& QoS via Wireless 9800 WLC begrijpen voor probleemoplossing (snelle referentie)

Inhoud

Inleiding

Dit document beschrijft QoS op 9800 draadloze LAN-controllers

Voorwaarden

Vereisten

Dit document behandelt hoe u aan het verkeer zowel stroomopwaarts als stroomafwaarts prioriteiten kunt toewijzen en labelen. Het legt de best practice-configuratie voor spraakverkeer op

draadloze LAN-controller (WLC) en technieken voor probleemoplossing uit voor een veel voorkomende spraakgerelateerde problemen.

Gebruikte componenten

9800 WLC op basis van 17.12 Cisco IOS® XE release.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een korte beschrijving van de IEEE 802.11e-standaard en Wi-Fi Multimedia (WMM)

WMM is een Wi-Fi Alliance die is gebaseerd op de IEEE 802.11e-standaard. WMM biedt Quality of Service (QoS)-functies door prioriteit te geven aan het verkeer volgens vier toegangscategorieën: spraak, video, beste prestaties en achtergrond, op basis van de methode Enhanced Distributed Channel Access (EDCA).

WMM inschakelen is essentieel voor het bereiken van optimale prestaties in Wi-Fi-netwerken, met name in omgevingen waar toepassingen met hoge bandbreedte en lage latentie gangbaar zijn. Zo is in 802.11n-netwerken WMM vereist om volledig gebruik te kunnen maken van de mogelijkheden van deze snelle Wi-Fi-standaard.

WMM-wachtrijen en uitgebreide gedistribueerde kanaaltoegang (EDCA)

Over het algemeen moet elk station luisteren naar het medium om te controleren of het niet actief is voordat de frames worden verzonden. Zodra het kader wordt verzonden, luistert het station naar het medium om te zien of er een botsing is opgetreden.

Draadloze clients kunnen de botsingen niet detecteren. Hiervoor wordt CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) gebruikt. Het maakt gebruik van een vaste en willekeurige timer (CWmin, CWmax) en elk frame dat wordt verzonden moet worden bevestigd zodat we weten dat er geen botsing is en alle klanten hun verkeer kunnen verzenden.

Zoals we eerder al vermeldden, hebben we vier toegangscategorieën (wachtrijen), elk van de wachtrijen gebruikt verschillende timers. Frames met de hogere prioriteit worden statistisch eerder verstuurd en de lagere prioriteitsframes hebben backoff parameters waardoor ze statistisch achteraf worden verstuurd.

Samengevat, het bestaan van de vier wachtrijen alleen garandeert Quality of Service (QoS) niet; wat echt van belang is, is hoe het verkeer binnen elke wachtrij effectief wordt beheerd.

QoS-implementatie

Standaard wordt zonder QoS-configuratie (Quality of Service) het netwerkverkeer gelijk behandeld, met een model voor levering van de beste inspanningen. Dit betekent dat al het verkeer, ongeacht het type of het belang ervan, dezelfde prioriteit en kans heeft om op elk moment geleverd te worden. Wanneer QoS-functies echter zijn ingeschakeld en correct zijn geconfigureerd, kan prioriteit worden toegewezen aan specifieke typen netwerkverkeer, zoals spraak en video.

Het configureren van QoS omvat twee hoofdcomponenten: classificatie en markering.

Classificatie:

De classificatie omvat het identificeren en categoriseren van netwerkverkeer op basis van specifieke criteria, zoals het type toepassing, het bron/bestemming IP-adres, het protocol of het poortnummer. Het verkeer is verdeeld in klassen of wachtrijen:

1. Spraak: AC_VO
2. Video: AC_VI
3. Best-inspanning: AC_BE
4. Achtergrond: AC_BK

Markering:

Zodra het verkeer in wachtrijen wordt geclassificeerd, moet u QoS-markeringen of -tags aan pakketten toewijzen om hun prioriteitsniveau aan te geven.

Er zijn verschillende manieren om het verkeer te markeren. De belangrijkste twee standaarden zijn Layer 2 802.1p CoS (serviceklasse) en Layer 3 DSCP (Differentiated Services Code Point).

Layer 2 "802.1p" CoS (serviceklasse)

In de 802.1p-standaard zijn er zeven niveaus van CoS, elk vertegenwoordigd door een 3-bits veld dat waarden kan aannemen van 0 tot 7. Deze waarden geven de prioriteit van het verkeer aan, waarbij 0 de laagste prioriteit is en 7 de hoogste prioriteit.

Opmerking: 802.1p is een subset van de 802.1q-standaard en wordt alleen weergegeven als er een VLAN-tag is, zoals op trunkpoorten.

Tabel 1: 802.1P- en WMM-classificatie

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

Layer 3 DSCP (gedifferentieerde servicescodepunt)

DSCP is een Layer 3-tag op de IP-header en gebruikt 6-bits voor 64 verschillende waarden (0 tot 63).

Tabel 2: DSCP- en WMM-classificatie

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

De overheersende DSCP-waarden zijn 46 (EF) voor spraak, 34 (AF41) voor video en 0 (BE) voor de beste inspanning.

Standaard DSCP-naar-UP toewijzing

Zoals we eerder hebben besproken, is een 3-bits veld in het Ethernet-frame, terwijl DSCP 6-bits is in de IP-header.

Hoe kunt u Layer 2 User Priority (UP)-waarde berekenen vanuit Layer 3 Differentiated Services Code Point (DSCP)?

Op dit moment is er geen specifieke standaard voor deze afbeelding, maar er wordt een algemene

methode gebruikt die bekend staat als 'Default DSCP-to-UP Mapping'.

DSCP-to-UP methode leidt de UP waarden af van het 3 msb van het DSCP pakket en brengt het dan in kaart op de juiste categorie van de Toegang.

Deze methode wordt gebruikt door Microsoft Windows-machines om een bekend probleem op te lossen dat in meer details wordt behandeld in Voorbeeld #2: Een bekend Microsoft Windows-clientprobleem in DSCP-to-UP-toewijzing

Tabel 3: Standaard DSCP-naar-UP-toewijzing

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	

Packet Flow en QoS Trust

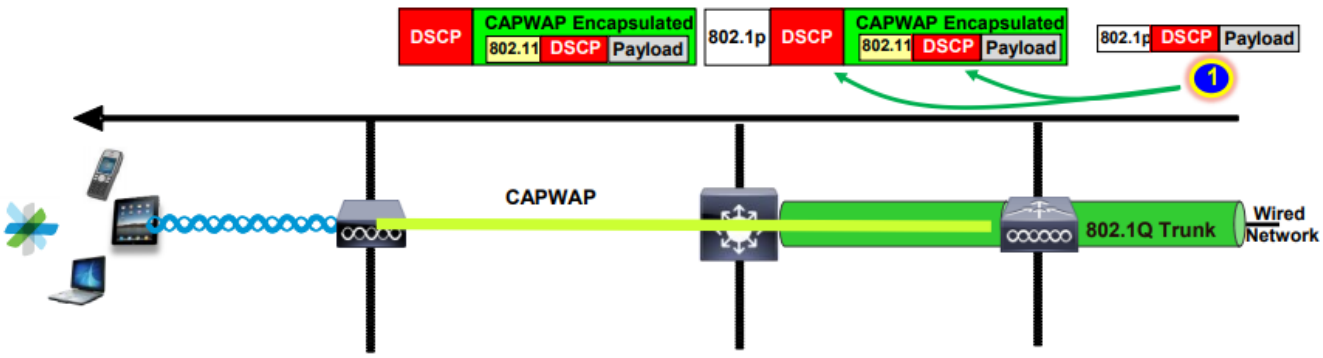
Deze sectie behandelt pakketstroom en vertrouwen QoS in deze verschillende scenario's:

1. Central Switching - Downstream Trust.
2. Central Switching - Upstream Trust.
3. FlexConnect lokaal switchingvertrouwen.

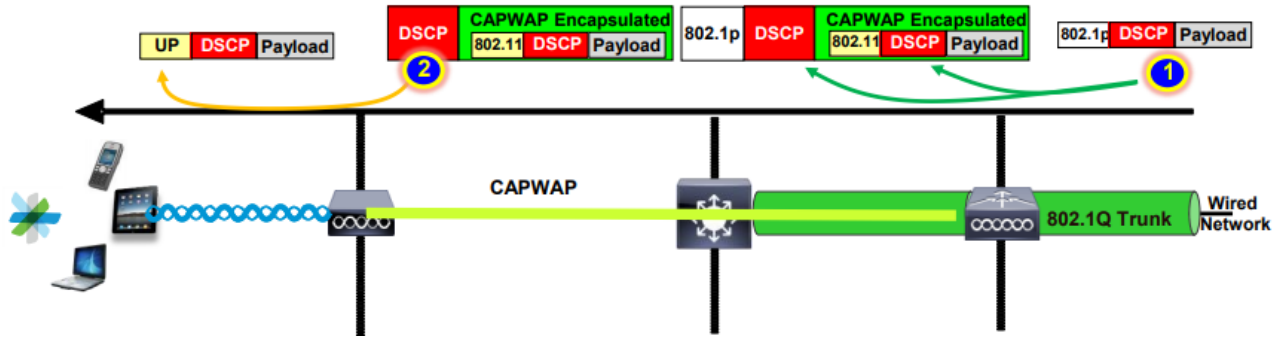
Central Switching - Downstream Trust

- Downstream - verkeer van bekabeld naar draadloos.
- Het stroomafwaartse verkeer is CAPWAP ingekapseld.

1- Een Ethernet-frame wordt ontvangen op de WLC 802.1q trunkpoort. De WLC gebruikt de binnenwaarde DSCP verzonden van het bekabelde netwerk en brengt het in kaart aan de buitenste DSCP in de CAPWAP-header, het caps de buitenste DSCP aan een maximumwaarde volgens het profiel QoS dat op WLC wordt gevormd.



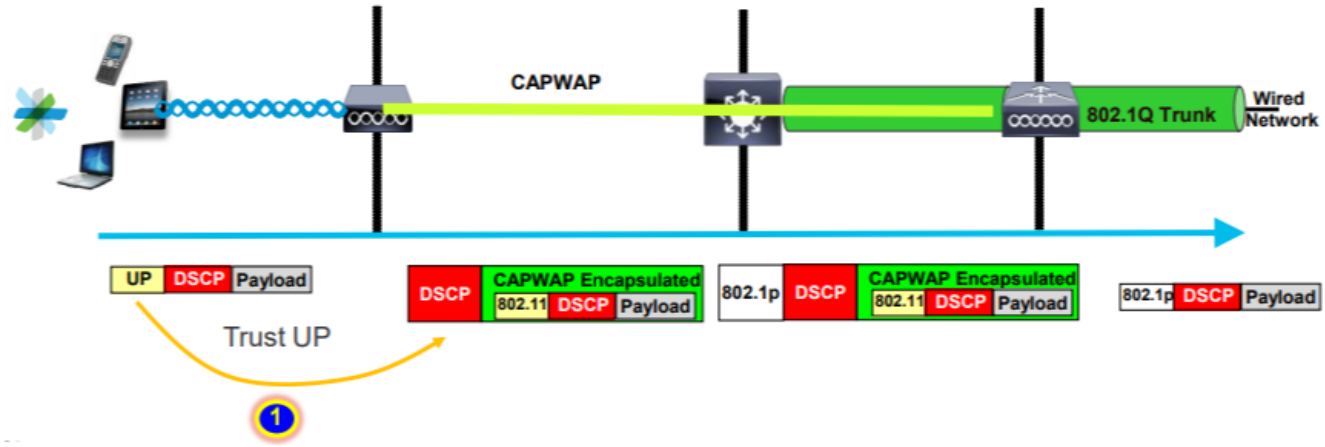
2- Zodra dit Ethernet-frame is ontvangen door het toegangspunt, brengt het toegangspunt de externe DSCP-waarde in kaart naar de UP-waarde en stuurt het naar de draadloze client met de juiste AC.



Central Switching - Upstream Trust

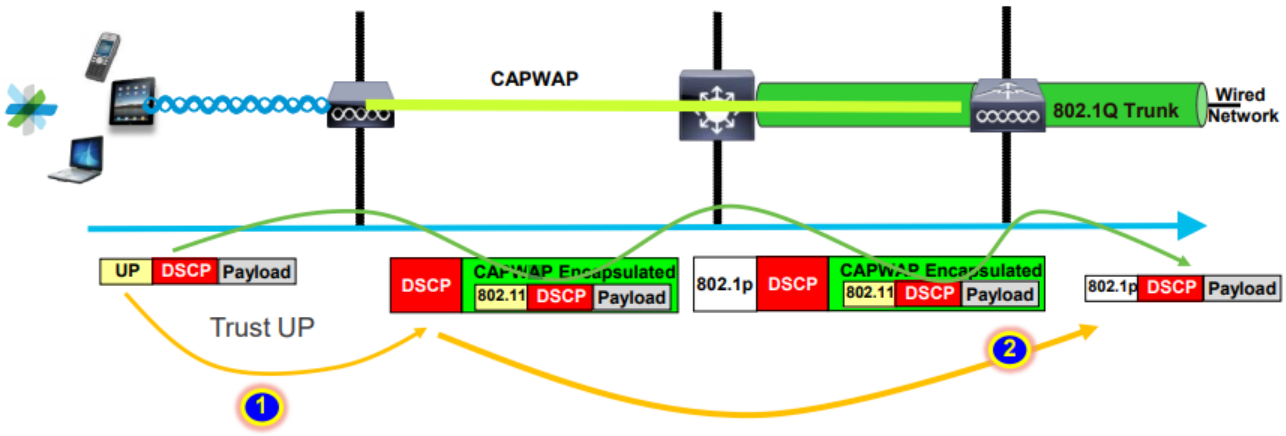
- Upstream verkeer van draadloos naar bekabeld.

1. De draadloze client verzendt het 802.11e (WMM) frame en dit wordt ontvangen door het toegangspunt.



2- AP kapselt het originele pakket in een kopbal CAPWAP in en brengt tot een buitenwaarde DSCP in kaart zolang het profiel QoS dat op WLC wordt gevormd dat niveau QoS toestaat. Het

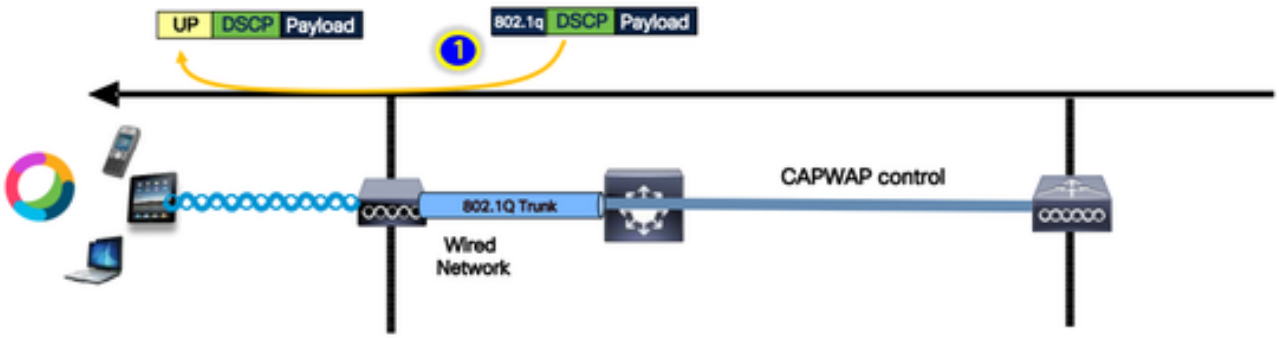
pakket wordt naar het bekabelde netwerk verzonden met de oorspronkelijke DSCP-waarde.



Flexconnect: lokaal switching

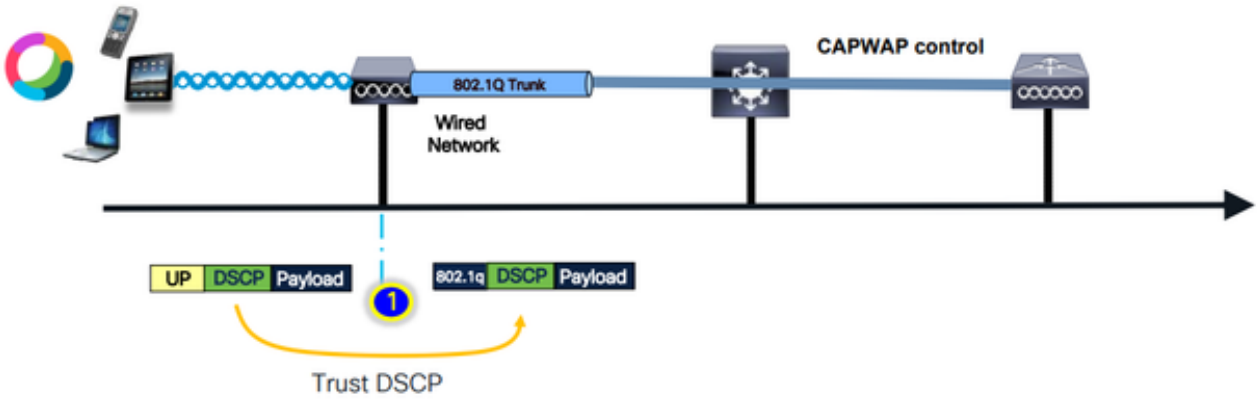
- Flexconnect lokaal switching - Downstream trust

Voor lokaal switched VLAN's neemt FlexConnect AP de DSCP-waarde van het IP-pakket, verwerkt elk QoS-beleid (bijvoorbeeld AVC-beleid), brengt het in kaart met de 802.11e UP-waarde op het draadloze frame en vormt het frame een wachtrij. Het stuurt het dan naar de klant.



- Flexconnect lokaal switching - Upstream trust

De client verzendt het frame en het wordt ontvangen door de AP. AP bekijkt de originele pakket DSCP waarde om om het even welk QoS beleid toe te passen alvorens het pakket naar bedraad te verzenden.



Gemeenschappelijke problemen voor upstream verkeer

Het verkeer in Upstream-scenario - tussen de draadloze client en het toegangspunt - is niet meer onder controle, wat betekent dat u geen controle hebt over de QoS die door de client via de ether wordt verzonden.

Voor een werkscenario wordt van de client verwacht dat deze een pakket met de juiste UP- en DSCP-waarden verzendt, zodat het verkeer in de juiste access-categorie valt.

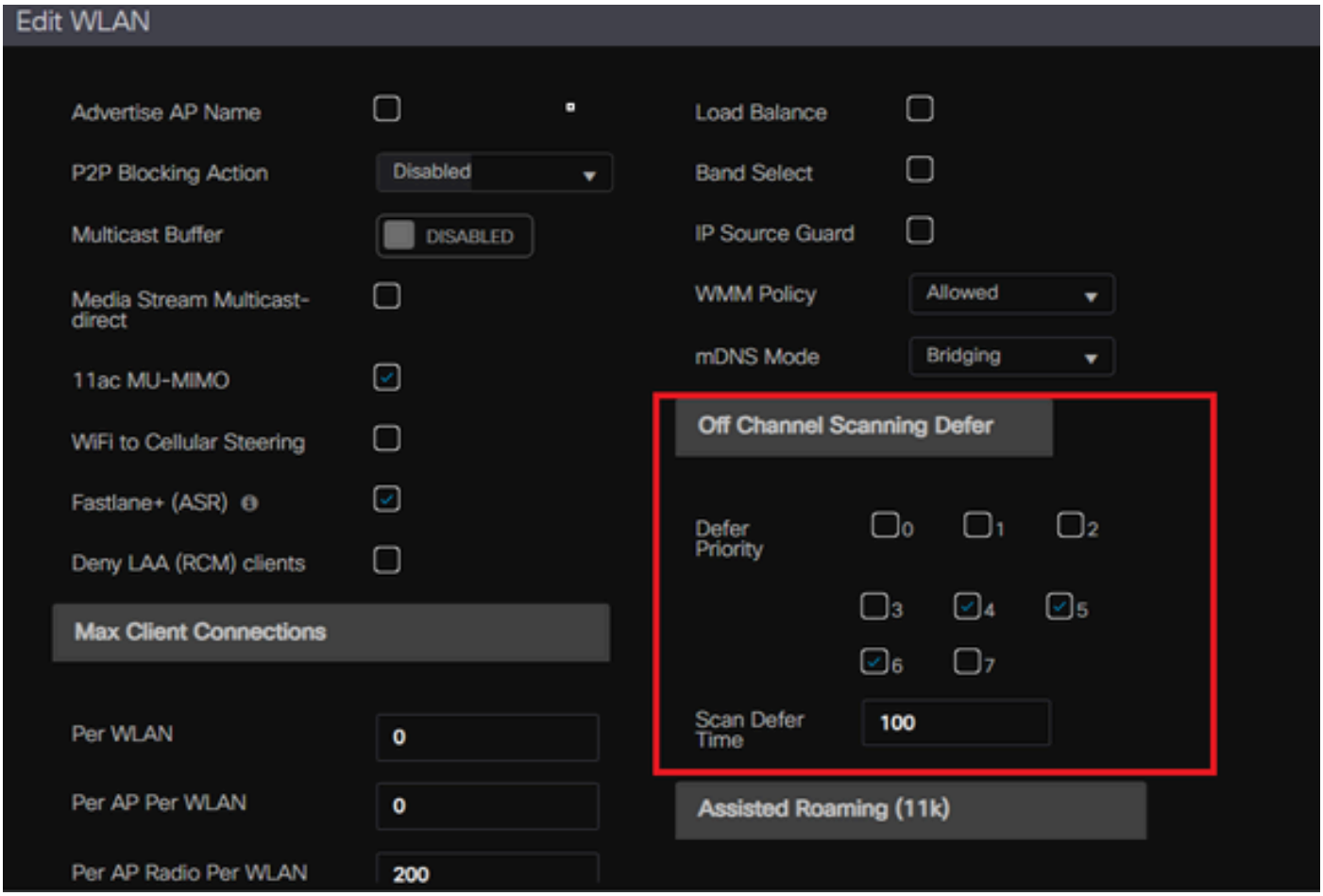
Wat gebeurt er als de client verkeer met een onjuiste UP-waarde verzendt?

Voorbeeld #1: Wanneer de client verkeer verzendt met een UP-waarde van "2"

Opmerking: AP's gaan off-channel om te scannen naar informatie die nodig is voor het RRM algoritme. Dit is zeker van invloed op gevoelig verkeer zoals spraak en video.

De optie Off Channel Scanning Defer is ingesteld in het tabblad WLAN Advanced. Standaard is deze optie ingeschakeld voor UP-klassen 4, 5 en 6, met een tijddrempel van 100 milliseconden, betekent dit dat de AP niet off-channel gaat om te scannen voor een periode van 100 ms na het zien van gevoelig verkeer (spraak of video).

Stel dat de draadloze client spraakapplicatie gebruikt, de verwachte UP-waarde is "6", maar de client heeft het pakket met de verkeerde UP-waarde "2" verzonden. AP gaat dan off-channel scannen en dit beïnvloedt de client prestaties en ervaring.



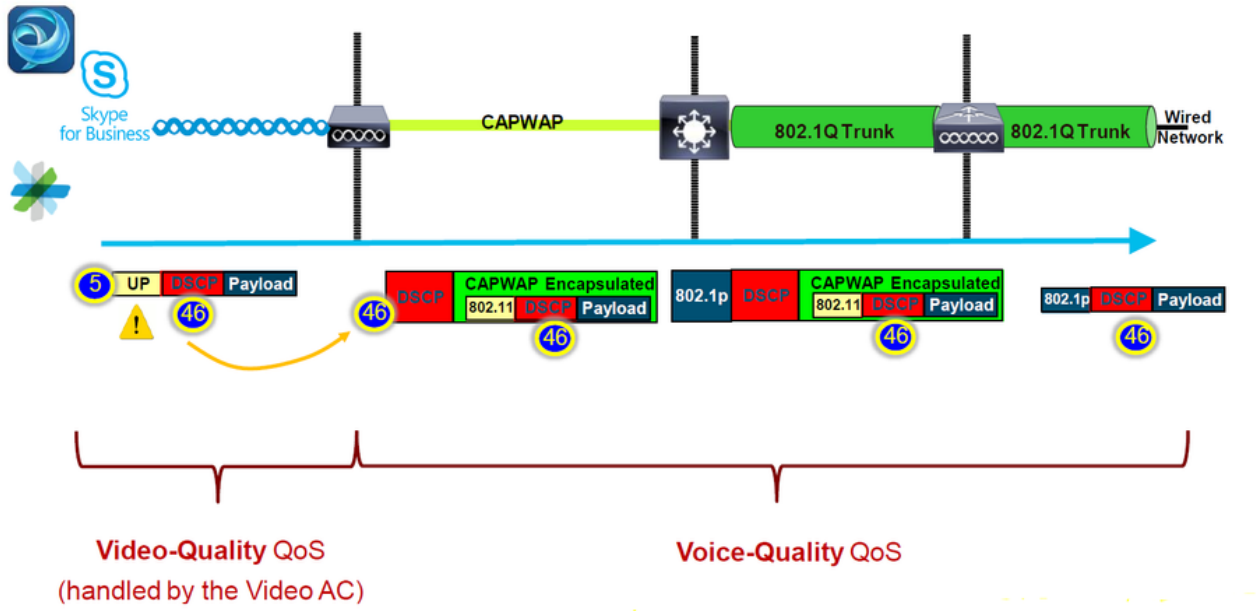
Kunt u Defer Scanning inschakelen voor lage UP-prioriteit?

Het antwoord is ja. Het inschakelen van Defer Scanning voor low UP prioriteitsverkeer voorkomt effectief dat het access point off-channel scans uitvoert en beïnvloedt daardoor de werking van het RRM en schurkendetectiealgoritmen. Om aan deze uitdaging het hoofd te bieden, is een alternatieve benadering nodig om het scannen van kanalen te vergemakkelijken en tegelijkertijd kritisch verkeer prioriteit te geven.

Voorbeeld #2: een bekend Microsoft Windows-clientprobleem in DSCP-to-UP toewijzing

Een veel voorkomend probleem bij MS Windows-machines treedt op wanneer de standaardtoewijzing tussen DHCP- en UP-waarden wordt gebruikt. In deze afbeelding wordt de gebruikersprioriteit (UP) bepaald aan de hand van de drie belangrijkste bits (msb) van de waarde van de gedifferentieerde servicescode (DSCP). Bijvoorbeeld, voor spraakverkeer met een DSCP-waarde van EF (101110), zou het worden toegewezen aan UP 5 (101).

Standaard vertrouwen AP's in Upstream de UP-waarde, waardoor het spraakverkeer wordt behandeld in de Video Access Category (AC_VI) met DSCP-waarde als 34 in plaats van de Voice Access Category (AC_VO) met DSCP-waarde als 46, waarvoor het is bedoeld. Hiervoor hebben de spraakframes langere wachttijden en een grotere kans op herhalingen.

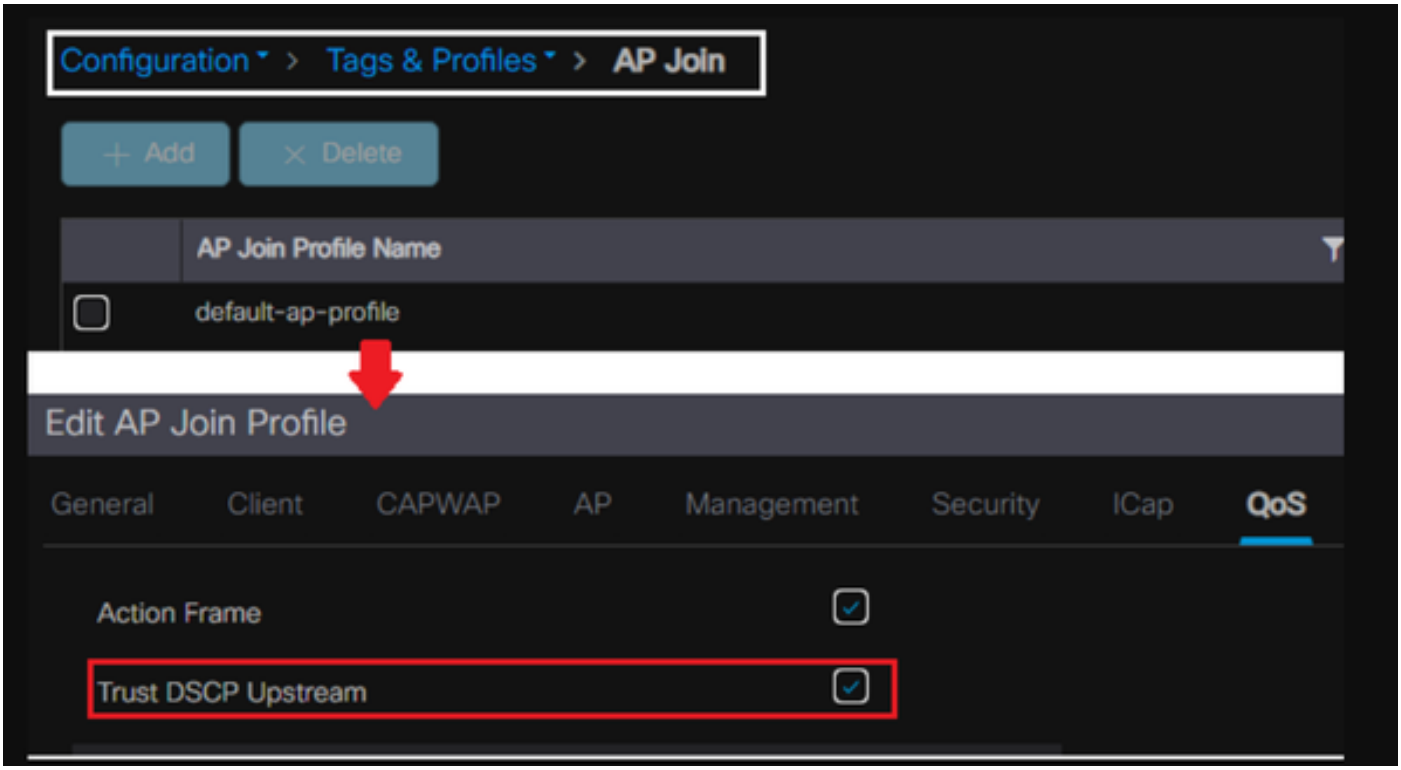


Is er een manier om dit op te lossen?

Het antwoord is ja als MS windows-machine spraakverkeer met de juiste DSCP-waarde verzenden.

Hoe kan dit worden verholpen?

Door de "vertrouwen DSCP Upstream" optie op de WLC te gebruiken. Deze optie dwingt de AP om de innerlijke DSCP in de Upstream te vertrouwen in plaats van de UP.



Raadpleeg voor meer instructies over het configureren van uw Windows-machine om het verkeer

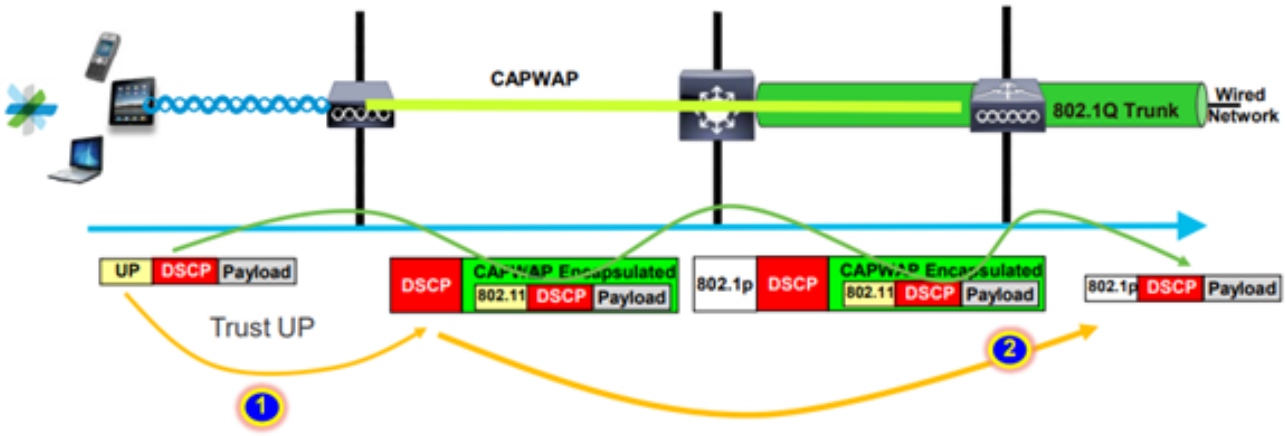
te overschrijven of te labelen ["Hoe kan ik DSCP-tagging op Windows-machines inschakelen"]

Welk protocol te vertrouwen: DSCP of COS?

Welk type vertrouwen te selecteren voor de WLC Switch Port?

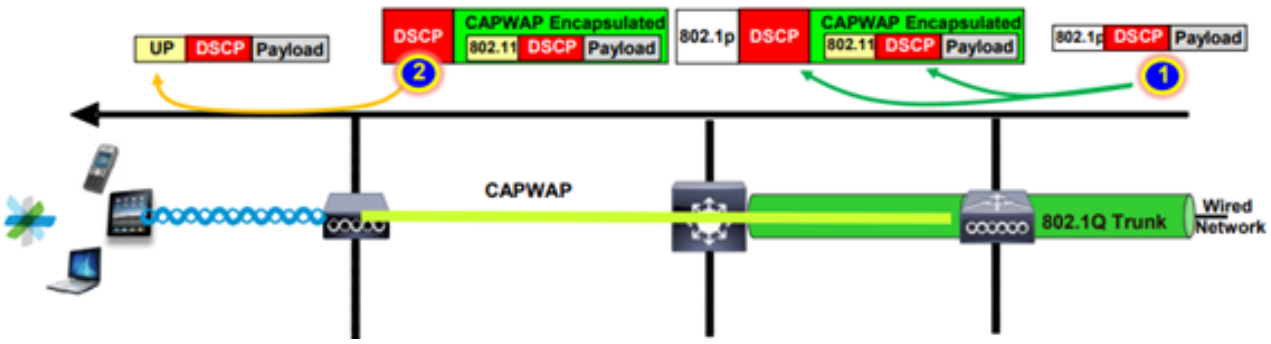
Eigenlijk kunnen we een van de vertrouwensopties kiezen. U moet echter in gedachten houden dat voor het Upstream-scenario als u ervoor kiest om CoS te vertrouwen; de switch herschrijft de buitenwaarde van DSCP op basis van de CoS-DSCP-toewijzingstabel die op de switch is geconfigureerd.

Als u er echter voor kiest om DSCP te vertrouwen, herschrijft de switch de externe DSCP-waarde niet omdat de inkomende innerlijke DSCP wordt vertrouwd.



Voor het stroomafwaartse scenario voegt de switch waar de WLC is aangesloten de 802.1p-waarde toe op basis van de DSCP-CoS-toewijzingstabel die daarop is geconfigureerd. Als u CoS vertrouwt, wordt de buitenwaarde DSCP gewijzigd op basis van de inkomende 802.1p-waarde.

Als u er echter voor kiest om DSCP te vertrouwen, herschrijft de Switch de externe DSCP-waarde niet.



Als voorbeeld op het bovenstaande; Draadloze client verbonden met een SSID toegewezen aan

de beheerinterface op het native VLAN.

Wat gebeurt er als u ervoor kiest om CoS te vertrouwen op de WLC Switch poort?

Clientverkeer bereikt de trunkpoort, het is niet gelabeld aan 802.1q omdat het een native untagged VLAN is.

Wat kun je doen om dit op te lossen?

U kunt de DSCP-vertrouwensoptie gebruiken in plaats van CoS, wat over het algemeen de aanbeveling is.

Beste praktijken voor draadloze LAN-controllers in QoS

Metaal QoS-profielen

We kunnen vier hoofdprofielen QoS configureren op de WLC (Platinum, Gold, Silver, Bronze).

- Platinum/Voice - garandeert een hoge servicekwaliteit voor spraak over draadloos
- Gold/video - ondersteunt hoogwaardige videotoepassingen
- Silver/best-inspanning - ondersteunt normale bandbreedte voor clients; dit is de standaardinstelling
- Bronze/background - biedt de laagste bandbreedte voor gastservices.

Het belangrijkste doel van dit QoS-profiel is om de maximale buitenste DSCP-waarde op de CAPWAP-header voor zowel upstream als downstream te beperken zonder de innerlijke DSCP te beïnvloeden.

Opmerking: de interne DSCP-waarde wordt gewijzigd door AVC.

Voor lokaal geschakeld verkeer wordt het QoS-profiel toegepast op downstream verkeer op basis van de UP-waarde. Als deze waarde hoger is dan de standaard WLAN-waarde, wordt de standaard WLAN-waarde gebruikt.

Voor upstream verkeer als de client een UP-waarde verzendt die hoger is dan de standaard WLAN-waarde; de standaard WLAN-waarde wordt gebruikt.

Voor meer informatie over de 9800 WLC best practice-configuratiehandleiding draadloze QoS voor Catalyst 9800 draadloze controller

Stappen voor probleemoplossing:

1. Begrijp het probleem.
2. Maak een solide actieplan.
    - Stel vragen over probleemoplossing en een netwerktopologiediagram.

- Logboeken verzamelen en debuggen.
- Vraag om IP-warmtekaarten.

3. Controleer WLC-configuraties.

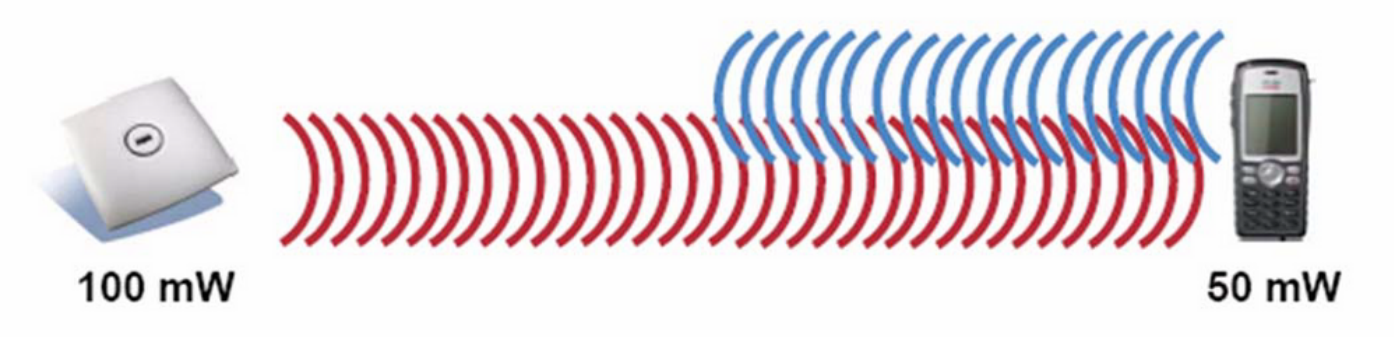
4. De debugs analyseren

5. Gebruik de VoWLAN-checklist om te bevestigen of de best practices werden gevolgd.

Het begrip van unidirectionele audio

Dit probleem doet zich vooral voor wanneer we asymmetrische macht hebben tussen de klant en de AP.

APs kan met maximummacht overbrengen, nochtans kunnen de draadloze apparaten zoals de telefoons van Cisco met minder macht overbrengen veroorzakend de telefoons van Cisco downstream de kaders van AP horen, maar AP hoort niet de kaders in Upstream van telefoons.



Aanbevolen wordt om de AP TX-voeding niet hoger te configureren dan de maximale ondersteunde TX-voeding op het draadloze apparaat.

- Actieplan
  - Controleer de clientverbinding en controleer of deze stabiel is en geen verbindingen verbreekt.
  - Controleer de RF-omgeving (AP-vermogen, signaalsterkte ... etc.).
  - Verzamel OTA opnamen om audioverkeer te controleren; het enige richtingsverkeer wordt gezien.

- Best practices:
  - DTPC inschakelen: het helpt CCX Clients om hun TX-vermogen aan te passen aan de AP-voeding.
  - Controleer de volume-instellingen op het clientapparaat.

De betekenis van Choppy en Robotic Audio

Zowel "Choppy" als "Robotic" audio gebeurt wanneer we veel pakketverlies hebben of het pakket wordt vertraagd.

Choppy voice beschrijft gaten en vertragingen in het geluid. Dit zijn voorbeelden van een choppy

en robotplaten.

- Actieplan
  - Controleer de verbinding met de client en zorg ervoor dat deze stabiel is en niet wordt losgekoppeld.
  - Controleer de RF-omgeving (gebruik van hoge kanalen, ruis en interferentie-apparaten ... enz.).
  - Verzamel Opnamen door de weg om pakketdalingen te controleren.
- Best practices:
  - Controleer QoS-configuraties op WLC.
  - Zorg ervoor dat QoS aan de bekabelde kant is geconfigureerd.

Gaten en geen geluid bij roaming begrijpen

Soms melden gebruikers lacunes en verlies van audioverbinding wanneer ze van de ene locatie naar de andere zwerven.

- Actieplan
  - Controleer RF-omgeving en bevestig dat u een goede dekkingcel tussen AP's hebt.
  - IP warmte MAP.
  - Verzamel Opnamen door de weg om pakketdalingen te controleren.
- Best practices:
  - Controleer de clientverbinding en controleer of deze stabiel is en geen verbindingen verbreekt.
  - Zorg ervoor dat de RSSI-waarde op de bestemmingspap groter of gelijk is aan -67

Referenties

Draadloze QoS-aanbevelingen

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

Application Visibility and Control implementatiegids voor Cisco Catalyst 9800 Series draadloze controllers

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.