# Comprensione di & Risoluzione dei problemi di QoS su Wireless 9800 WLC (riferimento rapido)

## Sommario



## Introduzione

Questo documento descrive QoS sui controller LAN wireless 9800

## Prerequisiti

### Requisiti

In questo documento viene descritto come assegnare le priorità e contrassegnare il traffico sia a monte che a valle.  Illustra la configurazione best practice per il traffico vocale sul controller WLC

(Wireless LAN Controller) e le tecniche di risoluzione dei problemi per un problema comune relativo alla voce.

### Componenti usati

9800 WLC basato sulla versione 17.12 di Cisco IOS® XE.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

### Breve descrizione dello standard IEEE 802.11e e di Wi-Fi Multimedia (WMM)

WMM è una Wi-Fi Alliance basata sullo standard IEEE 802.11e. WMM fornisce funzionalità QoS (Quality of Service) assegnando la priorità al traffico in base a quattro categorie di accesso: voce, video, massimo sforzo e sfondo in base al metodo EDCA (Enhanced Distributed Channel Access).

L'attivazione di WMM è essenziale per ottenere prestazioni ottimali nelle reti Wi-Fi, in particolare negli ambienti in cui sono prevalenti applicazioni a elevata larghezza di banda e bassa latenza. Ad esempio, nelle reti 802.11n, WMM è richiesto per sfruttare appieno le funzionalità di questo standard Wi-Fi ad alta velocità.

### Code WMM e EDCA (Enhanced Distributed Channel Access)

In generale, qualsiasi stazione deve ascoltare il supporto per verificare se è inattivo prima di inviare i frame. Una volta inviato il frame, la stazione ascolta il supporto per vedere se si è verificata una collisione.

I client wireless non possono rilevare le collisioni. A tale scopo, viene utilizzato CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Utilizza un timer fisso e casuale (CWmin, CWmax) e ogni frame inviato deve essere riconosciuto, in modo da essere certi che non ci siano collisioni e che tutti i client possano inviare il traffico.

Come accennato in precedenza, sono disponibili quattro categorie di accesso (code), ognuna delle code utilizza timer diversi. I frame con la priorità più alta vengono inviati statisticamente prima, mentre i frame con la priorità più bassa hanno parametri di backoff che li rendono statisticamente inviati successivamente.

In sintesi, l'esistenza delle quattro code da sola non garantisce la qualità del servizio (QoS); ciò che conta veramente è come il traffico all'interno di ciascuna coda viene gestito in modo efficace.

## Implementazione QoS

Per impostazione predefinita, senza QoS (Quality of Service) configurato, il traffico di rete viene

gestito in modo equo, con un modello di consegna basato sul massimo impegno. Ciò significa che tutto il traffico, indipendentemente dal tipo o dall'importanza, ha la stessa priorità e la stessa probabilità di essere consegnato in un determinato momento. Tuttavia, quando le funzionalità QoS sono abilitate e configurate correttamente, è possibile assegnare la priorità a tipi specifici di traffico di rete, ad esempio voce e video.

La configurazione di QoS comporta due componenti principali: Classificazione e Contrassegno.

Classificazione:

La classificazione implica l'identificazione e la classificazione del traffico di rete in base a criteri specifici, ad esempio il tipo di applicazione, l'indirizzo IP di origine/destinazione, il protocollo o il numero di porta. Il traffico è suddiviso in classi o code:

1. Voce: AC_VO
2. Video: AC_VI
3. Ottimo sforzo: AC_BE
4. Sfondo: AC_BK

Marcatura:

Una volta classificato il traffico nelle code, la segnalazione comporta l'assegnazione di contrassegni QoS o di tag ai pacchetti per indicarne il livello di priorità.

Esistono diversi modi per contrassegnare il traffico. I due standard principali sono il layer 2 802.1p CoS (Class of Service) e il layer 3 DSCP (Differentiated Services Code Point).

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

Nello standard 802.1p, ci sono sette livelli di CoS, ciascuno rappresentato da un campo a 3 bit che può assumere valori compresi tra 0 e 7. Questi valori indicano la priorità del traffico, dove 0 indica la priorità più bassa e 7 la priorità più alta.

Nota: 802.1p è un sottoinsieme dello standard 802.1q e viene presentato solo quando è presente un tag VLAN, ad esempio sulle porte trunk.

Tabella 1: classificazione 802.1P e 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 layer 3 (Differentiated Services Code Point)

DSCP è un tag di livello 3 nell'intestazione IP, utilizza 6 bit che consentono 64 valori diversi (da 0 a 63).

Tabella 2: classificazione DSCP e 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 |

I valori DSCP predominanti includono 46 (EF) per Voce, 34 (AF41) per Video e 0 (BE) per il massimo sforzo.

## Mapping predefinito da DSCP a UP

Come accennato in precedenza, UP è un campo a 3 bit all'interno del frame Ethernet, mentre DSCP è a 6 bit nell'intestazione IP.

Come è possibile calcolare il valore UP (User Priority) di layer 2 dal valore DSCP (Differentiated Services Code Point) di layer 3?

Attualmente non esiste uno standard specifico per questo mapping. Tuttavia, viene utilizzato un

metodo comune noto come 'Mapping predefinito da DSCP a UP'.

Il metodo di mapping da DSCP a UP deriva i valori UP dai 3 msb del pacchetto DSCP e quindi lo mappa sulla categoria di accesso corretta.

Questo metodo viene utilizzato dai computer Microsoft Windows per risolvere un problema noto, descritto in modo più dettagliato nell'esempio 2: Un problema noto del client Microsoft Windows in DSCP To UP Mapping

Tabella 3: mapping da DSCP a UP predefinito

| 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 | |

## Attendibilità flusso di pacchetti e QoS

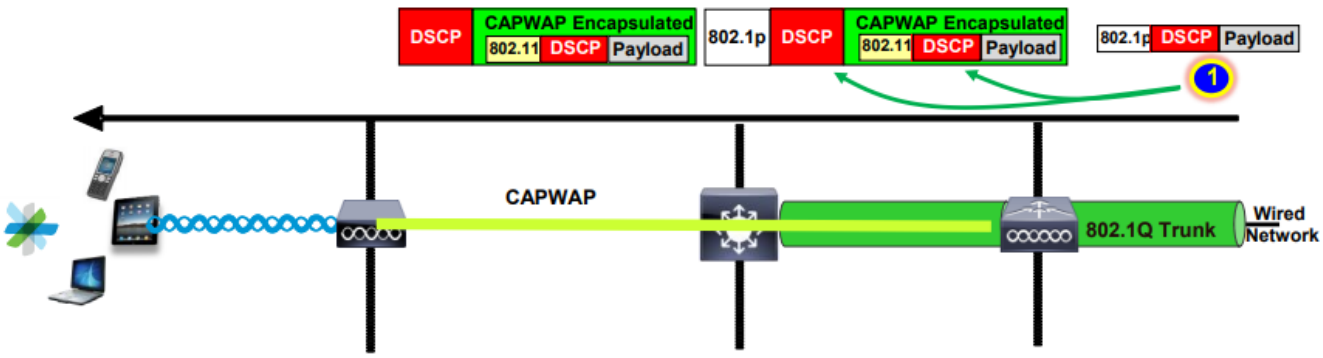
In questa sezione viene descritto il flusso di pacchetti e l'attendibilità del servizio QoS nei seguenti scenari:

1. Switching Centrale - Trust A Valle.
2. Switching Centrale - Trust Upstream.
3. Trust switching locale FlexConnect.

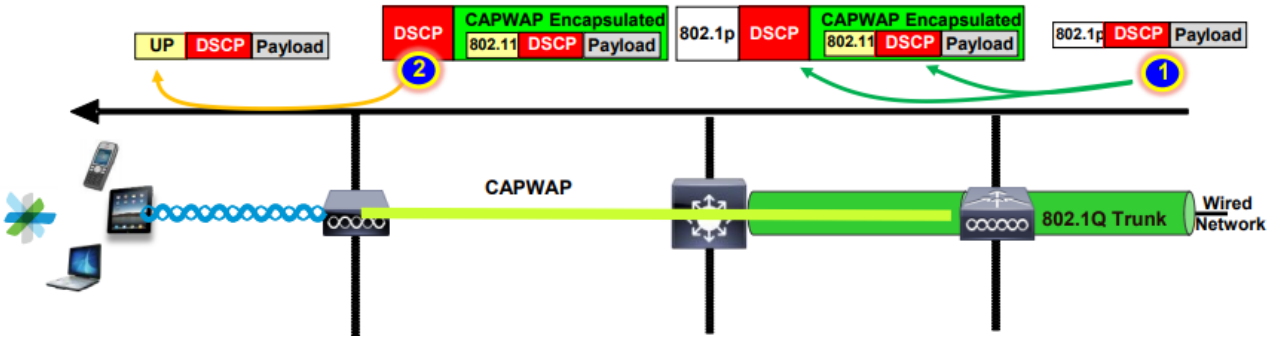
### Switching centrale - Trust a valle

- Downstream: traffico da rete cablata a rete wireless.
- Il traffico a valle è incapsulato in CAPWAP.

1- Si riceve un frame Ethernet sulla porta trunk WLC 802.1q. Il WLC utilizza il valore DSCP interno inviato dalla rete cablata e lo mappa al DSCP esterno nell'intestazione CAPWAP, limita il DSCP esterno a un valore massimo secondo il profilo QoS configurato sul WLC.



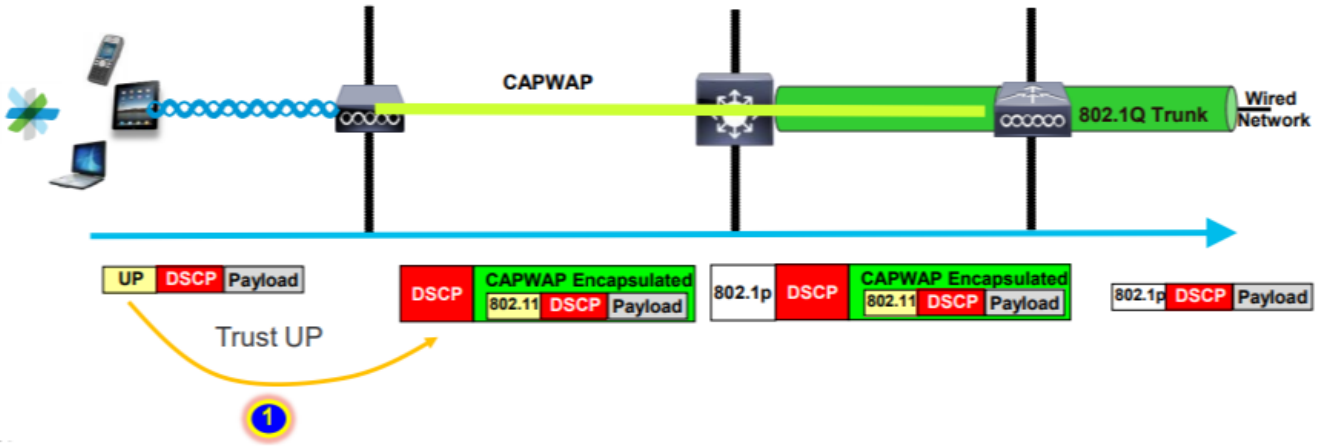

2- Una volta che il frame Ethernet è ricevuto dall'access point, il valore DSCP esterno viene mappato sul valore UP e inviato al client wireless con l'alimentazione CA corretta.



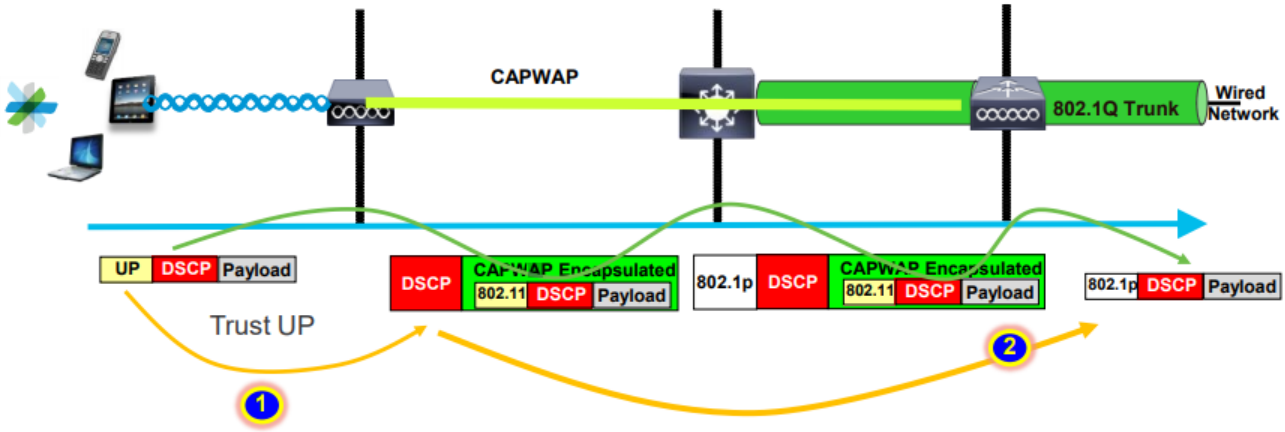

## Switching centrale - Trust a monte

- Upstream: traffico dal wireless al cablato.

1. Il client wireless invia il frame 802.11e (WMM) che viene ricevuto dall'access point.



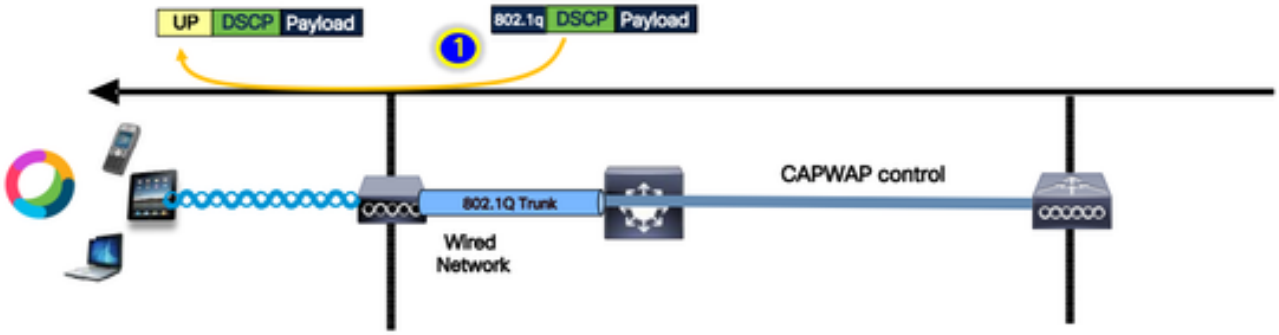

2- L'AP incapsula il pacchetto originale in un'intestazione CAPWAP e mappa l'UP a un valore DSCP esterno, a condizione che il profilo QoS configurato sul WLC consenta tale livello QoS. Il pacchetto viene inviato alla rete cablata con il valore DSCP originale.




## Trust switching locale Flexconnect

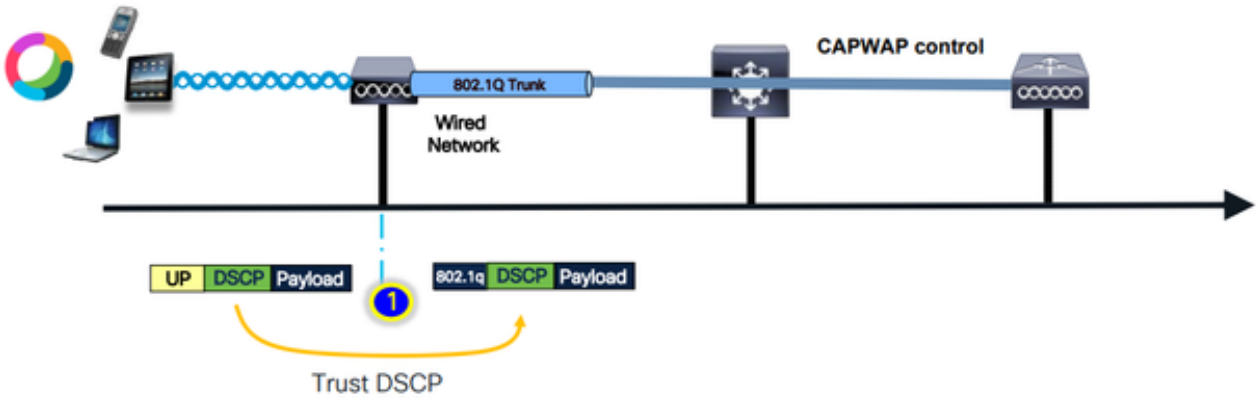
- Flexconnect local Switching - Affidabilità a valle

Per le VLAN a commutazione locale, l'access point FlexConnect assume il valore DSCP del pacchetto IP, elabora qualsiasi criterio QoS (ad esempio, un criterio AVC), lo mappa al valore 802.11e UP sul frame wireless e lo accoda. e lo invia al cliente.




- Flexconnect local Switching - Affidabilità upstream

Il client invia il frame che viene ricevuto dall'access point. L'access point controlla il valore DSCP del pacchetto originale per applicare qualsiasi criterio QoS prima di inviare il pacchetto al router cablato.




# Problemi Comuni Per Il Traffico A Monte

Il traffico nello scenario Upstream, tra il client wireless e l'access point, è fuori controllo, il che significa che non si ha alcun controllo sulle funzionalità QoS inviate dal client via etere.

In uno scenario di lavoro, il client deve inviare un pacchetto con i valori UP e DSCP corretti in modo che il traffico si trovi nella categoria di accesso corretta.

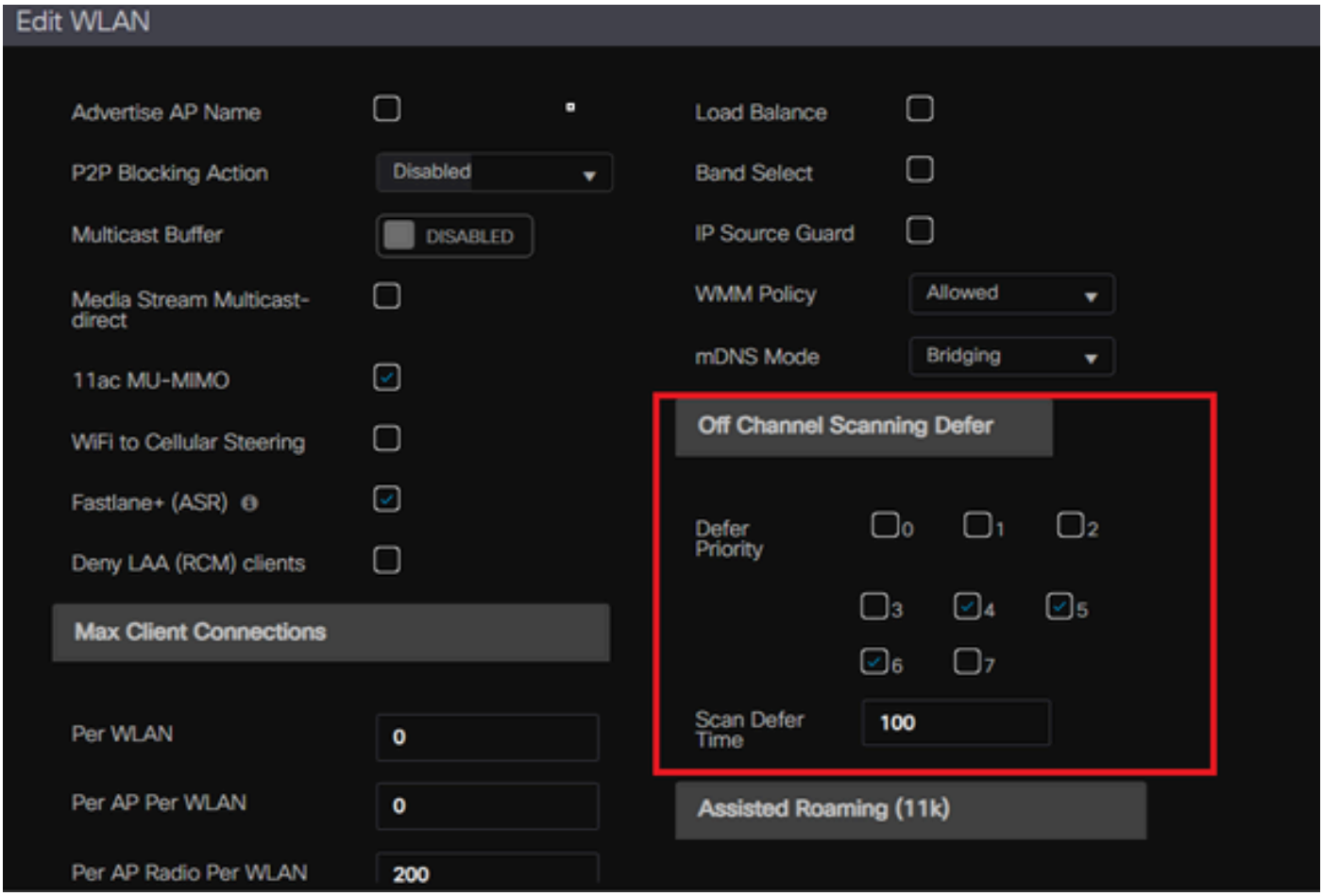
Cosa succede se il client trasmette il traffico con un valore UP non corretto?

## Esempio 1: quando il client trasmette il traffico con un valore UP pari a "2"

Nota: i punti di accesso escono dal canale per eseguire la scansione e raccogliere le informazioni necessarie per l'algoritmo RRM. Ciò avrà sicuramente un impatto sul traffico sensibile, ad esempio voce e video.

L'opzione Off Channel Scanning Defer (Rinvia scansione canali disattivata) è configurata nella scheda WLAN Advanced (Avanzate WLAN). Per impostazione predefinita, è abilitata per le classi UP 4, 5 e 6, con una soglia di tempo di 100 millisecondi; ciò significa che l'access point non esce dal canale per effettuare la scansione per un periodo di 100 ms dopo aver visto traffico sensibile (voce o video).

Supponendo che il client wireless utilizzi un'applicazione vocale, il valore UP previsto è "6". Tuttavia, il client ha inviato il pacchetto con il valore UP errato "2". Il punto di accesso passa quindi alla scansione off-channel e questo influisce sulle prestazioni e sull'esperienza del client.



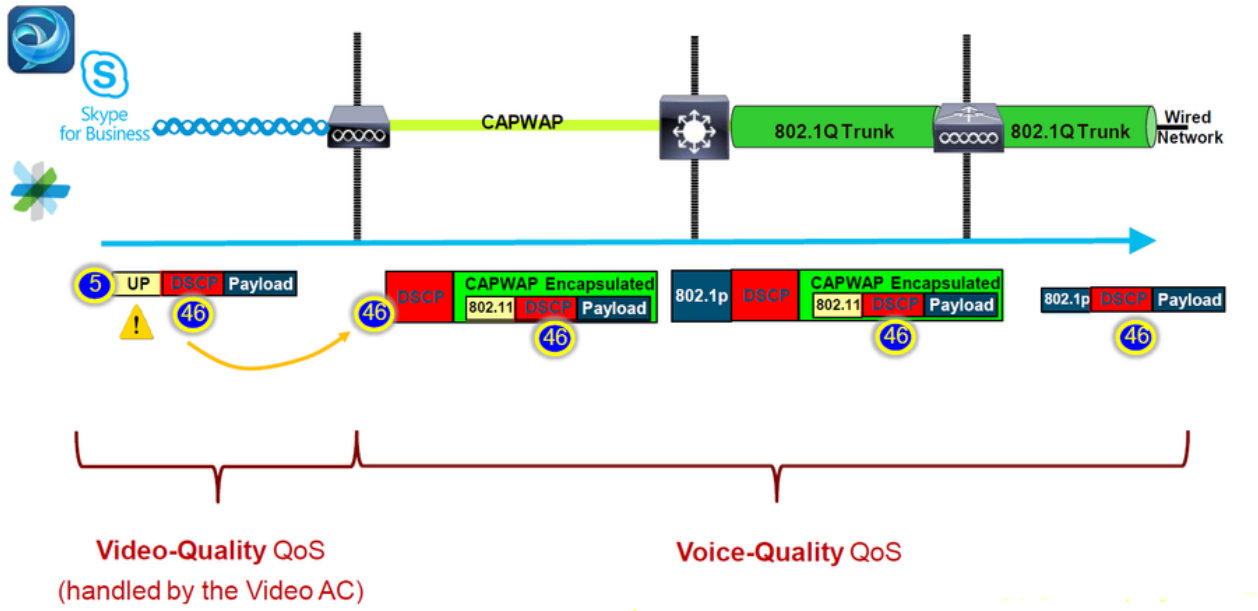

È possibile abilitare il posticipo della scansione per la priorità bassa?

La risposta è sì. L'attivazione della funzione di rinvio della scansione per il traffico a bassa priorità impedisce efficacemente al punto di accesso di eseguire scansioni off-channel, con un conseguente impatto sul funzionamento dell'RRM e sugli algoritmi di rilevamento rogue. Per risolvere questo problema, è necessario adottare un approccio alternativo per facilitare la scansione dei canali e assegnare le priorità al traffico.

## Esempio 2: Un Problema Conosciuto Del Client Microsoft Windows In DSCP Per Il Mapping UP

Un problema comune osservato nei computer MS Windows si verifica quando viene utilizzato il mapping predefinito tra i valori DHCP e UP. In questa mappatura, la priorità utente (UP) è determinata dai tre bit più significativi (msb) del valore DSCP (Differentiated Services Code Point). Ad esempio, per il traffico vocale con un valore DSCP di EF (101110), viene eseguito il mapping a UP 5 (101).

Per impostazione predefinita, i punti di accesso in upstream considerano attendibile il valore UP, in modo che il traffico vocale venga trattato nella categoria di accesso video (AC_VI) con il valore DSCP impostato su 34 anziché nella categoria di accesso vocale (AC_VO) con il valore DSCP impostato su 46, a cui è destinato. Per questo motivo, i frame vocali hanno tempi di attesa più lunghi e una maggiore possibilità di nuovi tentativi.

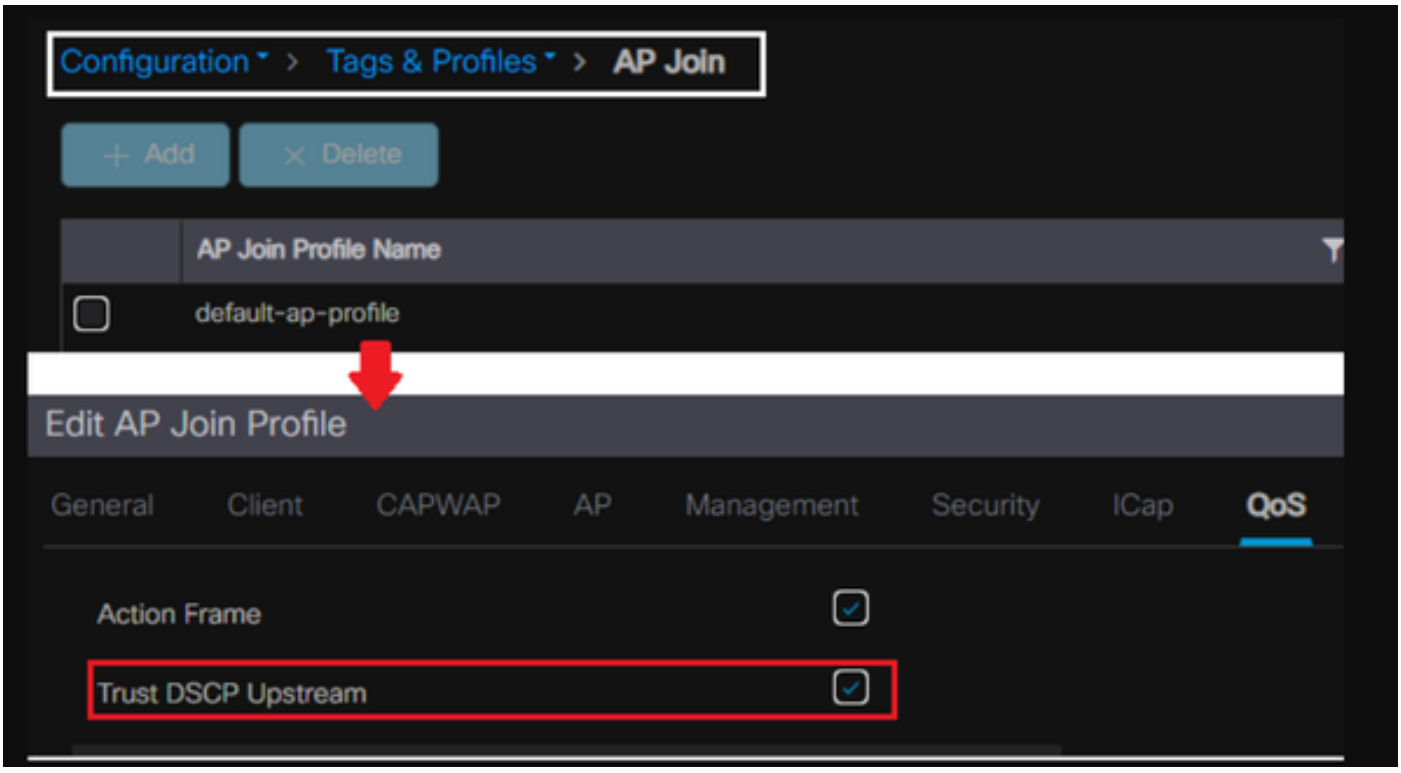



C'è un modo per riparare questo?

La risposta è sì se la macchina MS Windows invia traffico vocale con il valore DSCP corretto.

Come può essere risolto?

Utilizzando l'opzione "trust DSCP Upstream" sul WLC. Questa opzione forza l'access point a considerare attendibile il DSCP interno nell'upstream anziché nell'UP.



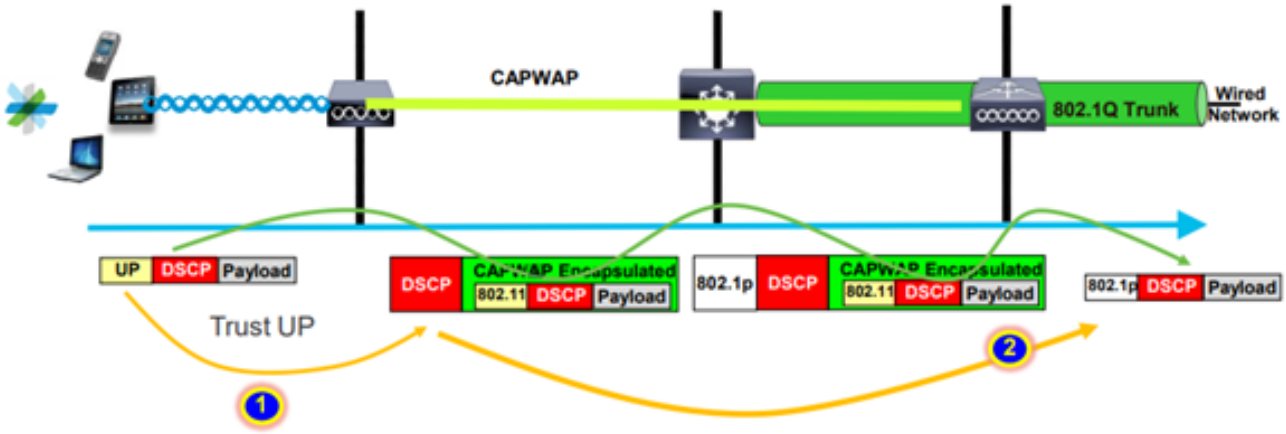

Per ulteriori istruzioni su come configurare il computer Windows in modo che ignori o contrassegni il traffico, vedere ["Come abilitare l'etichettatura DSCP sui computer Windows"]

# Quale protocollo considerare attendibile : DSCP o COS?

Quale tipo di trust selezionare per la porta dello switch WLC?

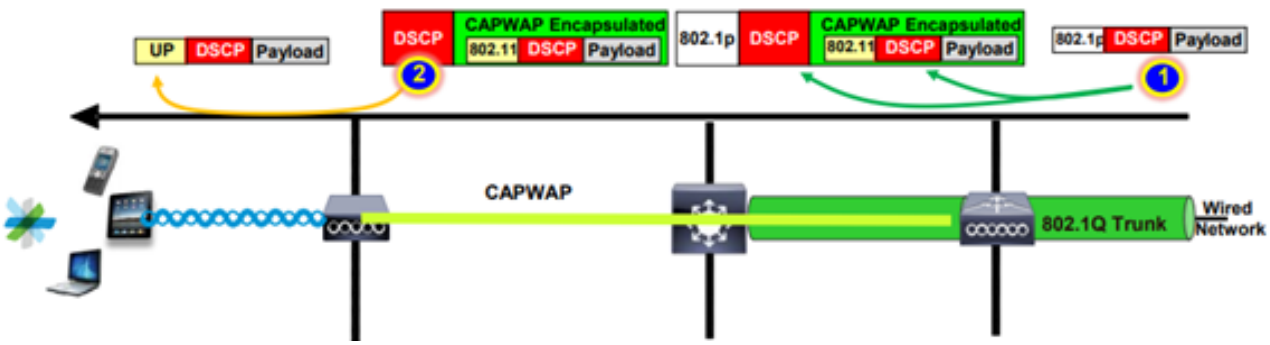
In realtà, possiamo scegliere una qualsiasi delle opzioni di trust. Tuttavia, se si sceglie di considerare attendibile il CoS, è necessario tenere presente che per lo scenario Upstream lo switch riscrive il valore DSCP esterno in base alla tabella di mapping CoS-DSCP configurata sullo switch.

Tuttavia, se si sceglie di considerare attendibile DSCP, lo switch non riscrive il valore DSCP esterno in quanto considera attendibile il DSCP interno in ingresso.




Nello scenario a valle, lo switch a cui è connesso il WLC aggiunge il valore 802.1p in base alla tabella di mapping DSCP-CoS configurata su di esso. Se si sceglie di considerare attendibile CoS, il valore DSCP esterno viene modificato in base al valore 802.1p in ingresso.

Tuttavia, se si sceglie di considerare attendibile DSCP, lo switch non riscrive il valore DSCP esterno.




Come esempio sopra: il client wireless si è connesso a un SSID mappato all'interfaccia di gestione sulla VLAN nativa.

Cosa succede se si sceglie di considerare attendibile il servizio CoS sulla porta dello switch WLC?

Il traffico client raggiunge la porta trunk, non è contrassegnato su 802.1q in quanto è una VLAN nativa senza tag.

Cosa puoi fare per risolvere questo problema?

È possibile utilizzare l'opzione di attendibilità DSCP anziché CoS, che in genere corrisponde alla raccomandazione.

# Best practice QoS per controller LAN wireless

## Profili QoS in metallo

Possiamo configurare quattro profili QoS principali sul WLC (Platinum, Gold, Silver, Bronze).

- Platinum/voice - garantisce un'alta qualità del servizio per la voce tramite wireless
- Gold/video - supporta applicazioni video di alta qualità
- Argento/massimo sforzo - supporta la larghezza di banda normale per i client; questa è l'impostazione predefinita
- Bronzo/sfondo - offre la larghezza di banda più bassa per i servizi guest.

Lo scopo principale di questo profilo QoS è quello di limitare il valore DSCP esterno massimo sull'intestazione CAPWAP sia per Upstream che per Downstream senza influire sul DSCP interno.

Nota: il valore DSCP interno viene modificato da AVC.

Per il traffico a commutazione locale, il profilo QoS viene applicato al traffico a valle in base al valore UP. se questo valore è superiore al valore WLAN predefinito, viene utilizzato il valore WLAN predefinito.

Per il traffico upstream, se il client invia un valore UP superiore al valore WLAN predefinito, viene utilizzato il valore WLAN predefinito.

Per ulteriori dettagli sulla guida alla configurazione delle best practice del WLC 9800, Wireless QoS per Catalyst 9800 Wireless Controller

Procedura di risoluzione dei problemi:

1. Comprendere il problema.
2. Creare un piano d'azione solido.
    - Fare domande sulla risoluzione dei problemi e creare un diagramma della topologia di rete.
    - Raccogli log e debug.
    - Chiedete mappe termiche PI.

3. Controllare le configurazioni del WLC.

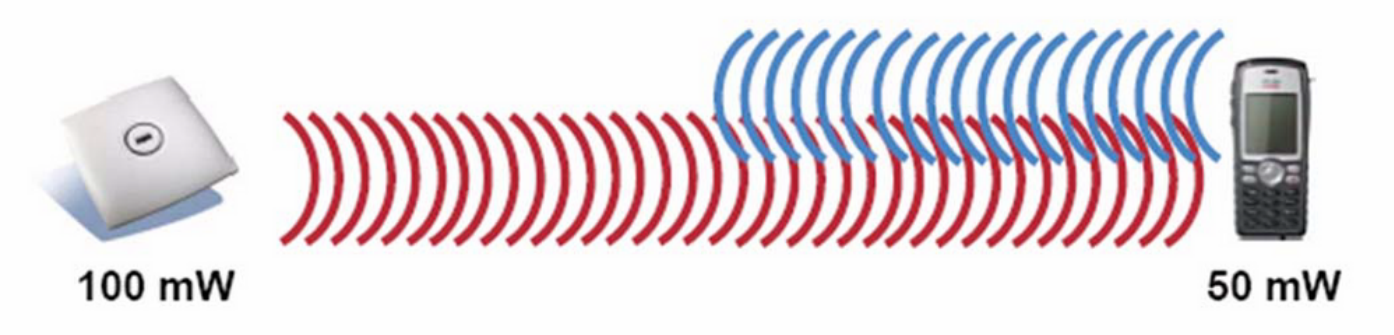
4. Analizzare i debug

5. Utilizzare l'elenco di controllo VoWLAN per verificare se sono state seguite le best practice.

## Informazioni sull'audio unidirezionale

Principalmente questo problema si verifica quando tra il client e l'access point esiste un potere asimmetrico.

I punti di accesso possono trasmettere con la massima potenza, tuttavia i dispositivi wireless come i telefoni Cisco possono trasmettere con una minore quantità di energia, facendo sì che i telefoni Cisco sentano i frame a valle dal punto di accesso, ma quest'ultimo non sente i frame a monte dai telefoni.




Si consiglia di non configurare una potenza TX del punto di accesso superiore alla potenza TX massima supportata sul dispositivo wireless.

- Piano d'azione:
  - Controllare la connessione client e assicurarsi che sia stabile e che non ci siano disconnessioni.
  - Controllare l'ambiente RF (alimentazione AP, forza del segnale, ecc.).
  - Raccogli le clip OTA per controllare il traffico audio; viene visualizzato il traffico in una sola direzione.

- Procedure ottimali:
  - Abilita DTPC: consente ai client CCX di regolare la propria potenza TX in base all'alimentazione AP.
  - Controllare le impostazioni del volume nel dispositivo client.

## Comprendere l'audio discontinuo e robotico

Sia l'audio "discontinuo" che quello "robotico" si verificano quando il pacchetto viene perso o ritardato.

La voce discontinua descrive gli spazi vuoti e il ritardo nel suono. Questi sono esempi di registrazioni traballanti e robotiche.

- Piano d'azione:
  - Controllare la connessione del client e assicurarsi che sia stabile e che non ci siano disconnessioni.
  - Controllare l'ambiente RF (utilizzo del canale elevato, dispositivi di disturbo e interferenza, ecc.).
  - Raccogli acquisizioni attraverso il percorso per verificare la presenza di perdite di pacchetti.
- Procedure ottimali:
  - Controllare le configurazioni QoS su WLC.
  - Verificare che QoS sia configurato sul lato cablato.

## Informazioni su gap e assenza di audio durante il roaming

Talvolta gli utenti segnalano interruzioni e perdita della connessione audio durante il roaming da una località all'altra.

- Piano d'azione:
  - Controllare l'ambiente RF e verificare che la cella di copertura tra i punti di accesso sia corretta.
  - Ottieni IP HEAT MAP.
  - Raccogli acquisizioni attraverso il percorso per verificare la presenza di perdite di pacchetti.
- Procedure ottimali:
  - Controllare la connessione client e assicurarsi che sia stabile e che non ci siano disconnessioni.
  - Accertarsi che il valore RSSI nell'access point di destinazione sia maggiore o uguale a -67

## Riferimenti

Raccomandazioni QoS wireless

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

Guida alla visibilità e al controllo dell'implementazione delle applicazioni per Cisco Catalyst serie 9800 Wireless Controller

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).