QoS über Wireless 9800 WLC verstehen und Fehler beheben (Kurzreferenz)

Inhalt

Einleitung

In diesem Dokument wird die QoS auf Wireless LAN-Controllern der Serie 9800 beschrieben.

Voraussetzungen

Anforderungen

In diesem Dokument wird erläutert, wie der Datenverkehr im Upstream- und Downstream-Bereich

priorisiert und gekennzeichnet wird. Es erläutert die Best Practice-Konfiguration für Sprachdatenverkehr auf dem Wireless LAN Controller (WLC) und Verfahren zur Fehlerbehebung bei typischen Problemen im Zusammenhang mit Sprachdaten.

Verwendete Komponenten

9800 WLC, basierend auf Version 17.12 von Cisco IOS® XE

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Eine kurze Beschreibung des IEEE 802.11e-Standards und von Wi-Fi Multimedia (WMM)

WMM ist eine Wi-Fi Alliance, die auf dem IEEE 802.11e-Standard basiert. WMM bietet Quality of Service (QoS)-Funktionen, indem der Datenverkehr anhand von vier Zugriffskategorien priorisiert wird: Sprache, Video, bestmöglicher Datenverkehr und Hintergrund, basierend auf der Enhanced Distributed Channel Access (EDCA)-Methode.

Die Aktivierung von WMM ist eine wesentliche Voraussetzung für optimale Leistung in Wi-Fi-Netzwerken, insbesondere in Umgebungen, in denen Anwendungen mit hoher Bandbreite und niedriger Latenz vorherrschen. In 802.11n-Netzwerken ist WMM beispielsweise erforderlich, um die Funktionen dieses Hochgeschwindigkeits-Wi-Fi-Standards vollständig nutzen zu können.

WMM-Warteschlangen und Enhanced Distributed Channel Access (EDCA)

Im Allgemeinen muss jede Station auf das Medium hören, um zu überprüfen, ob es inaktiv ist, bevor die Frames gesendet werden. Sobald der Frame gesendet wurde, hört die Station das Medium ab, um zu sehen, ob eine Kollision aufgetreten ist.

Wireless-Clients können die Kollisionen nicht erkennen. Hierfür wird CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) verwendet. Es verwendet einen festen und zufälligen Timer (CWmin, CWmax) und jeder gesendete Frame muss bestätigt werden, damit wir wissen, dass es keine Kollision gibt und alle Clients ihren Datenverkehr senden können.

Wie bereits erwähnt, gibt es vier Zugriffskategorien (Warteschlangen), für die jede Warteschlange unterschiedliche Timer verwendet. Frames mit der höheren Priorität werden statistisch früher gesendet, und Frames mit der niedrigeren Priorität verfügen über Backoff-Parameter, sodass sie statistisch gesehen später gesendet werden können.

Zusammenfassend lässt sich sagen, dass das Vorhandensein der vier Warteschlangen allein keine Garantie für Quality of Service (QoS) bietet. Entscheidend ist jedoch, wie der Datenverkehr innerhalb der einzelnen Warteschlangen effektiv verwaltet wird.

QoS-Implementierung

Ohne QoS-Konfiguration wird der Netzwerkverkehr standardmäßig gleich behandelt, mit einem bestmöglichen Bereitstellungsmodell. Das bedeutet, dass der gesamte Datenverkehr, unabhängig von Art oder Bedeutung, die gleiche Priorität und die gleiche Chance hat, zu einem bestimmten Zeitpunkt geliefert zu werden. Wenn jedoch QoS-Funktionen aktiviert und ordnungsgemäß konfiguriert sind, kann bestimmten Arten von Netzwerkverkehr wie Sprache und Video Priorität zugewiesen werden.

Die Konfiguration von QoS umfasst zwei Hauptkomponenten: Klassifizierung und Markierung.

Klassifizierung:

Die Klassifizierung umfasst die Identifizierung und Kategorisierung des Netzwerkverkehrs anhand bestimmter Kriterien, z. B. Art der Anwendung, Quell-/Ziel-IP-Adresse, Protokoll oder Portnummer. Der Datenverkehr wird in Klassen oder Warteschlangen unterteilt:

1. Sprache: AC_VO
2. Video: AC_VI
3. Best-Effort: AC_BE
4. Hintergrund: AC_BK

Markierung:

Sobald der Datenverkehr in Warteschlangen klassifiziert ist, umfasst die Markierung die Zuweisung von QoS-Markierungen oder -Tags für Pakete, um deren Prioritätsstufe anzugeben.

Es gibt mehrere Möglichkeiten, den Datenverkehr zu markieren. Die beiden wichtigsten Standards sind Layer 2 802.1p CoS (Class of Service) und Layer 3 DSCP (Differentiated Services Code Point).

Layer 2 "802.1p" CoS (Class of Service)

Beim 802.1p-Standard gibt es sieben CoS-Ebenen, die jeweils durch ein 3-Bit-Feld dargestellt werden und Werte zwischen 0 und 7 annehmen können. Diese Werte geben die Priorität des Datenverkehrs an, wobei 0 die niedrigste Priorität und 7 die höchste Priorität darstellt.

Hinweis: 802.1p ist eine Teilmenge des 802.1q-Standards. Sie wird nur angezeigt, wenn ein VLAN-Tag vorhanden ist, z. B. an Trunk-Ports.

Tabelle 1: 802.1P- und WMM-Klassifizierung

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 (Differentiated Services Code Point)

DSCP ist ein Layer-3-Tag auf dem IP-Header. Es verwendet 6 Bit und ermöglicht 64 verschiedene Werte (0 bis 63).

Tabelle 2: DSCP- und WMM-Klassifizierung

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

Die vorherrschenden DSCP-Werte umfassen 46 (EF) für Sprache, 34 (AF41) für Video und 0 (BE) für "Best Effort".

Standard-Zuordnung von DSCP zu UP

Wie bereits erwähnt, ist UP ein 3-Bit-Feld innerhalb des Ethernet-Frames, während DSCP 6 Bit im IP-Header umfasst.

Wie können Sie den Layer 2 User Priority (UP)-Wert aus dem Layer 3 Differentiated Services Code Point (DSCP)-Wert berechnen?

Derzeit gibt es keinen spezifischen Standard für diese Zuordnung. Es wird jedoch eine

gemeinsame Methode verwendet, die als "Standard-DSCP-to-UP-Zuordnung" bezeichnet wird.

Die DSCP-UP-Zuordnungsmethode leitet die UP-Werte aus den 3 MB des DSCP-Pakets ab und ordnet sie dann der richtigen Zugriffskategorie zu.

Diese Methode wird von Microsoft Windows-Computern verwendet, die zu einem bekannten Problem führen, das im Beispiel #2 ausführlicher behandelt wird: Ein bekanntes Microsoft Windows-Client-Problem bei der Zuordnung von DSCP zu UP

Tabelle 3: Standard-Zuordnung von DSCP zu UP

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	

Paketfluss und QoS-Vertrauen

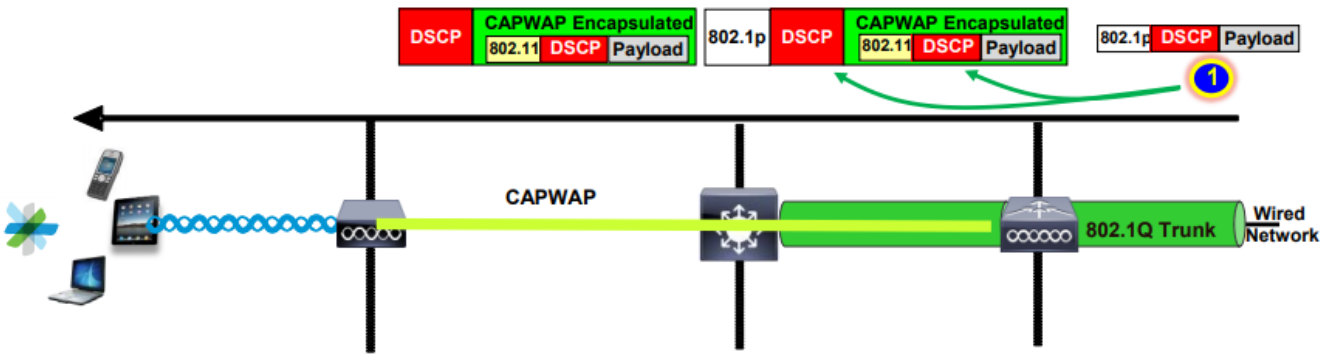
In diesem Abschnitt werden der Paketfluss und die QoS-Vertrauenswürdigkeit in den folgenden Szenarien beschrieben:

1. Central Switching - Downstream-Vertrauen.
2. Central Switching - Upstream-Vertrauenswürdigkeit.
3. FlexConnect Local Switching Trust.

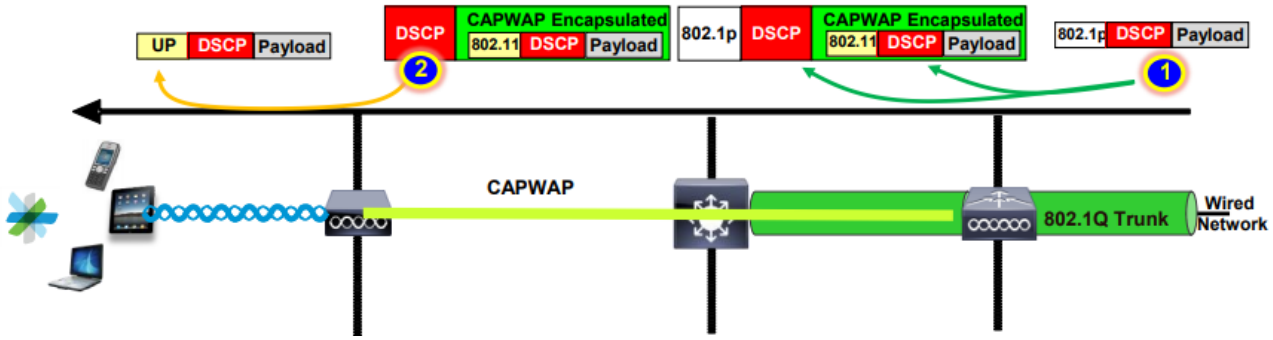
Central Switching - Downstream-Vertrauen

- Downstream - Datenverkehr von kabelgebunden zu Wireless
- Der Downstream-Datenverkehr ist CAPWAP-gekapselt.

1- Ein Ethernet-Frame wird am WLC 802.1q-Trunk-Port empfangen. Der WLC verwendet den inneren DSCP-Wert, der vom kabelgebundenen Netzwerk gesendet wird, und ordnet ihn dem äußeren DSCP im CAPWAP-Header zu. Der äußere DSCP-Wert wird gemäß dem auf dem WLC konfigurierten QoS-Profil auf einen Maximalwert begrenzt.



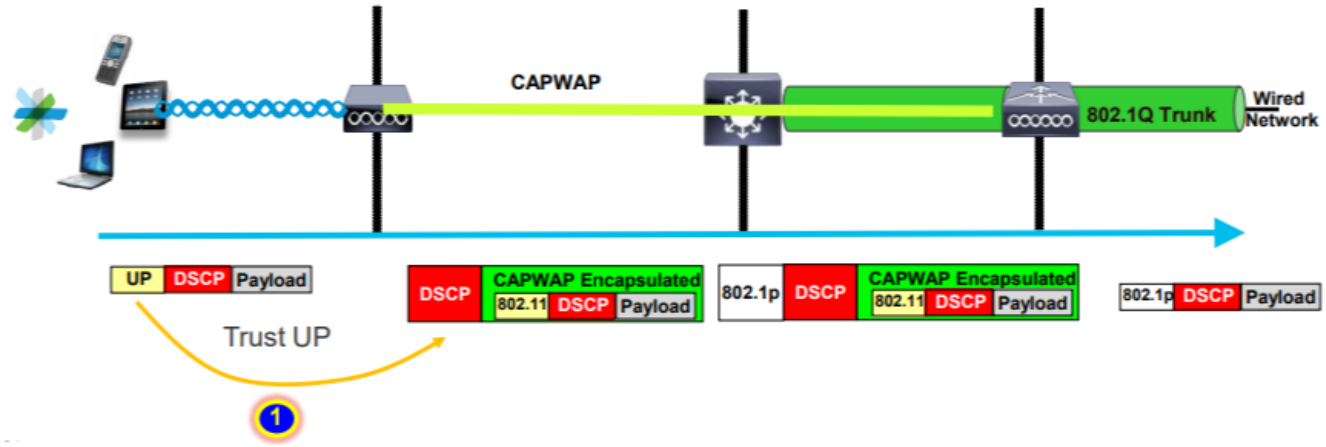
2- Sobald dieser Ethernet-Frame vom WAP empfangen wurde, ordnet der WAP den äußeren DSCP-Wert dem Wert "UP" zu und sendet ihn mit dem richtigen Wechselstrom an den Wireless-Client.



Zentrales Switching - Upstream-Vertrauen

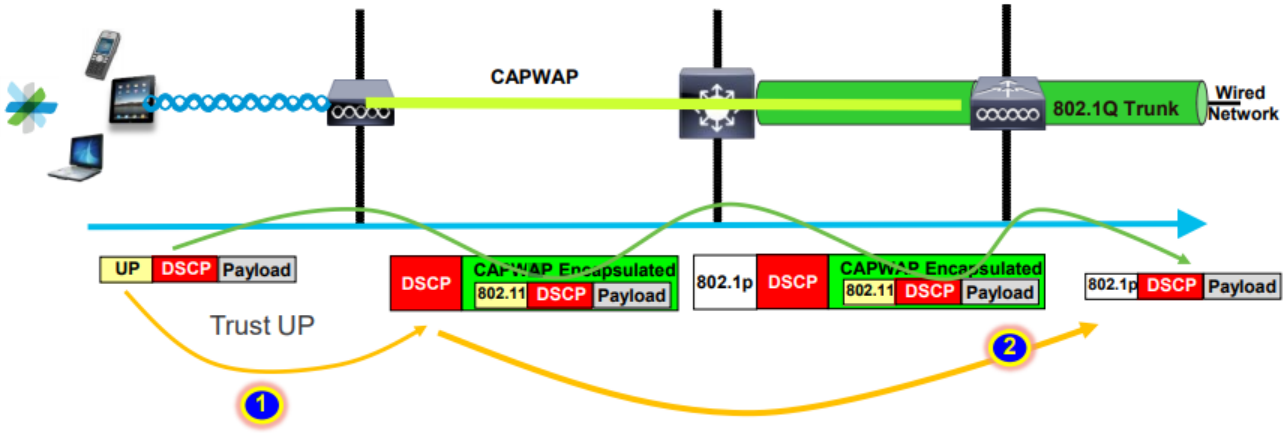
- Upstream - Datenverkehr von Wireless zu kabelgebunden

1. Der Wireless-Client sendet den 802.11e-Frame (WMM), und dieser wird vom Access Point empfangen.



2- Der WAP kapselt das ursprüngliche Paket in einen CAPWAP-Header und ordnet den UP einem äußeren DSCP-Wert zu, solange das auf dem WLC konfigurierte QoS-Profil diesen QoS-Wert

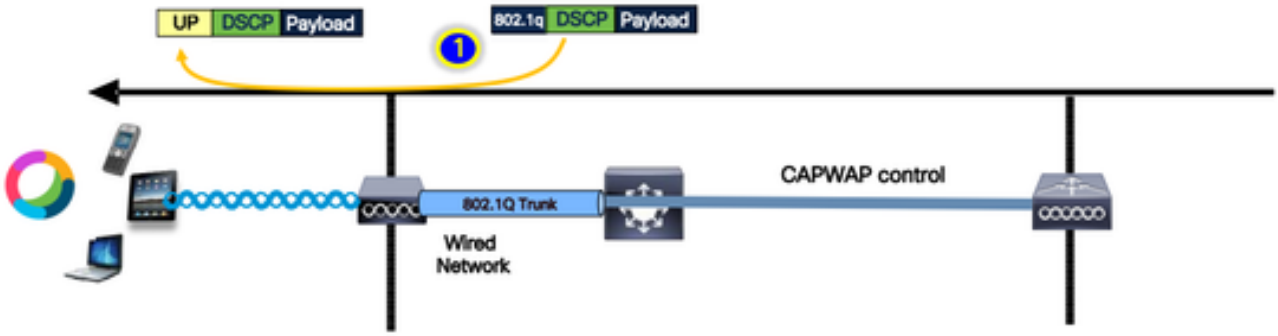
zulässt. Das Paket wird mit dem ursprünglichen DSCP-Wert an das kabelgebundene Netzwerk gesendet.



Flexconnect lokal Switching Trust

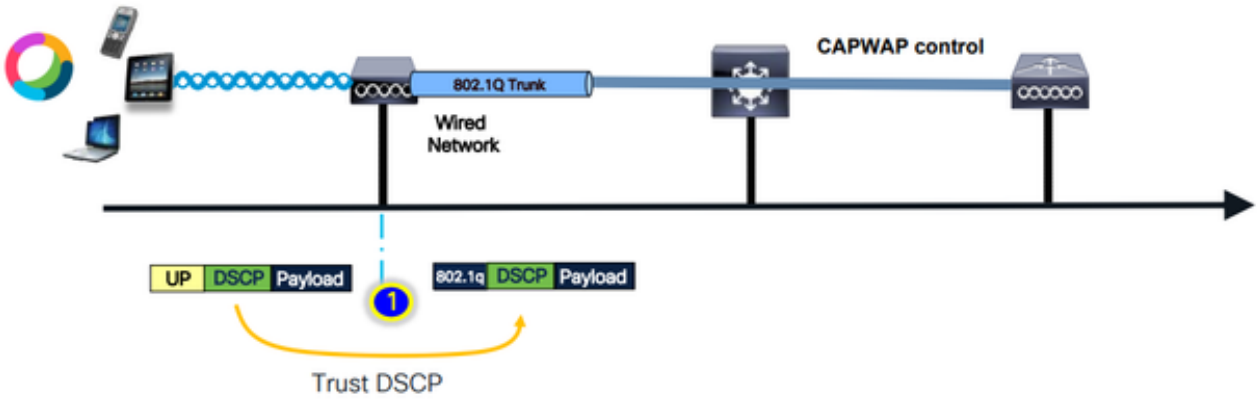
- Flexconnect lokal-Switching - Downstream-Trust

Bei lokal geschalteten VLANs übernimmt der FlexConnect-WAP den DSCP-Wert des IP-Pakets, verarbeitet alle QoS-Richtlinien (z. B. die AVC-Richtlinie), ordnet sie dem 802.11e-UP-Wert auf dem Wireless-Frame zu und reiht den Frame in die Warteschlange ein. Anschließend wird sie an den Client gesendet.



- Flexconnect lokal-Switching - Upstream-Trust

Der Client sendet den Frame und wird vom Access Point empfangen. Der WAP prüft den ursprünglichen DSCP-Paketwert, um eine QoS-Richtlinie anzuwenden, bevor das Paket an das kabelgebundene Netzwerk gesendet wird.



Häufige Probleme beim Upstream-Datenverkehr

Der Datenverkehr im Upstream-Szenario - zwischen dem Wireless-Client und dem Access Point - ist außer Kontrolle, d. h., Sie haben keine Kontrolle über die QoS, die per Funk vom Client gesendet wird.

Für ein funktionierendes Szenario wird vom Client erwartet, dass er ein Paket mit den richtigen UP- und DSCP-Werten sendet, sodass der Datenverkehr der richtigen Zugriffskategorie entspricht.

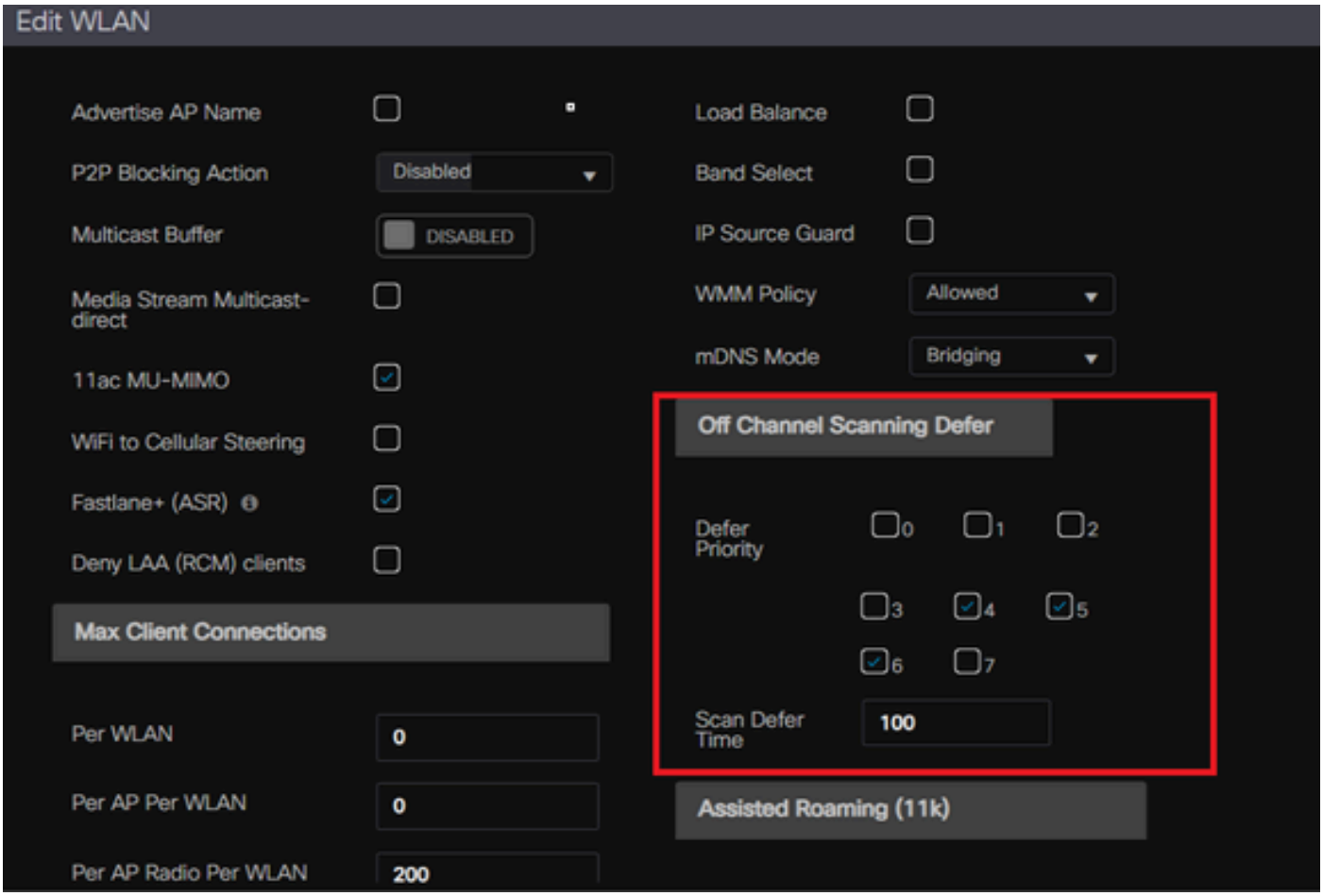
Was passiert, wenn der Client Datenverkehr mit einem falschen UP-Wert überträgt?

Beispiel #1: Wenn der Client Datenverkehr mit dem UP-Wert "2" überträgt

Hinweis: Die APs schalten den Kanal aus, um die für den RRM-Algorithmus erforderlichen Informationen zu sammeln. Dies wirkt sich natürlich auf empfindlichen Datenverkehr wie Sprache und Video aus.

Die Option "Aus-Kanal-Scan zurückstellen" wird auf der Registerkarte "WLAN Advanced" konfiguriert. Standardmäßig ist er für die UP-Klassen 4, 5 und 6 aktiviert. Bei einem Zeitschwellenwert von 100 Millisekunden bedeutet dies, dass der Access Point nach dem Erkennen von sensiblem Datenverkehr (Sprache oder Video) während eines Zeitraums von 100 ms nicht vom Kanal abschaltet, um einen Scan durchzuführen.

Angenommen, der Wireless-Client verwendet eine Sprachanwendung, der erwartete UP-Wert ist "6", aber der Client hat das Paket mit dem falschen UP-Wert "2" gesendet. Der Access Point führt dann einen Off-Channel-Scan durch, was sich auf die Client-Leistung und das Anwendererlebnis auswirkt.



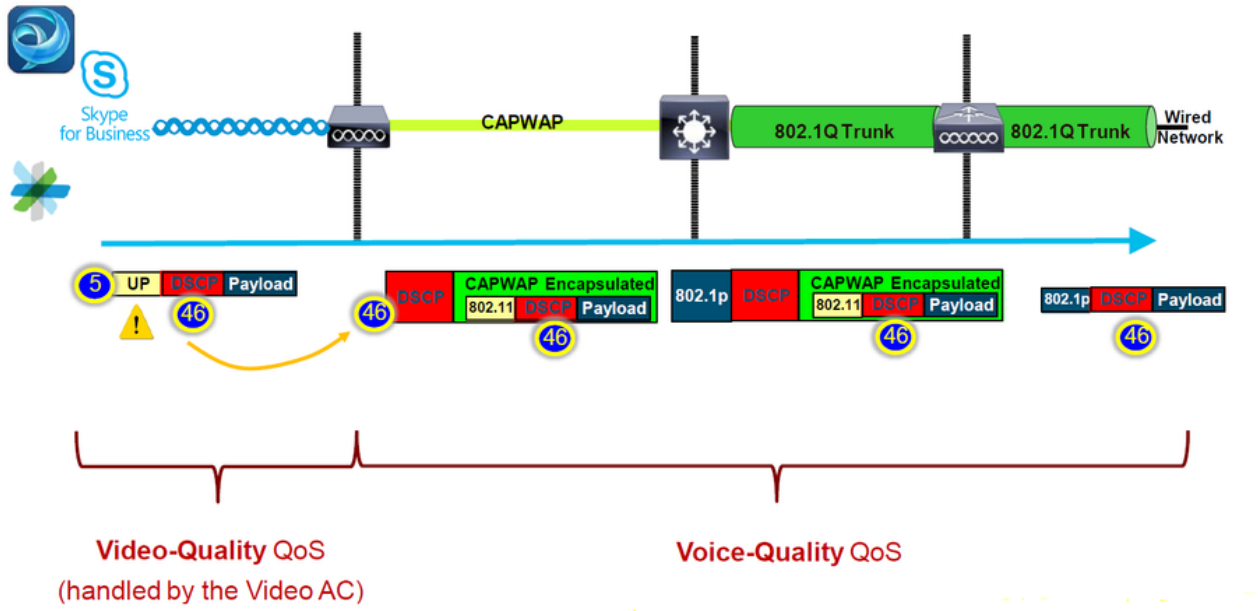
Können Sie das Zurückstellen der Suche für niedrige UP-Priorität aktivieren?

Die Antwort ist ja. Durch die Aktivierung der Funktion zum verzögerten Scannen für Datenverkehr mit niedriger Priorität nach oben wird verhindert, dass der Access Point Off-Channel-Scans durchführt. Dies beeinträchtigt den Betrieb des RRM und die Erkennungsalgorithmen für nicht autorisierte APs. Um dieses Problem zu lösen, ist ein alternativer Ansatz erforderlich, der das Scannen von Kanälen ermöglicht und gleichzeitig den kritischen Datenverkehr priorisiert.

Beispiel #2: Ein bekanntes Problem mit dem Microsoft Windows-Client in der DSCP-UP-Zuordnung

Ein häufig auftretendes Problem, das bei MS Windows-Systemen auftritt, tritt auf, wenn die Standardzuordnung zwischen DHCP- und UP-Werten verwendet wird. In dieser Zuordnung wird die Benutzerpriorität (UP) aus den drei höchstwertigen Bits (msb) des Differentiated Services Code Point (DSCP)-Werts bestimmt. Beispielsweise würde für Sprachdatenverkehr mit einem DSCP-Wert von EF (101110) dieser Wert UP 5 (101) zugeordnet.

Standardmäßig vertrauen APs im Upstream dem UP-Wert. Der Sprachverkehr wird in der Videozugriffskategorie (AC_VI) mit dem DSCP-Wert 34 behandelt, nicht in der Sprachzugriffskategorie (AC_VO) mit dem DSCP-Wert 46, für die er bestimmt ist. Dafür haben die Voice-Frames längere Wartezeiten und eine höhere Wahrscheinlichkeit von Wiederholungsversuchen.

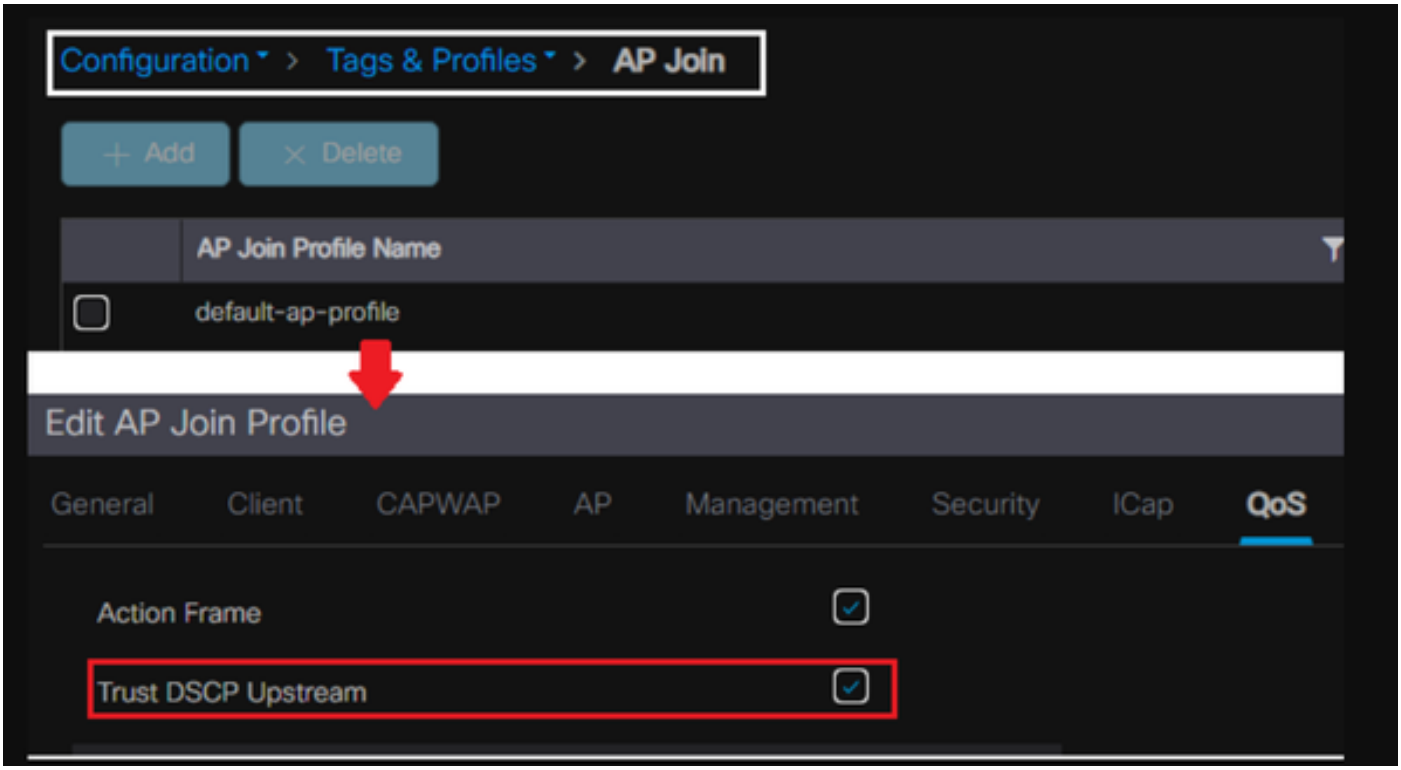


Gibt es eine Möglichkeit, das zu beheben?

Die Antwort ist "Ja", wenn MS Windows-Systeme Sprachdatenverkehr mit dem richtigen DSCP-Wert senden.

Wie kann es behoben werden?

Mit der Option "trust DSCP Upstream" (DSCP Upstream vertrauen) auf dem WLC. Diese Option erzwingt, dass der Access Point dem inneren DSCP im Upstream anstelle des UP vertraut.



Weitere Anweisungen zum Konfigurieren des Windows-Computers zum Überschreiben oder

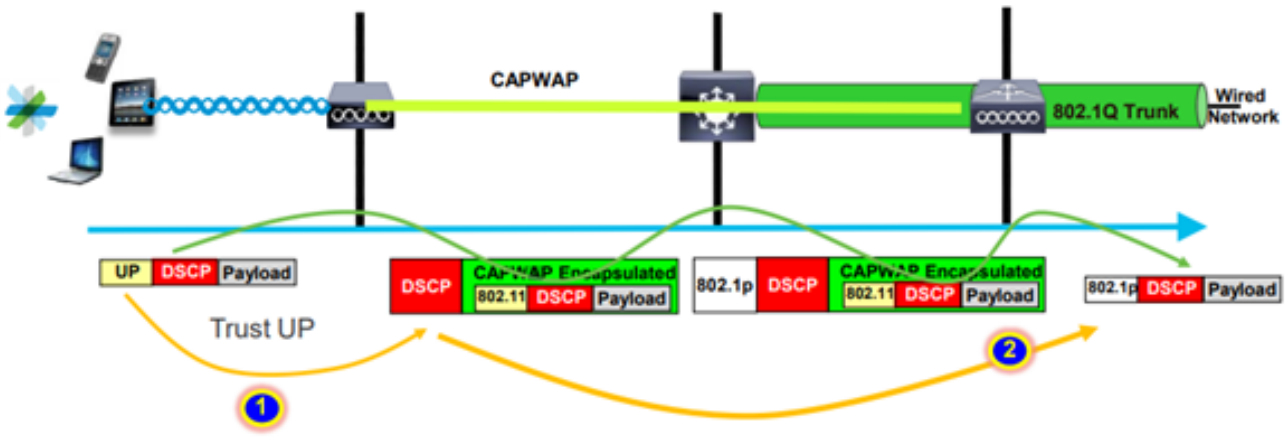
Taggen des Datenverkehrs finden Sie unter "Aktivieren von DSCP-Tagging auf Windows-Computern".

Welches Protokoll soll vertrauenswürdig sein: DSCP oder COS?

Welcher Vertrauenstyp soll für den WLC-Switch-Port ausgewählt werden?

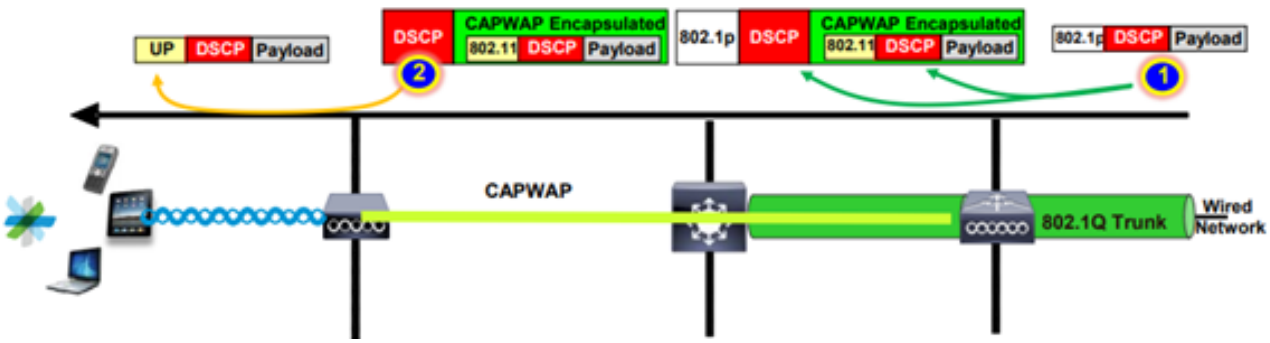
Tatsächlich können wir jede der Trust-Optionen wählen. Wenn Sie CoS jedoch als vertrauenswürdig einstufen, müssen Sie bedenken, dass der Switch im Upstream-Szenario den äußeren DSCP-Wert basierend auf der auf dem Switch konfigurierten CoS-DSCP-Zuordnungstabelle neu schreibt.

Wenn Sie sich jedoch dafür entscheiden, dem DSCP zu vertrauen, schreibt der Switch den äußeren DSCP-Wert nicht um, da er dem eingehenden inneren DSCP vertraut.



Für das Downstream-Szenario fügt der Switch, an dem der WLC angeschlossen ist, den 802.1p-Wert basierend auf der dafür konfigurierten DSCP-CoS-Zuordnungstabelle hinzu. Wenn Sie CoS vertrauen, wird der äußere DSCP-Wert auf Basis des eingehenden 802.1p-Werts geändert.

Wenn Sie sich jedoch dafür entscheiden, DSCP zu vertrauen, schreibt der Switch den äußeren DSCP-Wert nicht um.



Als Beispiel oben: Der Wireless-Client ist mit einer SSID verbunden, die der Verwaltungsschnittstelle des nativen VLAN zugeordnet ist.

Was passiert, wenn Sie CoS auf dem WLC-Switch-Port vertrauen?

Der Client-Datenverkehr erreicht den Trunk-Port. Er ist nicht mit 802.1q markiert, da es sich um ein natives, nicht markiertes VLAN handelt.

Was können Sie tun, um das zu beheben?

Anstelle von CoS können Sie die DSCP-Trust-Option verwenden, was in der Regel empfohlen wird.

Best Practices für die QoS von Wireless LAN-Controllern

Metall-QoS-Profile

Auf dem WLC können vier QoS-Hauptprofile (Platinum, Gold, Silver, Bronze) konfiguriert werden.

- Platinum/Voice - gewährleistet eine hohe Quality of Service für Voice over Wireless
- Gold/Video - unterstützt hochwertige Videoanwendungen
- Silver/Best Effort - unterstützt normale Bandbreite für Clients; dies ist die Standardeinstellung.
- Bronze/background: Bietet die geringste Bandbreite für Gastservices.

Der Hauptzweck dieses QoS-Profils besteht darin, den maximalen äußeren DSCP-Wert im CAPWAP-Header sowohl für Upstream als auch Downstream zu begrenzen, ohne den inneren DSCP zu beeinträchtigen.

Hinweis: Der innere DSCP-Wert wird durch AVC geändert.

Für den lokal geschalteten Datenverkehr wird das QoS-Profil auf den Downstream-Datenverkehr basierend auf dem UP-Wert angewendet. Wenn dieser Wert über dem Standard-WLAN-Wert liegt, wird der Standard-WLAN-Wert verwendet.

Wenn der Client für den Upstream-Datenverkehr einen UP-Wert sendet, der höher ist als der Standard-WLAN-Wert, wird der Standard-WLAN-Wert verwendet.

Weitere Informationen zum Best Practice-Konfigurationsleitfaden für den Catalyst 9800 WLC Wireless QoS für den Catalyst 9800 Wireless Controller

Schritte zur Fehlerbehebung:

1. Das Problem verstehen.
2. Erstellen Sie einen soliden Aktionsplan.
    - Stellen Sie Fehlerbehebungsfragen und ein Netzwerktopologiediagramm.

- Sammeln von Protokollen und Debuggen
- Fragen Sie nach PI Heat-Maps.

3. WLC-Konfigurationen überprüfen.

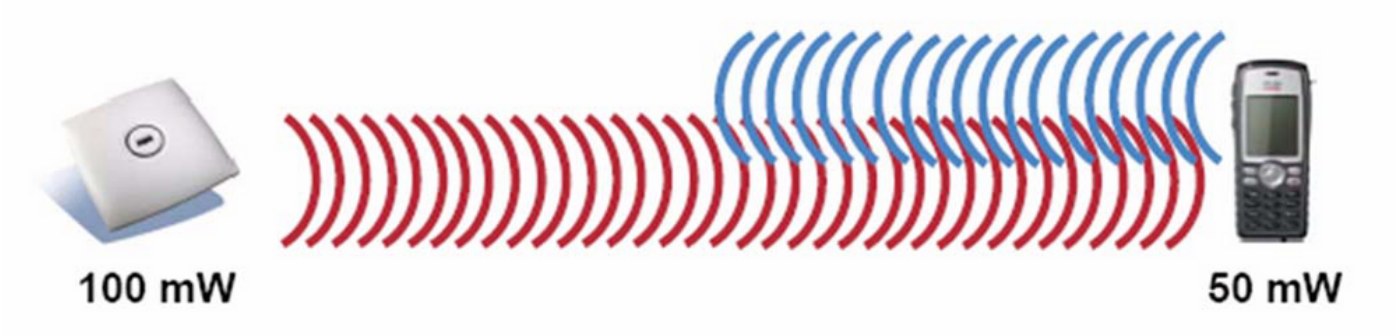
4. Analyse der Fehlersuche

5. Verwenden Sie die VoWLAN-Checkliste, um sicherzustellen, dass die Best Practices eingehalten wurden.

Einwege-Audio

Dieses Problem tritt hauptsächlich dann auf, wenn die Stromversorgung zwischen Client und Access Point asymmetrisch ist.

APs können mit maximaler Leistung senden, aber Wireless-Geräte wie Cisco Telefone können mit weniger Strom senden, sodass Cisco Telefone die nachgeschalteten Frames vom AP hören, aber der AP die Frames im Upstream nicht von Telefonen.



Es wird empfohlen, die AP-TX-Leistung nicht höher als die maximal unterstützte TX-Leistung auf dem Wireless-Gerät zu konfigurieren.

- Aktionsplan:
  - Überprüfen Sie die Client-Verbindung, und stellen Sie sicher, dass sie stabil ist und keine Verbindungen getrennt werden.
  - Prüfen der Funkumgebung (AP-Leistung, Signalstärke usw.)
  - Erfassen Sie OTA-Aufnahmen, um den Audiodatenverkehr zu überprüfen. Es wird Datenverkehr in eine Richtung angezeigt.

- Best Practices:
  - DTPC aktivieren: CCX-Clients können ihre TX-Leistung an die AP-Leistung anpassen.
  - Überprüfen Sie die Lautstärkeeinstellungen auf dem Client-Gerät.

Choppy und Robotic Audio verstehen

Sowohl "Choppy"- als auch "Robotic"-Audio tritt auf, wenn hohe Paketverluste auftreten oder das Paket verzögert wird.

Choppy voice beschreibt Lücken und Verzögerungen im Klang. Dies sind Beispiele für abgehackte

und robotische Aufzeichnungen.

- Aktionsplan:
  - Überprüfen Sie die Client-Verbindung, und stellen Sie sicher, dass sie stabil ist und keine Verbindungen getrennt werden.
  - Prüfen Sie die Funkumgebung (hohe Kanalauslastung, Rauschen und Störgeräte usw.).
  - Collect Captures über den Pfad, um Paketverluste zu prüfen.
- Best Practices:
  - Überprüfen Sie die QoS-Konfigurationen auf dem WLC.
  - Stellen Sie sicher, dass QoS für die kabelgebundene Seite konfiguriert ist.

Verstehen von Lücken und kein Audio beim Roaming

Manchmal melden Benutzer Lücken und einen Verlust der Audioverbindung, wenn sie von einem Standort zu einem anderen wechseln.

- Aktionsplan:
  - Prüfen Sie die Funkumgebung, und vergewissern Sie sich, dass zwischen den APs eine Funkabdeckung besteht.
  - PI Heat MAP abrufen.
  - Collect Captures über den Pfad, um Paketverluste zu prüfen.
- Best Practices:
  - Überprüfen Sie die Client-Verbindung, und stellen Sie sicher, dass sie stabil ist und keine Verbindungen getrennt werden.
  - Stellen Sie sicher, dass der RSSI-Wert auf dem Ziel-AP größer oder gleich -67 ist.

Referenzen

Wireless QoS-Empfehlungen

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 - Implementierungsleitfaden für Cisco Catalyst Wireless Controller der 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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.