Konfigurationsbeispiel für QoS auf konvergenten Access Controllern und Lightweight APs

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie QoS in einem konvergenten Cisco Zugangsnetzwerk mit Lightweight Access Points (LAPs) und mit dem Cisco Catalyst 3850 Switch oder dem Cisco 5760 Wireless LAN Controller (WLC) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der Konfiguration von LAPs und Cisco Converged Access Controllern
- Grundlegendes Routing und QoS in einem kabelgebundenen Netzwerk konfigurieren

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst Switch 3850 mit Cisco IOS? XE Softwareversion 3.2.2(SE)
- Cisco 5760 Wireless LAN Controller mit Cisco IOS XE Software Release 3.2.2(SE)
- Cisco Lightweight Access Points der Serie 3600

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

QoS bezieht sich auf die Fähigkeit des Netzwerks, einen Satz von Benutzern oder Anwendungen bessere oder spezielle Dienste zum Nachteil anderer Benutzer oder Anwendungen bereitzustellen.

Mit QoS kann die Bandbreite effizienter über LANs hinweg verwaltet werden, wozu auch WLANs und WANs gehören. QoS bietet erweiterte und zuverlässige Netzwerkservices mit folgenden Services:

- Unterstützt dedizierte Bandbreite für kritische Benutzer und Anwendungen.
- Steuert den Jitter und die Latenz, die für Echtzeitdatenverkehr erforderlich sind.
- Verwaltung und Minimierung von Netzwerküberlastungen
- Verteilt Netzwerkverkehr, um den Datenverkehrsfluss zu vereinfachen.
- Legt Netzwerkverkehrsprioritäten fest.

In der Vergangenheit wurden WLANs hauptsächlich für die Übertragung von Datenverkehr mit niedriger Bandbreite und Datenanwendungen verwendet. Durch die Erweiterung von WLANs in vertikale (z. B. Einzelhandel, Finanzwesen und Bildung) und Unternehmensumgebungen werden WLANs nun für die Übertragung von Datenanwendungen mit hoher Bandbreite in Verbindung mit zeitkritischen Multimedia-Anwendungen eingesetzt. Diese Anforderung führte zur Notwendigkeit von Wireless-QoS.

Die IEEE 802.11e-Arbeitsgruppe im IEEE 802.11-Normenausschuss hat die Standarddefinition abgeschlossen, und die Wi-Fi Alliance hat die Wi-Fi Multimedia-Zertifizierung (WMM) erstellt, aber die Einführung des 802.11e-Standards ist noch begrenzt. Die meisten Geräte sind WMM-zertifiziert, da die WMM-Zertifizierung für die 802.11n- und 802.11ac-Zertifizierung erforderlich ist. Viele Wireless-Geräte weisen den an die Datenverbindungs-Layer gesendeten Paketen keine unterschiedlichen QoS-Ebenen zu, sodass diese Geräte den Großteil des Datenverkehrs ohne QoS-Markierung und relative Priorisierung senden. Die meisten 802.11-IP-Telefone mit Voice-

over-Wireless LAN (VoWLAN) markieren und priorisieren jedoch ihren Sprachdatenverkehr. Dieses Dokument konzentriert sich auf die QoS-Konfiguration für VoWLAN IP-Telefone und videofähige Wi-Fi-Geräte, die deren Sprachdatenverkehr markieren.

> **Hinweis**: QoS-Konfiguration für Geräte, die keine interne Kennzeichnung durchführen, wird in diesem Dokument nicht behandelt.

Der 802.11e-Zusatz definiert acht Benutzerprioritätsstufen (User Priority Level, UP), die zwei bis zwei in vier QoS-Ebenen (Zugriffskategorien) gruppiert werden:

- Platinum/Voice (UP 7 und 6) - Gewährleistet eine hohe Quality of Service für Voice over Wireless.
- Gold/Video (UP 5 und UP 4) - Unterstützt hochwertige Videoanwendungen.
- Silver/Best Effort (UP 3 und 0) - Unterstützt die normale Bandbreite für Clients. Dies ist die Standardeinstellung.
- Bronze/Background (UP 2 und UP 1) - Bietet die niedrigste Bandbreite für Gastservices.

Platinum wird häufig für VoIP-Clients und Gold für Video-Clients verwendet. Dieses Dokument enthält ein Konfigurationsbeispiel, das veranschaulicht, wie QoS auf Controllern konfiguriert und mit einem kabelgebundenen Netzwerk kommuniziert wird, das mit QoS für VoWLAN- und Video-Clients konfiguriert ist.

Verbesserungen bei der L3-QoS-Paketkennzeichnung

Cisco Converged Access Controller unterstützen die Layer 3 (L3) IP Differentiated Services Code Point (DSCP)-Markierung von Paketen, die von WLCs und LAPs gesendet werden. Diese Funktion verbessert die Verwendung dieser L3-Informationen durch Access Points (APs), um sicherzustellen, dass Pakete die richtige Over-the-Air-Priorisierung vom Access Point zum Wireless-Client erhalten.

In einer WLAN-Architektur mit konvergentem Zugriff, die Catalyst 3850-Switches als Wireless Controller verwendet, sind die APs direkt mit dem Switch verbunden. In einer WLAN-Architektur mit konvergentem Zugriff, die 5760-Controller verwendet, werden die WLAN-Daten über das CAPWAP-Protokoll (Control and Provisioning of Wireless Access Points) zwischen dem WAP und dem WLC getunnelt. Um die ursprüngliche QoS-Klassifizierung in diesem Tunnel aufrechtzuerhalten, müssen die QoS-Einstellungen des gekapselten Datenpakets den Feldern Layer 2 (L2) (802.1p) und L3 (IP DSCP) des äußeren Tunnelpakets angemessen zugeordnet werden.

Wenn Sie QoS für VoWLAN und Video konfigurieren, können Sie eine QoS-Richtlinie speziell für Wireless-Clients und eine Richtlinie speziell für ein WLAN oder beide konfigurieren. Sie können die Konfiguration auch durch eine Konfiguration ergänzen, die speziell auf den Port abgestimmt ist, der den Access Point verbindet, insbesondere mit Catalyst 3850-Switches. Dieses Konfigurationsbeispiel konzentriert sich auf die QoS-Konfiguration für den Wireless-Client, das WLAN und den Port zum WAP. Die Hauptziele einer QoS-Konfiguration für VoWLAN- und Videoanwendungen sind:

- Erkennung von Sprach- und Videodatenverkehr (Klassifizierung und Markierung des Datenverkehrs), sowohl Upstream- als auch Downstream-Datenverkehr
- Zeichnen Sie den Sprach- und Videodatenverkehr mit einer Prioritätsebene für Sprache:

802.11e UP 6, 802.1p 5, DSCP 46 für Sprache.802.11e UP 5, DSCP 34 für Video.
- Zuweisung von Bandbreite für Sprachdatenverkehr, Sprachsignalisierung und Videodatenverkehr

Konfigurieren des Wireless-Netzwerks für QoS mit MQC

Bevor Sie QoS konfigurieren, müssen Sie die WCM-Funktion (Wireless Controller Module) des Catalyst 3850-Switches oder des Cisco 5760-WLC für den Basisbetrieb konfigurieren und die LAPs beim WCM registrieren. In diesem Dokument wird davon ausgegangen, dass der WCM für den Basisbetrieb konfiguriert ist und dass die LAPs beim WCM registriert sind.

Die Lösung für den konvergenten Zugriff verwendet die Kommandozeile (CLI) der Modular QoS (MQC). Weitere Informationen zur Verwendung von MQC in der QoS-Konfiguration auf dem Catalyst 3850-Switch finden Sie im QoS-Konfigurationshandbuch von Cisco IOS XE Release 3SE (Catalyst 3850-Switches).

Die Konfiguration von QoS mit MQC auf konvergenten Access Controllern beruht auf vier Elementen:

- **Klassenzuordnungen** werden zur Erkennung von interessantem Datenverkehr verwendet. Für Klassenzuordnungen können verschiedene Techniken (z. B. vorhandene QoS-Markierungen, Zugriffslisten oder VLANs) verwendet werden, um den Datenverkehr von Interesse zu identifizieren.
- Anhand von **Richtlinienzuordnungen** wird festgelegt, welche QoS-Einstellungen auf den relevanten Datenverkehr angewendet werden sollen. Richtlinienzuweisungen weisen Klassenzuordnungen auf und wenden verschiedene QoS-Einstellungen (z. B. spezifische Markierungen, Prioritätsstufen, Bandbreitenzuweisung usw.) auf jede Klasse an.
- **Service-Richtlinien** werden verwendet, um Richtlinienzuordnungen auf strategische Punkte im Netzwerk anzuwenden. In der konvergenten Zugriffslösung können Service-Richtlinien auf Benutzer, Service Set Identifiers (SSIDs), AP-Funkmodule und Ports angewendet werden. Port-, SSID- und Client-Richtlinien können vom Benutzer konfiguriert werden. Funkrichtlinien werden vom Wireless-Steuerungsmodul gesteuert. Wireless QoS-Richtlinien für Port, SSID, Client und Funkmodul werden in Downstream-Richtung angewendet, wenn der Datenverkehr vom Switch oder Controller an Wireless-Clients fließt.
- **Table-Maps** werden verwendet, um eingehende QoS-Markierungen zu untersuchen und ausgehende QoS-Markierungen zu bestimmen. Tabellenzuordnungen werden in auf SSIDs angewendeten Richtlinienzuordnungen positioniert. Mithilfe von Tabellen können Sie die Kennzeichnung behalten (kopieren) oder ändern. Außerdem können Sie mithilfe von Table-Maps eine Zuordnung zwischen kabelgebundenen und Wireless-Markierungen erstellen. Für die kabelgebundene Markierung wird DSCP (L3 QoS) oder 802.1p (L2 QoS) verwendet. Die Wireless-Markierung verwendet die Benutzerpriorität (UP). In der Regel werden mithilfe von Tabellenmaps bestimmt, welche DSCP-Markierungen für die einzelnen UPs des Interesses verwendet werden sollen und welche UP für jeden DSCP-Wert verwendet werden sollte. Tabellenzuordnungen sind für die QoS für den konvergenten Zugriff von grundlegender Bedeutung, da keine direkte Übersetzung zwischen DSCP- und UP-Werten erfolgt.

Die *Kopieranleitung* kann jedoch auch von DSCP zu UP-Tabellenzuordnungen *verwendet* werden. In diesem Fall verwendet die konvergente Zugriffslösung die Cisco Architecture for Voice, Video, and Integrated Data (AVVID)-Zuordnungstabelle, um die DSCP-To-UP- oder UP-to-DSCP-Übersetzung zu bestimmen:

Label-Index	Schlüsselfeld	Eingehender Wert	Äußeres DSCP	CoS	UP
0	Anmerkung:	Nicht aktiviert	0	0	0
1 bis 10	DSCP	0 bis 7	0 bis 7	0	0
11 bis 18	DSCP	8 bis 15	8 bis 15	1	2
19-26	DSCP	16-23	16-23	2	1
27-34	DSCP	24-31	24-31	1	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	1
68	CoS	1	24	1	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	UP	0	0	0	0
74	UP	1	8	1	1
75	UP	2	16	1	2
76	UP	1	24	2	1
77	UP	4	34	1	4
58	UP	5	34	4	5
79	UP	6	46	5	6
80	UP	7	46	7	7

Standardmäßige hartcodierte Richtlinien

Converged Access Controller übernehmen hardcodierte QoS-Richtlinienprofile, die auf WLANs angewendet werden können. Diese Profile wenden die Metal-Richtlinien (Platin, Gold usw.) an, die Administratoren von Cisco Unified Wireless Networks (CUWN)-Controllern bekannt sind. Wenn Sie nicht Richtlinien erstellen möchten, die dem Sprachverkehr eine bestimmte Bandbreite zuweisen, sondern lediglich sicherstellen, dass der Sprachverkehr die korrekte QoS-Markierung erhält, können Sie die hardcodierten Richtlinien verwenden. Die hardcodierten Richtlinien können auf das WLAN angewendet werden und können in der Upstream- und Downstream-Richtung unterschiedlich sein.

> **Hinweise**:
>
> Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.
>
> Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Platinum

Die hardcodierte Richtlinie für Sprache heißt Platin. Der Name kann nicht geändert werden.

Dies ist die Downstream-Richtlinie für die Platin-QoS-Ebene:

```
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
```

Dies ist die Upstream-Richtlinie für die Platinum-QoS-Ebene:

```
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
```

Gold

Die hardcodierte Videorichtlinie wird als Gold bezeichnet. Der Name kann nicht geändert werden.

Dies ist die Downstream-Richtlinie für die Gold-QoS-Ebene:

```
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
```

Dies ist die Upstream-Richtlinie für die Gold-QoS-Ebene:

```
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
```

Silber

Die hardcodierte Richtlinie für bestmögliche Leistung heißt Silver. Der Name kann nicht geändert werden.

Dies ist die Downstream-Richtlinie für die Silver-QoS-Ebene:

```
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
```

Dies ist die Upstream-Richtlinie für die Silver-QoS-Ebene:

```
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

Die hardcodierte Richtlinie für Hintergrunddatenverkehr wird als Bronze bezeichnet. Der Name kann nicht geändert werden.

Dies ist die Downstream-Richtlinie für die Bronze-QoS-Ebene:

```
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
```

Dies ist die Upstream-Richtlinie für die Bronze-QoS-Ebene:

```
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
```

Sobald Sie entschieden haben, welche Tabellenübersicht am besten zum Zieldatenverkehr für eine bestimmte SSID passt, können Sie die entsprechende Richtlinie auf Ihr WLAN anwenden. In diesem Beispiel wird eine Richtlinie in Downstream-Richtung (Ausgabe vom Access Point zum Wireless-Client) und eine Richtlinie in Upstream-Richtung (Eingabe vom Wireless-Client über den Access Point zum Controller) angewendet:

```
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#
```

Überprüfen Sie die WLAN-Konfiguration, um zu überprüfen, welche Richtlinie auf Ihr WLAN angewendet wurde:

```
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
```

Manuelle Konfiguration

Die hardcodierten Richtlinien wenden die Standard-QoS-Markierung an, wenden aber keine Bandbreitenzuweisung an. Die hardcodierten Richtlinien setzen auch voraus, dass Ihr Datenverkehr bereits markiert ist. In einer komplexen Umgebung können Sie eine Kombination von Richtlinien verwenden, um Sprach- und Videodatenverkehr angemessen zu erkennen und zu markieren, die Bandbreitenzuweisung in die Downstream- und Upstream-Richtung festzulegen und die Anrufzugangskontrolle zu verwenden, um die Anzahl der Anrufe zu begrenzen, die von der Wireless-Zelle aus initiiert werden.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Schritt 1: Identifikation und Markierung von Sprachdatenverkehr

Der erste Schritt besteht in der Erkennung von Sprach- und Videodatenverkehr. Sprachdatenverkehr kann in zwei Kategorien eingeteilt werden:

- Sprachdatenfluss, der den Audioteil der Kommunikation überträgt.
- Sprachsignalisierung, die statistische Informationen enthält, die zwischen Sprachendpunkten ausgetauscht werden.

Der Sprachfluss verwendet in der Regel RTP- (Real-Time Transport Protocol) und UDP-Zielports (User Datagram Protocol) im Bereich von 16384 bis 32767. Dies ist der Bereich. Die tatsächlichen Ports sind in der Regel enger und hängen von der Implementierung ab.

Es gibt mehrere Sprachsignalisierungsprotokolle. In diesem Konfigurationsbeispiel wird Jabber verwendet. Jabber verwendet diese TCP-Ports für Verbindungen und Verzeichnis:

- TCP 80 (HTTP)
- 143 (Internet Message Access Protocol [IMAP])
- 443 (HTTPS)
- 993 (IMAP) für Services wie Cisco Unified MeetingPlace oder Cisco WebEx für Meetings und Cisco Unity oder Cisco Unity Connection für Voicemail-Funktionen
- TCP 389/636 (LDAP-Server [Lightweight Directory Access Protocol] für Kontaktsuche)

- FTP (1080)
- TFTP (UDP 69) für die Dateiübertragung (z. B. Konfigurationsdateien) von Peers oder vom Server

Für diese Services ist u. U. keine spezifische Priorisierung erforderlich.

Jabber verwendet das Session Initiation Protocol (SIP) (UDP/TCP 5060 und 5061) für die Sprachsignalisierung.

Videodatenverkehr verwendet verschiedene Ports und Protokolle, die von der Implementierung abhängig sind. In diesem Konfigurationsbeispiel wird eine Tandberg PrecisionHD 720p-Kamera für Videokonferenzen verwendet. Die Tandberg PrecisionHD-Kamera 720p kann mehrere Codecs verwenden. Die verbrauchte Bandbreite hängt vom gewählten Codec ab:

- Die Codecs C20, C40 und C60 verwenden H.323/SIP und können Point-to-Point-Verbindungen mit bis zu 6 Mbit/s nutzen.
- Der C90-Codec verwendet dieselben Protokolle und kann bis zu 10 Mbit/s in standortübergreifenden Kommunikationen verbrauchen.

Bei der Implementierung von H.323 in Tandberg wird normalerweise UDP 970 für Video-Streaming, UDP 971 für Videosignalisierung, UDP 972 für Audio-Streaming und UDP 973 für Audiosignalisierung verwendet. Tandberg-Kameras verwenden auch andere Ports, z. B.:

- 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])

Diese zusätzlichen Ports benötigen möglicherweise keine spezifische Priorisierung.

Eine gängige Methode zur Identifizierung von Datenverkehr besteht in der Erstellung von Klassenzuordnungen, die auf den relevanten Datenverkehr abzielen. Jede Klassenzuordnung kann auf eine Zugriffsliste verweisen, die auf jeden Datenverkehr abzielt, der die Sprach- und Videoports verwendet:

```
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
```

Anschließend können Sie für jeden Datenverkehrstyp eine Klassenzuordnung erstellen. jede Klassenzuordnung verweist auf die relevante Zugriffsliste:

```
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
```

Nachdem Sprachdatenverkehr und Videodatenverkehr über Klassenzuordnungen identifiziert wurden, stellen Sie sicher, dass der Datenverkehr korrekt gekennzeichnet ist. Dies kann über die Tabellen-Maps auf der WLAN-Ebene erfolgen und auch über Client-Richtlinienzuordnungen erfolgen.

In den Tabellen-Maps wird die QoS-Markierung für eingehenden Datenverkehr überprüft und die ausgehende QoS-Markierung bestimmt. Tabellenzuordnungen sind daher nützlich, wenn eingehender Datenverkehr bereits über eine QoS-Markierung verfügt. Tabellenkarten werden ausschließlich auf SSID-Ebene verwendet.

Im Gegensatz dazu können Richtlinienzuordnungen Datenverkehr gezielt einbeziehen, der durch Klassenzuordnungen identifiziert wurde, und sind besser an potenziell nicht gekennzeichneten Datenverkehr angepasst. In diesem Konfigurationsbeispiel wird davon ausgegangen, dass Datenverkehr von der kabelgebundenen Seite bereits korrekt markiert wurde, bevor er in den Catalyst 3850-Switch oder den Cisco 5760 WLC eintritt. Ist dies nicht der Fall, können Sie eine Richtlinienzuweisung verwenden und auf der SSID-Ebene als Client-Richtlinie anwenden. Da der Datenverkehr von Wireless-Clients möglicherweise nicht markiert wurde, müssen Sie den Sprach- und Videodatenverkehr korrekt markieren:

- Sprache in Echtzeit sollte mit DSCP 46 (Expedited Forwarding [EF]) markiert sein.
- Video sollte als DSCP 34 (Assured Forwarding Class 41 [AF41]) markiert sein.
- Die Signalisierung für Sprache und Video muss mit DSCP 24 (Class Selector Service Value 3 [CS3]) markiert sein.

Erstellen Sie zum Anwenden dieser Markierungen eine Richtlinienzuordnung, die jede dieser Klassen aufruft und den entsprechenden Datenverkehr markiert:

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

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

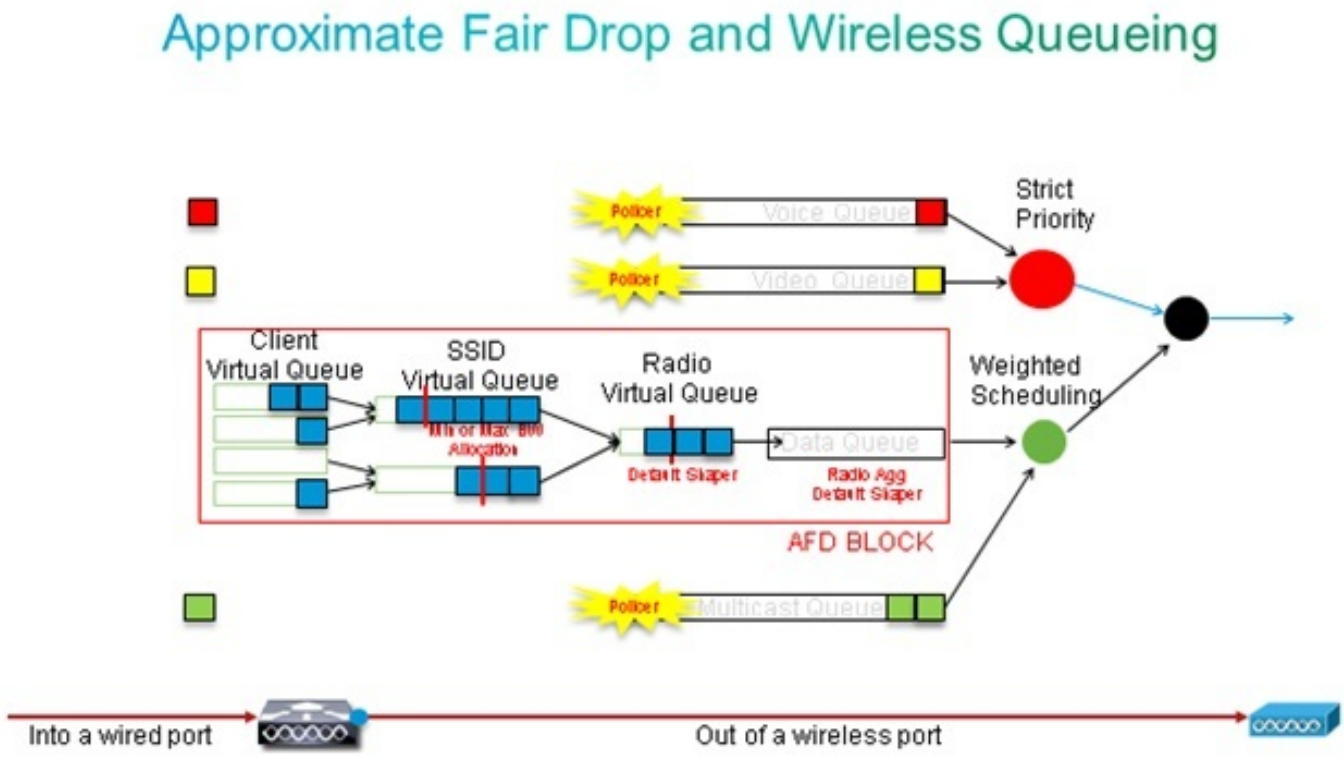
Schritt 2: Bandbreiten- und Prioritäts-Management auf Port-Ebene

Im nächsten Schritt wird eine QoS-Richtlinie für Ports festgelegt, die zu APs gehen. Dieser Schritt gilt hauptsächlich für Catalyst 3850-Switches. Wenn Ihre Konfiguration auf einem Cisco 5760 Controller vorgenommen wird, ist dieser Schritt nicht obligatorisch. Catalyst 3850-Ports übertragen Sprach- und Videodatenverkehr, der von Wireless-Clients und APs an Wireless-Clients gesendet wird oder von diesen stammt. Die QoS-Konfiguration in diesem Kontext erfüllt zwei Anforderungen:

1. Weisen Sie Bandbreite zu. Sie können festlegen, wie viel Bandbreite für die einzelnen Datenverkehrstypen zugewiesen wird. Diese Bandbreitenzuweisung kann auch auf der

SSID-Ebene erfolgen. Legen Sie die Port-Bandbreitenzuweisung fest, um festzulegen, wie viel Bandbreite von jedem AP empfangen werden kann, der die Ziel-SSID bedient. Diese Bandbreite muss für alle SSIDs auf dem Ziel-AP festgelegt werden. In diesem vereinfachten Konfigurationsbeispiel wird davon ausgegangen, dass es nur eine SSID und einen Access Point gibt. Daher entspricht die Port-Bandbreitenzuweisung für Sprache und Video der globalen Bandbreitenzuweisung für Sprache und Video auf SSID-Ebene. Jeder Datenverkehrstyp wird 6 Mbit/s zugewiesen und so geregelt, dass die zugewiesene Bandbreite nicht überschritten wird.

2. **Priorisierung des Datenverkehrs**. Der Port verfügt über vier Warteschlangen. Die ersten beiden Warteschlangen werden priorisiert und für Echtzeitdatenverkehr reserviert - in der Regel für Sprache und Video. Die vierte Warteschlange ist für Multicast-Datenverkehr in Echtzeit reserviert, die dritte Warteschlange enthält den gesamten anderen Datenverkehr. Bei einer konvergenten Zugriffswarteschlangenlogik wird der Datenverkehr für jeden Client einer virtuellen Warteschlange zugewiesen, in der QoS konfiguriert werden kann. Das Ergebnis der Client-QoS-Richtlinie wird in die virtuelle SSID-Warteschlange eingespeist, in der auch QoS konfiguriert werden kann. Da mehrere SSIDs auf einer bestimmten AP-Funkeinheit vorhanden sein können, wird das Ergebnis jeder SSID, die auf einer AP-Funkeinheit vorhanden ist, in die virtuelle AP-Funkwarteschlange eingespeist, in der der Datenverkehr basierend auf der Funkkapazität geformt wird. Der Datenverkehr kann in jeder dieser Phasen durch einen QoS-Mechanismus verzögert oder fallen gelassen werden, der als ungefährer Fair Drop (AFD) bezeichnet wird. Das Ergebnis dieser Richtlinie wird dann an den AP-Port (der so genannte Wireless-Port) gesendet, wo den ersten beiden Warteschlangen (bis zu einer konfigurierbaren Bandbreite) Priorität eingeräumt wird, und dann an die dritte und vierte Warteschlange, wie oben in diesem Absatz beschrieben.



In diesem Konfigurationsbeispiel werden Sprache mithilfe des Befehls **Prioritätsstufe** in die Warteschlange mit der ersten Priorität und Video in die zweite Prioritätswarteschlange gestellt. Der restliche Datenverkehr wird der restlichen Port-Bandbreite zugewiesen.

Beachten Sie, dass Sie keine Klassenzuordnungen für Datenverkehr verwenden können, die auf Zugriffskontrolllisten (ACLs) basieren. Richtlinien, die auf Portebene angewendet werden, können Datenverkehr auf der Grundlage von Klassenzuordnungen anvisieren. Diese Klassenzuordnungen sollten jedoch auf Datenverkehr abzielen, der durch seinen QoS-Wert identifiziert wird. Wenn Sie Datenverkehr anhand von ACLs identifiziert und diesen Datenverkehr auf der Client-SSID-Ebene korrekt markiert haben, ist es redundant, diesen Datenverkehr auf Port-Ebene einer zweiten eingehenden Überprüfung zu unterziehen. Wenn der Datenverkehr den Port erreicht, der zum AP führt, wird er bereits korrekt markiert.

In diesem Beispiel verwenden Sie die allgemeinen Klassenzuordnungen, die für die SSID-Richtlinie erstellt wurden, und richten direkt auf den Sprach-RTP- und Video-Echtzeit-Datenverkehr aus:

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

Sobald Sie den Datenverkehr identifiziert haben, können Sie entscheiden, welche Richtlinie angewendet werden soll. Die Standardrichtlinie (übergeordneter Port genannt) wird automatisch auf jeden Port angewendet, wenn ein AP erkannt wird. Sie sollten diesen Standardwert nicht ändern, der wie folgt festgelegt ist:

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

Da die default parent_port-Richtlinie die port_child_policy aufruft, besteht eine Option darin, die port_child_policy zu bearbeiten. (Sie sollten den Namen nicht ändern.) Diese untergeordnete Richtlinie legt fest, welcher Datenverkehr in den einzelnen Warteschlangen übertragen und wie viel Bandbreite zugewiesen werden soll. Die erste Warteschlange hat die höchste Priorität, die zweite Warteschlange die zweithöchste Priorität usw. Diese beiden Warteschlangen sind für Echtzeitdatenverkehr reserviert. Die vierte Warteschlange wird für Multicast-Datenverkehr verwendet, der nicht in Echtzeit stattfindet. Die dritte Warteschlange enthält den gesamten anderen Datenverkehr.

In diesem Beispiel entscheiden Sie, den Sprachverkehr der ersten Warteschlange und den Videodatenverkehr der zweiten Warteschlange zuzuweisen und den einzelnen Warteschlangen und dem gesamten anderen Datenverkehr Bandbreite zuzuweisen:

```
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 dieser Richtlinie können Sie mit der Prioritätsanweisung für die Sprach- und die Videosignalisierungsklassen diesen Datenverkehr der entsprechenden Prioritätswarteschlange zuweisen. Beachten Sie jedoch, dass die Prozentangaben der Polizeibeamten nur für Multicast- und nicht für Unicast-Verkehr gelten.

Sie müssen diese Richtlinie nicht auf Portebene anwenden, da sie automatisch angewendet wird, sobald ein Access Point erkannt wird.

Schritt 3: Bandbreiten- und Prioritäts-Management auf SSID-Ebene

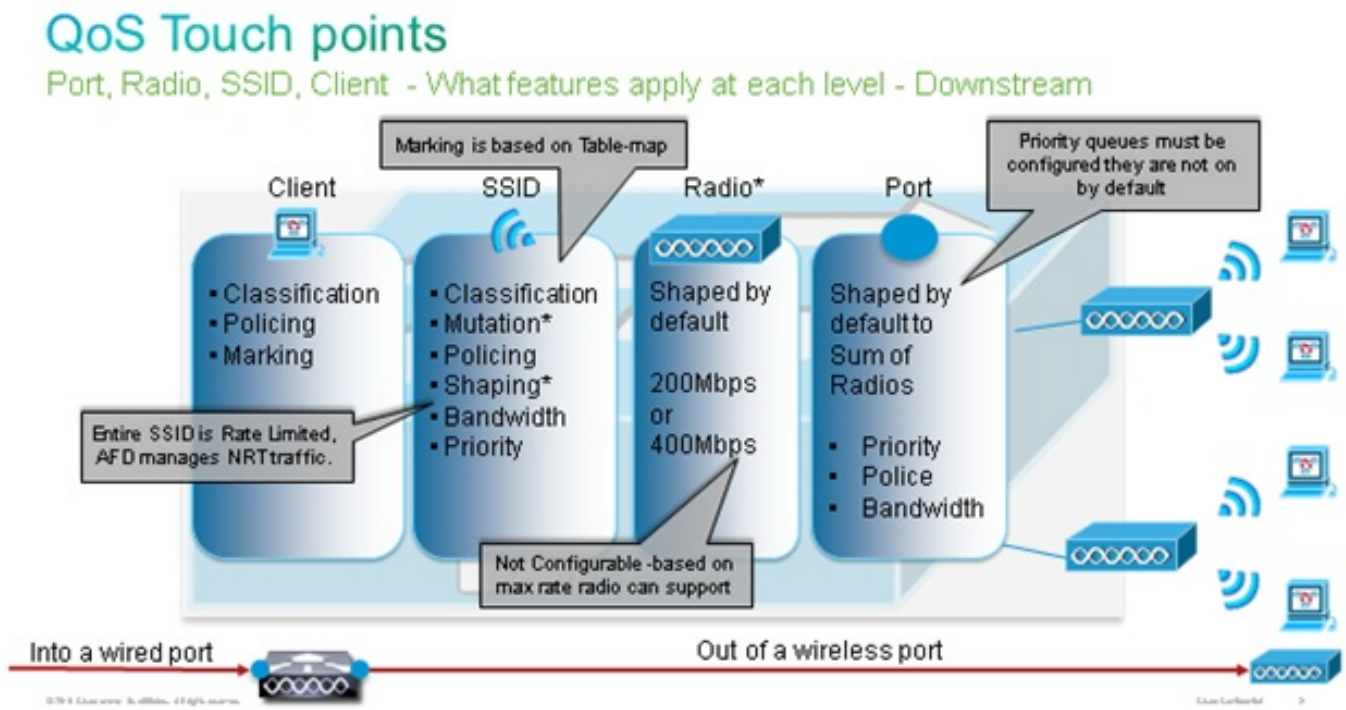
Der nächste Schritt besteht darin, die QoS-Richtlinie auf SSID-Ebene zu übernehmen. Dieser Schritt gilt sowohl für den Catalyst 3850-Switch als auch für den 5760-Controller. Bei dieser Konfiguration wird davon ausgegangen, dass Sprach- und Videodatenverkehr mithilfe von Klassenzuordnungen und Zugriffslisten identifiziert und korrekt gekennzeichnet wird. Bei einigen eingehenden Datenverkehr, der nicht von der Zugriffsliste betroffen ist, wird jedoch möglicherweise die QoS-Markierung nicht angezeigt. In diesem Fall können Sie festlegen, ob dieser Datenverkehr mit einem Standardwert gekennzeichnet oder nicht markiert werden soll. Die gleiche Logik gilt für Datenverkehr, der bereits markiert, aber nicht von den Klassenzuordnungen erfasst wurde. Verwenden Sie die *standardmäßige copy*-Anweisung in einer Tabellenübersicht, um sicherzustellen, dass nicht markierter Datenverkehr nicht markiert bleibt und der getaggte Datenverkehr das Tag behält und nicht neu gekennzeichnet wird.

Table-Maps bestimmen den ausgehenden DSCP-Wert, werden aber auch zur Erstellung eines 802.11-Frames verwendet, um den Frame-UP-Wert festzulegen.

In diesem Beispiel behält eingehender Datenverkehr, der die Sprach-QoS-Ebene (DSCP 46) anzeigt, seinen DSCP-Wert bei, und der Wert wird der entsprechenden 802.11-Markierung (UP 6) zugeordnet. Eingehender Datenverkehr, der die Video-QoS-Ebene (DSCP 34) anzeigt, behält seinen DSCP-Wert bei, und der Wert wird der entsprechenden 802.11-Markierung (UP 5) zugeordnet. Entsprechend kann der mit DSCP 24 gekennzeichnete Datenverkehr Sprachsignalisierung sein. Der DSCP-Wert sollte beibehalten und in 802.11 UP 3 umgewandelt werden:

```
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
```

Die Markierung kann auch auf der Ebene eingehender kabelgebundener Ports erfolgen. Diese Abbildung zeigt, welche QoS-Aktionen bei der Übertragung des Datenverkehrs von kabelgebundenen zu Wireless-Netzwerken möglich sind:



Dieses Konfigurationsbeispiel konzentriert sich auf den Wireless-Aspekt der QoS-Konfiguration und markiert den Datenverkehr auf der Ebene der Wireless-Clients. Nachdem die Markierung abgeschlossen ist, müssen Sie Bandbreite zuweisen. Dabei ist 6 Mbit/s Bandbreite Sprachdatenströmen zugewiesen. (Obwohl dies die gesamte Bandbreitenzuweisung für Sprache ist, würde jeder Anruf weniger verbrauchen, z. B. 128 Kbit/s.) Diese Bandbreite wird mit dem Befehl **Police** zugewiesen, um die Bandbreite zu reservieren und den Datenverkehr zu stark zu reduzieren.

Der Videodatenverkehr wird ebenfalls 6 Mbit/s zugewiesen und überwacht. Bei diesem Konfigurationsbeispiel wird davon ausgegangen, dass nur ein Videofluss vorhanden ist.

Der Signalisierungsteil des Video- und Sprachverkehrs muss auch Bandbreite zugewiesen werden. Es gibt zwei mögliche Strategien.

- Verwenden Sie den Befehl **shape average**, mit dem überzähliger Datenverkehr gepuffert und später gesendet werden kann. Diese Logik ist für den Sprach- oder Videodatenfluss selbst nicht effizient, da diese Datenflüsse konsistente Verzögerungen und Jitter erfordern. Sie kann jedoch effizient für die Signalisierung verwendet werden, da die Signalisierung leicht verzögert werden kann, ohne dass die Anrufqualität beeinträchtigt wird. Bei der konvergenten Zugriffslösung akzeptieren die Shape-Befehle nicht so genannte Buckets-Konfigurationen, die festlegen, wie viel Datenverkehr über die zugewiesene Bandbreite hinaus gepuffert werden kann. Daher muss ein zweiter Befehl, das **Warteschlangen-Puffer-Verhältnis 0**, hinzugefügt werden, um anzugeben, dass die Größe des Buckets 0 ist. Wenn Sie die Signalisierung in den restlichen Datenverkehr einbinden und Befehle für die Form verwenden, kann der Signalisierungsverkehr in Zeiten hoher Überlastung fallen. Dies kann wiederum dazu führen, dass der Anruf verworfen wird, da beide Enden feststellen, dass keine Kommunikation mehr stattfindet.
- Um das Risiko verworfener Anrufe zu vermeiden, können Sie die Signalisierung in eine der Prioritätswarteschlangen einbeziehen. In diesem Konfigurationsbeispiel wurden zuvor die

Prioritätswarteschlangen als Sprache und Video definiert und der Videowarteschlange die Signalisierung hinzugefügt.

Die Richtlinie verwendet die Call Admission Control (CAC) für den Sprachdatenfluss. CAC ist auf Wireless-Datenverkehr ausgerichtet und entspricht einem bestimmten UP (in diesem Konfigurationsbeispiel UP 6 und 7). Die CAC bestimmt dann die maximale Bandbreite, die dieser Datenverkehr verwenden soll. Bei einer Konfiguration, bei der der Sprachverkehr überwacht wird, sollte der CAC ein Teil der gesamten Bandbreite zugewiesen werden, die der Sprachkommunikation zugewiesen wurde. Wenn beispielsweise die Sprachsteuerung auf 6 Mbit/s festgelegt ist, darf die CAC 6 Mbit/s nicht überschreiten. CAC wird in einer Richtlinienzuordnung (einer so genannten untergeordneten Richtlinie) konfiguriert, die in die zentrale Downstream-Richtlinienzuweisung (die so genannte übergeordnete Richtlinie) integriert ist. CAC wird mit dem Befehl **permit cac wmm-tspec** gefolgt von den Ziel-UPs und der Bandbreite für den Zieldatenverkehr eingeführt.

Bei jedem Anruf wird nicht die gesamte der Sprachkommunikation zugewiesene Bandbreite belegt. Beispielsweise kann jeder Anruf auf jede Weise 64 Kbit/s verbrauchen, was zu einer effektiven bidirektionalen Bandbreitennutzung von 128 Kbit/s führt. Die Übertragungsratenanweisung bestimmt die Bandbreitennutzung aller Anrufe, während die Richtlinienanweisung die dem Sprachverkehr zugewiesene Gesamtbandbreite festlegt. Wenn alle Anrufe innerhalb der Zelle fast die maximal zulässige Bandbreite nutzen, wird jeder neue Anruf, der innerhalb der Zelle initiiert wird und dazu führt, dass die verbrauchte Bandbreite die für Sprache zulässige maximale Bandbreite überschreitet, abgelehnt. Sie können diesen Prozess durch die Konfiguration der CAC auf Bandebene optimieren, wie in Schritt 4 erläutert: Anrufbegrenzung mit CAC.

Daher müssen Sie eine untergeordnete Richtlinie konfigurieren, die CAC-Anweisungen enthält und in die Haupt-Downstream-Richtlinie integriert ist. CAC ist in der Upstream-Richtlinienzuordnung nicht konfiguriert. CAC gilt für Sprachanrufe, die von der Zelle aus initiiert werden. Da es sich jedoch um eine Antwort auf diese Anrufe handelt, wird CAC nur in der Downstream-Richtlinienzuordnung festgelegt. Die Upstream-Richtlinienzuordnung ist unterschiedlich. Sie können die zuvor erstellten Klassenzuordnungen nicht verwenden, da diese Klassenzuordnungen auf einem ACL-Zieldatenverkehr basieren. Der in die SSID-Richtlinie eingespeiste Datenverkehr durchlief bereits die Client-Richtlinie. Daher sollten Sie die Pakete nicht erneut einer eingehenden Prüfung unterziehen. Stattdessen sollte Zieldatenverkehr mit einer QoS-Markierung anvisiert werden, die aus der Client-Richtlinie resultiert.

Wenn Sie die Signalisierung nicht in der Standardklasse belassen, müssen Sie auch die Signalisierung priorisieren.

In diesem Beispiel befinden sich Signalisierungs- und Videofunktionen in derselben Klasse, und dieser Klasse wird mehr Bandbreite zugewiesen, um den Signalisierungsteil unterzubringen. 6 Mbit/s sind für Videodatenverkehr (ein Point-to-Point-Datenfluss der Tandberg-Kamera) und 1 Mbit/s für die Signalisierung aller Sprachanrufe und des Video-Datenflusses zugewiesen:

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

Die Downstream-Kinderrichtlinie ist:

```
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
```

Die Downstream-übergeordneten Richtlinien sind:

```
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
```

Upstream-Datenverkehr ist Datenverkehr, der von Wireless-Clients stammt und an den WCM gesendet wird, bevor der Datenverkehr über einen kabelgebundenen Port gesendet oder an eine andere SSID gesendet wird. In beiden Fällen können Sie Richtlinienzuordnungen konfigurieren, die die Bandbreite definieren, die den einzelnen Datenverkehrstypen zugewiesen ist. Die Richtlinien unterscheiden sich möglicherweise je nachdem, ob der Datenverkehr über einen kabelgebundenen Port oder an eine andere SSID gesendet wird.

In der Upstream-Richtung besteht Ihr Hauptanliegen darin, die Priorität zu bestimmen, nicht die Bandbreite. Mit anderen Worten: Ihre Upstream-Richtlinienzuordnung weist nicht jedem Datenverkehrstyp Bandbreite zu. Da sich der Datenverkehr bereits am Access Point befindet und bereits den Flaschenhals des Halbduplex-Wireless-Raumes passiert hat, ist es Ihr Ziel, diesen Datenverkehr zur Weiterverarbeitung an die Controller-Funktion des Catalyst 3850-Switches oder des Cisco 5760-WLC zu bringen. Wenn der Datenverkehr auf AP-Ebene erfasst wird, können Sie entscheiden, ob Sie potenziellen vorhandenen QoS-Markierungen vertrauen möchten, um die an den Controller gesendeten Datenverkehrsflüsse zu priorisieren. In diesem Beispiel können vorhandene DSCP-Werte vertrauenswürdig sein:

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

Wenden Sie die Richtlinienzuordnungen nach der Erstellung auf das WLAN an. In diesem Beispiel wird erwartet, dass jedes Gerät, das mit dem WLAN verbunden ist, WMM unterstützt. WMM ist daher erforderlich.

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

Schritt 4: Anrufeinschränkung mit CAC

Der letzte Schritt besteht darin, die CAC an Ihre spezifische Situation anzupassen. In der in Schritt 3 erläuterten CAC-Konfiguration: Bandbreiten- und Prioritäts-Management auf SSID-Ebene

verwirft der Access Point jedes Sprachpaket, das die zugewiesene Bandbreite überschreitet.

Um die maximale Bandbreite zu vermeiden, müssen Sie auch den WCM so konfigurieren, dass getätigte Anrufe und Anrufe, die zu einer Überschreitung der Bandbreite führen, erkannt werden. Einige Telefone unterstützen die WMM Traffic Specification (TSPEC) und informieren die Wireless-Infrastruktur über die Bandbreite, die der geplante Anruf voraussichtlich nutzen wird. Der WCM kann den Anruf dann ablehnen, bevor er platziert wird.

Einige SIP-Telefone unterstützen TSPEC nicht, aber der WCM und der AP können so konfiguriert werden, dass an SIP-Ports gesendete Anruflösepakete erkannt werden. Anhand dieser Informationen kann festgestellt werden, dass ein SIP-Anruf getätigt werden soll. Da das SIP-Telefon keine Bandbreite für den Anruf vorgibt, muss der Administrator die erwartete Bandbreite basierend auf dem Codec, der Abtastzeit usw. bestimmen.

CAC berechnet die genutzte Bandbreite auf jeder AP-Ebene. CAC kann so eingestellt werden, dass nur die Client-Bandbreitennutzung bei ihren Berechnungen (statische CAC) verwendet wird oder auch benachbarte APs und Geräte auf demselben Kanal (lastenbasierte CAC) berücksichtigt werden. Cisco empfiehlt, statische CAC für SIP-Telefone und lastenbasierte CAC für TSPEC-Telefone zu verwenden.

Beachten Sie schließlich, dass CAC auf Bandbasis aktiviert wird.

In diesem Beispiel verwenden Telefone für die Initiierung von Sitzungen SIP anstelle von TSPEC. Jeder Anruf verwendet für jede Streamrichtung 64 Kbit/s, lastenbasierte CAC ist deaktiviert, wenn statische CAC aktiviert ist, und 75 % jeder AP-Bandbreite wird dem Sprachdatenverkehr zugewiesen:

```
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
```

Sie können dieselbe Konfiguration für das 2,4-GHz-Band wiederholen:

```
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
```

Sobald CAC für jedes Band angewendet wurde, müssen Sie auch SIP CAC auf WLAN-Ebene anwenden. Dieser Prozess ermöglicht es dem AP, Layer-4-Informationen (L4) des Wireless-Client-Datenverkehrs zu überprüfen, um an den UDP 5060 gesendete Abfragen zu identifizieren, die SIP-Anrufversuche anzeigen. TSPEC wird auf der 802.11-Ebene betrieben und von APs nativ erkannt. SIP-Telefone verwenden TSPEC nicht, daher muss der AP eine tiefere Paketprüfung durchführen, um SIP-Datenverkehr zu identifizieren. Da Sie nicht möchten, dass der Access Point diese Überprüfung auf allen SSIDs durchführt, müssen Sie bestimmen, welche SSID SIP-Datenverkehr erwarten. Sie können dann auf diesen SSIDs das Snooping aktivieren, um nach Sprachanrufen zu suchen. Sie können auch festlegen, welche Aktion ausgeführt werden soll, wenn ein SIP-Anruf abgelehnt werden muss: Trennen Sie die Verknüpfung zum SIP-Client, oder senden Sie eine SIP-Besetztnachricht.

In diesem Beispiel ist Call Snooping aktiviert, und eine Besetztzeichen-Nachricht wird gesendet, wenn der SIP-Anruf abgelehnt werden muss. Durch Hinzufügen der QoS-Richtlinie aus Schritt 3: Bandbreiten- und Prioritätsverwaltung auf SSID-Ebene, dies ist die SSID-Konfiguration für das Beispiel-WLAN:

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

Überprüfen

Verwenden Sie diese Befehle, um zu überprüfen, ob Ihre QoS-Konfiguration ordnungsgemäß funktioniert.

> **Hinweise**:
>
> Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.
>
> Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Klassenzuordnung anzeigen

Dieser Befehl zeigt die auf der Plattform konfigurierten Klassenzuordnungen an:

```
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
```

Richtlinienzuweisung anzeigen

Dieser Befehl zeigt die auf der Plattform konfigurierten Richtlinienzuweisungen an:

```
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
```

Show-WLAN

Dieser Befehl zeigt die WLAN-Konfigurations- und Service-Richtlinienparameter an:

```
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
```

Anzeige der Richtlinienzuweisungsschnittstelle

Dieser Befehl zeigt die für eine bestimmte Schnittstelle installierte Richtlinienzuordnung an:

```
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
```

Anzeige von Plattform-QoS-Richtlinien

Dieser Befehl zeigt die für Ports, AP-Funkmodule, SSIDs und Clients installierten QoS-Richtlinien an. Beachten Sie, dass Sie die Funkrichtlinien überprüfen, aber nicht ändern können:

```
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

Dieser Befehl zeigt die auf Client-Ebene angewendeten Richtlinienzuweisungen an:

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.