Comprender & Solucionar problemas de QoS en el WLC 9800 inalámbrico (Referencia rápida)

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
  - Breve descripción del estándar IEEE 802.11e y Wi-Fi Multimedia (WMM)
  - Colas WMM y acceso de canal distribuido mejorado (EDCA)
- Implementación de QoS
  - CoS "802.1p" de capa 2 (clase de servicio)
  - DSCP de capa 3 (punto de código de servicios diferenciados)
  - Asignación DSCP-a-UP predeterminada
- Flujo de paquetes y confianza de QoS
  - Switching central: confianza descendente
  - Switching central: confianza ascendente
  - Confianza de switching local de Flexconnect
- Problemas Comunes Para El Tráfico Ascendente
  - Ejemplo #1: Cuando el cliente transmite tráfico con un valor UP de "2"
  - Ejemplo #2: Un problema bien conocido del cliente Microsoft Windows en el mapeo DSCP a UP
- ¿Qué protocolo se debe confiar: DSCP o COS?
- Prácticas recomendadas de QoS del controlador de LAN inalámbrica
  - Perfiles de QoS de metal
  - Descripción del audio unidireccional
  - Comprensión del audio entrecortado y robótico
  - Descripción de las lagunas y ausencia de audio durante la itinerancia
  - Referencias

Introducción

Este documento describe QoS en los controladores de LAN inalámbrica 9800

Prerequisites

Requirements

Este documento explica cómo priorizar y etiquetar el tráfico tanto en sentido ascendente como descendente. Explica las prácticas recomendadas para la configuración del tráfico de voz en el

controlador de LAN inalámbrica (WLC) y las técnicas de solución de problemas para problemas comunes relacionados con la voz.

Componentes Utilizados

9800 WLC basado en la versión 17.12 del IOS® XE de Cisco.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Breve descripción del estándar IEEE 802.11e y Wi-Fi Multimedia (WMM)

WMM es una alianza Wi-Fi basada en el estándar IEEE 802.11e. WMM proporciona funciones de calidad de servicio (QoS) mediante la priorización del tráfico según cuatro categorías de acceso: voz, vídeo, mejor esfuerzo y fondo, según el método de acceso de canal distribuido mejorado (EDCA).

La habilitación de WMM es esencial para lograr un rendimiento óptimo en las redes Wi-Fi, especialmente en entornos en los que predominan aplicaciones de gran ancho de banda y baja latencia. Por ejemplo, en las redes 802.11n, WMM debe aprovechar al máximo las capacidades de este estándar Wi-Fi de alta velocidad.

Colas WMM y acceso de canal distribuido mejorado (EDCA)

En términos generales, cualquier estación debe escuchar el medio para verificar si está inactivo antes de enviar las tramas. Una vez enviada la trama, la estación escucha el medio para ver si se ha producido una colisión.

Los clientes inalámbricos no pueden detectar las colisiones. Para ello, se utiliza CSMA/CA (acceso múltiple por detección de portadora con prevención de colisiones). Utiliza un temporizador fijo y aleatorio (CWmin, CWmax) y cada trama que se envía debe ser reconocida para que sepamos que no hay colisión y todos los clientes puedan enviar su tráfico.

Como hemos mencionado anteriormente, tenemos cuatro categorías de acceso (colas), cada una de las colas utiliza diferentes temporizadores. Las tramas con la prioridad más alta se envían estadísticamente antes, y las tramas de prioridad más baja tienen parámetros de backoff que estadísticamente se envían después.

En resumen, la existencia de las cuatro colas por sí sola no garantiza la calidad del servicio (QoS); lo que verdaderamente importa es cómo se gestiona eficazmente el tráfico dentro de cada cola.

Implementación de QoS

De forma predeterminada, si no se configura la calidad del servicio (QoS), el tráfico de red se trata de la misma manera, con un modelo de entrega de mejor esfuerzo. Esto significa que todo el tráfico, independientemente de su tipo o importancia, tiene la misma prioridad y posibilidad de ser entregado en un momento dado. Sin embargo, cuando las funciones de QoS están activadas y configuradas correctamente, se puede asignar prioridad a tipos específicos de tráfico de red, como voz y vídeo.

La configuración de QoS implica dos componentes principales: Clasificación y Marcado.

Clasificación:

La clasificación implica identificar y categorizar el tráfico de red en función de criterios específicos, como el tipo de aplicación, la dirección IP de origen/destino, el protocolo o el número de puerto. El tráfico se divide en clases o colas:

1. Voz: AC_VO
2. Vídeo: AC_VI
3. Mejor esfuerzo: AC_BE
4. Antecedentes: AC_BK

Marcación:

Una vez que el tráfico se clasifica en colas, el marcado implica la asignación de etiquetas o marcas de QoS a los paquetes para indicar su nivel de prioridad.

Hay varias maneras de marcar el tráfico. Los dos estándares principales son 802.1p CoS (clase de servicio) de capa 2 y DSCP (punto de código de servicios diferenciados) de capa 3.

CoS "802.1p" de capa 2 (clase de servicio)

En el estándar 802.1p, hay siete niveles de CoS, cada uno representado por un campo de 3 bits que puede asumir valores que van del 0 al 7. Estos valores significan la prioridad del tráfico, siendo 0 la prioridad más baja y 7 la prioridad más alta.

Nota: 802.1p es un subconjunto del estándar 802.1q y se presenta solo cuando hay una etiqueta VLAN, como en los puertos troncales.

Tabla 1: Clasificación de 802.1P y WMM

802.1P Priority	Access Category_WMM Designation	Access Category "AC"	QoS
1	AC_BK	Background	Bronze
2	AC_BK	Background	Bronze
0	AC_BE	Best Effort	Silver
3	AC_BE	Best Effort	Silver
4	AC_VI	Video	Gold
5	AC_VI	Video	Gold
6	AC_VO	Voice	Platinum
7	AC_VO	Voice	Platinum

DSCP de capa 3 (punto de código de servicios diferenciados)

DSCP es una etiqueta de capa 3 en el encabezado IP, utiliza 6 bits que permiten 64 valores diferentes (0 a 63).

Tabla 2: Clasificación de DSCP y WMM

DSCP	Access Category_WMM Designation	Access Category "AC"	QoS
0-7	AC_BE	Best Effort	Silver
24-31	AC_BE	Best Effort	Silver
8-15	AC_BK	Background	Bronze
16-23	AC_BK	Background	Bronze
32-39	AC_VI	Video	Gold
40-47	AC_VI	Video	Gold
48-55	AC_VO	Voice	Platinum
56-63	AC_VO	Voice	Platinum

Los valores DSCP predominantes incluyen 46 (EF) para voz, 34 (AF41) para vídeo y 0 (BE) designado para el mejor esfuerzo.

Asignación DSCP-a-UP predeterminada

Como hemos comentado anteriormente, UP es un campo de 3 bits dentro de la trama Ethernet, mientras que DSCP es de 6 bits en el encabezado IP.

¿Cómo puede calcular el valor de prioridad de usuario (UP) de capa 2 a partir del valor de punto de código de servicios diferenciados (DSCP) de capa 3?

Actualmente, no existe un estándar específico para esta asignación; sin embargo, se utiliza un

método común conocido como "Asignación DSCP a UP predeterminada".

El método de mapeo de DSCP a UP deriva los valores UP de los 3 msb del paquete DSCP y luego los mapea en la categoría de acceso correcta.

Este método es utilizado por las máquinas de Microsoft Windows ceden a un problema conocido que se trata con más detalle en el Ejemplo #2: Un problema bien conocido del cliente de Microsoft Windows en el mapeo DSCP a UP

Tabla 3: Asignación DSCP-a-UP predeterminada

DSCP	DSCP (binary)	802.11e UP (binary)	802.11e UP (decimal)	Access Category Assignment
56-63	111000 - 111111	111	7	Voice
48-55	110000 - 110111	110	6	
40-47	101000 - 101111	101	5	Video
32-39	100000 - 100111	100	4	
24-31	011000 - 011111	011	3	Best Effort
0-7	000000 – 000101	000	0	
16-23	010000 - 010111	010	2	Background
8-15	001111 - 001111	001	1	

Flujo de paquetes y confianza de QoS

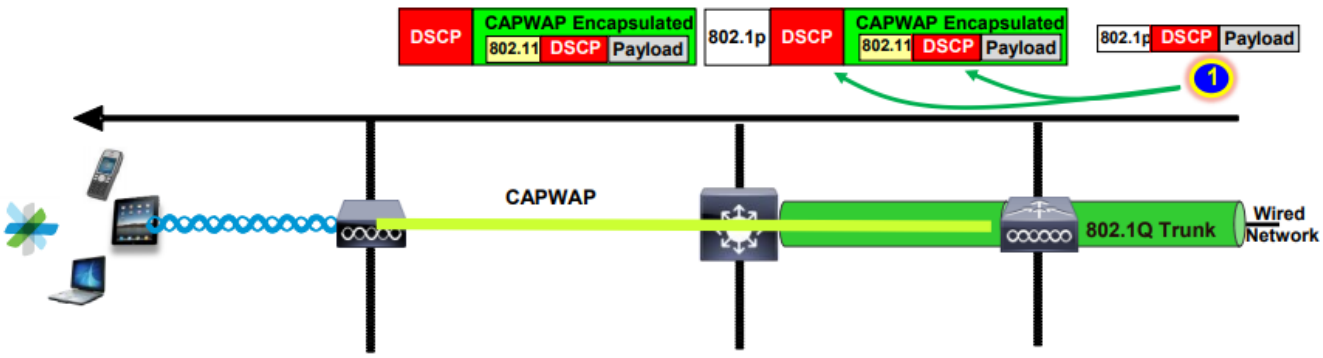
Esta sección trata sobre el flujo de paquetes y la confianza de QoS en estos diferentes escenarios:

1. Switching central: confianza descendente.
2. Switching central: confianza ascendente.
3. Confianza en switching local de FlexConnect.

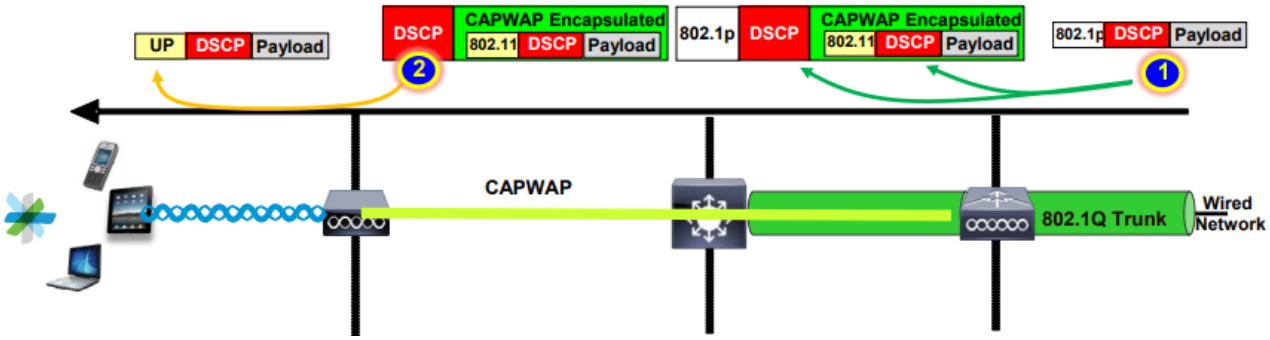
Switching central: confianza descendente

- Flujo descendente: tráfico de red por cable a inalámbrica.
- El tráfico descendente está encapsulado CAPWAP.

1- Se recibe una trama Ethernet en el puerto trunk del WLC 802.1q. El WLC utiliza el valor DSCP interno enviado de la red cableada y lo mapea al DSCP externo en el encabezado CAPWAP, y limita el DSCP externo a un valor máximo según el perfil de QoS configurado en el WLC.



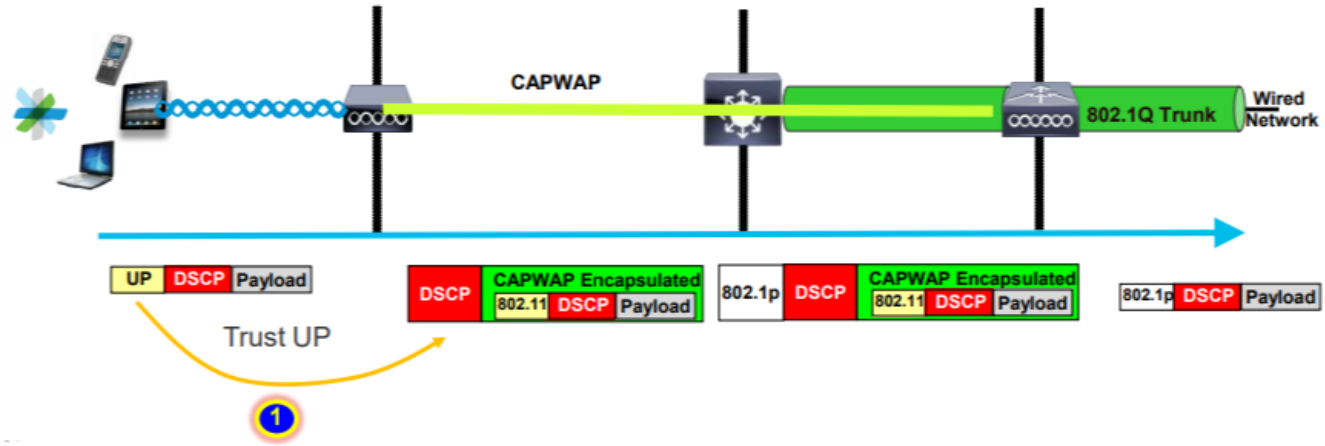
2- Una vez que el AP recibe esta trama Ethernet, el AP mapea el valor DSCP del router al valor UP y lo envía al cliente inalámbrico con el AC correcto.



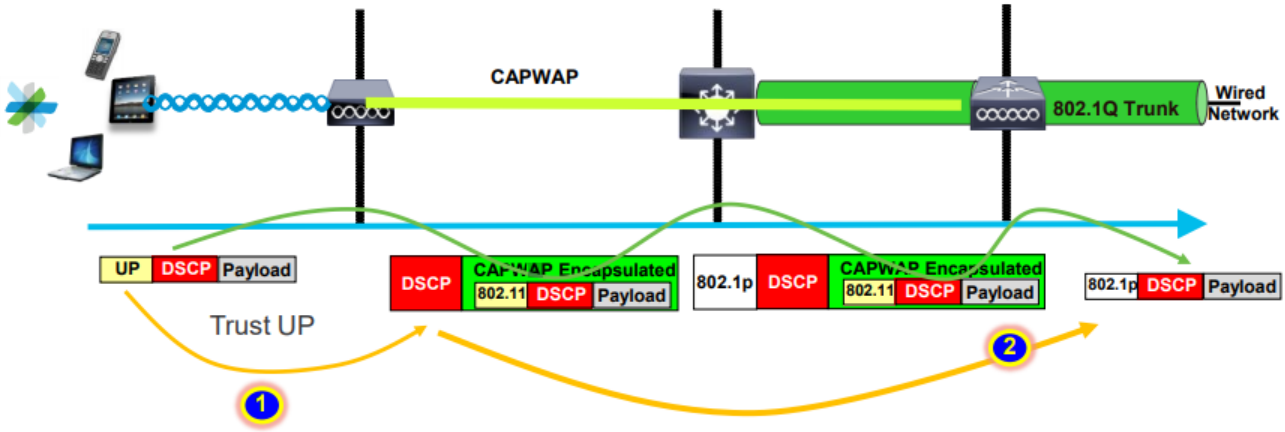
Switching central: confianza ascendente

- Flujo ascendente: tráfico de inalámbrico a por cable.

1. El cliente inalámbrico envía la trama 802.11e (WMM) y el AP la recibe.



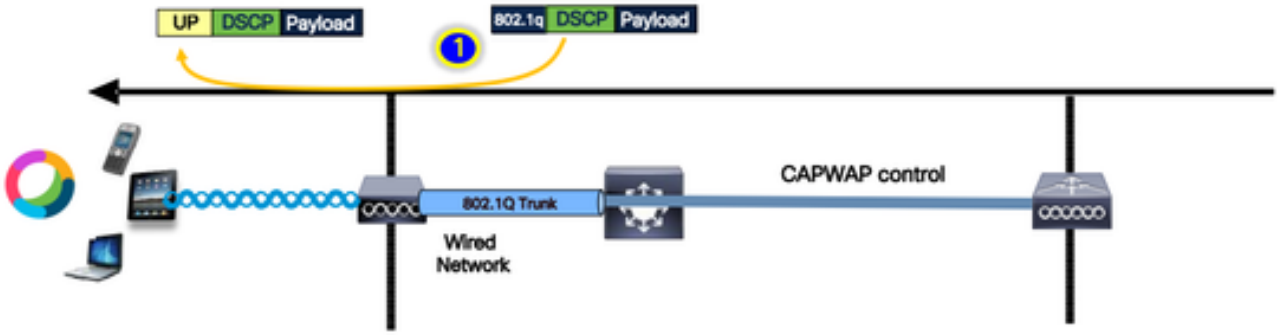
2- El AP encapsula el paquete original en un encabezado CAPWAP y mapea la UP a un valor DSCP de router siempre que el perfil de QoS configurado en el WLC permita ese nivel de QoS. El paquete se envía a la red con cables con el valor DSCP original.



Confianza de switching local de Flexconnect

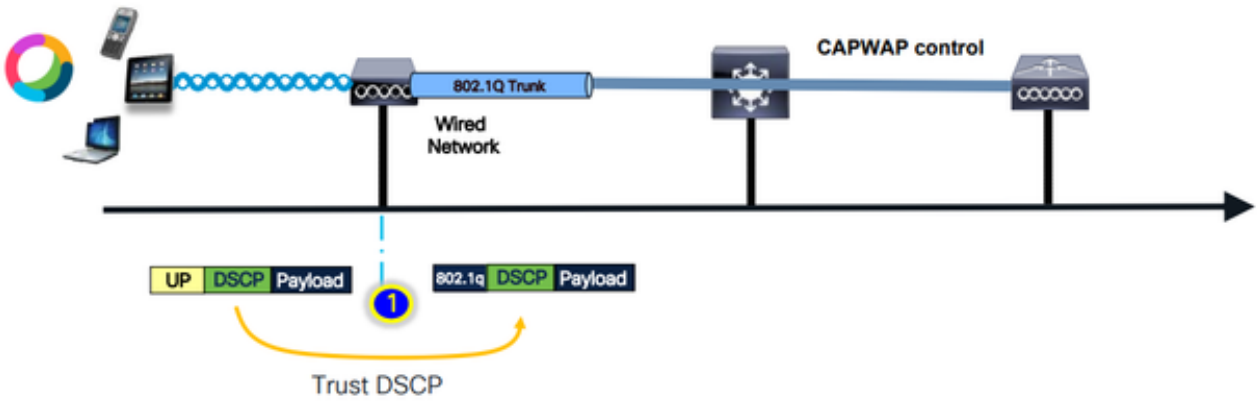
- Switching local Flexconnect: confianza descendente

Para las VLAN conmutadas localmente, el AP FlexConnect toma el valor DSCP del paquete IP, procesa cualquier política de QoS (por ejemplo, la política AVC), la asigna al valor UP 802.11e en la trama inalámbrica y pone en cola la trama . Luego se lo envía al cliente.



- Switching local de Flexconnect: confianza ascendente

El cliente envía la trama y es recibida por el AP. El AP observa el valor DSCP del paquete original para aplicar cualquier política de QoS antes de enviar el paquete al cableado.



Problemas Comunes Para El Tráfico Ascendente

El tráfico en el escenario ascendente -entre el cliente inalámbrico y el AP- está fuera de control, lo que significa que no tiene control sobre la QoS enviada desde el cliente por el aire.

Para un escenario de trabajo, se espera que el cliente envíe un paquete con los valores correctos de UP y DSCP para que el tráfico esté en la categoría de acceso correcta.

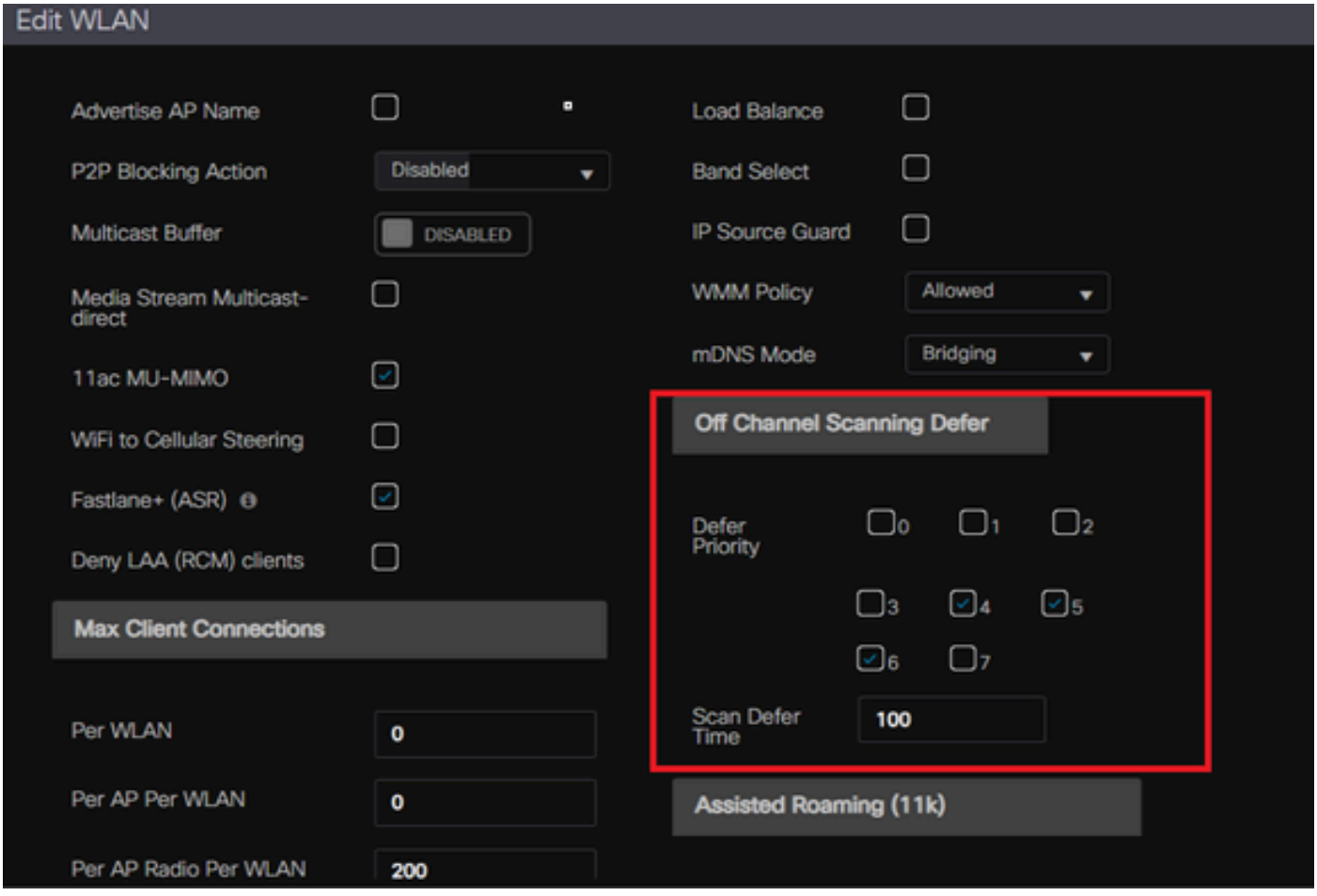
¿Qué ocurre si el cliente transmite tráfico con un valor UP incorrecto?

Ejemplo #1: Cuando el cliente transmite tráfico con un valor UP de "2"

Nota: Los AP salen del canal para escanear y recopilar la información necesaria para el algoritmo RRM. Esto sin duda afecta al tráfico sensible, como el de voz y vídeo.

La opción de aplazamiento del escaneo fuera de canal se configura en la ficha Avanzadas de WLAN. De forma predeterminada, está habilitado para las clases UP 4, 5 y 6, con un umbral de tiempo de 100 milisegundos, lo que significa que el AP no sale del canal para escanear durante un período de 100 ms después de ver el tráfico sensible (voz o video).

Suponga que el cliente inalámbrico está utilizando la aplicación de voz, el valor UP esperado es "6"; sin embargo, el cliente envió el paquete con un valor UP "2" incorrecto. El AP luego pasa por el escaneo fuera del canal y esto afecta el rendimiento y la experiencia del cliente.



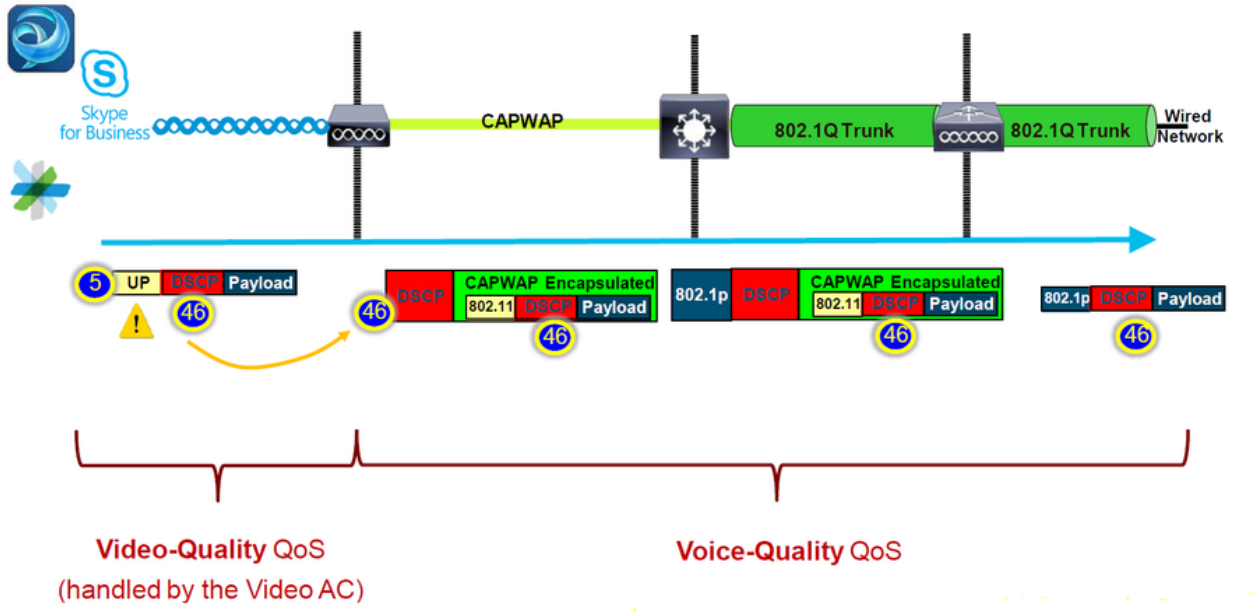
¿Puede activar el aplazamiento del análisis para prioridad baja UP?

La respuesta es sí. La activación de la exploración diferida para el tráfico de baja prioridad UP evita de forma efectiva que el punto de acceso realice exploraciones fuera del canal, lo que afecta al funcionamiento de los algoritmos de detección de RRM y de acceso no autorizado. Para hacer frente a este reto, se requiere un enfoque alternativo que facilite el análisis de canales y, al mismo tiempo, siga dando prioridad al tráfico crítico.

Ejemplo #2: Un problema bien conocido del cliente Microsoft Windows en el mapeo DSCP a UP

Un problema común observado en las máquinas MS Windows ocurre cuando se utiliza la correspondencia predeterminada entre los valores DHCP y UP. En esta asignación, la prioridad de usuario (UP) se determina a partir de los tres bits más significativos (msb) del valor del punto de código de servicios diferenciados (DSCP). Por ejemplo, para el tráfico de voz con un valor DSCP de EF (101110), se asignaría a UP 5 (101).

De forma predeterminada, los AP en Upstream confían en el valor UP, lo que hace que el tráfico de voz se trate en la categoría de acceso de vídeo (AC_VI) con un valor DSCP de 34 en lugar de en la categoría de acceso de voz (AC_VO) con un valor DSCP de 46, para la que está previsto. Para esto, las tramas de voz tienen tiempos de espera más largos y una mayor probabilidad de reintentos.



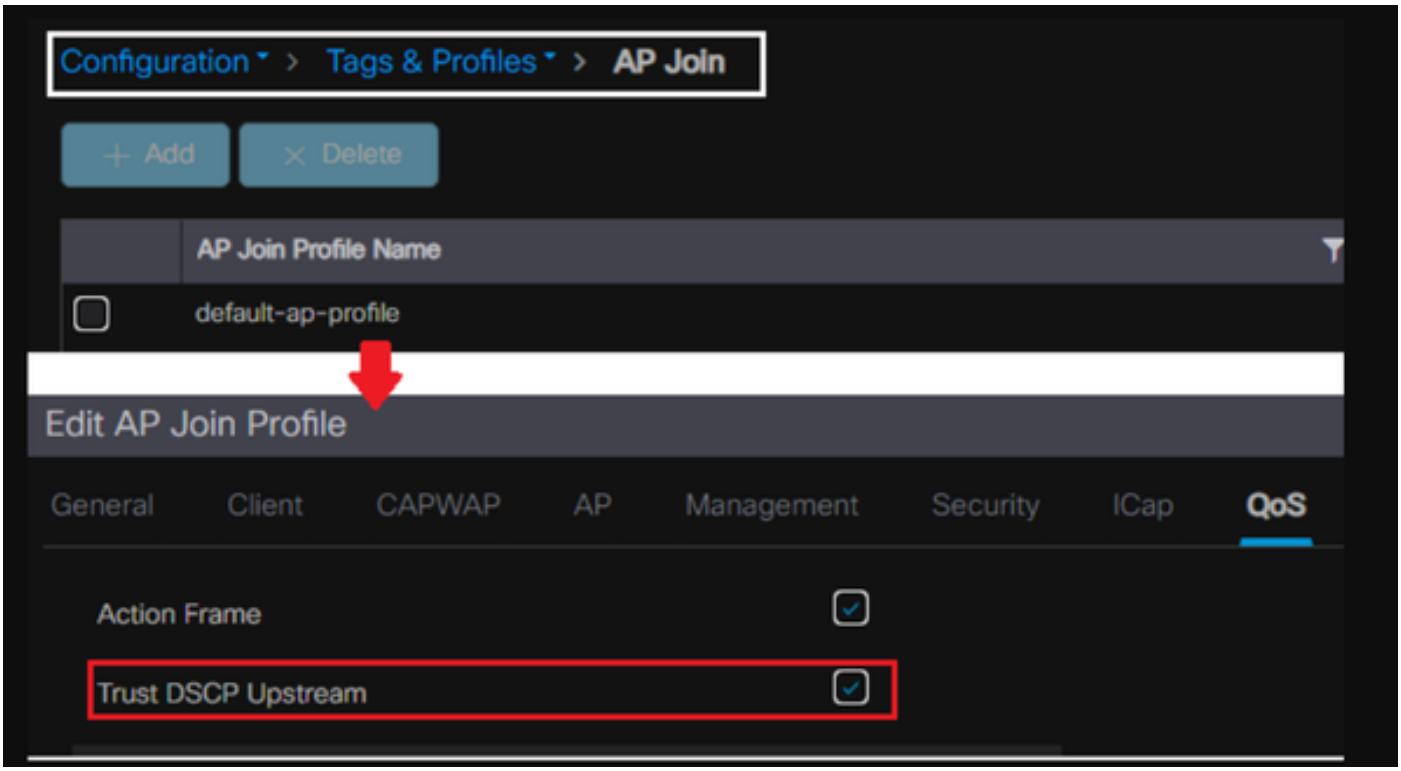
¿Hay alguna manera de arreglar esto?

La respuesta es sí si la máquina MS Windows envía tráfico de voz con el valor DSCP correcto.

¿Cómo se puede arreglar?

Usando la opción "trust DSCP Upstream" en el WLC. Esta opción fuerza al AP a confiar en el

DSCP interno en el Upstream en lugar de en el UP.



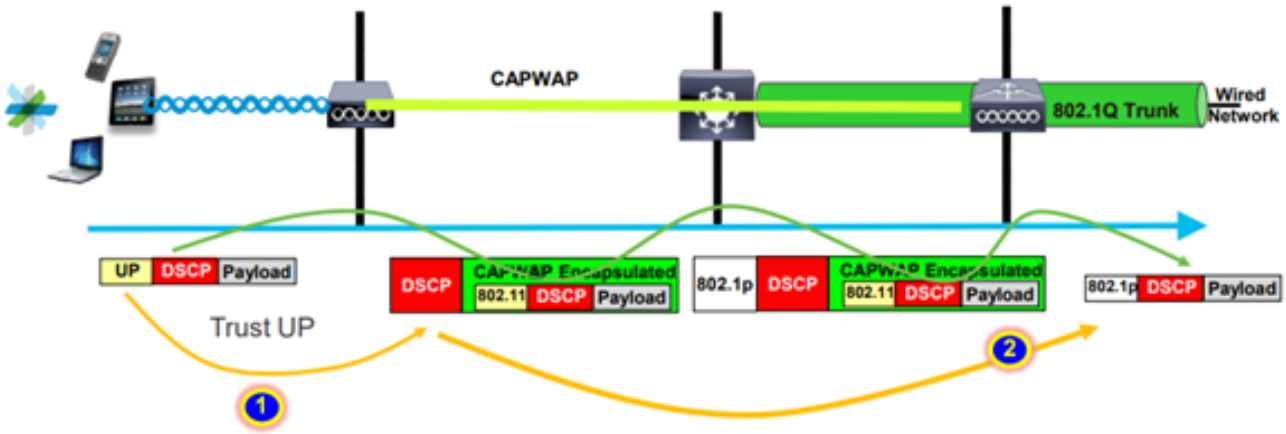
Para obtener más instrucciones sobre cómo configurar su máquina con Windows para anular o etiquetar el tráfico, consulte "Cómo habilitar el etiquetado DSCP en máquinas con Windows"

¿Qué protocolo se debe confiar: DSCP o COS?

¿Qué tipo de confianza seleccionar para el puerto del switch WLC?

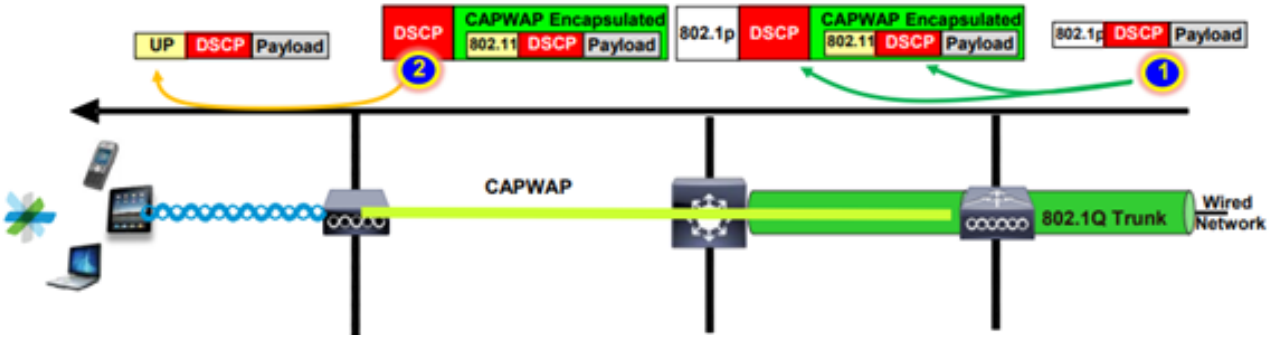
En realidad, podemos elegir cualquiera de las opciones de confianza. Sin embargo, debe tener en cuenta que para el escenario Upstream si elige confiar en la CoS; el switch reescribe el valor DSCP externo basado en la tabla de asignación CoS-DSCP configurada en el switch.

Sin embargo, si elige confiar en DSCP, el switch no vuelve a escribir el valor DSCP externo ya que confía en el DSCP interno entrante.



Para el escenario descendente, el switch donde el WLC está conectado agrega el valor 802.1p basado en la tabla de mapping DSCP-CoS configurada en él. Si elige confiar en la CoS, el valor DSCP externo se cambia en función del valor 802.1p entrante.

Sin embargo, si elige confiar en DSCP, el switch no reescribe el valor DSCP exterior.



Como ejemplo de lo anterior, el cliente inalámbrico se conectó a un SSID asignado a la interfaz de administración en la VLAN nativa.

¿Qué sucede si elige confiar en CoS en el puerto del switch WLC?

El tráfico del cliente llega al puerto troncal, no está etiquetado a 802.1q, ya que es una VLAN nativa sin etiquetas.

¿Qué puedes hacer para arreglar esto?

Puede utilizar la opción de confianza DSCP en lugar de CoS, que es generalmente la recomendación.

Prácticas recomendadas de QoS del controlador de LAN inalámbrica

Perfiles de QoS de metal

Podemos configurar cuatro perfiles QoS principales en el WLC (Platino, Oro, Plata, Bronce).

- Platino/voz: garantiza un servicio de alta calidad para voz sobre tecnología inalámbrica
- Gold/vídeo: admite aplicaciones de vídeo de alta calidad
- Silver/best effort: admite ancho de banda normal para clientes; este es el parámetro predeterminado
- Bronze/background: proporciona el ancho de banda más bajo para los servicios de invitados.

El propósito principal de estos perfiles de QoS es limitar el valor máximo de DSCP externo en el encabezado CAPWAP tanto para el flujo ascendente como para el descendente sin afectar el DSCP interno.

Nota: AVC modifica el valor DSCP interno.

Para el tráfico conmutado localmente, el perfil de QoS se aplica al tráfico descendente basado en el valor UP. Si este valor es mayor que el valor predeterminado de WLAN, se utiliza el valor predeterminado de WLAN.

Para el tráfico ascendente, si el cliente envía un valor UP mayor que el valor WLAN predeterminado; se utiliza el valor WLAN predeterminado.

Para obtener más detalles sobre la guía de configuración de prácticas recomendadas del WLC 9800 QoS inalámbrica para el controlador inalámbrico Catalyst 9800

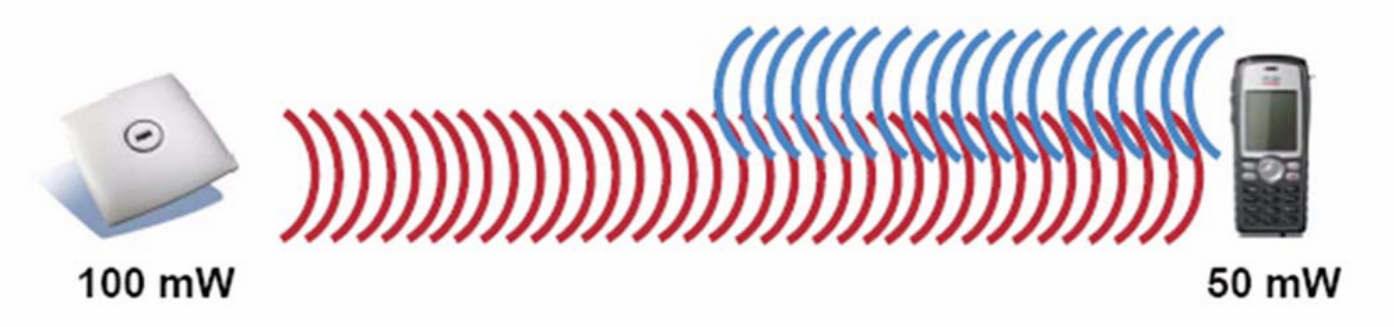
Pasos para la resolución de problemas:

1. Entienda el problema.
2. Cree un plan de acción sólido.
    - Haga preguntas sobre resolución de problemas y elabore un diagrama de topología de red.
    - Recopilar registros y depuraciones.
    - Pregunte por los Mapas de Calor PI.
3. Compruebe las configuraciones del WLC.
4. Analizar las depuraciones
5. Utilice la lista de comprobación de VoWLAN para confirmar si se han seguido las prácticas recomendadas.

Descripción del audio unidireccional

Principalmente, este problema ocurre cuando tenemos energía asimétrica entre el cliente y el AP.

Los AP pueden transmitir con la potencia máxima, sin embargo los dispositivos inalámbricos tales como los teléfonos de Cisco pueden transmitir con menos energía haciendo que los teléfonos de Cisco oigan las tramas descendentes del AP, pero AP no oye las tramas en Upstream de los teléfonos.



Se recomienda no configurar la potencia TX del punto de acceso superior a la potencia TX máxima admitida en el dispositivo inalámbrico.

- Plan de acción:
  - Compruebe la conexión del cliente y asegúrese de que es estable y que no hay desconexiones.
  - Compruebe el entorno de radiofrecuencia (potencia del punto de acceso, potencia de la señal, etc.).
  - Recopile capturas de OTA para verificar el tráfico de audio; se ve el tráfico de una sola dirección.

- Mejores medidas:
  - Habilitar DTPC: ayuda a los clientes CCX a ajustar su potencia TX para que coincida con la potencia AP.
  - Compruebe la configuración del volumen en el dispositivo cliente.

Comprensión del audio entrecortado y robótico

Tanto el audio "entrecortado" como el "robótico" se producen cuando se produce una gran pérdida de paquetes o cuando el paquete se retrasa.

La voz entrecortada describe los huecos y el retardo en el sonido. Estos son ejemplos de registros entrecortados y robóticos.

- Plan de acción:
  - Compruebe la conexión del cliente y asegúrese de que es estable y que no hay desconexiones.
  - Compruebe el entorno de RF (utilización de canales altos, dispositivos con interferencias y ruido, etc.).
  - Recopile las capturas a través de la ruta para verificar si se han descartado paquetes.
- Mejores medidas:
  - Verifique las configuraciones de QoS en el WLC.
  - Asegúrese de que QoS esté configurado en el lado cableado.

Descripción de las lagunas y ausencia de audio durante la itinerancia

A veces, los usuarios informan de lagunas y pérdida de la conexión de audio cuando se desplazan de una ubicación a otra.

- Plan de acción:
  - Verifique el entorno de RF y confirme que tiene una buena celda de cobertura entre los AP.
  - Obtener mapa de calor PI.
  - Recopile las capturas a través de la ruta para verificar si se han descartado paquetes.
- Mejores medidas:
  - Compruebe la conexión del cliente y asegúrese de que es estable y que no hay desconexiones.
  - Asegúrese de que el valor RSSI en el AP de destino sea mayor o igual a -67

Referencias

Recomendaciones de QoS inalámbrica

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg/m_wireless_qos_cg_vewlc1_from_17_3_1_onwards.html

Guía de implementación de Visibilidad y control de aplicaciones para controladores inalámbricos Cisco Catalyst serie 9800

https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-1/deployment-guide/c9800-avc-deployment-guide-rel-17-1.pdf

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).