QoS op geconvergeerde toegangscontrollers en lichtgewicht APs Configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u QoS kunt configureren in een Cisco geconvergeerd toegangsnetwerk met lichtgewicht access points (LAP's) en met de Cisco Catalyst 3850 switch of de Cisco 5760 draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van hoe u LAP's en Cisco geconvergeerde toegangscontrollers kunt configureren
- Kennis van de manier om basisrouting en QoS in een bekabeld netwerk te configureren

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 3850 switch die Cisco IOS-software draait? XE-softwarerelease 3.2.2(SE)S
- Cisco 5760 draadloze LAN-controller voor Cisco IOS XE-softwarerelease 3.2.2(SE)
- Cisco 3600 Series lichtgewicht access points

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

Achtergrondinformatie

QoS verwijst naar de mogelijkheid van het netwerk om een reeks gebruikers of toepassingen beter of speciaal te onderhouden ten koste van andere gebruikers of toepassingen.

Met QoS kan de bandbreedte efficiënter worden beheerd via LAN's, waaronder draadloze LAN's (WLAN's) en WAN's. QoS biedt verbeterde en betrouwbare netwerkdiensten met deze services:

- Ondersteunt specifieke bandbreedte voor kritische gebruikers en toepassingen.
- Bestuurt de jitter en de latentie die bij real-time verkeer vereist zijn.
- Beheert en minimaliseert netwerkcongestie.
- Vormen netwerkverkeer om de stroom van verkeer te vlot te trekken.
- Hiermee worden prioriteiten voor netwerkverkeer ingesteld.

In het verleden werden WLAN's vooral gebruikt om weinig bandbreedte te verzenden, gegevenstoepassingsverkeer. Dankzij de uitbreiding van WLAN's naar verticale (zoals retail-, financiële en educatieve) omgevingen en ondernemingsomgevingen, worden WLAN's nu gebruikt om hoge bandbreedte-gegevenstoepassingen te transporteren in combinatie met tijdgevoelige, multimediatoepassingen. Deze vereiste leidde tot de noodzaak van draadloze QoS.

De IEEE 802.11e-werkgroep binnen het comité van de normen van IEEE 802.11 heeft de standaarddefinitie voltooid en de Wi-Fi Alliance heeft de Wi-Fi Multimedia (WMM)-certificering gecreëerd, maar de adoptie van de 802.11e-standaard is nog beperkt. De meeste apparaten zijn WMM-gecertificeerd, omdat WMM-certificering nodig is voor 802.11n- en 802.11ac-certificering. Veel draadloze apparaten wijzen geen verschillende QoS niveaus toe aan pakketten die naar de Data Link Layer worden verzonden, zodat die apparaten het grootste deel van hun verkeer zonder QoS-markering en geen relatieve prioriteit verzenden. Echter, de meeste 802.11 Voice over Wireless LAN (VoWLAN) IP-telefoons markeren en prioriteren hun spraakverkeer. Dit document concentreert zich op QoS-configuratie voor VoWLAN IP-telefoons en op video-enabled Wi-Fi-apparaten die hun spraakverkeer markeren.

Opmerking: QoS-configuratie voor apparaten die geen interne markering uitvoeren, valt niet binnen het bereik van dit document.

Het 802.11e-amendement definieert acht prioriteitsniveaus (UP), verdeeld op twee in vier QoS-niveaus (toegangscategorieën):

- Platinum/Voice (UP 7 en 6) - Zorgt voor een hoge kwaliteit van de service voor spraak via draadloze verbindingen.
- Goud/Video (UP 5 en 4) - Ondersteunt videotoepassingen van hoge kwaliteit.
- Silver/Best Performance (UP 3 en 0) - Ondersteunt normale bandbreedte voor klanten. Dit is de standaardinstelling.
- Bronze/achtergrond (UP 2 en 1) - levert de laagste bandbreedte voor gastenservices.

Platinum wordt gewoonlijk gebruikt voor VoIP-klanten en Gold voor videocassablanten. Dit document biedt een configuratievoorbeeld dat illustreert hoe u QoS op controllers kunt configureren en met een bekabeld netwerk kunt communiceren dat met QoS is geconfigureerd voor VoWLAN en videoclients.

Verbeteringen in L3 QoS-pakketmarkering

Cisco geconvergeerde access controllers ondersteunen Layer 3 (L3) IP Gedifferentieerde Services Code Point (DSCP)-markering van pakketten die door WLC's en LAP's worden verzonden. Deze optie verbetert de manier waarop access points (APs) deze L3 informatie gebruiken om ervoor te zorgen dat pakketten de juiste boven-de-lucht prioritering van AP aan de draadloze client ontvangen.

In een geconvergeerde access WLAN-architectuur die Catalyst 3850 switches als draadloze controllers gebruikt, verbinden APs zich rechtstreeks met de switch. In een geconvergeerde access WLAN-architectuur die 5760 controllers gebruikt, worden WLAN-gegevens via het AP en de WLC via het CAPWAP-protocol (Control and Provisioning of Wireless Access Point) geconverteerd. Om de oorspronkelijke QoS-classificatie over deze tunnel te behouden, moeten de QoS-instellingen van het ingekapselde gegevenspakket op de juiste manier in kaart worden gebracht aan Layer 2 (L2) (802.1p) en L3 (IP DSCP) velden van het buitentunnelpakket.

Wanneer u QoS voor VoWLAN en video vormt, kunt u een QoS-beleid dat specifiek is voor draadloze clients en een beleid dat specifiek is voor een WLAN, of beide. U kunt de instellingen ook aanvullen met een configuratie die specifiek is voor de poort die de AP verbindt, vooral met Catalyst 3850 switches. Dit configuratievoorbeeld concentreert zich op QoS configuratie voor de draadloze client, WLAN, en de poort naar de AP. De primaire doelstellingen van een QoS-configuratie voor VoWLAN en videotoepassingen zijn:

- Herkende stem- en videoverkeer (verkeersclassificatie en markering), zowel upstream als downstream.
- Spraak en videoverkeer met een prioriteitsniveau voor spraak markeren: 802.11e UP 6, 802.1p 5, DSCP 46 voor spraak.802.11e UP 5, DSCP 34 voor video.
- Wijs bandbreedte voor spraakverkeer, spraaksignalering en videoverkeer toe.

Draadloos netwerk voor QoS met MQC configureren

Voordat u QoS configureren moet u de WCM-functie (Wireless Controller module) van de Catalyst

3850 switch of Cisco 5760 WLC configureren voor basisbediening en de LAP's registreren bij de WCM. In dit document wordt ervan uitgegaan dat de WCM is ingesteld voor een eenvoudige bediening en dat de LAP's bij de WCM zijn geregistreerd.

De geconvergeerde toegangsoplossing gebruikt de modulaire QoS (MQC) opdrachtregel interface (CLI). Raadpleeg de QoS Configuration Guide, Cisco IOS XE release 3SE (Catalyst 3850 Switches) voor extra informatie over het gebruik van MQC in QoS-configuratie voor de Catalyst 3850 switch.

Configuratie van QoS met MQC op geconvergeerde toegangscontrollers is gebaseerd op vier elementen:

- **Class-maps** worden gebruikt om het verkeer van belangen te herkennen. Class-maps kunnen verschillende technieken gebruiken (zoals bestaande QoS-markering, toegangslijsten of VLAN's) om het verkeer van belangen te identificeren.
- **Beleidskaarten** worden gebruikt om te bepalen welke QoS-instellingen moeten worden toegepast op het verkeer van belangen. Beleids-kaarten roepen class-maps en passen verschillende QoS-instellingen (zoals specifieke markering, prioriteitsniveaus, bandbreedte-toewijzing, enzovoort) toe op elke klasse.
- **Servicebeleid** wordt gebruikt om beleidskaarten toe te passen op strategische punten van uw netwerk. In de geconvergeerde toegangsoplossing kan het service-beleid worden toegepast op gebruikers, Service Set Identifier (SSID's), AP radio's en poorten. Poorten, SSID en clientbeleid kunnen door de gebruiker worden ingesteld. Het radiobeleid wordt bepaald door de draadloze controlemodule. Draadloos QoS beleid voor poort, SSID, client en radio wordt in de stroomafwaartse richting toegepast wanneer het verkeer van de switch of controller naar draadloze klanten stroomt.
- **Tabelkaarten** worden gebruikt om de inkomende QoS-markering te onderzoeken en om te beslissen of er geen QoS-markering wordt gebruikt. Tabelkaarten worden geplaatst in beleidskaarten die op SSID's worden toegepast. Tabelkaarten kunnen worden gebruikt om de markering te bewaren (kopiëren) of te wijzigen. Tabelkaarten kunnen ook worden gebruikt om een mapping tussen bekabelde en draadloze markering te maken. Draadloze markering gebruikt DSCP (L3 QoS) of 802.1p (L2 QoS). Draadloze markering gebruikt User Priority (UP). Tabelkaarten worden meestal gebruikt om te bepalen welke DSCP-markering moet worden gebruikt voor elke UP van rente en welke UP moet worden gebruikt voor elke DSCP-waarde van rente. Tabelkaarten zijn van fundamenteel belang voor geconvergeerde toegang tot QoS, omdat er geen directe vertaling tussen DSCP- en UP-waarden is.

Maar DSCP naar UP tabelkaarten maken ook de *kopie*-instructie mogelijk. In dat geval gebruikt de geconvergeerde toegangsoplossing de Cisco Architecture for Voice, Video en Integrated Data (AVVID) mapping tabel om de DSCP naar UP of UP naar DSCP te bepalen:

Label Index	Sleutelveld	inkomende waarde	Buitenste DSCP	CoS	OMHOOG
0	N.B.	Niet afgevinkt	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	OMHOOG	0	0	0	0
74	OMHOOG	1	8	1	1
75	OMHOOG	2	16	1	2
76	OMHOOG	3	24	2	3
77	OMHOOG	4	34	3	4
78	OMHOOG	5	34	4	5
79	OMHOOG	6	46	5	6
80	OMHOOG	7	46	7	7

Standaard gehard beleid

Geconconvergeerde toegangscontrollers onderbreken hardcodeerde QoS-beleidsprofielen die op WLAN's kunnen worden toegepast. Deze profielen passen het metalen beleid (platina, goud, enz.) toe dat aan beheerders van Cisco Unified Wireless Networks (CUWN)-controllers bekend is. Als uw doel geen beleid is te creëren dat specifieke bandbreedte aan stemverkeer toevoegt maar gewoonweg om te verzekeren dat spraakverkeer de juiste QoS markering ontvangt, kunt u het gecodeerde beleid gebruiken. Het gecodeerde beleid kan op de WLAN worden toegepast en kan in de upstream en de downstream-richtingen anders zijn.

> **Opmerkingen:**
>
> Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.
>
> De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

platina

Het harde beleid voor stem heet platinum. De naam kan niet worden gewijzigd.

Dit is het stroomafwaarts beleid voor het niveau van het platina 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
```

Dit is het upstreambeleid voor het Platinum QoS-niveau:

```
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
```

goud

Het gecodeerde beleid voor video wordt goud genoemd. De naam kan niet worden gewijzigd.

Dit is het downstreambeleid voor het niveau van de kwantitatieve versoepeling voor goud:

```
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
```

Dit is het stroomopwaarts beleid voor het kwantitatieve versoepeling voor goud:

```
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
```

Zilver

Het gecodeerde beleid voor de beste inspanning wordt zilver genoemd. De naam kan niet worden gewijzigd.

Dit is het downstreambeleid voor het niveau van de zilveren QoS:

```
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
```

Dit is het stroomopwaarts beleid voor het zilveren QoS-niveau:

```
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
```

Bronze

Het harde beleid voor achtergrondverkeer wordt bronzen genoemd. De naam kan niet worden gewijzigd.

Dit is het downstreambeleid voor het niveau van de bronzen QoS:

```
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
```

Dit is het stroomopwaarts beleid voor het niveau van de bronzen QoS:

```
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
```

Zodra u hebt besloten welke tabel-kaart het beste bij het doelverkeer voor een bepaalde SSID aansluit, kunt u het overeenkomende beleid op uw WLAN toepassen. In dit voorbeeld wordt één beleid toegepast in de stroomafwaartse richting (output, van het AP naar de draadloze client), en één beleid wordt toegepast in de stroomopwaartse richting (input, van de draadloze client via het AP naar de 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#
```

Controleer de WLAN-configuratie om te controleren welk beleid op uw WLAN is toegepast:

```
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
```

Handmatig configureren

Het gecodeerde beleid is standaard QoS-markering maar past geen bandbreedte-toewijzing toe. Het gecodeerde beleid veronderstelt ook dat uw verkeer reeds gemerkt is. In een complex milieu, kunt u een combinatie van beleid willen gebruiken om stem en videoverkeer correct te herkennen en te markeren, om bandbreedte toewijzing in de stroomafwaartse en stroomopwaartse richting in te stellen, en om vraag toelatingscontrole te gebruiken om het aantal oproepen te beperken die van de draadloze cel worden geïnitieerd.

> **Opmerking:** Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Stap 1: Identificatie en markering van spraakverkeer

De eerste stap is het herkennen van spraak- en videoverkeer. Spraakverkeer kan in twee categorieën worden ingedeeld:

- Spraakstroom, die het audiogedeelte van de communicatie transporteert.
- Spraaksignalering, waarmee statistische informatie wordt uitgewisseld tussen spraakendpoints.

De spraakstroom gebruikt gewoonlijk Real-time Transport Protocol (RTP) en User Datagram Protocol (UDP)-doelpoorten tussen 16384 en 32767. Dit is het bereik; de werkelijke havens zijn doorgaans kleiner en afhankelijk van de uitvoering .

Er zijn verschillende stemsignaleringsprotocollen. Dit configuratievoorbeeld gebruikt Jabber. Jabber gebruikt deze TCP-poorten voor verbinding en directory:

- TCP 880 (HTTP)
- 143 (Internet Message Access Protocol [IMAP])
- 443 (HTTPS)
- 993 (IMAP) voor services zoals Cisco Unified MeetingPlace of Cisco Webex voor vergaderingen en Cisco Unity of Cisco Unity Connection voor voicemail-functies
- TCP 389/636 (Lichtgewicht Directory Access Protocol [LDAP] server voor contactzoekingen)
- FTP (1080)
- TFTP (UDP 69) voor bestandsoverdracht (zoals configuratiebestanden) van peers of van server

Deze diensten hebben misschien geen specifieke prioriteit nodig.

Jabber gebruikt het Session Initiation Protocol (SIP) (UDP/TCP 5060 en 5061) voor spraaksignalering.

Het videoverkeer gebruikt verschillende poorten en protocollen die afhankelijk zijn van uw implementatie. Dit configuratievoorbeeld gebruikt een Tandberg PrecisionHD 720p camera voor videoconferenties. De Tandberg PrecisionHD 720p-camera kan meerdere codecs gebruiken; de verbruikte bandbreedte is afhankelijk van de gekozen codec:

- C20, C40 en C60 codecs gebruiken H.323/SIP en kunnen tot 6 Mbps gebruiken in point-to-point verbindingen.

- De C90-codec gebruikt deze zelfde protocollen en kan tot 10 Mbps gebruiken in multi-site communicatie.

De implementatie van Tandberg van H.323 gebruikt gewoonlijk UDP 970 voor streaming video, UDP 971 voor video signalering, UDP 972 voor streaming audio en UDP 973 voor audio signalering. De camera's van Tandberg gebruiken ook andere havens, zoals:

- UDP 161
- UDP 962 (Simple Network Management Protocol [SNMP])
- TCP 963 (netlog), TCP 964 (FTP)
- TCP 965 (virtuele netwerkcomputing [VNC])
- UDP 974 (Session notice Protocol [SAP])

Deze extra havens hebben misschien geen specifieke prioriteit nodig.

Een gezamenlijke manier om verkeer te identificeren is class-maps te maken die het verkeer van belangen richten. Elke class-map kan naar een toegangslijst wijzen die op elk verkeer gericht is dat de stem en de videopoorten gebruikt:

```
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
```

U kunt dan één class-map maken voor elk type verkeer; elke class-map punten naar de desbetreffende toegangslijst:

```
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
```

Zodra het spraakverkeer en het videoverkeer via klassenkaarten zijn geïdentificeerd, moet u ervoor zorgen dat het verkeer goed wordt gemarkeerd. Dit kan op WLAN-niveau worden gedaan via de tabelkaarten en kan ook worden gedaan via clientbeleidskaarten.

In tabelkaarten wordt de QoS-markering van het inkomende verkeer onderzocht en wordt bepaald wat de uitgaande QoS-markering moet zijn. Tabelkaarten zijn dus nuttig wanneer inkomend verkeer al QoS-markering heeft. Tabelkaarten worden uitsluitend op SSID-niveau gebruikt.

Beleidskaarten kunnen daarentegen gericht zijn op verkeer dat door klassekaarten wordt geïdentificeerd en zijn beter aangepast aan potentieel niet-getemperde belangenverstrengeling. Dit configuratievoorbeeld veronderstelt dat het verkeer van de bekabelde kant reeds goed is

gemarkeerd voordat het de Catalyst 3850 switch of Cisco 5760 WLC ingaat. Als dit niet het geval is, kunt u een beleidskaart gebruiken en het op het niveau van SSID toepassen als een clientbeleid. Omdat het verkeer van draadloze clients mogelijk niet is gemarkeerd, moet u ook spraak- en videoverkeer correct markeren:

- Realtime spraak moet worden gemarkeerd met DSCP 46 (versnelde doorsturen [EF]).
- Video moet worden gemarkeerd met DSCP 34 (Gegarandeerd doorsturen klasse 41 [AF41]).
- Signalering voor spraak en video moet worden gemarkeerd met DSCP 24 (Class Selector Service value 3 [CS3]).

Om deze markeringen toe te passen, creëren een beleid-kaart die elk van deze klassen roept en die het equivalente verkeer markeert:

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

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

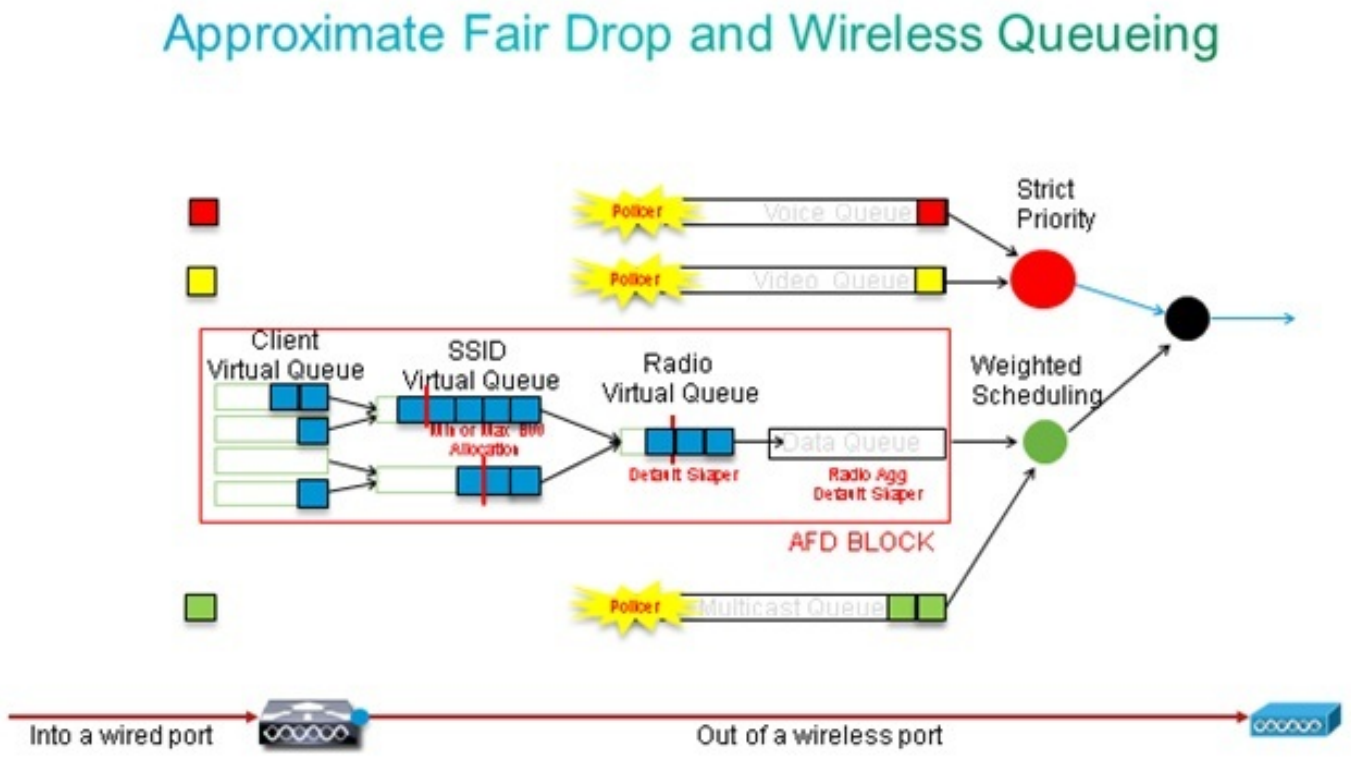
Stap 2: Bandbreedte- en prioriteitsbeheer op poortniveau

De volgende stap is het bepalen van een QoS-beleid voor havens die naar AP's komen. Deze stap is voornamelijk van toepassing op Catalyst 3850-switches. Als uw configuratie is uitgevoerd op een Cisco 5760-controller, is deze stap niet verplicht. Catalyst 3850-poorten dragen spraak- en videoverkeer dat naar of van draadloze klanten en APs gaat. De QoS-configuratie in deze context voldoet aan twee vereisten:

1. **Wijs bandbreedte toe**. U kunt besluiten hoeveel bandbreedte voor elk type verkeer wordt toegewezen. Deze bandbreedtetoewijzing kan ook op het niveau van SSID worden uitgevoerd. Stel de toewijzing van de havenbandbreedte in om te verfijnen hoeveel bandbreedte door elke AP kan worden ontvangen die het doel SSID dient. Deze bandbreedte moet voor alle SSID’s op de doelAP worden ingesteld. Dit vereenvoudigde configuratievoorbeeld veronderstelt dat er slechts één SSID en één AP zijn, zodat de toewijzing van de poortbandbreedte voor stem en video hetzelfde is als de globale bandbreedte toewijzing voor spraak en video op het niveau van SSID. Elk verkeerstype wordt toegewezen 6 Mbps en wordt gecontroleerd zodat deze toegewezen bandbreedte niet wordt overschreden.

2. **Prioriseer het verkeer**. De haven heeft vier rijen. De eerste twee wachtrijen worden geprioriteerd en gereserveerd voor realtime verkeer - normaal gesproken spraak en video, respectievelijk. De vierde rij is gereserveerd voor niet-realtime multicast verkeer en de derde rij bevat al het andere verkeer. Met geconvergeerde toegangs wachtrijen logica wordt het verkeer voor elke client toegewezen aan een virtuele wachtrij, waar QoS kan worden geconfigureerd. Het resultaat van het QoS-beleid van de cliënt wordt in de virtuele wachtrij van SSID geïnjecteerd, waar QoS ook kan worden geconfigureerd. Aangezien meerdere SSID’s op een bepaalde AP-radio kunnen bestaan, wordt het resultaat van elke SSID die op een AP-radio aanwezig is in de virtuele wachtrij van AP-radio geïnjecteerd, waar het verkeer

op basis van de radiocapaciteit wordt gevormd. Het verkeer kan in een van deze fasen worden uitgesteld of laten vallen door gebruik te maken van een QoS-mechanisme dat Approximate Fair Drop (AFD) wordt genoemd. Het resultaat van dit beleid wordt dan verzonden naar de AP poort (genaamd de draadloze poort), waar prioriteit wordt gegeven aan de eerste twee wachtrijen (tot een configureerbare hoeveelheid bandbreedte), en dan naar de derde en vierde wachtrijen zoals eerder in deze paragraaf beschreven.



Dit configuratievoorbeeld plaatst stem in de eerste prioriteitsrij en video in de tweede prioriteitsrij door gebruik van de opdracht **prioriteitsniveau**. De rest van het verkeer wordt toegewezen de rest van de havenbandbreedte.

Merk op dat u geen class-maps kunt gebruiken die verkeer richten op basis van toegangscontrolelijsten (ACL's). Beleid dat op het niveau van de haven wordt toegepast kan op verkeer zijn gebaseerd op klassenkaarten, maar deze klassenkaarten moeten zich richten op het verkeer dat door zijn QoS-waarde wordt geïdentificeerd. Zodra u op ACL's gebaseerd verkeer hebt geïdentificeerd en dit verkeer correct op het niveau van client SSID heeft gemerkt, zou het overtollig zijn om een tweede diepe inspectie van dat zelfde verkeer op het havenniveau uit te voeren. Wanneer het verkeer de poort bereikt die naar de AP gaat, wordt het reeds correct gemarkeerd.

In dit voorbeeld hergebruikt u de algemene class-maps die voor het SSID-beleid worden gemaakt en richt direct het verkeer van de stem RTP en het video in real time verkeer aan:

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

Zodra u het verkeer van belangen hebt geïdentificeerd, kunt u beslissen welk beleid van toepassing is. Het standaard beleid (parent_port genoemd) wordt automatisch toegepast op elke poort wanneer een AP wordt gedetecteerd. U dient deze standaard niet te wijzigen, deze is

ingesteld op:

```
policy-map parent_port
class class-default
shape average 1000000000
service-policy port_child_policy
```

Omdat het standaard parent_port beleid port_child_policy aanroept, is één optie de port_child_policy te bewerken. (U dient de naam niet te wijzigen). Dit kindbeleid bepaalt wat het verkeer in elke rij zou moeten gaan en hoeveel bandbreedte zou moeten worden toegewezen. De eerste rij heeft de hoogste prioriteit, de tweede rij heeft de op één na hoogste prioriteit, enzovoort. Deze twee rijen zijn gereserveerd voor real-time verkeer. De vierde rij wordt gebruikt voor niet-realtime multicast verkeer. De derde rij bevat al het andere verkeer.

In dit voorbeeld, besluit u om stemverkeer aan de eerste rij en videoverkeer aan de tweede rij toe te wijzen en bandbreedte aan elke rij en aan al ander verkeer toe te wijzen:

```
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 dit beleid staat de prioritaire verklaring die gekoppeld is aan de 'stem' en de 'video en signalering'-klassen u toe dat verkeer te koppelen aan de relevante prioriteitswachtrij. Merk op dat de cijfers van de politie alleen van toepassing zijn op multicast, niet op unicast, verkeer.

U hoeft dit beleid niet op havenniveau toe te passen, omdat het automatisch wordt toegepast zodra een AP wordt gedetecteerd.

Stap 3: Bandbreedte- en prioriteitsbeheer op SSID-niveau

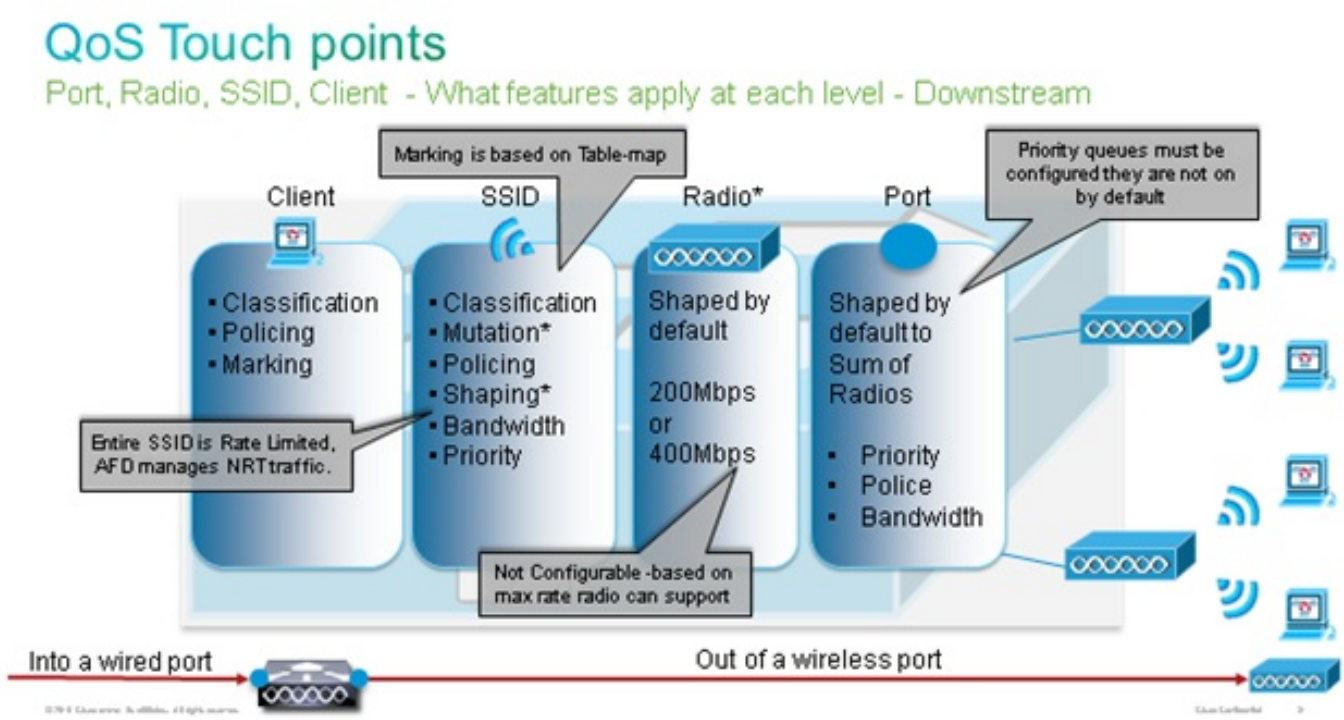
De volgende stap is het zorgen voor het QoS-beleid op het niveau van SSID. Deze stap is van toepassing op zowel Catalyst 3850-switch als de 5760-controller. Deze configuratie veronderstelt dat spraak- en videoverkeer door het gebruik van class-map en toegangslijsten wordt geïdentificeerd en correct getagd. Sommige inkomende verkeer die niet het doelwit is van de toegangslijst, tonen echter mogelijk geen QoS-markering. In dat geval kunt u beslissen of dit verkeer moet worden gemarkeerd met een standaardwaarde of zonder tag. Dezelfde logica geldt voor verkeer dat al gemarkeerd is maar niet op de klassenkaarten is gericht. Gebruik het *standaard kopiëren* statement in een tabel-map om er zeker van te zijn dat niet-gemarkeerd verkeer niet gemarkeerd is en dat het gelabelde verkeer de tag behoudt en niet opnieuw gemarkeerd wordt.

Tabel-kaarten beslissen de uitgaande DSCP-waarde maar worden ook gebruikt om een kader van 802.11 te maken om de frame-UP-waarde te bepalen.

In dit voorbeeld handhaaft het inkomende verkeer dat het niveau van spraak QoS (DSCP 46) toont zijn DSCP waarde, en de waarde wordt in kaart gebracht aan de equivalente 802.11 markering (UP 6). Inkomend verkeer dat het niveau van de QoS-video weergeeft (DSCP 34) handhaaft zijn DSCP-waarde, en de waarde wordt in kaart gebracht aan de equivalente 802.11-markering (UP 5). Op dezelfde manier kan met een verkeersmerk gemarkeerde DSCP 24 spraaksignalering zijn; de DSCP-waarde moet worden gehandhaafd en worden vertaald in het UP 802.11:

```
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
```

Markeren kon ook worden uitgevoerd op het inkomende kabelniveau. Dit getal laat zien wat QoS acties kunnen worden ondernomen als verkeer overschakelt van draadloos:



Dit configuratievoorbeeld concentreert zich op het draadloze aspect van QoS configuratie en tekent verkeer op draadloos clientniveau. Nadat het markeringsgedeelte is voltooid, moet u bandbreedte toewijzen; Hier, 6 Mbps van bandbreedte wordt toegewezen aan spraakverkeer. (Terwijl dit de algemene bandbreedte toewijzing voor spraak is, zou elke vraag minder verbruiken - bijvoorbeeld, 128 kbps.) Deze bandbreedte wordt toegewezen aan de **politie** opdracht om de bandbreedte te reserveren en meer verkeer te laten vallen.

Het videoverkeer wordt ook toegewezen 6 Mbps en gecontroleerd. Dit configuratievoorbeeld veronderstelt dat er slechts één videostroom is.

Het signalerende deel van het video en stemverkeer moet ook bandbreedte worden toegewezen. Er zijn twee mogelijke strategieën.

- Gebruik de opdracht **vorm gemiddelde**, waardoor meer verkeer gebufferd en later verzonden kan worden. Deze logica is niet efficiënt voor de spraak- of videostroom zelf, omdat die stromen een consistente vertraging en jitter vereisen; het kan echter efficiënt zijn voor signalering omdat signalering iets kan worden uitgesteld zonder effect op de oproepkwaliteit . In de geconvergeerde toegangsoplossing, aanvaarden vormopdrachten niet wat "emmers configuraties" wordt genoemd, die bepalen hoeveel verkeer meer dan de toegewezen bandbreedte kan worden gebufferd. Daarom moet een tweede opdracht, **wachtrij-buffers ratio 0**, worden toegevoegd om aan te geven dat de emmer grootte 0 is. Als u signalering in de rest van het verkeer en het gebruik van vormopdrachten omvat, kan het signaleringsverkeer vallen in tijden van grote congestie. Dit kan op zijn beurt de vraag laten vallen omdat elk eind bepaalt dat de communicatie niet meer plaatsvindt.
- Om het risico van gedaald vraag te vermijden, kunt u signalering in één van de prioriteitsrijen omvatten. Dit configuratievoorbeeld definieerde eerder de prioriteitswachtrijen als spraak en video en voegt nu signalering toe aan de videowachtrij.

Het beleid gebruikt de Call Admission Control (CAC) voor de spraakstroom. CAC richt draadloos verkeer en past een specifieke UP aan (in dit configuratievoorbeeld, UP 6 en 7). CAC bepaalt vervolgens de maximale hoeveelheid bandbreedte die dit verkeer moet gebruiken. In een configuratie waar u het spraakverkeer van de politie controleert, zou CAC een subset moeten worden toegewezen van de totale hoeveelheid bandbreedte die voor spraak is toegewezen. Bijvoorbeeld, als een stem aan 6 Mbps wordt gecontroleerd, kan CAC niet meer dan 6 Mbps bedragen. CAC is geconfigureerd in een beleidskaart (een kinderbeleid genoemd) die geïntegreerd is in de voornaamste beleidskaart stroomafwaarts (de zogenoemde 'moederpolitiek'). CAC wordt geïntroduceerd met de **opdracht Wmm-tspec** toegeven, gevolgd door de doel-UPs en de bandbreedte toegewezen aan het gerichte verkeer.

Elke vraag verbruikt niet alle bandbreedte die aan stem wordt toegewezen. Bijvoorbeeld, elke vraag kan 64 kbps elke manier consumeren, wat in 128 kbps van effectief bi-directionele bandbreedte-verbruik resulteert. De tarief instructie bepaalt elke vraag bandbreedte consumptie, terwijl het politieverklaring de algemene bandbreedte bepaalt die aan stemverkeer wordt toegewezen. Als alle oproepen die binnen het celgebruik plaatsvinden dichtbij de maximum toegestane bandbreedte, zal elke nieuwe vraag die vanuit de cel wordt geïnitieerd en die de verbruikte bandbreedte veroorzaakt om de maximum toegestane bandbreedte voor spraak te overschrijden, worden ontkend. U kunt dit proces verfijnen door de configuratie van CAC op het bandniveau in te stellen, zoals uitgelegd in Stap 4: Gespreksbeperking bij CAC.

Daarom moet je een kinderbeleid vormen dat de CAC-instructies bevat en dat geïntegreerd is in het hoofdbeleid stroomafwaarts. CAC is niet ingesteld in de upstream beleidsmap. CAC is wel van toepassing op spraakoproepen die vanuit de cel worden geïnitieerd, maar omdat het een reactie is op die oproepen, wordt CAC alleen in de downstreambeleidskaart gezet. De upstream beleidskaart zal anders zijn. U kunt de class-maps niet gebruiken die eerder gemaakt zijn omdat deze class-maps op basis van een ACL richten. Verkeer ingespoten in het SSID beleid ging reeds door het cliëntenbeleid, zodat u geen diepe inspectie op de pakketten een tweede keer zou moeten uitvoeren. In plaats daarvan richt u het verkeer aan met een QoS-markering die het resultaat is van het klantenbeleid.

Als u wilt voorkomen dat signalering in de standaardinstelling achterblijft, dient u ook prioriteit te geven aan signalering.

In dit voorbeeld zijn signalering en video in dezelfde klasse en wordt meer bandbreedte aan die klasse toegewezen om het signaleringsgedeelte te kunnen gebruiken; 6 Mbps worden toegewezen voor videoverkeer (één Tandberg camera point-to-point flow), en 1 Mbps wordt

toegewezen aan signalering voor alle spraakoproepen en de videostroom:

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

Het navenant kinderbeleid is:

```
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
```

Het ouderbeleid volgt:

```
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
```

Het stroomopwaarts verkeer is verkeer dat van draadloze klanten komt en naar de WCM wordt verzonden vóór het verkeer uit een bekabelde poort wordt verstuurd of naar een andere SSID wordt verzonden. In beide gevallen, kunt u beleid-kaarten configureren die de bandbreedte bepalen die aan elk type verkeer wordt toegewezen. Het beleid zal waarschijnlijk verschillen afhankelijk van de vraag of het verkeer vanuit een bekabelde poort of naar een andere SSID wordt verstuurd.

In de stroomopwaartse richting is uw belangrijkste zorg om de prioriteit te beslissen, niet de bandbreedte. Met andere woorden, uw upstream beleidskaart wijst geen bandbreedte toe aan elk type verkeer. Omdat het verkeer al bij het AP is en de flessenhals al door de half-tweezijdige draadloze ruimte is gekruist, is uw doel dit verkeer naar de controlemodule van de Catalyst 3850 switch of Cisco 5760 WLC voor verdere verwerking te brengen. Wanneer het verkeer op AP niveau wordt verzameld, kunt u besluiten of u potentiële bestaande QoS markering zou moeten vertrouwen om voorrang te geven aan verkeersstromen die naar de controller worden verzonden. In dit voorbeeld kunnen bestaande DSCP-waarden worden vertrouwd:

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

Wanneer uw beleid eenmaal is gecreëerd, pas de beleidskaarten op WLAN toe. In dit voorbeeld wordt van elk apparaat dat verbinding maakt met de WLAN-ondersteuning verwacht, zodat WM-ondersteuning nodig is.

```
wlan test1
```

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

Stap 4: Gespreksbeperking met CAC

De laatste stap is het CAC op uw specifieke situatie af te stemmen. In de CAC-configuratie wordt in Stap 3 uitgelegd: Bandbreedte en Prioriteitsbeheer op SSID Niveau, daalt AP elk stempakket dat de toegewezen bandbreedte overschrijdt.

Om het maximum van de bandbreedte te vermijden, moet u ook de WCM configureren om oproepen te herkennen die worden geplaatst en oproepen die de bandbreedte zullen veroorzaken om te worden overschreden. Sommige telefoons ondersteunen WMM Traffic Specification (TSPEC) en informeren de draadloze infrastructuur van de bandbreedte dat de geprojecteerde vraag naar verwachting zal consumeren. De WCM kan dan de oproep weigeren voordat deze wordt geplaatst.

Sommige SIP-telefoons ondersteunen TSPEC niet, maar WCM en AP kunnen worden ingesteld om callinitiatiepakketten die naar SIP-poorten worden verzonden te herkennen en kunnen deze informatie gebruiken om aan te tonen dat een SIP-oproep op het punt staat te worden geplaatst. Omdat de SIP-telefoon niet de bandbreedte specificeert die door de oproep moet worden geconsumeerd, moet de beheerder de verwachte bandbreedte bepalen, gebaseerd op de codec, de bemonsteringstijd, enzovoort.

CAC berekent de verbruikte bandbreedte op elk AP niveau. CAC kan worden ingesteld om alleen het bandbreedteverbruik van de client te gebruiken in zijn berekeningen (statische CAC) of om ook aangrenzende AP's en apparaten op hetzelfde kanaal te overwegen (op belasting gebaseerde CAC). Cisco raadt u aan om statische CAC voor SIP-telefoons en op lading gebaseerde CAC voor TSPEC-telefoons te gebruiken.

Ten slotte zij erop gewezen dat CAC per band wordt geactiveerd.

In dit voorbeeld, gebruiken telefoons SIP in plaats van TSPEC voor hun sessieinitiatie, gebruikt elke vraag 64 kbps voor elke stroomrichting, is op lading gebaseerde CAC uitgeschakeld wanneer statische CAC wordt ingeschakeld en wordt 75% van elke AP bandbreedte max toegewezen aan spraakverkeer:

```
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
```

U kunt dezelfde configuratie herhalen voor de 2,4 GHz-band:

```
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
```

Wanneer CAC voor elke band is toegepast, moet u ook SIP CAC op WLAN-niveau toepassen. Dit

proces stelt AP in staat om Layer 4 (L4) informatie van het draadloze clientverkeer te onderzoeken om vragen te identificeren die naar UDP 5060 worden verzonden die op SIP-callpogingen wijzen. TSPEC is actief op het niveau 802.11 en wordt door AP's niet herkend. SIP-telefoons gebruiken geen TSPEC, dus moet AP een diepere pakketinspectie uitvoeren om SIP-verkeer te identificeren. Omdat u niet wilt dat AP deze inspectie op alle SSIDs uitvoert, moet u bepalen welke SSIDs het SIP verkeer verwacht. U kunt dan verbinding op die SSID's inschakelen om naar spraakoproepen te zoeken. U kunt ook bepalen welke actie u moet uitvoeren als een SIP-oproep moet worden afgewezen - de SIP-client wordt losgekoppeld of een SIP druk bericht wordt verzonden.

In dit voorbeeld wordt Call snooping ingeschakeld en wordt een druk bericht verstuurd als de SIP-oproep moet worden afgewezen. Met toevoeging van het QoS-beleid uit stap 3: Bandbreedte en Prioriteitsbeheer op niveau van SSID, is dit de configuratie van SSID voor het voorbeeld WLAN:

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

Verifiëren

Gebruik deze opdrachten om te bevestigen dat de QoS-configuratie correct werkt.

> **Opmerkingen:**
>
> Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.
>
> De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

toespitsen op tekaart

Deze opdracht geeft de class-maps weer die op het platform zijn ingesteld:

```
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
```

politieke kaart weergeven

Deze opdracht geeft de beleidskaarten weer die op het platform zijn ingesteld:

```
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
```

tonen wlan

Deze opdracht geeft de WLAN-configuratie en -serviceparameters weer:

```
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
```

Beleids- en kaartinterface tonen

Deze opdracht toont de beleidskaart die voor een specifieke interface is geïnstalleerd:

```
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
```

quotiepe van het platform weergeven

Deze opdracht geeft het QoS-beleid weer dat voor poorten, AP-radio's, SSID's en clients is geïnstalleerd. Merk op dat u het radiobeleid kunt controleren maar niet kunt wijzigen:

```
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
```

Wi-Fi-mailadres van draadloze client voor <mac>-service-beleid tonen

Deze opdracht geeft de beleidskaarten weer die op clientniveau zijn toegepast:

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.