Présentation du dépannage de la QoS sur un WLC sans fil 9800 (& de référence)

Table des matières

Introduction

Ce document décrit la QoS sur les contrôleurs LAN sans fil 9800

Conditions préalables

Exigences

Ce document explique comment hiérarchiser et étiqueter le trafic en amont et en aval. Il explique

les meilleures pratiques de configuration du trafic vocal sur le contrôleur de réseau local sans fil (WLC) et les techniques de dépannage pour les problèmes vocaux courants.

Composants utilisés

WLC 9800 basé sur la version 17.12 de Cisco IOS® XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Brève description de la norme IEEE 802.11e et du Wi-Fi Multimedia (WMM)

WMM est une Wi-Fi Alliance basée sur la norme IEEE 802.11e. WMM fournit des fonctionnalités de qualité de service (QoS) en hiérarchisant le trafic selon quatre catégories d'accès : voix, vidéo, meilleur effort et arrière-plan, en fonction de la méthode EDCA (Enhanced Distributed Channel Access).

L'activation de WMM est essentielle pour obtenir des performances optimales dans les réseaux Wi-Fi, en particulier dans les environnements où les applications à bande passante élevée et à faible latence sont répandues. Par exemple, dans les réseaux 802.11n, WMM est nécessaire pour tirer pleinement parti des fonctionnalités de cette norme Wi-Fi haut débit.

Files d'attente WMM et EDCA (Enhanced Distributed Channel Access)

En règle générale, toute station doit écouter le support pour vérifier s'il est inactif avant d'envoyer les trames. Une fois la trame envoyée, la station écoute le support pour voir si une collision s'est produite.

Les clients sans fil ne peuvent pas détecter les collisions. Pour cela, CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) est utilisé. Il utilise un temporisateur fixe et aléatoire (CWmin, CWmax) et chaque trame qui est envoyée doit être reconnue afin que nous sachions qu'il n'y a pas de collision et que tous les clients puissent envoyer leur trafic.

Comme nous l'avons mentionné précédemment, nous avons quatre catégories d'accès (files d'attente), chacune d'elles utilisant des compteurs différents. Les trames de priorité supérieure sont envoyées statistiquement plus tôt, et les trames de priorité inférieure ont des paramètres de réémission différée, ce qui les rend statistiquement envoyées ensuite.

En résumé, l'existence de quatre files d'attente ne garantit pas à elle seule la qualité de service (QoS) ; ce qui compte vraiment, c'est la manière dont le trafic au sein de chaque file d'attente est géré efficacement.

Mise en œuvre de QoS

Par défaut, si la qualité de service (QoS) n'est pas configurée, le trafic réseau est traité de manière égale, avec un modèle de livraison au mieux. Cela signifie que tout le trafic, quel que soit son type ou son importance, a la même priorité et la même chance d'être acheminé à tout moment. Cependant, lorsque les fonctionnalités QoS sont activées et correctement configurées, la priorité peut être attribuée à des types spécifiques de trafic réseau, tels que la voix et la vidéo.

La configuration de la qualité de service comporte deux composants principaux : la classification et le marquage.

Classification :

La classification implique l'identification et la catégorisation du trafic réseau en fonction de critères spécifiques, tels que le type d'application, l'adresse IP source/de destination, le protocole ou le numéro de port. Le trafic est divisé en classes ou en files d'attente :

1. Voix : AC_VO
2. Vidéo : AC_VI
3. Au mieux : AC_BE
4. Contexte : AC_BK

Marquage :

Une fois que le trafic est classé dans des files d'attente, le marquage implique l'attribution de marquages ou de balises QoS aux paquets pour indiquer leur niveau de priorité.

Il y a plusieurs façons de marquer le trafic. Les deux principales normes sont la classe de service 802.1p de couche 2 (Class of Service) et le DSCP de couche 3 (Differentiated Services Code Point).

CoS « 802.1p » de couche 2 (classe de service)

Dans la norme 802.1p, il existe sept niveaux de CoS, chacun représenté par un champ de 3 bits pouvant prendre des valeurs comprises entre 0 et 7. Ces valeurs indiquent la priorité du trafic, 0 étant la priorité la plus faible et 7 la priorité la plus élevée.

Remarque : 802.1p est un sous-ensemble de la norme 802.1q. Il n'est présenté que lorsqu'une étiquette VLAN est présente, par exemple sur les ports d'agrégation.

Tableau 1 : Classification 802.1P et 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 couche 3 (Differentiated Services Code Point)

DSCP est une balise de couche 3 sur l'en-tête IP, il utilise 6 bits permettant 64 valeurs différentes (0 à 63).

Tableau 2 : Classification DSCP et 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

Les valeurs DSCP prédominantes sont 46 (EF) pour la voix, 34 (AF41) pour la vidéo et 0 (BE) pour le meilleur effort.

Mappage DSCP vers UP par défaut

Comme nous l’avons vu précédemment, UP est un champ de 3 bits dans la trame Ethernet, tandis que DSCP est un champ de 6 bits dans l’en-tête IP.

Comment pouvez-vous calculer la valeur UP (User Priority) de couche 2 à partir de la valeur DSCP (Differentiated Services Code Point) de couche 3 ?

Actuellement, il n'existe pas de norme spécifique pour ce mappage. Cependant, une méthode

courante est utilisée et connue sous le nom de « mappage DSCP vers UP par défaut ».

La méthode de mappage DSCP vers UP dérive les valeurs UP des 3 msb du paquet DSCP, puis le mappe sur la catégorie d'accès appropriée.

Cette méthode est utilisée par les machines Microsoft Windows et donne lieu à un problème bien connu qui est traité plus en détail dans l'Exemple #2 : Un problème de client Microsoft Windows bien connu dans le mappage DSCP vers UP

Tableau 3 : Mappage DSCP vers UP par défaut

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	

Flux de paquets et confiance QoS

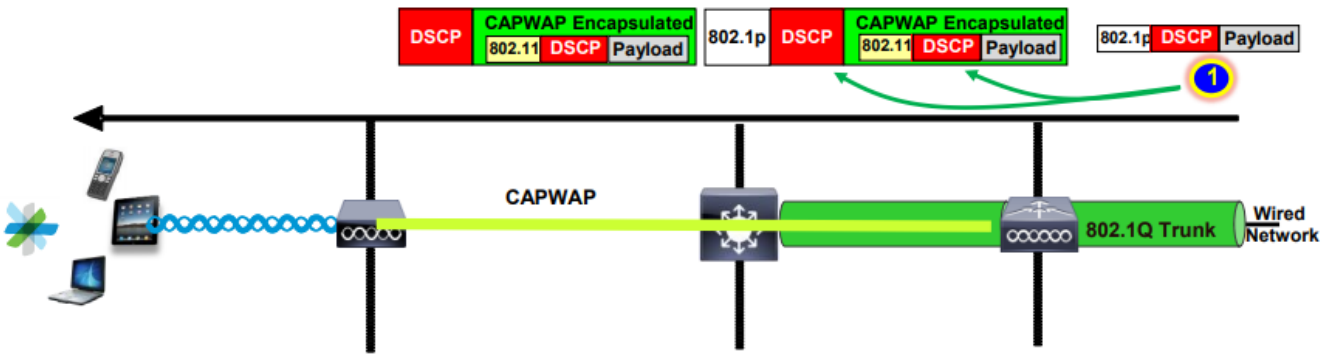
Cette section traite du flux de paquets et de la confiance QoS dans ces différents scénarios :

1. Commutation centrale - Confiance en aval.
2. Commutation centrale - Confiance en amont.
3. Confiance de commutation locale FlexConnect.

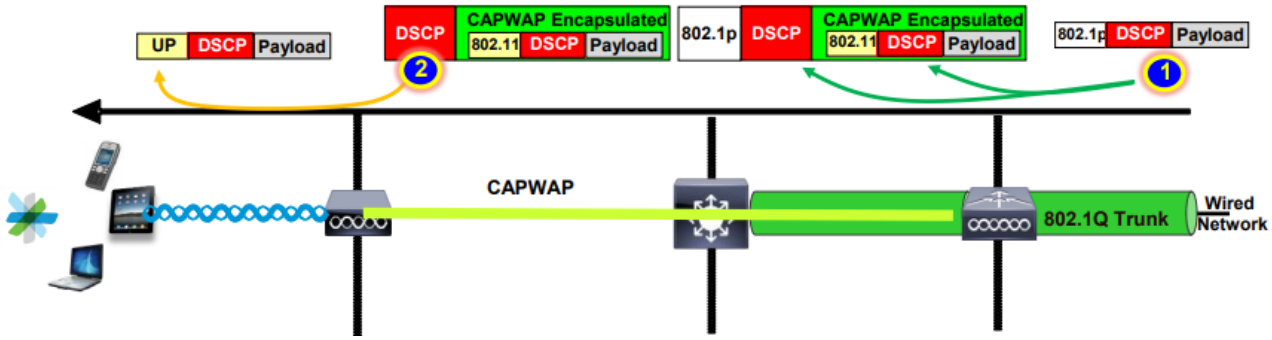
Commutation centrale - Confiance en aval

- En aval : trafic du filaire au sans fil.
- Le trafic en aval est encapsulé CAPWAP.

1- Une trame Ethernet est reçue sur le port trunk WLC 802.1q. Le WLC utilise la valeur DSCP interne envoyée depuis le réseau câblé et la mappe au DSCP externe dans l'en-tête CAPWAP, il limite le DSCP externe à une valeur maximale selon le profil QoS configuré sur le WLC.



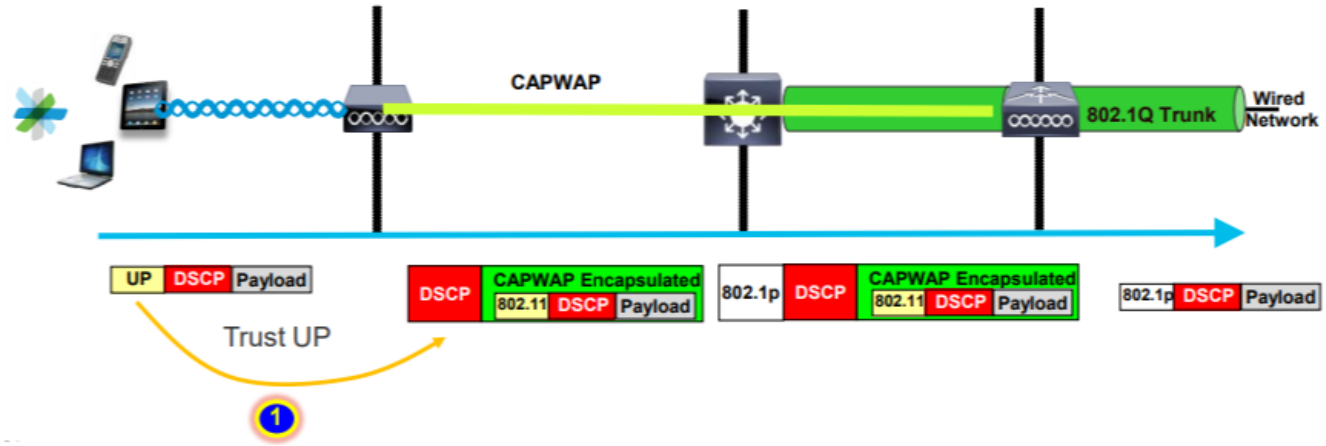
2- Une fois que cette trame Ethernet est reçue par le point d'accès, le point d'accès mappe la valeur DSCP externe à la valeur UP et l'envoie au client sans fil avec le bon CA.



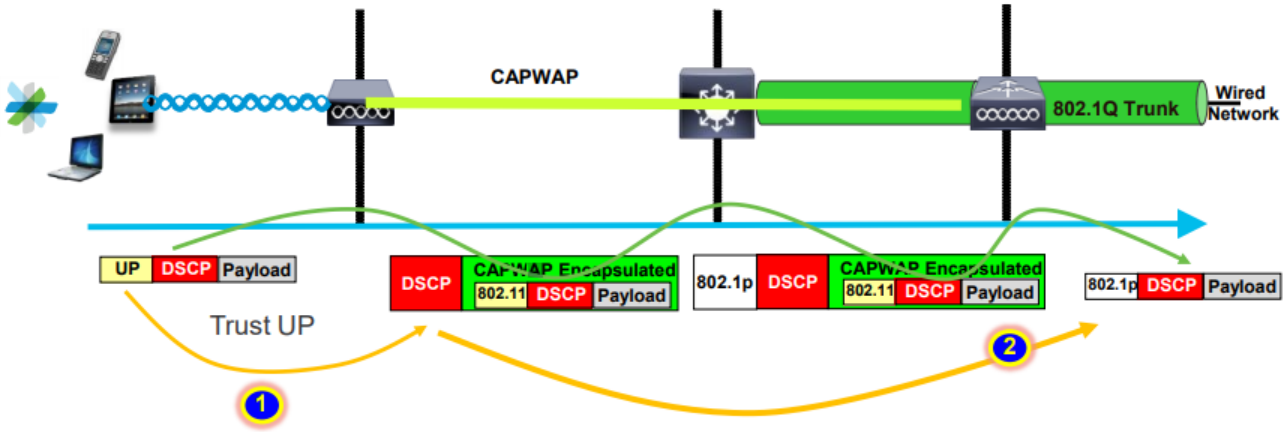
Commutation centrale - Confiance en amont

- En amont : trafic du réseau sans fil au réseau filaire.

1. Le client sans fil envoie la trame 802.11e (WMM) et celle-ci est reçue par le point d'accès.



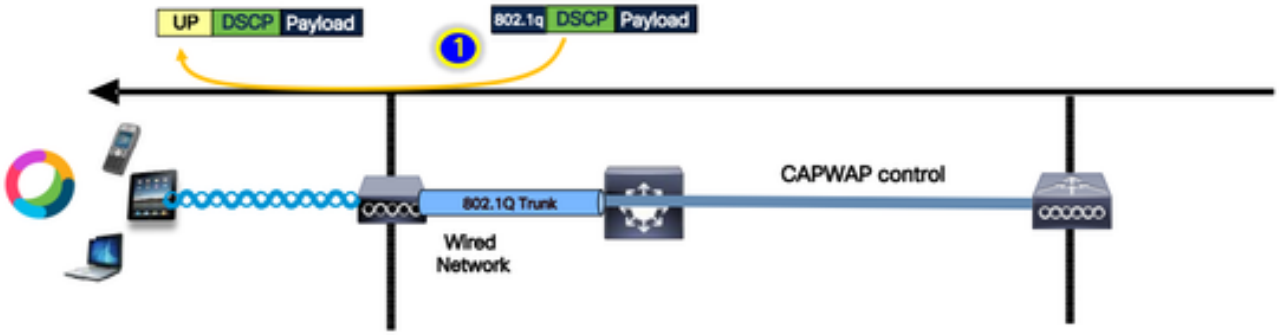
2- Le point d'accès encapsule le paquet d'origine dans un en-tête CAPWAP et mappe le point d'accès à une valeur DSCP externe tant que le profil QoS configuré sur le WLC autorise ce niveau de QoS. Le paquet est envoyé au réseau câblé avec la valeur DSCP d'origine.



Confiance de commutation locale Flexconnect

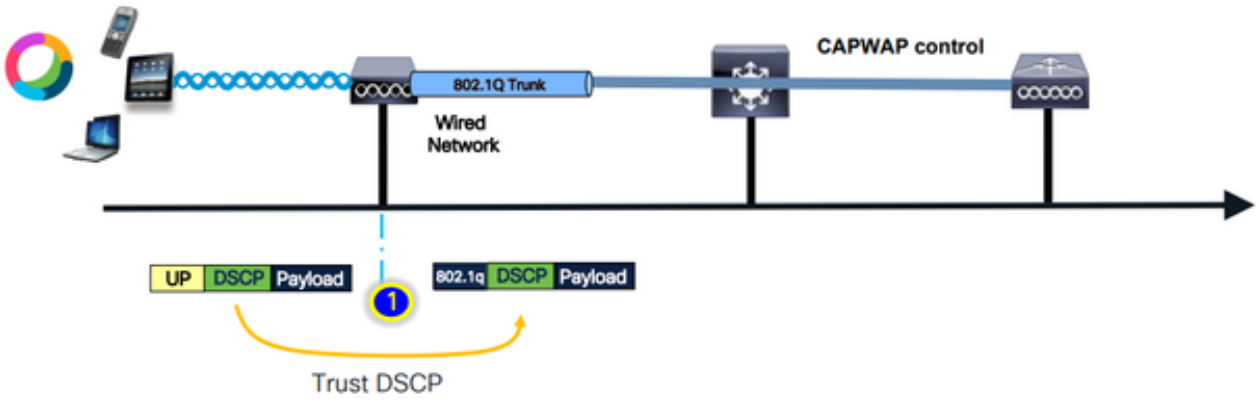
- Commutation locale Flexconnect - Confiance en aval

Pour les VLAN commutés localement, le point d'accès FlexConnect prend la valeur DSCP du paquet IP, traite toute stratégie QoS (par exemple la stratégie AVC), la mappe à la valeur 802.11e UP sur la trame sans fil et met la trame en file d'attente . Il l'envoie ensuite au client.



- Commutation locale Flexconnect - Confiance en amont

Le client envoie la trame et elle est reçue par le point d'accès. Le point d'accès examine la valeur DSCP du paquet d'origine pour appliquer une stratégie QoS avant d'envoyer le paquet au réseau câblé.



Problèmes courants pour le trafic en amont

Le trafic en amont (entre le client sans fil et le point d'accès) est hors de contrôle, ce qui signifie que vous n'avez aucun contrôle sur la qualité de service envoyée par le client par liaison radio.

Dans un scénario de travail, le client est censé envoyer un paquet avec les valeurs UP et DSCP correctes afin que le trafic soit dans la catégorie d'accès correcte.

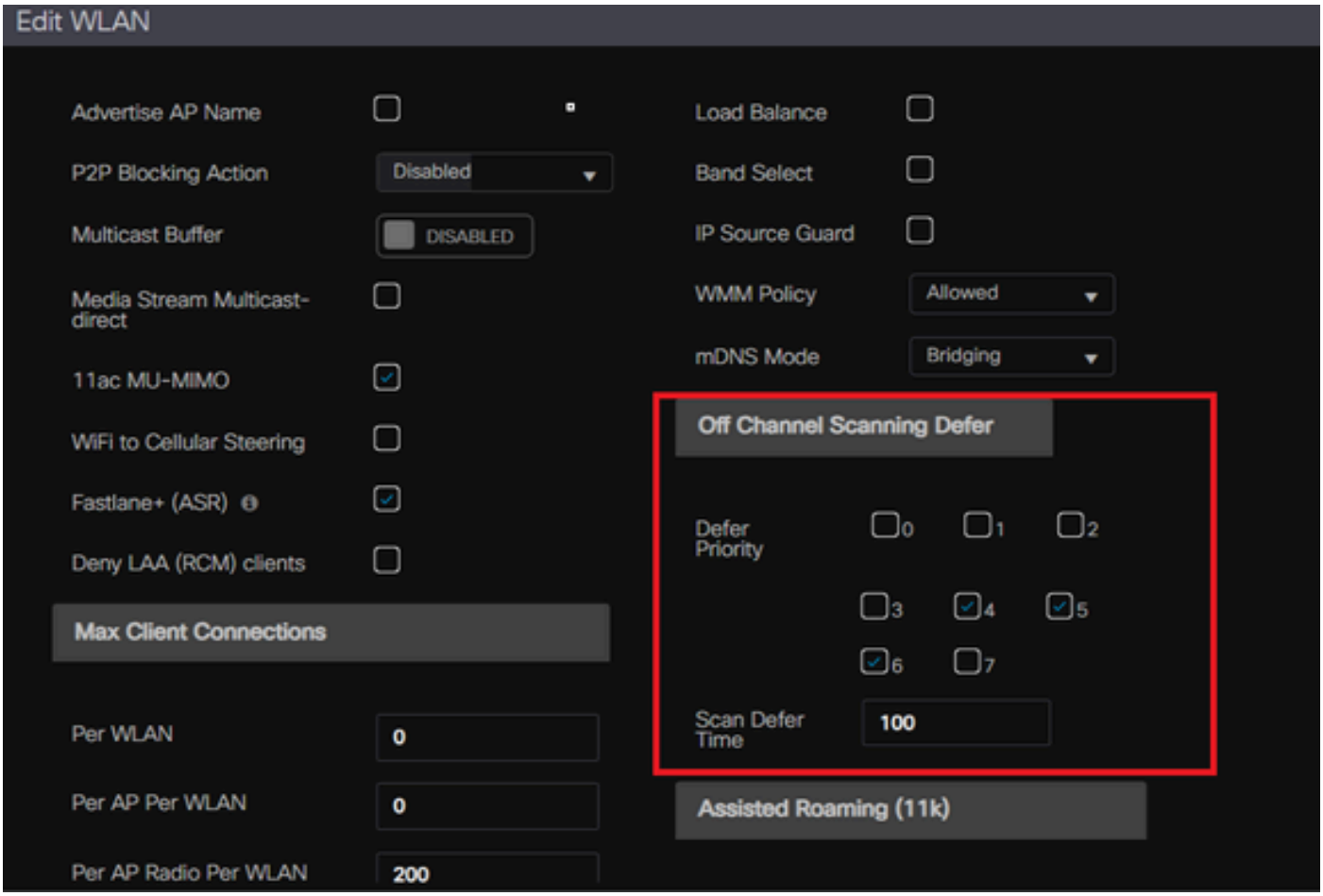
Que se passe-t-il si le client transmet du trafic avec une valeur UP incorrecte ?

Exemple #1 : lorsque le client transmet du trafic avec une valeur UP de "2"

Remarque : les points d'accès sortent du canal pour effectuer une analyse afin de collecter les informations nécessaires à l'algorithme RRM. Cela a un impact certain sur le trafic sensible comme la voix et la vidéo.

L'option Off Channel Scanning Defer est configurée sous l'onglet WLAN Advanced. Par défaut, il est activé pour les classes UP 4, 5 et 6, avec un seuil de temps de 100 millisecondes, cela signifie que le point d'accès ne sort pas du canal pour scanner pendant une période de 100 ms après avoir vu le trafic sensible (voix ou vidéo).

Supposons que le client sans fil utilise une application vocale, la valeur UP attendue est « 6 ». Toutefois, le client a envoyé le paquet avec une valeur UP « 2 » incorrecte. Le point d’accès effectue ensuite une analyse hors canal, ce qui a un impact sur les performances et l’expérience du client.



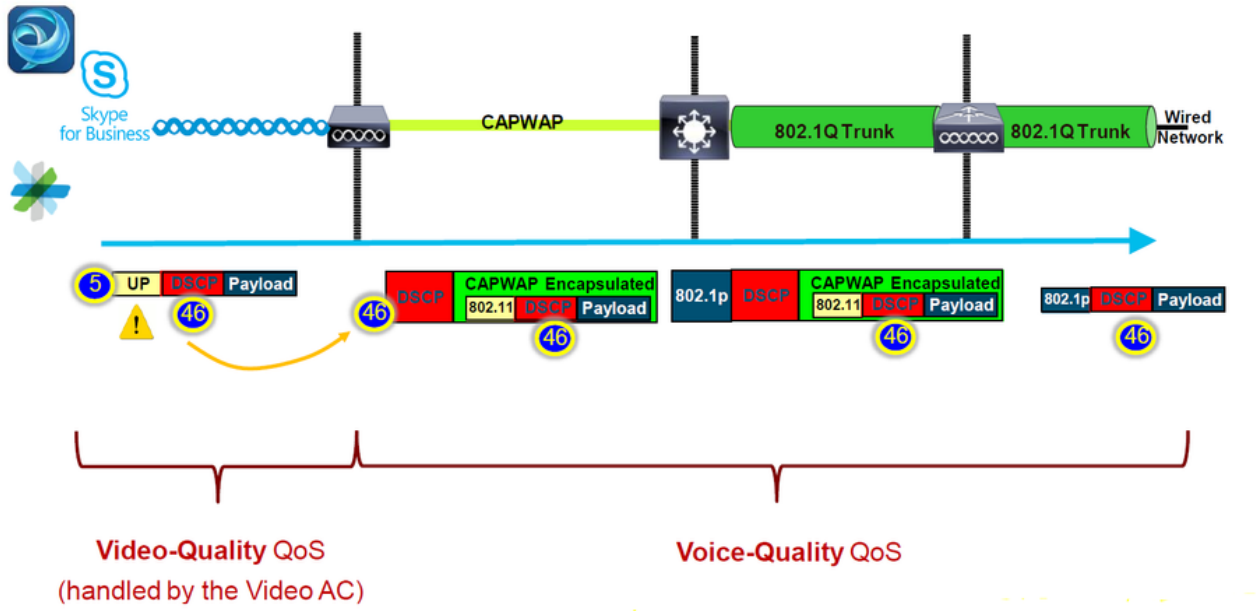
Pouvez-vous activer l'option Différer l'analyse pour une priorité faible ?

La réponse est oui. L'activation de l'option Différer l'analyse pour le trafic de faible priorité UP empêche efficacement le point d'accès d'effectuer des analyses hors canal, ce qui a un impact sur le fonctionnement du RRM et des algorithmes de détection des systèmes non fiables. Pour relever ce défi, une autre approche est nécessaire pour faciliter l'analyse des canaux tout en hiérarchisant le trafic critique.

Exemple #2 : Un problème bien connu de client Microsoft Windows dans le mappage DSCP vers UP

Un problème courant observé sur les ordinateurs MS Windows se produit lorsque le mappage par défaut entre les valeurs DHCP et UP est utilisé. Dans ce mappage, la priorité utilisateur (UP) est déterminée à partir des trois bits de poids fort (msb) de la valeur DSCP (Differentiated Services Code Point). Par exemple, pour le trafic vocal avec une valeur DSCP EF (101110), il serait mappé à UP 5 (101).

Par défaut, les points d'accès en amont font confiance à la valeur UP, ce qui entraîne le traitement du trafic vocal dans la catégorie d'accès vidéo (AC_VI) avec la valeur DSCP 34 au lieu de la catégorie d'accès vocal (AC_VO) avec la valeur DSCP 46, pour laquelle elle est prévue. Pour cela, les trames vocales ont des temps d'attente plus longs et une plus grande probabilité de nouvelles tentatives.

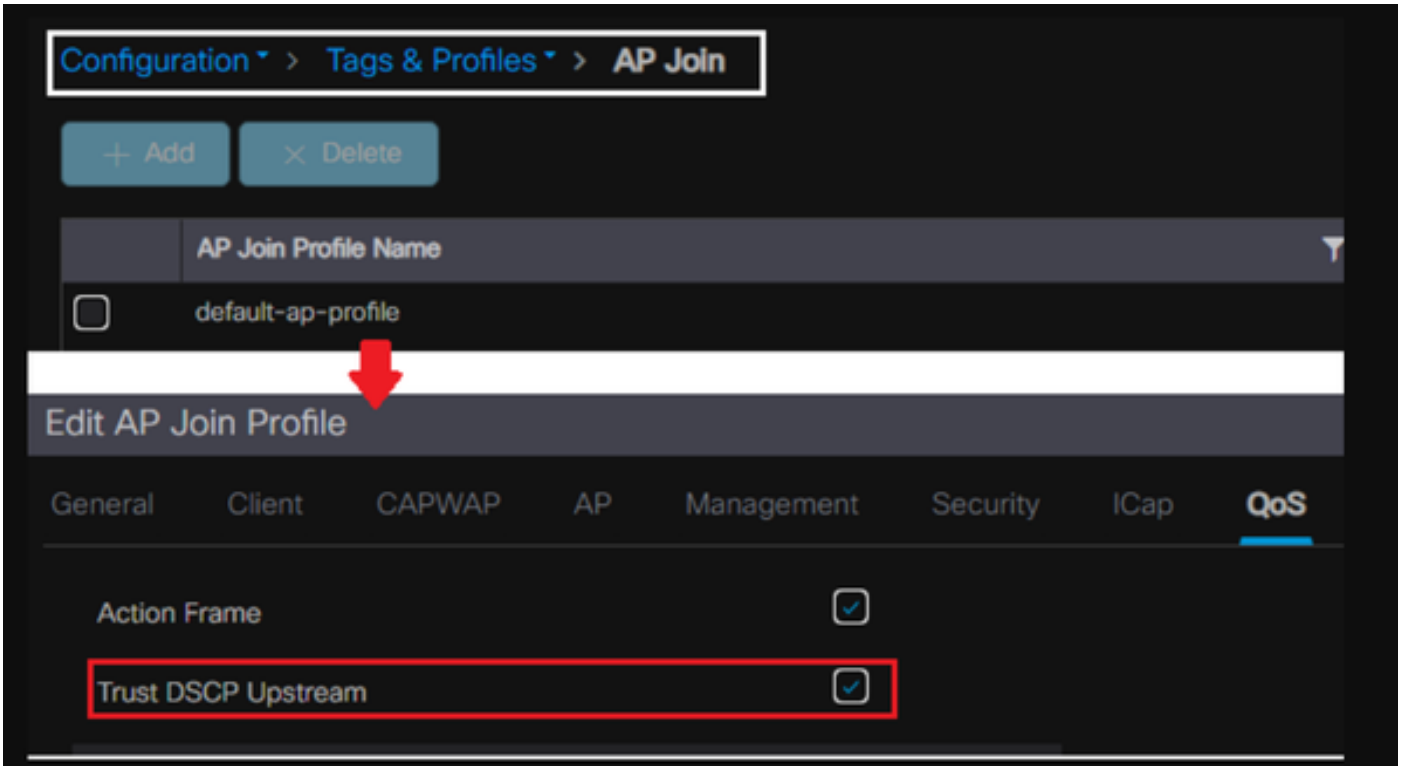


Y a-t-il un moyen de réparer ça ?

La réponse est oui si la machine MS Windows envoie du trafic vocal avec la valeur DSCP correcte.

Comment peut-il être réparé ?

En utilisant l'option « trust DSCP Upstream » sur le WLC. Cette option force l'AP à faire confiance au DSCP interne dans l'Upstream au lieu de l'UP.



Pour plus d'instructions sur la configuration de votre machine Windows pour remplacer ou

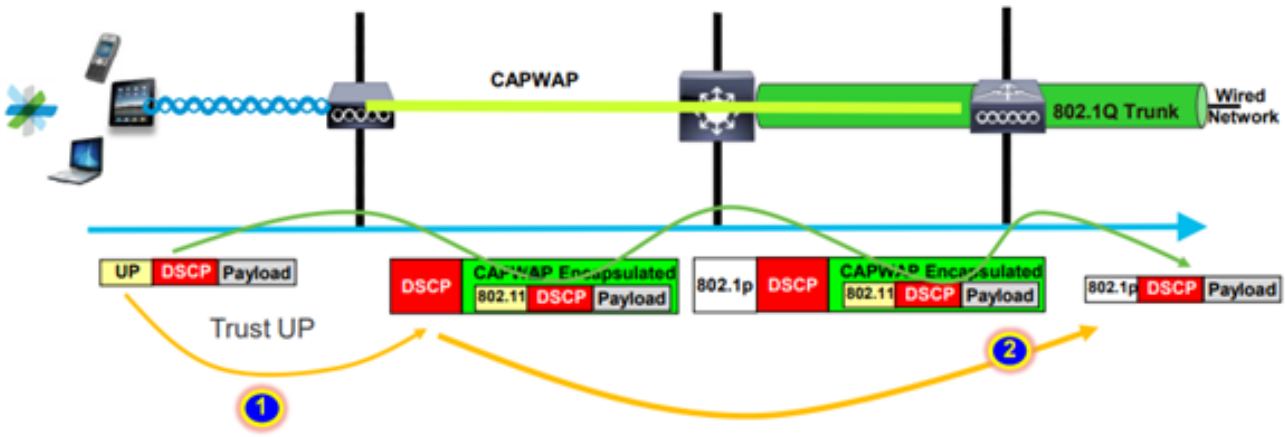
marquer le trafic, veuillez vous référer à "Comment activer le marquage DSCP sur les machines Windows"

Quel protocole faire confiance à : DSCP ou COS ?

Quel type d'approbation sélectionner pour le port de commutateur WLC ?

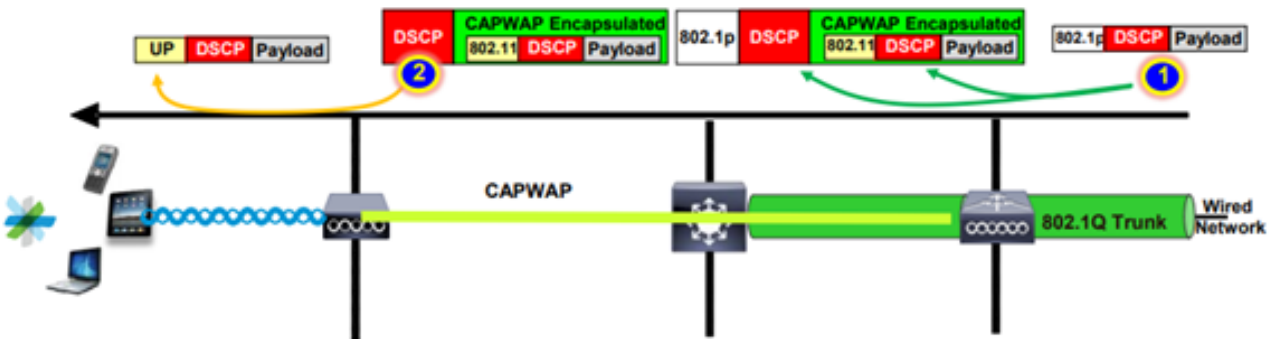
En fait, nous pouvons choisir n'importe laquelle des options de confiance. Cependant, vous devez garder à l'esprit que pour le scénario en amont, si vous choisissez d'approuver CoS, le commutateur réécrit la valeur DSCP externe en fonction de la table de mappage CoS-DSCP configurée sur le commutateur.

Cependant, si vous choisissez d'approuver le DSCP, le commutateur ne réécrit pas la valeur DSCP externe car il approuve le DSCP interne entrant.



Pour le scénario en aval, le commutateur où le WLC est connecté ajoute la valeur 802.1p basée sur la table de mappage DSCP-CoS configurée sur celui-ci. Si vous choisissez d'approuver la CoS, la valeur DSCP externe est modifiée en fonction de la valeur 802.1p entrante.

Cependant, si vous choisissez d'approuver DSCP, le commutateur ne réécrit pas la valeur DSCP externe.



Comme exemple ci-dessus, client sans fil connecté à un SSID mappé à l'interface de gestion sur le VLAN natif.

Que se passe-t-il si vous choisissez de faire confiance à CoS sur le port de commutateur WLC ?

Le trafic client atteint le port trunk, il n'est pas étiqueté sur 802.1q car il s'agit d'un VLAN natif non étiqueté.

Que pouvez-vous faire pour réparer ceci ?

Vous pouvez utiliser l'option de confiance DSCP au lieu de CoS, ce qui est généralement recommandé.

Meilleures pratiques QoS du contrôleur LAN sans fil

Profils QoS métalliques

Nous pouvons configurer quatre profils QoS principaux sur le WLC (Platinum, Gold, Silver, Bronze).

- Platinum/voix : garantit une qualité de service élevée pour la voix sur sans fil.
- Gold/vidéo - prend en charge des applications vidéo de haute qualité
- Silver/best effort - prend en charge la bande passante normale pour les clients ; il s'agit du paramètre par défaut
- Bronze/arrière-plan : fournit la bande passante la plus faible pour les services invités.

L'objectif principal de ce profil QoS est de limiter la valeur DSCP externe maximale sur l'en-tête CAPWAP pour les flux amont et aval sans affecter le DSCP interne.

Remarque : la valeur DSCP interne est modifiée par AVC.

Pour le trafic commuté localement, le profil QoS est appliqué au trafic en aval en fonction de la valeur UP. Si cette valeur est supérieure à la valeur WLAN par défaut, la valeur WLAN par défaut est utilisée.

Pour le trafic en amont, si le client envoie une valeur UP supérieure à la valeur WLAN par défaut, la valeur WLAN par défaut est utilisée.

Pour plus d'informations sur le guide de configuration des meilleures pratiques du WLC 9800 QoS sans fil pour le contrôleur sans fil Catalyst 9800

Étapes de dépannage :

1. Comprendre le problème.
2. Créez un plan d'action solide.

- Posez des questions de dépannage et un schéma de topologie du réseau.
- Collecter les journaux et les débogages.
- Demandez des cartes thermiques IP.

3. Vérifiez les configurations WLC.

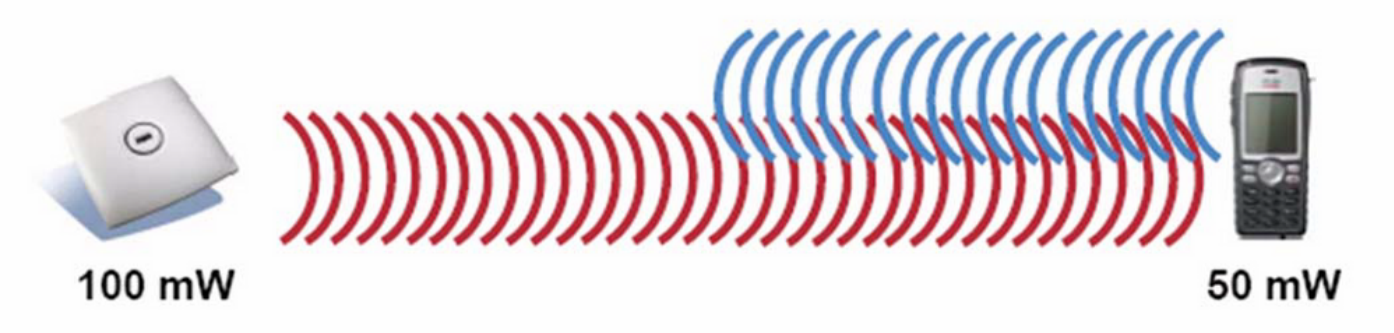
4. Analysez les débogages

5. Utilisez la liste de contrôle VoWLAN pour vérifier si les meilleures pratiques ont été suivies.

Présentation de l'audio unidirectionnel

Ce problème se produit principalement lorsque nous avons une puissance asymétrique entre le client et le point d'accès.

Les points d'accès peuvent transmettre avec une puissance maximale, mais les périphériques sans fil tels que les téléphones Cisco peuvent transmettre avec moins de puissance, ce qui amène les téléphones Cisco à entendre les trames en aval du point d'accès, mais le point d'accès n'entend pas les trames en amont des téléphones.



Il est recommandé de ne pas configurer une puissance TX AP supérieure à la puissance TX maximale prise en charge sur le périphérique sans fil.

- Plan d'action :
  - Vérifiez la connexion du client et assurez-vous qu'elle est stable et qu'aucune déconnexion n'a lieu.
  - Vérifiez l'environnement RF (puissance du point d'accès, intensité du signal, etc.).
  - Collectez les captures OTA pour contrôler le trafic audio ; le trafic à direction unique est détecté.

- Meilleures pratiques :
  - Activer DTPC : il aide les clients CCX à ajuster leur puissance TX pour correspondre à la puissance AP.
  - Vérifiez les paramètres de volume dans le périphérique client.

Présentation de l'audio saccadé et robotique

L'audio « saccadé » et « robotique » se produit lorsque la perte de paquets ou le retard de paquets est important.

La voix instable décrit les lacunes et les retards dans le son. Ce sont des exemples de dossiers instables et robotiques.

- Plan d'action :
  - Vérifiez la connexion du client et assurez-vous qu'elle est stable et qu'aucune déconnexion n'est détectée.
  - Vérifier l'environnement RF (utilisation élevée des canaux, bruits et interférences ... etc.).
  - Collectez les captures via le chemin pour vérifier les abandons de paquets.
- Meilleures pratiques :
  - Vérifiez les configurations QoS sur le WLC.
  - Assurez-vous que la QoS est configurée du côté câblé.

Présentation des interruptions et de l'absence d'audio en itinérance

Parfois, les utilisateurs signalent des interruptions et des pertes de connexion audio lorsqu'ils se déplacent d'un emplacement à un autre.

- Plan d'action :
  - Vérifiez l'environnement RF et assurez-vous que vous avez une bonne cellule de couverture entre les points d'accès.
  - Obtenez la carte de chaleur PI.
  - Collectez les captures via le chemin pour vérifier les abandons de paquets.
- Meilleures pratiques :
  - Vérifiez la connexion du client et assurez-vous qu'elle est stable et qu'aucune déconnexion n'a lieu.
  - Assurez-vous que la valeur RSSI sur l'AP de destination est supérieure ou égale à -67

Références

Recommandations QoS sans fil

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

Guide de déploiement de la visibilité et du contrôle des applications pour les contrôleurs sans fil Cisco Catalyst 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.