

CISCO *Live!*



#CiscoLiveAPJC



The bridge to possible

Design and Deployment of QoS for Modern Wireless Networks

Tjie Seng, Njauw , Technical Solutions Architect

BRKEWN-2031



#CiscoLiveAPJC

Cisco Webex App

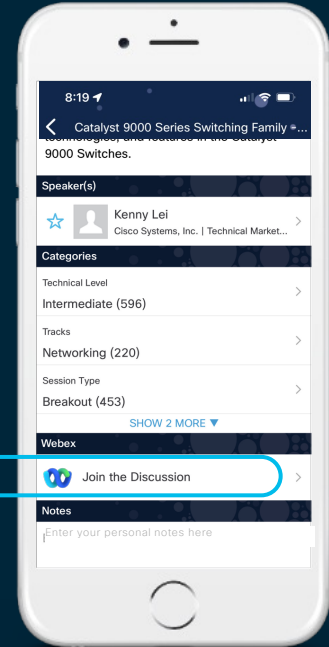
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until Thursday 22 December, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2031>

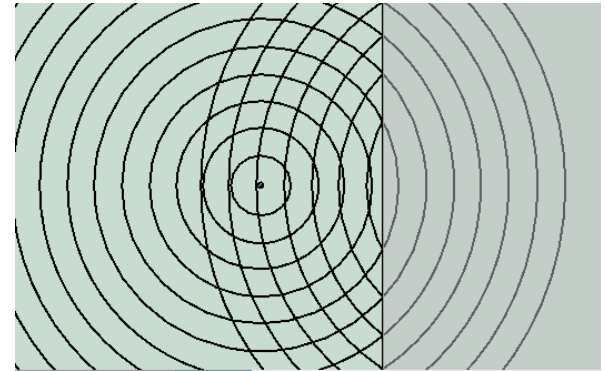


Agenda

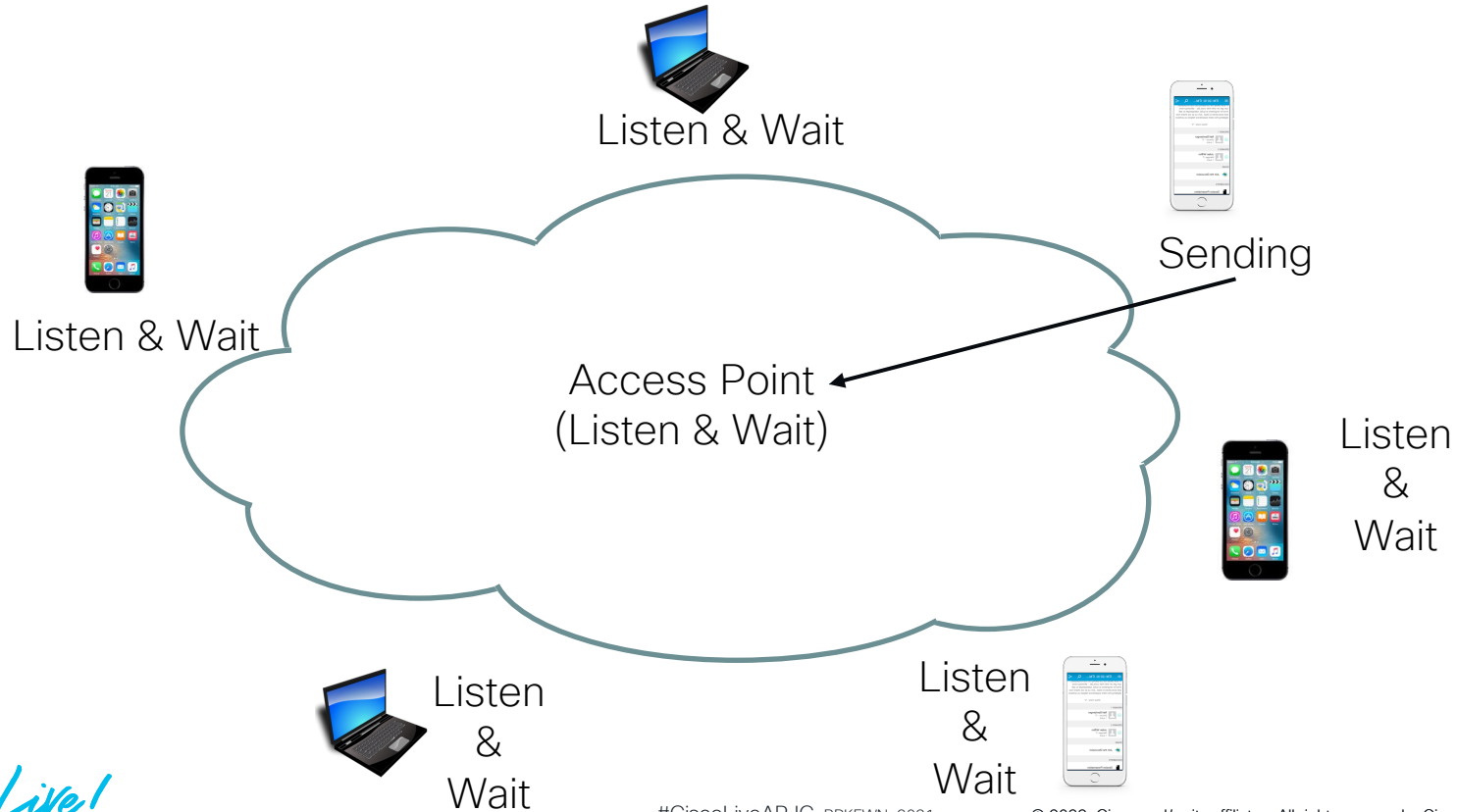
- 802.11 QoS Building Blocks
- How QoS Works in Wi-Fi6/6E
- IOS-XE / Catalyst 9800 QoS Deployments
- Fastlane+

Carrier Sense Multiple Access / Collision Avoidance

- Wired Hubs use CSMA/CD (collision detection)
 - A station must listen to the medium to see if it is idle before sending it's frame. When it seems idle, it sends the frame.
 - After sending, it listens to see if a collision has occurred
- 802.11 networks use CSMA/CA (collision avoidance)
 - Wireless networks have no way to detect that a collision even occurred!
 - Uses a system of fixed and random wait timers to ensure everyone gets a chance to send
 - Every frame must be acknowledged

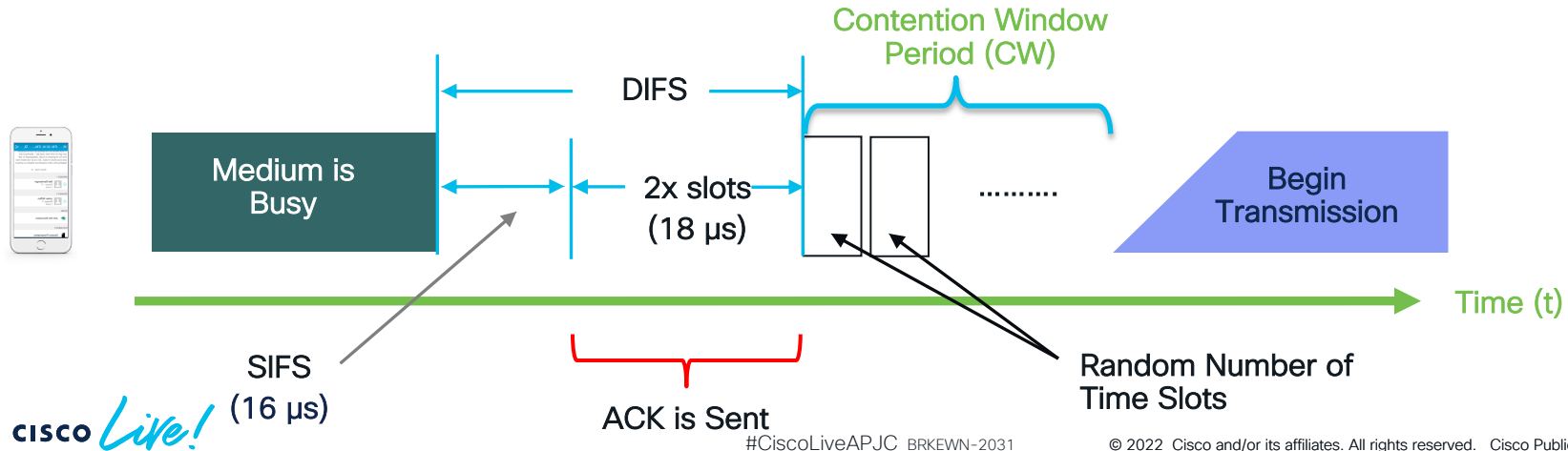


Wi-Fi Media Access is Contention-Based



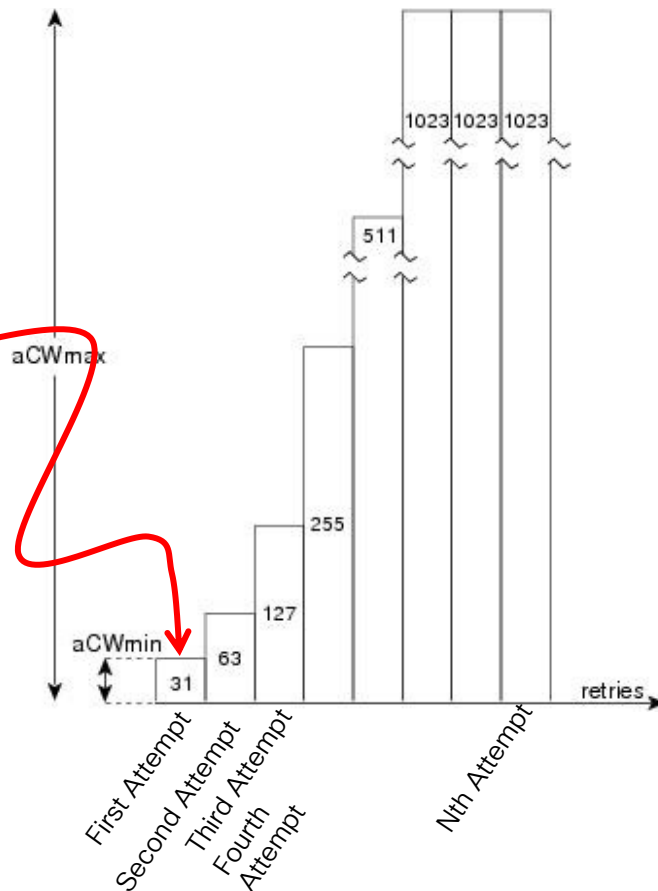
Distributed Coordination Function (DCF)

- When ready to transmit, all stations must first wait the DCF Interframe space (DIFS)
 - Allows all stations to sense end of frame Tx and allow ACK to be sent back
- Once DIFS has counted down to zero, a random backoff countdown timer (the Contention Window) is generated if the medium is not free.
 - Initially, this value is between zero and a value known as CW_{min}
 - Once the CW counts down to zero, the frame is transmitted

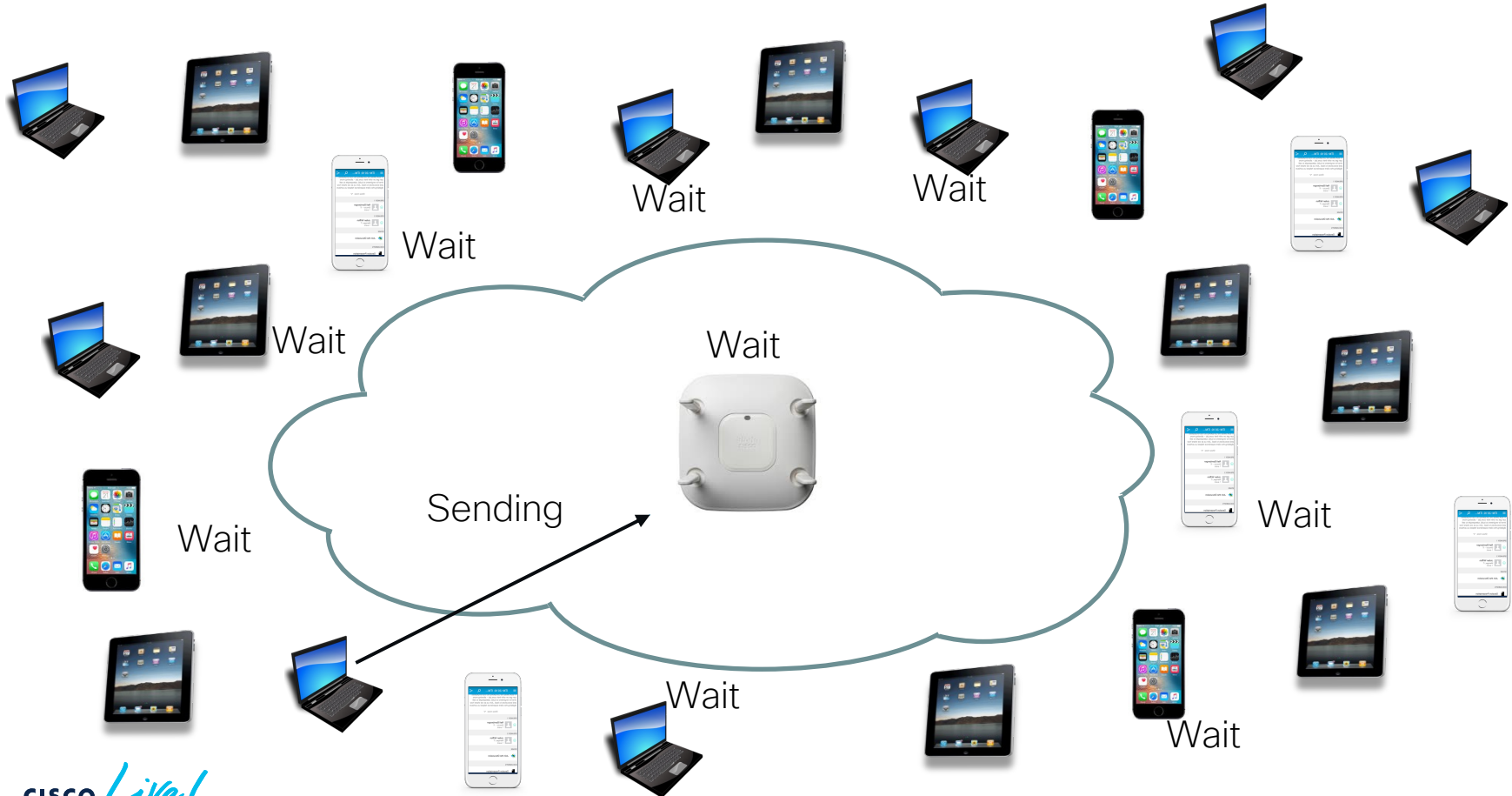


What if Your Frame Doesn't Get Ack'd?

- How do you know the transmission got through okay? The receiving station must send an acknowledgment.
- If the first attempt didn't work (no ACK received), double the previous CW size and pick a new random number.
 - Keep doing this until the CW reaches a maximum size of 1023 slot times.
- How many times should the station keep trying?
 - In Cisco APs, the maximum number of attempts is 64 before the frame is discarded.

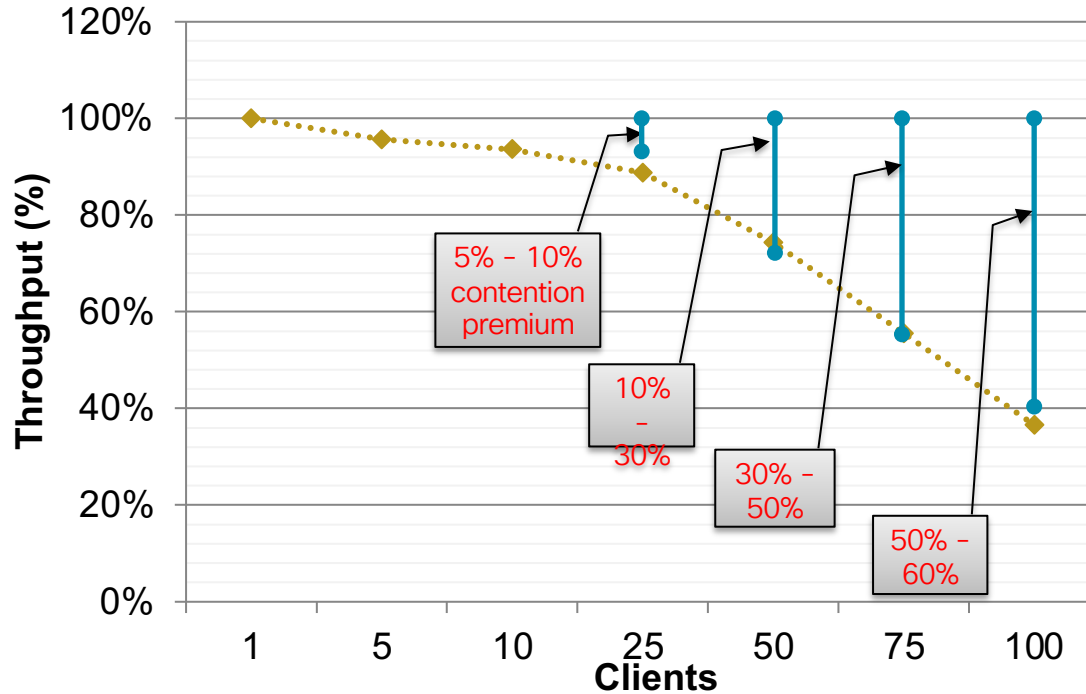


What Happens When the Client Count Goes Up?



The Contention Breaking Point (802.11ac)

(source: IEEE 802.11-15/0351r2)



As more clients associate and transmit, WLAN contention increases for all clients, degrading performance for all

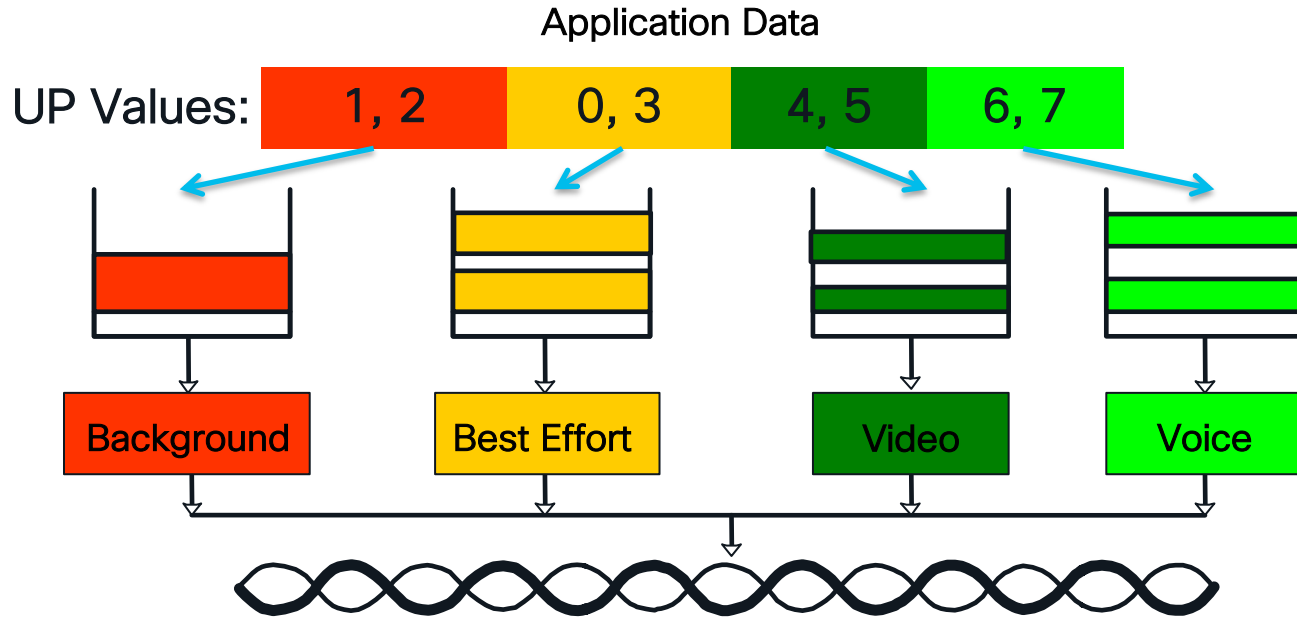
The Enhanced Distributed Channel Access (EDCA)

802.11e Introduced the Enhanced Distributed Channel Access (EDCA) Model in 2005

- 802.11e was tasked with bringing QoS to Wi-Fi
- EDCA was introduced by IEEE 802.11e in 2005, and has been adopted by the Wi-Fi Alliance as Wireless Multimedia (WMM)
- WMM is now a mandatory part of modern Wi-Fi
 - 802.11a/b/g are based on DCF (no QoS)
 - 802.11n/ac are based on EDCA (QoS is supported)
- Continual improvements, including the 802.11-2016 “rollup”

#1 Access Categories (ACs)

When wireless frames are transmitted, a 3-bit QoS value known as the **User Priority (UP)** is written into the 802.11 header



Default DSCP ↔ UP Mapping Table

Traffic Type	DSCP	802.11e UP / WMM	Access Category
Voice	46 (EF)	6	Voice
Interactive Video	34 (AF41)	5	Video
Call Signaling	24 (CS3)	3	Best Effort
Transactional / Interactive Data	18 (AF21)	3	Best Effort
Bulk Data	10 (AF11)	2	Background
Best Effort	0 (BE)	0	Best Effort



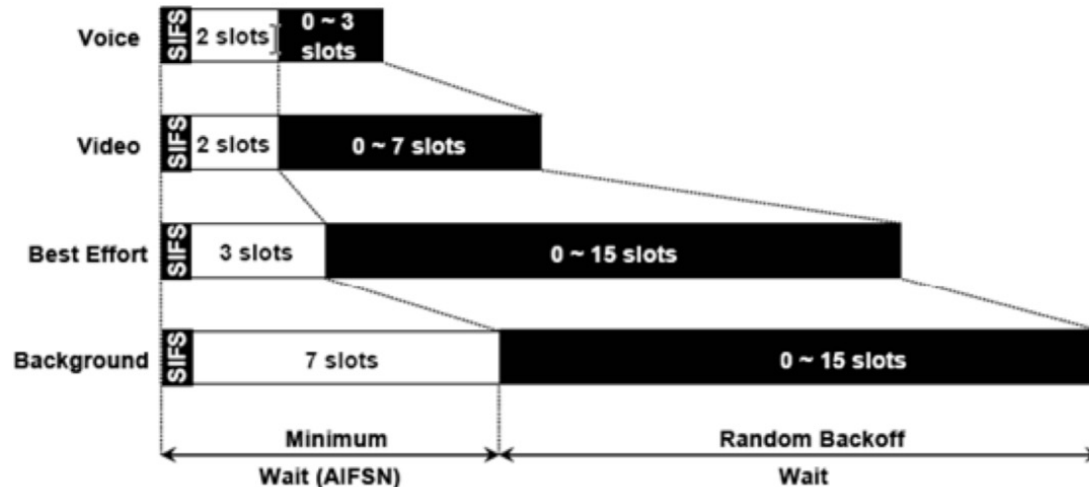
#2 Assign Backoff Timers for the Access Category

- EDCA manages the ACs in the following way:
 - Variable Arbitration Interframe Spacing (AIFS)
 - Variable CW_{min} and CW_{max} values depending on traffic type
 - Values shown are “slot times” – 9μs per slot in 802.11

EDCA / WMM AC	AIFS Number	CWmin	CWmax
Legacy DCF	DIFS > 2	15*	1023
Voice	2	3	7
Video	2	7	15
Best Effort	3	15	1023
Background	7	15	1023

Understanding the Effect of EDCA Timers

- By combining these timers, the theoretical probability of higher priority frames getting serviced first is greatly improved (but is not guaranteed in every case)
- Simply having a queue doesn't give you QoS – how you manage the queue is what matters.



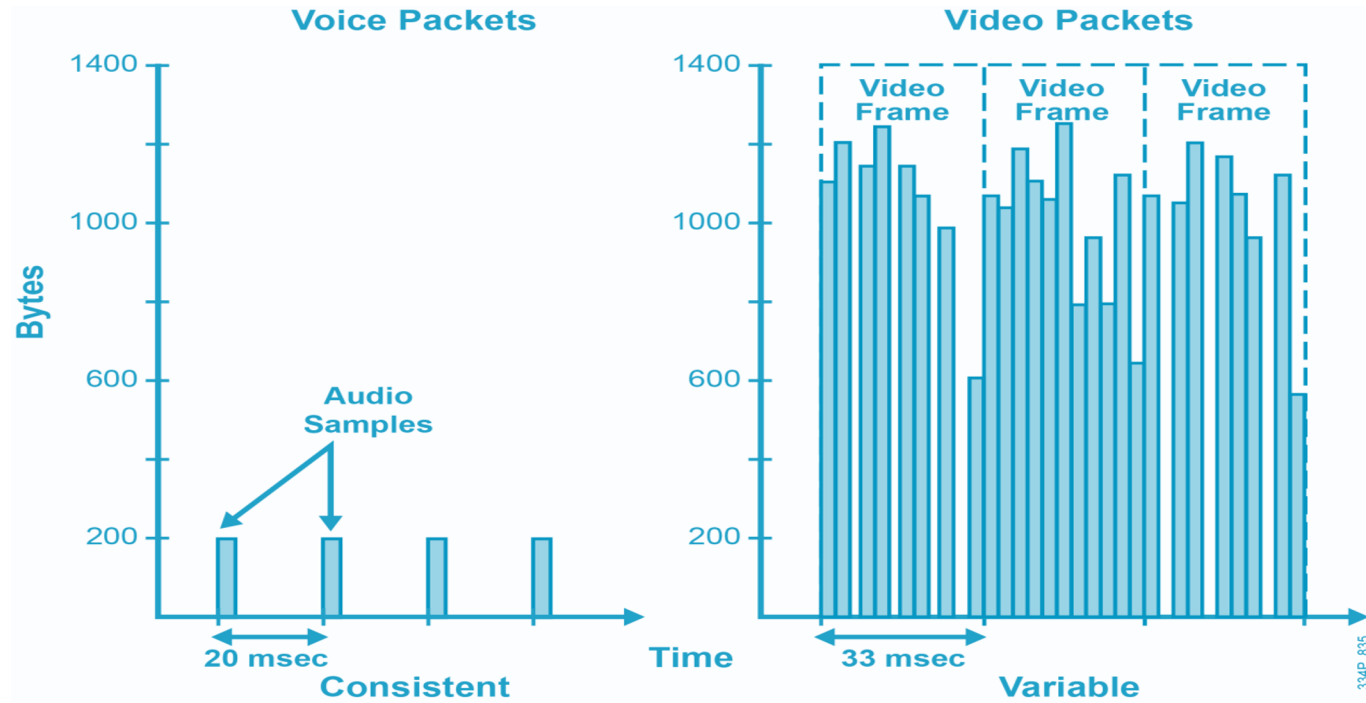
#3 Transmission Opportunity (TXOP)

- TXOP is a timer – a station keeps sending until it's TXOP timer counts down to zero
- DCF had no such thing – send one frame and then start again!

EDCA / WMM AC	TXOP (μ s)	TXOP (Units)
Voice	2080	65
Video	4096	128
Best Effort	2528	79
Background	2528	79

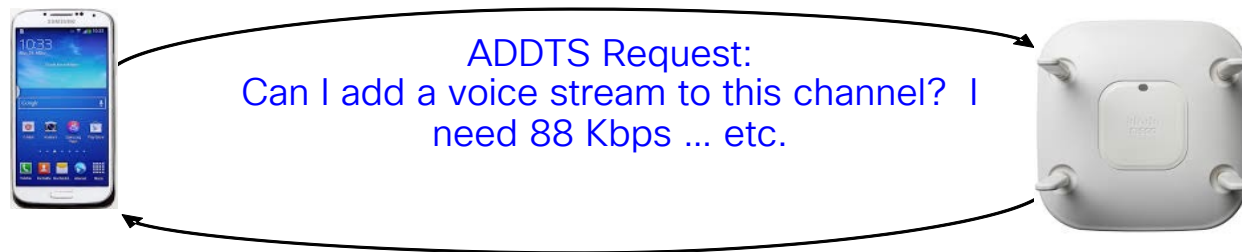
Real Time Voice vs. Real Time Video Traffic Profile

Traffic Profile Helps Model TXOP Timers



#4 Transmission Specification (TSpec)

- TSpec is basically Call Admission Control – management of the number of voice and video traffic flows per AP radio
- Client signals to AP to request it's traffic stream be added to AP (ADDTS)
- TSpec includes data rate, packet size, number of stream & more



ADDTS Response:
Sorry, there's no room for this traffic!

Summary: Four Key 802.11e QoS Enhancements

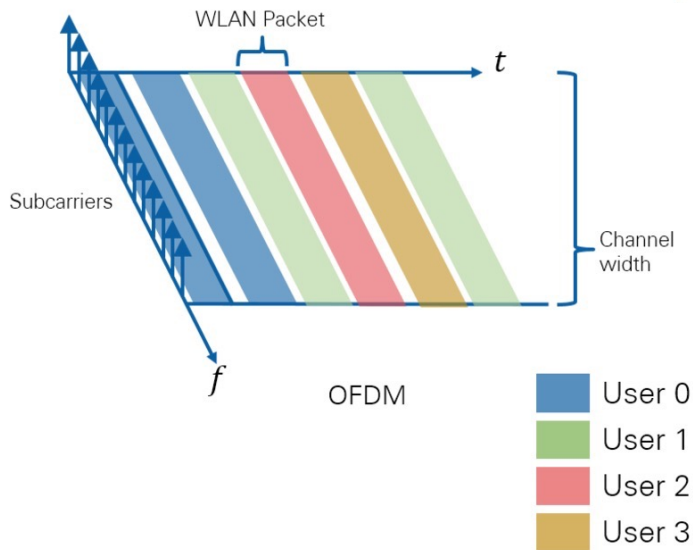
Enhanced Distributed Channel Access (EDCA):

1. Establishment of four Access Categories and 3-bit User Priority QoS field
2. New timers replacing legacy static DIFS and CW
3. Each AC get's its own Transmission Opportunity (TXOP)
4. Call Admission Control (CAC) with TSpec

How QoS Works in Wi-Fi6 / 6E (802.11ax)

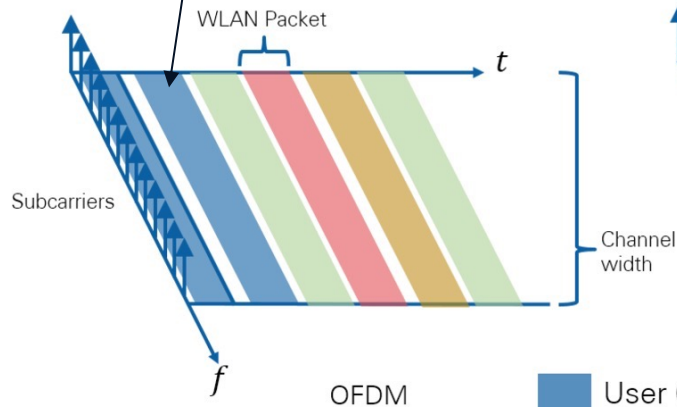
OFDMA (Orthogonal Frequency Division Multiple Access)

- Subcarriers (Resource Units – RUs) can be assigned to different users for uplink transmissions
 - Can be combined with UL MU MIMO

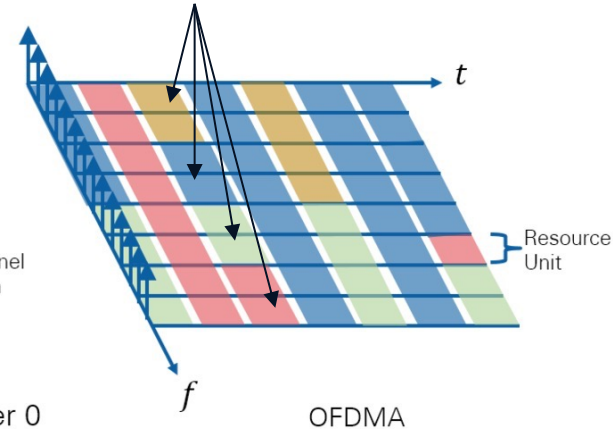
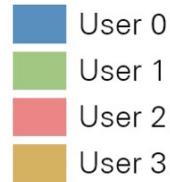


OFDMA (Orthogonal Frequency Division Multiple Access)

A Single Station Transmits in a Timeslot won by the contention algorithm (EDCA)

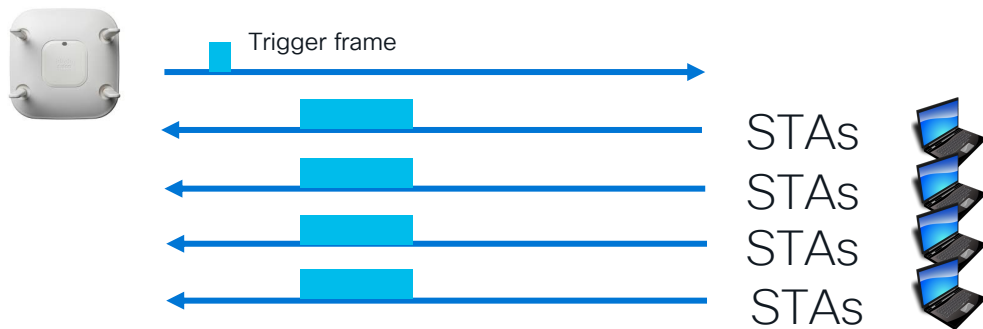


Multiple Stations Transmit in a scheduled Timeslot



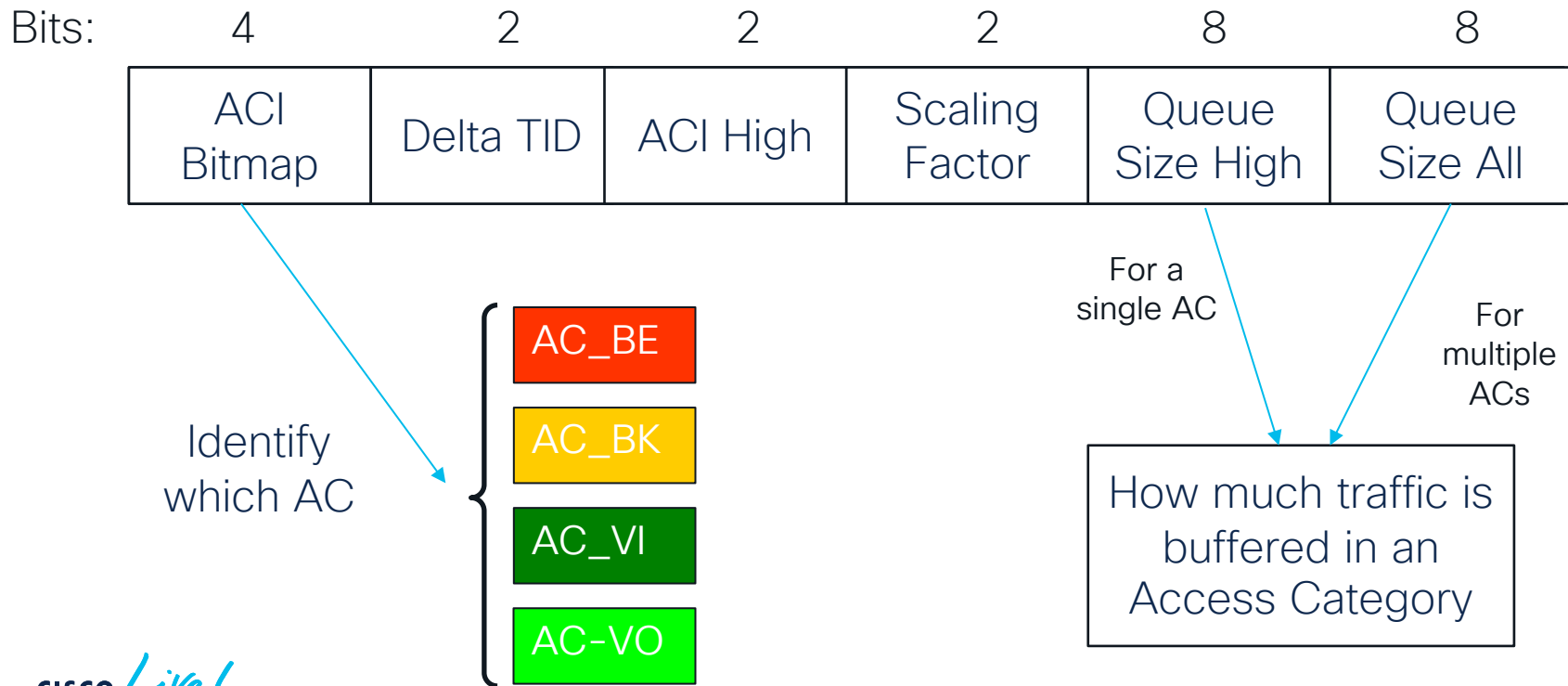
802.11ax Uplink (UL) MU-MIMO

- 802.11ac allows for downlink MU-MIMO
- 802.11ax adds uplink MU-MIMO
 - AP checks which STAs can send together
 - AP sends trigger frame and STAs respond all at the same time



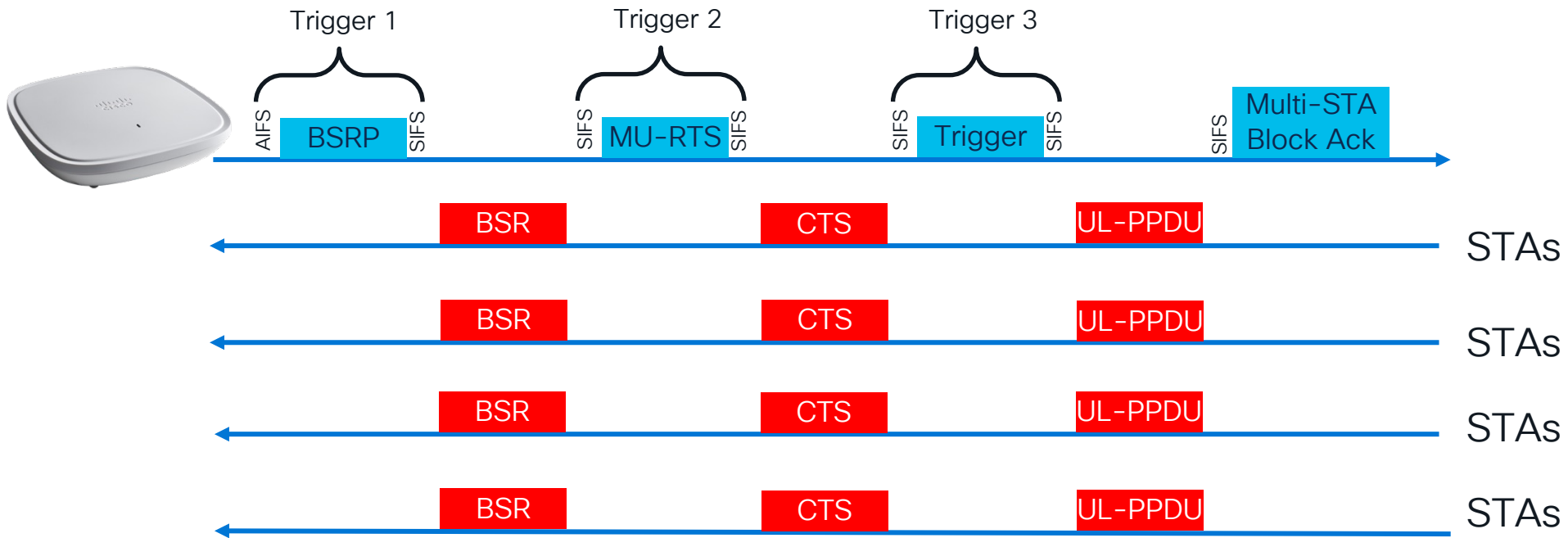
Unsolicited Buffer Status Reports

STAs may send QoS information in the **BSR Control** subfield of any frame



Buffer Status Report Polling (BSRP)

(Figuring out how many RUs to Assign)

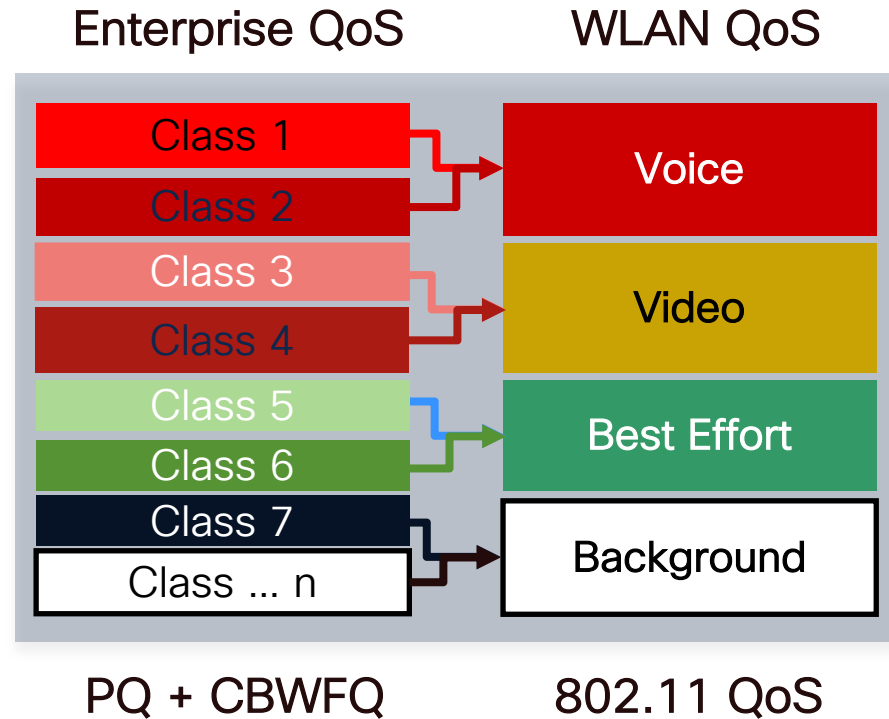


IOS-XE / Catalyst 9800 QoS Deployment

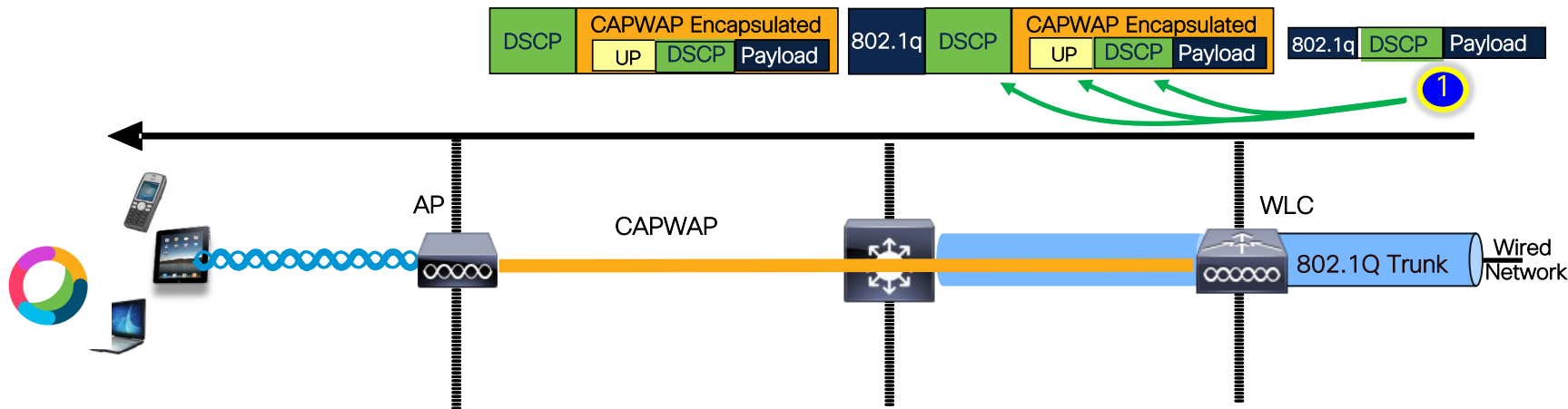


A Consistent QoS Strategy: Unifying Wired and Wireless QoS

- By definition of IEEE 802.11e standard there are only 4 levels of service (Access Categories)
- The class-based QoS model should align with the four AC model in the wireless network
- Need to make sure the QoS markings are consistent end-to-end through the network and the design is consistent



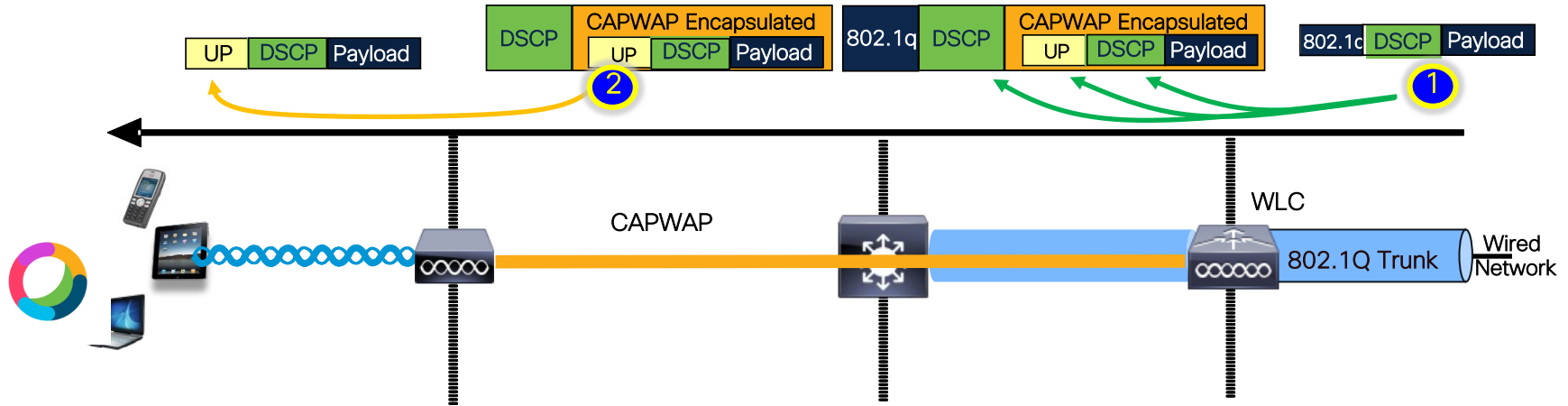
Catalyst 9800 Downstream QoS Model



- 1 The client packet is received over an 802.1q trunk by the WLC. The WLC uses the DSCP value of the original IP packet and maps it to the outer DSCP of the CAPWAP tunnel (assuming no ceiling value is applied via Metal QoS at the WLC). It also maps DSCP to UP and set it in the inner 802.11e header

Note: class of Service (CoS) tagging is not supported in 9800 (supported but not recommended in AireOS)

Catalyst 9800 Downstream QoS Model

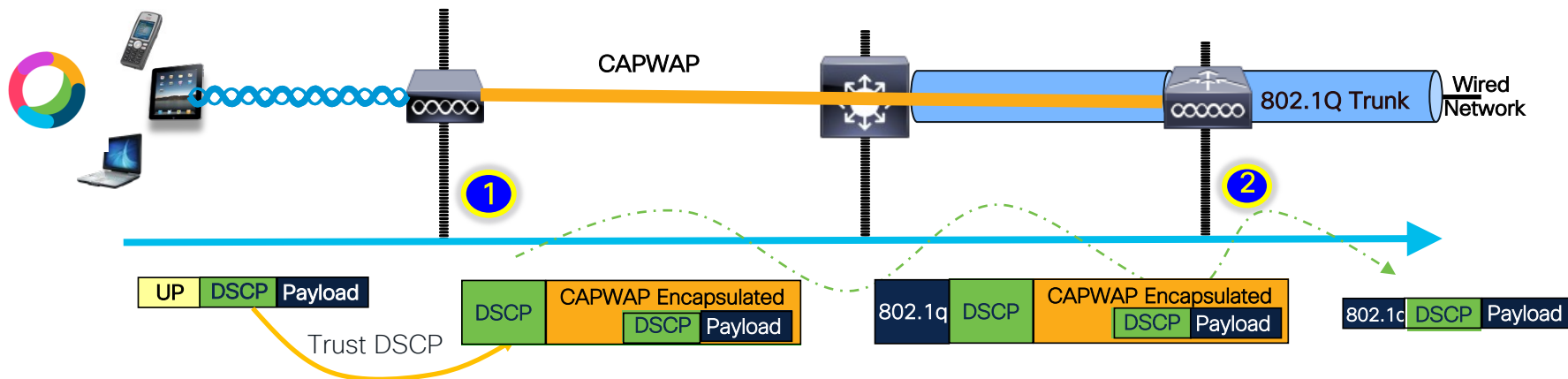


- 1 The client packet is received over an 802.1q trunk by the WLC. The WLC uses the DSCP value of the original IP packet and maps it to the outer DSCP of the CAPWAP tunnel (assuming no ceiling value is applied via Metal QoS at the WLC). It also maps DSCP to UP and set it in the inner 802.11e header
- 2 The AP leverages the inner UP value received from the WLC for internal QoS processing and queuing. The 802.11e UP value is also copied in the egress wireless 802.11 frame to the client, over the air

Catalyst 9800 Upstream QoS Model

1

The client 802.11e frame is received by the AP. The AP utilizes the DSCP value in the original packet for internal QoS processing and then maps it to the outer CAPWAP IP header, (assuming no ceiling value is applied via Metal QoS at the WLC)(*).



2

This allow preservation of the DSCP value from the client all the way through the network, emerging untouched from the WLC (assuming no Metal QoS or AVC policy is applied to remark DSCP)

Example of Webex VoIP Call

10390	0.015556	08:50:11.045078	23.89.129.108	192.168.1.51	UDP	348	UDP	9000	52413	244 Default Best Effort (Best Effort)	90 → 52413 Len=236
10394	0.000001	08:50:11.058079	192.168.1.51	23.89.129.108	UDP	156	UDP	52413	9000	52 Expedited... Voice (Voice)	413 → 9000 Len=44
10399	0.000001	08:50:11.063979	192.168.1.51	23.89.129.108	UDP	228	UDP	52413	9000	124 Expedited... Voice (Voice)	413 → 9000 Len=116
10401	0.001501	08:50:11.065056	23.89.129.108	192.168.1.51	UDP	368	UDP	9000	52413	264 Default Best Effort (Best Effort)	90 → 52413 Len=256
10403	0.003666	08:50:11.069329	23.89.129.108	192.168.1.51	UDP	152	UDP	9000	52413	48 Default Best Effort (Best Effort)	90 → 52413 Len=40
10404	0.000006	08:50:11.069335	23.89.129.108	192.168.1.51	UDP	152	UDP	9000	52413		
10407	0.002501	08:50:11.087700	170.72.80.250	192.168.1.51	TCP	1344	TCP				
10408	0.000711	08:50:11.088411	170.72.80.250	192.168.1.51	TCP	1344	TCP			Default Best Effort (Best Effort)	443 → 43470 [ACK] Seq=64111 Ack=1065
10409	0.000003	08:50:11.088414	170.72.80.250	192.168.1.51	TLSv1.2	686	TCP			Default Best Effort (Best Effort)	[TCP Retransmission] 443 → 43470 [A
10413	0.000001	08:50:11.089574	192.168.1.51	170.72.80.250	TCP	124	TCP			Default Best Effort (Best Effort)	Application Data
10417	0.000001	08:50:11.090576	192.168.1.51	170.72.80.250	TCP	124	TCP			Default Best Effort (Best Effort)	43470 → 443 [ACK] Seq=1069 Ack=6533:
10419	0.000567	08:50:11.091144	23.89.129.108	192.168.1.51	UDP	348	UDP	9000	52413	244 Default Best Effort (Best Effort)	9000 → 52413 Len=236
10420	0.000003	08:50:11.091147	170.72.80.250	192.168.1.51	TLSv1.2	227	TCP			Default Best Effort (Best Effort)	Application Data

```
.0... .. = Protected flag: Data is not protected
0... .. = +HTC/Order flag: Not strictly ordered
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: Cisco_82:69:e5 (14:16:9d:82:69:e5)
Transmitter address: ca:44:b4:6b:a3:29 (ca:44:b4:6b:a3:29)
Destination address: AztechEl_bc:94:f5 (00:26:75:bc:94:f5)
Source address: ca:44:b4:6b:a3:29 (ca:44:b4:6b:a3:29)
BSS Id: Cisco_82:69:e5 (14:16:9d:82:69:e5)
STA address: ca:44:b4:6b:a3:29 (ca:44:b4:6b:a3:29)
.... .. 0000 = Fragment number: 0
0000 0000 0110 .... = Sequence number: 6
Frame check sequence: 0x1e3853a9 [unverified]
[FCS Status: Unverified]
✓ Qos Control: 0x0006
.... .. 0110 = TID: 6
[.... .. 110 = Priority: Voice (Voice) (6)]
.... .. 00 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
.... .. 00. .... = Ack Policy: Normal Ack (0x0)
.... .. 0... .... = Payload Type: MSDU
0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
> Logical Link Control
✓ Internet Protocol Version 4, Src: 192.168.1.51, Dst: 23.89.129.108
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
✓ Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
1011 10... = Differentiated Services Codepoint: Expedited Forwarding (46)
.... .. 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 72
Identification: 0xde02 (56834)
> Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x014a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.51
Destination Address: 23.89.129.108
```

Example of WhatsApp VoIP Call

552	0.153540	07:19:17.616406	192.168.1.51	192.168.1.254	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) request	id=0x0001,
553	0.000002	07:19:17.616408	192.168.1.51	4.2.2.2	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) request	id=0x0004,
554	0.000666	07:19:17.617874	192.168.1.51	192.168.1.254	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) request	id=0x0002,
555	0.002094	07:19:17.619168	192.168.1.254	192.168.1.51	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) reply	id=0x0001,
556	0.000005	07:19:17.619173	192.168.1.254	192.168.1.51	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) reply	id=0x0002,
557	0.002130	07:19:17.621303	4.2.2.2	192.168.1.51	ICMP	168	ICMP	Default	Best Effort (Best Effort)	no (ping) reply	id=0x0004,
558	0.000343	07:19:17.621646	4.2.2.2	192.168.1.51	ICMP	168	ICMP	Default	Best Effort (Best Effort)	no (ping) reply	id=0x0004,
559	0.021922	07:19:17.643568	192.168.1.51	157.240.15.62	UDP	138	UDP	34 Class Selector 6	Network Control (Voice)	762 → 43768 Len=26	
560	0.011839	07:19:17.655407	157.240.15.62	192.168.1.51	UDP	234	UDP	130 Default	Best Effort (Best Effort)	78 → 43762 Len=122	
561	0.000006	07:19:17.655413	157.240.15.62	192.168.1.51	UDP	181	UDP	77 Default	Best Effort (Best Effort)	78 → 43762 Len=69	
562	0.000003	07:19:17.655416	157.240.15.62	192.168.1.51	UDP	234	UDP	130 Default	Best Effort (Best Effort)	78 → 43762 Len=122	
563	0.000001	07:19:17.655417	157.240.15.62	192.168.1.51	UDP	181	UDP	77 Default	Best Effort (Best Effort)	78 → 43762 Len=69	
564	0.000978	07:19:17.656395	157.240.15.62	192.168.1.51	UDP	234	UDP	130 Default	Best Effort (Best Effort)	78 → 43762 Len=122	
565	0.000006	07:19:17.656401	157.240.15.62	192.168.1.51	UDP	181	UDP	77 Default	Best Effort (Best Effort)	78 → 43762 Len=69	
566	0.000872	07:19:17.657273	157.240.15.62	192.168.1.51	UDP	234	UDP	130 Default	Best Effort (Best Effort)	78 → 43762 Len=122	
567	0.000006	07:19:17.657279	157.240.15.62	192.168.1.51	UDP	181	UDP	77 Default	Best Effort (Best Effort)	78 → 43762 Len=69	
568	0.008646	07:19:17.665925	192.168.1.51	157.240.15.62	STUN	132	UDP	28 Class Selector 0	Network Control (Voice)	Unknown Request	
569	0.021778	07:19:17.687783	157.240.15.62	192.168.1.51	STUN	132	UDP	28 Default	Best Effort (Best Effort)	Unknown Request	
570	0.075375	07:19:17.763878	192.168.1.51	157.240.15.62	UDP	321	UDP	217 Class Selector 6	Network Control (Voice)	43762 → 3478 Len=209	
571	0.075375	07:19:17.763878	157.240.15.62	192.168.1.51	UDP	147	UDP	28 Default	Best Effort (Best Effort)	3478 → 43762 Len=30	
> Frame 560: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)											
> Radiotap Header v0, Length 46											
> 802.11 radio information											
IEEE 802.11 QoS Data, Flags:F.C											
Type/Subtype: QoS Data (0x0028)											
Frame Control Field: 0x8802											
...000 0000 0011 0000 = Duration: 48 microseconds											
Receiver address: ca:44:b4:6b:a3:29 (ca:44:b4:6b:a3:29)											
Transmitter address: Cisco_82:69:e5 (14:16:9d:82:69:e5)											
Destination address: ca:44:b4:6b:a3:29 (ca:44:b4:6b:a3:29)											
Source address: ArtechIL_be:94:f5 (00:26:75:bc:94:f5)											
BSS Id: Cisco_82:69:e5 (14:16:9d:82:69:e5)											
STA address: ca:44:b4:6b:a3:29 (ca:44:b4:6b:a3:29)											
.... 0000 = Fragment number: 0											
0011 1110 1010 = Sequence number: 1002											
Frame check sequence: 0xab8960cf [unverified]											
[FCS Status: Unverified]											
QoS Control: 0x8000											
.... 0000 = TID: 0											
[.... 0000 = Priority: Best Effort (Best Effort) (0)]											
.... 0000 = EOSP: Service period											
.... 0000 = Ack Policy: Normal Ack (0x0)											
.... 0000 = Payload Type: MSDU											
> 0000 0000 = QAP PS Buffer State: 0x00											
Logical-Link Control											
Internet Protocol Version 4, Src: 157.240.15.62, Dst: 192.168.1.51											
0100 = Version: 4											
.... 0101 = Header Length: 20 bytes (5)											
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)											
0000 00.. = Differentiated Services Codepoints: Default (0)											
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)											
Total Length: 150											
Identification: 0x6c31 (27697)											
Flags: 0x40, Don't fragment											
...0 0000 0000 0000 = Fragment Offset: 0											
Time to Live: 62											

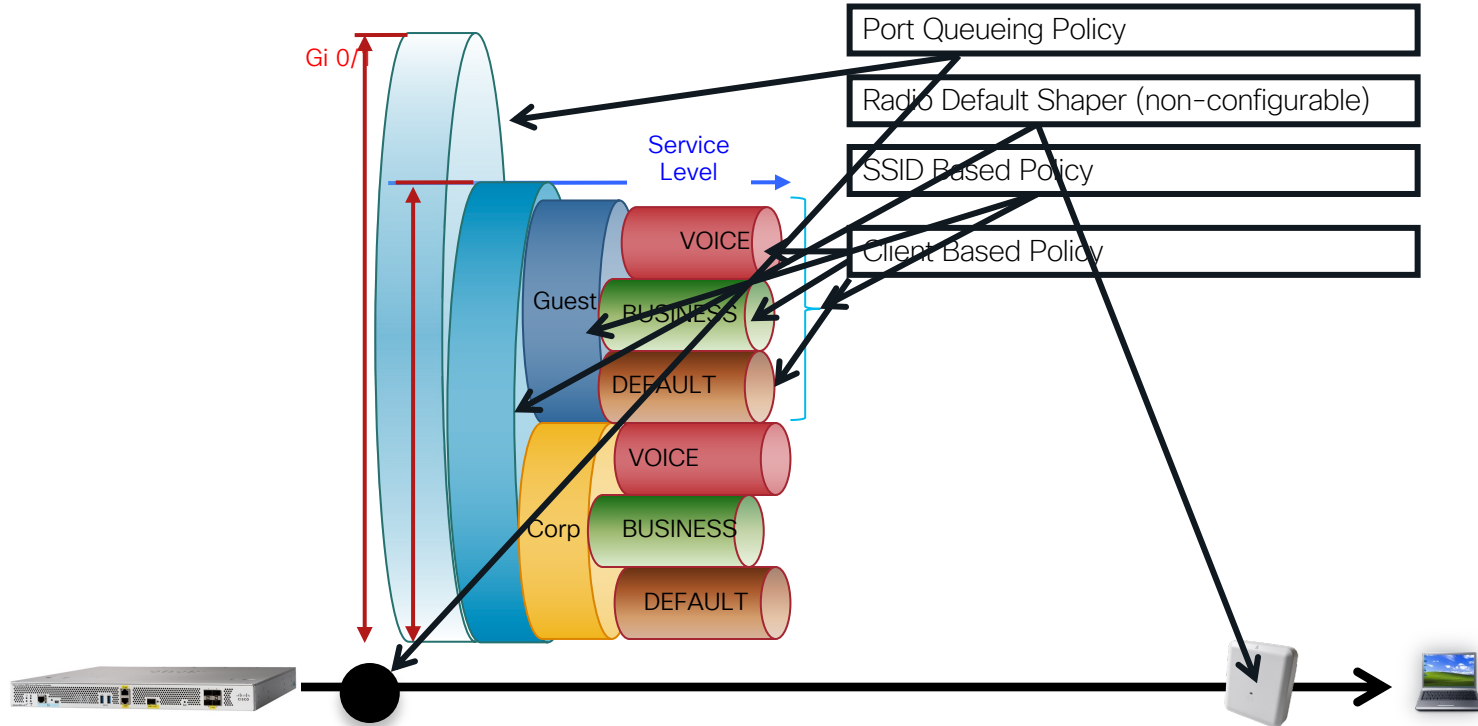
Example of Microsoft Teams VoIP free version

4617	0.048357	08:26:10.414968	192.168.1.51	192.168.1.254	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) request	id=0x000		
4618	0.002582	08:26:10.417550	192.168.1.254	192.168.1.51	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) reply	id=0x000		
4619	0.043420	08:26:10.460970	192.168.1.51	192.168.1.254	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) request	id=0x000		
4620	0.000122	08:26:10.461092	192.168.1.51	4.2.2.2	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) request	id=0x000		
4621	0.002315	08:26:10.463407	192.168.1.254	192.168.1.51	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) reply	id=0x000		
4622	0.002127	08:26:10.465534	4.2.2.2	192.168.1.51	ICMP	168	ICMP	Default	Best Effort (Best Effort)	Echo (ping) reply	id=0x000		
4623	0.017006	08:26:10.482540	192.168.1.51	23.102.90.243	UDP	228	UDP	39797	3480	124	Default	Best Effort (Best Effort)	39797 → 3480 Len=116
4624	0.119689	08:26:10.602229	23.102.90.243	192.168.1.51	UDP	184	UDP	3480	397...	80	Default	Best Effort (Best Effort)	180 → 39797 Len=72
4625	0.003226	08:26:10.685455	23.102.90.243	192.168.1.51	UDP	229	UDP	3480	397...	125	Default	Best Effort (Best Effort)	180 → 39797 Len=117
4626	0.021030	08:26:10.706485	23.102.90.243	192.168.1.51	UDP	258	UDP	3480	397...	154	Default	Best Effort (Best Effort)	180 → 39797 Len=146
4627	0.000015	08:26:10.706500	23.102.90.243	192.168.1.51	UDP	268	UDP	3480	397...	164	Default	Best Effort (Best Effort)	180 → 39797 Len=156
4628	0.016037	08:26:10.722537	23.102.90.243	192.168.1.51	UDP	188	UDP	3480	206...	180	Default	Best Effort (Best Effort)	180 → 20648 Len=76
4629	0.002592	08:26:10.725129	23.102.90.243	192.168.1.51	UDP	243	UDP	3480	397...	139	Default	Best Effort (Best Effort)	3480 → 39797 Len=131
4630	0.021880	08:26:10.747009	23.102.90.243	192.168.1.51	UDP	242	UDP	3480	397...	138	Default	Best Effort (Best Effort)	3480 → 39797 Len=130
4631	0.020618	08:26:10.767627	23.102.90.243	192.168.1.51	UDP	239	UDP	3480	397...	135	Default	Best Effort (Best Effort)	3480 → 39797 Len=127
4632	0.018803	08:26:10.786430	23.102.90.243	192.168.1.51	UDP	239	UDP	3480	397...	135	Default	Best Effort (Best Effort)	3480 → 39797 Len=127
4633	0.020322	08:26:10.806752	23.102.90.243	192.168.1.51	UDP	242	UDP	3480	397...	138	Default	Best Effort (Best Effort)	3480 → 39797 Len=130
4634	0.020416	08:26:10.827168	23.102.90.243	192.168.1.51	UDP	156	UDP	3480	397...	52	Default	Best Effort (Best Effort)	3480 → 39797 Len=44
4635	0.000005	08:26:10.827173	23.102.90.243	192.168.1.51	UDP	1332	UDP	3480	397...	1228	Default	Best Effort (Best Effort)	3480 → 39797 Len=1220

```
Source address: ca:44:b4:6b:a3:29 (ca:44:b4:6b:a3:29)
BSS Id: Cisco_82:69:e5 (14:16:9d:82:69:e5)
STA address: ca:44:b4:6b:a3:29 (ca:44:b4:6b:a3:29)
.... 0000 = Fragment number: 0
1000 0111 1000 .... = Sequence number: 2168
Frame check sequence: 0xb87b30cf [unverified]
[FCS Status: Unverified]
  Qos Control: 0x0000
    .... 0000 = TID: 0
    [...] .... 0000 = Priority: Best Effort (Best Effort) (0)
    .... 0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
    .... 00 .... = Ack Policy: Normal Ack (0x0)
    .... 0000 .... = Payload Type: MSDU
    0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.51, Dst: 23.102.90.243
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 144
  Identification: 0x5977 (22903)
> 010 .... = Flags: 0x2, Don't fragment
... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xacb1 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.51
  Destination Address: 23.102.90.243
> User Datagram Protocol, Src Port: 39797, Dst Port: 3480
  Source Port: 39797
  Destination Port: 3480
  Length: 124
  Checksum: 0x9074 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
> [Timestamps]
```

```
0000 00 00 2e 00 6b 08 18 40 a2 41 d8 04 00 00 00 00 ...k...@...A.....
0010 10 00 a8 09 80 04 c a 07 00 1f 14 07 18 10 00 00 ...f...D...k...J...
0020 08 00 00 00 00 10 18 03 04 00 01 33 18 00 88 01 0 ...3.....
0030 30 00 14 16 9d 82 69 e5 ca 44 b4 6b a3 29 00 26 0 ...4...D...k...J...
0040 75 bc 94 f5 80 87 00 80 a0 aa 03 00 00 00 08 00 u.....
0050 45 00 00 00 59 77 40 00 40 11 ac b1 c0 a8 01 33 E...Yw...@.....3
0060 17 66 5a f3 9b 75 0d 98 00 7c 90 74 ff 10 00 70 ...fZ...u...j...t...p
0070 d6 7f 35 50 dc 77 52 3f 00 01 00 54 21 12 a4 42 ...SP...w?...T...B
0080 d4 76 f4 03 a6 90 28 c4 25 ac 61 0f 00 06 00 00 v...f...
0090 2b 52 42 73 3a 66 64 34 57 00 00 00 00 70 00 04 +RBS:fda W...p...
00a0 00 00 00 07 00 24 00 04 66 67 c0 03 00 2a 00 08 ...f...fg...
00b0 00 00 00 70 4b 2c 70 08 80 37 00 00 00 00 00 04 ...pK,p...7.....
00c0 00 00 00 14 53 4d 46 dc 8b af 50 12 de 6c d7 08 ...SMF...P...L...
00d0 93 78 00 76 8d 00 c9 80 28 00 04 e2 e4 d3 83 ...xV...N...N...
00e0 cf 30 7b b8
```

Controller Hierarchical Wireless QoS



Catalyst 9800 Auto QoS – explained

- **Voice**: sets the recommended QoS policy to correctly mark and prioritize voice at the SSSI level and enables CAC.
- **Guest**: sets the recommended QoS policy at SSID level to mark everything to Best Effort
- **Enterprise**: sets the recommended QoS policy at SSID level to mark VoIP Data, and Signaling, Multimedia, Transaction, Bulk-Data and Scavenger traffic
- **Fastlane**: sets the specific EDCA parameters. Fastlane also sets clients specific policies only for Apple clients.
- **All**: queuing is configured on the C9800 egress port for prioritizing voice and CAPWAP traffic
- Once Auto-QoS profile is applied on the policy Profile, you can view the policies via the “**show policy map**” command and show the configuration via “show run”

Catalyst 9800 – Improving Metal QoS Profiles

- QoS Metal Profiles in C9800:
 - The inner DSCP value may also be re-written
 - For C9800 you can apply Metal QoS on Egress and Ingress direction separately
 - On the GUI, you can only set the Metal QoS per SSID. On CLI you can also configure it on client target
 - For each profile, a max DSCP setting is used to remark any traffic in excess of the DSCP limit

Qos Profile	Max DSCP
Bronze	8
Silver	0
Gold	34
Platinum	46

The screenshot shows the 'Edit Policy Profile' configuration page with the 'QoS and AVC' tab selected. The 'Auto QoS' dropdown is set to 'None'. Under 'QoS SSID Policy', the 'Egress' direction is configured with a dropdown menu open, showing a list of policies: 'MyPolicy', 'platinum' (highlighted), 'gold', 'silver', and 'bronze'. The 'Ingress' direction is currently empty. Under 'QoS Client Policy', the 'Egress' direction is empty and the 'Ingress' direction has a 'Search or Select' dropdown menu.

QoS Workflow

Add applications and assign a policy

The screenshot shows the 'Add QoS' configuration window. At the top, there's a table with columns: Match Type, Match Value, Mark Type, Mark Value, Police Value (kbps), Drop, AVC/User Defined, and Actions. Below this is a pagination bar showing '0' items per page and 'No items to display'. The main configuration area includes:

- AVC/User Defined:** A dropdown menu set to 'AVC'. An annotation 'Select "AVC" Mode' points to this dropdown.
- Match:** Radio buttons for 'Any' (selected) and 'All'.
- Mark Type:** A dropdown menu set to 'DSCP'.
- Mark Value:** A dropdown menu set to '46'. An annotation 'Assign a policy' points to this dropdown.
- Drop:** An unchecked checkbox.
- Police(kbps):** A text box containing '8 - 100000000'.
- Match Type:** A dropdown menu set to 'protocol'. An annotation 'Choose Protocol' points to this dropdown.
- Available Protocol(s):** A list box containing 'ms-lync', 'ms-lync-control', and 'ms-lync-media'.
- Selected Protocol(s):** A list box containing 'cisco-jabber-audio', 'cisco-phone', and 'ms-lync-audio'. An annotation 'Select a number of applications' points to this list box.

At the bottom, there are 'Cancel' and 'Save' buttons.

You can also choose User Defined and input application ports

Fastlane+



Cisco and Apple Fastlane+ Feature Overview



OFDMA Efficiency
in High Load
Network

Supports all Wi-Fi 6
iOS 14 Apple
devices



Improved VoIP
App User
Experience

Simple 2-Step
Enable Workflow



Take your already incredible Wi-Fi 6 experience to the next level with Fastlane+

Pain Points of Wi-Fi 6

Behavior of OFDMA in a High Channel Utilization Environment

1

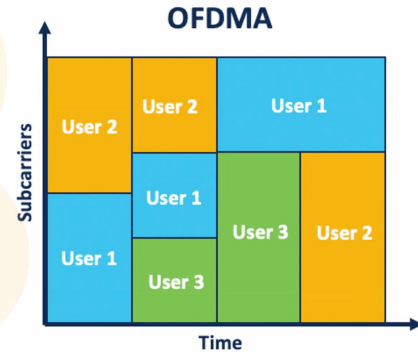
Wi-Fi 6 devices use OFDMA to pass traffic in parallel.

2

OFDMA periodically collects BSRs from joined devices.

3

Polling for BSRs adds load to a network and increases latency.



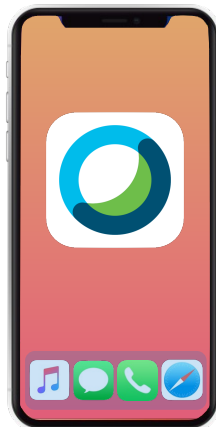
BSR = Buffer Status Report

How Fastlane+ Solves the Problem of Efficiency

1 iOS device sends ASR trigger to the network.

2 ASR session is established between network and client.

3 Network uses ASR trigger data to estimate all future BSRs.



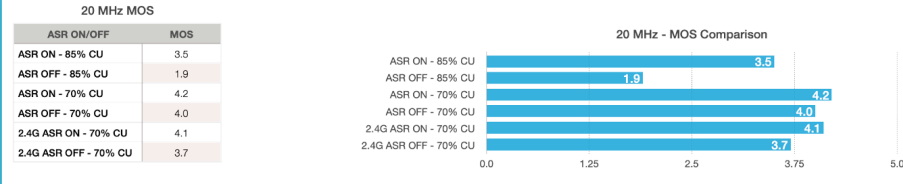
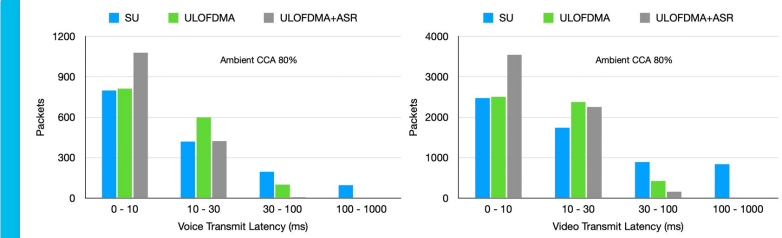
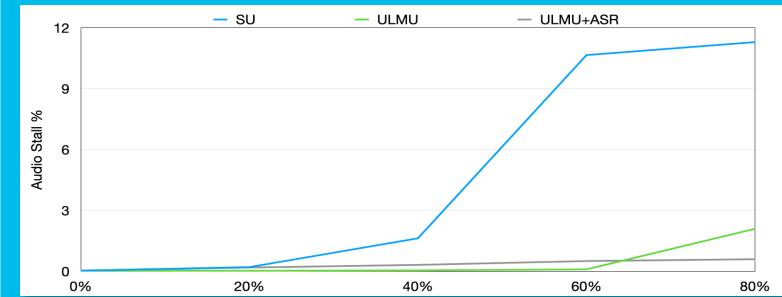
1 ASR Trigger:
• Periodicity of traffic
• Traffic bitrate

2 ASR Session Established

ASR = Advanced Scheduling Request

BSR = Buffer Status Report

Fastlane+ Enabled vs Disabled Wireless Network Performance Numbers



Fastlane+ provide more benefits the higher the channel load (Fastlane+ is referenced as ASR)

Summary

- Understanding the function of wireless QoS is foundational to any good deployment – especially the differences between EDCA and Wi-Fi6
- Think about how you will adapt a multi-class policy to wireless, which has only 4 classes
- Be aware of how Wi-Fi handles QoS mappings and markings, end-to-end
- IOS-XE improves on capabilities of AireOS, including the precious metal QoS model, extending AVC flexibility, and much more

Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one
Meet the Expert meeting



Attend the interactive education with DevNet,
Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions
at www.CiscoLive.com/on-demand

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals



The bridge to possible

Thank you

CISCO *Live!*

