Let's go

cisco Live!

The bridge to possible

The Inner Working of QoS for Modern Wireless Networks

Robert Barton, Distinguished Architect, America's Sales

BRKEWN-2031

Cisco Webex App

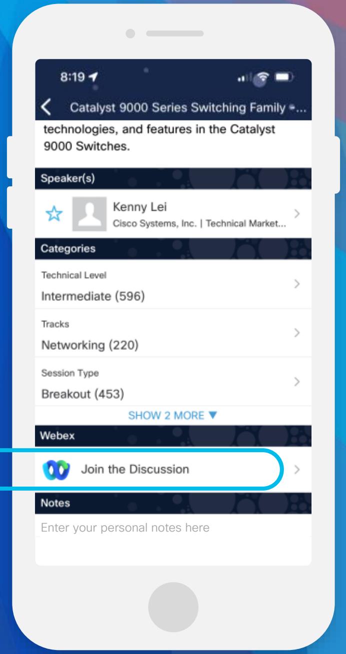
Questions?

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 June 9, 2023.



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

Agenda

- 802.11 QoS Building Blocks
- Legacy QoS:
  The Enhanced Distributed
  Channel Access (EDCA) Model
- How QoS Works in Wi-Fi6/6E
- AireOS Wireless LAN QoS Deployments
- IOS-XE / Catalyst 9800 QoS Deployments
- Next-Gen QoS: IEEE 802.11be and beyond

802.11 QoS Building Blocks

Comparing Wired and Wireless QoS

- Wired environments are Full Duplex, Wireless is Half Duplex (for now)
  - Half duplex environments are very susceptible to collisions
- Thus, wired QoS is mostly concerned with managing packet loss due to congestion problems (solved with queuing, etc.)

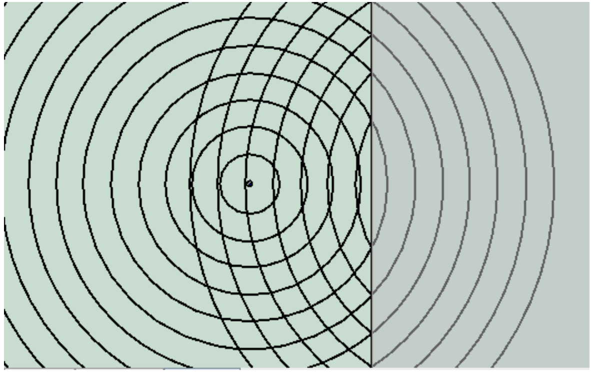
Wireless QoS is focused on a much bigger problem:

1. WLAN QoS is mostly concerned with reducing the *probability* of a collision for high-priority traffic, based on it's QoS classification
2. Managing congestion is a secondary concern

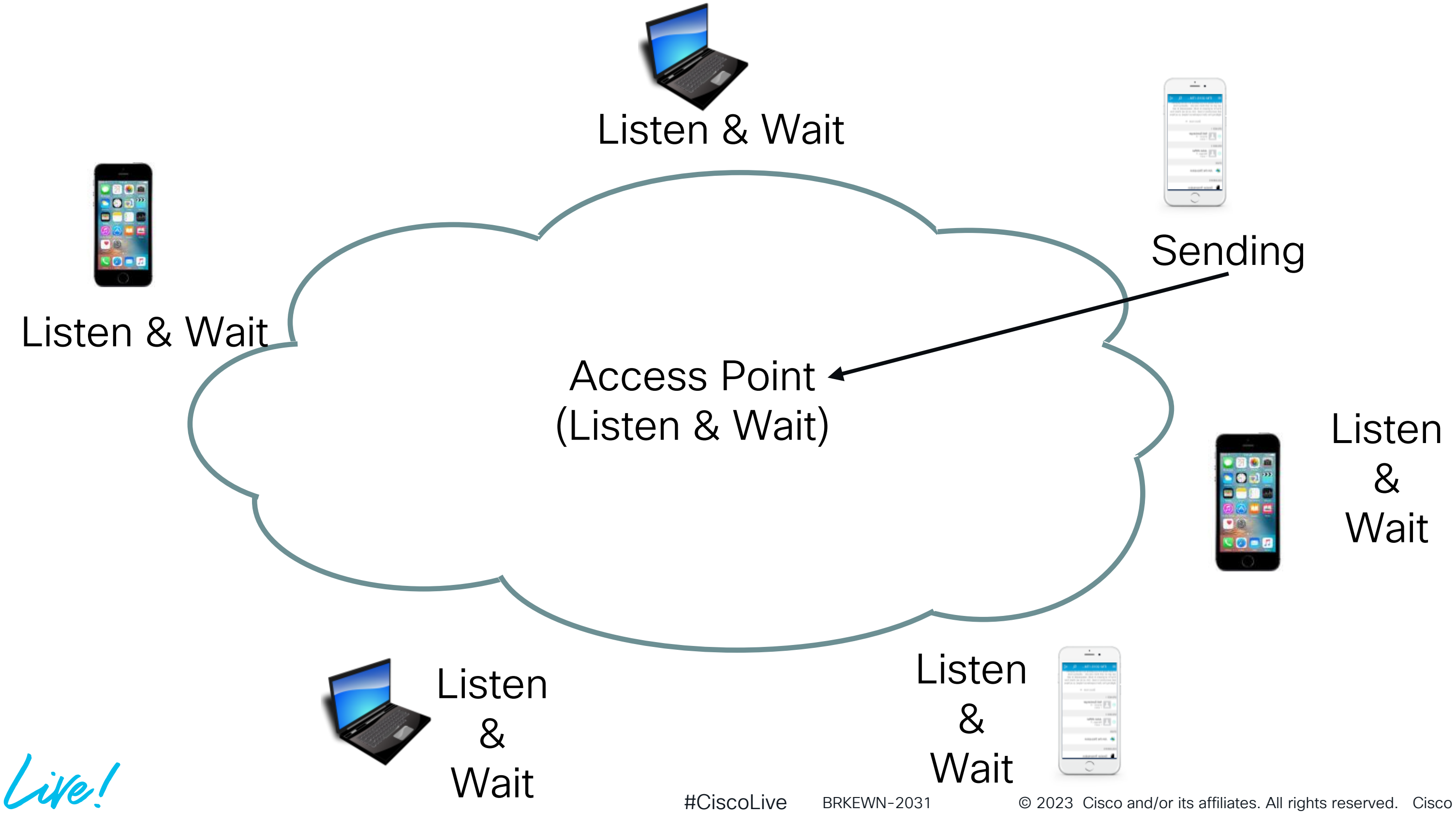
Carrier Sense Multiple Access / Collision Avoidance

- 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

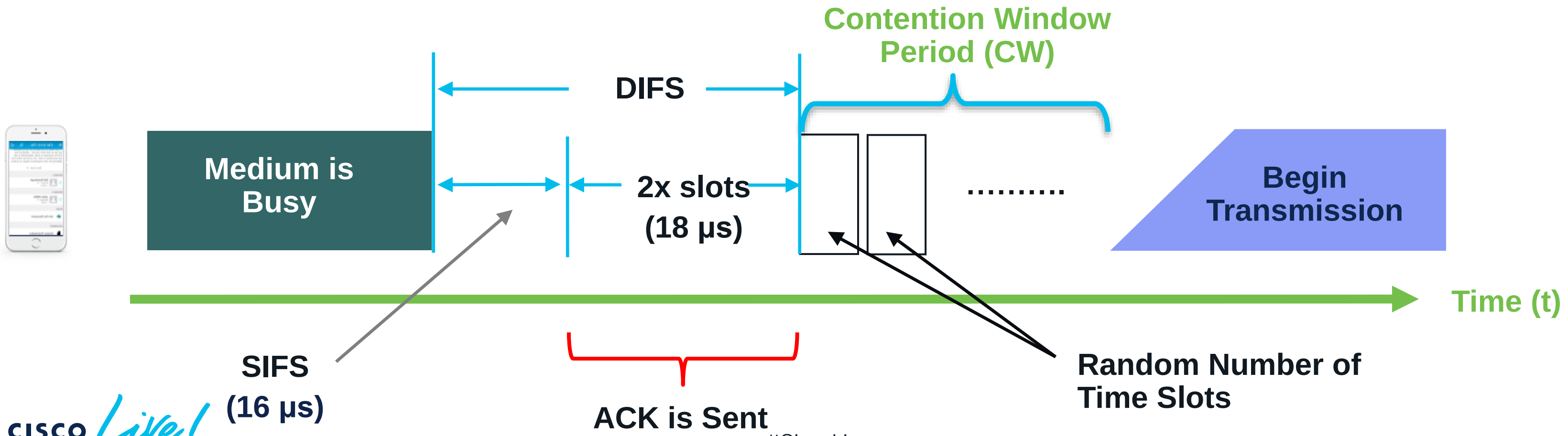


Wi-Fi Media Access is Contention-Based



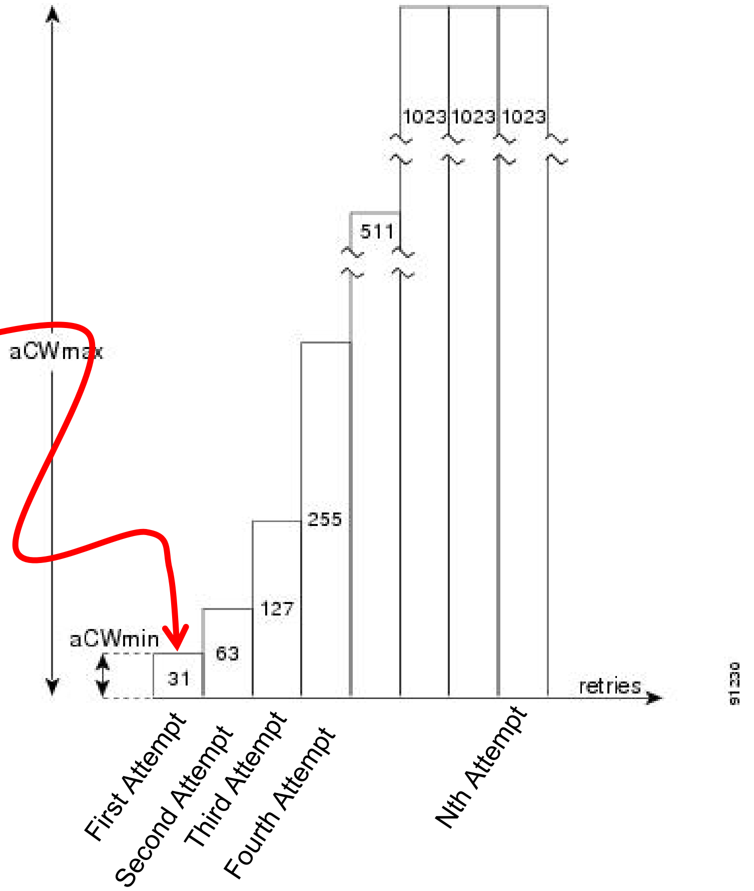
Distributed Coordination Function (DCF)

- 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

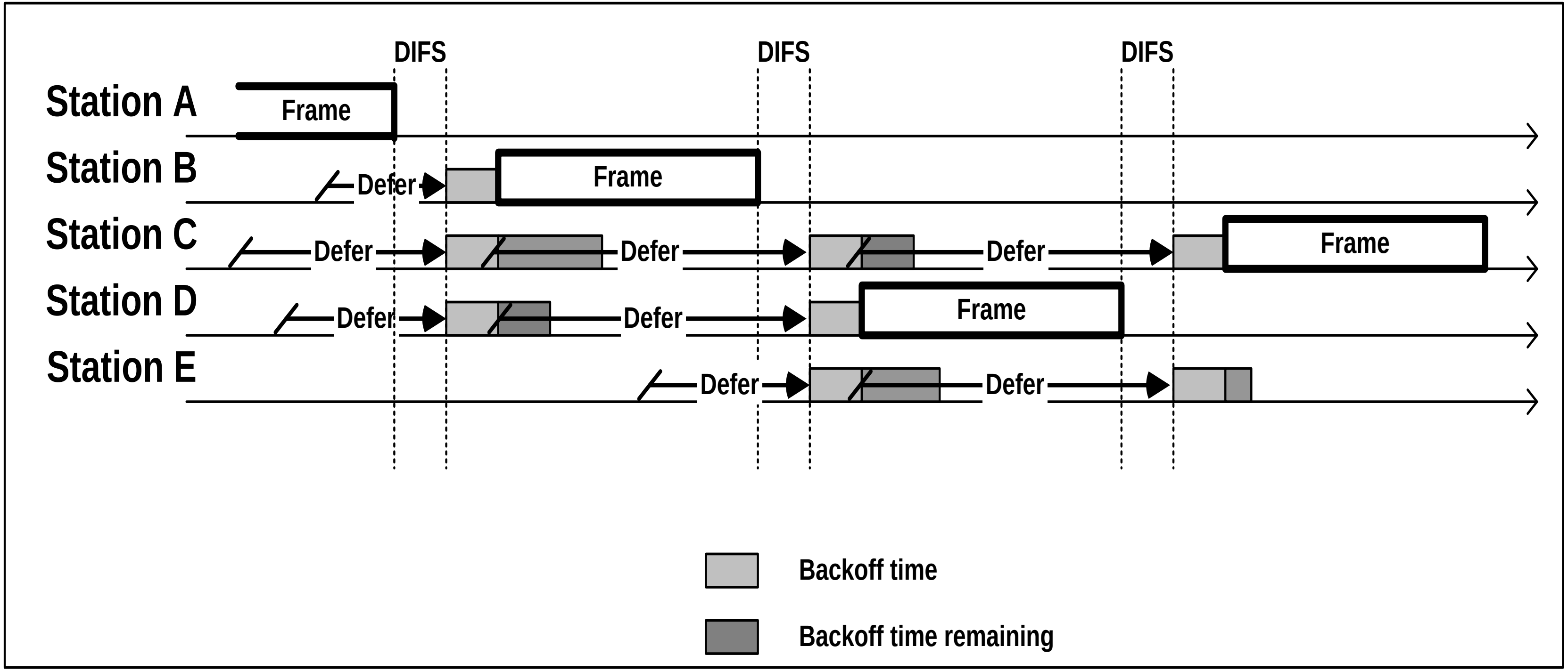


What if Your Frame Doesn't Get Ack'd?

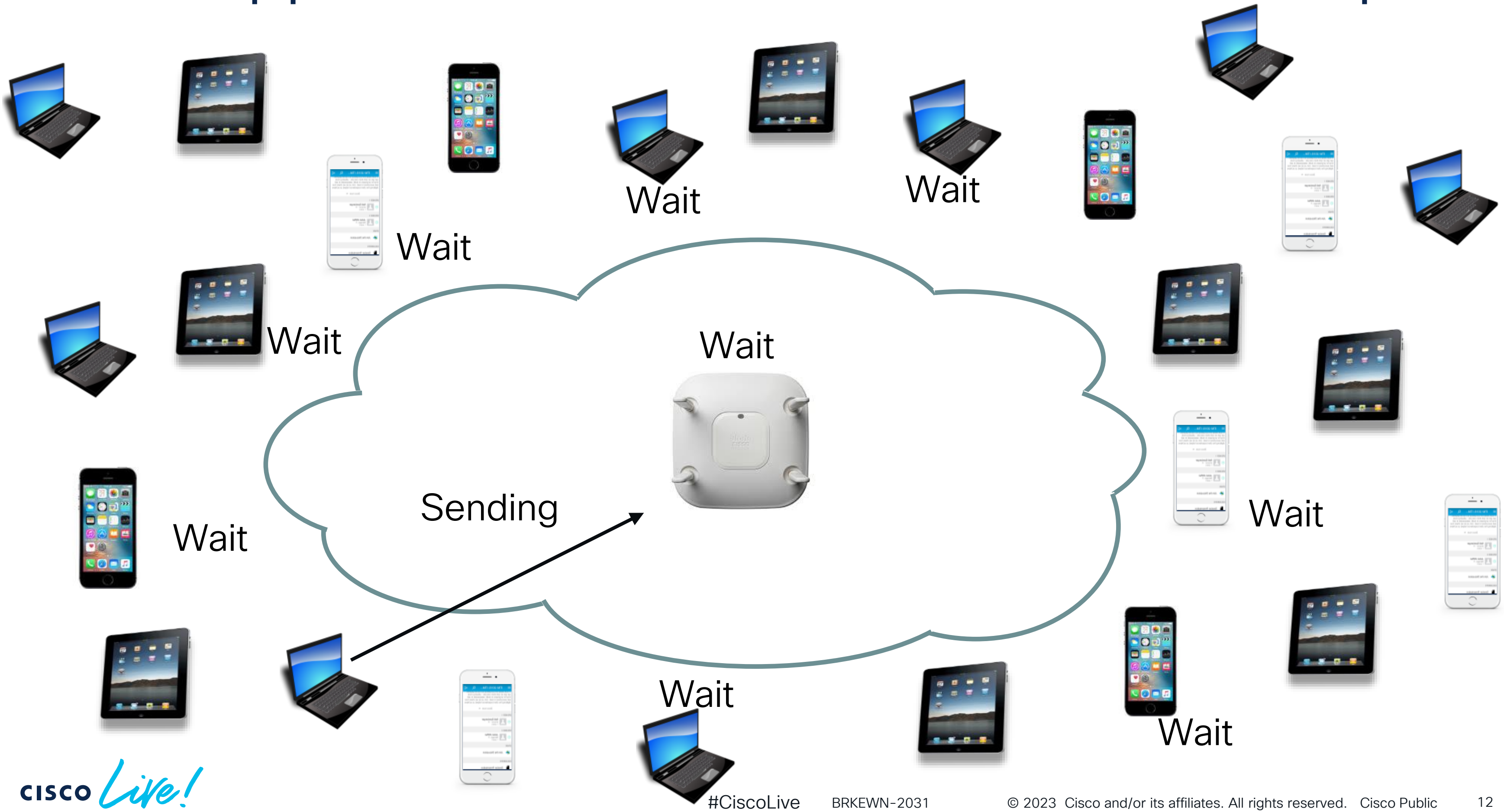
- How do you know the transmission got through okay? The receiving station must send an acknowledgment.
- If the first attempt didn't work (no ACK received), double the previous CW size and pick a new random number.
  - Keep doing this until the CW reaches a maximum size of 1023 slot times.
- How many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



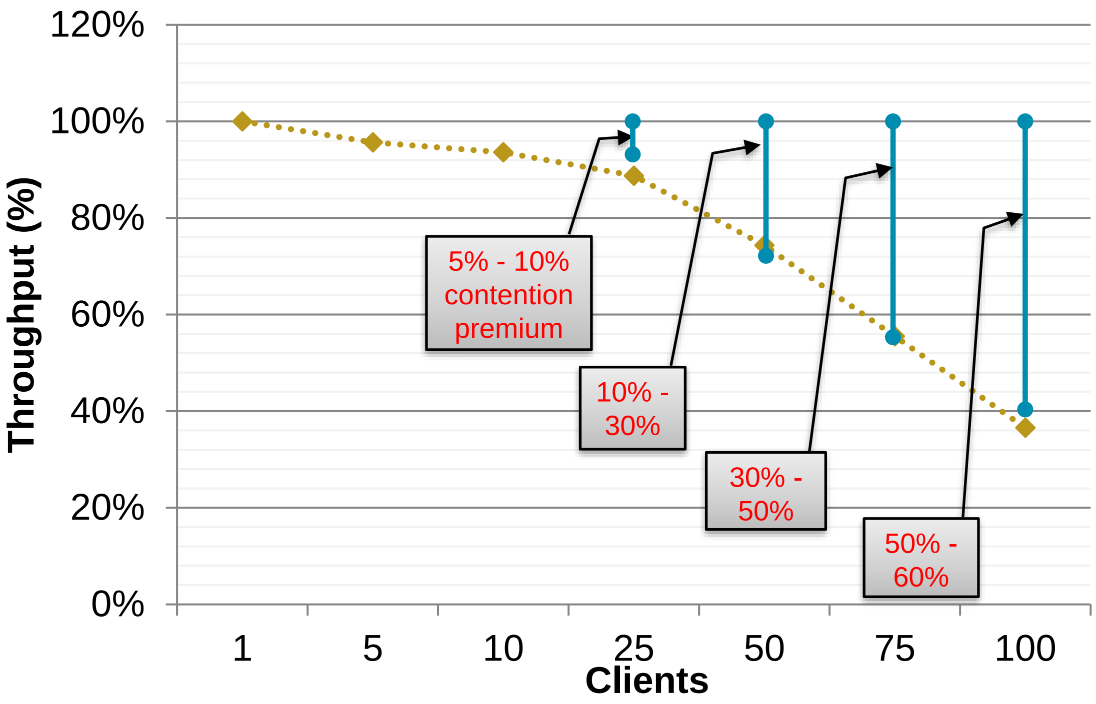
Simplified Example - DCF In Action:



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

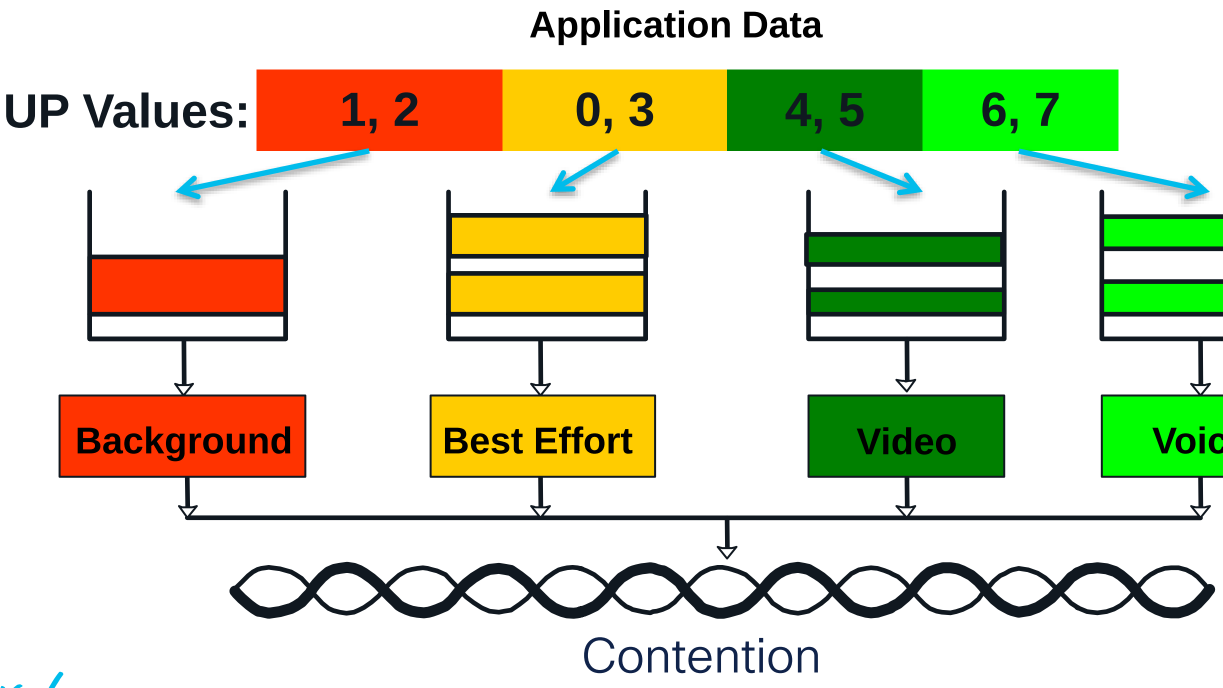
Legacy QoS:
The Enhanced Distributed Channel Access (EDCA) Model

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

RFC 8325
Mapping DiffServ to IEEE 802.11

- Reconciles RFC 4594 with IEEE 802.11
- Summarizes our internal consensus on DSCP-to-UP mapping
- Advocates DSCP-trust in the upstream direction
(vs. UP-to-DSCP mapping)

https://tools.ietf.org/html/rfc8325

Internet Engineering Task Force (IETF)
Request for Comments: 8325
Category: Standards Track
ISSN: 2070-1721

T. Szigeti
J. Henry
Cisco Systems
F. Baker

February 2018

Mapping Diffserv to IEEE 802.11

Abstract

As Internet traffic is increasingly sourced from and destined to wireless endpoints, it is crucial that Quality of Service (QoS) be aligned between wired and wireless networks; however, this is not always the case by default. This document specifies a set of mappings from Differentiated Services Code Point (DSCP) to IEEE 802.11 User Priority (UP) to reconcile the marking recommendations offered by the IETF and the IEEE so as to maintain consistent QoS treatment between wired and IEEE 802.11 wireless networks.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8325.

#2 Assign Backoff Timers for the Access Category

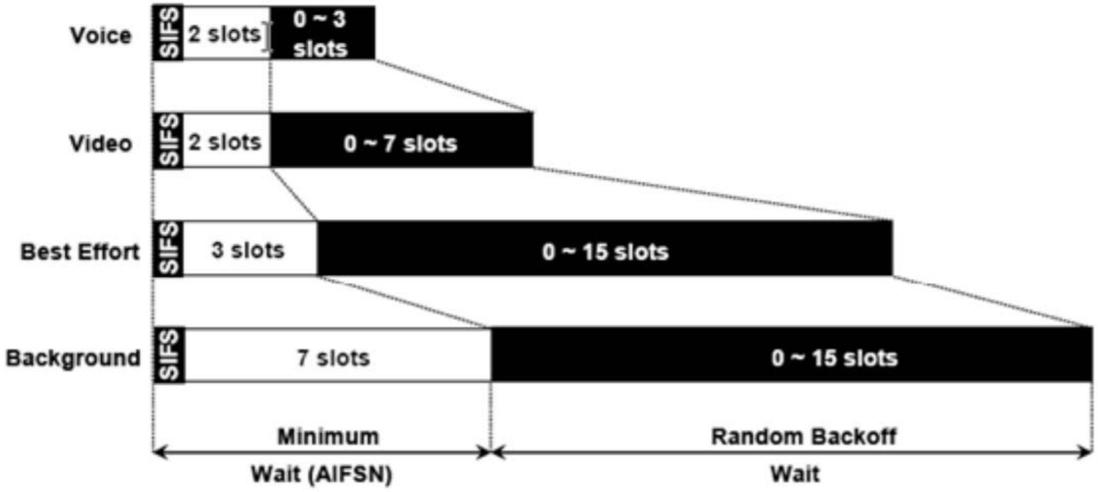
- EDCA manages the ACs in the following way:
  - Variable Arbitration Interframe Spacing (AIFS)
  - Variable CW_{min} and CW_{max} values depending on traffic type
  - Values shown are “slot times” – 9µs per slot in 802.11

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

*For 802.11a/g. 802.11b uses 31

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.



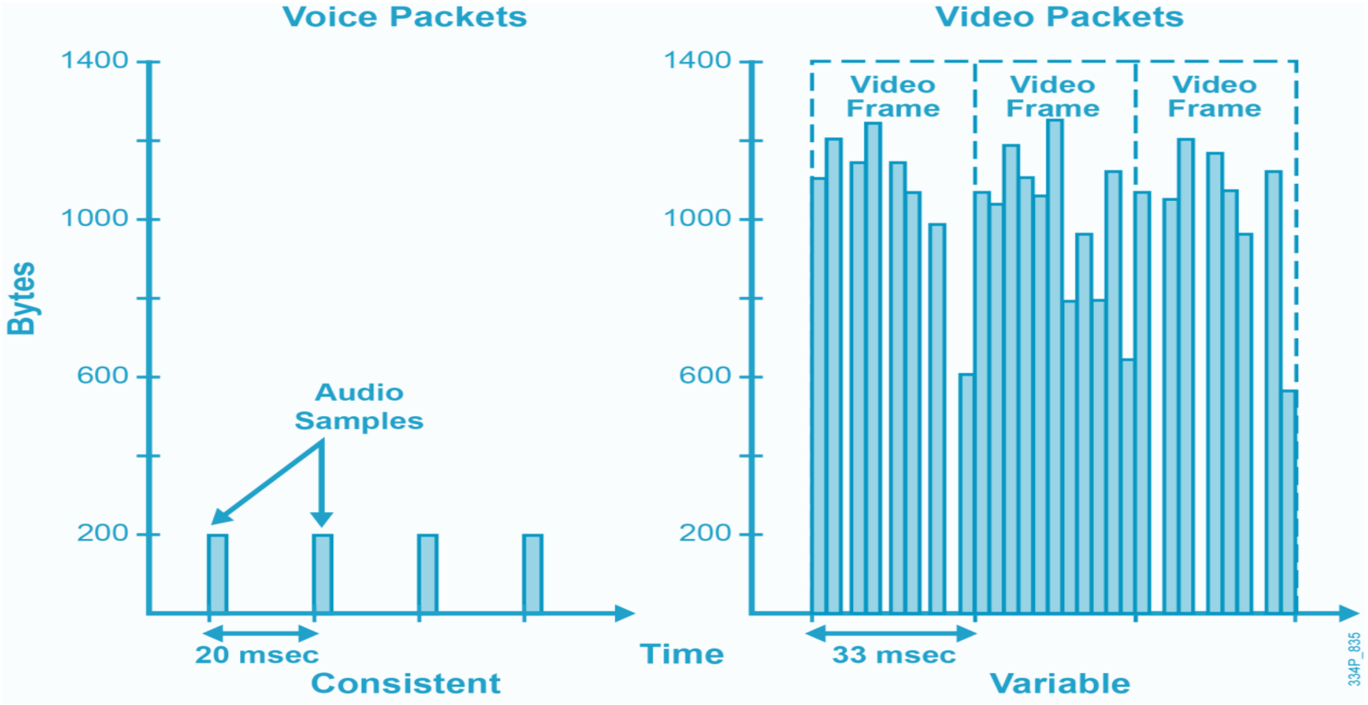
#3 Transmission Opportunity (TXOP)

- 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!
- Why is video smaller than the other TXOPs?

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

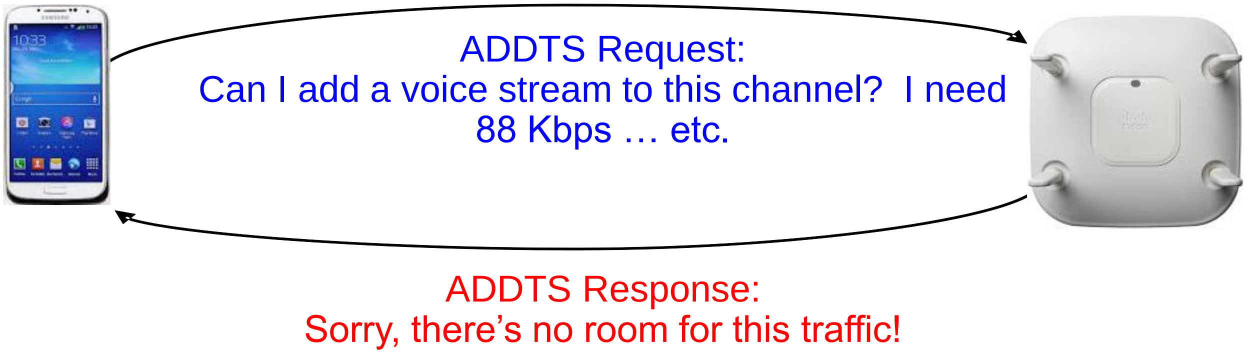
Real Time Voice vs. Real Time Video Traffic Profile

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



Summary: Four Key 802.11e QoS Enhancements

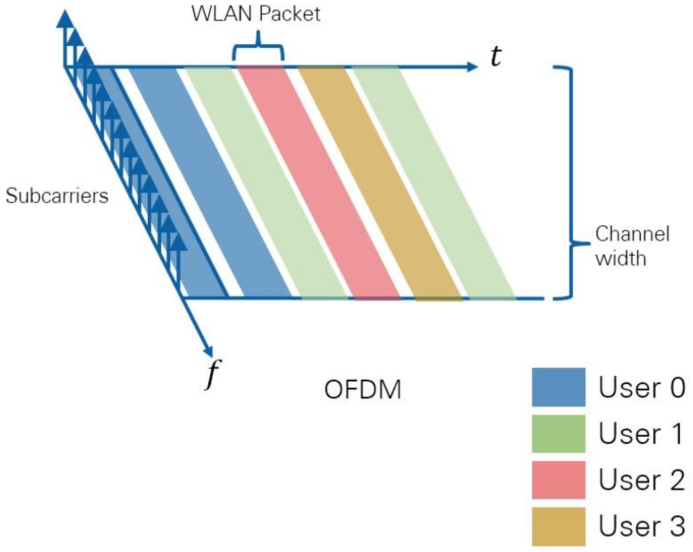
Enhanced Distributed Channel Access (EDCA):

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)

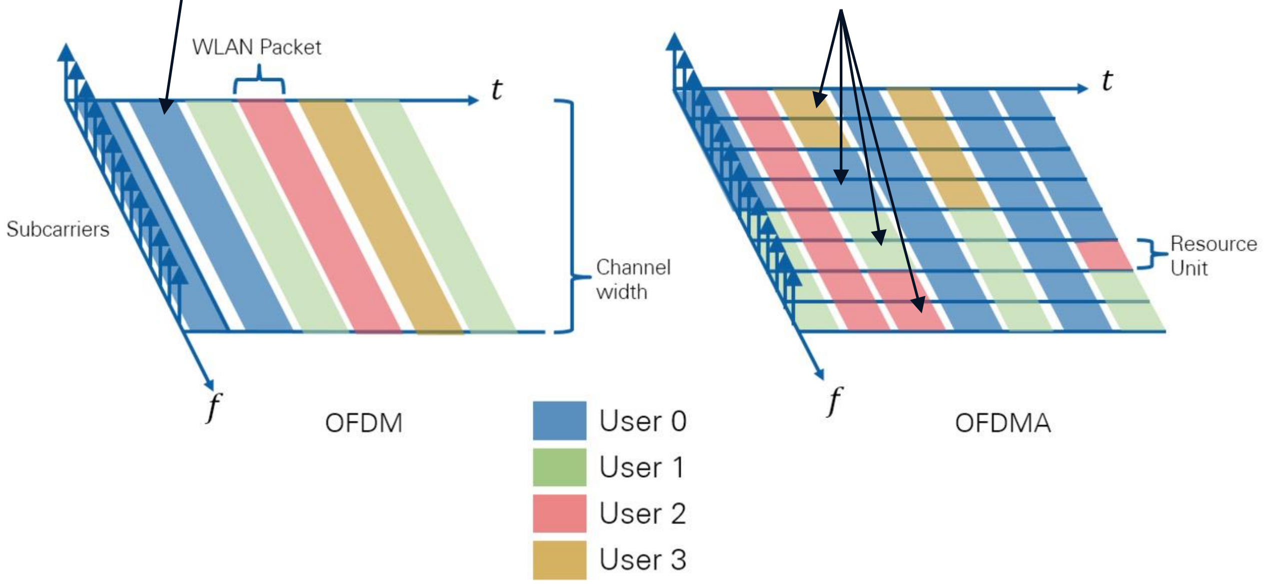
- Subcarriers (Resource Units – RUs) can be assigned to different users for uplink transmissions
  - Can be combined with UL MU MIMO



OFDMA (Orthogonal Frequency Division Multiple Access)

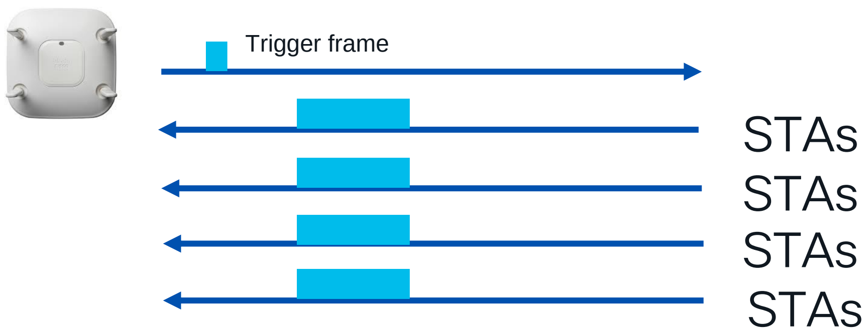
A Single Station Transmits in a Timeslot won by the contention algorithm (EDCA)

Multiple Stations Transmit in a scheduled Timeslot



802.11ax Uplink (UL) MU-MIMO

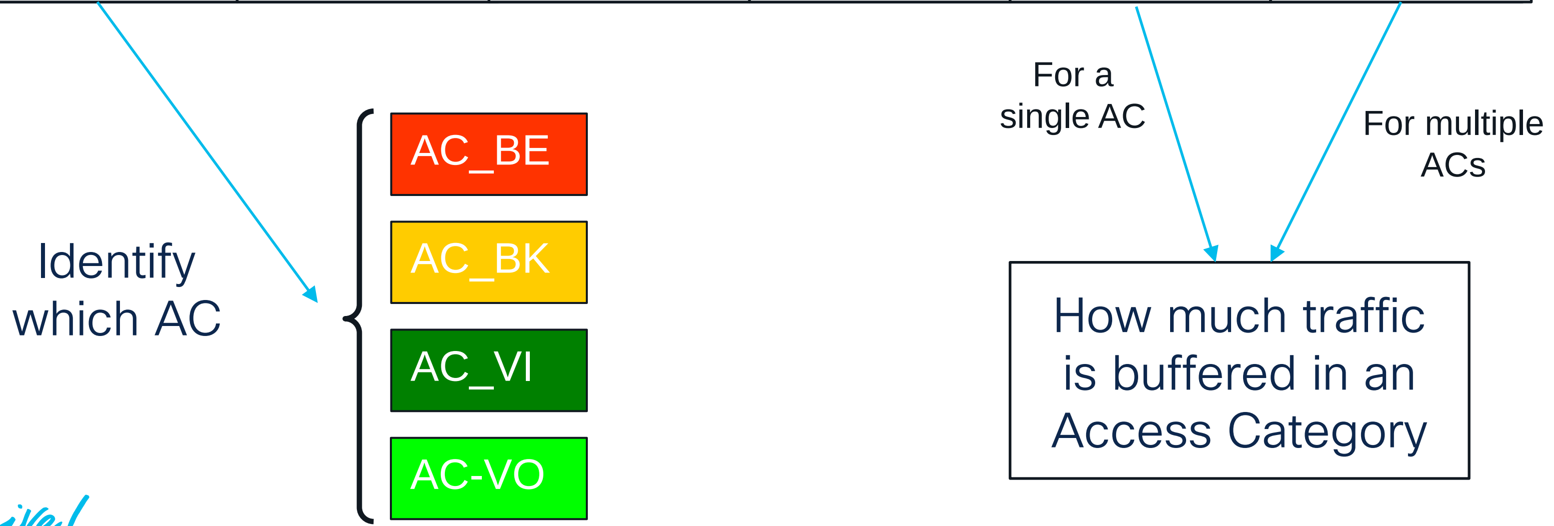
- 802.11ac allows for downlink MU-MIMO
- 802.11ax adds uplink MU-MIMO
  - AP checks which STAs can send together
  - AP sends trigger frame and STAs respond all at the same time



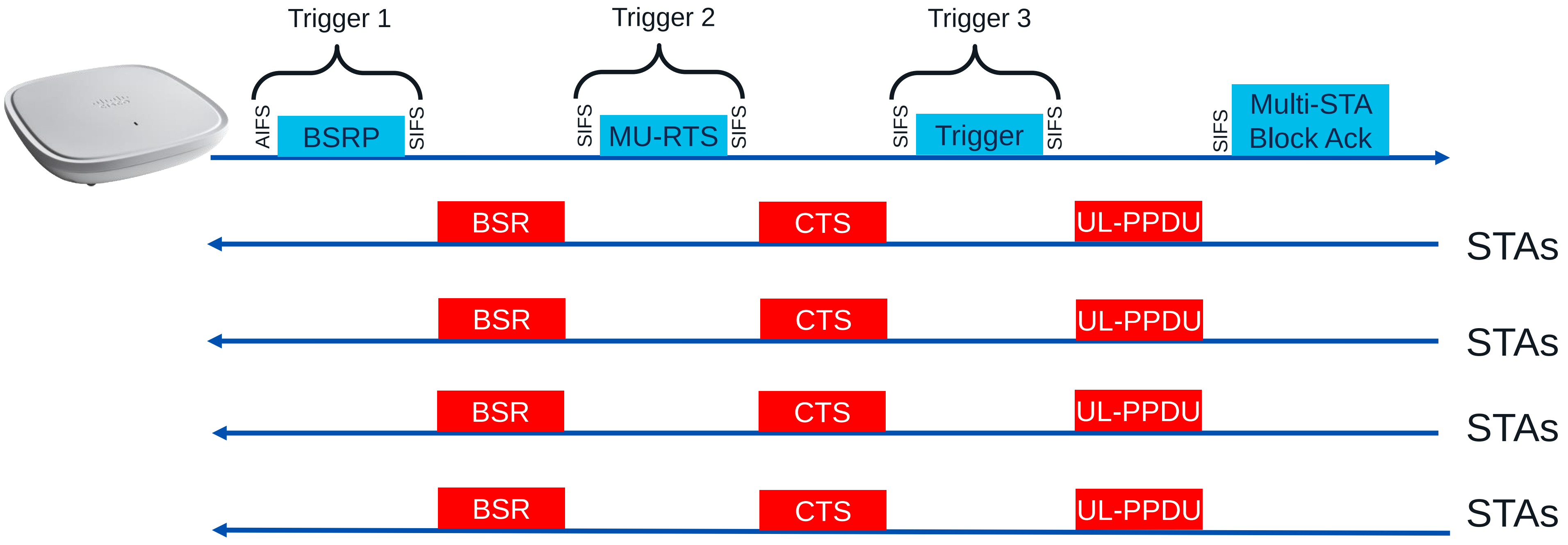
Buffer Status Reports (BSRs)

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

Bits:	4	2	2	2	8	8
	ACI Bitmap	Delta TID	ACI High	Scaling Factor	Queue Size High	Queue Size All

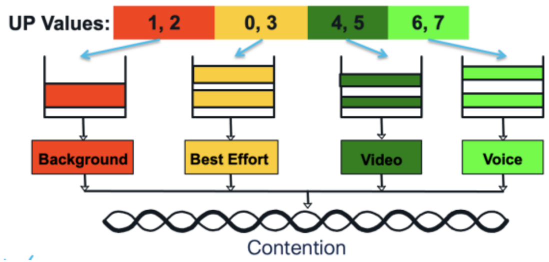


Buffer Status Report Polling (BSRP)
(Figuring out how many RUs to Assign)

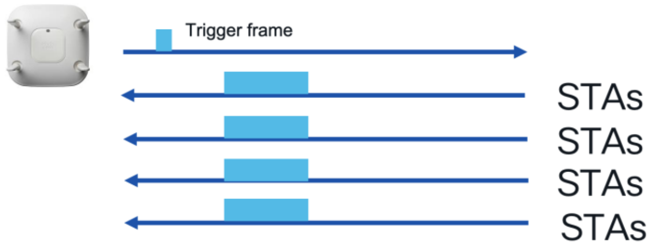


How Does This Work in Mixed Environments?

- 6GE spectrum is safe – only 11ax clients can work in this spectrum!
- In the lower bands, the AP will need to contend with legacy clients to win the EDCA algorithm so it can perform OFDMA / Multi-User Uplink
  - Over time, as legacy clients go away the medium will shift to a predominant OFDMA model (good)



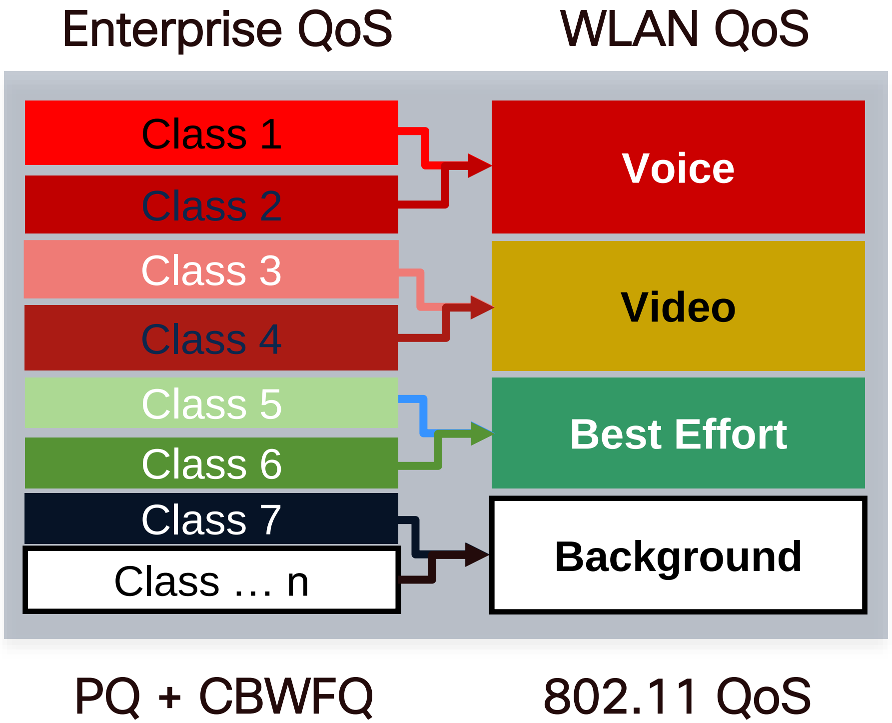
Vs.



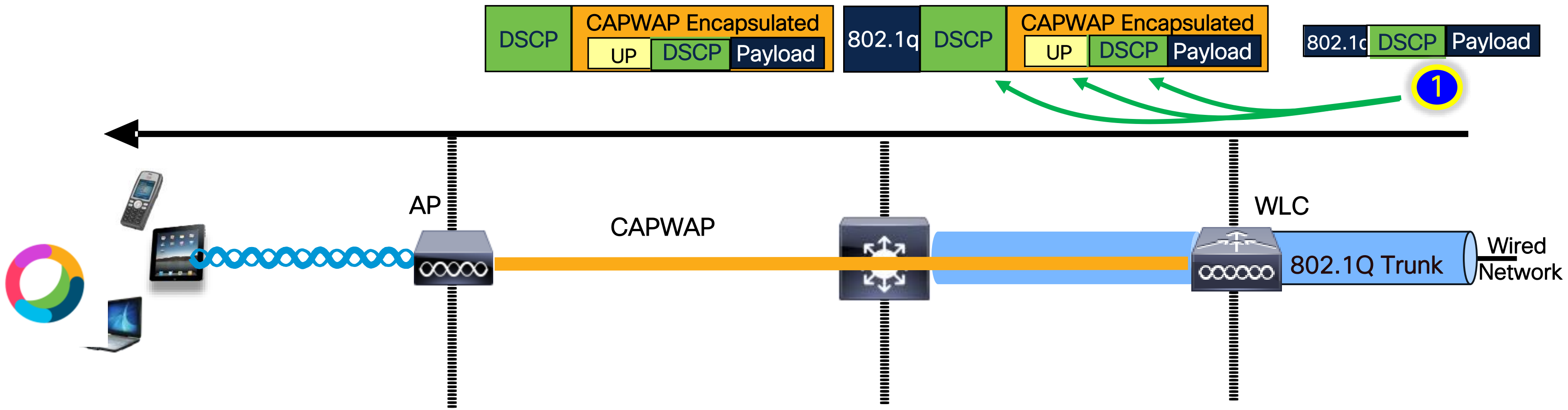
IOS-XE / Catalyst 9800 QoS Deployment

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



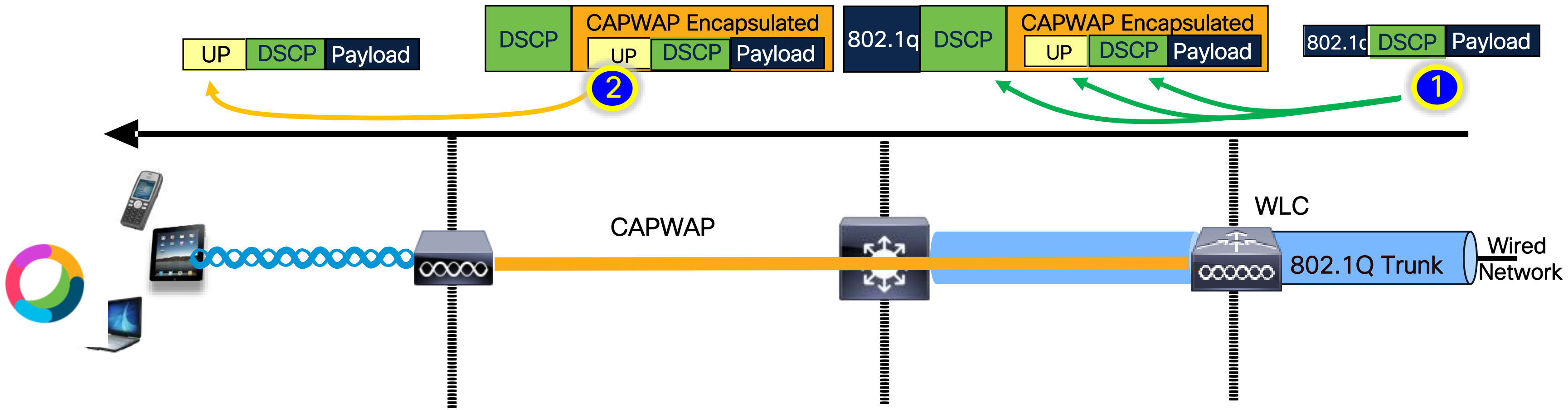
Catalyst 9800 Downstream QoS Model



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

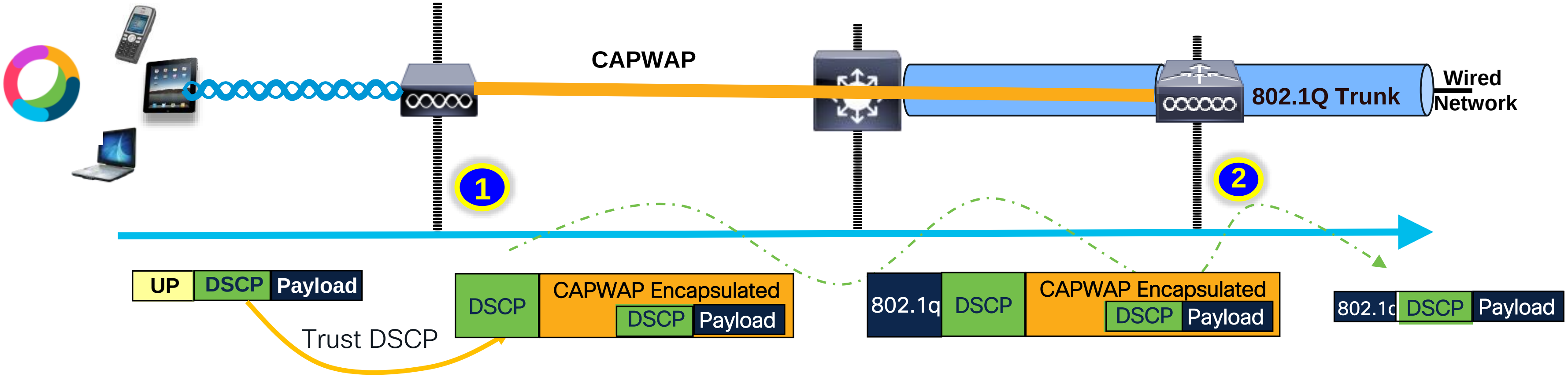


1. The client packet is received over an 802.1q trunk by the WLC. The WLC uses the DSCP value of the original IP packet and maps it to the outer DSCP of the CAPWAP tunnel (assuming no ceiling value is applied via Metal QoS at the WLC). It also maps DSCP to UP and set it in the inner 802.11e header

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

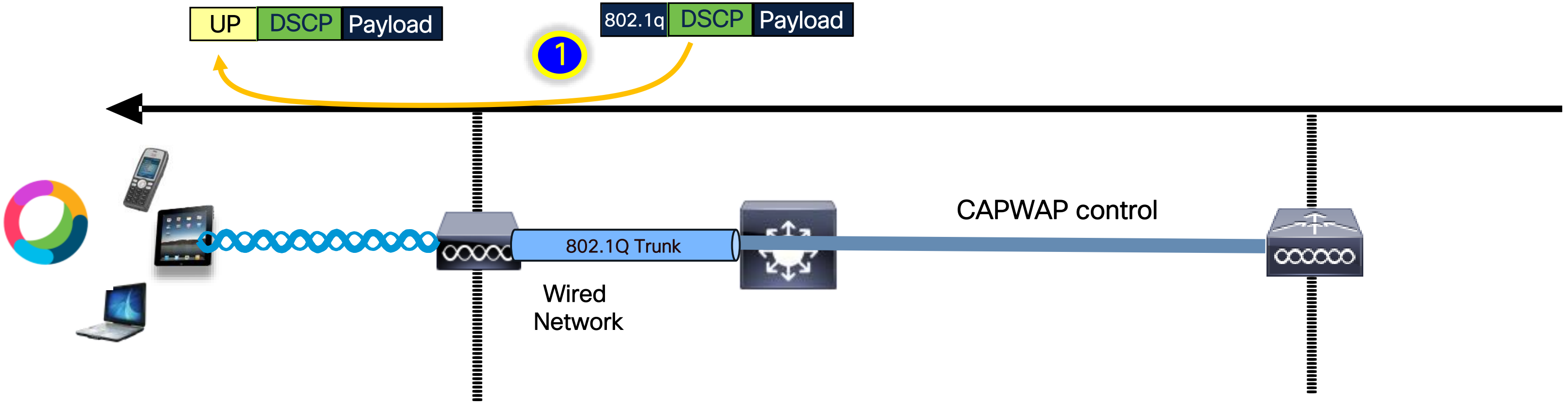
Catalyst 9800 Upstream QoS Model

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)

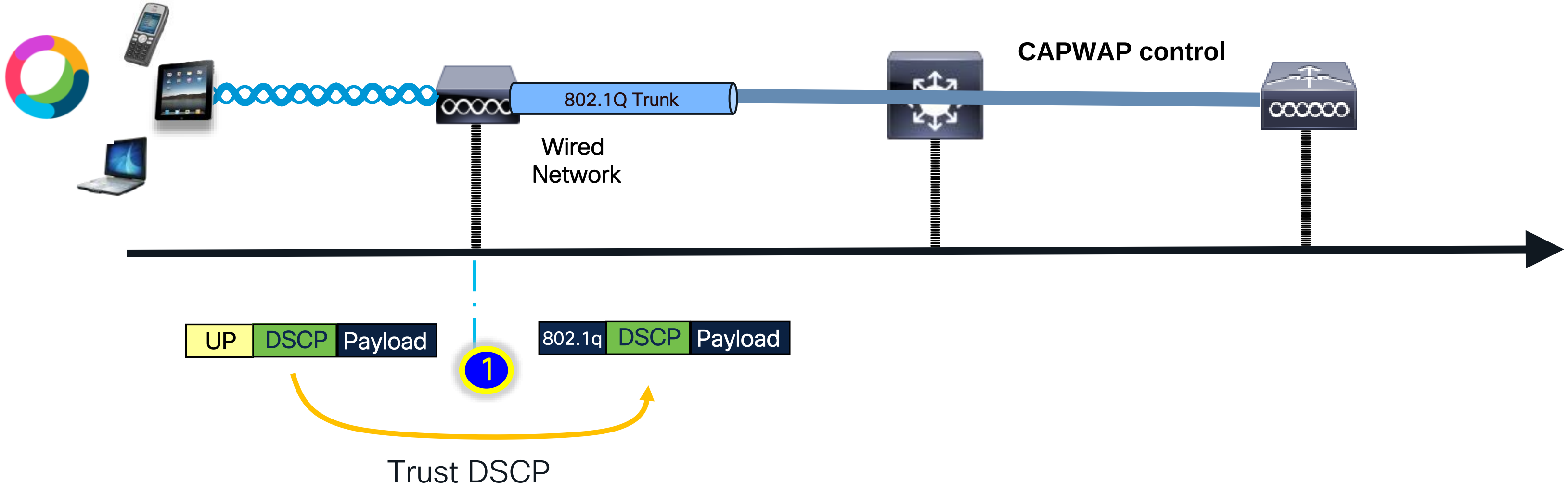
Downstream QoS Variant: Flex Local Switching



1 Once the Ethernet frame is received, the AP takes the DSCP value of the IP packet, process any QoS policy (e.g., AVC policy), maps it to the 802.11e UP value on the wireless frame and queue the frame accordingly. The frame is then sent to the client.

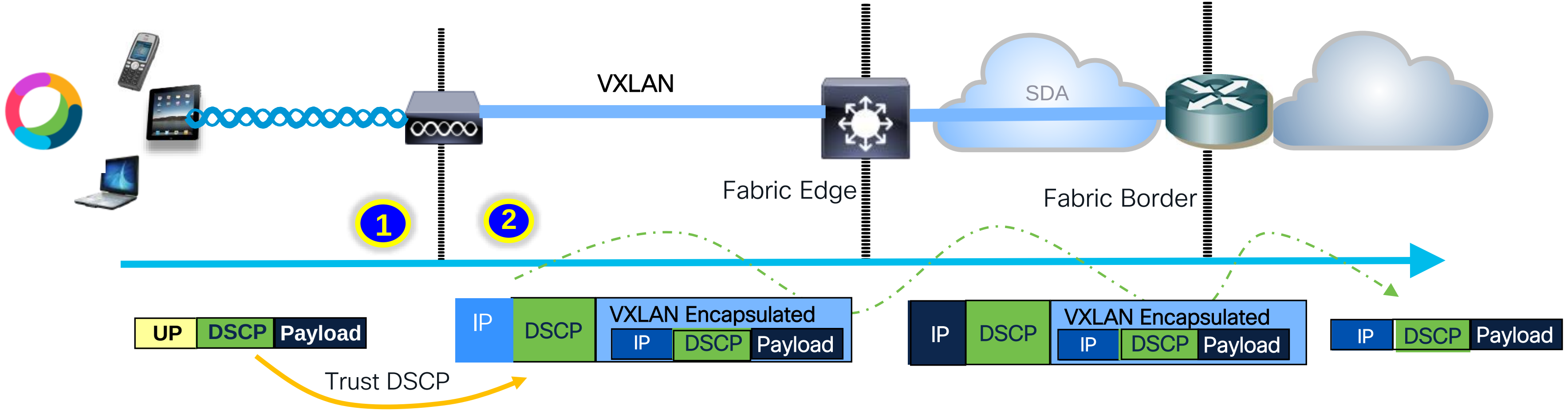
Upstream QoS Variant: Flex Local Switching

1 The client 802.11e frame is received by the AP. The AP looks at the original packet DSCP to apply any QoS policy before sending the packet onto the wire



Upstream QoS Variant 2: SDA Fabric

1. The client 802.11e frame is received by the AP. The AP utilizes the DSCP value in the original IP packet for internal QoS processing and then maps it to the outer VXLAN header(*)
2. This allow preservation of the DSCP value from the client all the way through the network, emerging untouched from the Border (assuming no Metal QoS or AVC policy is applied to remark DSCP)



(*) Before release 17.4, you need to explicitly configure "qos-map trust-dscp-upstream" under the AP join profile. If this setting is not there, the AP will use the UP value in the received frame to derive the outer DSCP value of the VXLAN header

Under the Hood:
Catalyst 9800 IOS-XE is Based on Modular QoS

- Catalyst QoS model is based on **Modular QoS CLI (MQC)**
- In IOS-XE, **MQC** is used to implement the Differentiated Service model QoS
- The main MQC constructs:
  - **Class-map:** to classify traffic
  - **Policy-map:** to bind traffic class to actions
  - **Service-policy:** to attach policy-map to target/direction

Classification ACL

```
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
 10 permit udp any eq 5246 16666 any
```

Class-map definition

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
 match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
 match dscp ef
```

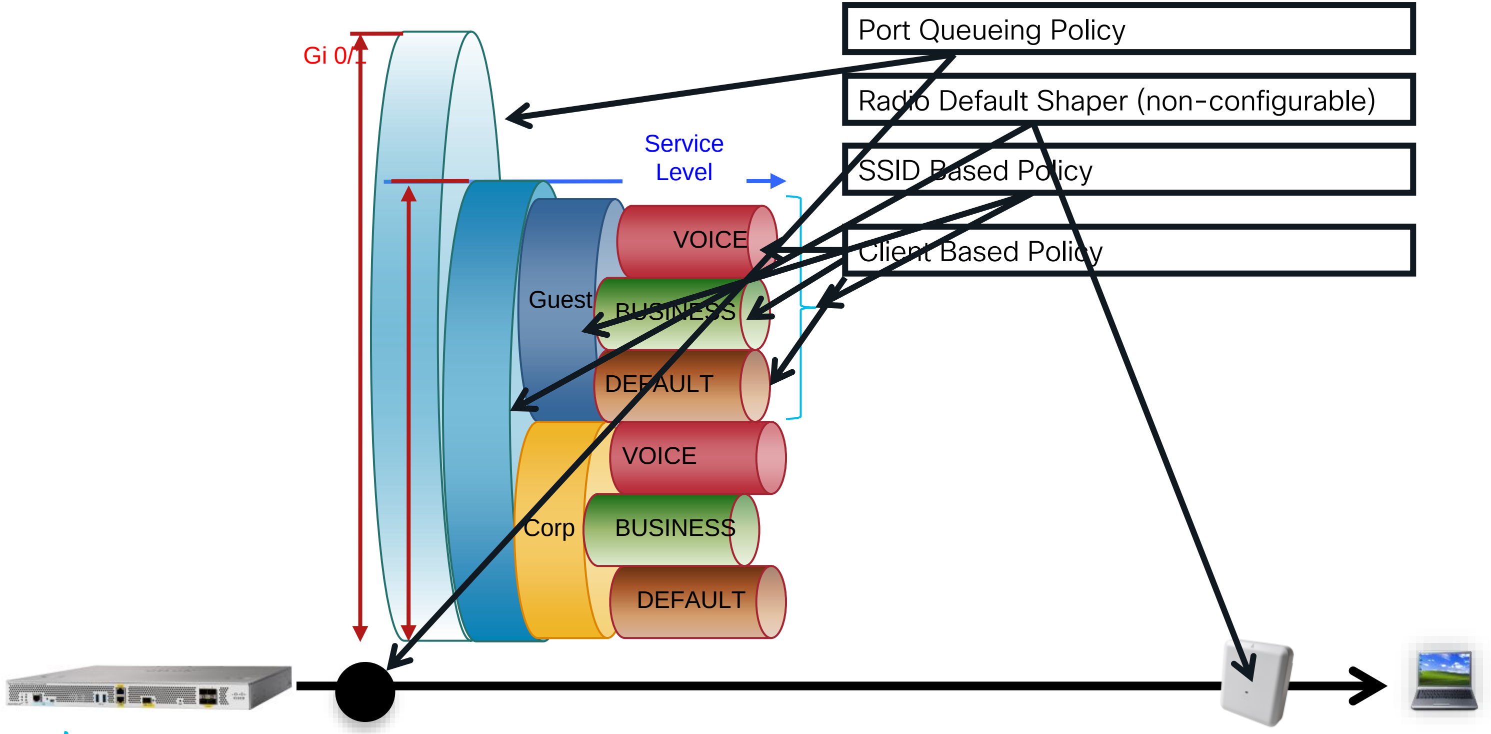
Policy-map definition

```
policy-map AutoQos-4.0-wlan-Port-Output-Policy
 class AutoQos-4.0-Output-CAPWAP-C-Class
  priority level 1
 class AutoQos-4.0-Output-Voice-Class
  priority level 2
 class class-default
```

Service-policy attachment

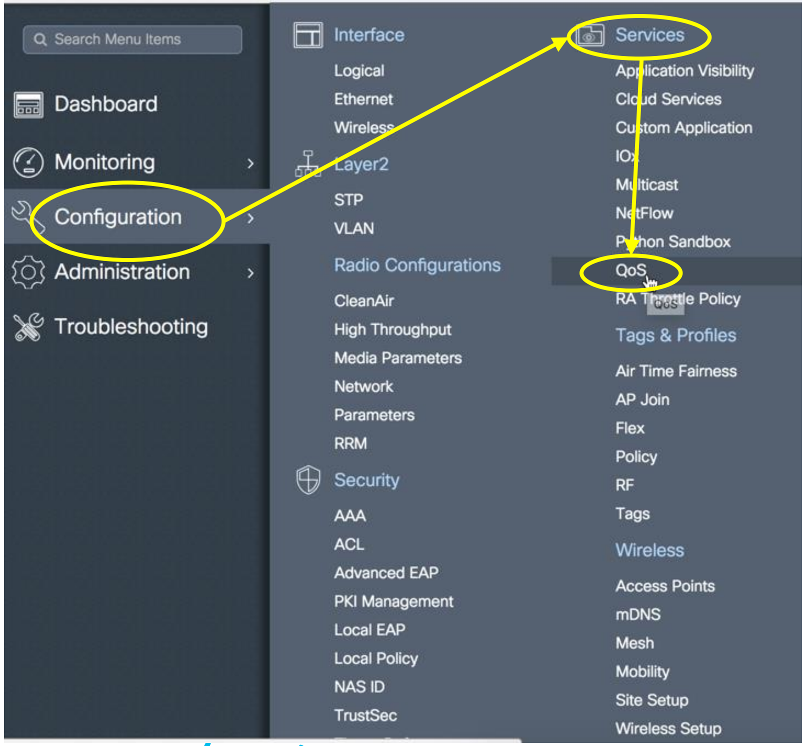
```
interface TenGigabitEthernet0/0/0
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
```

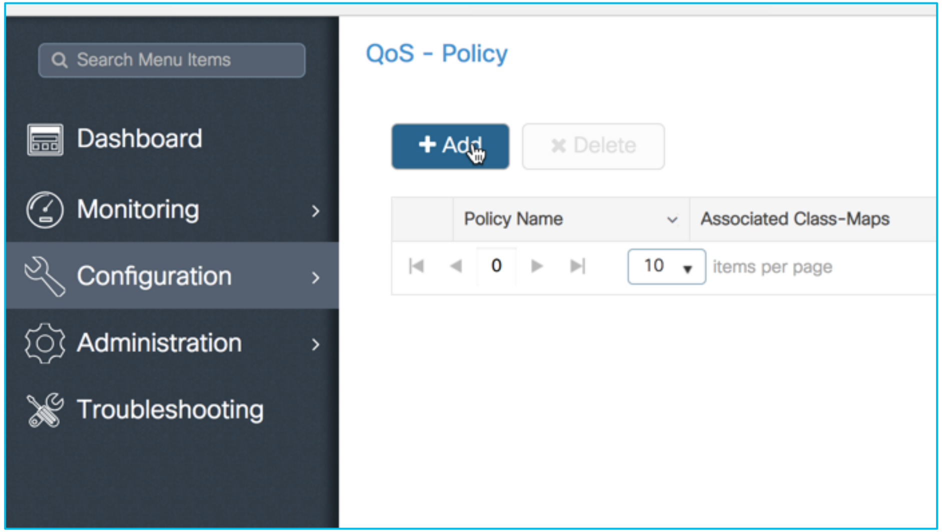
Controller Hierarchical Wireless QoS



Configuring QoS on the Catalyst 9800 Controller

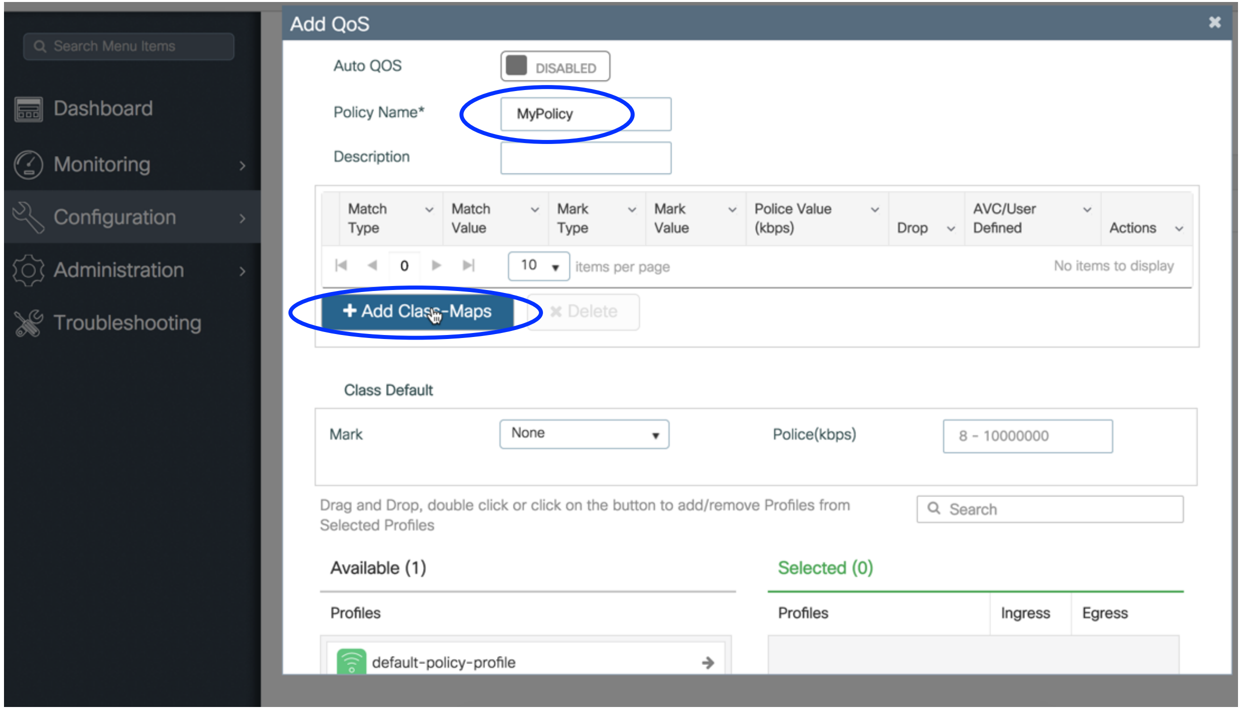
Begin by Navigating to Services > QoS and Add a new policy





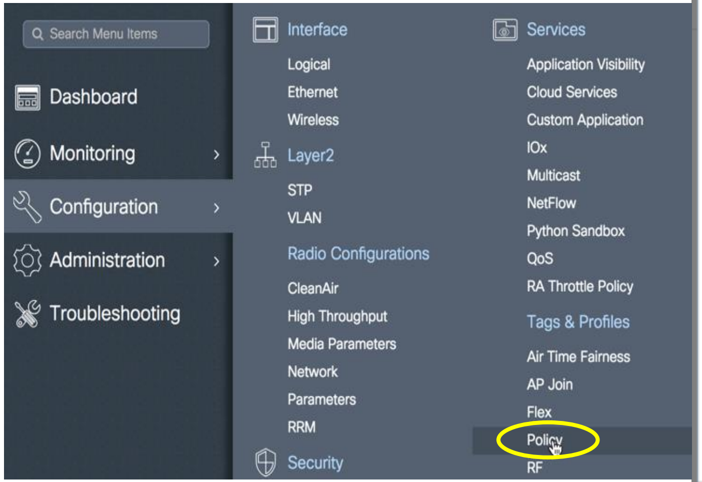
QoS Policy Workflow

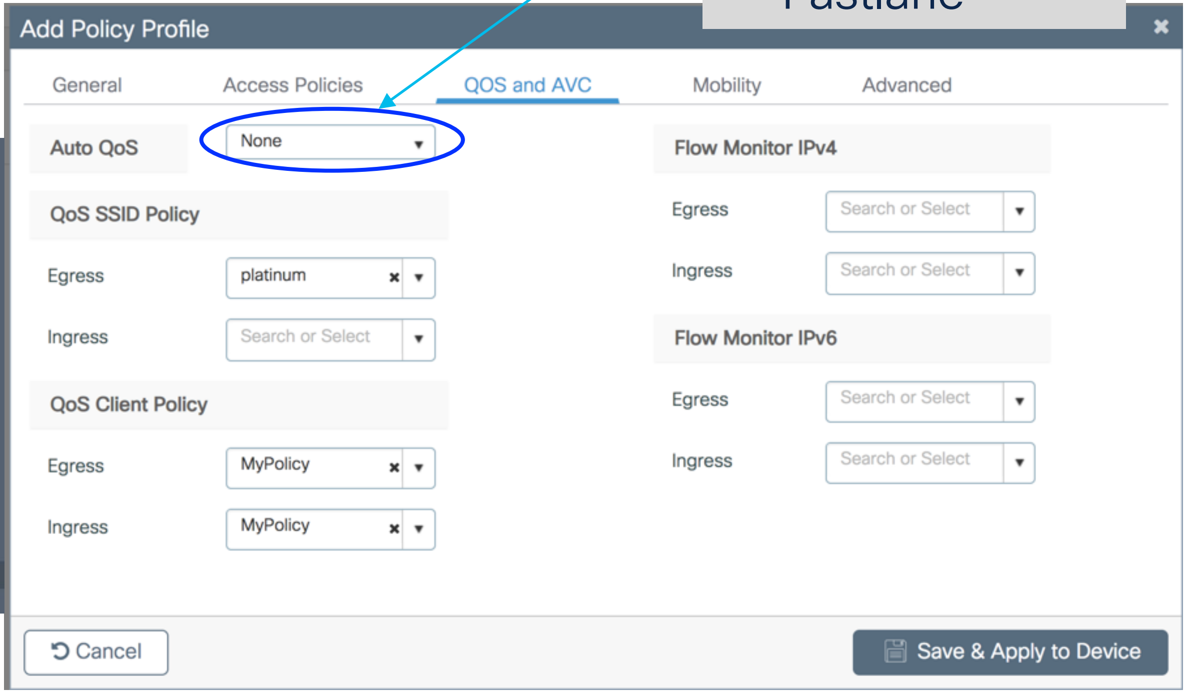
Name your policy, add applications (Class-maps)



Making Things Easy with Auto QoS

- None
- Guest
- Enterprise
- Voice
- Fastlane

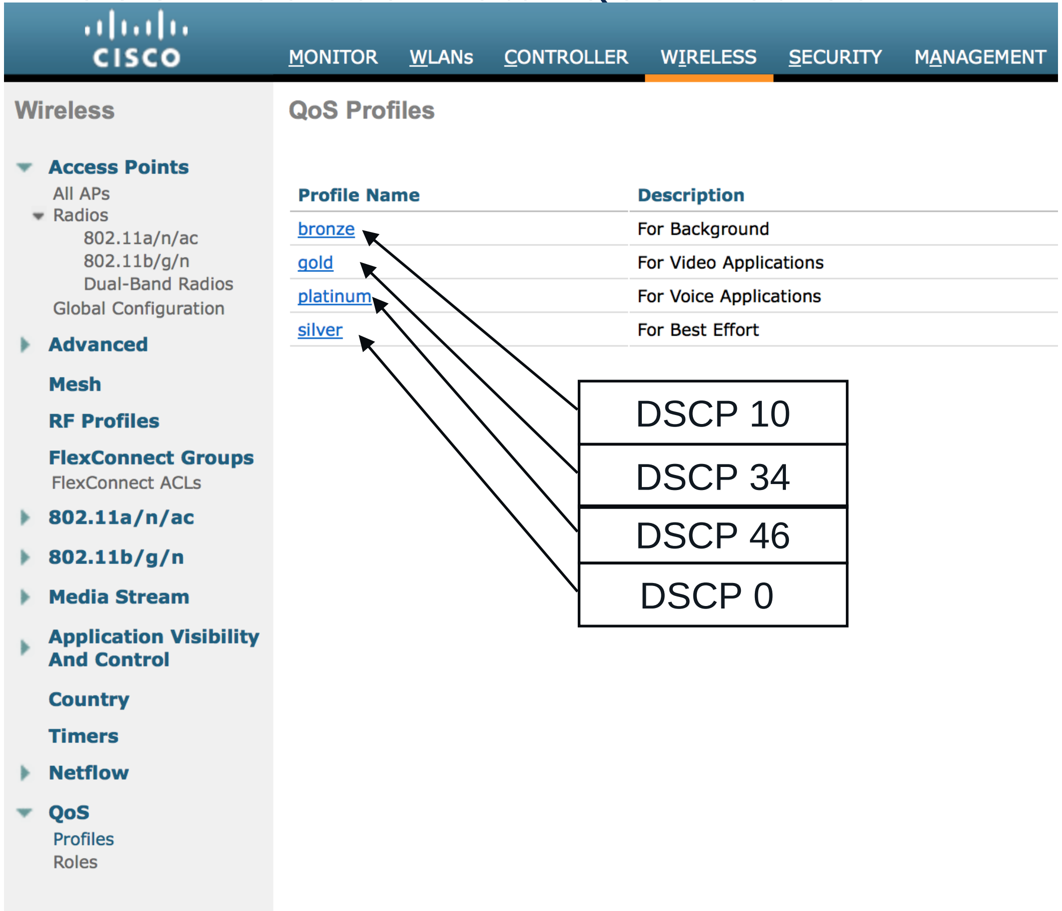




Catalyst 9800 Auto QoS – explained

- Voice: sets the recommended QoS policy to correctly mark and prioritize voice at the SSID 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.
    - With All options 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"

Remember this?
AireOS Precious Metal QoS Method

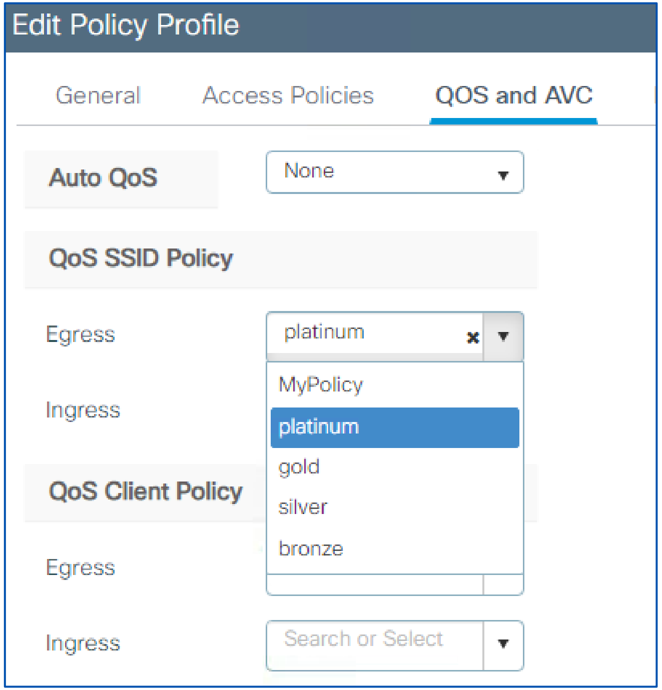


- The main purpose of the QoS profile is to limit the maximum DSCP allowed on a CAPWAP tunnel, and thus limit the 802.11 UP value
- QoS profiles may be used and applied to each WLAN (SSID)

Catalyst 9800 – Improving Metal QoS Profiles

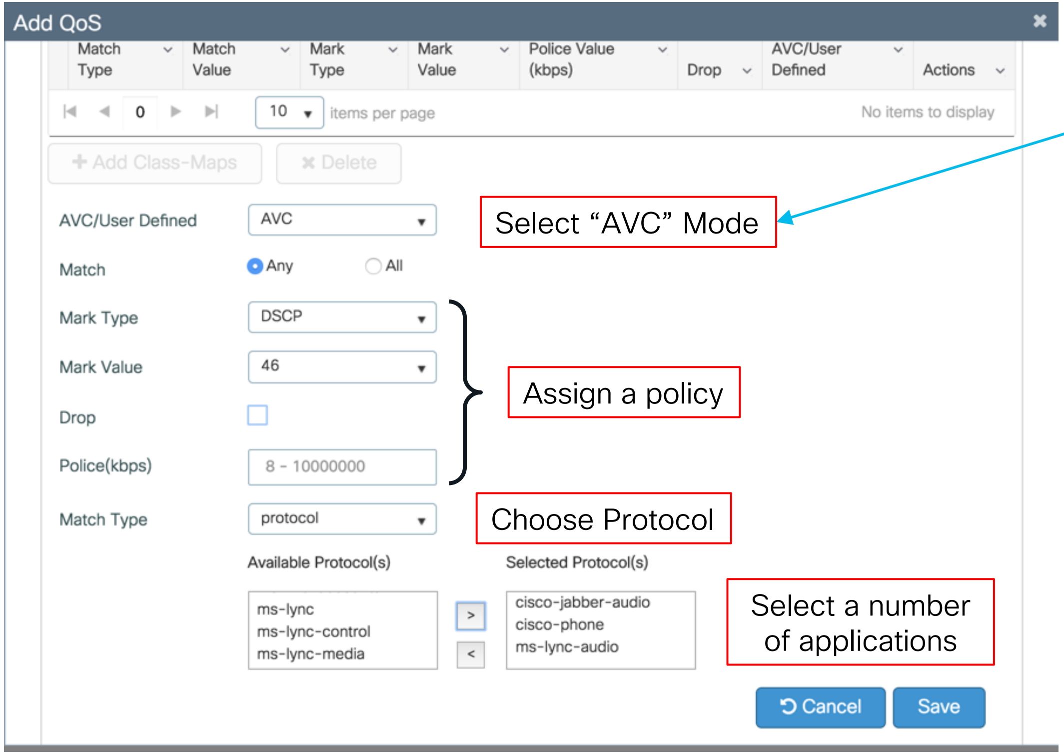
- QoS Metal Profiles in C9800:
  - For C9800 you can apply Metal QOS on Egress and Ingress direction separately
  - On the GUI, you can only set the Metal QoS per SSID. On CLI you can also configure it on client target
  - For each profile, a max DCSP setting is used to remark any traffic in excess of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

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



AVC QoS Workflow

Add applications and assign a policy



You can also choose User Defined and input application ports

Cat 9800 Custom AVC Capabiliites

Custom apps and attributes can be defined by the user

Custom IP, Port, DSCP

```
eWLC-AVC(config)#ip nbar custom customapp transport udp
eWLC-AVC(config-custom)#?
Custom protocol commands:
  direction   Flow direction
  dscp        DSCP in IPv4 and IPv6 packets
  exit        Exit from custom configuration mode
  ip          ip address
  ipv6        ipv6 address
  no          Negate a command or set its defaults
  port        ports
```

Example:

C9800(config)#ip nbar custom my_app **transport** udp

C9800(config-custom)# **ip address** 9.9.71.50 9.9.71.11 9.9.71.14

C9800(config-custom)# **port** 1111

C9800(config-custom)# **dscp** 0

C9800(config-custom)# **direction** any

Custom HTTP Host and URL

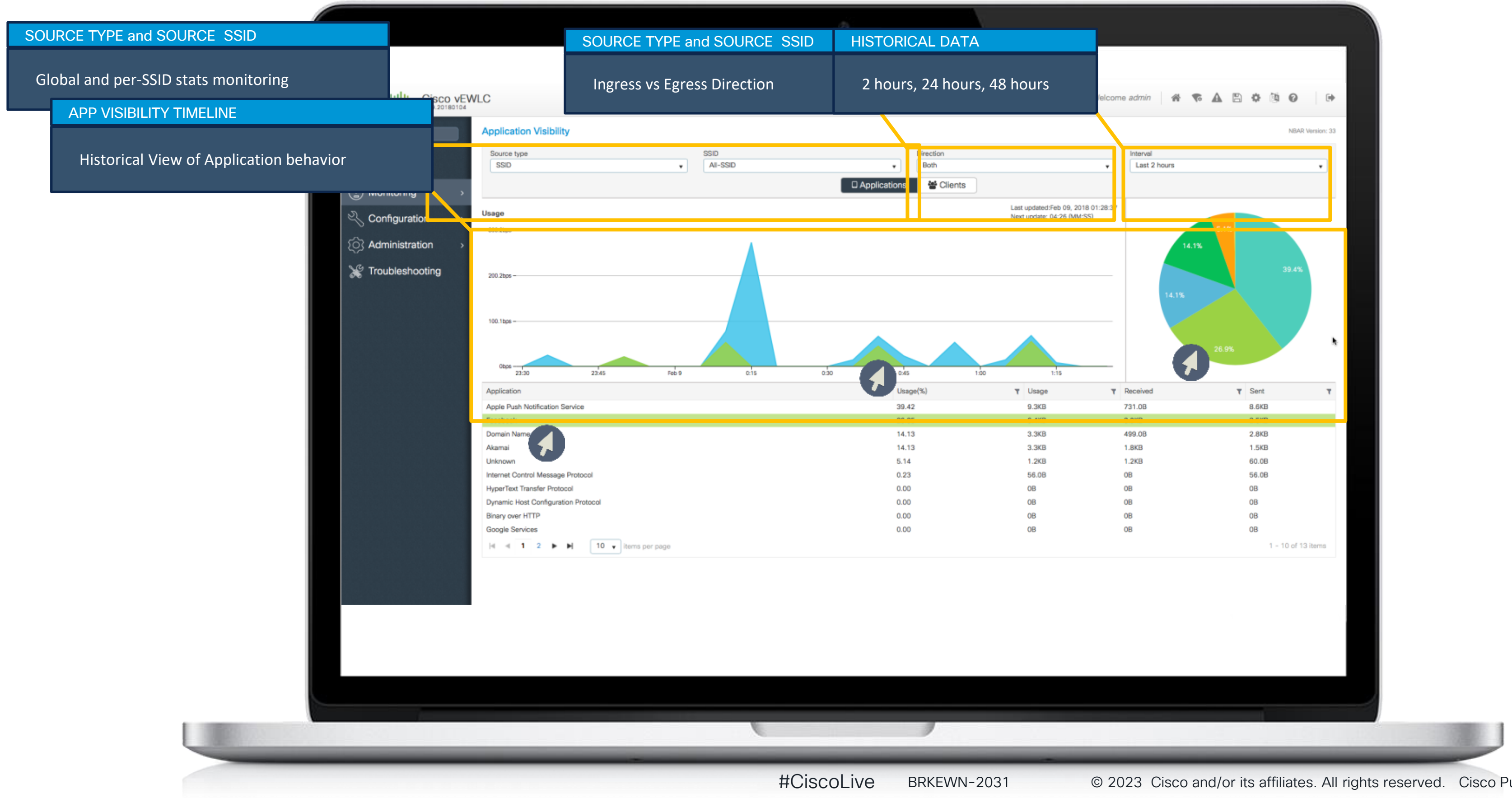
C9800(config)#ip nbar custom my_http http **url** “latest/whatsnew.html”

C9800(config)#ip nbar custom my_http http **host** “www.anydomain.com”

C9800(config)#ip nbar custom my_http http **url** “latest/whatsnew” **host** “www.anydomain.com”

The URL or host specification strings can take the form of a **regular expressions**

Improved AVC Visualization and Reporting



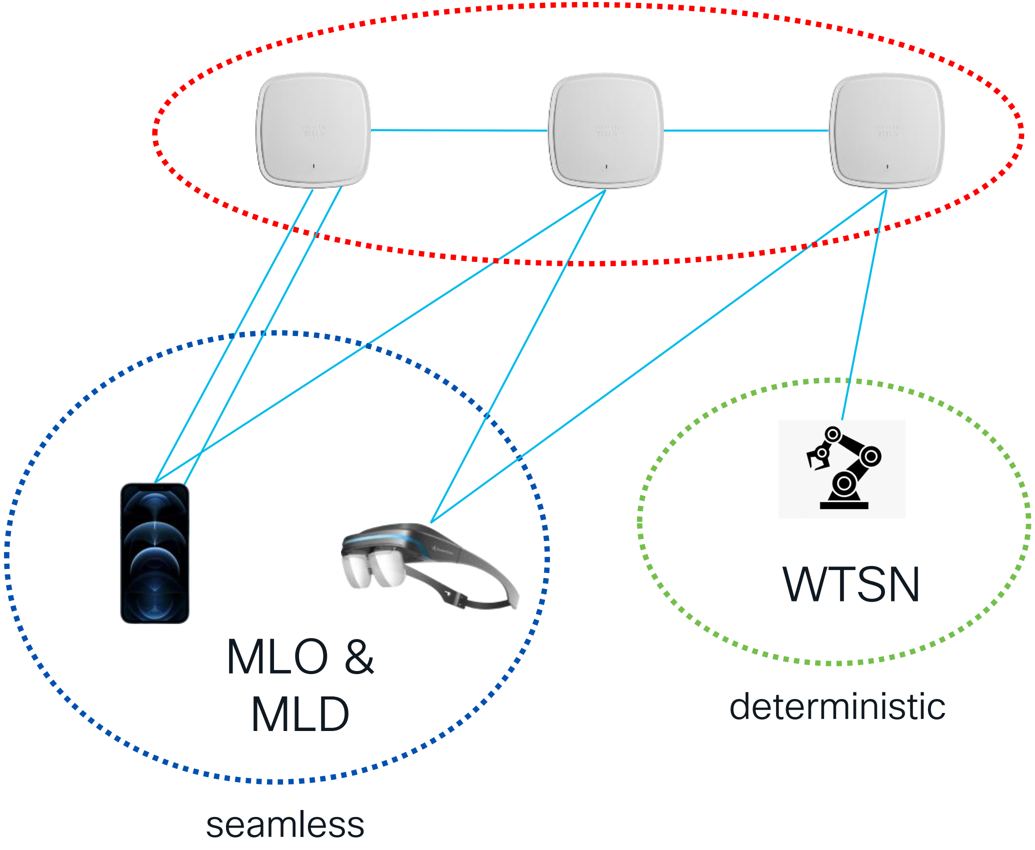
Looking to the Future: IEEE 802.11be and Beyond

Ultra Reliable and Deterministic Wireless

- 5G Release 16 introduced Ultra-Reliable Low Latency Communication (URLLC) for fast moving vehicles and seamless roaming
- Cisco CURWB (Fluidmesh) supports this today
- Wi-Fi will follow soon with 802.11be (Wi-Fi7)

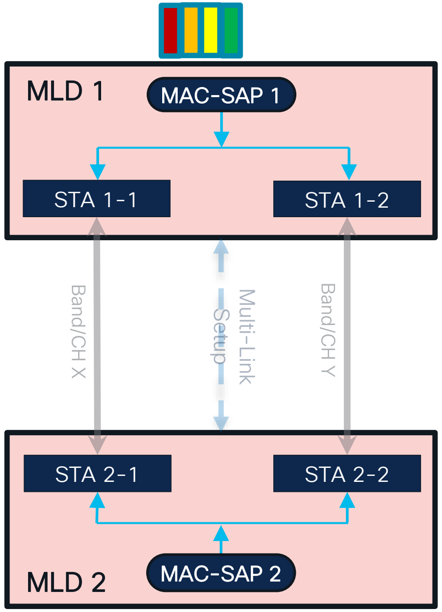
IEEE 802.11be key capabilities

- Multi-Link Operations (MLO)
  - **Ability to Tx and Rx on multiple channels**
  - **QoS-based** link selection/steering
- MAPC
  - Time and space scheduling across multiple APs
- Wireless Time Sensitive Networking (TSN)
- Enhanced QoS Capabilities
  - **SLA-based** KPI delivery (latency, jitter, etc.)
  - **Network** and client-side support

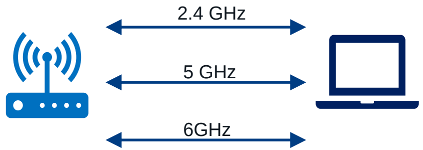


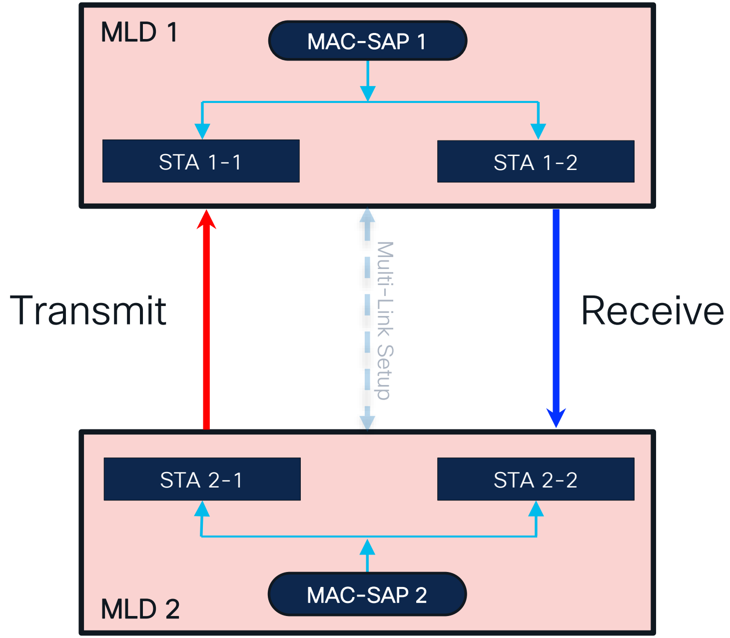
Multi-Link Operation (MLO)

- A **MLO-capable** device is called a Multi-Link Device (**MLD**)
- The MLD can be associated to both/all radios of an AP using both or all of its radios
- MLDs have more than one affiliated Stations (STAs), but generally **ONE** MAC Service Access Point (SAP) connected to the LLC
- The SAP is tasked with aggregating data from multiple links

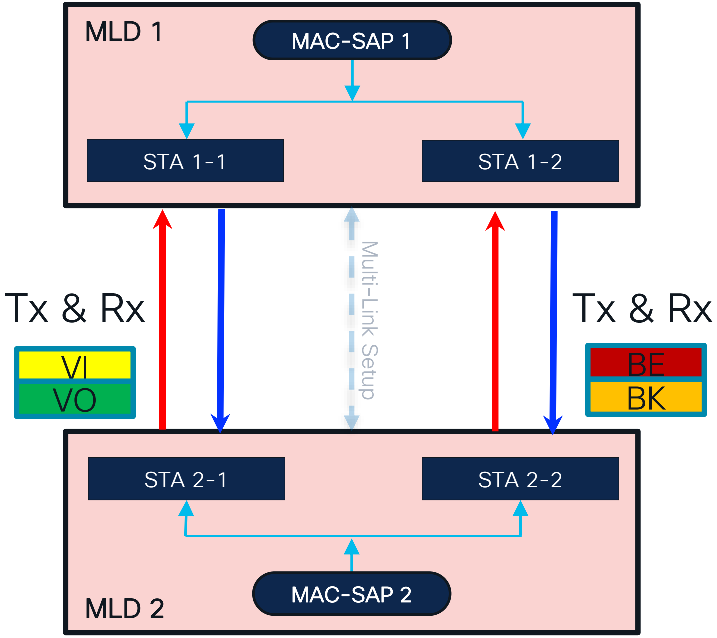


Multi-Link Operation (MLO) Enables new Capabilities

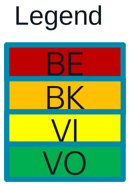




STR Mode (Simultaneous Tx and Rx)
Essentially Full-Duplex

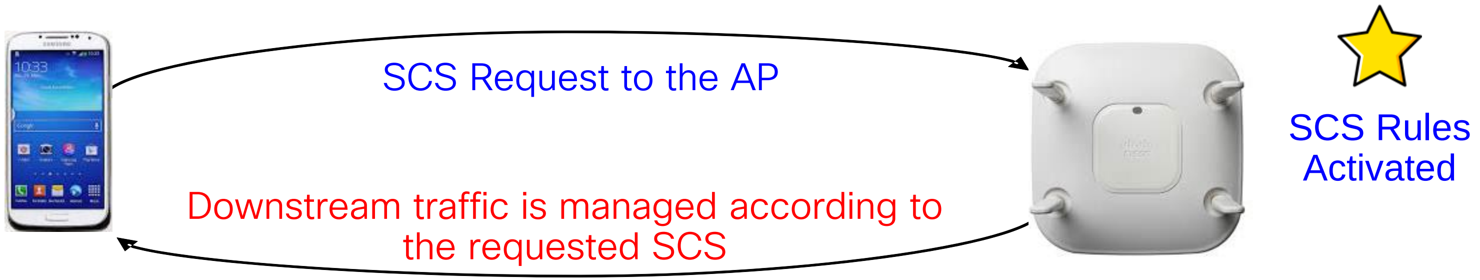


NSTR Mode (Non-Simultaneous Tx and Rx)
Load balanced traffic across multiple links



A New QoS Paradigm: 802.11aa Stream Classification Service (SCS)

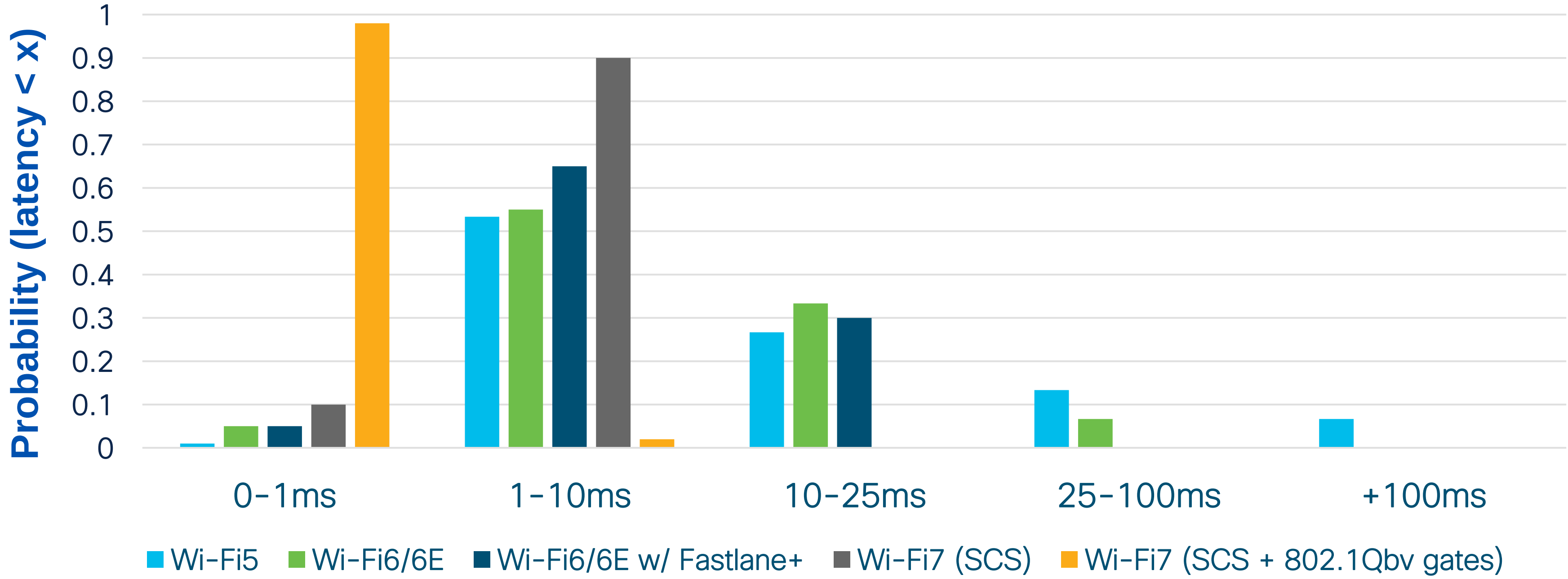
- SCS (Stream Classification Service) specifies traffic flows using an SCS request frame (a QoS **Information Element / IE**)
- The AP derives QoS rules by monitoring the corresponding uplink flows
- Allows the STA to explicitly provide traffic classifiers and priority for each downlink flow



802.11be / Wi-Fi7 QoS

- Traffic Identifiers (TIDs)
  - **TIDs** are a 4-bit QoS field in 802.11 header (the first 3 bits are where the UP value comes from) which are communicated in the SCS request
  - With 802.11be TIDs may be used to select optimal links (5GHz vs. 6GHz, etc.) – TID to radio link mapping
    - E.g. “Let’s send all low-latency HD video on 6GHz, but everything else on 5GHz”
- The SCS QoS IE specifies **traffic characteristics & requirements**
  - Inter-arrival-time / periodicity (max/min scheduling interval)
  - Delay, reliability (delivery ratio) & jitter (indirectly) requirements
  - Burst characteristics (size and window)
  - Exact alignment (e.g. TSN 802.1Qbv) via service-start-time (SST)

Enhanced QoS: 802.11be SCS Enables Determinism



Latency performance improvements in high-traffic scenarios

Source: https://mentor.ieee.org/802.11/dcn/22/11-22-0634-00-00be-802-11be-enhancements-for-tsn-time-aware-scheduling-and-network-management-considerations.pptx

Summary

Conclusions

- 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
- 802.11be QoS Innovations are coming in Wi-Fi to support new use cases

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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

The bridge to possible

Thank you

#CiscoLive

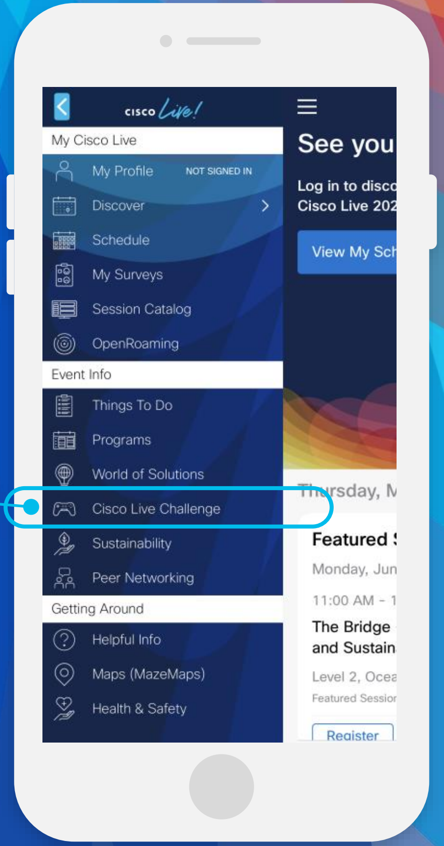
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge’ in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

Let’s go