

# Glosario de términos de puntos de acceso inalámbricos

## Objetivo

Este artículo contiene la lista de términos utilizados para configurar, configurar y solucionar problemas de los puntos de acceso inalámbricos (WAP) de Cisco.

## Dispositivos aplicables

- Puntos de acceso inalámbricos

## Lista de términos generales

- VLAN basada en 802.1Q: la especificación IEEE 802.1Q establece un método estándar para etiquetar tramas Ethernet con información de pertenencia a VLAN, y define el funcionamiento de los puentes VLAN que permiten la definición, el funcionamiento y la administración de topologías VLAN dentro de una infraestructura LAN puentada. El estándar 802.1Q está diseñado para abordar el problema de cómo dividir las redes grandes en partes más pequeñas, de modo que el tráfico de difusión y multidifusión no utilice más ancho de banda del necesario. El estándar también ayuda a proporcionar un mayor nivel de seguridad entre los segmentos de las redes internas.
- Suplicante 802.1X: suplicante es una de las tres funciones del estándar IEEE 802.1X. El 802.1X se desarrolló para proporcionar seguridad en la capa 2 del modelo OSI. Se compone de los siguientes componentes: Supplicant, Authenticator y Authentication Server. Un suplicante es el cliente o software que se conecta a una red para que pueda acceder a los recursos de esa red. Necesita proporcionar credenciales o certificados para obtener una dirección IP y ser parte de esa red en particular. Un solicitante no puede tener acceso a los recursos de la red hasta que se haya autenticado.
- ACL: una lista de control de acceso (ACL) es una lista de filtros de tráfico de red y acciones correlacionadas utilizadas para mejorar la seguridad. Bloquea o permite a los usuarios acceder a recursos específicos. Una ACL contiene los hosts a los que se permite o se niega el acceso al dispositivo de red. Las ACL se pueden definir de una de dos maneras: por dirección IPv4 o por dirección IPv6.
- Band Steer: El equilibrio de carga avanzado, más conocido como dirección de banda, es una función que detecta dispositivos capaces de transmitir a una banda de 5 GHz. La banda de 2,4 GHz suele estar congestionada y sufre interferencias de diferentes dispositivos, como Bluetooth, e incluso hornos microondas. Esta función permite al punto de acceso dirigir y dirigir los dispositivos a una frecuencia de radio más óptima, lo que mejora el rendimiento de la red.
- Utilización del ancho de banda: la utilización del ancho de banda permite colocar un umbral en la transferencia de datos correcta media a través de una ruta de comunicación. Algunas de las técnicas utilizadas para mejorar esto son el modelado, la gestión, el tope y la asignación del ancho de banda.
- Bonjour: Bonjour permite descubrir un punto de acceso y sus servicios mediante el uso de DNS multicast. Anuncia sus servicios a la red y responde a las preguntas sobre los tipos de servicios que admite, lo que simplifica la configuración de la red en entornos de pequeñas empresas. Cuando Bonjour está habilitado en un dispositivo WAP soportado, cualquier cliente

Bonjour puede detectar y acceder a la utilidad basada en web sin configuración previa. Bonjour funciona tanto en redes IPv4 como IPv6.

- Portal cautivo: el método de portal cautivo obliga a los usuarios o hosts de la red a ver una página web especial antes de que puedan acceder a la red pública normalmente. El portal cautivo convierte un navegador web en un dispositivo de autenticación. La página web requiere la interacción o autenticación del usuario antes de permitir que el acceso utilice la red.
- Aislamiento de canales: un dispositivo con administración de canales habilitada asigna automáticamente los canales de radio inalámbricos a los otros dispositivos WAP del clúster. La asignación automática de canales reduce la interferencia con otros puntos de acceso fuera de su clúster y maximiza el ancho de banda Wi-Fi para ayudar a mantener la eficiencia de la comunicación a través de la red inalámbrica.
- QoS de cliente: la asociación de calidad de servicio (QoS) de cliente es una sección que proporciona opciones adicionales para la personalización de la QoS de un cliente inalámbrico. Estas opciones incluyen el ancho de banda permitido para enviar, recibir o garantizar. La asociación de QoS de cliente puede manipularse aún más con el uso de listas de control de acceso (ACL).
- Registro de eventos: los eventos del sistema son actividades del sistema que pueden requerir atención y acciones necesarias para ejecutar el sistema sin problemas y evitar fallos. Estos eventos se registran como registros. Los registros del sistema permiten al administrador realizar un seguimiento de los eventos concretos que se producen en el dispositivo. Los registros de eventos son útiles para la resolución de problemas de red, la depuración del flujo de paquetes y la supervisión de eventos.
- Fast Roaming: la itinerancia rápida entre los puntos de acceso inalámbricos permite una conectividad inalámbrica rápida, segura e ininterrumpida para lograr una experiencia móvil perfecta para aplicaciones en tiempo real como FaceTime, Skype y Cisco Jabber.
- HTTPS: el protocolo de transferencia de hipertexto seguro (HTTPS) es un protocolo de transferencia más seguro que HTTP. El punto de acceso se puede administrar a través de conexiones HTTP y HTTPS cuando se configuran los servidores HTTP/HTTPS. Algunos exploradores web utilizan HTTP mientras que otros utilizan HTTPS. Un punto de acceso debe tener un certificado SSL (Secure Socket Layer) válido para utilizar el servicio HTTPS.
- IPv4: IPv4 es un sistema de direccionamiento de 32 bits utilizado para identificar un dispositivo en una red. Es el sistema de direccionamiento utilizado en la mayoría de las redes informáticas, incluida Internet.
- IPv6: IPv6 es un sistema de direccionamiento de 128 bits utilizado para identificar un dispositivo en una red. Es el sucesor de IPv4 y la versión más reciente del sistema de direccionamiento utilizado en las redes informáticas. IPv6 se está implantando actualmente en todo el mundo. Una dirección IPv6 se representa en ocho campos de números hexadecimales, cada uno de los cuales contiene 16 bits. Una dirección IPv6 se divide en dos partes, cada una de las cuales consta de 64 bits. La primera parte es la dirección de red y la segunda parte la dirección de host.
- LLDP: protocolo de detección de capa de enlace (LLDP) es un protocolo de detección definido en el estándar IEEE 802.1AB. LLDP permite a los dispositivos de red anunciar información sobre ellos mismos a otros dispositivos de la red. LLDP utiliza los servicios de Control de link lógico (LLC) para transmitir y recibir información hacia y desde otros agentes LLDP. LLC proporciona un punto de acceso de servicio de enlace (LSAP) para el acceso a LLDP. Cada trama LLDP se transmite como una única solicitud de servicio MAC. La entidad LLC recibe cada trama LLDP entrante en el punto de acceso al servicio MAC (MSAP) como

indicación de servicio MAC.

- **Balanceo de Carga:** El Balanceo de Carga es una terminología de red que se utiliza para distribuir la carga de trabajo entre varios ordenadores, enlaces de red y otros recursos para lograr una utilización adecuada de los recursos, maximizar el rendimiento, el tiempo de respuesta y, principalmente, evitar la sobrecarga.
- **MAC ACL:** el control de acceso a medios (MAC) basado en la lista de control de acceso (ACL) es una lista de direcciones MAC de origen. Si un paquete viene de un punto de acceso inalámbrico a un puerto LAN o viceversa, este dispositivo verificará si la dirección MAC de origen del paquete coincide con cualquier entrada de esta lista y verifica las reglas ACL en relación con el contenido de la trama. Luego utiliza los resultados coincidentes para permitir o denegar este paquete. Sin embargo, los paquetes de LAN a puerto LAN no se verificarán.
- **Varios SSID:** puede configurar varios identificadores de conjunto de servicios (SSID) o puntos de acceso virtuales (VAP) en el punto de acceso y asignar diferentes parámetros de configuración a cada SSID. Todos los SSID pueden estar activos al mismo tiempo. Los dispositivos cliente pueden asociarse al punto de acceso mediante cualquiera de los SSID.
- **Modo de funcionamiento:** el dispositivo WAP puede actuar como un único punto de acceso de modo punto a punto, puente punto a multipunto y como repetidor. En el modo punto a punto, un solo dispositivo WAP acepta conexiones de clientes y otros dispositivos de la red. En un modo de puente punto a multipunto, un único dispositivo WAP se comporta como un link común entre muchos puntos de acceso. El dispositivo WAP también puede actuar como repetidor, donde puede establecer una conexión entre puntos de acceso que están muy alejados entre sí. Los clientes inalámbricos pueden conectarse a este repetidor. Se puede comparar un sistema de funciones de Wireless Distribution System (WDS) de forma similar a la función del repetidor.
- **Captura de paquetes:** la captura de paquetes es una función de un dispositivo de red que le permite capturar y almacenar paquetes transmitidos y recibidos por el dispositivo. Los paquetes capturados pueden ser analizados por un analizador de protocolo de red para resolver problemas o optimizar el rendimiento. El archivo de paquete capturado se puede descargar a través de HTTP/HTTPS o servidor TFTP. Se puede compartir y luego analizar más a fondo para comprender el flujo de paquetes en la red. La página Captura de paquetes se puede utilizar para configurar la captura de paquetes remota o local, descargar un archivo de captura de paquetes o ver el estado de captura actual.
- **QoS:** la calidad del servicio (QoS) permite dar prioridad al tráfico de diferentes aplicaciones, usuarios o flujos de datos. También puede utilizarse para garantizar el rendimiento a un nivel específico, afectando así la calidad del servicio del cliente. La QoS se ve generalmente afectada por los siguientes factores: fluctuación, latencia y pérdida de paquetes.
- **Servidor RADIUS:** el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un mecanismo de autenticación para que los dispositivos se conecten y utilicen un servicio de red. Se utiliza para fines de autenticación, autorización y contabilidad centralizados. Un servidor RADIUS regula el acceso a la red mediante la verificación de la identidad de los usuarios a través de las credenciales de inicio de sesión introducidas. Por ejemplo, una red Wi-Fi pública se instala en un campus universitario. Sólo los alumnos que tienen la contraseña pueden acceder a estas redes. El servidor RADIUS verifica las contraseñas introducidas por los usuarios y concede o deniega el acceso según corresponda.
- **Administración remota:** la administración remota está manipulando los parámetros de un dispositivo de red desde una ubicación remota. Esto se suele hacer en dispositivos como ordenadores, switches, routers y muchos otros que tienen una dirección IP. Permite a los administradores de red responder rápidamente a las solicitudes o los retos, ya que no tienen

que estar físicamente en el sitio. El acceso a los dispositivos en la administración remota es casi como hacerlo localmente, excepto que la dirección IP local del dispositivo se utiliza para acceder al dispositivo localmente, mientras que la IP de WAN del dispositivo se utiliza cuando se hace en un dispositivo remoto.

- **Detección de puntos de acceso no autorizados:** un punto de acceso no autorizado (AP) es un punto de acceso que se ha instalado en una red sin autorización explícita de un administrador del sistema. Los puntos de acceso desconocidos suponen una amenaza para la seguridad, ya que cualquier persona con acceso al área puede instalar de forma consciente o inconsciente un punto de acceso inalámbrico que permita a las partes no autorizadas acceder a la red. La función Rogue AP Detection en su punto de acceso le permite ver estos puntos de acceso no autorizados que están dentro del rango y muestra su información en la utilidad basada en web. Puede agregar cualquier punto de acceso autorizado a la lista AP de confianza.
- **RSTP:** el protocolo de árbol de extensión rápido (RSTP) es una mejora del STP. RSTP proporciona una convergencia de árbol de extensión más rápida después de un cambio de topología. El STP puede tardar de 30 a 50 segundos en responder a un cambio de topología mientras que el RSTP responde en el triple del tiempo de saludo configurado. RSTP es compatible con el STP en sentido inverso.
- **Planificador:** el planificador inalámbrico ayuda a programar un intervalo de tiempo para que un punto de acceso virtual (VAP) o una radio funcione, lo que ayuda a ahorrar energía y aumentar la seguridad. Puede asociar hasta 16 perfiles a diferentes VAP o interfaces de radio, pero cada interfaz sólo tiene permitido un perfil. Cada perfil puede tener un cierto número de reglas de tiempo que controlan el tiempo de actividad del VAP o WLAN asociados.
- **Single Point Setup:** Single Point Setup es una sencilla tecnología de gestión de varios dispositivos que le permite implementar y administrar un grupo de puntos de acceso compatibles con la función. Ofrece la comodidad de configurar un grupo de puntos de acceso desde un único punto en lugar de configurarlos individualmente. También le permite administrar los puntos de acceso de forma local o remota.
- **SNMP:** el protocolo simple de administración de red (SNMP) es un estándar de red para almacenar y compartir información sobre los dispositivos de red. SNMP facilita la administración, resolución de problemas y mantenimiento de la red.
- **Spanning Tree:** protocolo de árbol de extensión (STP) es un protocolo de red utilizado en una LAN. El propósito de STP es asegurar una topología sin loops para una LAN. El STP elimina los loops a través de un algoritmo que garantiza que sólo hay una trayectoria activa entre dos dispositivos de red. STP garantiza que el tráfico tome la ruta más corta posible dentro de la red. STP también puede volver a habilitar automáticamente las rutas redundantes como rutas de respaldo si falla una trayectoria activa.
- **SSID:** el identificador del conjunto de servicios (SSID) es un identificador único al que los clientes inalámbricos pueden conectarse o compartir entre todos los dispositivos de una red inalámbrica. Distingue entre mayúsculas y minúsculas y no debe superar los 32 caracteres alfanuméricos. También se denomina Wireless Network Name (Nombre de red inalámbrica).
- **SSID Broadcast (Difusión de SSID):** cuando un dispositivo inalámbrico busca en el área redes inalámbricas a las que puede conectarse, detectará las redes inalámbricas dentro de su alcance a través de sus nombres de red o SSID. La difusión del SSID está habilitada de forma predeterminada. Sin embargo, también puede optar por desactivarla.
- **TSPEC:** Especificación de tráfico (TSPEC) es una especificación de tráfico enviada desde un cliente inalámbrico con capacidad para QoS a un dispositivo WAP que solicita una cierta cantidad de acceso a la red para el flujo de tráfico (TS) que representa.

- **VLAN:** una red de área local virtual (VLAN) es una red conmutada segmentada lógicamente por función, área o aplicación, independientemente de las ubicaciones físicas de los usuarios. Las VLAN son un grupo de hosts o puertos que se pueden ubicar en cualquier lugar de una red pero que se comunican como si estuvieran en el mismo segmento físico. Las VLAN ayudan a simplificar la administración de la red al permitirle mover un dispositivo a una nueva VLAN sin cambiar ninguna conexión física.
- **WDS:** Wireless Distribution System (WDS) es una función que permite la interconexión inalámbrica de puntos de acceso en una red. Permite al usuario ampliar la red con varios puntos de acceso de forma inalámbrica. WDS también conserva las direcciones MAC de las tramas cliente a través de los links entre los puntos de acceso. Esta capacidad es fundamental porque proporciona una experiencia perfecta para los clientes de roaming y permite la gestión de varias redes inalámbricas.
- **WMM:** Wi-Fi Multimedia (WMM) es una función que asigna diferentes prioridades de proceso a diferentes tipos de tráfico. WMM es también una función de QoS que mejora el rendimiento de la red inalámbrica estableciendo la prioridad del paquete de datos inalámbrico en función de cuatro categorías: voz, vídeo, mejor esfuerzo y fondo. De forma predeterminada, WMM está activado. Si una aplicación no requiere WMM, se le da menor prioridad que el vídeo y la voz.
- **Aislamiento inalámbrico:** evita la comunicación y las transferencias de archivos entre equipos conectados a diferentes SSID. El tráfico en un SSID no se reenviará a ningún otro SSID.
- **WPA/WPA2:** el acceso Wi-Fi protegido (WPA y WPA2) son protocolos de seguridad que se utilizan en las redes inalámbricas para proteger la privacidad mediante el cifrado de los datos transmitidos a través de la red inalámbrica. WPA y WPA2 son compatibles con reenvío con IEEE 802.11e y 802.11i. WPA y WPA2 han mejorado las funciones de autenticación y cifrado en comparación con el protocolo de seguridad Wired Equivalent Privacy (WEP).

### Lista de términos en redes de malla

- **Punto de acceso (AP):** Dispositivo de una red que se utiliza para permitir a los usuarios conectarse a la red de forma inalámbrica. Se pueden agregar etiquetas específicas a esto dependiendo de su función: Principal, Remoto, Raíz, Subordinado, etc.
- **Red de malla inalámbrica:** Tipo de topología en la que los puntos de acceso inalámbricos se conectan entre sí para transmitir información. Estas redes funcionan de forma dinámica para ajustar las necesidades y mantener la conectividad para todos los usuarios.
- **AP principal:** El AP principal proporciona administración y control de la red inalámbrica y la topología. Es el puente al resto de la red externa (normalmente Internet) mediante un proveedor de servicios de Internet (ISP). El AP primario se conecta directamente al router de la instalación que, a su vez, enruta el tráfico a la interfaz del ISP WAN. El AP primario es el orquestador de todos los nodos que proporcionan servicios inalámbricos dentro de la red de interconexión. Administra la información de los nodos de la red, la calidad de cada conexión del cliente y la información del vecino para tomar la mejor decisión sobre la mejor ruta para los servicios inalámbricos optimizados hacia el cliente móvil.
- **Primario principal:** El AP actual se encarga de la administración de la WLAN.
- **Primario preferido:** Configuración en la que se muestra un AP específico con capacidad primaria como preferido. Si falla el AP primario, el AP primario preferido tomará el control. Una vez que el AP preferido está de vuelta, no se conmuta automáticamente de nuevo. No ha designado un Primario preferido.
- **AP con capacidad principal:** Un AP que tiene una conexión física cableada de vuelta a la red. Este AP debe estar conectado a Ethernet y puede convertirse en el AP primario si falla el AP

primario.

- **Extender de malla:** Un AP subordinado remoto en la red que no está conectado a la red por cable.
- **AP subordinado:** Término general que se puede aplicar a cualquier AP de malla que no se configura como primario.
- **AP principal:** Un AP primario es un AP que proporciona la mejor ruta de regreso al AP primario.
- **Punto de acceso secundario:** Un AP secundario es un extensor de malla que selecciona el AP primario como su mejor ruta de regreso al AP primario.
- **AP ascendente:** Un AP ascendente es un término general que se refiere a la dirección que los datos fluyen a través de APs cuando van del cliente al servidor.
- **AP descendente:** Un AP de flujo descendente transporta los datos desde Internet hasta el cliente.
- **AP co-ubicados:** Extensores de malla que se encuentran dentro del rango de difusión del canal de red de retorno.
- **Nodos:** En este artículo, los AP se denominan nodos. En general, los nodos describen cualquier dispositivo que realiza una conexión o interacción dentro de una red, o que tiene la capacidad de enviar, recibir y almacenar información, comunicarse con Internet y tener una dirección IP. En una red de malla, los parámetros de radio optimizados en todos los nodos garantizan una cobertura inalámbrica máxima al tiempo que reducen la interferencia de radio entre los nodos para proporcionar velocidades de datos y rendimiento superiores.
- **Red de retorno:** En una red de malla inalámbrica, la información de la red de área local (LAN) necesita llegar a un punto de acceso con cables para alcanzar Internet. La red de retorno es el proceso para devolver esa información al punto de acceso por cable.