depende del tipo de AP y de antena utilizados, la sección de 5 GHz simple vs dual explora esto con más detalle.

En esta etapa, es una buena idea dividir la red en distintas áreas, con los recuentos de dispositivos esperados por área. Recuerde, esta sección tiene como objetivo estimar un número mínimo de AP y antenas.

Considere un ejemplo de tres áreas de cobertura distintas, se proporciona el conteo de clientes esperado para cada área y se utiliza un valor (saludable) de 75 clientes por radio para estimar el número de radios requeridas.

Area	Expected Devices	Devices / Radio	Radios
Area 1	1000	75	14
Area 2	2000	75	27
Area 3	2500	75	34
Total			75

Recuento esperado de radios/clientes por área

Estos números iniciales ahora deben combinarse con la comprensión de qué tipos de AP y antenas se implementan en cada área, y si se utiliza 5 GHz simple o dual. Los cálculos de 6 GHz siguen la misma lógica que los de 5 GHz. En este ejemplo no se tiene en cuenta la velocidad de 2,4 GHz.

Supongamos que cada una de las tres áreas utiliza una combinación de antena de interconexión 2566P y la antena de estadio 9104, con una combinación de 5 GHz individual y dual; este escenario se utiliza para ilustrar.

Area	Total Radios	2566P (Dual 5GHz)	2566P (Single 5GHz)	9104 (Dual 5GHz)
Area 1	14	0	6	4
Area 2	27	6	3	6
Area 3	34	7	0	10
Total Antennas		26	9	20
Total APs		13	9	0 (integrated)

Antenas por área

Cada área enumera el tipo de antenas y AP necesarios. Tenga en cuenta que en el caso de la dual 5GHz la relación es dos antenas a un AP.

Esta sección muestra un enfoque para estimar un número inicial de antenas y puntos de acceso necesarios para una implementación. La estimación requiere una comprensión de las áreas físicas, las posibles opciones de montaje en cada área, el tipo de antenas que se utilizarán en cada área y el número de dispositivos cliente previstos.

Cada despliegue es diferente y a menudo se necesita equipo adicional para cubrir áreas específicas o difíciles, este tipo de estimación solo tiene en cuenta la capacidad del cliente (no la cobertura) y sirve para esbozar la escala de la inversión necesaria. Las ubicaciones finales de colocación de AP/antena y los totales de equipos siempre están sujetos a un conocimiento exhaustivo del caso práctico y a la verificación in situ por parte de un profesional inalámbrico experimentado.

Rendimiento esperado

Cada canal inalámbrico puede ofrecer una cantidad de capacidad disponible que normalmente se traduce en rendimiento. Esta capacidad se comparte entre todos los dispositivos conectados a la radio, lo que significa que el rendimiento de cada usuario disminuye a medida que se agregan más conexiones de usuario a la radio. Este descenso en el rendimiento no es lineal y también depende de la combinación exacta de clientes conectados.

Las capacidades del cliente difieren entre los dispositivos en función del conjunto de chips del cliente y el número de secuencias espaciales que admite el cliente. Las velocidades de datos de cliente máximas para cada número de secuencias espaciales admitidas se enumeran en la tabla siguiente.

Client Capability	20MHz channel Wi-Fi 5 (802.11ac)	20MHz channel Wi-Fi 6 (802.11ax)
1 Spatial Stream(s)	86.7Mbps	121.9Mbps
2 Spatial Stream(s)	173.3Mbps	243.8Mbps
3 Spatial Stream(s)	288.9Mbps	365.6Mbps
4 Spatial Stream(s)	346.7Mbps	487.5Mbps

Rendimiento real máximo esperado para cada tipo de cliente

Las velocidades indicadas son velocidades máximas teóricas de MCS (Modulation and Coding Scheme, esquema de modulación y codificación) derivadas del estándar 802.11 y asumen una relación señal-ruido (SNR) >30 dBm. El principal objetivo de diseño de las redes inalámbricas de buen rendimiento es alcanzar este nivel de SNR para todos los clientes en todas las ubicaciones, aunque esto no suele suceder. Las redes inalámbricas son dinámicas por naturaleza y utilizan frecuencias sin licencia; varias interferencias no controladas tienen un impacto en el SNR del cliente, además de las capacidades del cliente.

Incluso en los casos en los que se alcanza el nivel requerido de SNR, las velocidades enumeradas anteriormente no tienen en cuenta la sobrecarga del protocolo, por lo tanto, no se asignan directamente al rendimiento real (medido por varias herramientas de prueba de velocidad). En el mundo real siempre es inferior a la tasa de MCS.

Para todas las redes inalámbricas (incluidas las grandes redes públicas), el rendimiento del cliente siempre depende de:

- Capacidades del cliente.
- Relación señal-ruido del cliente en ese momento específico.
- Número de otros clientes conectados en ese momento específico.
- Capacidades de otros clientes en ese momento específico.
- Actividad de otros clientes en ese momento específico.
- Interferencia en ese momento específico.

En función de la variabilidad de estos factores, no es posible garantizar un mínimo por cliente para las redes inalámbricas, independientemente del proveedor del equipo.

Para obtener más información, consulte la Guía de validación del rendimiento Wi-Fi: pruebas y supervisión.

Plataforma WLC

Elegir su plataforma del WLC puede parecer fácil. Lo primero en lo que puede pensar es en mirar

el conteo estimado de AP y el conteo de clientes que pretende administrar. La hoja de datos para cada plataforma WLC contiene todos los objetos máximos soportados en la plataforma: ACL, conteo de clientes, etiquetas de sitio, etc. Son números máximos literales y a menudo hay una aplicación estricta. No puede unir 6001 AP a un 9800-80 que soporta solamente 6000 AP, por ejemplo. Pero, ¿es prudente buscar el máximo en todas partes?

Los controladores inalámbricos de Cisco se han probado para poder alcanzar esos máximos, pero no necesariamente pueden alcanzar todos los máximos documentados en todas las condiciones al mismo tiempo. Veamos el ejemplo del rendimiento: un 9800-80 puede alcanzar hasta 80 Gbps de reenvío de datos de cliente, pero esto sucede cuando cada paquete de cliente tiene el tamaño máximo y óptimo de 1500 bytes. Con una mezcla de tamaños de paquete, el rendimiento máximo efectivo es menor. Si habilita el cifrado DTLS, el rendimiento se reduce aún más, y lo mismo sucede con la visibilidad de la aplicación. Es optimista esperar más de 40 Gbps de un 9800-80 en condiciones realistas en una red de gran tamaño con muchas funciones activadas. Dado que esto varía mucho según las características en uso y el tipo de actividad de la red, la única manera de tener una idea real de la capacidad es medir la utilización de la ruta de datos mediante este comando. Céntrese en la métrica de carga, que es un porcentaje del rendimiento máximo que el controlador puede reenviar.

```
WLC#show platform hardware chassis active qfp datapath utilization summary

  CPP 0:                      5 secs        1 min        5 min       60 min

Input:     Total (pps)            9            5            5            8

                  (bps)        17776         7632         9024        10568

Output:    Total (pps)            5            3            3            6

                  (bps)        11136        11640        11440        41448

Processing: Load (pct)            0            0            0            0


WLC#
```

De manera similar, el 9800-80 puede manejar perfectamente 6000 AP con actividad regular. Sin embargo, 6000 AP en un lugar público como un estadio o un aeropuerto no cuentan como actividad regular. Teniendo en cuenta la cantidad de roaming del cliente y sondeo del ambiente, las redes públicas de gran tamaño a escala máxima pueden causar un mayor uso de la CPU en un solo WLC. Si agrega trampas de monitoreo y SNMP que se enviarán cada vez que los clientes se mueven, la carga puede convertirse rápidamente en demasiado. Una de las características clave de un gran evento o un gran evento público es que hay muchos más eventos de incorporación de clientes a medida que las personas se mueven y se asocian/disocian constantemente, por lo que esto provoca una presión adicional sobre la CPU y el plano de control.

Numerosas implementaciones han demostrado que un solo par (HA) de controladores

inalámbricos 9800-80 puede gestionar una gran implementación en un estadio con más de 1000 puntos de acceso. También es común distribuir los AP en dos o más pares de controladores para eventos críticos donde el tiempo de actividad y la disponibilidad son preocupaciones principales. Cuando las redes grandes se distribuyen sobre los WLC múltiples existe la complejidad adicional del roaming entre los controladores, el roaming del cliente se debe considerar cuidadosamente en espacios confinados tales como un tazón del estadio.

Consulte también la sección Etiqueta del sitio en este documento.

WLC de alta disponibilidad

Se recomienda utilizar un par de conmutación stateful de alta disponibilidad (HA SSO), que proporciona redundancia de hardware y protege frente a fallos de software. Con HA SSO, un desperfecto del software en un dispositivo es transparente para los usuarios finales como el WLC secundario toma el control sin problemas. Otra ventaja de un par HA SSO son las actualizaciones sin impacto que ofrece la función In-Service Software Upgrade (ISSU).

Si la red es lo suficientemente grande, también se recomienda utilizar un controlador adicional (N+1). Puede servir a varios propósitos que el HA SSO no puede cumplir. Puede probar una nueva versión de software en este WLC antes de actualizar el par de producción (y migrar solo unos pocos AP de prueba para probar una sección específica de la red). Algunas condiciones poco comunes pueden afectar tanto a los WLC en un par HA (cuando el problema se replica en el standby) y aquí el N+1 permite tener un WLC seguro en un escenario activo-activo donde usted podría migrar progresivamente los AP hacia y desde. También podría servirle como controlador de aprovisionamiento para configurar nuevos AP.

Los 9800-CL son muy escalables y potentes. Cabe destacar que tienen una capacidad de reenvío de datos mucho menor (de 2 Gbps a 4 Gbps para la imagen SR-IOV), lo que tiende a restringirlos a los escenarios de switching local de FlexConnect (y posiblemente a un pequeño número de AP en switching central). Sin embargo, pueden ser útiles como dispositivos N+1 cuando necesite controladores adicionales durante una ventana de mantenimiento o cuando resuelva un problema.

Sistemas externos

Si bien este documento se centra principalmente en el componente inalámbrico de las redes de eventos grandes, también hay numerosos sistemas de apoyo que requieren consideración durante la fase de escalado y diseño, algunos de ellos se discuten aquí.

Red principal

Las redes inalámbricas de gran tamaño se suelen implementar en modo de switching central y con subredes de gran tamaño. Esto implica que un gran número de entradas ARP y direcciones MAC de cliente se envían a la infraestructura cableada adyacente. Es fundamental que los sistemas adyacentes dedicados a las diversas funciones L2 y L3 posean los recursos adecuados para manejar esta carga. En el caso de los switches L2, una configuración común es el ajuste de la plantilla del administrador de dispositivos del switch (SDM), que es responsable de la asignación de los recursos del sistema, equilibrando las funciones L2 y L3 en función de la

función del dispositivo dentro de la red. Es importante asegurarse de que los dispositivos de núcleo L2 puedan admitir el número de entradas de dirección MAC esperado.

NAT de gateway

El caso práctico más común de las redes públicas es proporcionar acceso a Internet a los visitantes. En algún punto de la ruta de datos debe haber un dispositivo responsable de la traducción NAT/PAT. Los gateways de Internet deben poseer los recursos de hardware y la configuración del conjunto de IP necesarios para gestionar la carga. Recuerde que un único dispositivo cliente inalámbrico puede ser responsable de numerosas traducciones NAT/PAT.

DNS/DHCP

Estos dos sistemas son clave para garantizar una buena experiencia del cliente. Tanto los servicios DNS como DHCP requieren no solo el escalado adecuado para gestionar la carga, sino también consideración con respecto a la ubicación dentro de la red. Sistemas rápidos y receptivos, colocados en la misma ubicación que el WLC asegura la mejor experiencia y evitar largos tiempos de incorporación del cliente.

AAA/portal web

A nadie le gusta una página web lenta, la elección de un sistema adecuado y bien escalado para la autenticación web externa es importante para una buena experiencia de incorporación del cliente. Del mismo modo que para AAA, los servidores de autenticación RADIUS deben ser capaces de satisfacer las demandas del sistema inalámbrico. Tenga en cuenta que, en algunos casos, la carga puede aumentar en momentos clave, por ejemplo, la mitad del tiempo durante un partido de fútbol, lo que puede generar una carga de autenticación alta en una pequeña cantidad de tiempo. La escalabilidad del sistema para una carga concurrente adecuada es clave. Se debe tener especial cuidado al utilizar funciones como la contabilidad AAA. Evite la contabilidad basada en tiempo a toda costa y, si utiliza la contabilidad, intente desactivar la contabilidad provisional. Otro elemento importante a considerar es el uso de balanceadores de carga, donde se deben utilizar mecanismos de anclaje de sesión para garantizar flujos de autenticación completos. Asegúrese de mantener el tiempo de espera RADIUS en 5 segundos o más.

Si utiliza un SSID 802.1X con un gran número de clientes (por ejemplo, con OpenRoaming), asegúrese de activar 802.11r Fast Transition (FT); de lo contrario, los clientes pueden provocar una tormenta de autenticación cada vez que se desplazan.

DNS/DHCP

Algunas recomendaciones para DHCP:

- Asegúrese de que el conjunto DHCP sea al menos tres veces el número de clientes esperado. Las IP permanecen asignadas durante algún tiempo incluso después de que el cliente se desconecte, por lo que dependiendo del tiempo de permanencia de los invitados esto puede consumir más direcciones IP. Intente que el tiempo de concesión coincida con la duración esperada de la visita del usuario al lugar de celebración de eventos. No tiene sentido asignar una dirección IP para una semana si la duración típica de una visita es de

dos horas, esto ayuda a eliminar los arrendamientos obsoletos.
- Se recomienda el uso de una sola subred grande para los clientes, el WLC tiene una función ARP proxy y no reenvía las difusiones por defecto (que no sea DHCP). El uso de una subred de cliente grande (por ejemplo, /16) para los clientes no representa un problema. Una sola VLAN grande es más sencilla en comparación con un grupo de VLAN con muchas VLAN. La configuración de muchas subredes más pequeñas (por ejemplo /24) y grupos de VLAN no influye en el dominio de broadcast y solo resulta en una configuración más complicada, lo que resulta en problemas como VLAN sucias y tener que realizar un seguimiento de varios agrupamientos DHCP que no se pueden utilizar uniformemente.
- Mantenga DHCP en modo de puente en el controlador inalámbrico con la funcionalidad de relé DHCP manejada por el gateway de Capa 3 de la subred. Esto permite una eficacia y simplicidad máximas. La idea es no tener el controlador inalámbrico involucrado en el proceso DHCP.
- Use DHCP Required en cualquier WLAN pública, independientemente del método de autenticación. Aunque esto puede desencadenar un pequeño porcentaje de asociaciones de clientes fallidas, podría evitar problemas de seguridad significativos, ya sea por parte de los clientes que intentan asignarse direcciones IP estáticas o por clientes que se comportan mal e intentan reutilizar una dirección IP anterior sin permiso.

Funcionamiento de la red

La configuración adecuada

Es tentador habilitar una gran cantidad de opciones para beneficiarse de todas las características más recientes de la Wi-Fi moderna. Sin embargo, algunas funciones funcionan muy bien en entornos pequeños, pero tienen un gran impacto en entornos grandes y densos. Del mismo modo, algunas características pueden plantear problemas de compatibilidad. Aunque el equipo de Cisco respeta todos los estándares y ofrece compatibilidad con una amplia variedad de clientes probados, el mundo está lleno de dispositivos cliente únicos que a veces tienen versiones de software de controlador con errores o incompatibilidad con ciertas funciones.

Dependiendo del nivel de control que tenga sobre los clientes, debe ser conservador. Por ejemplo, si implementa la red Wi-Fi para la gran reunión anual de su empresa, sabrá que la mayoría de los clientes son dispositivos de la empresa y podrá planificar el conjunto de funciones para que se habilite en consecuencia. Por otro lado, si utiliza una conexión Wi-Fi de aeropuerto, el nivel de satisfacción de los invitados está directamente relacionado con su capacidad para conectarse a la red y no tiene ningún tipo de control sobre los dispositivos cliente que las personas pueden utilizar.

SSID

¿Cuántos SSID?

La recomendación siempre ha sido utilizar el menor número posible de SSID. Esto se agrava en las redes de alta densidad ya que la posibilidad de tener varios AP en el mismo canal está casi garantizada. Normalmente, muchas implementaciones utilizan demasiados SSID, reconocen que

tienen demasiados SSID, pero declaran que no pueden utilizar menos. Debe realizar un estudio técnico y empresarial de cada SSID para comprender las similitudes entre los SSID y las opciones para contraer varios SSID en uno solo.

Veamos algunos tipos de seguridad/SSID y su uso.

WPA2/3 Personal

Un SSID de clave precompartida es inmensamente popular debido a su simplicidad. Puede imprimir la clave en algún lugar en insignias o en papel o carteles o comunicársela de alguna manera a los visitantes. A veces, incluso para un SSID de invitado, se prefiere un SSID de clave previamente compartida (siempre que todos los asistentes conozcan bien la clave). Puede ayudar a evitar el agotamiento del conjunto DHCP debido a la naturaleza deliberada de la conexión. Los dispositivos que pasan no se conectan automáticamente a la red, por lo que no pueden consumir una dirección IP del conjunto DHCP.

WPA2 PSK no proporciona privacidad, ya que el tráfico se puede descifrar fácilmente, ya que todos los usuarios utilizan la misma clave. Por el contrario, WPA3 SAE proporciona privacidad, e incluso si todos tienen la clave maestra, no es posible derivar la clave de cifrado utilizada por otros clientes.

WPA3 SAE es la mejor opción para la seguridad y muchos smartphones, ordenadores portátiles y sistemas operativos la admiten. Algunos dispositivos de IoT o dispositivos portátiles inteligentes pueden seguir teniendo una compatibilidad limitada y los clientes más antiguos en general son susceptibles de sufrir problemas si no han recibido controladores o actualizaciones de firmware recientes.

Puede ser tentador considerar un modo de transición WPA2 PSK-WPA3 SAE SSID para simplificar las cosas, pero esto se ha demostrado en el campo para causar algunos problemas de compatibilidad. Los clientes mal programados no esperan dos tipos de métodos de clave compartida en el mismo SSID. Si desea ofrecer las opciones WPA2 y WPA3, se recomienda configurar SSID independientes.

WPA2/3 Enterprise

WPA3 Enterprise (con encriptación AES de 128 bits) es técnicamente el mismo método de seguridad (al menos como se anuncia en las balizas SSID) que WPA2 Enterprise, que proporciona la máxima compatibilidad.

Para 802.1X, se recomienda un SSID de modo de transición, ya que no se observan problemas de compatibilidad con dispositivos recientes (se han notificado problemas con Android 8 o con versiones antiguas de Apple IOS). IOS XE 17.12 y versiones posteriores permiten tener un único SSID empresarial de transición en el que solo se utiliza y anuncia WPA3 en 6 GHz, mientras que WPA2 se ofrece como opción en la banda de 5 GHz. Recomendamos habilitar WPA3 en los SSID empresariales lo antes posible.

Los SSID de WPA Enterprise se pueden utilizar para los usuarios clave para los que existe una base de datos de proveedor de identidad que permite devolver parámetros AAA (como VLAN o

ACL) en función de la identidad del usuario. Estos tipos de SSID pueden incluir eduroam o OpenRoaming que combinan las ventajas de los SSID de invitados (permitiendo a los visitantes conectarse fácilmente sin introducir ninguna credencial) con la seguridad de un SSID corporativo. Reducen en gran medida la complejidad de la incorporación asociada normalmente a 802.1X, ya que los clientes no tienen que hacer nada para unirse al eudroam o al SSID de OpenRoaming, siempre que tengan un perfil en el teléfono (que se puede proporcionar fácilmente a través de una aplicación de eventos)

SSID de invitado

Un SSID de invitado suele ser sinónimo de autenticación abierta. Puede agregar un portal web (o no) detrás de él (en función de la facilidad deseada o los requisitos locales) en sus diversas formas: autenticación web externa, local o central, pero el concepto sigue siendo el mismo. Al utilizar un portal de invitados, la escalabilidad puede convertirse rápidamente en un problema en entornos de gran tamaño. Consulte la sección Configuración para Escalabilidad para obtener más información al respecto.

Las operaciones de 6 GHz requieren que el SSID de invitado utilice la función de apertura mejorada en lugar de la función de apertura. De este modo, se puede conectar a cualquier usuario, pero se proporciona privacidad (incluso mejor que con WPA2-PSK) y cifrado, todo ello sin proporcionar ninguna clave ni credenciales al conectarse al SSID. Los principales proveedores de smartphones y sistemas operativos admiten ahora Enhanced Open, pero la compatibilidad aún no está muy extendida en la base de clientes inalámbricos. El modo de transición de apertura mejorada proporciona una buena opción de compatibilidad en la que los dispositivos compatibles se conectan al SSID de invitado cifrado (mediante la función de apertura mejorada), y los dispositivos que no son compatibles siguen utilizando el SSID como simplemente abierto como antes. Aunque los usuarios finales solo detectan un SSID, tenga en cuenta que este modo de transición difunde dos SSID en las balizas (aunque solo uno está visible).

En grandes eventos y lugares, a menudo se recomienda configurar un PSK en el SSID de invitado en lugar de dejarlo puramente abierto (sería mejor mejorar el modo de transición abierta, pero eso crea dos SSID y la compatibilidad con el cliente aún debe probarse exhaustivamente). Aunque esto hace que la incorporación sea un poco más complicada (debe imprimir la PSK en los distintivos o tickets de las personas o anunciarla de algún modo), evita que los clientes ocasionales se conecten a la red automáticamente sin que el usuario final tenga intención de utilizar la red. Cada vez más proveedores de sistemas operativos móviles también eliminan las prioridades de las redes abiertas y muestran una advertencia de seguridad. En otras situaciones, puede desear un número máximo de transeúntes para conectar y, por lo tanto, abrir es la mejor opción.

Conclusión sobre el número de SSID

No puede haber una respuesta satisfactoria a la pregunta de a cuántos SSID debe adherirse. El efecto depende de la velocidad de datos configurada mínima, el número de SSID y el número de AP que transmiten en el mismo canal. En un gran evento de Cisco, la infraestructura inalámbrica utilizó 5 SSID: el principal WPA2 PSK, un SSID WPA 3 SAE para la seguridad y la cobertura de 6

GHz, un SSID Eduroam empresarial para facilitar el acceso a los asistentes educativos, un SSID OpenRoaming para dar la bienvenida de forma segura a cualquiera que haya configurado Wi-Fi desde la aplicación del evento y un SSID 802.1X independiente para el personal y el acceso a la red de administración. Esto ya era demasiado, pero el efecto seguía siendo razonable gracias al gran número de canales disponibles y a las antenas direccionales utilizadas para reducir el solapamiento de canales tanto como fuera posible.

Conceptos de SSID heredado frente a SSID principal

Durante un período determinado, se aconsejó restringir el servicio de 2,4 GHz a un SSID separado "heredado" que solo se anunciaba en 2,4 GHz. Esto es cada vez menos popular, ya que la gente deja de proporcionar el servicio de 2,4 GHz por completo. Sin embargo, la idea puede y debe persistir pero con otros conceptos. ¿Desea implementar WPA3 SAE, pero el modo de transición le está dando problemas de compatibilidad con sus clientes? Disponen de un SSID WPA2 "heredado" y un SSID WPA3 SAE principal. Al nombrar el SSID de menor rendimiento como "heredado", no atrae a los clientes y puede ver fácilmente cuántos clientes siguen teniendo problemas de compatibilidad con su SSID principal y requieren este SSID heredado.

Pero, ¿por qué parar ahí? ¿Ha oído rumores de que 802.11v causaba problemas con algunos clientes más antiguos o de que a algunos controladores de clientes no les gusta ver el análisis de dispositivos habilitado en el SSID? Active todas esas útiles funciones en su SSID principal avanzado y déjelas desactivadas en su SSID heredado/de compatibilidad. Esto le permite probar la implementación de nuevas funciones en su SSID principal, a la vez que proporciona un SSID de máxima compatibilidad para que los clientes recurran a él. Este sistema sólo funciona de esta manera. Si utiliza el nombre opuesto de SSID basado en la compatibilidad como principal y asigna a su SSID avanzado un nombre como "<name>-WPA3", observará que las personas se adhieren al antiguo SSID al que estaban acostumbradas y que la adopción se mantiene pequeña durante muchos años en el "nuevo" SSID. La implementación de nuevas configuraciones o funciones no tiene resultados concluyentes debido al menor número de clientes que se conectan a ellas.

Funciones de SSID

- Es mejor mantener las extensiones Aironet inhabilitadas. Estos son especialmente útiles para los estudios de sitio y las operaciones de WGB, pero a veces causan problemas con algunos clientes heredados. Aironet IE también anuncia el nombre de host AP que no es deseado en las implementaciones conscientes de la seguridad.
- CCKM es un protocolo obsoleto (a favor de FT) y debe desactivarse.
- En este momento, es mejor utilizar el cifrado AES-128, incluso en WPA3, debido a la baja compatibilidad del cliente con cifrados más altos (a menos que pueda permitirse un SSID específico más seguro y restrictivo)
- La detección de taladros de cobertura es mejor que esté desactivada (para todos los SSID). Las implementaciones de gran tamaño suelen utilizar antenas direccionales, por lo que se requiere un completo estudio del sitio. Los niveles de potencia de cada antena serían el resultado del proceso de diseño de radiofrecuencia y normalmente se configurarían en niveles específicos.

- La FT adaptativa debe estar deshabilitada, ya que algunos clientes pueden tener problemas cuando FT no está totalmente anunciado pero está presente en algunos atributos. Deshabilite completamente FT (para una compatibilidad máxima) o utilice FT+802.1X, que la mayoría de los clientes (a menos que sean antiguos o estén más orientados a IoT) admiten. Al configurar FT+802.1X, incluso los clientes que no son FT pueden unirse al SSID. El único problema posible es con algunos clientes que no tolerarían ver dos opciones de seguridad en el mismo SSID.
- Desactive 802.11ac MU-MIMO. Añade complejidad y tiene muy pocas ventajas en 802.11ac.
- Inhabilite el tiempo de activación de destino de BSS. En la actualidad, su adopción es baja en el lado del cliente.
- Inhabilite el balanceo de carga agresivo y la selección de banda. La selección de la banda no es necesaria si no anuncia el SSID en 2.4GHz (o si está en un SSID dedicado) y el balanceo de carga agresivo retrasa la asociación del cliente rechazando al cliente un par de veces antes de aceptarlo finalmente si insiste en conectarse a un AP cargado. De todos modos, ha cargado AP en un entorno ocupado y esto es negativo para la experiencia del cliente.
- Desactive Fastlane+.
- Inhabilite la administración universal, esta función era para el AP 3700 y solamente en el dominio -UX. Dejándolo encendido deja abierto un vector de ataque innecesario.
- Mantenga activado el almacenamiento en caché de claves oportunista (OKC). Sirve como mecanismo de itinerancia rápida para los clientes que no soportan FT.
- Mantenga WMM permitido. Si se desactiva, la red volvería a la era de 802.11g y su uso no supondría ninguna ventaja en la plataforma 9800.
- Active IP Source Guard.
- Inhabilite la creación de perfiles RADIUS. En un entorno muy ocupado, esto puede enviar demasiados mensajes de contabilización RADIUS (siempre que los clientes hagan DHCP o envíen paquetes HTTP) y tiene un potencial muy real de sobrecargar su servidor RADIUS.
- Evite utilizar SSID ocultos. Esto no sirve para ningún propósito de seguridad, el nombre de SSID todavía se puede descubrir fácilmente con aplicaciones simples o tomando una captura de sabueso. Al ocultar el SSID se ralentiza el roaming de todos los clientes, ya que ya no se benefician del escaneo de baliza pasivo y deben confiar en el escaneo activo para obtener la información de AP vecino.
- Intente no utilizar más de cuatro WLAN por radio, ya que tiene un impacto significativo en la utilización de RF. No es un límite difícil, el uso de cinco WLAN puede funcionar, pero ser muy consciente del tiempo de aire desperdiciado mediante el uso de más y más WLAN.
- Los estándares 802.11v y 802.11k son cada vez más compatibles con los tipos de clientes más habituales. Por lo general, no plantean ningún problema con respecto a la conexión del cliente. Las ventajas que aportan dependen en gran medida de cómo los clientes utilizan esos protocolos y, en ocasiones (en el caso de 802.11k), pueden provocar un uso ligeramente mayor de la CPU. Puede mantenerlos fuera de su IoT o SSID heredado, pero deben estar habilitados si es posible en su SSID de producción.

Etiqueta del sitio

Las etiquetas del sitio son un elemento de configuración que permite agrupar los puntos de

acceso que comparten la misma configuración de FlexConnect, así como la configuración del perfil de unión al punto de acceso (como las credenciales, los detalles de SSH y el código de país). ¿Por qué son importantes las etiquetas del sitio? Las etiquetas del sitio también definen cómo los AP son manejados por el proceso WNCD dentro del Catalyst 9800. Veamos algunos ejemplos para ilustrar lo siguiente:

- Si configura cuatro etiquetas de sitio en un 9800-80 que tiene ocho procesos WNCD, cada etiqueta de sitio se asigna a un proceso WNCD diferente (ejecutando cada uno en un núcleo de CPU separado) y cuatro procesos WNCD no hacen nada. Esto significa que no está utilizando todas las CPU de su 9800-80 y no se recomienda cargarlo con el máximo de 6000 AP soportados.

Site tag 1	Site tag 2	Site tag 3	Site tag 4	-	-	-	-
WNCD 1	WNCD 2	WNCD 3	WNCD 4	WNCD 5	WNCD 6	WNCD 7	WNCD 8
CPU	CPU	CPU	CPU	CPU	CPU	CPU	CPU

Primer ejemplo de equilibrio de etiquetas de sitio

- Si configura 10 etiquetas laterales en un 9800-80 que tiene ocho procesos WNCD, dos procesos WNCD se encargan de dos etiquetas de sitio cada uno, mientras que los seis restantes se encargan de una etiqueta de sitio cada uno.

Site tag 1 Site tag 9	Site tag 2 Site tag 10	Site tag 3	Site tag 4	Site tag 5	Site tag 6	Site tag 7	Site tag 8
WNCD 1	WNCD 2	WNCD 3	WNCD 4	WNCD 5	WNCD 6	WNCD 7	WNCD 8
CPU	CPU	CPU	CPU	CPU	CPU	CPU	CPU

Segundo ejemplo de balance de etiquetas de sitio

En el caso de implementaciones geográficamente grandes con muchos sitios y muchas etiquetas de sitios, se recomienda que el número de etiquetas de sitios sea un múltiplo del número de procesos WNCD de la plataforma que esté utilizando.

Sin embargo, en el caso de redes de eventos que suelen estar bajo un mismo techo o varios edificios en el mismo lugar, se recomienda hacer coincidir el número de etiquetas de sitio con el número exacto de WNCD de la plataforma en cuestión. El objetivo final es que cada proceso WNCD (y, por lo tanto, cada núcleo de CPU asignado a tareas inalámbricas) gestione un número más o menos similar de eventos de itinerancia del cliente, de modo que la carga esté equilibrada en todos los núcleos de CPU.

Platform type	Number of WNCD processes
9800-CL small OVA	1
9800-CL medium OVA	3
9800-CL large OVA	7
9800-L	1
9800-40/CW9800-M	5
9800-80/CW9800-H	8

Número de procesos WNCD para cada tipo de plataforma

En el núcleo, lo que realmente importa es agrupar los AP que están en el mismo vecindario físico en la misma etiqueta de sitio, de modo que los eventos de roaming de cliente frecuentes entre estos AP permanezcan en el mismo proceso de CPU. Esto significa que incluso si tiene un solo lugar grande, se recomienda dividir el lugar en varias etiquetas de sitio (tantos como tenga procesos WNCD que gestionan el lugar) y agrupar los AP de la forma más lógica posible en estos para formar grupos de vecindarios de RF lógicos que también se distribuyan uniformemente entre las etiquetas de sitio.

A partir de IOS XE 17.12, se puede habilitar un algoritmo de balanceo de carga para que el WLC agrupe los AP en función de su proximidad de RF. Esto quita la carga de sus manos y crea una distribución equilibrada de los APs a través del proceso WNCD. Esto puede ser útil si no puede dibujar fácilmente grupos de AP vecinos para colocarlos en la cantidad correcta de etiquetas de sitio. Una especificidad de este algoritmo es que asigna los AP al proceso WNCD independientemente de su asignación de la etiqueta del sitio, esto significa que no cambia la asignación de la etiqueta del sitio del AP. A continuación, puede asignar etiquetas de sitio puramente básicas en una lógica de configuración y dejar que el algoritmo equilibre los AP a través de las CPU de la manera más óptima.

La función de Balanceo de Carga de AP Automático basado en RF se documenta en la Guía de Configuración del Software del Controlador Inalámbrico Cisco Catalyst 9800 Series, Cisco IOS XE Dublin 17.12.x.

El uso de la CPU de los procesos WNCD se debe supervisar durante eventos de gran tamaño. Si uno o más procesos WNCD muestran una utilización alta, puede ser que el WNCD esté manejando demasiados AP o clientes, o que los AP o clientes que maneja estén más ocupados que el promedio (si todos ellos vagan constantemente, como en un aeropuerto, por ejemplo).

Perfil de política

- Habilitar ARP y el Proxy de la detección de direcciones duplicadas (DAD), esto permite que el WLC responda en nombre de los clientes inalámbricos cuando un dispositivo está intentando aprender la dirección MAC de un dispositivo inalámbrico. Esto también ahorra

baterías de clientes inalámbricos.
- No habilite las funciones de WGB a menos que sea necesario.
- Active DHCP necesario para evitar clientes con direcciones IP estáticas.
- Mantenga idle-timeout corto (300 segundos). Algunos administradores tardan mucho en evitar que los clientes tengan que volver a autenticarse, pero el tiempo de espera de inactividad prolongado provoca entradas de clientes fantasma (lo que afecta a los informes) a medida que el recuento de clientes se retrasa en tiempo real. Es mejor mantener el tiempo de espera inactivo menor que el temporizador de rotación de clave de grupo para evitar inundaciones de cuentas cuando se eliminan los clientes. El intervalo de rotación de clave de grupo se puede configurar en la interfaz de usuario web en Configuration > Security > Advanced EAP como "EAP-Broadcast Key Interval" (Intervalo de clave de difusión de EAP)
- Haga que el tiempo de espera de la sesión sea de 86400 segundos para evitar desconexiones y reautenticaciones innecesarias.

Perfil de unión a PA

- Asegúrese de que TCP adjust MSS esté habilitado.
- Habilite Trust DSCP upstream. Por desgracia, muchos clientes inalámbricos no realizan etiquetado WMM UP 802.11e. Confiar en el campo DSCP es una forma segura de proporcionar la prioridad adecuada a las aplicaciones de voz.
- Active Syslog para sus puntos de acceso. La configuración de una IP del servidor Syslog hace que los AP unicast sus registros de la consola a él. No solo es útil para resolver problemas de AP, sino que también es mejor para la red que la configuración predeterminada que hace que los AP difundan su Syslog en la VLAN local. El registro de AP puede generar una carga significativa de mensajes, incluso en los casos en los que no se monitorea el Syslog de AP, sigue siendo una buena idea limitar el número de eventos estableciendo la gravedad de mensaje apropiada y/o configurando una dirección IP de Syslog ficticia (por ejemplo, 0.0.0.0) para evitar que se transmitan mensajes.
- Maximice los reintentos CAPWAP y el tiempo de espera. Los problemas se detectan con menos rapidez, pero la red es más resistente a las caídas de paquetes transitorios menores.
- Habilite SSH y configure las credenciales. Inhabilite la consola AP.
- Habilite el monitor AP si es necesario pero no el monitor de radio.
- Active la detección de elementos no fiables y configure un umbral RSSI de -70 dBm.

Supervisión de la red

Una vez que la red está en funcionamiento, debe supervisarla estrechamente para detectar posibles problemas. En un entorno de oficina estándar, los usuarios conocen la red y pueden ayudarse entre sí en caso de problemas o abrir un ticket de soporte interno. En un lugar más grande con muchos visitantes vienen que desea centrarse en los problemas más grandes en lugar de individuos específicos que solo puede tener una configuración errónea, por lo que necesita tener la estrategia de supervisión correcta.

Es posible supervisar la red desde la CLI o la GUI de Catalyst 9800, pero no es la mejor herramienta que se puede supervisar a diario. Es el más directo cuando ya tienes sospechas y/o datos sobre el problema y quieres ejecutar comandos específicos en tiempo real. Las principales

opciones de supervisión son Cisco Catalyst Center o, potencialmente, un panel de telemetría personalizado. Es posible utilizar herramientas de supervisión de terceros, pero cuando éstas utilizan SNMP como protocolo, los datos distan mucho de ser en tiempo real y las herramientas de supervisión habituales de terceros no son lo suficientemente granulares con todas las especificidades de los proveedores inalámbricos. Si elige el protocolo SNMP, asegúrese de utilizar SNMPv3, ya que SNMPv2 tiene una seguridad obsoleta.

Cisco Catalyst Center es la mejor opción, ya que le permite administrar la red además de supervisarla. Además de la supervisión, también permite solucionar problemas en tiempo real y solucionar muchas situaciones.

Un panel de telemetría personalizado puede ser útil si desea mostrar métricas y widgets muy específicos en una pantalla de forma siempre activa para un NOC o SOC. Si hay áreas muy específicas de la red que desea vigilar, puede crear widgets dedicados para mostrar las métricas de red en esas áreas de la forma que prefiera.

Para las redes de eventos, es una buena idea monitorear las estadísticas de RF de todo el sistema, en particular la utilización del canal y el número de clientes por AP. Esto se puede hacer desde la CLI, pero solo proporciona una instantánea en un momento específico, el uso del canal tiende a ser dinámico y es más adecuado para la supervisión a lo largo del tiempo. Para este tipo de supervisión, un panel personalizado suele ser un buen enfoque. Otras métricas que son más valiosas cuando se supervisan a lo largo del tiempo pueden incluir la utilización de WNCD, el número de clientes y sus estados, y las métricas específicas de los lugares. Un ejemplo de indicadores específicos de un lugar de celebración de eventos sería el control del uso o la carga de un área o ubicación específica, por ejemplo, el salón X en el caso de un centro de conferencias, o el área de asientos Y en el caso de un lugar de celebración de eventos.

Para la supervisión personalizada, tanto NETCONF RPC (pull) como NETCONF streaming telemetry (push) son enfoques válidos, aunque el uso de la telemetría de transmisión personalizada junto con Catalyst Center requiere cierta diligencia, ya que hay un límite en el número de suscripciones de telemetría que se pueden configurar en el WLC y Catalyst Center rellena previamente (y utiliza) muchos de estos.

Cuando se utiliza NETCONF RPC, se requieren algunas pruebas para garantizar que el WLC no esté sobrecargado con solicitudes NETCONF, lo que es especialmente importante tener en cuenta son las tasas de actualización para algunos de los puntos de datos y el tiempo que se tarda en devolver los datos. Por ejemplo, el uso del canal AP se actualiza (de AP a WLC) cada 60 segundos, y la recolección de las métricas de RF para 1000 AP (de WLC) puede tomar varios segundos, en este ejemplo el sondeo del WLC cada 5 segundos no sería útil, un mejor enfoque sería recolectar las métricas de RF en todo el sistema cada 3 minutos.

NETCONF es siempre el preferido sobre SNMP.

Por último, no se puede pasar por alto la supervisión de los componentes de la red principal, incluida la utilización del conjunto DHCP, el número de entradas NAT en los routers principales, etc. Como la falla de cualquiera de estos puede ser fácilmente la causa de una interrupción inalámbrica.

Problemas específicos de las redes grandes

Si tiene un SSID que utiliza autenticación web, un problema pueden ser los clientes que se conectan a ese SSID y obtienen una dirección IP, pero nunca se autentican porque el usuario final no está intentando conectarse de forma activa (el dispositivo se conecta automáticamente). El controlador debe interceptar cada paquete HTTP enviado por aquellos clientes que están en el estado llamado autenticación web pendiente y esto utiliza recursos WLC. Una vez que la red se está ejecutando, vigile periódicamente el número de clientes que se encuentran en estado pendiente de autenticación web en un momento determinado para ver su comparación con los números de línea de base. Lo mismo para los clientes en el estado IP Learn. Siempre tiene clientes en ese estado cuando están realizando su proceso DHCP, pero saber cuál es un número de trabajo adecuado para su red ayuda a establecer una línea de base e identificar los momentos en los que este número puede ser demasiado alto e indicar un problema mayor.

Para lugares grandes, no es raro ver ~10% de los clientes en el estado Pendiente de autenticación Web.

Supervisión en el día 2: Vigile la satisfacción del usuario

Una vez que la red está en funcionamiento, existen dos tipos típicos de quejas de los usuarios finales: no pueden conectarse o les resulta difícil conectarse (se desconectan), o el funcionamiento de la red Wi-Fi es más lento de lo esperado. Esto último es muy difícil de identificar porque primero depende de las expectativas de la velocidad, así como de la densidad en tiempo real de un área determinada. Tratemos algunos recursos que pueden ser útiles para la supervisión diaria de una red de grandes recintos públicos.

Validar el rendimiento de Wi-Fi: guía de pruebas y supervisión. Este documento cisco.com explica cómo monitorear una red para detectar problemas de rendimiento. Se trata de averiguar cuánto rendimiento pueden esperar razonablemente los clientes en su red cuando las cosas están tranquilas y de estimar cuánto disminuyen estas estimaciones a medida que aumenta el número de clientes y la carga. Esto es clave para evaluar si una queja del usuario final sobre el rendimiento es legítima desde un punto de vista técnico o no, y si necesita rediseñar esa área para la carga que enfrenta potencialmente.

Cuando los clientes informan de problemas de conectividad, después de que se aisló y aclaró con Catalyst Center, eche un vistazo al Flujo de Resolución de Problemas de Conectividad del Cliente de Catalyst 9800.

Por último, como una buena práctica general, esté atento a las métricas clave generales del WLC con la ayuda de Monitor Catalyst 9800 KPIs (Indicadores de Rendimiento Clave).

Configuración para escalabilidad

SVI e interfaces en el 9800

Evite crear SVI para VLAN de cliente en el WLC. Los administradores que se utilizan para WLC de AireOS más antiguos tienden a tener el reflejo de crear una interfaz de capa 3 para cada VLAN

de cliente, pero esto rara vez es necesario. Las interfaces aumentan el vector de ataque del plano de control y pueden requerir más ACL con entradas más complejas. Se puede acceder al WLC, de forma predeterminada, en cualquiera de sus interfaces, se necesita más trabajo para proteger un WLC con más interfaces. También complica el ruteo, por lo que es mejor evitarlo.

A partir de IOS XE 17.9, las interfaces SVI ya no son necesarias para los escenarios de snooping mDNS o de retransmisión DHCP. Por lo tanto, hay muy pocas razones para configurar una interfaz SVI en una VLAN de cliente.

Respuesta de sondeo agregada

Para redes públicas de gran tamaño, se recomienda modificar el intervalo de sondeo agregado predeterminado enviado por los puntos de acceso. De forma predeterminada, los AP actualizan el WLC cada 500ms sobre los sondeos enviados por los clientes. Esta información se utiliza para las funciones de equilibrio de carga, selección de banda, ubicación y 802.11k. Si hay muchos clientes y puntos de acceso, es recomendable modificar el intervalo de actualización para evitar problemas de rendimiento del plano de control en el WLC. La configuración recomendada es de 50 respuestas de sondeo agregadas cada 64 segundos. También asegúrese de que sus AP no estén reportando sondas de direcciones MAC administradas localmente ya que no hay punto de seguimiento de aquellos que consideran que un solo cliente podría estar usando muchas MAC administradas localmente mientras escanea para evitar el rastreo a propósito.

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6

Muchos administradores de red siguen sin aceptar IPv6. Solo hay dos opciones aceptables con IPv6: o bien lo admite y debe implementar una configuración adecuada en cualquier lugar, o bien no lo hace, y debe bloquearlo. No es aceptable no preocuparse por IPV6 y dejarlo habilitado en algunos lugares sin la configuración adecuada. Esto dejaría a salvo todo ese mundo de IP al que no tendría acceso la seguridad de su red.

Si habilita IPv6, es obligatorio configurar una dirección IPv6 virtual en el rango 2001:DB8::/32 (este es un paso a menudo olvidado).

Es importante tener en cuenta que, aunque IPv6 depende mucho de la multidifusión para sus operaciones básicas, todavía puede funcionar si inhabilita el reenvío de multidifusión en el WLC. El reenvío de multidifusión hace referencia al reenvío de datos de multidifusión del cliente y no a la detección de vecinos, las solicitudes de router y otros protocolos necesarios para utilizar IPv6.

Si la conexión a Internet o el proveedor de servicios de Internet proporcionan direcciones IPv6, puede decidir permitir IPv6 para sus clientes. Se trata de una decisión diferente a la de habilitar IPv6 en su infraestructura. Sus AP podrían seguir funcionando en IPv4 solamente pero todavía

llevar tráfico de datos del cliente IPv6 dentro de sus paquetes CAPWAP. La habilitación de IPv6 en su infraestructura también requiere que piense en proteger el acceso del cliente a sus AP, WLC y subred de administración.

Verifique la frecuencia RA de sus gateways de cliente. El WLC ofrece una política de limitación de RA que limita el número de RAs reenviados a los clientes ya que éstos pueden conseguir chatty a veces.

mDNS

En general, es mejor mantener mDNS completamente desactivado en una implementación de grandes instalaciones.

mDNS bridging hace referencia al concepto de permitir que los paquetes mDNS se envíen como multidifusión de Capa 2 (por lo tanto, a toda la subred del cliente). mDNS se hizo popular en escenarios de oficinas pequeñas y domésticas donde es muy práctico detectar servicios en su subred. Sin embargo, en una red grande, esto significa enviar el paquete a todos los clientes en la subred, lo cual es problemático desde una perspectiva de tráfico en una red pública grande. Por otro lado, el bridging no causa ninguna sobrecarga a la CPU AP o WLC, ya que se considera como tráfico de datos regular. El proxy mDNS o gateway mDNS se refiere al concepto de uso del WLC como directorio para todos los servicios en la red. Esto permite ofrecer servicios mDNS a través de los límites de la capa 2 de una manera eficaz y también reducir el tráfico general. Con el gateway mDNS, una impresora, por ejemplo, envía su anuncio periódico del servicio vía mDNS con una multidifusión de la capa 2 de la misma subred pero el WLC no lo reenvía a todos los otros clientes inalámbricos. En su lugar, toma nota del servicio ofrecido y lo registra en su directorio de servicios. Cada vez que cualquier cliente pide servicios de un tipo dado disponible, el WLC responde en nombre de la impresora con el anuncio. De este modo, se evita que el resto de clientes inalámbricos oigan hablar de ofertas de servicios y solicitudes innecesarias, y solo obtengan una respuesta cuando pregunten por los servicios existentes. Aunque mejora en gran medida la eficiencia del tráfico, sí causa una sobrecarga en el WLC (o el AP, si confía en mDNS del AP en escenarios de FlexConnect) debido al snooping del tráfico mDNS. Si utiliza la puerta de enlace mDNS, es fundamental vigilar el uso de la CPU.

Su conexión en puente provoca una tormenta de multidifusión en su subred grande y la detección (con la función de gateway mDNS) provoca una gran utilización de la CPU. Desactívela de forma global, así como en cada WLAN.

Algunos administradores habilitan mDNS porque un par de servicios lo necesitan en lugares específicos, pero es importante entender cuánto tráfico no deseado esto agrega. Los dispositivos de Apple a menudo se anuncian a sí mismos y buscan constantemente servicios, lo que provoca un ruido de fondo de las consultas de mDNS incluso cuando nadie hace un uso particular de ningún servicio. Si necesita permitir mDNS debido a un determinado requisito empresarial, habilítelo globalmente y, a continuación, hágalo solo en la WLAN donde sea necesario e intente restringir el alcance donde mDNS está permitido.

Refuerzo de la red

Security

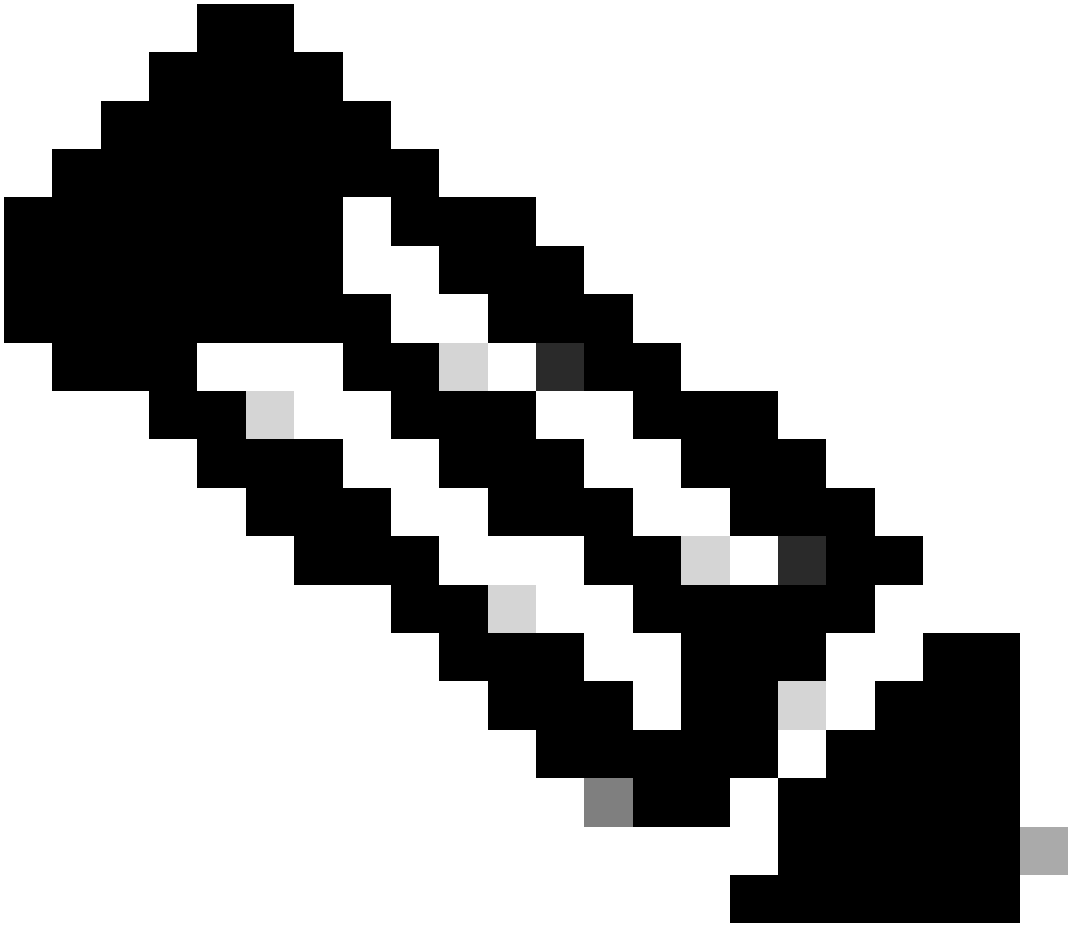
En las grandes redes públicas, pueden ocurrir muchas cosas sin que el administrador se entere. La gente solicita que los cables se descarten en lugares aleatorios, o que conecten un switch de nivel doméstico en una ubicación para tener más puertos de switch para sus travesuras, ... Normalmente prueban estas cosas sin pedir permiso primero. Esto significa que, incluso sin la intervención de un mal actor, la seguridad ya puede verse comprometida por la buena disposición de los clientes o empleados. A continuación, resulta muy sencillo para un actor malintencionado simplemente desplazarse y buscar un cable al que conectarse y ver el acceso a la red que obtiene desde allí. La configuración de la autenticación 802.1X en todos los puertos de switch es casi un requisito para mantener una seguridad decente en una red de gran tamaño. Catalyst Center puede ayudarle a automatizar esta implementación y se pueden hacer excepciones para dispositivos específicos que no admiten la autenticación 802.1X, pero que intentan confiar lo menos posible en la autenticación basada en MAC, ya que (sinceramente) no se trata de una seguridad real.

Puntos de acceso no autorizados

Su estrategia para combatir a los pícaros depende de algunos factores. Muchos administradores instintivamente optan por reglas muy estrictas, pero las preguntas principales son:

- Cuando recibe cientos (si no miles) de alertas no autorizadas, ¿dispone de los recursos humanos necesarios para examinarlas todas y tomar medidas al respecto?
- ¿Su objetivo es eliminar físicamente a los pícaros para mantener un espectro de RF limpio? Si es así, se necesita mucha gente para llevar a cabo esta operación. O tal vez su objetivo es solo mantener un ojo en el factor de seguridad y asegurarse de que los pícaros no representan ningún peligro? Esto tiene un costo de trabajo humano mucho más manejable.
- La activación de la detección de elementos no fiables puede afectar a su tiempo de emisión, y la contención de elementos no fiables suele tener un impacto aún mayor. ¿Analizó este impacto y lo tuvo en cuenta?

Con respecto al impacto de la detección de acceso no deseado, los routers 9120 y 9130 cuentan con un chip CleanAir dedicado que se encarga del escaneo fuera del canal (y, por lo tanto, de la detección de acceso no deseado), lo que hace que el impacto en la radio que atiende al cliente sea prácticamente nulo. Los AP de la serie 9160 con su chip CleanAir Pro tienen una capacidad de escaneo similar sin impacto, pero otros AP que no tienen el chip CleanAir necesitan tomar su radio de servicio al cliente fuera del canal para escanear en busca de pícaros o para hacer contención. Por lo tanto, el modelo de AP que está utilizando juega un papel en la decisión de utilizar AP dedicados en modo de monitoreo para la detección y contención de acceso no autorizado o no.

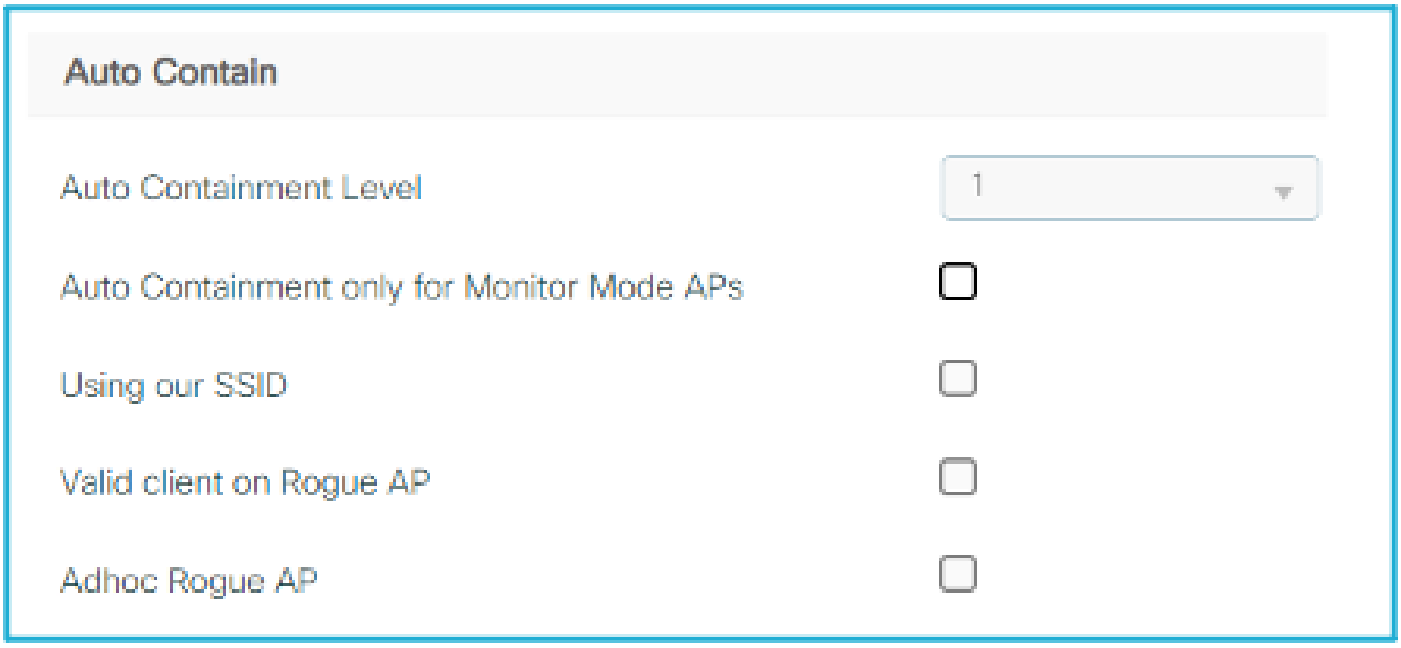


Nota: los teléfonos móviles que comparten una zona Wi-Fi funcionan en modo de "infraestructura", al igual que los puntos de acceso tradicionales. El modo "ad-hoc" hace referencia a una conexión directa entre dispositivos móviles y es menos común.

La contención de elementos no autorizados suele estar prohibida por las normas, por lo que es fundamental que consulte a su autoridad local antes de habilitarla. Contener un acceso no autorizado no significa cerrar el acceso no autorizado de forma remota, sino enviar spam a los clientes que intenten conectarse al punto de acceso no autorizado con tramas de desautenticación para que no se conecten. Esto sólo puede funcionar en SSID de seguridad heredado (no funciona en WPA3 o cuando PMF está habilitado en WPA2) porque los puntos de acceso no pueden firmar las tramas de desautenticación correctamente. La contención tiene un impacto negativo en el rendimiento de RF en el canal de destino, ya que sus AP están llenando el tiempo de transmisión con tramas de desautenticación. Por lo tanto, solo debe considerarse como una medida de seguridad para evitar que sus propios clientes legítimos se asocien a un punto de acceso no autorizado por error. Por todas las razones mencionadas, se recomienda no hacer ninguna contención, ya que no resuelve el problema de acceso no autorizado por completo y causa más problemas de RF. Si necesita utilizar la contención, solo tiene sentido activarla para

los pícaros que suplantan uno de sus SSID gestionados, ya que es un ataque de honeypot obvio.

Puede configurar la contención automática con la opción "using our SSIDs" (utilizando nuestros SSID):



Contener configuración automáticamente

También puede configurar reglas de acceso dudosas para clasificarlas como puntos de acceso dudosos maliciosos según sus propios criterios. No olvide introducir el nombre de los SSID vecinos y aprobados como "amigos desconocidos" para eliminarlos de la lista de alarmas.

Habilite la autenticación de AP o PMF para proteger sus AP de la suplantación.

Un acceso no autorizado por cable es un punto de acceso no autorizado conectado a la red por cable, lo que supone, obviamente, una mayor amenaza para la seguridad. La detección de sistemas no fiables conectados por cable es más complicada, ya que la dirección MAC de Ethernet de un sistema no fiable suele diferir de su dirección MAC de radio. Cisco Catalyst Center cuenta con algoritmos que aún tratan de detectar si un cliente no autorizado tiene cables y busca MAC de clientes no fiables que se escuchan por el aire y se ven en la infraestructura por cable. La mejor solución para evitar por completo los accesos no deseados por cable es proteger todos los puertos de switch con autenticación 802.1X.

Si va a actuar físicamente en un punto de acceso no autorizado, es fundamental aprovechar Cisco Spaces para tener una ubicación exacta del no autorizado. Lo más probable es que todavía tenga que buscar una vez en el sitio, ya que las personas tienden a ocultar puntos de acceso no autorizados a veces, pero la reducción del área de búsqueda a unos pocos metros hace que sea un esfuerzo muy factible. Sin Spaces, el pícaro se muestra en el mapa junto al AP detectándolo el más fuerte que hace para un área de búsqueda bastante grande. Existen muchos dispositivos y herramientas inalámbricas que muestran la señal del punto de acceso no autorizado en tiempo real para ayudarle a localizar físicamente al no autorizado.

No está relacionado exactamente con los equipos desconocidos, pero como CleanAir acaba de

aparecer, es importante tener en cuenta que la activación de CleanAir no tiene un impacto negativo apreciable en el rendimiento, excepto en la detección de balizas BLE, ya que afecta al rendimiento de 2,4 GHz. Puede configurar la red inalámbrica para que ignore las interferencias de Bluetooth, ya que están omnipresentes en el mundo actual, y no puede impedir que sus clientes activen su Bluetooth.

WiPS

WiPS cubre vectores de ataque más avanzados que simplemente detectar la presencia de un dispositivo no autorizado. Además de estos ataques, a veces también proporciona una PCAP del evento para el análisis forense.

Aunque se trata de una función de seguridad muy útil para la empresa, una red pública debe enfrentarse a la eterna pregunta: ¿qué hacer en contra de ella?

Con la dificultad de gestionar muchos clientes que no controlas, es posible dividir las alarmas en dos categorías. Las alarmas que puede decidir ignorar de Cisco Catalyst Center si observa que demasiadas de ellas son:

- 10001: DoS: alarma de saturación de autenticación
- 10002: DoS: alarma de solicitud de asociación
- 10003: DoS: alarma de inundación de sonda de difusión
- 10004: DoS: Alarma de inundación por desasociación
- 10005: DoS: alarma de desasociación de difusión
- 10006: DoS: alarma de inundación de desautenticación
- 10007: DOS: alarma de desautenticación de difusión
- 10008: DOS: Alarma de ataque de cierre de sesión de EAPOL
- 10009: alarma de inundación CTS
- 10010: Alarma de solicitud de asociación RTS
- 10011: Desautenticación inundación por par
- 10021: Sesión de Airdrop (esta suele producirse con frecuencia en cualquier red y simplemente representa la actividad normal de igual a igual entre dispositivos Apple)
- 10022: Solicitud de asociación incorrecta
- 10023: Inundación por firma de fallo de autenticación
- 10024: MAC OUI no válido por firma
- 10025: autenticación incorrecta

Estas alarmas pueden ser causadas potencialmente por un cliente que se comporta mal. No es posible evitar automáticamente un ataque de denegación de servicio ya que, básicamente, no se puede evitar que un cliente defectuoso mantenga ocupado el tiempo de transmisión. Incluso si la infraestructura ignora al cliente, podría seguir utilizando el medio y el tiempo de transmisión, lo que afectaría al rendimiento de los clientes que lo rodean.

Las otras alarmas son tan específicas que lo más probable es que representen un ataque malintencionado real y que difícilmente puedan producirse debido a controladores de clientes inadecuados. Es mejor seguir monitoreando estas alarmas:

- 10012: Baliza difusa
- 10013: Solicitud de sonda fusionada
- 10014: Respuesta de sonda fusionada
- 10015: Inundación de sondeo de PS por firma
- 10016: EAPOL Start V1 Flood by Signature
- 10017: Inundación de solicitud de reasociación por destino
- 10018: Inundación de baliza por firma
- 10019: Inundación de respuesta de sondeo por destino
- 10020: Bloqueo de confirmación de inundación por firma
- 10026/10027: ataque de detección de portadora virtual RTS y CTS

La infraestructura inalámbrica a veces puede tomar medidas de mitigación, como bloquear el dispositivo infractor, pero la única acción real para deshacerse de un ataque de este tipo es ir físicamente allí y eliminar el dispositivo infractor.

Se recomienda habilitar todas las formas de exclusión de clientes para ahorrar tiempo de transmisión perdido al interactuar con clientes defectuosos.

Restricción del Acceso de Cliente

Se aconseja habilitar el bloqueo peer-to-peer en todas sus WLAN (a menos que tenga un requisito estricto para la comunicación cliente-a-cliente - pero esto debe ser considerado cuidadosamente y posiblemente limitado). Esta función evita que los clientes en la misma WLAN se comuniquen entre sí. Esta no es una solución perfecta ya que los clientes en las diversas WLANs pueden todavía ponerse en contacto unos con otros y los clientes que pertenecen a diversos WLCs en el grupo de la movilidad también pueden saltarse esta restricción. Sin embargo, actúa como un primer nivel de seguridad y optimización fácil y eficiente. Una ventaja más de esta función de bloqueo de igual a igual es que también evita el ARP de cliente a cliente, que impide que las aplicaciones descubran otros dispositivos en la red local. Sin el bloqueo de igual a igual, la instalación de una aplicación simple en el cliente podría mostrar todos los otros clientes conectados en la subred con posiblemente su dirección IP y nombres de host.

Además, se recomienda aplicar una ACL IPv4 e IPv6 (si utiliza IPv6 en la red) en las WLAN para evitar la comunicación cliente a cliente. La aplicación de una ACL que bloquea la comunicación cliente a cliente en el nivel WLAN funciona independientemente de si tiene o no SVI de cliente.

El otro paso obligatorio es impedir el acceso del cliente inalámbrico a cualquier forma de gestión de su controlador inalámbrico.

Ejemplo:

```
ip access-list extended ACL_DENY_CLIENT_VLANS

 10 deny ip any 10.131.0.0 0.0.255.255

 20 deny ip 10.131.0.0 0.0.255.255 any

 30 deny ip any 10.132.0.0 0.0.255.255
```

```
 40 deny ip 10.132.0.0 0.0.255.255 any

 50 deny ip any 10.133.0.0 0.0.255.255

 60 deny ip 10.133.0.0 0.0.255.255 any

 70 deny ip any 10.134.0.0 0.0.255.255

 80 deny ip 10.134.0.0 0.0.255.255 any

 90 deny ip any 10.135.0.0 0.0.255.255

 100 deny ip 10.135.0.0 0.0.255.255 any

 110 deny ip any 10.136.0.0 0.0.255.255

 120 deny ip 10.136.0.0 0.0.255.255 any

 130 deny ip any 10.137.0.0 0.0.255.255

 140 deny ip 10.137.0.0 0.0.255.255 any

 150 permit ip any any
```

Esta ACL se puede aplicar en la interfaz de administración SVI:

```
interface Vlan130

 ip access-group ACL_DENY_CLIENT_VLANS in
```

Esto se hace en un WLC con las VLAN 131 a 137 del cliente creadas en la base de datos de VLAN de la capa 2 pero sin ninguna SVI correspondiente, y solamente existe una SVI para la VLAN 130 que es cómo se maneja el WLC. Esta ACL evita que todos los clientes inalámbricos envíen tráfico a los planos de control y administración del WLC completamente. No olvide que la administración de SSH o de la interfaz de usuario web no es lo único que necesita permitir, ya que también es necesario permitir una conexión CAPWAP hacia todos los AP. Esta es la razón por la que esta ACL tiene un permiso predeterminado, pero bloquea los rangos de clientes inalámbricos, en lugar de depender de una acción de negación de todo predeterminada que requeriría especificar todos los rangos de administración y rangos de subred de AP permitidos.

De manera similar, puede crear otra ACL que especifique todas las subredes de administración posibles:

```
ip access-list standard ACL_MGMT

 10 permit 10.128.0.0 0.0.255.255

 20 permit 10.127.0.0 0.0.255.255
```

```
 30 permit 10.100.0.0 0.0.255.255

 40 permit 10.121.0.0 0.0.255.255

 50 permit 10.141.0.0 0.0.255.255
```

A continuación, puede aplicar esta ACL para el acceso CLI:

```
line vty 0 50

 access-class ACL_MGMT in

 exec-timeout 180 0

 ipv6 access-class ACL_IPV6_MGMT in

 logging synchronous

 length 0

 transport preferred none

 transport input ssh

 transport output ssh
```

La misma ACL también se puede aplicar para el acceso de administración web.

Protección contra tormentas de tráfico

Algunas aplicaciones utilizan más las multidifusión y las difusiones que otras. Cuando se considera una red solo con cables, la protección frente a tormentas de difusión es a menudo la única precaución que se toma. Sin embargo, un multicast es tan doloroso como un broadcast cuando se envía por el aire y es importante entender por qué. En primer lugar, imagine un paquete enviado (ya sea a través de difusión o multidifusión) a todos sus clientes inalámbricos, que rápidamente se suma a muchos destinos. A continuación, cada punto de acceso debe transmitir esta trama por el aire de la manera más fiable posible (aunque no se garantiza que sea fiable) y eso se logra mediante el uso de una velocidad de datos obligatoria (a veces la más baja, a veces configurable). En términos sencillos, esto significa que la trama se envía usando una velocidad de datos OFDM (802.11a/g), que claramente no es excelente.

En una red pública de gran tamaño, no se recomienda confiar en la multidifusión para conservar el tiempo de transmisión. Sin embargo, en una red empresarial de gran tamaño, puede tener el requisito de mantener la multidifusión habilitada para una aplicación específica, aunque debe controlarla todo lo posible para limitar su impacto. Es una buena idea documentar los detalles de la aplicación, la IP de multidifusión y asegurarse de bloquear otras formas de multidifusión. La activación del reenvío de multidifusión no es un requisito para activar IPv6, como se ha explicado anteriormente. Es mejor mantener el reenvío de difusión deshabilitado completamente. Las

aplicaciones utilizan a veces las transmisiones para detectar otros dispositivos en la misma subred, lo que supone claramente un problema de seguridad en una red de gran tamaño.

Si habilita el reenvío de multidifusión global, asegúrese de utilizar la configuración CAPWAP de PA de multidifusión-multidifusión. Con esto habilitado, cuando el WLC recibe un paquete multicast de la infraestructura cableada, lo envía a todos los AP interesados con un solo paquete multicast, ahorrando en una gran cantidad de duplicación de paquetes. Asegúrese de establecer una IP multicast CAPWAP diferente para cada uno de sus WLCs de otra manera los APs reciben el tráfico multicast de otros WLCs que no se desea.

Si sus AP están en otras subredes de su interfaz de administración inalámbrica del WLC (que es probable en una red grande), debe habilitar el ruteo multicast en su infraestructura cableada. Puede verificar que todos sus AP estén recibiendo correctamente el tráfico multicast con el comando:

```
show ap multicast mom
```

También se recomienda que la multidifusión IGMP (para multidifusión IPv4) y MLD (para IPv6) esté habilitada en todos los casos si necesita confiar en la multidifusión. Permiten que solo los clientes inalámbricos interesados (y por lo tanto solo los AP que tienen clientes interesados) reciban el tráfico multicast. El WLC hace proxy del registro al tráfico multicast y se encarga de mantener el registro activo, descargando así a los clientes.

Conclusión

Las redes públicas de gran tamaño son complejas, cada una de ellas es única, con requisitos y resultados específicos.

Respetar las directrices de este documento es un buen punto de partida y ayuda a lograr el éxito en la implementación, a la vez que se evitan los problemas más comunes. Sin embargo, las directrices son sólo directrices y pueden tener que interpretarse o ajustarse en el contexto del lugar específico.

Cisco CX cuenta con equipos de profesionales inalámbricos dedicados a grandes implementaciones inalámbricas, con experiencia en numerosos eventos de gran tamaño, incluidos eventos deportivos y conferencias. Póngase en contacto con su equipo de cuentas para obtener más ayuda.

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).