Esempio di configurazione di QoS sui Converged Access Controller e sui Lightweight Access Point

Sommario

Introduzione

In questo documento viene descritto come configurare QoS in una rete Cisco ad accesso convergente con Lightweight Access Point (LAP) e con lo switch Cisco Catalyst 3850 o il Cisco 5760 Wireless LAN Controller (WLC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di come configurare i LAP e i Cisco Converged Access Controller
- Conoscenza di come configurare il routing di base e la funzionalità QoS in una rete cablata

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst 3850 con Cisco IOS? Software XE release 3.2.2(SE)
- Controller LAN wireless Cisco 5760 con software Cisco IOS XE versione 3.2.2(SE)
- Cisco serie 3600 Lightweight Access Point

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

QoS indica la capacità della rete di fornire un servizio migliore o speciale a un insieme di utenti o applicazioni a scapito di altri utenti o applicazioni.

Con QoS, la larghezza di banda può essere gestita in modo più efficiente sulle LAN, incluse le WLAN (Wireless LAN) e le WAN. QoS offre servizi di rete avanzati e affidabili con i seguenti servizi:

- Supporta larghezza di banda dedicata per utenti e applicazioni critiche.
- Controlla la variazione e la latenza richieste dal traffico in tempo reale.
- Gestisce e riduce al minimo la congestione della rete.
- Forma il traffico di rete per facilitarne il flusso.
- Imposta le priorità del traffico di rete.

In passato, le WLAN venivano usate principalmente per trasportare il traffico delle applicazioni dati a bassa larghezza di banda. Con l'espansione delle WLAN in ambienti verticali (come il settore retail, finanziario ed education) e aziendali, le WLAN vengono ora utilizzate per il trasporto di applicazioni dati a elevata larghezza di banda in combinazione con applicazioni multimediali sensibili al tempo. Questo requisito ha reso necessaria la QoS wireless.

Il gruppo di lavoro IEEE 802.11e all'interno del comitato per gli standard IEEE 802.11 ha completato la definizione standard e la Wi-Fi Alliance ha creato la certificazione Wi-Fi Multimedia (WMM), ma l'adozione dello standard 802.11e è ancora limitata. La maggior parte dei dispositivi è certificata WMM, in quanto la certificazione WMM è necessaria per le certificazioni 802.11n e 802.11ac. Molti dispositivi wireless non assegnano livelli QoS diversi ai pacchetti inviati al livello di collegamento dati, quindi questi dispositivi inviano la maggior parte del traffico senza contrassegno QoS e senza assegnazione di priorità relativa. Tuttavia, la maggior parte dei telefoni IP Voice over Wireless LAN (VoWLAN) 802.11 contrassegna e assegna la priorità del traffico vocale. Questo documento si concentra sulla configurazione QoS per telefoni IP VoWLAN e su

dispositivi wi-fi con funzionalità video che contrassegnano il loro traffico vocale.

> **Nota:** La configurazione QoS per i dispositivi che non eseguono il contrassegno interno esula dall'ambito di questo documento.

La modifica 802.11e definisce otto livelli di priorità utente (UP), raggruppati due per due in quattro livelli QoS (categorie di accesso):

- Platinum/Voice (UP 7 e 6) - Garantisce un'elevata qualità del servizio per la comunicazione vocale wireless.
- Gold/Video (UP-5 e 4) - Supporta applicazioni video di alta qualità.
- Argento/Massimo sforzo (UP 3 e 0) - Supporta la normale larghezza di banda per i client. Si tratta dell'impostazione predefinita.
- Bronzo/Background (UP 2 e 1) - Fornisce la larghezza di banda più bassa per i servizi guest.

Platinum viene comunemente utilizzato per i client VoIP e Gold per i client video. Questo documento offre un esempio di configurazione che illustra come configurare QoS sui controller e comunicare con una rete cablata configurata con QoS per client VoWLAN e video.

Miglioramenti Contrassegno pacchetti QoS L3

I Cisco Converged Access Controller supportano il contrassegno DSCP (IP Differentiated Services Code Point) di layer 3 (L3) per i pacchetti inviati da WLC e LAP. Questa funzione migliora il modo in cui i punti di accesso utilizzano le informazioni L3 per garantire che i pacchetti ricevano la corretta assegnazione di priorità over-the-air dall'access point al client wireless.

In un'architettura WLAN ad accesso convergente che usa gli switch Catalyst 3850 come controller wireless, gli access point si connettono direttamente allo switch. In un'architettura WLAN ad accesso convergente che usa i controller 5760, i dati WLAN vengono tunneling tra l'AP e il WLC tramite il protocollo CAPWAP (Control and Provisioning of Wireless Access Point). Per mantenere la classificazione QoS originale su questo tunnel, le impostazioni QoS del pacchetto dati incapsulato devono essere mappate in modo appropriato sui campi layer 2 (L2) (802.1p) e L3 (IP DSCP) del pacchetto del tunnel esterno.

Quando si configura QoS per VoWLAN e video, è possibile configurare un criterio QoS specifico per i client wireless e un criterio specifico per una WLAN o entrambi. Inoltre, è possibile integrare l'installazione con una configurazione specifica della porta che collega l'access point, in particolare con gli switch Catalyst 3850. In questo esempio viene descritta la configurazione QoS del client wireless, la WLAN e la porta del punto di accesso. Gli obiettivi principali di una configurazione QoS per applicazioni VoWLAN e video sono:

- Riconoscere il traffico voce e video (classificazione e contrassegno del traffico), sia a monte che a valle.
- Contrassegna traffico voce e video con un livello di priorità voce: 802.11e UP 6, 802.1p 5, DSCP 46 per la voce.802.11e UP 5, DSCP 34 per video.
- Assegnazione della larghezza di banda per il traffico vocale, la segnalazione vocale e il traffico video.

Configurazione di una rete wireless per QoS con MQC

Prima di configurare QoS, è necessario configurare la funzione Wireless Controller Module (WCM) dello switch Catalyst 3850 o Cisco 5760 WLC per il funzionamento di base e registrare i LAP su WCM. in questo documento si presume che WCM sia configurato per le operazioni di base e che i LAP siano registrati su WCM.

La soluzione di accesso convergente utilizza l'interfaccia della riga di comando (CLI) Modular QoS (MQC). Per ulteriori informazioni sull'uso di MQC nella configurazione QoS dello switch Catalyst 3850, consultare la guida alla configurazione QoS di Cisco IOS XE versione 3SE (switch Catalyst 3850).

La configurazione di QoS con MQC sui controller degli accessi convergenti si basa su quattro elementi:

- Le **mappe di classe** vengono usate per riconoscere il traffico di interesse. Le mappe di classe possono utilizzare diverse tecniche (come il contrassegno QoS esistente, gli elenchi degli accessi o le VLAN) per identificare il traffico di interesse.
- Le **policy-map** vengono usate per determinare le impostazioni QoS da applicare al traffico di interesse. Le mappe dei criteri chiamano le mappe delle classi e applicano diverse impostazioni QoS (come indicazione specifica, livelli di priorità, allocazione della larghezza di banda e così via) a ciascuna classe.
- Le **policy di servizio** vengono utilizzate per applicare le policy-map ai punti strategici della rete. Nella soluzione di accesso convergente è possibile applicare criteri di servizio a utenti, SSID (Service Set Identifier), radio AP e porte. I criteri relativi a porte, SSID e client possono essere configurati dall'utente. I criteri radio sono controllati dal modulo di controllo wireless. I criteri QoS wireless per porta, SSID, client e radio vengono applicati nella direzione a valle quando il traffico passa dallo switch o dal controller ai client wireless.
- Le **mappe tabella** vengono usate per esaminare il contrassegno QoS in arrivo e per decidere i contrassegni QoS in uscita. Le mappe tabella sono posizionate nelle mappe criteri applicate agli SSID. È possibile utilizzare le mappe tabella per mantenere (copiare) o modificare l'indicazione. È inoltre possibile utilizzare le mappe tabella per creare una mappatura tra la marcatura per reti cablate e wireless. Il contrassegno per reti cablate utilizza DSCP (L3 QoS) o 802.1p (L2 QoS). Il contrassegno wireless utilizza Priorità utente (UP). Le mappe tabella vengono comunemente utilizzate per determinare quale contrassegno DSCP deve essere utilizzato per ogni UP di interesse e quale UP deve essere utilizzato per ogni DSCP di interesse. Le mappe di tabella sono fondamentali per l'accesso convergente a QoS perché non esiste una traduzione diretta tra i valori DSCP e UP.

Tuttavia, le mappe tabella da DSCP a UP consentono anche l'istruzione *copy*. In questo caso, la soluzione di accesso convergente utilizza l'architettura Cisco per la tabella di mappatura voce, video e dati integrati (AVVID) per determinare la traduzione da DSCP a UP o UP a DSCP:

Indice etichetta	Campo chiave	Valore in ingresso	DSCP esterno	CoS	SU
0	N.D.	Non selezionato	0	0	0
1-10	DSCP	0-7	0-7	0	0
11-18	DSCP	8-15	8-15	1	2
19-26	DSCP	16-23	16-23	2	3
27-34	DSCP	24-31	24-31	3	4
35-46	DSCP	32-39	32-39	4	5
47-48	DSCP	40-47	40-47	5	6
49-63	DSCP	48-55	48-55	6	7
64	DSCP	56-63	56-63	7	7

65	CoS	0	0	0	0
66	CoS	1	8	1	2
67	CoS	2	16	2	3
68	CoS	3	24	3	4
69	CoS	4	32	4	5
70	CoS	5	40	5	6
71	CoS	6	48	6	7
72	CoS	7	56	7	7
73	SU	0	0	0	0
74	SU	1	8	1	1
75	SU	2	16	1	2
76	SU	3	24	2	3
77	SU	4	34	3	4
78	SU	5	34	4	5
79	SU	6	46	5	6
80	SU	7	46	7	7

Criteri hardcoded predefiniti

I controller degli accessi convergenti avviano profili di criteri QoS hardcoded che possono essere applicati alle WLAN. Questi profili applicano le policy di metallo (platinum, gold e così via) che sono familiari agli amministratori dei controller Cisco Unified Wireless Networks (CUWN). Se l'obiettivo non è creare policy che assegnino una larghezza di banda specifica al traffico vocale, ma semplicemente garantire che il traffico vocale riceva il contrassegno QoS appropriato, è possibile utilizzare le policy hardcoded. Le policy hardcoded possono essere applicate alla WLAN e possono essere diverse nelle direzioni a monte e a valle.

> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).
>
> Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Platino

La politica hardcoded per la voce è chiamata platinum. Impossibile modificare il nome.

Questa è la politica a valle per il livello Platinum QoS:

```
Policy-map platinum
Class class-default
 set dscp dscp table plat-dscp2dscp
 set wlan user-priority dscp table plat-dscp2up
Table-map plat-dscp2dscp
   from 45 to 45
   from 46 to 46
   from 47 to 47
```

```
   default copy
Table-map plat-dscp2up
   from 34 to 4
   from 46 to 6
   default copy
```

Questa è la politica a monte per il livello QoS Platinum:

```
Policy-map platinum-up
   Class class-default
     set dscp wlan user-priority table plat-up2dscp

Table-map plat-up2dscp
   from 4 to 34
   from 5 to 34
   from 6 to 46
   from 7 to 8
   default copy
```

Oro

La politica hardcoded per i video si chiama gold. Impossibile modificare il nome.

Questa è la politica a valle per il livello Gold QoS:

```
Policy Map gold
   Class class-default
     set dscp dscp table gold-dscp2dscp
     set wlan user-priority dscp table gold-dscp2u
Table Map gold-dscp2dscp
   from 45 to 34
   from 46 to 34
   from 47 to 34
   default copy

Table Map gold-dscp2up
   from 45 to 4
   from 46 to 4
   from 47 to 4
   default copy
```

Questa è la politica a monte per il livello Gold QoS:

```
Policy Map gold-up
   Class class-default
     set dscp wlan user-priority table gold-up2dscp

Table Map gold-up2dscp
   from 6 to 34
   from 7 to 34
   default copy
```

Argento

La politica hardcoded per il massimo sforzo è chiamata silver. Impossibile modificare il nome.

Questa è la policy a valle per il livello QoS silver:

```
Policy Map silver
   Class class-default
     set dscp dscp table silver-dscp2dscp
     set wlan user-priority dscp table silver-dscp2up

Table Map silver-dscp2dscp
   from 34 to 0
   from 45 to 0
   from 46 to 0
   from 47 to 0
   default copy
Table Map silver-dscp2up
   from 34 to 0
   from 45 to 0
   from 46 to 0
   from 47 to 0
   default copy
```

Questa è la policy a monte per il livello QoS silver:

```
Policy Map silver-up
   Class class-default
     set dscp wlan user-priority table silver-up2dscp
Table Map silver-up2dscp
   from 4 to 0
   from 5 to 0
   from 6 to 0
   from 7 to 0
   default copy
```

Bronzo

La politica hardcoded per il traffico in background è chiamata bronzo. Impossibile modificare il nome.

Questa è la politica a valle per il livello QoS di bronzo:

```
Policy Map bronze
   Class class-default
     set dscp dscp table bronze-dscp2dscp
 set wlan user-priority dscp table bronze-dscp2up

Table Map bronze-dscp2dscp
   from 0 to 8
   from 34 to 8
   from 45 to 8
   from 46 to 8
   from 47 to 8
   default copy

Table Map bronze-dscp2up
   from 0 to 1
   from 34 to 1
   from 45 to 1
   from 46 to 1
   from 47 to 1
   default copy
```

Questa è la politica a monte per il livello QoS di bronzo:

```
Policy Map bronze-up
   Class class-default
     set dscp wlan user-priority table bronze-up2dscp
Table Map bronze-up2dscp
   from 0 to 8
   from 1 to 8
   from 4 to 8
   from 5 to 8
   from 6 to 8
   from 7 to 8
   default copy
```

Dopo aver deciso quale tabella-mappa corrisponde meglio al traffico di destinazione per un determinato SSID, è possibile applicare il criterio di corrispondenza alla WLAN. In questo esempio, un criterio viene applicato nella direzione a valle (output, dal punto di accesso al client wireless) e un criterio nella direzione a monte (input, dal client wireless, attraverso il punto di accesso, al controller):

```
3850#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3850(config)#wlan test1
3850(config-wlan)#service-policy output platinum
3850(config-wlan)#service-policy input platinum-up
3850(config-wlan)#end
3850#
```

Controllare la configurazione WLAN per verificare quale criterio è stato applicato alla WLAN:

```
3850#show wlan name test1
WLAN Profile Name     : test1
===============================================
Identifier                                : 1
Network Name (SSID)                       : test1
Status                                    : Disabled
Broadcast SSID                            : Enabled
Maximum number of Associated Clients      : 0
AAA Policy Override                       : Disabled
Network Admission Control
 NAC-State                               : Disabled
Number of Active Clients                  : 0
Exclusionlist Timeout                     : 60
Session Timeout                           : 1800 seconds
CHD per WLAN                              : Enabled
Webauth DHCP exclusion                    : Disabled
Interface                                 : default
Interface Status                          : Up
Multicast Interface                       : Unconfigured
WLAN IPv4 ACL                             : unconfigured
WLAN IPv6 ACL                             : unconfigured
DHCP Server                               : Default
DHCP Address Assignment Required          : Disabled
DHCP Option 82                            : Disabled
DHCP Option 82 Format                     : ap-mac
DHCP Option 82 Ascii Mode                 : Disabled
DHCP Option 82 Rid Mode                   : Disabled
QoS Service Policy - Input
 Policy Name                             : platinum-up
 Policy State                            : Validation Pending
QoS Service Policy - Output
 Policy Name                             : platinum
```

```
 Policy State                                    : Validation Pending
QoS Client Service Policy
 Input  Policy Name                              : unknown
 Output Policy Name                              : unknown
WMM                                               : Allowed
Channel Scan Defer Priority:
 Priority (default)                              : 4
 Priority (default)                              : 5
 Priority (default)                              : 6
Scan Defer Time (msecs)                           : 100
Media Stream Multicast-direct                     : Disabled
CCX - AironetIe Support                           : Enabled
CCX - Gratuitous ProbeResponse (GPR)              : Disabled
CCX - Diagnostics Channel Capability              : Disabled
Dot11-Phone Mode (7920)                           : Invalid
Wired Protocol                                    : None
Peer-to-Peer Blocking Action                      : Disabled
Radio Policy                                      : All
DTIM period for 802.11a radio                     : 1
DTIM period for 802.11b radio                     : 1
Local EAP Authentication                          : Disabled
Mac Filter Authorization list name                : Disabled
Accounting list name                              : Disabled
802.1x authentication list name                   : Disabled
Security
   802.11 Authentication                          : Open System
   Static WEP Keys                                : Disabled
   802.1X                                         : Disabled
   Wi-Fi Protected Access (WPA/WPA2)              : Enabled
       WPA (SSN IE)                               : Disabled
       WPA2 (RSN IE)                              : Enabled
           TKIP Cipher                            : Disabled
           AES Cipher                             : Enabled
       Auth Key Management
           802.1x                                 : Enabled
           PSK                                    : Disabled
           CCKM                                   : Disabled
   CKIP                                           : Disabled
   IP Security                                    : Disabled
   IP Security Passthru                           : Disabled
   L2TP                                           : Disabled
   Web Based Authentication                       : Disabled
   Conditional Web Redirect                       : Disabled
   Splash-Page Web Redirect                       : Disabled
   Auto Anchor                                    : Disabled
   Sticky Anchoring                               : Enabled
   Cranite Passthru                               : Disabled
   Fortress Passthru                              : Disabled
   PPTP                                           : Disabled
   Infrastructure MFP protection                  : Enabled
   Client MFP                                     : Optional
   Webauth On-mac-filter Failure                  : Disabled
   Webauth Authentication List Name               : Disabled
   Webauth Parameter Map                          : Disabled
   Tkip MIC Countermeasure Hold-down Timer        : 60
Call Snooping                                     : Disabled
Passive Client                                    : Disabled
Non Cisco WGB                                     : Disabled
Band Select                                       : Disabled
Load Balancing                                    : Disabled
IP Source Guard                                   : Disabled
```

Configurazione manuale

I criteri hardcoded applicano il contrassegno QoS predefinito ma non l'allocazione della larghezza di banda. I criteri hardcoded presuppongono anche che il traffico sia già contrassegnato. In un ambiente complesso, è possibile utilizzare una combinazione di criteri per riconoscere e contrassegnare il traffico voce e video in modo appropriato, per impostare l'allocazione della larghezza di banda nelle direzioni a valle e a monte e per utilizzare il controllo dell'ammissione di chiamata per limitare il numero di chiamate avviate dalla cella wireless.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Passaggio 1: Identificazione e contrassegno del traffico vocale

Il primo passo è riconoscere il traffico voce e video. Il traffico vocale può essere classificato in due categorie:

- Flusso vocale, che trasmette la parte audio della comunicazione.
- Segnalazione vocale, che trasmette informazioni statistiche scambiate tra endpoint voce.

Il flusso vocale in genere utilizza porte di destinazione Real-time Transport Protocol (RTP) e User Datagram Protocol (UDP) nell'intervallo 16384 - 32767. Questo è l'intervallo. le porte effettive sono in genere più strette e dipendono dall'implementazione.

Esistono diversi protocolli di segnalazione vocale. In questo esempio di configurazione viene utilizzato Jabber. Jabber utilizza le seguenti porte TCP per la connessione e la directory:

- TCP 80 (HTTP)
- 143 (Internet Message Access Protocol [IMAP])
- 443 (HTTPS)
- 993 (IMAP) per servizi come Cisco Unified MeetingPlace o Cisco WebEx per le riunioni e Cisco Unity Connection per le funzionalità della segreteria telefonica
- TCP 389/636 (server LDAP (Lightweight Directory Access Protocol) per ricerche di contatti)
- FTP (1080)
- TFTP (UDP 69) per il trasferimento di file (ad esempio file di configurazione) dai peer o dal server

Per questi servizi potrebbe non essere necessaria una definizione di priorità specifica.

Jabber utilizza il protocollo SIP (Session Initiation Protocol) (UDP/TCP 5060 e 5061) per la segnalazione vocale.

Il traffico video utilizza porte e protocolli diversi che dipendono dall'implementazione. In questa configurazione viene utilizzata una telecamera Tandberg PrecisionHD 720p per le videoconferenze. La telecamera Tandberg PrecisionHD 720p può utilizzare diversi codec; la larghezza di banda utilizzata dipende dal codec scelto:

- I codec C20, C40 e C60 utilizzano lo standard H.323/SIP e possono consumare fino a 6 Mbps in connessioni point-to-point.
- Il codec C90 utilizza gli stessi protocolli e può consumare fino a 10 Mbps nelle comunicazioni multisito.

L'implementazione Tandberg di H.323 utilizza tipicamente UDP 970 per lo streaming video, UDP

971 per il segnale video, UDP 972 per lo streaming audio e UDP 973 per il segnale audio. Le telecamere Tandberg usano anche altre porte, come:

- UDP 161
- UDP 962 (Simple Network Management Protocol [SNMP])
- TCP 963 (netlog), TCP 964 (FTP)
- TCP 965 (virtual network computing [VNC])
- UDP 974 (Session Announcement Protocol [SAP])

Èpossibile che per queste porte aggiuntive non sia necessaria una definizione di priorità specifica.

Un modo comune per identificare il traffico è quello di creare mappe di classe che indirizzino il traffico di interesse. Ogni mappa delle classi può puntare a un elenco degli accessi destinato a qualsiasi traffico che utilizza le porte voce e video:

```
ip access-list extended JabberVOIP
permit udp any any range 16384 32767
ip access-list extended JabberSIGNALING
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended H323Videostream
permit udp any any eq 970
ip access-list extended H323Audiostream
permit udp any any eq 972
ip access-list extended H323VideoSignaling
permit udp any any eq 971
ip access-list extended H323AudioSignaling
permit udp any any eq 973
```

Èquindi possibile creare una mappa di classe per ogni tipo di traffico; ciascuna mappa delle classi rimanda all'elenco degli accessi pertinente:

```
class-map RTPaudio
match access-group name JabberVOIP
match access-group name H323Audiostream
class-map H323realtimevideo
match access-group name H323Videostream
class-map signaling
match access-group name JabberSIGNALING
match access-group name H323VideoSignaling
match access-group name H323AudioSignaling
```

Dopo aver identificato il traffico vocale e il traffico video tramite le mappe di classe, verificare che il traffico sia contrassegnato correttamente. Questa operazione può essere eseguita a livello di WLAN tramite tabelle-map o tramite mappe delle policy client.

Le mappe di tabella esaminano il contrassegno QoS del traffico in entrata e determinano quale deve essere il contrassegno QoS in uscita. Pertanto, le mappe a tabella sono utili quando il traffico in entrata ha già un contrassegno QoS. Le mappe tabella vengono utilizzate esclusivamente a livello SSID.

Al contrario, le policy map possono indirizzare il traffico identificato da class-map e sono più adatte al traffico potenzialmente senza tag di interesse. In questo esempio di configurazione si presume che il traffico proveniente dal lato cablato sia già stato contrassegnato correttamente prima di entrare nello switch Catalyst 3850 o nel Cisco 5760 WLC. In caso contrario, è possibile utilizzare una mappa dei criteri e applicarla a livello SSID come criterio client. Poiché il traffico proveniente dai client wireless potrebbe non essere stato contrassegnato, è necessario contrassegnare

correttamente il traffico voce e video:

- La voce in tempo reale deve essere contrassegnata con DSCP 46 (Expedited Forwarding [EF]).
- Il video deve essere contrassegnato con DSCP 34 (Assured Forwarding Class 41 [AF41]).
- I segnali vocali e video devono essere contrassegnati con DSCP 24 (Class Selector Service value 3 [CS3]).

Per applicare questi contrassegni, creare una mappa dei criteri che chiami ognuna di queste classi e che contrassegni il traffico equivalente:

```
policy-map taggingPolicy
 class RTPaudio
 set dscp ef

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

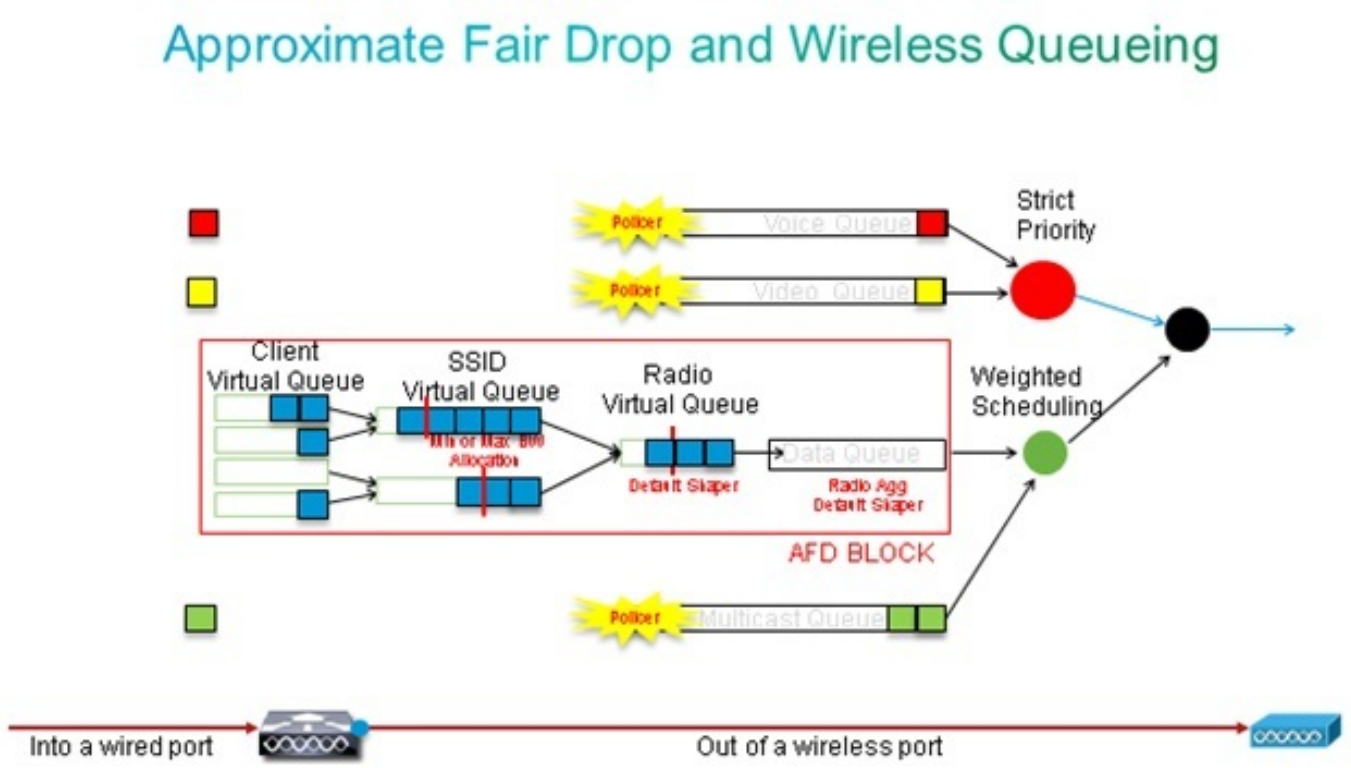
Passaggio 2: Gestione della larghezza di banda e delle priorità a livello di porta

Il passaggio successivo è quello di determinare un criterio QoS per le porte destinate e ricevute dagli access point. Questa procedura si applica principalmente agli switch Catalyst 3850. Se la configurazione viene eseguita su un controller Cisco 5760, questo passaggio non è obbligatorio. Le porte Catalyst 3850 trasportano il traffico voce e video diretto a o proveniente da client e access point wireless. La configurazione QoS in questo contesto soddisfa due requisiti:

1. **Allocazione della larghezza di banda**. È possibile decidere la larghezza di banda allocata per ogni tipo di traffico. Questa allocazione della larghezza di banda può essere effettuata anche a livello SSID. Impostare l'allocazione della larghezza di banda della porta per definire con maggiore precisione la larghezza di banda che può essere ricevuta da ciascun access point che serve il SSID di destinazione. Questa larghezza di banda deve essere impostata per tutti gli SSID sul punto di accesso di destinazione. L'esempio di configurazione semplificata presuppone la presenza di un solo SSID e di un punto di accesso, quindi l'allocazione della larghezza di banda della porta per voce e video è uguale all'allocazione globale della larghezza di banda per voce e video a livello SSID. A ogni tipo di traffico vengono allocati 6 Mbps e viene eseguito il policy in modo che la larghezza di banda allocata non venga superata.

2. **Assegnare priorità al traffico**. La porta ha quattro code. Le prime due code sono assegnate a una priorità e riservate al traffico in tempo reale - in genere voce e video, rispettivamente. La quarta coda è riservata al traffico multicast non in tempo reale e la terza coda contiene tutto il resto del traffico. Con la logica di accodamento degli accessi convergenti, il traffico di ogni client viene assegnato a una coda virtuale, in cui è possibile configurare QoS. Il risultato del criterio QoS del client viene inserito nella coda virtuale SSID, in cui è possibile configurare anche QoS. Poiché su una determinata radio AP possono esistere più SSID, il risultato di ogni SSID presente su una radio AP viene inserito nella coda virtuale della radio AP, in cui il traffico viene modellato in base alla capacità della radio. Il traffico può essere ritardato o interrotto in una di queste fasi utilizzando un meccanismo QoS chiamato Approximate Fair

Drop (AFD). Il risultato di questo criterio viene quindi inviato alla porta AP (detta porta wireless), dove viene data priorità alle prime due code (fino a una quantità configurabile di larghezza di banda), quindi alla terza e alla quarta coda come descritto in precedenza in questo paragrafo.



Questo esempio di configurazione inserisce la voce nella prima coda di priorità e il video nella seconda coda di priorità tramite il comando **priority level**. Al resto del traffico viene assegnata la restante larghezza di banda della porta.

Si noti che non è possibile utilizzare mappe classi per indirizzare il traffico in base agli elenchi di controllo di accesso (ACL, Access Control List). Le policy applicate a livello di porta possono indirizzare il traffico in base alle mappe di classe, ma queste mappe di classe devono indirizzare il traffico identificato dal relativo valore QoS. Dopo aver identificato il traffico in base agli ACL e averlo contrassegnato correttamente a livello di SSID del client, non è più necessario eseguire una seconda ispezione approfondita dello stesso traffico a livello di porta. Quando il traffico raggiunge la porta che raggiunge il punto di accesso, è già contrassegnato correttamente.

In questo esempio vengono riutilizzate le mappe di classe generali create per la policy SSID e vengono indirizzati direttamente il traffico RTP vocale e il traffico in tempo reale video:

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
match dscp cs3
```

Dopo aver identificato il traffico di interesse, è possibile decidere quale politica applicare. Il criterio predefinito, denominato porta_padre, viene applicato automaticamente a ciascuna porta quando viene rilevato un access point. Non modificare questa impostazione predefinita, impostata come:

```
policy-map parent_port
class class-default
```

```
shape average 1000000000
service-policy port_child_policy
```

Poiché il criterio parent_port predefinito chiama il criterio port_child_policy, un'opzione consiste nel modificare il criterio port_child_policy. Non è necessario modificarne il nome. Questo criterio figlio determina il traffico da inserire in ogni coda e la larghezza di banda da allocare. La prima coda ha la priorità più alta, la seconda ha la seconda priorità più alta e così via. Queste due code sono riservate al traffico in tempo reale. La quarta coda viene utilizzata per il traffico multicast non in tempo reale. La terza coda contiene tutto il resto del traffico.

Nell'esempio, si decide di allocare il traffico vocale alla prima coda e il traffico video alla seconda coda e di allocare la larghezza di banda a ciascuna coda e a tutto il resto del traffico:

```
Policy-map port_child_policy
Class allvoice
 Priority level 1
 police rate percent 10
 conform-action transmit
 exceed-action drop
class videoandsignaling
 priority level 2
 police rate percent 20
 conform-action transmit
 exceed-action drop
class non-client-nrt-class
 bandwidth remaining ratio 7
class class-default
 bandwidth remaining ratio 63
```

In questa informativa, l'istruzione di priorità associata alle classi "voce" e "segnalazione video" consente di assegnare il traffico alla coda di priorità desiderata. Si noti, tuttavia, che le istruzioni relative alla percentuale di frequenza della polizia si applicano solo al traffico multicast, non unicast.

Non è necessario applicare questo criterio a livello di porta perché viene applicato automaticamente non appena viene rilevato un access point.

Passaggio 3: Gestione della larghezza di banda e delle priorità a livello SSID

Il passo successivo è occuparsi della policy QoS a livello SSID. questo passaggio è valido sia per lo switch Catalyst 3850 che per il controller 5760. Questa configurazione presuppone che il traffico voce e video sia identificato tramite l'uso di mappe di classi e elenchi degli accessi e sia contrassegnato correttamente. Tuttavia, è possibile che parte del traffico in arrivo non interessato dall'elenco degli accessi non visualizzi il relativo contrassegno QoS. In tal caso, è possibile decidere se il traffico deve essere contrassegnato con un valore predefinito o se non deve essere contrassegnato. La stessa logica viene applicata al traffico già contrassegnato ma non indirizzato dalle mappe di classe. Utilizzare l'istruzione *copy predefinita* in una tabella-mappa per assicurarsi che il traffico non contrassegnato non venga contrassegnato e che il traffico contrassegnato mantenga il contrassegno e non il contrassegno.

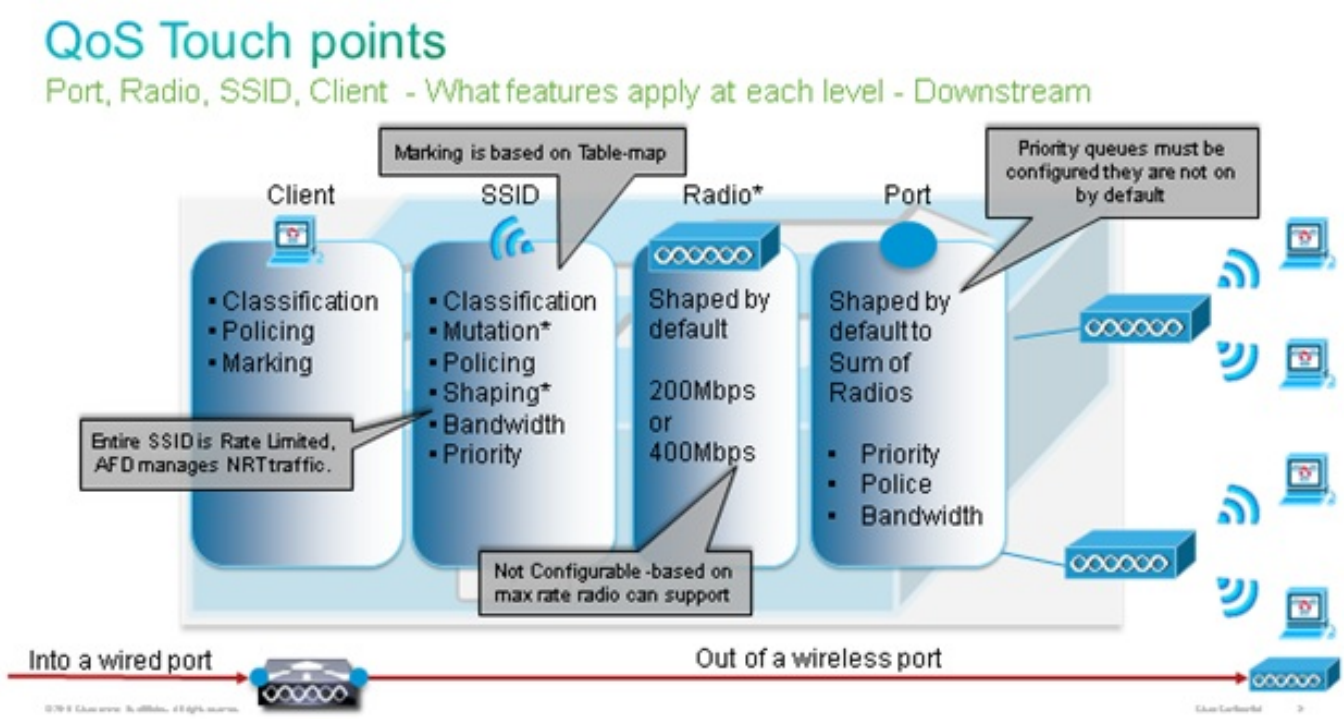
Le mappe tabella determinano il valore DSCP in uscita, ma vengono anche utilizzate per creare un frame 802.11 per stabilire il valore del frame UP.

Nell'esempio, il traffico in entrata che visualizza il livello QoS vocale (DSCP 46) mantiene il valore DSCP e il valore viene mappato sul contrassegno 802.11 equivalente (UP 6). Il traffico in entrata

che visualizza il livello QoS video (DSCP 34) mantiene il valore DSCP e il valore viene mappato sul contrassegno 802.11 equivalente (UP 5). Analogamente, il traffico contrassegnato con DSCP 24 può essere costituito da segnalazione vocale; il valore DSCP deve essere mantenuto e tradotto in 802.11 UP 3:

```
Table-map dscp2dscp
Default copy
Table-map dscp2up
Map from 46 to 6
Map from 24 to 3
Map from 34 to 5
Default copy
```

Il contrassegno può essere eseguito anche a livello di porta cablata in ingresso. Nella figura viene mostrato come agire QoS durante il passaggio del traffico da rete cablata a rete wireless:



Questo esempio di configurazione è incentrato sull'aspetto wireless della configurazione QoS e contrassegna il traffico a livello di client wireless. Una volta completata la parte relativa al contrassegno, è necessario allocare la larghezza di banda. qui, 6 Mbps di larghezza di banda vengono assegnati ai flussi di traffico voce. (Anche se questa è l'allocazione complessiva della larghezza di banda per la voce, ogni chiamata consumerebbe meno - ad esempio, 128 kbps). Questa larghezza di banda viene assegnata con il comando **Police** per riservare la larghezza di banda e per far cadere il traffico in eccesso.

Anche il traffico video viene allocato a 6 Mbps e controllato. In questo esempio di configurazione si presume che esista un solo flusso video.

Anche la parte del traffico voce e video che segnali deve essere assegnata alla larghezza di banda. Ci sono due possibili strategie.

- Utilizzare il comando **shape average** per memorizzare nel buffer e inviare successivamente il traffico in eccesso. Questa logica non è efficiente per il flusso voce o video in sé, in quanto tali

flussi richiedono un ritardo e un tremolio costanti; tuttavia, può essere efficiente nella segnalazione in quanto può essere leggermente ritardata senza influire sulla qualità delle chiamate. Nella soluzione di accesso convergente, i comandi shape non accettano le cosiddette "configurazioni bucket", che determinano la quantità di traffico in eccesso rispetto alla larghezza di banda allocata che può essere memorizzata nel buffer. È quindi necessario aggiungere un secondo comando, **queue-buffers ratio 0**, per specificare che le dimensioni del bucket sono pari a 0. Se si include la segnalazione nel resto del traffico e si utilizzano i comandi Shape, il traffico di segnalazione potrebbe essere interrotto in periodi di elevata congestione. Ciò potrebbe a sua volta causare l'interruzione della chiamata perché una delle due estremità determina che la comunicazione non viene più eseguita.

- Per evitare il rischio di chiamate ignorate, è possibile includere la segnalazione in una delle code prioritarie. In questo esempio di configurazione le code prioritarie erano definite come voce e video e ora viene aggiunta la segnalazione alla coda video.

Il criterio utilizza il controllo di ammissione di chiamata (CAC) per il flusso vocale. CAC è destinato al traffico wireless e corrisponde a un valore UP specifico (in questo esempio di configurazione, UP 6 e 7). CAC determina quindi la quantità massima di larghezza di banda che deve essere utilizzata da questo traffico. In una configurazione in cui il traffico vocale viene controllato, a CAC deve essere allocato un sottoinsieme della larghezza di banda complessiva allocata per il traffico vocale. Ad esempio, se la voce viene controllata a 6 Mbps, CAC non può superare 6 Mbps. CAC è configurato in una mappa dei criteri (denominata criterio figlio) integrata nella mappa dei criteri a valle principale (denominata criterio padre). La funzione CAC viene introdotta con il comando **admit cac wmm-tspec**, seguito dagli UP di destinazione e dalla larghezza di banda assegnata al traffico di destinazione.

Ogni chiamata non utilizza tutta la larghezza di banda allocata alla voce. Ad esempio, ogni chiamata può consumare 64 kbps in ogni direzione, il che equivale a 128 kbps di utilizzo effettivo della larghezza di banda bidirezionale. L'istruzione di velocità determina il consumo della larghezza di banda di ogni chiamata, mentre l'istruzione della polizia determina la larghezza di banda complessiva assegnata al traffico vocale. Se tutte le chiamate che si verificano all'interno della cella utilizzano una larghezza di banda vicina a quella massima consentita, qualsiasi nuova chiamata che venga avviata dalla cella e che determini il superamento della larghezza di banda massima consentita per la voce da parte della larghezza di banda utilizzata verrà negata. È possibile ottimizzare questo processo tramite la configurazione di CAC a livello di banda, come spiegato nel passo 4: Limitazione delle chiamate con CAC.

Èpertanto necessario configurare un criterio figlio che contenga le istruzioni CAC e sia integrato nel criterio downstream principale. CAC non configurato nella mappa dei criteri a monte. CAC si applica alle chiamate vocali avviate dalla cella, ma poiché è una risposta a tali chiamate, CAC viene impostato solo nella mappa dei criteri a valle. La mappa dei criteri a monte sarà diversa. Non è possibile usare le mappe di classe create in precedenza perché queste mappe di classe indirizzano il traffico basato su un ACL. Il traffico inserito nei criteri SSID è già stato sottoposto ai criteri client, quindi è consigliabile non eseguire un'ispezione approfondita dei pacchetti una seconda volta. Indirizzare invece il traffico con un contrassegno QoS risultante dai criteri client.

Se si decide di non lasciare la segnalazione nella classe predefinita, sarà inoltre necessario assegnare la priorità alla segnalazione.

In questo esempio, la segnalazione e il video sono nella stessa classe e a tale classe viene assegnata una larghezza di banda maggiore per supportare la parte di segnalazione; Al traffico video vengono assegnati 6 Mbps (un flusso point-to-point per una telecamera Tandberg) e 1 Mbps per la segnalazione di tutte le chiamate vocali e del flusso video:

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
Match dscp cs3
```

Criteri figlio a valle:

```
Policy-map SSIDout_child_policy
class allvoice
priority level 1
police 6000000
admit cac wmm-tspec
rate 128
wlan-up 6 7
class videoandsignaling
priority level 2
police 1000000
```

Criterio padre a valle:

```
policy-map SSIDout
class class-default
set dscp dscp table dscp2dscp
set wlan user-priority dscp table dscp2up
shape average 30000000
queue-buffers ratio 0
service-policy SSIDout_child_policy
```

Il traffico in upstream è il traffico proveniente da client wireless e inviato a WCM prima che venga inviato da una porta cablata o a un altro SSID. In entrambi i casi è possibile configurare mappe dei criteri che definiscono la larghezza di banda allocata a ogni tipo di traffico. I criteri variano probabilmente a seconda che il traffico venga inviato da una porta cablata o a un altro SSID.

Nella direzione a monte, la vostra preoccupazione principale è di decidere la priorità, non la larghezza di banda. In altre parole, la mappa dei criteri a monte non alloca larghezza di banda a ogni tipo di traffico. Poiché il traffico si trova già nell'access point e ha già attraversato il collo di bottiglia formato dallo spazio wireless half-duplex, l'obiettivo è portare il traffico alla funzione controller dello switch Catalyst 3850 o del Cisco 5760 WLC per un'ulteriore elaborazione. Quando il traffico viene raccolto a livello AP, è possibile decidere se considerare attendibile il contrassegno QoS potenziale esistente per assegnare la priorità ai flussi di traffico inviati al controller. In questo esempio, i valori DSCP esistenti possono essere considerati attendibili:

```
Policy-map SSIDin
Class class-default
set dscp dscp table dscp2dscp
```

Una volta create le policy, applicare le policy-map alla WLAN. Nell'esempio, si prevede che i dispositivi che si connettono alla WLAN supportino WMM, quindi è necessario WMM.

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
```

Passaggio 4: Limitazione delle chiamate con CAC

L'ultimo passaggio consiste nel personalizzare il CAC in base alla propria situazione specifica. Nella configurazione CAC spiegata al passo 3: Gestione della larghezza di banda e delle priorità a livello SSID, l'access point scarta qualsiasi pacchetto voce che superi la larghezza di banda allocata.

Per evitare la larghezza di banda massima, è inoltre necessario configurare WCM in modo da riconoscere le chiamate effettuate e quelle che causeranno il superamento della larghezza di banda. Alcuni telefoni supportano la specifica TSPEC (WMM Traffic Specification) e informano l'infrastruttura wireless della larghezza di banda che la chiamata prevista dovrebbe utilizzare. WCM può quindi rifiutare la chiamata prima che venga effettuata.

Alcuni telefoni SIP non supportano TSPEC, ma WCM e l'access point possono essere impostati in modo da riconoscere i pacchetti di avvio delle chiamate inviati alle porte SIP e possono utilizzare queste informazioni per stabilire che sta per essere effettuata una chiamata SIP. Poiché il telefono SIP non specifica la larghezza di banda che deve essere utilizzata dalla chiamata, l'amministratore deve determinare la larghezza di banda prevista, in base al codec, al tempo di campionamento e così via.

CAC calcola la larghezza di banda utilizzata a ogni livello AP. È possibile impostare CAC in modo che utilizzi solo l'utilizzo della larghezza di banda del client nei calcoli (CAC statico) o che consideri anche i punti di accesso e i dispositivi adiacenti sullo stesso canale (CAC basato sul carico). Cisco consiglia di utilizzare il CAC statico per i telefoni SIP e il CAC basato sul carico per i telefoni TSPEC.

Infine, il CAC viene attivato per singola banda.

Nell'esempio, i telefoni usano SIP anziché TSPEC per l'avvio della sessione, ciascuna chiamata usa 64 kbps per ciascuna direzione di flusso, la funzione CAC con carico viene disabilitata quando la funzione CAC statica è abilitata e il 75% della larghezza di banda massima di ciascun access point è allocato al traffico vocale:

```
ap dot11 5ghz shutdown
ap dot11 5ghz cac voice acm
no ap dot11 5ghz cac voice load-based
ap dot11 5ghz cac voice max-bandwidth 75
ap dot11 5ghz cac voice sip bandwidth 64
no ap dot11 5ghz shutdown
```

Èpossibile ripetere la stessa configurazione per la banda a 2,4 GHz:

```
ap dot11 24ghz shutdown
ap dot11 24ghz cac voice acm
no ap dot11 24ghz cac voice load-based
ap dot11 24ghz cac voice max-bandwidth 75
ap dot11 24ghz cac voice sip bandwidth 64
no ap dot11 24ghz shutdown
```

Una volta che il CAC è stato applicato per ciascuna banda, è necessario applicare il SIP CAC anche a livello di WLAN. Questo processo consente all'access point di esaminare le informazioni di layer 4 (L4) del traffico client wireless per identificare le query inviate all'UDP 5060 che indicano i tentativi di chiamata SIP. TSPEC funziona al livello 802.11 ed è rilevato in modo nativo dai punti di accesso. I telefoni SIP non usano il TSPEC, quindi l'AP deve eseguire un'ispezione più

approfondita dei pacchetti per identificare il traffico SIP. Poiché non si desidera che l'access point esegua questa ispezione su tutti gli SSID, è necessario determinare quali SSID prevedono traffico SIP. È quindi possibile attivare lo snooping delle chiamate su questi SSID per cercare le chiamate vocali. È inoltre possibile determinare l'azione da eseguire se una chiamata SIP deve essere rifiutata, ovvero annullare l'associazione del client SIP o inviare un messaggio SIP occupato.

In questo esempio, lo snooping delle chiamate è abilitato e, se la chiamata SIP deve essere rifiutata, viene inviato un messaggio di stato occupato. Con l'aggiunta della policy QoS dalla Fase 3: Gestione della larghezza di banda e delle priorità a livello di SSID, questa è la configurazione SSID per l'esempio di WLAN:

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
call-snoop
sip-cac send-486busy
```

Verifica

Per verificare che la configurazione QoS funzioni correttamente, utilizzare questi comandi.

> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).
>
> Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

show class-map

Con questo comando vengono visualizzate le mappe classi configurate sulla piattaforma:

```
3850#show class-map
 Class Map match-any H323realtimeaudio (id 6)
  Match access-group name H323Audiostream
Class Map match-any H323realtimevideo (id 7)
  Match access-group name H323Videostream
Class Map match-any allvideo (id 10)
  Match   dscp af41 (34)
Class Map match-any jabberaudiosignaling (id 11)
  Match access-group name JabberSIGNALING
Class Map match-any allvoice (id 12)
  Match   dscp ef (46)
Class Map match-any RTPaudio (id 19)
  Match access-group name JabberVOIP
  Match access-group name H323Audiostream
Class Map match-any class-default (id 0)
  Match any
Class Map match-any jabberRTPaudio (id 14)
```

```
  Match access-group name JabberVOIP
Class Map match-any non-client-nrt-class (id 1)
  Match non-client-nrt
Class Map match-any H323audiosignaling (id 17)
  Match access-group name H323AudioSignaling
Class Map match-any H323videosignaling (id 18)
  Match access-group name H323VideoSignaling
Class Map match-any signaling (id 20)
  Match access-group name JabberSIGNALING
  Match access-group name H323VideoSignaling
  Match access-group name H323AudioSignaling
```

show policy-map

Questo comando visualizza i mapping dei criteri configurati sulla piattaforma:

```
3850 #show policy-map
show policy-map
 Policy Map port_child_policy
   Class non-client-nrt-class
     bandwidth remaining ratio 7
   Class allvoice
     priority level 1
    police rate percent 10
      conform-action transmit
      exceed-action drop
   Class allvideo
     priority level 2
    police rate percent 20
      conform-action transmit
      exceed-action drop
   Class class-default
     bandwidth remaining ratio 63
 Policy Map SSIDin
   Class class-default
     set dscp dscp table dscp2dscp
 Policy Map SSIDout_child_policy
   Class allvoice
     priority level 1
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
     admit cac wmm-tspec
       rate 6000 (kbps)
       wlan-up 6
   Class allvideo
     priority level 2
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
     admit cac wmm-tspec
       rate 6000 (kbps)
       wlan-up 4 5
 Policy Map taggingPolicy
   Class RTPaudio
     set dscp ef
   Class H323realtimevideo
     set dscp af41
   Class signaling
     set dscp cs3
 Policy Map SSIDout
```

```
   Class class-default
     set dscp dscp table dscp2dscp
     set wlan user-priority dscp table dscp2up
     shape average 30000000 (bits/sec)
     queue-buffers ratio 0
     service-policy SSIDout_child_policy
 Policy Map parent_port
   Class class-default
     shape average 1000000000 (bits/sec) op
```

mostra wlan

Con questo comando vengono visualizzati la configurazione WLAN e i parametri dei criteri del servizio:

```
3850# show wlan name test1 | include Policy
AAA Policy Override                              : Disabled
QoS Service Policy - Input
 Policy Name                                    : SSIDin
 Policy State                                   : Validated
QoS Service Policy - Output
 Policy Name                                    : SSIDout
 Policy State                                   : Validated
QoS Client Service Policy
 Input  Policy Name                             : taggingPolicy
 Output Policy Name                             : taggingPolicy
Radio Policy                                     : All
```

show policy-map interface

Con questo comando viene visualizzata la mappa dei criteri installata per un'interfaccia specifica:

```
3850#show policy-map interface wireless ssid name test1

Remote SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00C2EB000000001F
 Service-policy input: SSIDin
   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

Remote SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00D0D08000000021

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E

 Service-policy input: SSIDin
```

```
    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp dscp table dscp2dscp

  Service-policy output: SSIDout

    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp dscp table dscp2dscp
        wlan user-priority dscp table dscp2up
      shape (average) cir 30000000, bc 120000, be 120000
      target shape rate 30000000
      queue-buffers ratio 0

      Service-policy : SSIDout_child_policy

        Class-map: allvoice (match-any)
          Match:  dscp ef (46)
            0 packets, 0 bytes
            30 second rate 0 bps
          Priority: Strict,

          Priority Level: 1
          police:
              cir 6000000 bps, bc 187500 bytes
            conformed 0 bytes; actions:
              transmit
            exceeded 0 bytes; actions:
              drop
            conformed 0000 bps, exceed 0000 bps
          cac wmm-tspec rate 6000 kbps

        Class-map: allvideo (match-any)
          Match:  dscp af41 (34)
            0 packets, 0 bytes
            30 second rate 0 bps
          Priority: Strict,

          Priority Level: 2
          police:
              cir 6000000 bps, bc 187500 bytes
            conformed 0 bytes; actions:
              transmit
            exceeded 0 bytes; actions:
              drop
            conformed 0000 bps, exceed 0000 bps
          cac wmm-tspec rate 6000 kbps

        Class-map: class-default (match-any)
          Match: any
            0 packets, 0 bytes
            30 second rate 0 bps

SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00DB568000000020

  Service-policy input: SSIDin

    Class-map: class-default (match-any)
```

```
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp dscp table dscp2dscp

 Service-policy output: SSIDout

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp
       wlan user-priority dscp table dscp2up
     shape (average) cir 30000000, bc 120000, be 120000
     target shape rate 30000000
     queue-buffers ratio 0

     Service-policy : SSIDout_child_policy

       Class-map: allvoice (match-any)
         Match:  dscp ef (46)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 1
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: allvideo (match-any)
         Match:  dscp af41 (34)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 2
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: class-default (match-any)
         Match: any
           0 packets, 0 bytes
           30 second rate 0 bps

3850#show policy-map interface wireless client
Client 8853.2EDC.68EC iifid:
0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E.0x00E0D04000000022

 Service-policy input: taggingPolicy
```

```
  Class-map: RTPaudio (match-any)
    Match: access-group name JabberVOIP
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323Audiostream
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp ef

  Class-map: H323realtimevideo (match-any)
    Match: access-group name H323Videostream
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp af41

  Class-map: signaling (match-any)
    Match: access-group name JabberSIGNALING
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323VideoSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323AudioSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp cs3
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps

Service-policy output: taggingPolicy

  Class-map: RTPaudio (match-any)
    Match: access-group name JabberVOIP
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323Audiostream
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp ef

  Class-map: H323realtimevideo (match-any)
    Match: access-group name H323Videostream
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp af41

  Class-map: signaling (match-any)
    Match: access-group name JabberSIGNALING
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323VideoSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323AudioSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
```

```
      dscp cs3
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
```

mostra criteri qos della piattaforma

Con questo comando vengono visualizzati i criteri QoS installati per porte, radio AP, SSID e client. Si noti che è possibile verificare, ma non modificare, i criteri radio:

```
3850#show platform qos policies PORT
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------- --------------
L:0 Gi1/0/20           0x01023f4000000033 OUT defportangn      INSTALLED IN HW
L:0 Gi1/0/20           0x01023f4000000033 OUT port_child_policyINSTALLED IN HW

3850#show platform qos policies RADIO
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------------------------
L:0 R56356842871193604 0x00c8384000000004 OUT def-11an         INSTALLED IN HW
L:0 R68373680329064451 0x00f2e98000000003 OUT def-11gn         INSTALLED IN HW
3850#show platform qos policies SSID
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------------------------
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout_child_policyINSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout_child_policyINSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout          INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout          INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b IN  SSIDin           INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 IN  SSIDin           INSTALLED IN HW

3850#show platform qos policies CLIENT
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------- --------------
L:0 8853.2edc.68ec     0x00e0d04000000022 IN  taggingPolicy    NOT INSTALLED IN HW
L:0 8853.2edc.68ec     0x00e0d04000000022 OUT taggingPolicy    NOT INSTALLED IN HW
```

show wireless client mac-address <mac> service-policy

Con questo comando vengono visualizzati i mapping dei criteri applicati a livello client:

```
3850#show wireless client mac-address 8853.2EDC.68EC service-policy output
Wireless Client QoS Service Policy
Policy Name  : taggingPolicy
Policy State : Installed
3850#sh wireless client mac-address 8853.2EDC.68EC service-policy in
3850#sh wireless client mac-address 8853.2EDC.68EC service-policy input
Wireless Client QoS Service Policy
Policy Name  : taggingPolicy
Policy State : Installed
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.