
TOMORROW starts here.
cisco
Cisco live!

Converged Access QoS

BRKCRS-2890

Ken Briley – NOSTG TME

Cisco live!

Stages of enlightenment……

Stage 1: UGH!

Stage 2: Hmmm…

Stage 3: Aha!

Agenda

- Converged Access QoS architecture overview
- QoS Refresher
- Existing QoS deployment – architecture refresher and challenges
- What Converged Access offers
- The Converged Access QoS architecture in detail
  - The QoS toolbox
  - Default behavior and QoS touch points
  - Queuing and the end of “trust”
- Converged Access QoS design options
  - SRND comparison
  - Use Case

Agenda

- **Converged Access QoS architecture overview**
- QoS Refresher
- Existing QoS deployment – architecture refresher and challenges
- What Converged Access offers
- The Converged Access QoS architecture in detail
  - The QoS toolbox
  - Default behavior and QoS touch points
  - Queuing and the end of “trust”
- Converged Access QoS design options
  - SRND comparison
  - Use Case

Design Scenarios –
Driving a Continuum of Wired and Wireless Options

- Mobility required for devices, and all devices wireless-capable
- Wired factors not applicable
- Cost considerations limit wired ports

Examples –

Laptops, Tablets, Smart Phones, Other Mobile Devices

- **Mobility and wired factors both important**
- **Different situations require different media**

- Deterministic Behavior
  – High Availability
  – Scalability –Security
  – Power – Bandwidth / Video – Legacy Devices
- Mobility not required for devices / users
- Cost considerations limit wireless APs

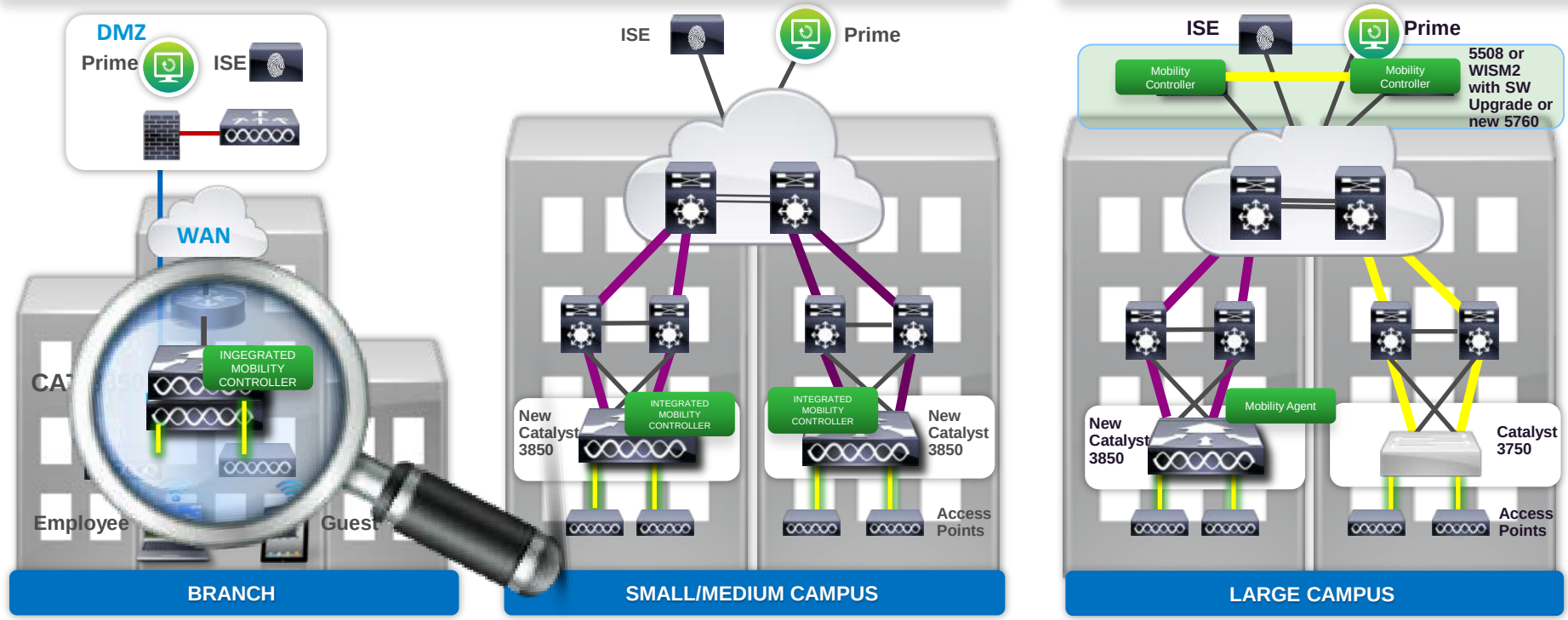
Examples –

Mission-Critical Systems, Video Clients, Security Devices, PoE Devices

Evolution of Converged Access

INTEGRATED CONTROLLER OPTIONS

EXTERNAL MOBILITY CONTROLLER NEEDED



BRANCH

UP TO 50 ACCESS POINTS
UP TO 2,000 CLIENTS
ALL WAN SERVICES AVAILABLE

SMALL/MEDIUM CAMPUS

UP TO 250 ACCESS POINTS
UP TO 16,000 CLIENTS
VISIBILITY, CONTROL, RESILIENCY

LARGE CAMPUS

UP TO 72,000 ACCESS POINTS
UP TO 864,000 CLIENTS
LARGEST LAYER 3 ROAMING DOMAINS

Capwap Tunnel

Standard Ethernet, No Tunnels

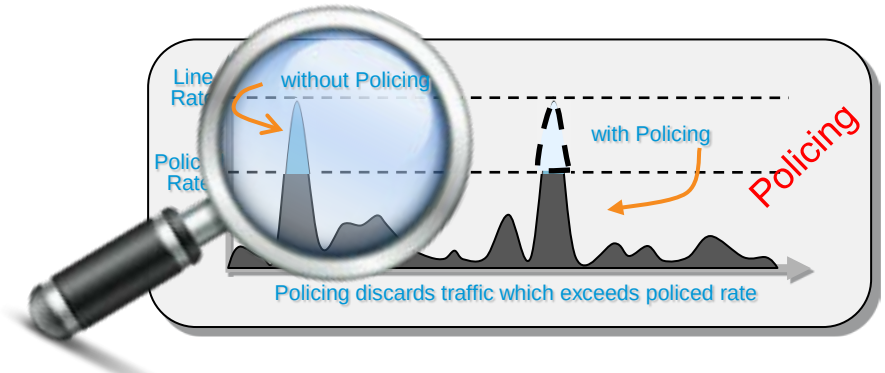
Guest Tunnel from Switch to DMZ Controller

Agenda

- Converged Access QoS architecture overview
- **QoS Refresher**
- Existing QoS deployment – architecture refresher and challenges
- What Converged Access offers
- The Converged Access QoS architecture in detail
  - The QoS toolbox
  - Default behavior and QoS touch points
  - Queuing and the end of “trust”
- Converged Access QoS design options
  - SRND comparison
  - Use Case

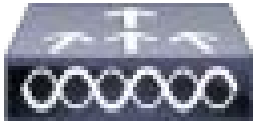
What is QoS made of?

- Classification
- Marking/Mutation
- Shaping/Policing
- Queueing
- Bandwidth Allocation
- Trust



What is QoS made of?

DSCP 46

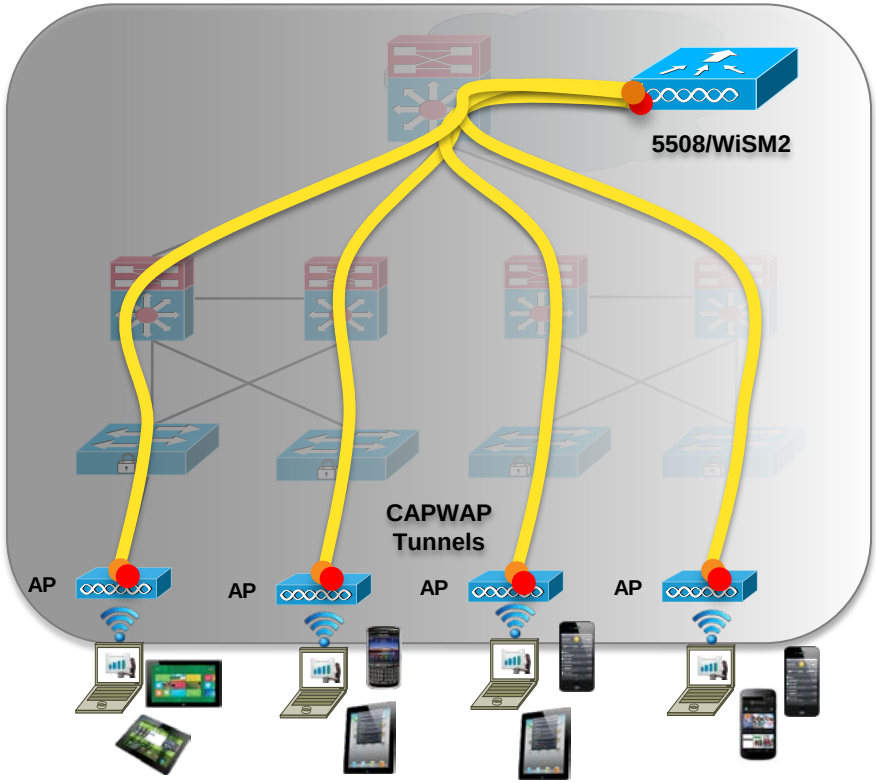


Agenda

- Converged Access QoS architecture overview
- QoS Refresher
- **Existing QoS deployment – architecture refresher and challenges**
- What Converged Access offers
- The Converged Access QoS architecture in detail
  - The QoS toolbox
  - Default behavior and QoS touch points
  - Queuing and the end of “trust”
- Converged Access QoS design options
  - SRND comparison
  - Use Case

CUWN Architecture –
Overview – Challenges of QoS

Current Mobility Architecture



Challenges –

Overlay model with multiple points of policy application*

Limited **visibility** into applications at the edge

Lack of **granular classification** at the edge

Software based **QoS**

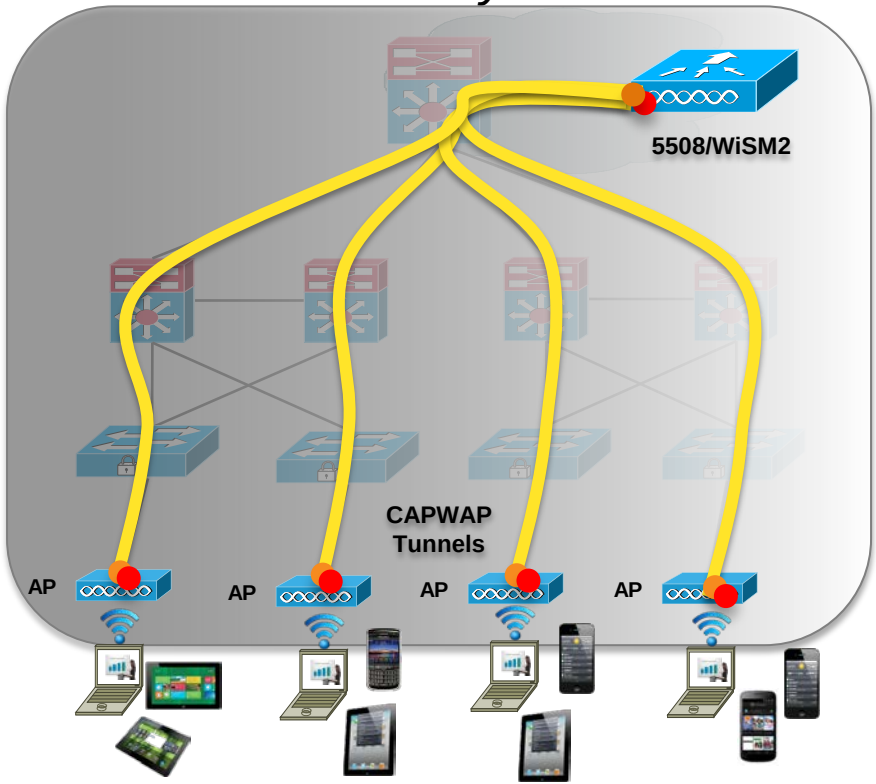
*** Overlay model applies to CUWN local mode and FlexConnect centralized mode**

Marking Policing

Wireless QoS Today (AireOS 7.4)

How wireless QoS is deployed today

Current Mobility Architecture



- **Classification/Marking**
  - Based on QoS marking from WMM client but subjected to profile chosen on WLC
  - SSID level QoS based on **“Precious Metals”** (Platinum, Gold, Silver, Bronze) selection
  - WMM client marking is allowed **up to profile** value
  - Non-WMM client traffic marked to profile value
  - DSCP value is set in the CAPWAP header corresponding to the marking

- **Policing**
  - Per-user bandwidth **contracts applied downstream** at WLC and upstream at AP
  - Per SSID (per AP/per radio) bandwidth contracts applied upstream and downstream at AP

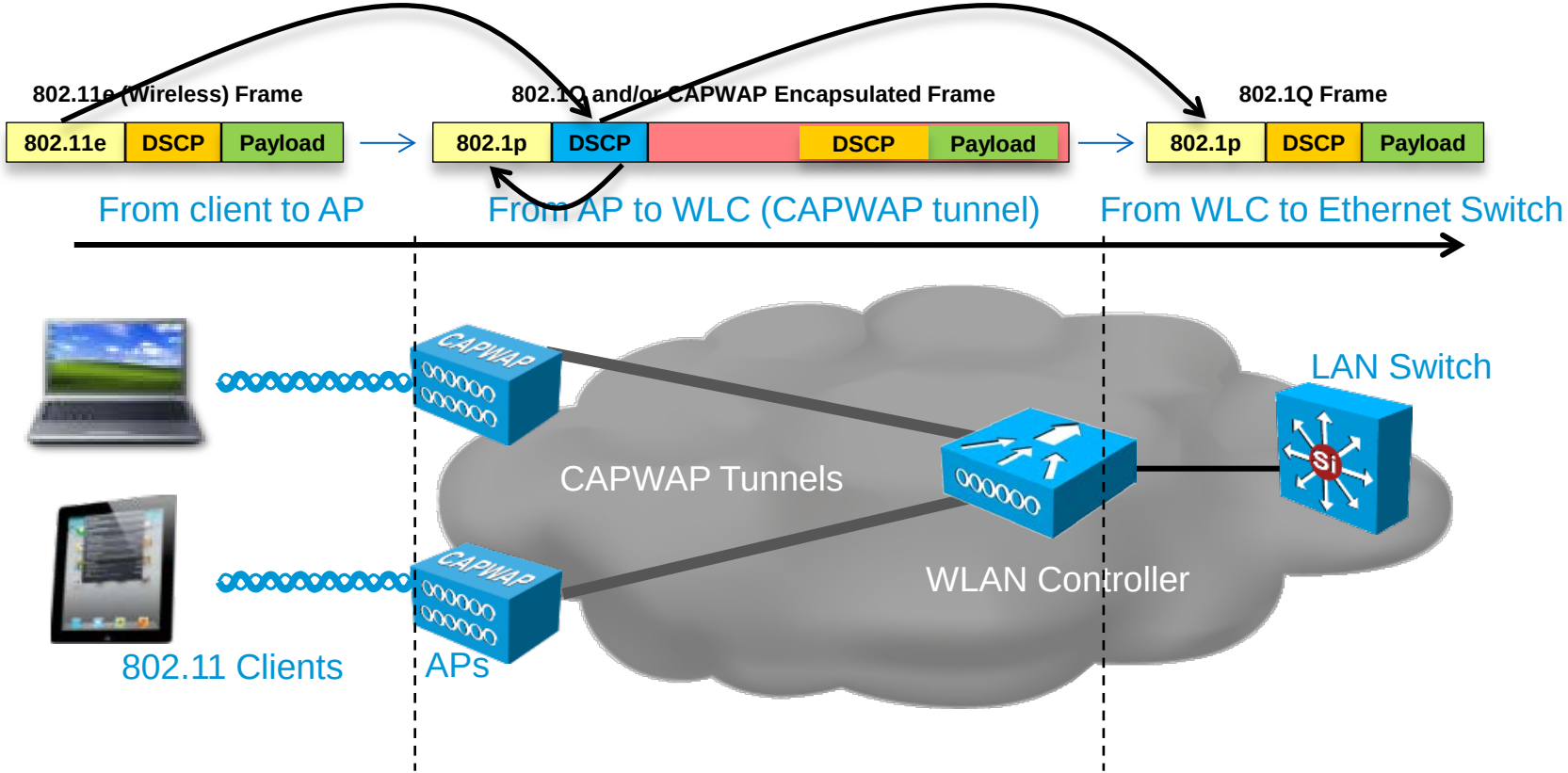
Admission Control

- TSPEC or SIP-based

Marking Policing

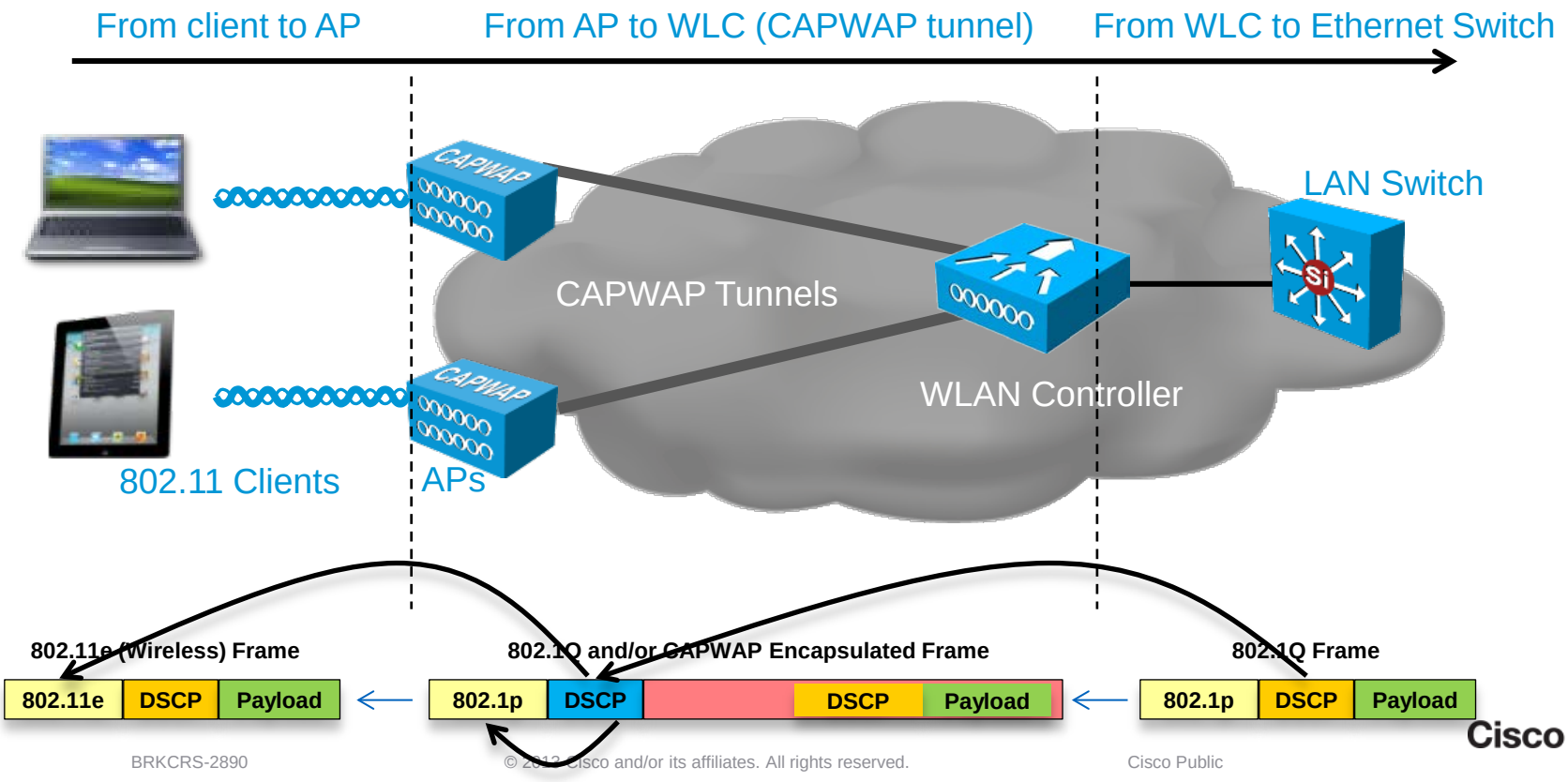
Wireless QoS Today

QoS Bits – how are they carried thought the network

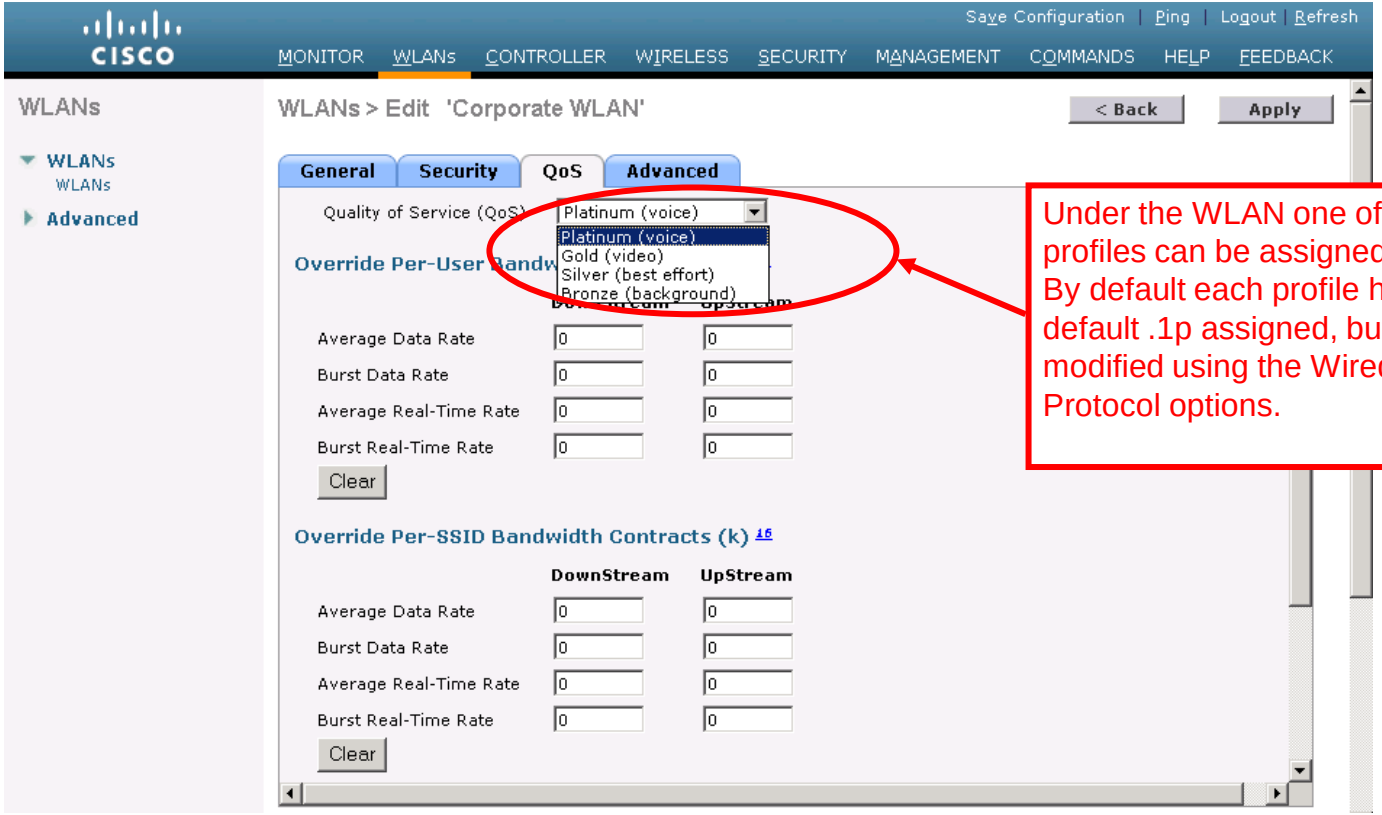


Wireless QoS Today

QoS Bits – how are they carried thought the network



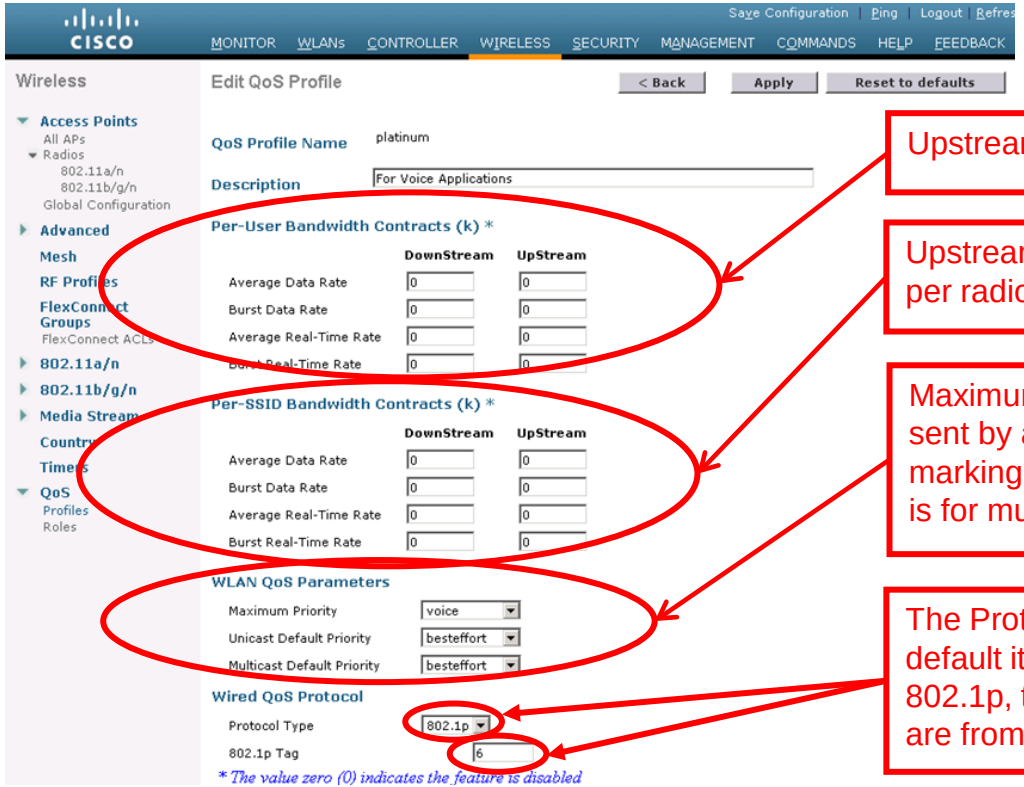
How do we enable QoS today?
Wireless



Under the WLAN one of four QoS profiles can be assigned.
By default each profile has a default .1p assigned, but it can be modified using the Wired QoS Protocol options.

*NOTE: Assignment of QoS profile to WLAN

How do we enable QoS today?
Wireless



Upstream per- user contracts added in 7.3.

Upstream and downstream per- SSID (per AP per radio) contracts added in 7.3.

Maximum Priority is the maximum marking which can be sent by a WMM client. Unicast Default Priority is the default marking of non-WMM client traffic. Multicast Default Priority is for multicast traffic.

The Protocol Type has two options: None & 802.1p. By default it is set to None. If the Protocol Type is set to 802.1p, then the 802.1p tag can be modified. Valid values are from 0 to 7.

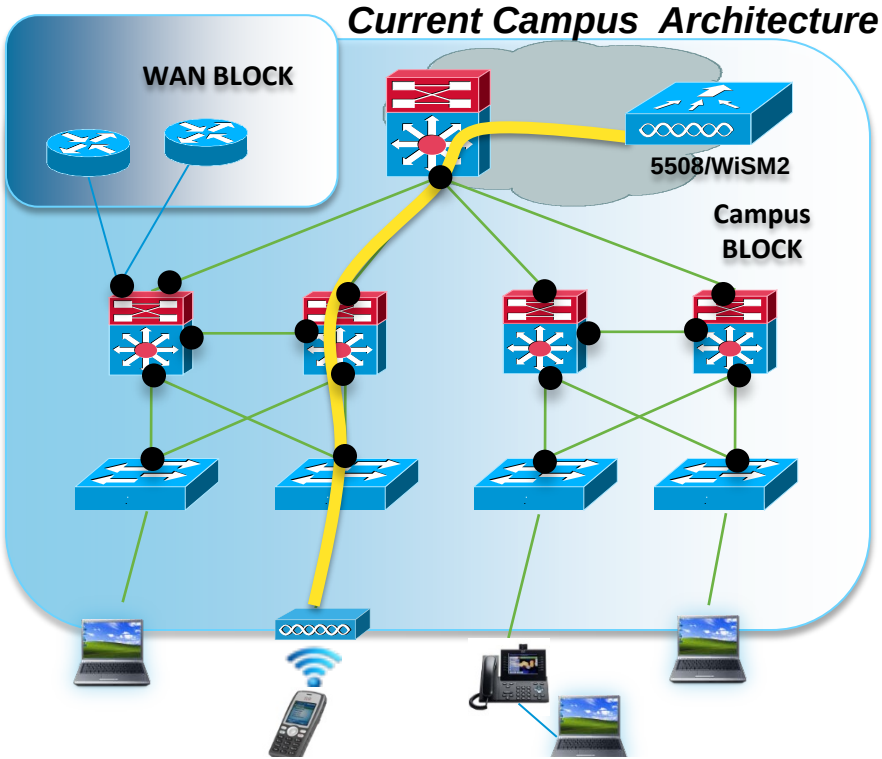
Wireless QoS Features
Where are they applied today?

Feature	Direction	Device	Note:
Classification	Upstream	AP	AP uses profile
		WLC	WLC uses DSCP in capwap, sip snooping
	Dowstream	AP	AP uses DSCP in capwap
		WLC	WLC uses .1p/DSCP in .1Q
Marking	Upstream	AP	AP uses profile and max wmm value as limit
	Downstream	AP	AP uses DSCP in capwap to mark wmm
Per-User Bandwidth Contracts	Upstream	AP	User limited to specific rate
	Downstream	WLC	User limited to specific rate
Per-SSID Bandwidth Contracts	Upstream	WLC	BSSID (per ssid, per radio) bandwidth limit
	Downstream	WLC	BSSID (per ssid, per radio) bandwidth limit
AVC	Upstream/Downstream	WLC	Classification, marking, drop actions all on WLC – marking is bidirectional

Campus QoS architecture

How campus QoS is deployed today (QoS SRND 4.0)

- Untrusted Endpoint Port QoS:
  - No Trust – Acl/DSCP classification
  - Optional Ingress Marking and/or Policing
  - 1P3QyT Egress Queueing
- Trusted Endpoint Port QoS:
  - Trust-DSCP
  - Optional Ingress Marking and/or Policing
  - 1P3QyT Egress Queueing
- Conditionally Trusted Endpoint Port QoS
  - Conditional Trust with Trust-CoS
  - Optional Ingress Marking and/or Policing
  - 1P3QyT Egress Queueing
- Switch-to-Switch/Router port QoS:
  - Trust DSCP
  - 1P3QyT or 1P7QyT Egress Queueing



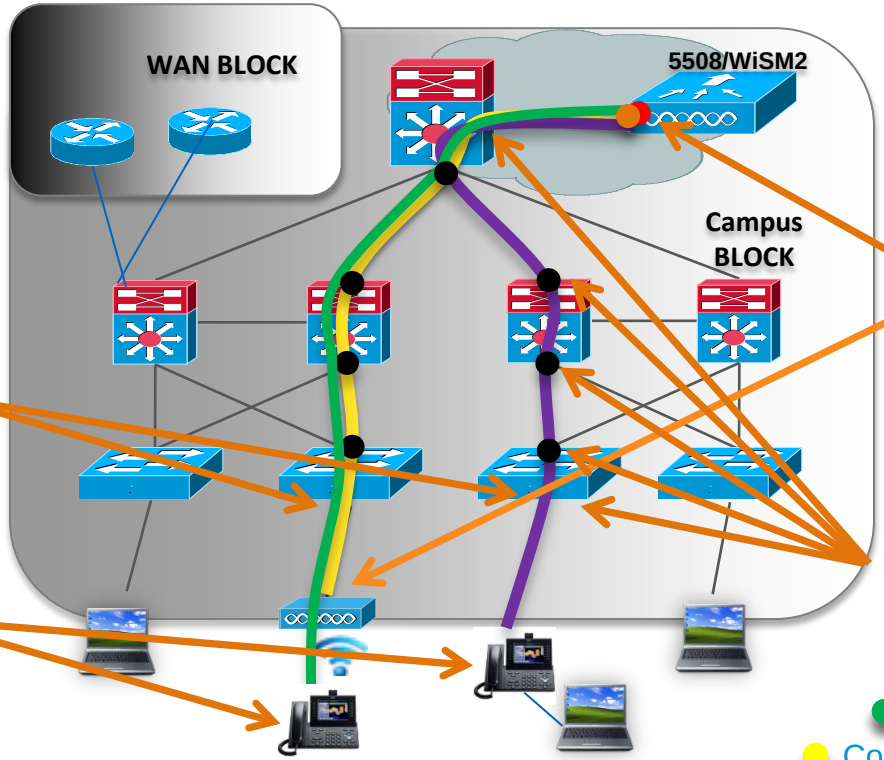
How do we enable QoS today?
Wired: mls based CLI exposes hardware

```
C3750-X(config)#mls qos
C3750-X(config)#interface GigabitEthernet 1/0/1
C3750-X(config-if)#mls qos trust dscp

C3750-X(config)#mls qos queue-set output 1 buffers 15 30 35 20
C3750-X(config)#mls qos queue-set output 1 threshold 1 100 100 100 100
C3750-X(config)#mls qos queue-set output 1 threshold 2 80 90 100 400
C3750-X(config)#mls qos queue-set output 1 threshold 3 100 100 100 400
C3750-X(config)#mls qos queue-set output 1 threshold 4 60 100 100 400
C3750-X(config)#mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 46

C3750-X(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
C3750-X(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34
36 38
C3750-X(config)#mls qos srr-queue output dscp-map queue 2 threshold 2 24
C3750-X(config)#mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
C3750-X(config)#mls qos srr-queue output dscp-map queue 3 threshold 3 0
C3750-X(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 8
C3750-X(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14

C3750-X(config)#interface range GigabitEthernet1/0/1-48
C3750-X(config-if-range)# queue-set 1
C3750-X(config-if-range)# srr-queue bandwidth shape 1 30 35 5
C3750-
```

NOTE: Only class based policing and marking are available today **– last box with mls cli - Cat 3750**

Existing QoS deployments
How we overlay QoS policies today

Current QoS Architecture



Separate Schools of thought On QoS created Misaligned markings

Switch Sees:
Wireless – Voice EF, Video AF41
Wired – Voice AF41, Video AF41

Video Phone Call
Phone Sends:
Voice AF41 – WMM 6
Video AF41 – WMM 5

Separate **policies and services** for wired and wireless users

Wireless policies implemented on controller pushed to AP

Wired policies implemented on switch

Trust Marking Policing
Conditional Trust Queuing

Agenda

- Converged Access QoS architecture overview
- QoS Refresher
- Existing QoS deployment – architecture refresher and challenges
- **What Converged Access offers**
- The Converged Access QoS architecture in detail
  - The QoS toolbox
  - Default behavior and QoS touch points
  - Queuing and the end of “trust”
- Converged Access QoS design options
  - SRND comparison
  - Use Case

What's new with Converged Access

Wired (Cat 3850)

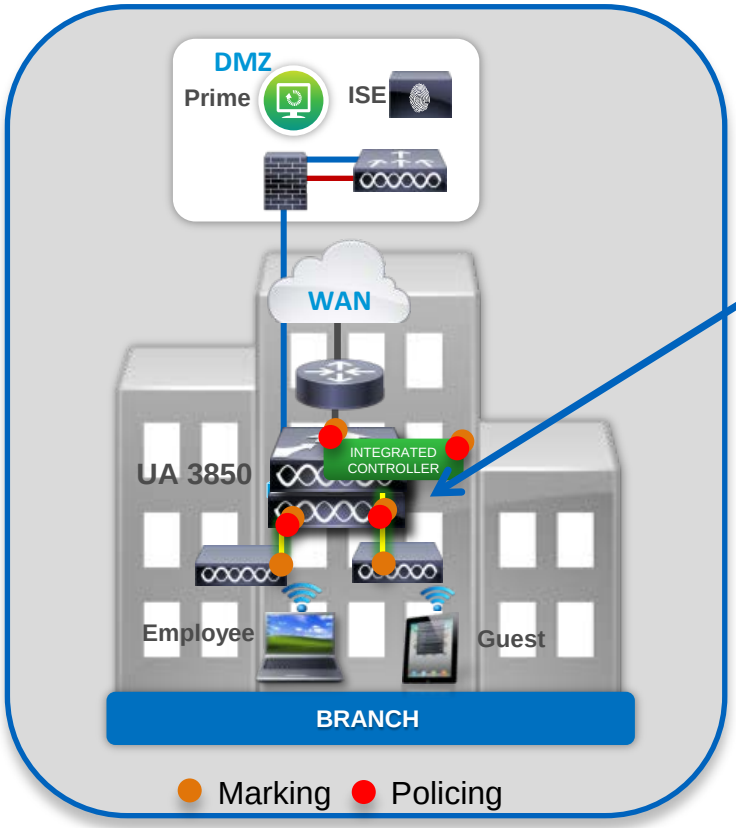
- Modular QoS based CLI (MQC)
  - Alignment with 4500E series (Sup6, Sup7)
  - Class-based Queueing, Policing, Shaping, Marking
- More Queues
  - Up to 2P6Q3T queueing capabilities
  - Standard 3750 provides 1P3Q3T
  - Not limited to 2 queue-sets
  - Flexible MQC Provisioning abstracts queueing hardware

Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network
- Enhanced Bandwidth Management
  - Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic
- Wireless Specific Interface Control
  - Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  - AAA support for dynamic Client based QoS and Security policies
- Per SSID Bandwidth Management

*** **NOT** available on CT 5760 at FCS

What's new with Converged Access



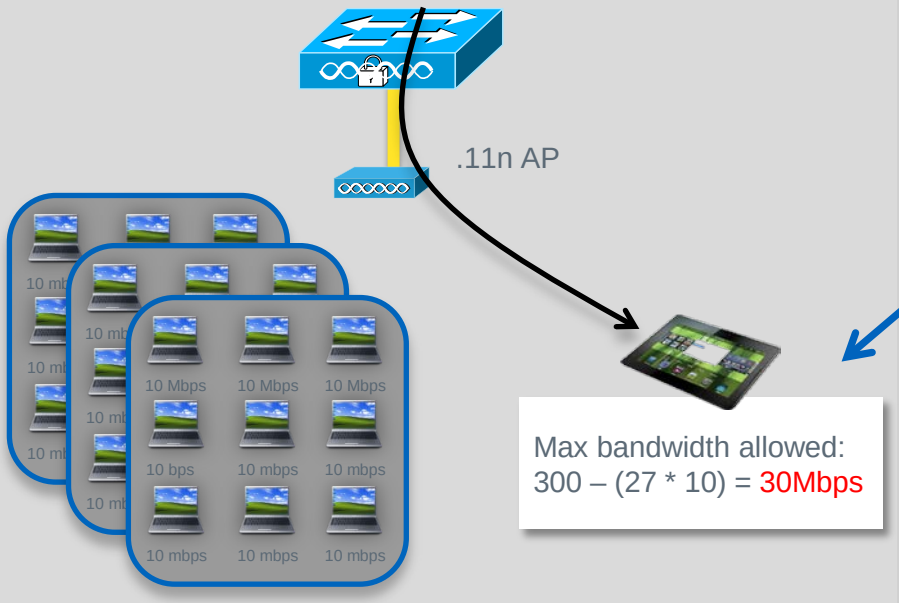
Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network
- Enhanced Bandwidth Management
  - Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic
- Wireless Specific Interface Control
  - Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  - AAA support for dynamic Client based QoS and Security policies
- Per SSID Bandwidth Management

What's new with Converged Access

With the CT 5760 or CAT 3850

Usage based fair allocation without configuration



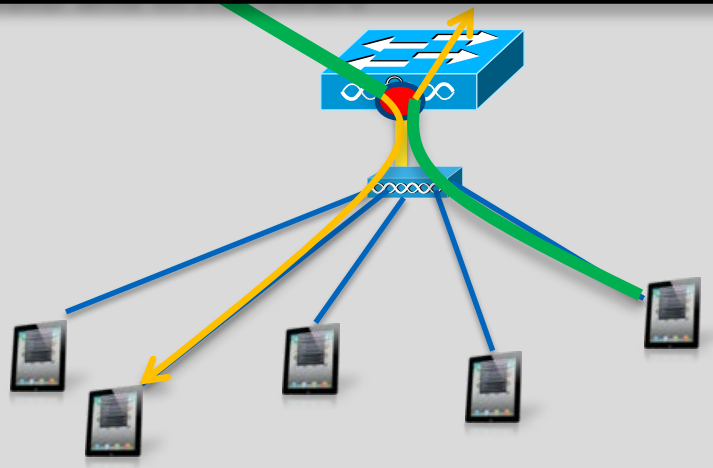
Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network
- Enhanced Bandwidth Management
  - Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic
- Wireless Specific Interface Control
  - Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  - AAA support for dynamic Client based QoS and Security policies
- Per SSID Bandwidth Management

What's new with Converged Access

With the 3850

Bidirectional policing at the edge per- user , per-SSID and in Hardware



- SSID: BYOD
- QoS policy on 3850 used to police each client bidirectionally
- Policy can be sent via AAA to provide specific per-client policy
- Allocate Bandwidth or police/shape SSID as a whole

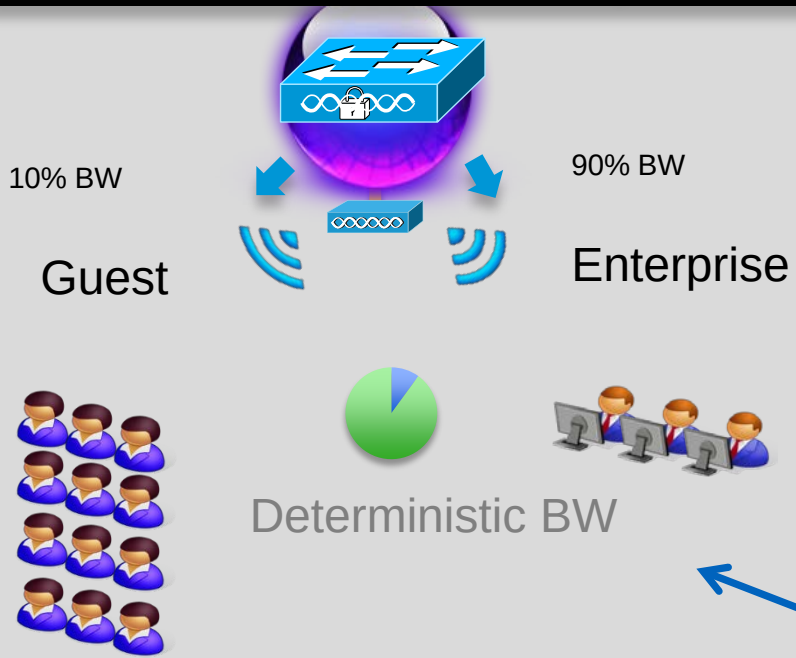
Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network
- Enhanced Bandwidth Management
  - Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic
- Wireless Specific Interface Control
  - Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  - AAA support for dynamic Client based QoS and Security policies
- Per SSID Bandwidth Management

What's new with Converged Access

With the CT 5760 or CAT 3850

Deterministic bandwidth is allocated per SSID



Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network
- Enhanced Bandwidth Management
  - Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic
- Wireless Specific Interface Control
  - Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  - AAA support for dynamic Client based QoS and Security policies
- Per SSID Bandwidth Management

What's new with Converged Access

mls based CLI exposes hardware – MQC provides a unified provisioning Language

```
C3750-X(config)#mls qos
C3750-X(config)#interface GigabitEthernet 1/0/1
C3750-X(config-if)#mls qos trust dscp

C3750-X(config)#mls qos queue-set output 1 buffers 15 30 35 20
C3750-X(config)#mls qos queue-set output 1 threshold 1 100 100 100 100
C3750-X(config)#mls qos queue-set output 1 threshold 2 80 90 100 400
C3750-X(config)#mls qos queue-set output 1 threshold 3 100 100 100 400
C3750-X(config)#mls qos queue-set output 1 threshold 4 60 100 100 400
C3750-X(config)#mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 46

C3750-X(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
C3750-X(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34
36 38
C3750-X(config)#mls qos srr-queue output dscp-map queue 2 threshold 2 24
C3750-X(config)#mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
C3750-X(config)#mls qos srr-queue output dscp-map queue 3 threshold 3 0
C3750-X(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 8
C3750-X(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14

C3750-X(config)#interface range GigabitEthernet1/0/1-48
C3750-X(config-if-range)# queue-set 1
C3750-X(config-if-range)# srr-queue bandwidth share 1 30 35 5
C3750-X(config-if-range)# priority-queue out
```

```
policy-map 3850-QoS

class PRIORITY-QUEUE
  priority level 1
   police rate percent 20

class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 30
  queue-limit dscp cs2  percent 80
  queue-limit dscp cs3  percent 90
  queue-limit dscp cs6  percent 100

class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 5
  queue-limit dscp af23 percent 80
  queue-limit dscp af22 percent 90
  queue-limit dscp af21 percent 100

class BULKDATA-QUEUE
  bandwidth remaining percent 35
  queue-limit dscp af13 cs1 percent 80
  queue-limit dscp af12 percent 90
  queue-limit dscp af11 percent 100
```

*NOTE: Only class based policing and marking are available today **– last box with mls cli - Cat 3750**

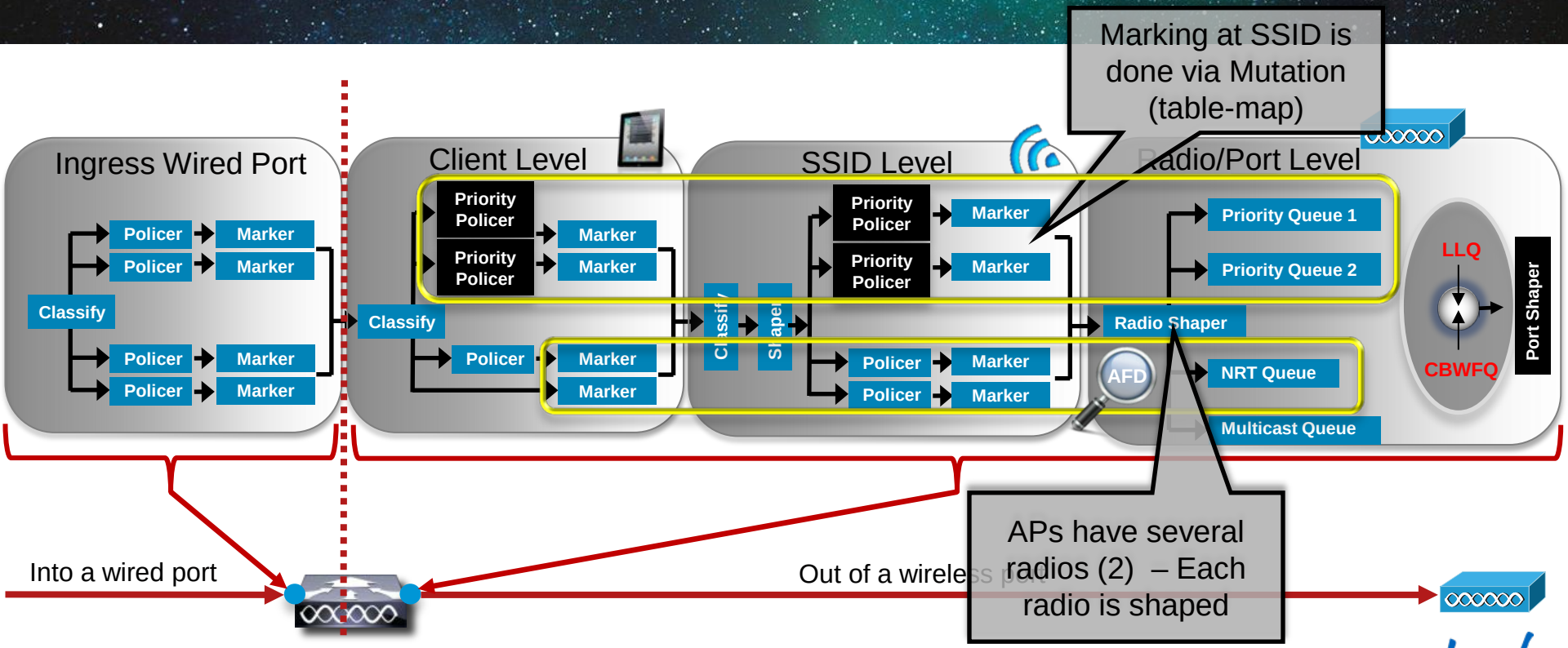
Agenda

- Converged Access QoS architecture overview
- QoS Refresher
- Existing QoS deployment – architecture refresher and challenges
- What Converged Access offers
- **The Converged Access QoS architecture in detail**
  - The QoS toolbox
  - Default behavior and QoS touch points
  - Queuing and the end of “trust”
- Converged Access QoS design options
  - SRND comparison
  - Use Case

The Catalyst 3850 QoS Toolbox

Wired to Wireless

Conceptual View

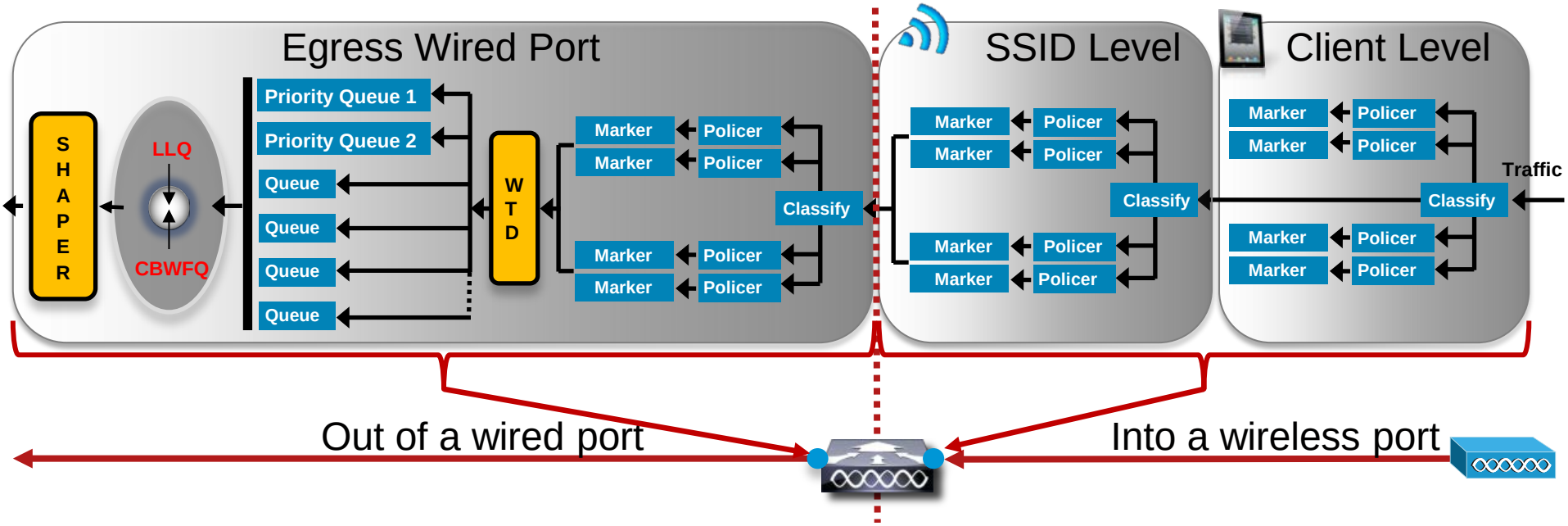


Cisco live!

The Catalyst 3850 QoS Toolbox

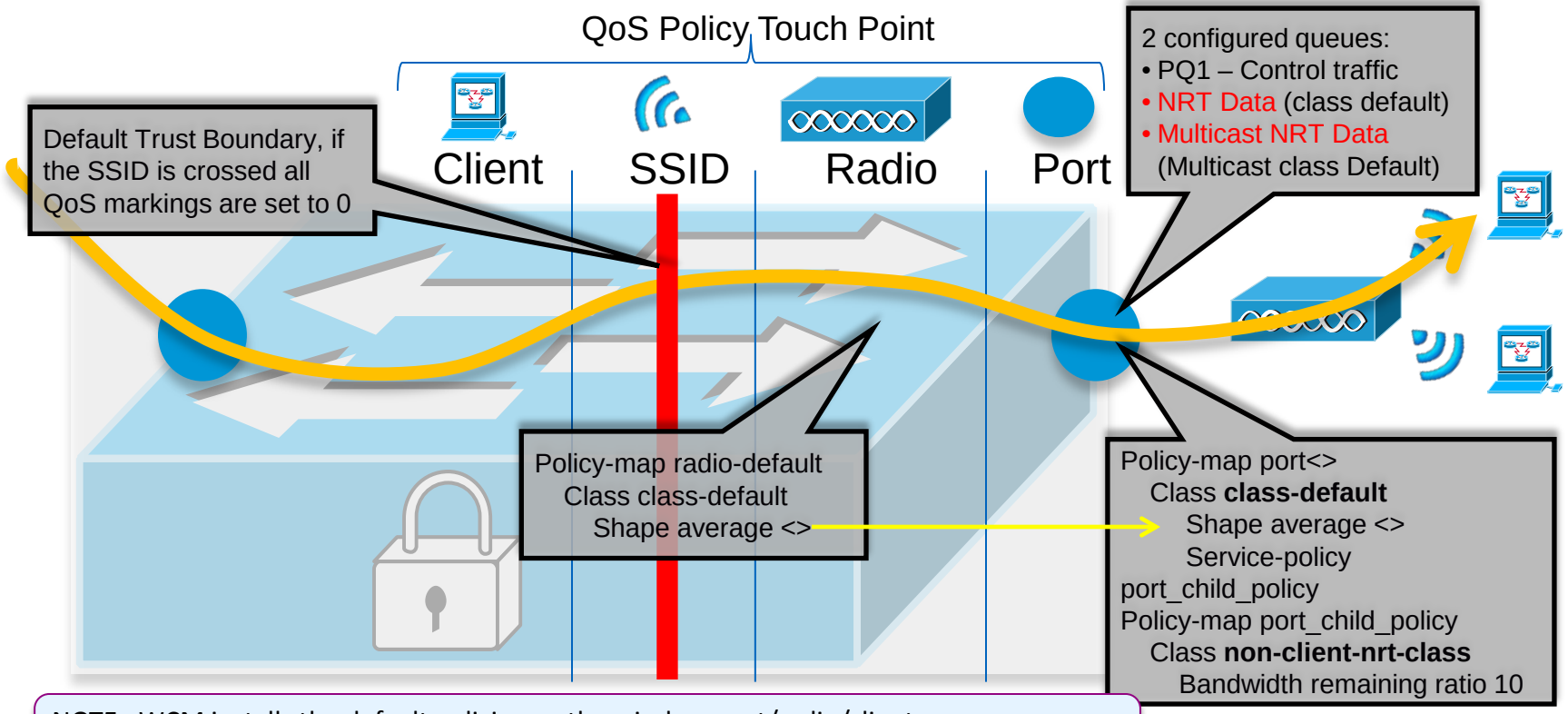
Wired to Wireless

Conceptual View



Cisco live!

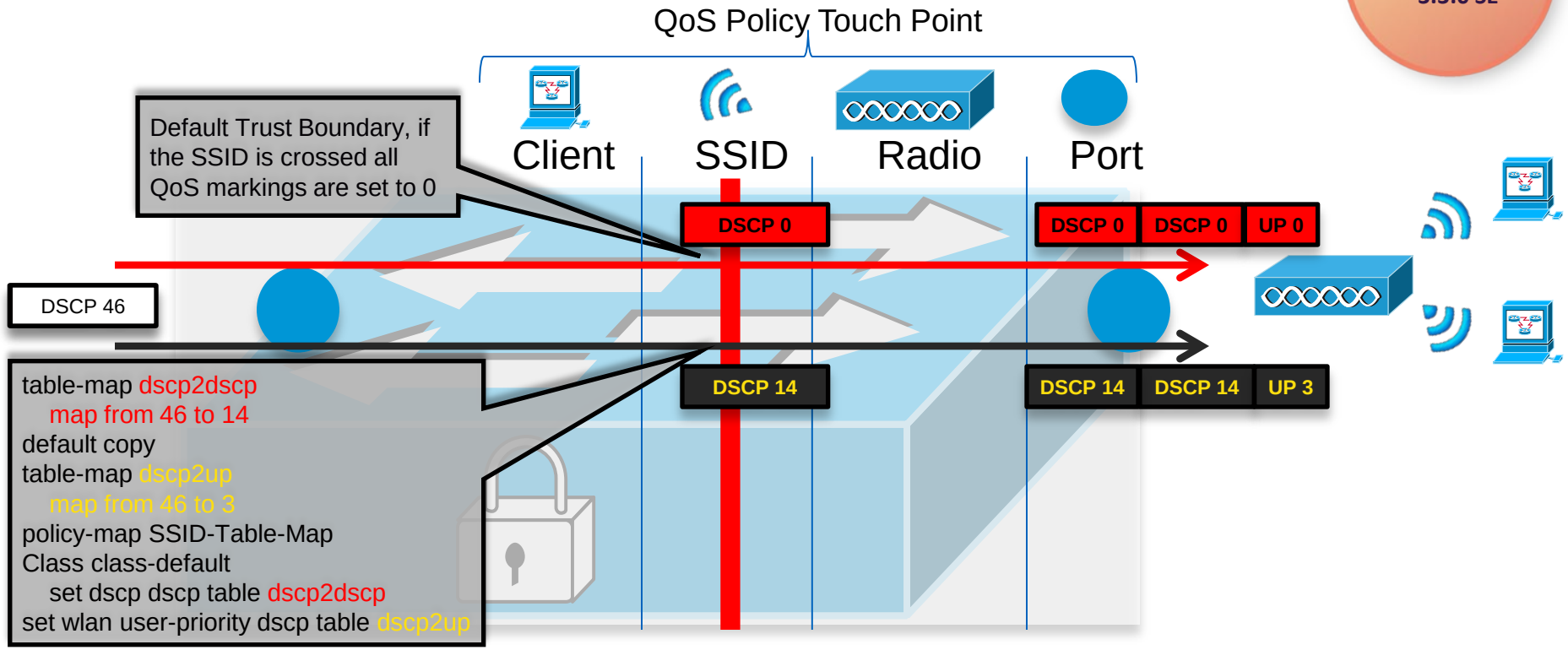
QoS default behavior



Marking with table-maps and the end of “trust”

Table map example

Trust Boundary Will be removed 3.3.0 SE

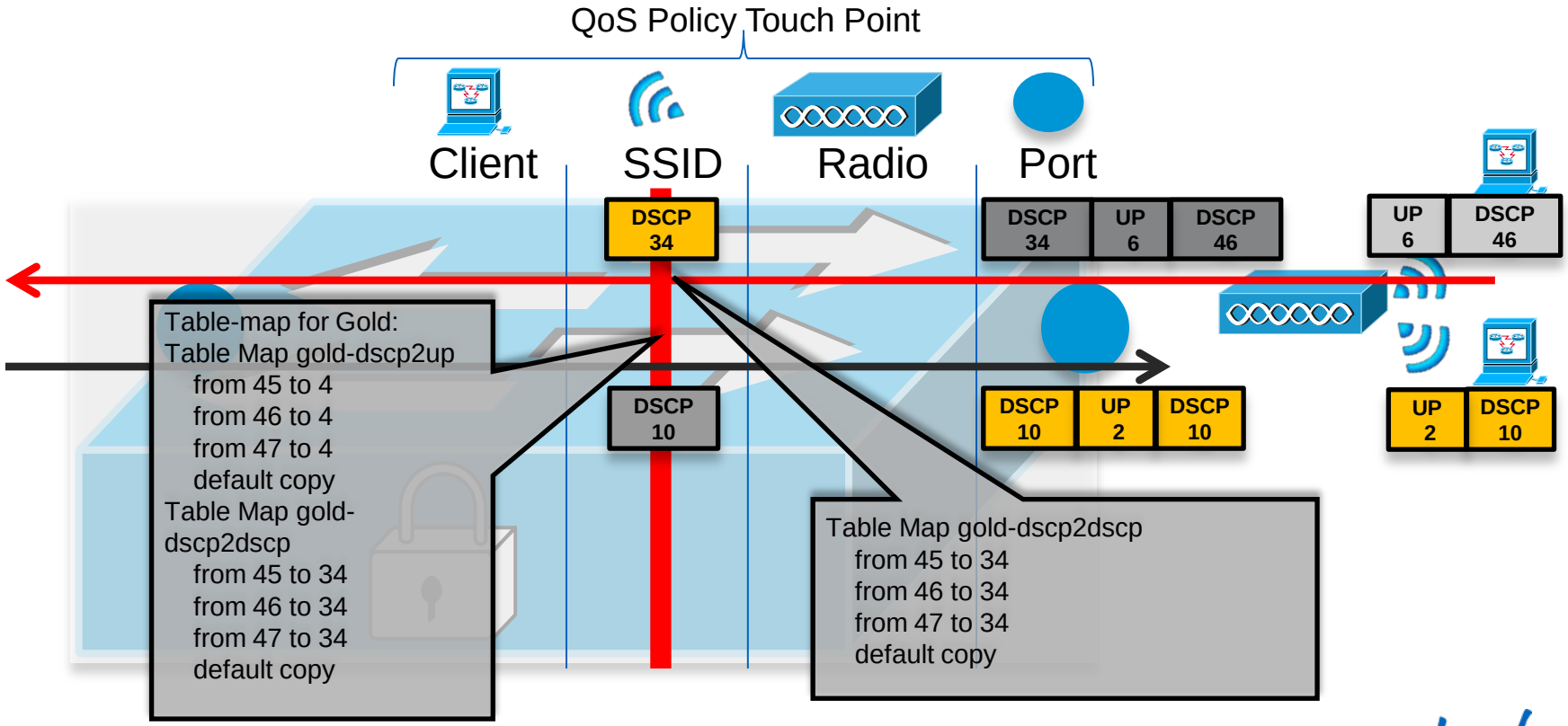


Into a wire

NOTE: “Trust” does not exist in MQC based platforms. By default only wired to wired traffic will retain QoS markings, all other will be remarked to 0 unless a Table-map is used.

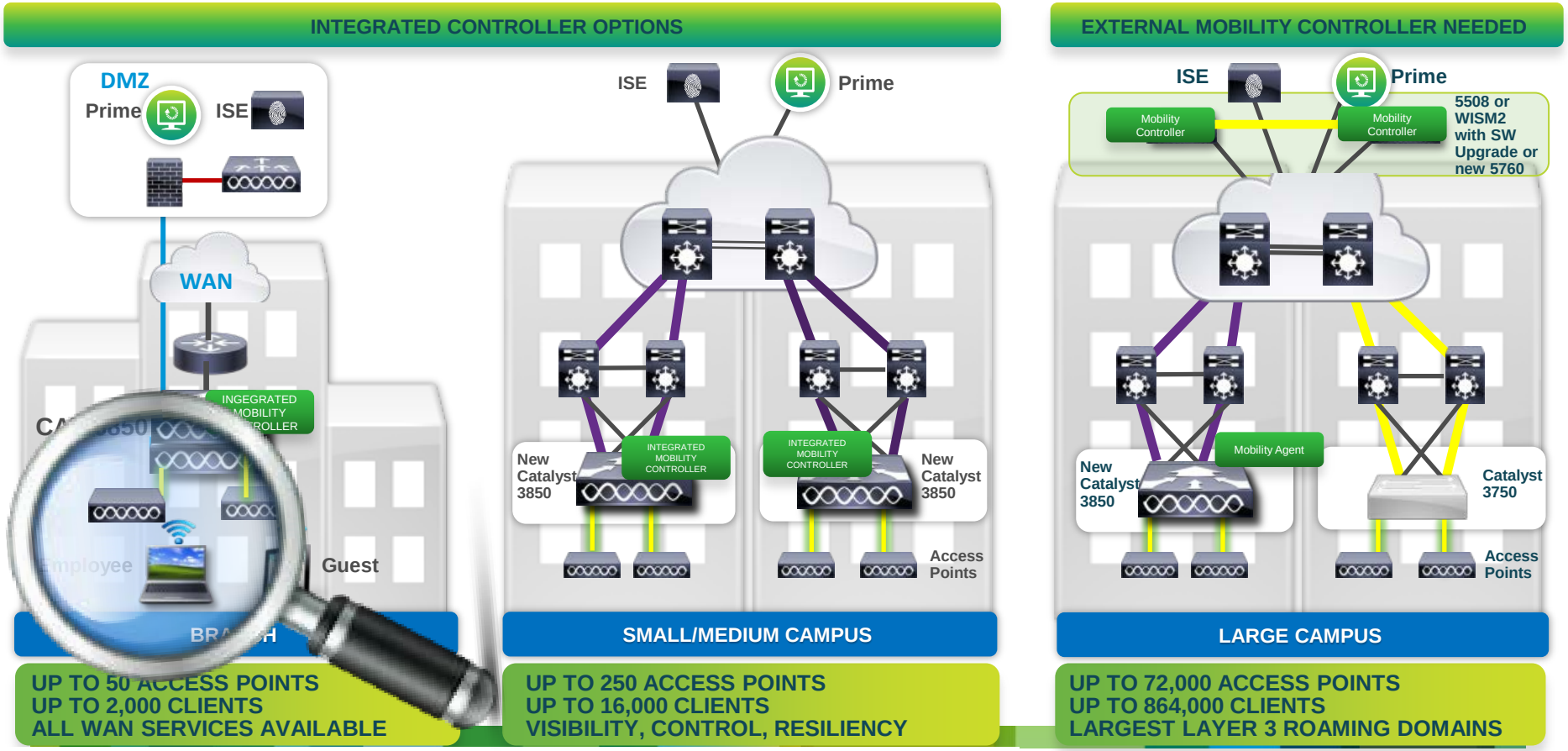
Marking with table-maps and “GOLD” marking

Backward-compatible table-maps



Wireless Queuing and Approximate Fair Drop (AFD)

Evolution of Converged Access



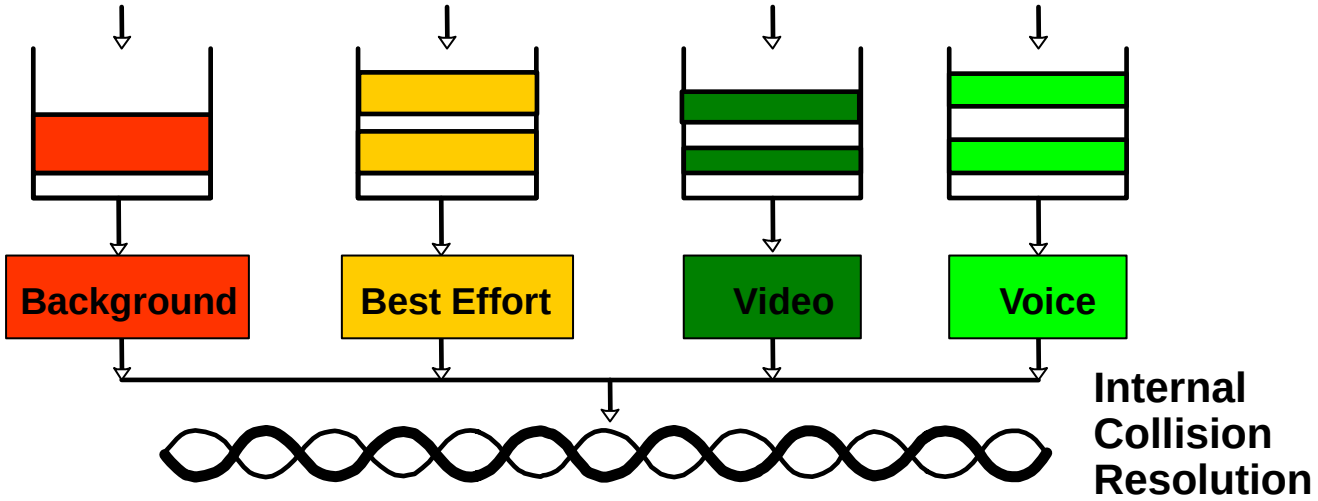
802.11e / WMM Does Not Change

802.1p UP-Based Traffic Type	IP DSCP	802.1p UP (CoS)	IEEE 802.11e UP	Notes
Reserved (Network Control)	56	7	7	802.1p UP 7 requires special handling because it is reserved for CAPWAP control. So data packets with UP = 7 should always get degraded to UP 6 / DSCP 46. CAPWAP Control UP = 7 also translates to DSCP 46 because there are no other logical options.
Reserved	48	6		
Voice	46 (EF)	5	6	
Video	34 (AF41)	4	5	
Voice Control	26 (AF31)	3	4	
Background (Gold)	18 (AF21)	2		
Background (Silver) Best Effort	10 (AF11) 0 (BE)	1 0	1 0,3	

Cisco L2/L3 QoS packet marking mappings and IEEE mappings

802.11e / WMM Media Access Classifications

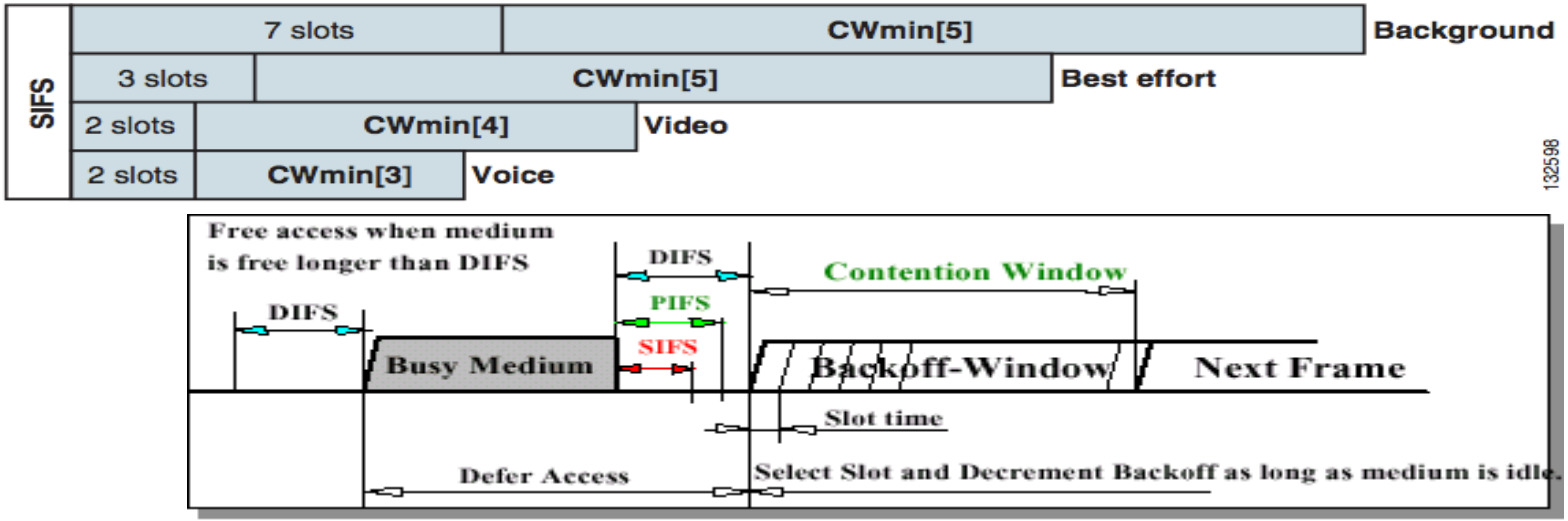
- Separates traffic types in to 4 QoS access categories (AC)
- Background, Best Effort, Video, Voice
- These 4 ACs also have unique delay and random back off characteristics for accessing the RF channel (EDCA)



Wi-Fi Enhanced Distributed Channel Access (EDCA)

- Frames in each access category queue have different backoff delays, referred to as the Arbitration Interframe Space Number (AIFSN), followed by varied contention windows

  This is advertised in the AP's beacon frames and probe responses



Wireless Multimedia (WMM)
a Wi-Fi Alliance subset of 802.11e

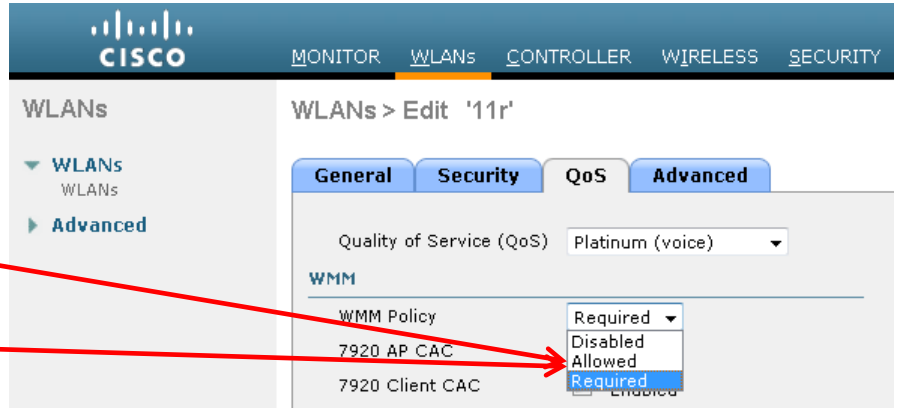
WLAN Configurations of WMM affect QoS Behaviors:

WMM Allowed

Non-WMM clients and WMM enabled Client can join the WLAN

WMM Required

Only WMM enabled Clients can join the WLAN



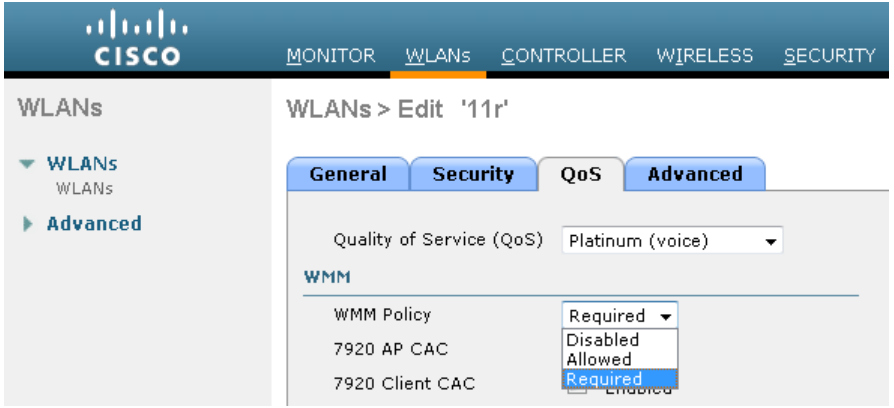
- WMM enabled Clients transmit all packets with WMM QoS Header
- Non-WMM Clients transmit no packets with WMM QoS Header
  - Non-WMM can not receive packets from the AP that have a WMM QoS Header
- All packets from and to Non-WMM Clients are sent with Best Effort Wi-Fi Channel Access, therefore elevated QoS is not provided

WMM Configuration Options

Cat 3850 Configuration:

```
(config)# wlan <your WLAN name>
(config-wlan)# shutdown
(config-wlan)# broadcast
! Shows all beacons in the sniffer trace
(config-wlan)# radio all
! Enables WLAN configuration on both AP radios
  and all Wi-Fi protocols
(config-wlan)# wmm require
! Requires iPhone to mark voice and video
  packets
(config-wlan)# no shutdown
```

WLC Example

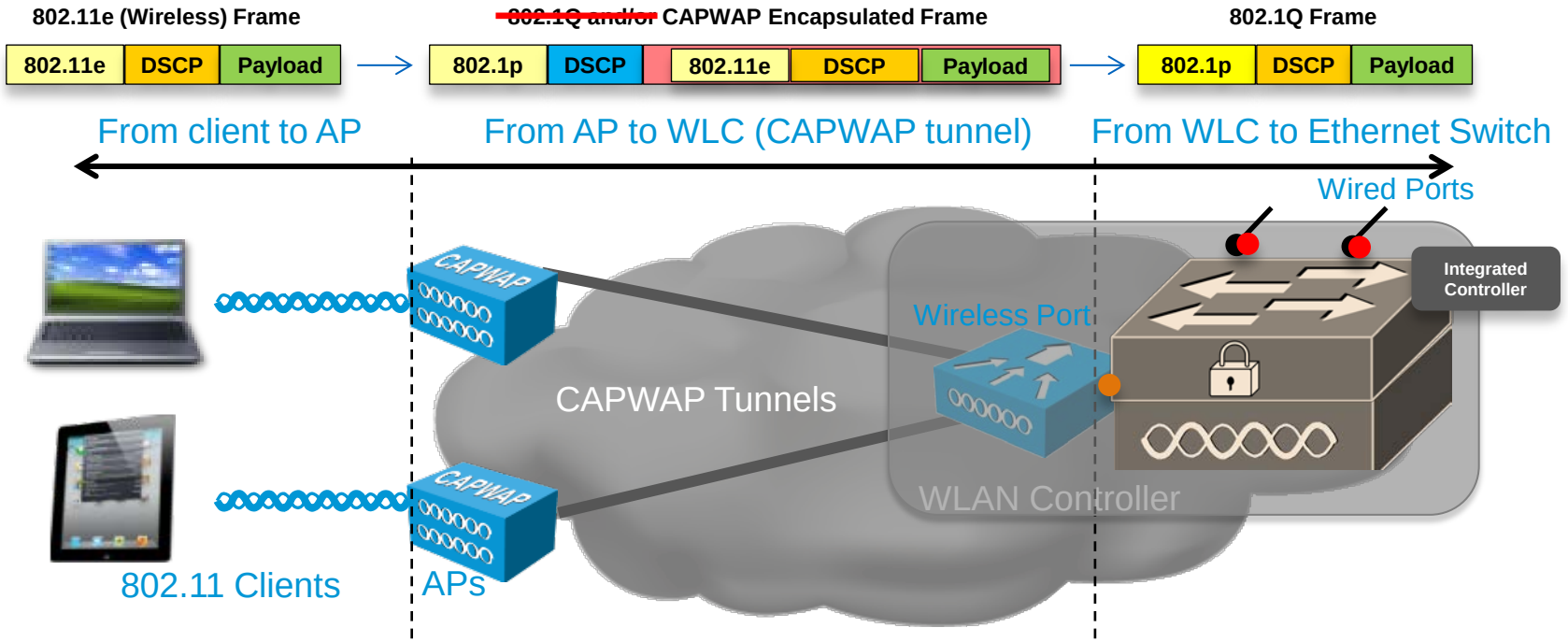


Agenda

- Converged Access QoS architecture overview
- QoS Refresher
- Existing QoS deployment – architecture refresher and challenges
- What Converged Access offers
- The Converged Access QoS architecture in detail
  - The QoS toolbox
  - Default behavior and QoS touch points
  - Queuing and the end of “trust”
- **Converged Access QoS design**
  - **SRND comparison**
  - Use Case

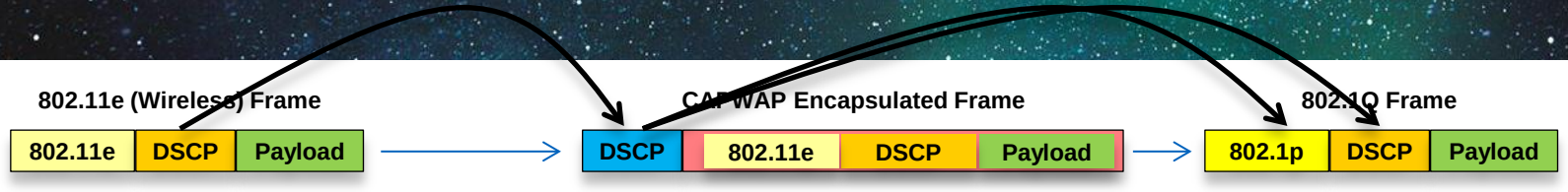
Wireless QoS

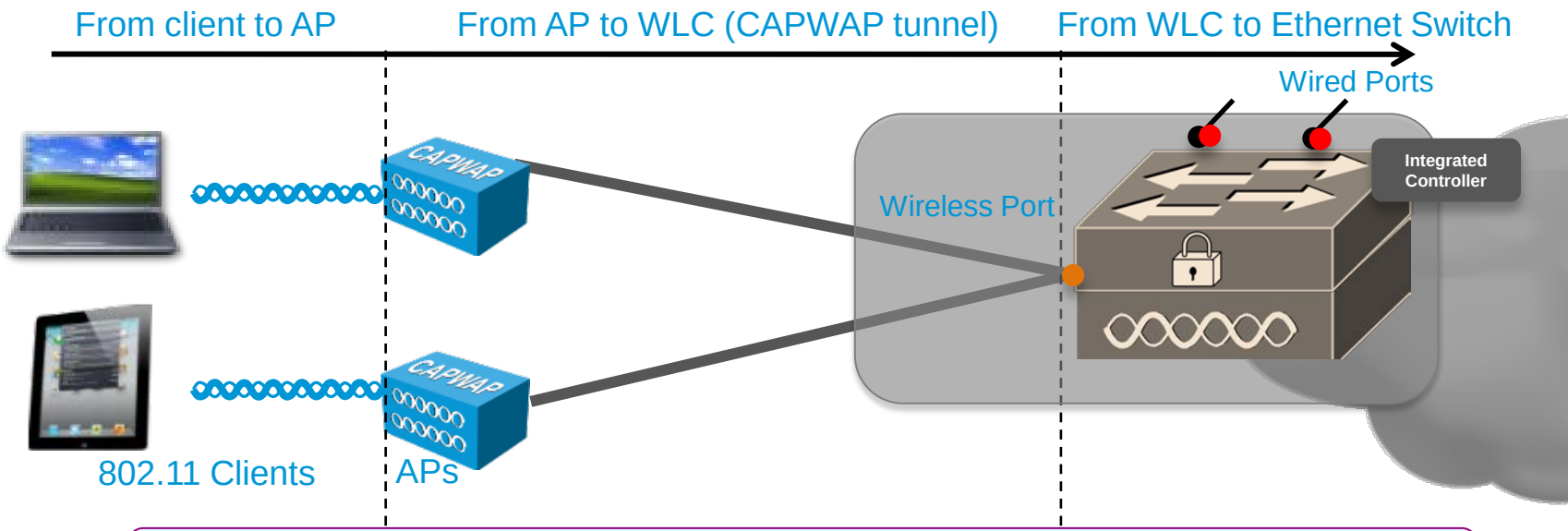
5508 WLC with AireOS 7.3 to Converged Access



Wireless QoS

3850 WLC – “TRUST DSCP”

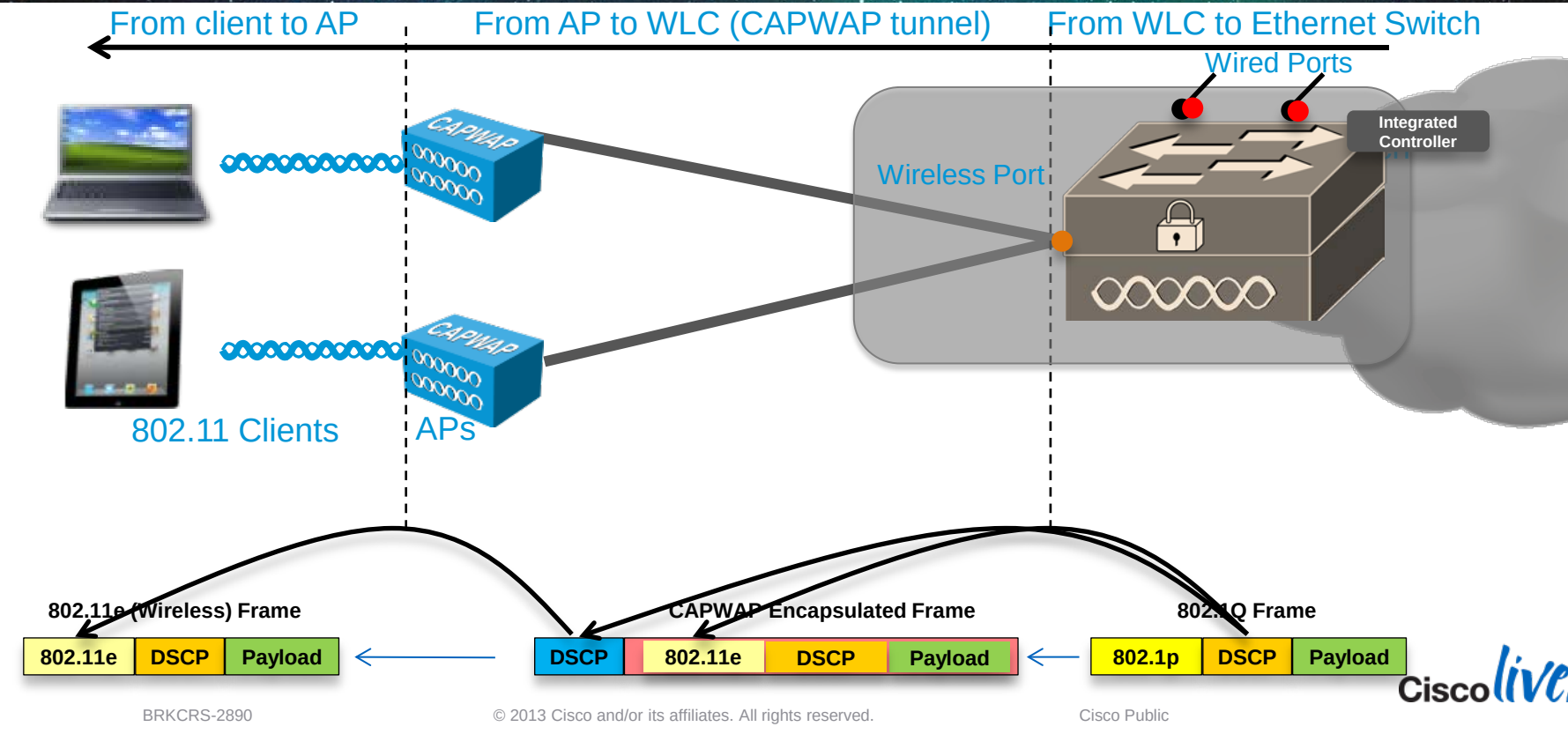




NOTE: Upstream SSID policies are pushed to APs. In this case Trust DSCP is extremely important.

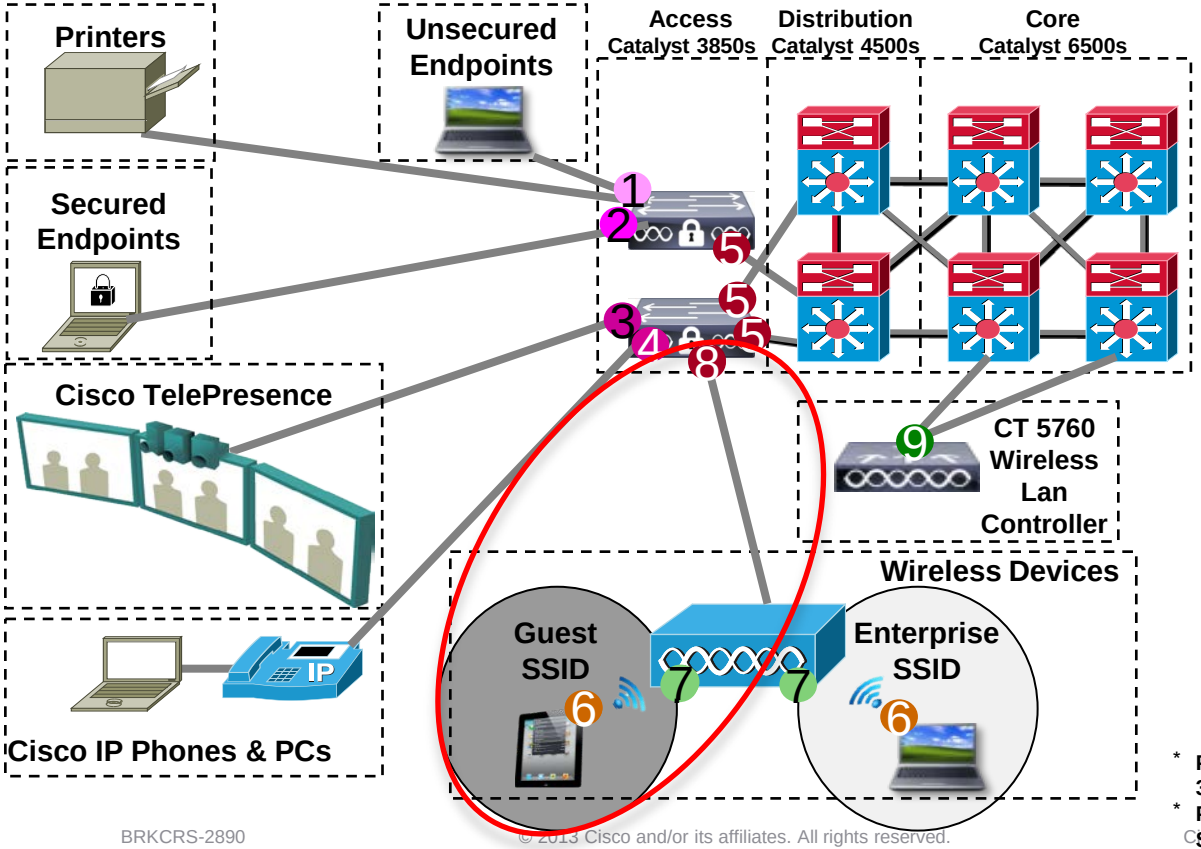
Wireless QoS

3850 WLC – “TRUST DSCP”



Catalyst 3850 Campus QoS Design

QoS Roles in Campus Networks



1 No Trust [OR] Classification/Marking + Egress Queuing

2 Trust DSCP + Egress Queuing

3 4 Conditional Trust + Egress Queuing

5 Trust DSCP + Egress Queueing

6* Classification/Marking + [Optional Policing] + Egress Queuing

7* Trust/Mark DSCP/WMM

8 Classification/Marking + [Optional Policing]+ Egress Queuing

9 Trust DSCP + Egress Queuing

* **Policies for wireless clients (6) reside on Catalyst 3850**

* **Policies for APs (7) are pushed from the upstream SSID level policy of Catalyst 3850**

What does a voice-only ssid look like now?

Option 1: Backward Compatible – Marking Only

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

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

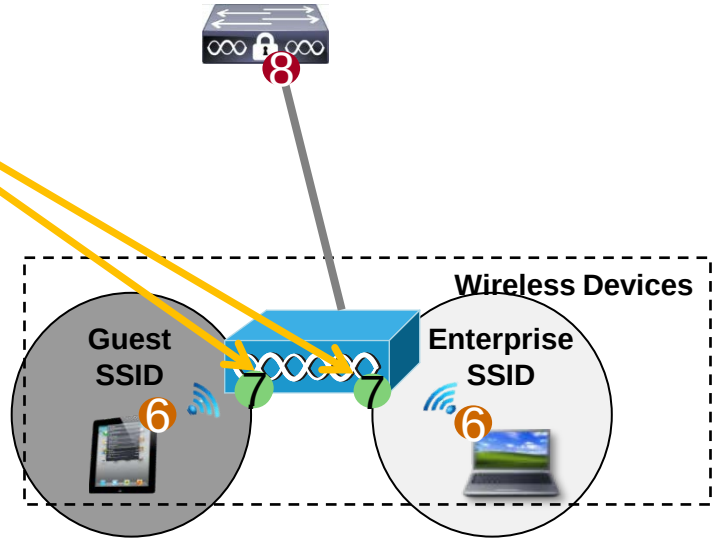
Table Map gold-dscp2dscp
- from 45 to 34
- from 46 to 34
- from 47 to 34
- default copy

SSID Policy - Platinum

7

```
policy-map platinum-up
 class class-default
   set dscp dscp table plat-dscp2dscp

policy-map platinum-down
 class class-default
   set dscp dscp table plat-dscp2dscp
   set wlan user-priority dscp table plat-dscp2up

wlan BRILEY-1 2 BRILEY-1
 aaa-override
 band-select
 client vlan 200
nac
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list method_list
 no shutdown
 service-policy input platinum-up
```

NOTE: Upstream classification/marking pushed to APs.



NOTE: Ingress DSCP values are trusted not classified based on application. Upstream no wmm value is used, downstream both dscp and wmm are required.

What does a voice-only ssid look like now?

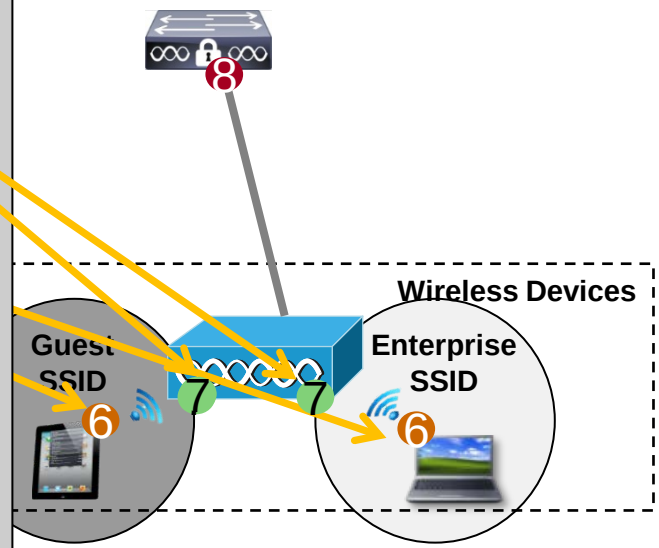
Option 2: Upstream **Limiter/Marker**

```
policy-map per-user-voice
 class VOIP
  set dscp ef
  police 128000 conf transmit exceed drop
 class VIDEO
  set dscp AF41
  police 384000 conf transmit exceed drop
 class SIGNALING
  set dscp cs3
  police 32000 conf transmit exceed drop
 class class-default
  set dscp default

wlan BRILEY-1 2 BRILEY-1
 aaa-override
 band-select
 client vlan 200
 …
 service-policy client input per-user-voice
 session-timeout 600
 no shutdown
```

SSID Policy – TRUST

```
policy-map tru…
 class class-…
  set dscp …

policy-ma…
 class clas…
  set dscp …
  set wlan us…ble dscp2up

wlan BRILEY-1 2 BRILEY-1
 aaa-override
 band-select
 client vlan 200
nac
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list method_list
 no shutdown
service-policy input trust-up
service-policy output trust-down
```

Trust Boundary Will be removed 3.3.0 SE



NOTE: Class-maps not shown for brevity – can be based on ACL, port ranges and DSCP/CoS…

What does CAC look like now?

SSID Policy – Platinum + CAC

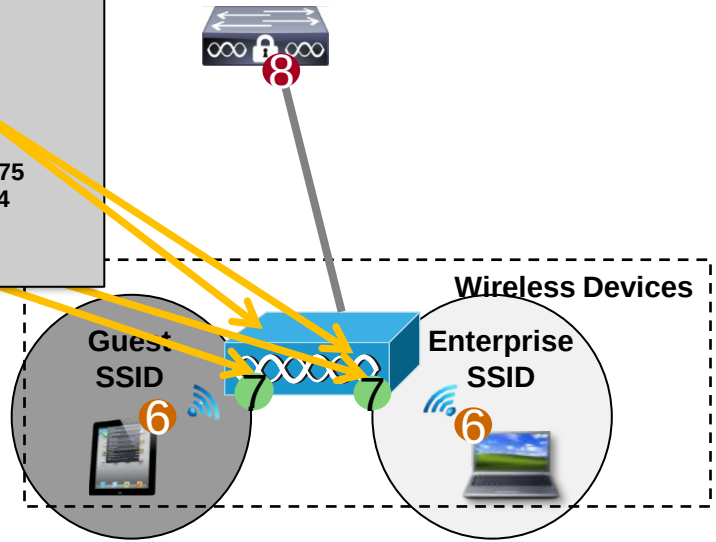
7

```
policy-map platinum-cac
 class voice-signaling
    priority level 1
    police cir  5m conform tran
    admit cac wmm-tspec
          rate 128
          wlan-up 6 7
 class video
     priority level 2
     police cir 15m conform tra

policy-map platinum-down
 class class-default
   shape average 20000000
      queue-buffer ratio 0
     set dscp dscp table plat-dscp2dscp
     set wlan user-priority dscp table plat-dscp2up
   service-policy platinum-cac

wlan BRILEY-1 2 BRILEY-1
 aaa-override
 band-select
 client vlan 200
 …
 no shutdown
 service-policy input platinum-up
 service-policy output platinum-down
 session-timeout 600
 no shutdown
```

Voice CAC

7

```
C3850# config t

C3850(config)#   ap dot11 5ghz shutdown

C3850(config)#   ap dot11 5ghz cac voice acm
C3850(config)#  no  ap dot11 5ghz cac voice load-based
 ! For Cisco 7925 - We set up a static CAC for iPhone
 ! NO – sets up static CAC
C3850(config)#  ap dot11 5ghz cac voice max-bandwidth 75
C3850(config)#  ap dot11 5ghz cac voice sip bandwidth 64

C3850(config)#  no ap dot11 5ghz shutdown
```

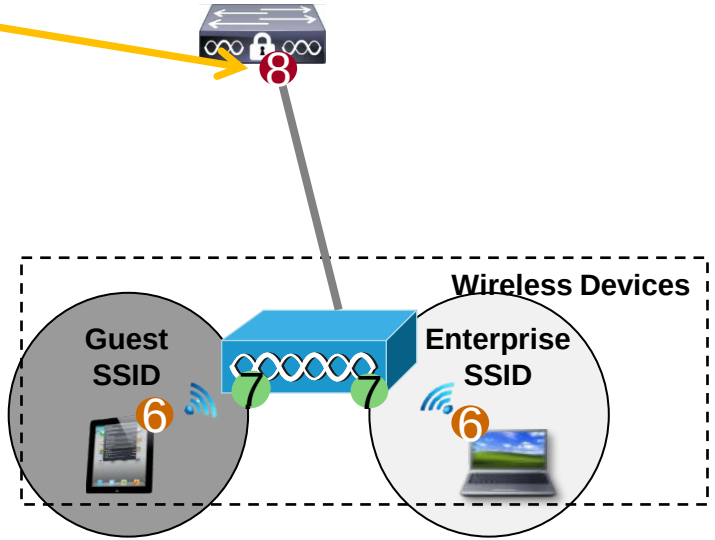


What does wireless port queuing look like now?

Wireless Port Policy

8

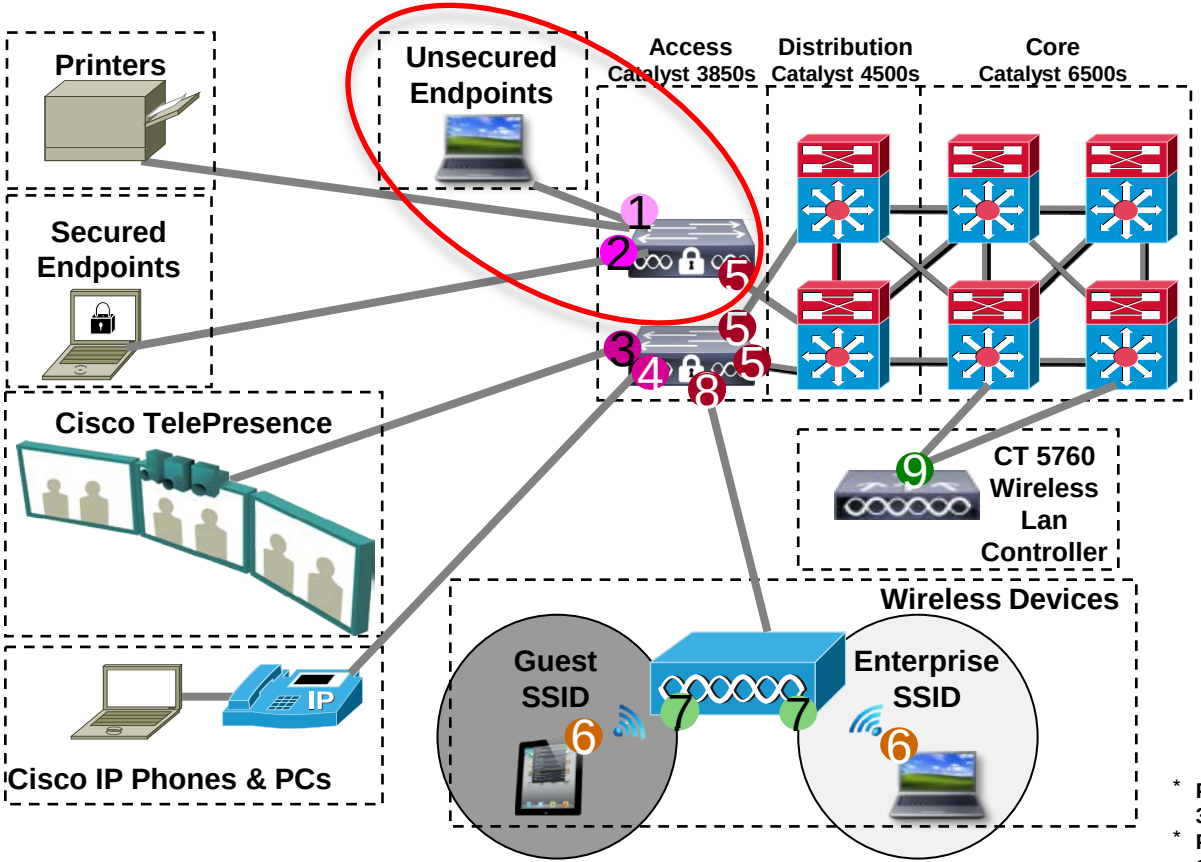
```
policy-map port_child_policy
class non-client-nrt-class
  bandwidth remaining ratio 7
class voice
  priority level 1
 police rate percent 10
   conform-action transmit
   exceed-action drop
class video
  priority level 2
 police rate percent 20
   conform-action transmit
   exceed-action drop
class class-default
  bandwidth remaining ratio 63
```



NOTE: Policing at the port level is for Multicast traffic, SSID or Client level policers are Unicast.

Catalyst 3850 Campus QoS Design

QoS Roles in Campus Networks



1 No Trust [OR] Classification/Marking + Egress Queuing

2 Trust DSCP + Egress Queuing

3 4 Conditional Trust + Egress Queuing

5 Trust DSCP + Egress Queueing

6* Classification/Marking + [Optional Policing] + Egress Queuing

7* Trust/Mark DSCP/WMM

8 Classification/Marking + [Optional Policing]+ Egress Queuing

9 Trust DSCP + Egress Queuing

* Policies for wireless clients (6) reside on Catalyst 3850

* Policies for APs (7) are pushed from the upstream SSID level policy of Catalyst 3850

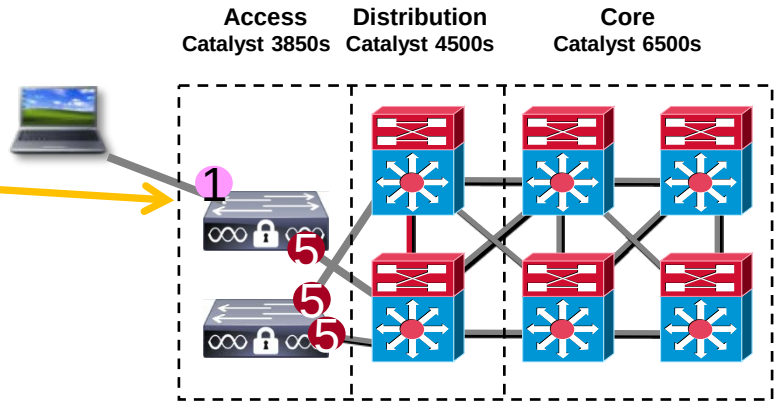
Catalyst 3850 Campus QoS Design
Service Policy Model Example – Marking Policy

Wired Untrusted Client Port Policy

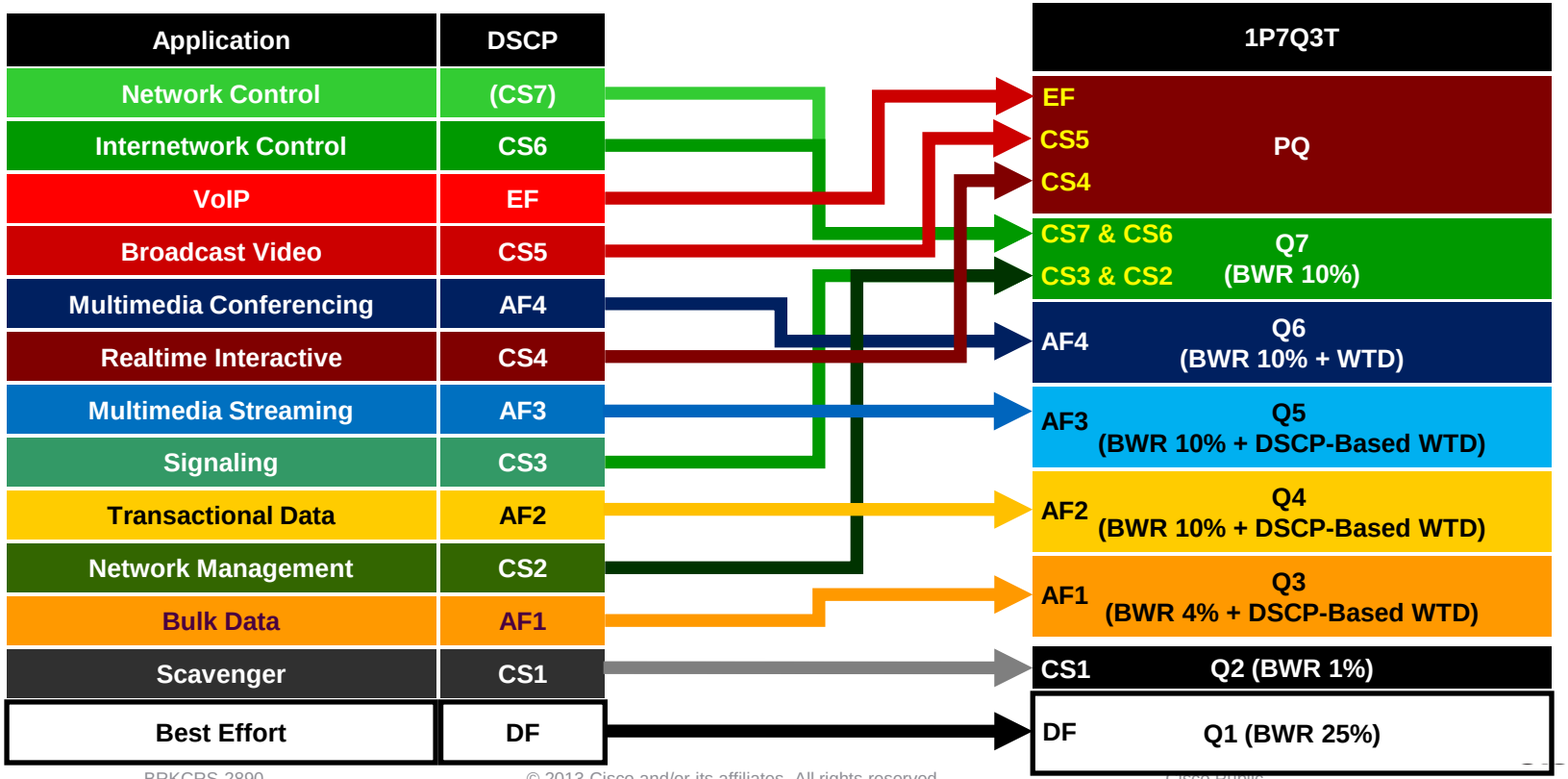
1

[class-maps omitted for brevity]

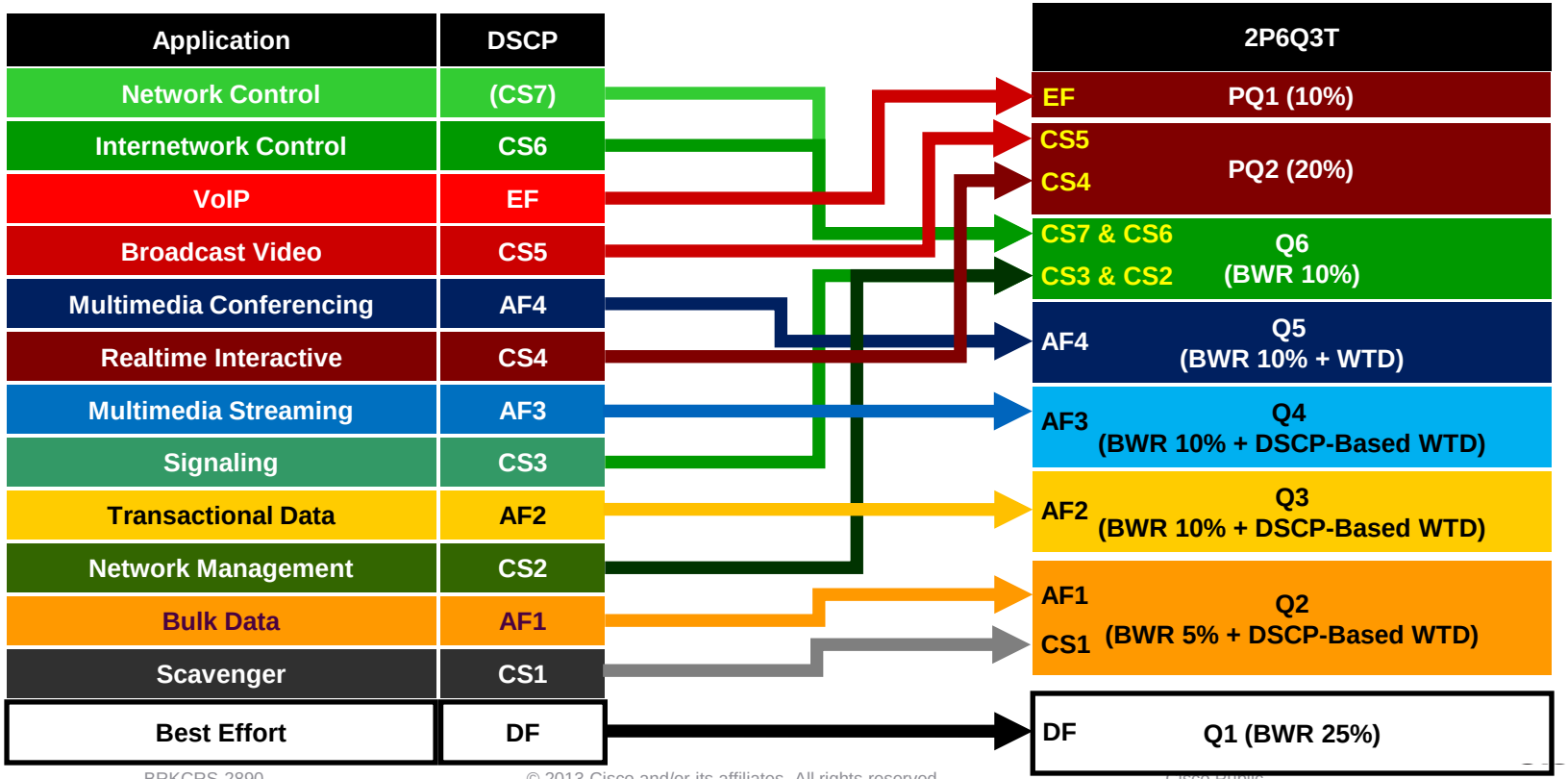
```
policy-map MARKING-POLICY
 class VOIP
  set dscp ef
 class MULTIMEDIA-CONFERENCING
  set dscp af41
 class SIGNALING
  set dscp cs3
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class DEFAULT
  set dscp default

Interface GigabitEthernet 1/0/1
service-policy input MARKING-POLICY
```



Catalyst 3850 Campus QoS Design
Egress Queuing (1P7Q3T with WTD) Model



Catalyst 3850 Campus QoS Design
Egress Queuing (2P6Q3T with WTD) Model



Catalyst 3850 Campus QoS Design

Egress Queuing (2P6Q3T) Example – Part 2 (Policy-Map)

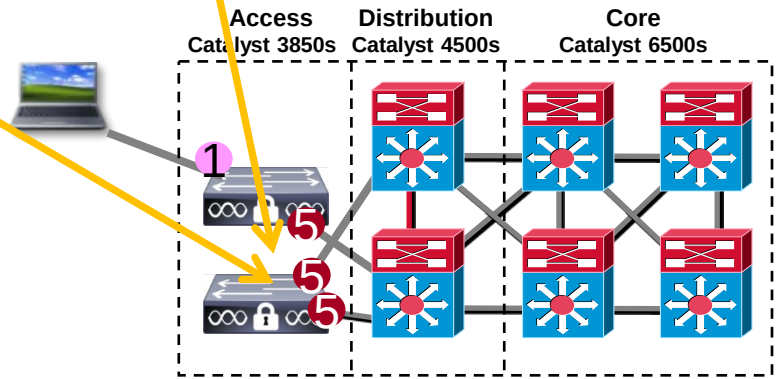
```
! This section configures policy-map
policy-map 2PQ3T
 class PRIORITY-QUEUE
  priority level 1
   police rate percent 20 …
Class REAL-TIME-VIDEO-QUEUE
  priority level 2
   police rate percent 10 …
class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
class MULTIMEDIA-CONFERENCING-QUEUE
 bandwidth remaining percent 10
  queue-limit dscp af43 percent 80
  queue-limit dscp af42 percent 90
  queue-limit dscp af41 percent 100
class MULTIMEDIA-STREAMING-QUEUE
 bandwidth remaining percent 10
  queue-limit dscp af33 percent 80
  queue-limit dscp af32 percent 90
  queue-limit dscp af31 percent 100
class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 10
  queue-limit dscp af23 percent 80
  queue-limit dscp af22 percent 90
  queue-limit dscp af21 percent 100
```

5

```
[continued]
  class BULK-SCAVENGER-DATA-QUEUE
  bandwidth remaining percent 5
  queue-limit dscp cs1 percent 80
  queue-limit dscp af12 percent 90
  queue-limit dscp af11 percent 100
 class class-default
  bandwidth remaining percent 25
```

5

```
! This section attaches the policy to the int(s)
service-policy output 2P6Q3T
```



Agenda

- Converged Access QoS architecture overview
- QoS Refresher
- Existing QoS deployment – architecture refresher and challenges
- What Converged Access offers
- The Converged Access QoS architecture in detail
  - The QoS toolbox
  - Default behavior and QoS touch points
  - Queuing and the end of “trust”
- Converged Access QoS design options
  - SRND comparison
  - **Use Case**

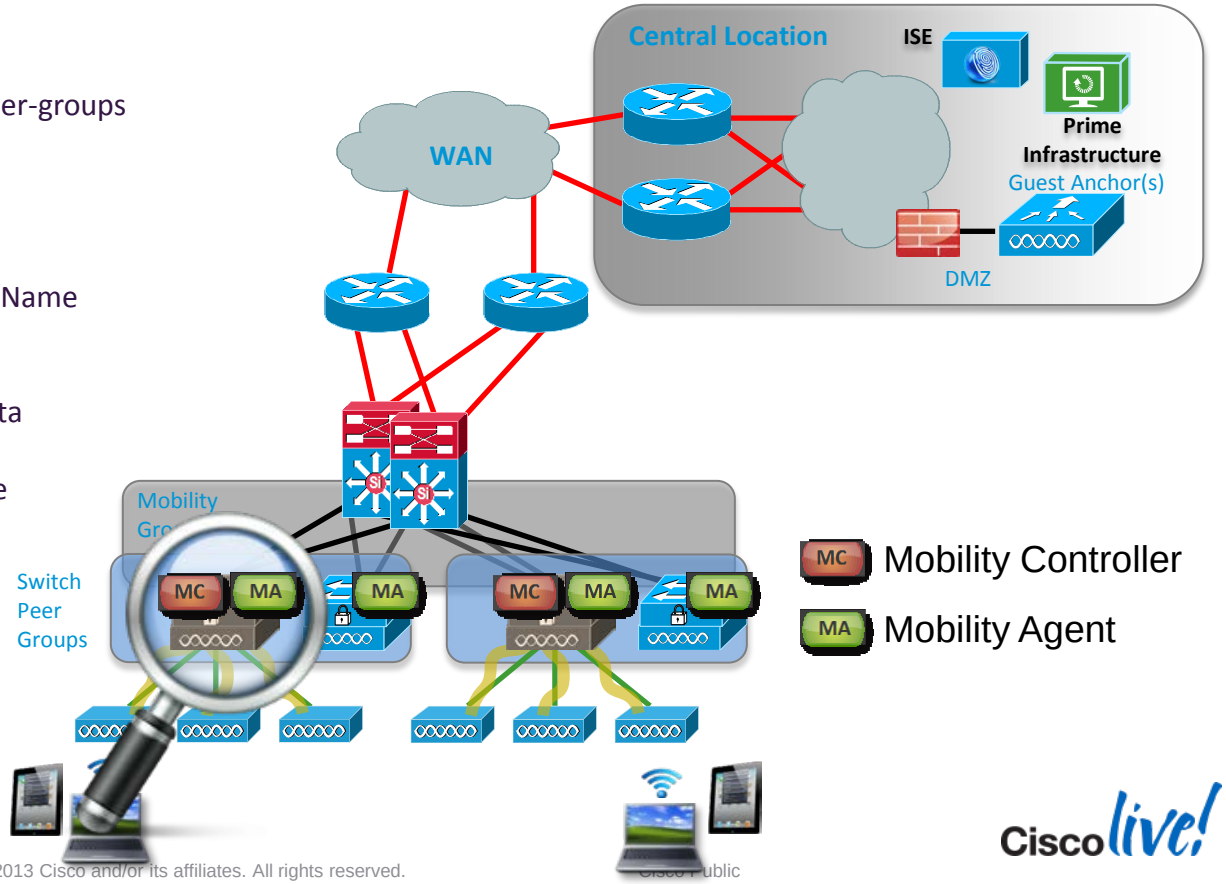
Converged Access – Deployment Scenario

Goals:

- Use ISE to incrementally add new users/user-groups
- Align Wired and Wireless QoS policies

Details of Deployment:

- ISE provisions users and ties to QoS policy Name
- Deploy 2 SSIDs – FACULTY, STUDENT
- Faculty and Students are authenticated
- Both groups provided Voice, Video and Data guarantees
- Each group is given a bandwidth guarantee
- Each user provided fairness

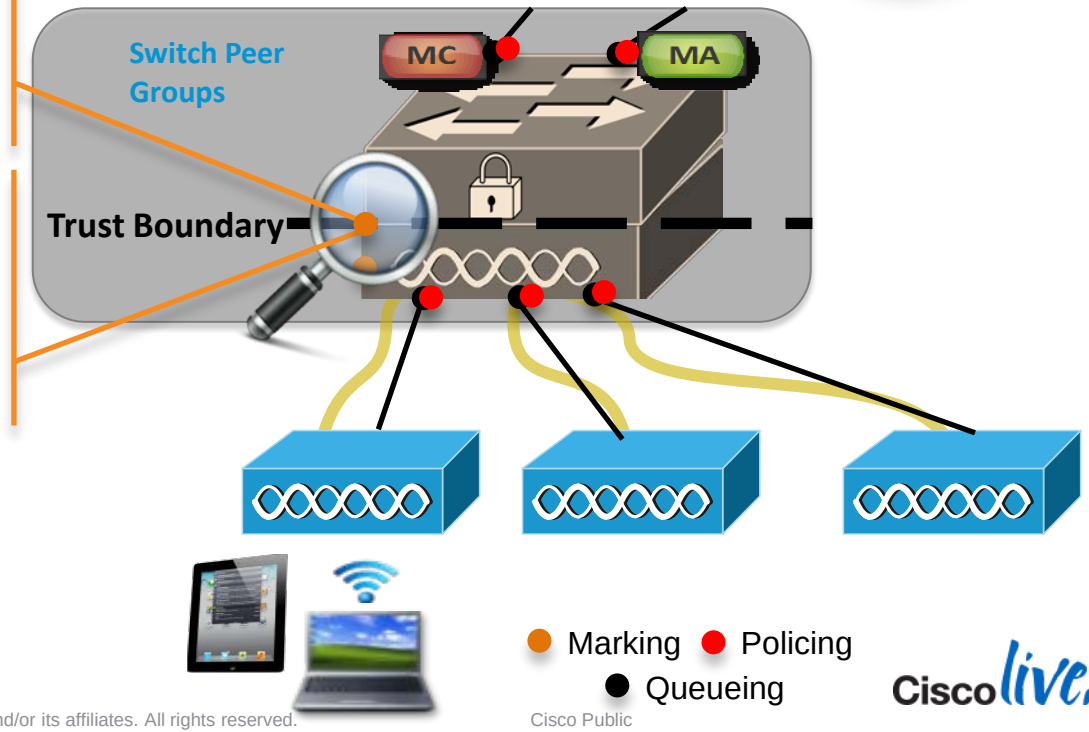


Converged Access – Deployment Scenario
Bandwidth unfairness

Trust Boundary Will be removed 3.3.0 SE

```
table-map dscp2dscp
default copy

Policy-map TRUST-BW-FACULTY
Class class-default
  set dscp dscp table dscp2dscp
  set wlan user-priority dscp table dscp2up
   bandwidth remaining ratio 90
```

```
table-map dscp2dscp
default copy

Policy-map TRUST-BW-STUDENTS
Class class-default
  set dscp dscp table dscp2dscp
  set wlan user-priority dscp table dscp2up
   bandwidth remaining ratio 10
```



Interface Configuration:

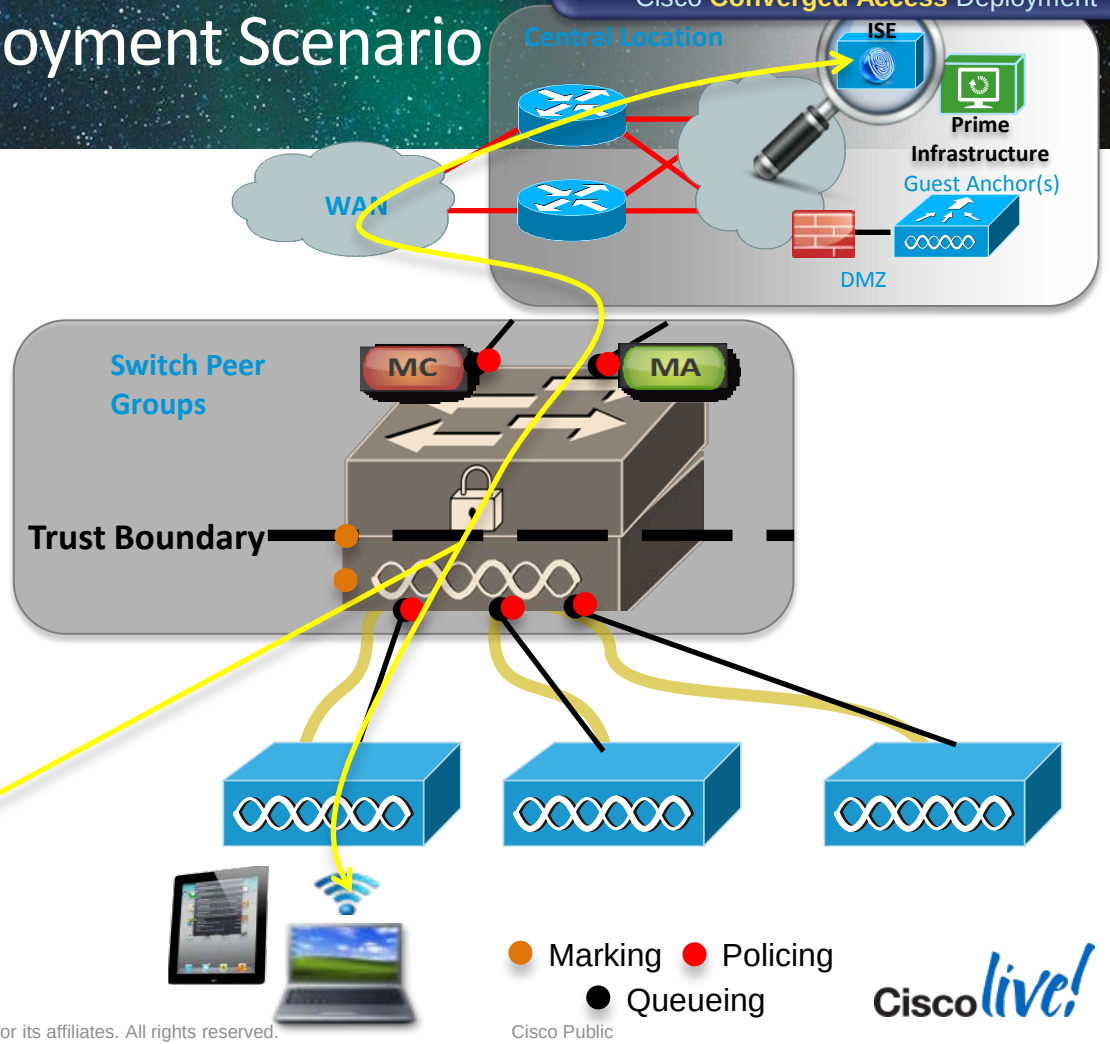
```
wlan FACULTY 3 FACULTY
 aaa-override
 client vlan 67
 …
service-policy out TRUST-BW-FACULTY
```

Converged Access – Deployment Scenario
Classification and Marking

Cisco Identity Services Engine (ISE)
- Group configured for FACULTY
- Group configured for FACULTY via ISE or AD
- QoS policy name provided per Group
- QoS policy name pushed to 3850 from ISE

Per user MQC policy
- QoS Policy pre-configured on 3850
- After client authentication, policy applied to client on ingress

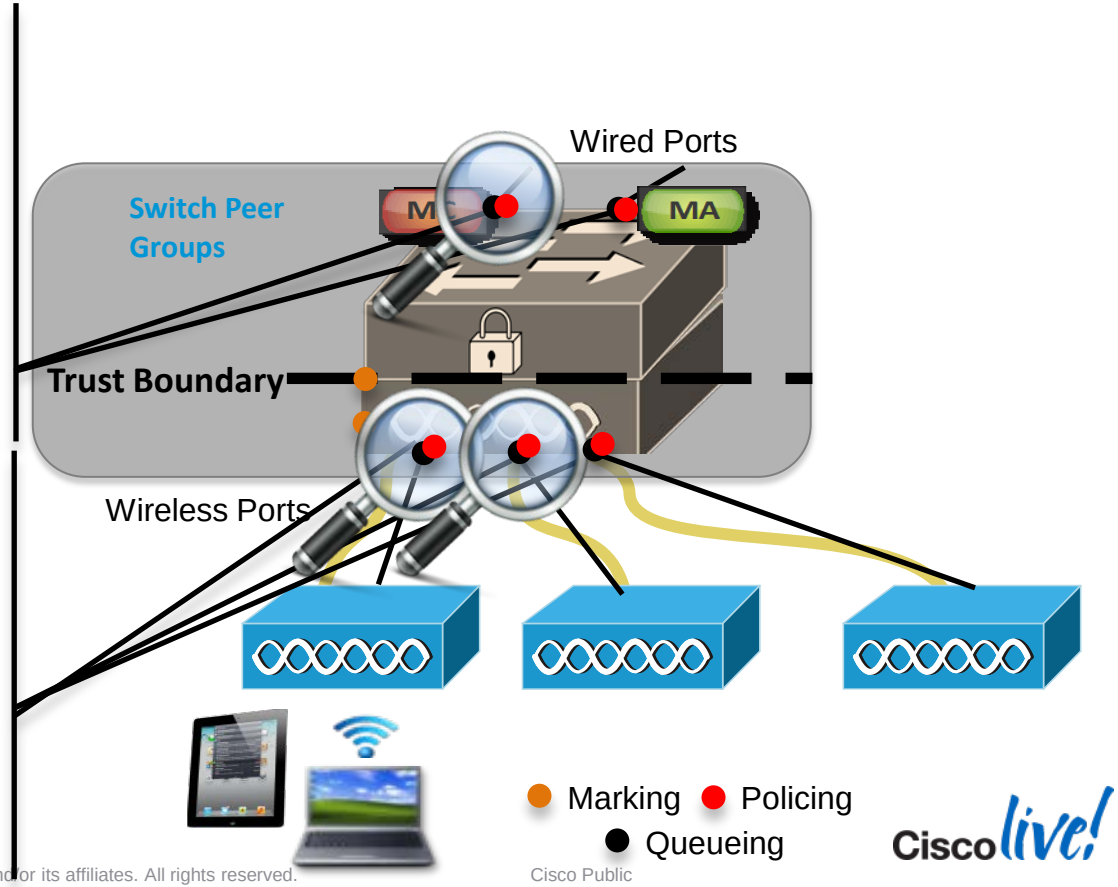
```
policy-map FACULTY
 class VOIP
   set dscp ef
   police 128000 conf transmit exceed drop
 class VIDEO
   set dscp AF41
   police 384000 conf transmit exceed drop
 class SIGNALING
   set dscp cs3
   police 32000 conf transmit exceed drop
 class TRANSACTIONAL-DATA
   set dscp af21
 class class-default
   set dscp default
```



Converged Access – Deployment Scenario
Queuing

```
policy-map 2P6Q3T
 class PRIORITY-QUEUE-1
   priority level 1
    police rate per 10 conf tran exceed drop
 class PRIORITY-QUEUE-2
   priority level 2
    police rate per 20 conf tran exceed drop
 class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 20
 class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 20
 class SCAVENGER
    bandwidth remaining percent 5
 class class-default
    bandwidth remaining percent 25
```

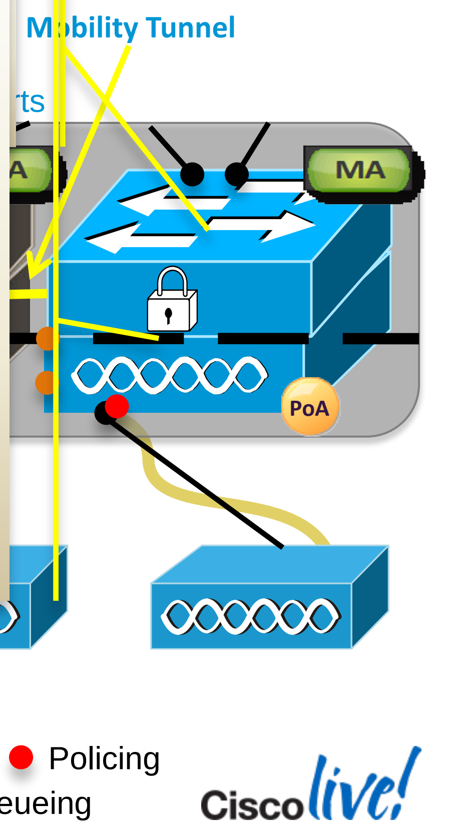
```
policy-map port_child_policy
 class non-client-nrt-class
  bandwidth remaining ratio 7
 class voice
  priority level 1
  police rate percent 10
   conform-action transmit
   exceed-action drop
 class video
  priority level 2
  police rate percent 20
   conform-action transmit
   exceed-action drop
 class class-default
  bandwidth remaining ratio 63
```



Converged Access, Deployment – QoS and Mobility

```
L09-3850-2#sh wireless client sum
Number of Local Clients : 1

                                                WLAN State
-----------------------------------
                                                4    UP
2123.345d det

fe23 345d
System
port
40 (36413)
```

```
L09-3850-1#show policy-map int wireless client
L09-3850-1#sh wireless client sum
Number of Local Clients : 1

MAC Address    AP Name                          WLAN State              Protocol
--------------------------------------------------------------------------------
c8aa.2123.345d 10.101.2.109                     4    UP                 Mobile
Mac Address    VlanId IP Address      Src If                 Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
c8aa.2123.345d   3000 10.101.255.1    0x00DCD1C00000000B RUN      ANCHOR
Protocol
-----------------------------------------------------------------------------
---
c8aa.2123.345d APd48c.b5e4.4e8a                 4    UP
11n(2.4)

L09-3850-1#show policy-map int wireless client

Client C8AA.2123.345D iifid:
0x0105C38000000019.0x00CBD9000000003E.0x00CE020000000040.0x00F4BC0000000041

  Service-policy input: FACULTY

    Class-map: VOIP (match-any)
      Match: ip dscp ef (46)
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 4000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps  …
```



Cisco live!

Things to know before you go

- Make sure the radios are up
- What defaults cannot be changed
  - Radio shapers, Port shaper on wireless ports
  - AFD cannot be turned off
- Troubleshooting commands that are quite useful:
  - Show policy-map interface
  - Show platform qos dscp-cos counters gigabit
  - Show platform qos policy hw_state target gigabit
  - Show platform qos queue config gigabit
  - Show platform qos queue stats gigabit
  - Show platform qos policies (client, port, radio, ssid)

Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Cisco Daily Challenge points for each session evaluation you complete.
- Complete your session evaluation online now through either the mobile app or internet kiosk stations.

Maximize your Cisco Live experience with your free Cisco Live 365 account. Download session PDFs, view sessions on-demand and participate in live activities throughout the year. Click the Enter Cisco Live 365 button in your Cisco Live portal to log in.


CISCO
TM

Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Cisco Daily Challenge points for each session evaluation you complete.
- Complete your session evaluation online now through either the mobile app or internet kiosk stations.

Maximize your Cisco Live experience with your free Cisco Live 365 account. Download session PDFs, view sessions on-demand and participate in live activities throughout the year. Click the Enter Cisco Live 365 button in your Cisco Live portal to log in.

Note: This slide is now a Layout choice


CISCO
TM