
TOMORROW starts here.
cisco
Cisco live!

Call Admission Control and Quality of Service for Collaboration

BRKUCC-2667

Glen Lavers

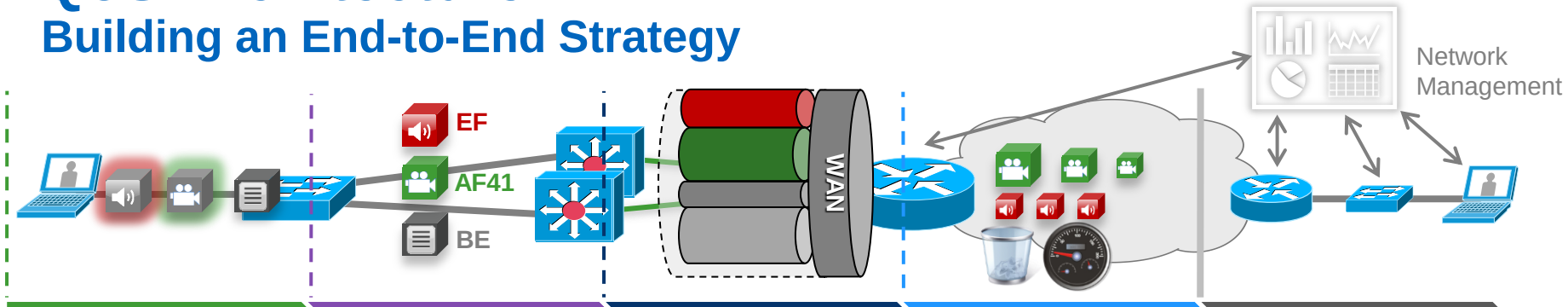
Senior Technical Marketing Engineer

Cisco live!

Agenda

- Introduction – Session Overview
- Media Resilience and Adaptation
  - Resilience techniques
  - Dynamic adaptation and advantages
- Enhanced Locations CAC Architecture
  - Network Modelling
  - Locations Bandwidth Manager (LBM)
  - Inter-Cluster E-LCAC with LBM
- QoS Architecture
  - Approach Overview
  - Identification & Classification
  - Queuing / Scheduling

QoS Architecture
Building an End-to-End Strategy



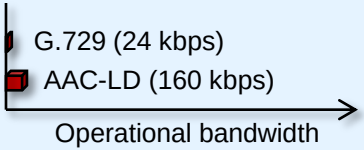
Identify	Classify	Schedule	Provision Resource Control	Monitor Troubleshoot Optimise

• Trusted devices
• Untrusted devices:
  • Map UDP/TCP Port Ranges
  • Medianet Metadata
• Wireless
	• Map identified traffic to its correct QoS marking
	• QoS marking: COS, DSCP, UP (WiFi)
	
	BRKCRS-2501: Campus QoS Design Simplified
		• Low Latency Queuing (LLQ)
		  • Priority Queuing (PQ)
		  • Class Based Weighted Fair Queue (CBWFQ)
		• Weighted Random Early Detection (WRED)
			• Call Admission Control
			• Media Resilience and Rate Adaptation
			• Bandwidth Provisioning
				• Prime Collaboration Monitoring Assurance and Diagnostics
				• Monitors Voice, Video, Inventory and Fault Management
				
				BRKEVT-2804: "Monitoring and troubleshooting network impairments in video deployments"

Media Resilience and Adaptation

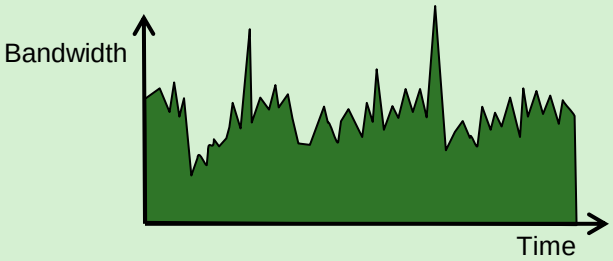
Video Traffic: Requirements and Profiles

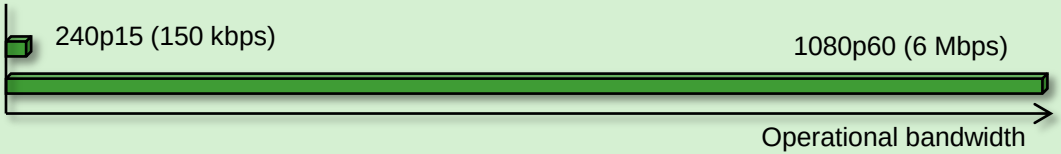
AUDIO



- **Bandwidth**:
  - Constant bitrate (smooth)
  - Small footprint
  - Narrow operational range (1:6)
- **Loss**-sensitive
- **Delay**-sensitive

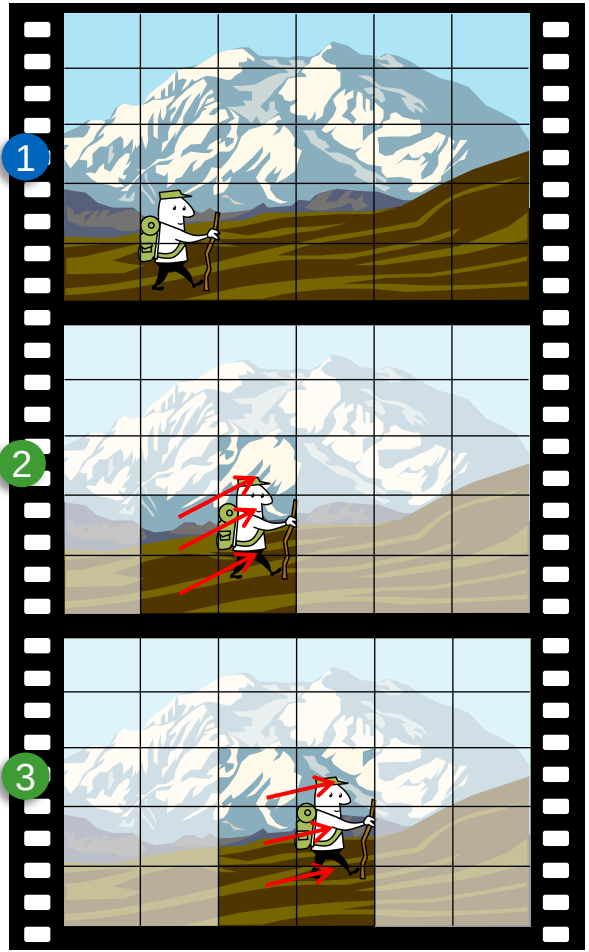
VIDEO





- **Bandwidth**:
  - Variable bitrate (bursty)
  - Medium/large footprint
  - Wide operational range (1:40)
- **Loss**-sensitive
- **Delay**-sensitive

Video Traffic
Video Encoding Basics



1 I-Frame
"Intra-coded" picture

- Entire picture encoded as a static image
- No reference to other frames

2 P-Frame
"Predicted" picture

- Based on a previously encoded frame (1)
- Only the differences from that frame are encoded

3 P-Frame
"Predicted" picture

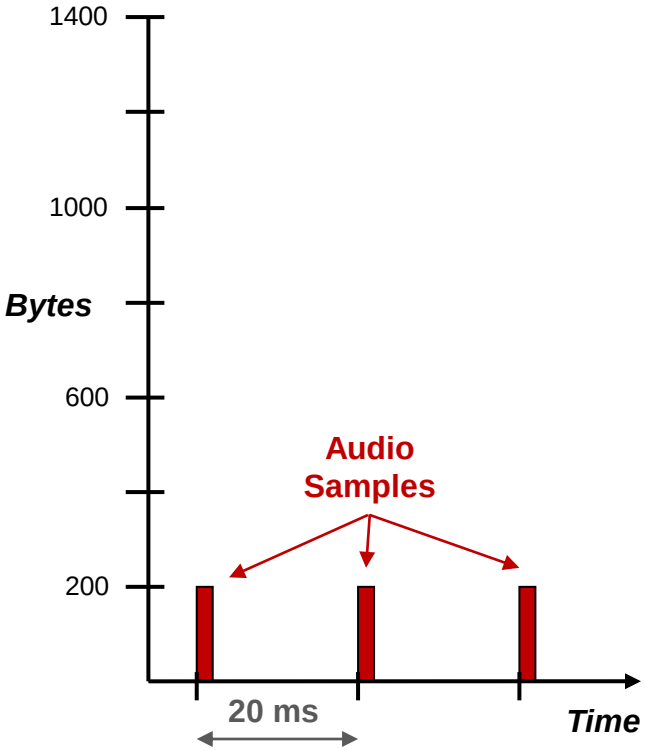
- Reference for prediction can be another P-Frame (2)

For more, see **BRKCOL-2777**: "Emerging Video Technologies: H.265, SVC, WebRTC / HTML5"

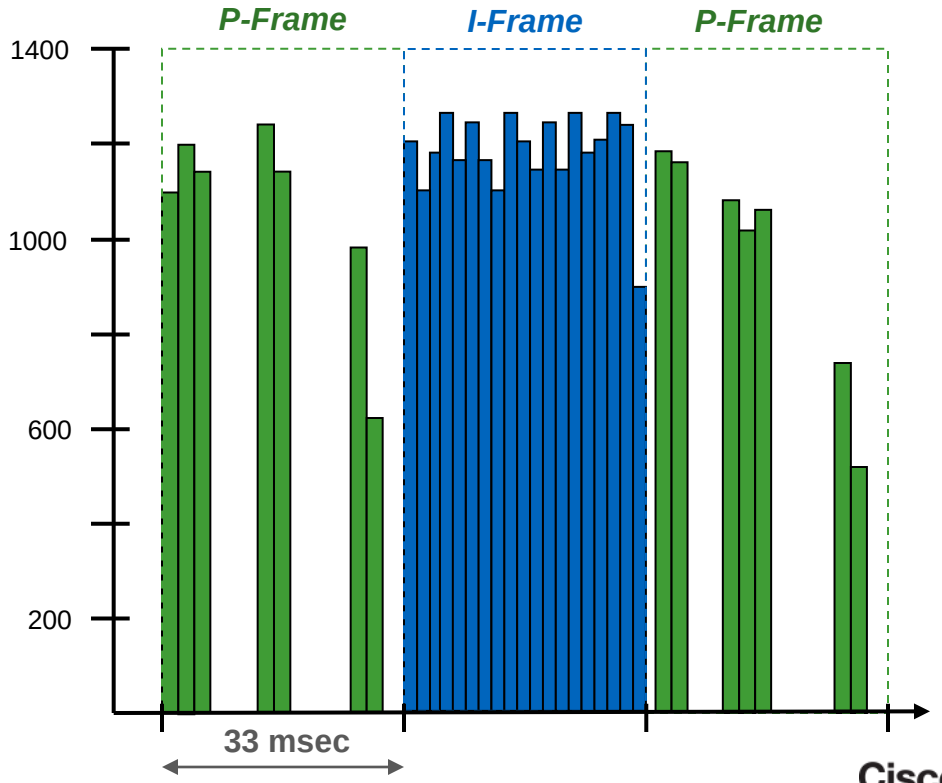
Video Traffic

Audio vs. Video Packet Distribution

Audio Packets

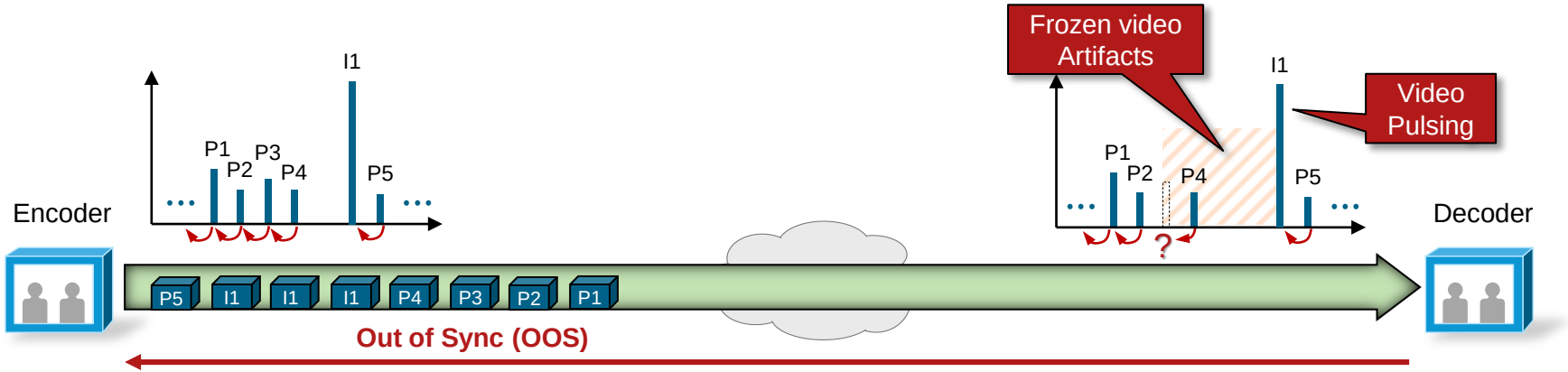


Video Packets



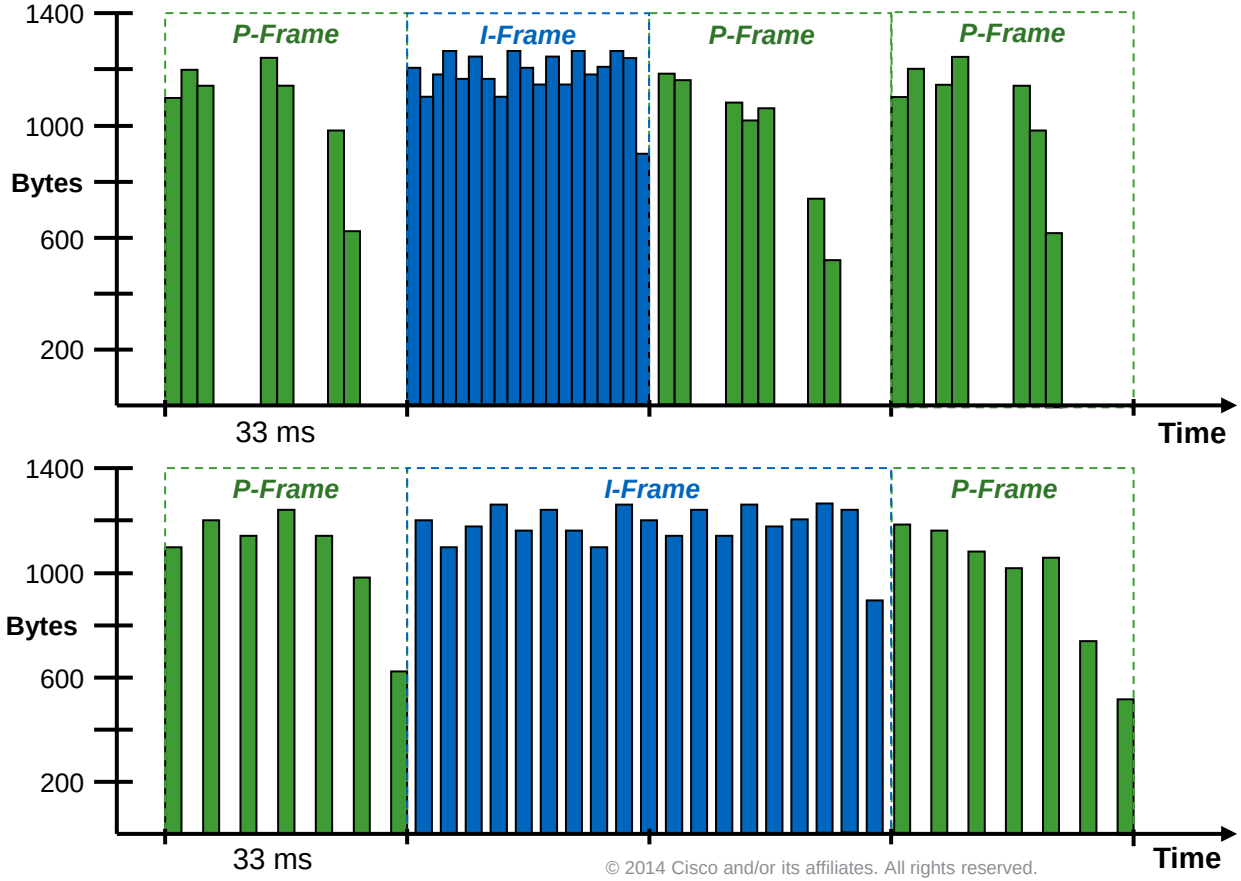
Video Traffic

Impact of Packet Loss on a Video Stream



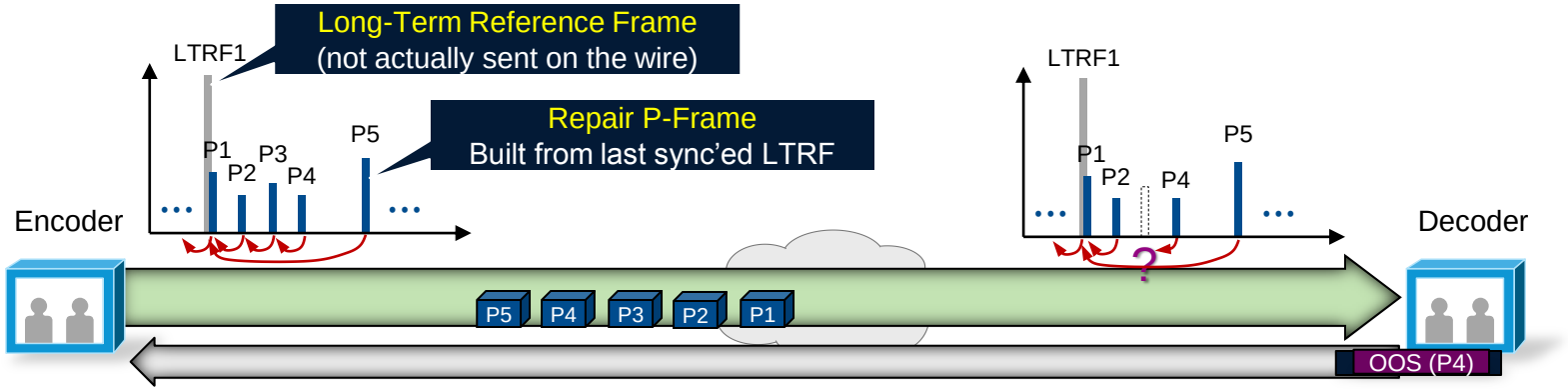
- Loss of a P-frame triggers request for a new I-frame
  - Encoding and transmitting large I-frame takes time
  - If any of the I-frame packets get lost, the process needs to restart
  - I-frame creates burst that risks exacerbating network congestion (more packet loss!)
- Flickering/pulsing of video when new I-frame arrives
  - Video freeze or artifacts when multiple packets are lost

Media Resilience
Encoder Pacing



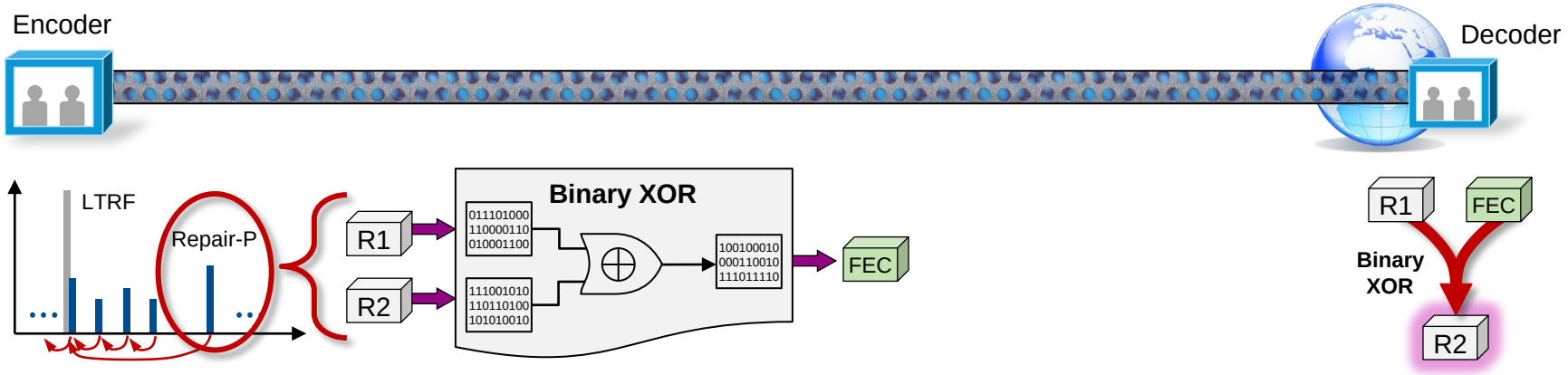
- Each frame must be packetised onto the wire in 33 ms
- Endpoint packet scheduler disperses packets as evenly as possible
- Large I-frames may need to be “spread” over 2 or 3 frame intervals
  - Encoder may then ‘skip’ 1-2 frames to stay within bitrate budget

Media Resilience
Long Term Reference Frame (LTRF) with Repair



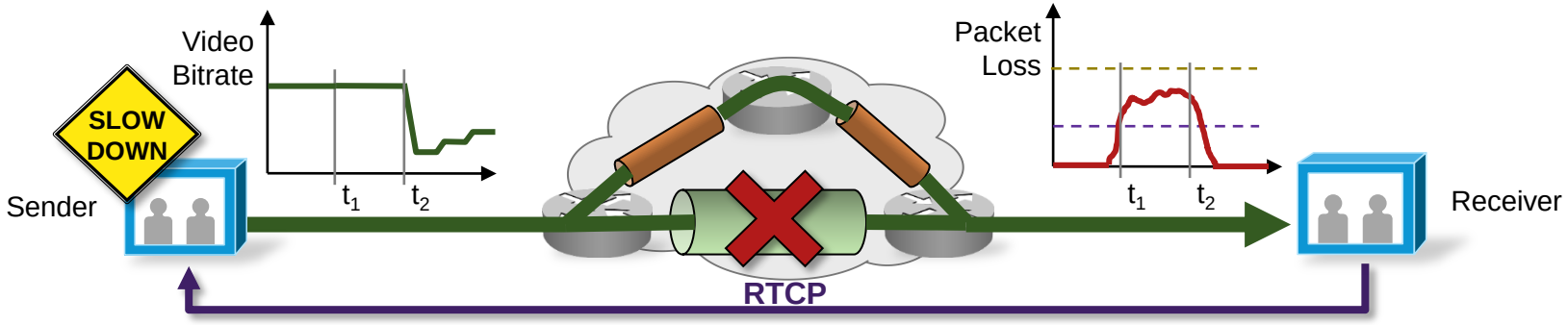
- Keep encoder and decoder in sync with active feedback messages
  - Encoder instructs decoder to store raw frames at specific sync points as Long-Term Reference Frames (part of H.264 standard)
  - Decoder uses "back channel" (i.e. RTCP) to acknowledge LTRF's
- When a frame is lost, encoder creates a "Repair" P-frame based on the last synchronised LTRF instead of generating a new I-frame

Media Resilience
Forward Error Correction (FEC)



- Allows decoder to recover from limited amount of packet loss without losing synchronisation
- Can be applied at different levels (*x* FEC packets every *N* data packets) to protect “important” frames in lossy environments
- Correction code can be basic (binary XOR) or more advanced (Reed-Solomon)
- Trade-off is bandwidth increase—best suited for non-bursty loss

Rate Adaptation
Key Idea



- Receiver observes delay and packet loss over periods of time and signals back using RTCP Receiver Reports (RR)
- Reports cause the sender to adjust bitrate so as to adapt to network conditions *(downspeeding, upspeeding)*
- Two approaches possible:
  - **Sender-initiated** adjustment based on RTCP Receiver Reports
  - **Receiver-initiated** adjustment via call signalling (H.323 flow control, TMBRR, SIP Re-invite) or explicit request in RTCP message

“Smart” Media Techniques

Support in Cisco Collaboration Devices

remove encoder pacing column if removing encoder pacing slide

Endpoint / Bridge	Encoder Pacing	Rate Adaptation	FEC	LTRF Repair
89xx, 99xx	✓	*future*	*future*	--
DX	✓	✓	*future*	*future*
WebEx	✓	✓	✓	*future*
TX	✓	✓	*future*	✓
Jabber	✓	✓	✓	✓
C/EX/MX/SX/Profile	✓	✓	✓	✓
TS	✓	✓	✓ *(3.1)*	✓ *(3.1)*
MCU	✓	✓	✓ *(4.5)*	✓ *(4.5)*

ClearPath

“Smart” Media Techniques
Key Takeaways

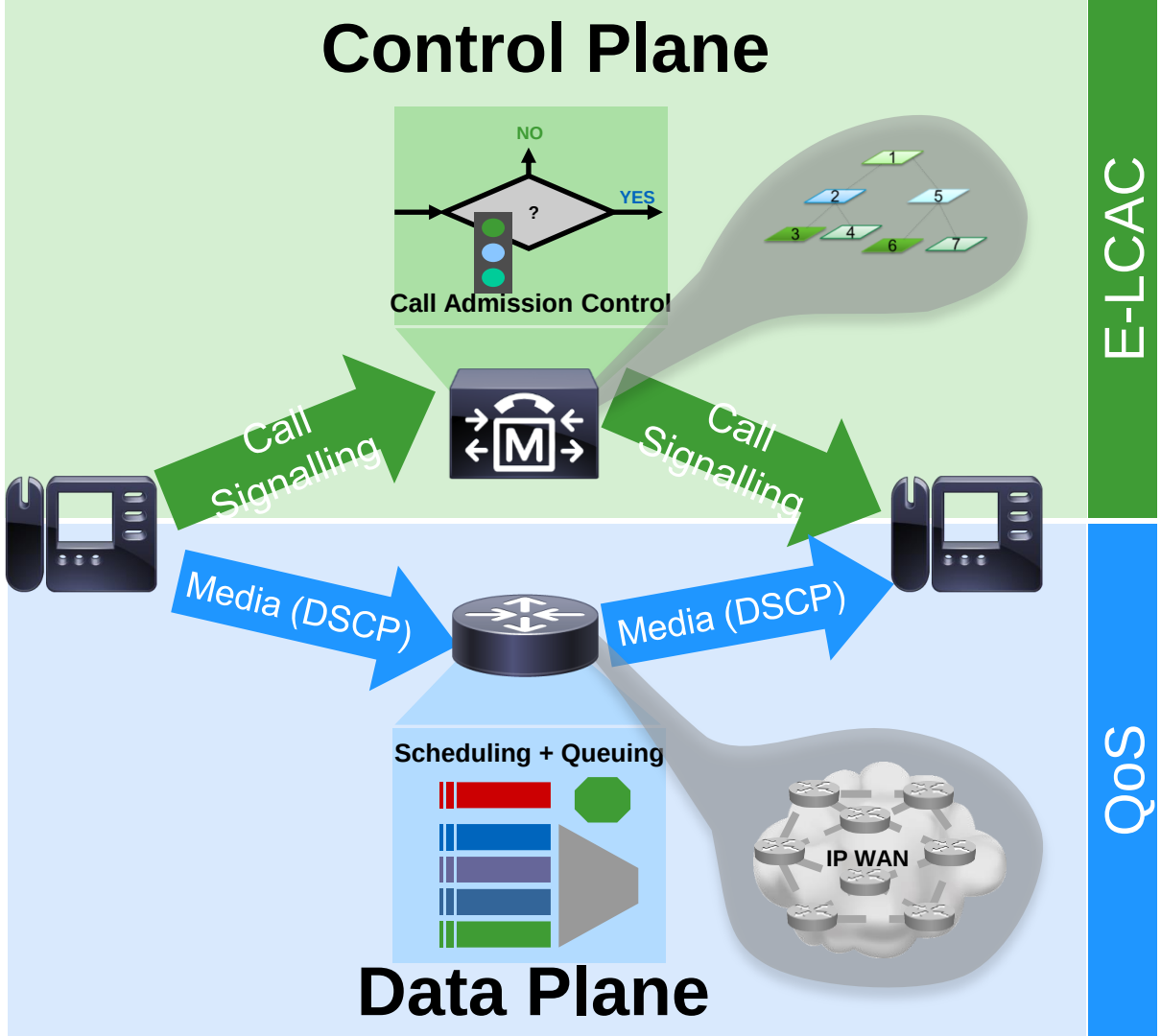
- Burstiness of traffic and mobility of the endpoints make deterministic provisioning for interactive video difficult for network administrators
- **Media resilience** mechanisms help mitigate impact of video traffic on the network and impact of network impairments on video
- Dynamic **rate adaptation** creates an opportunity for more flexible provisioning models for interactive video in Enterprise networks
- Media resilience and rate adaptation also help preserve user experience when video traffic traverses the Internet or non-QoS-enabled networks

Provisioning and Resource Control Agenda

- **Enhanced Locations CAC Architecture**
  - **Network Modelling**
  - **Locations Bandwidth Manager (LBM)**
  - **Inter-Cluster E-LCAC with LBM**

What's New for Enhanced Locations CAC in 10.0

- Full support for Cross Cluster Extension Mobility
  - Nothing special to configure
  - Requires ELCAC, Inter-cluster ELCAC and Cross Cluster Extension Mobility to all be functioning individually.
- Video Promotion and Flexible DSCP
  - Supported on DX650
  - Planned support for 99xx/98xx video phones, CTS, TX and C series
- Support for Encrypted signalling between inter-cluster LBM Hubs (only related to inter-cluster ELCAC)


Control Plane
NO
YES
?
Call Admission Control
1
2
5
3
4
6
7
Call Signalling
Call Signalling
M
Media (DSCP)
Media (DSCP)
Scheduling + Queuing
IP WAN
Data Plane
E-LCAC
QoS

LCAC Limitations

Limited WAN Topology Support:

- Hub and Spoke WAN topology support
- Large gap between RSVP and Locations CAC

Multi Cluster Support:

- Multiple Clusters that managed endpoints in same branch sites could only inefficiently subdivide inter-branch bandwidth to avoid quality degradation (Ships in the night CAC)

TelePresence:

- Did not Support CAC (overlay design)
- TelePresence and UC or 3rd party video on a single cluster
- Limited CAC support for TelePresence video interoperability (P2P calls without an MCU)

E-LCAC Solutions

Network Modelling:

- Convert UCM locations to a model capable of supporting real network topologies

Inter-Cluster (Inter-cluster) CAC:

- Implement a bandwidth-accounting scheme that works between multiple Unified CM clusters and dynamically learns the topology from one another

Immersive Bandwidth Allocations:

- Implement an immersive BW pool in locations CAC
- Provide better CAC interop support between TelePresence Video and Desktop Video

Network Modelling




Enhanced Locations CAC Architecture

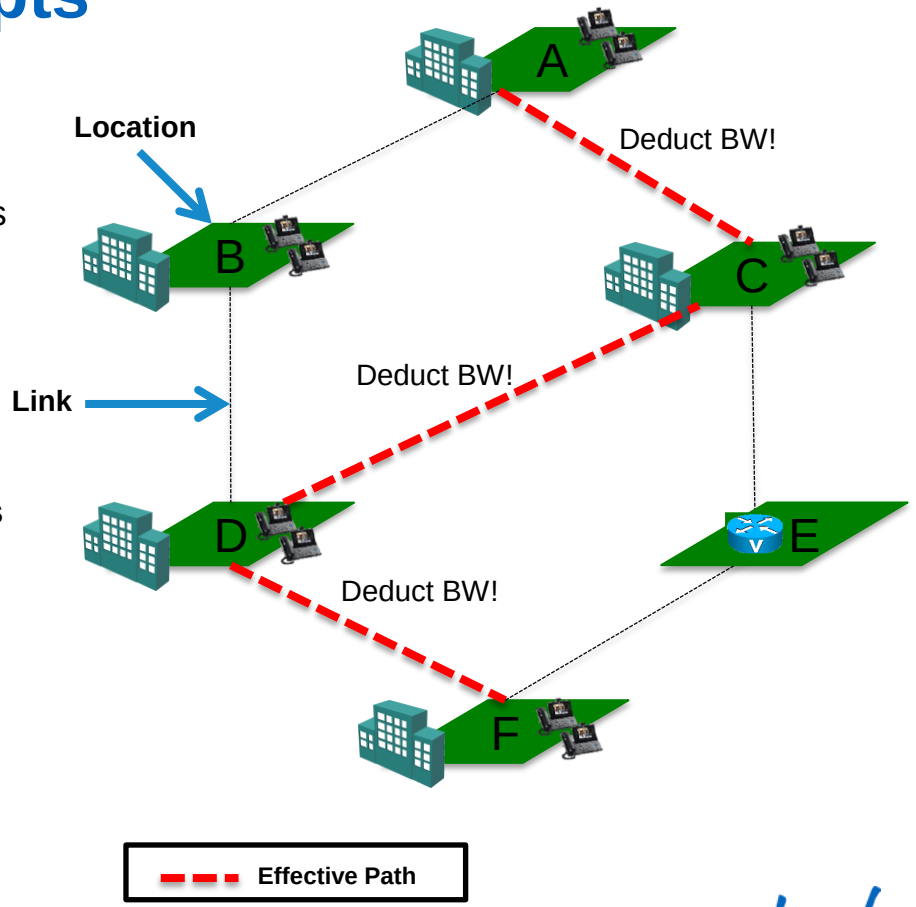
Network Modelling

Locations Bandwidth Manager (LBM)

Inter-Cluster E-LCAC with LBM

Network Modelling - Concepts

- Administrator builds a Network Model using locations and links
- A **Location** represents a LAN. It could contain endpoints or simply serve as a transit location between links for WAN network modelling
- **Links** interconnect locations and are used to define bandwidth available **between** locations. Links logically represent the WAN link
- **Weights** are used on links to provide a “cost” to the “effective path”. Weights are pertinent only when there is more than 1 path between any 2 locations
- UCM calculates shortest paths (least cost) from all locations to all locations and builds the effective paths
- The **Effective paths** are the paths with the “least cumulative weight”
- UCM tracks bandwidth across any link that the network model indicates from originating Location to terminating location.



Network Modelling – Locations and Links

Location A

BW	Allocated
Audio	Unlimited
Video	100MB
Immersive	250MB

WITHIN

IN/OUT

Locations Provide Bandwidth Accounting WITHIN the Location as well as IN or OUT of the Location

BETWEEN

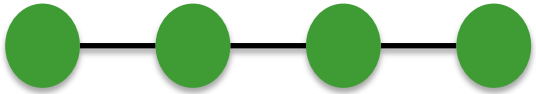
Link A < > B

BW	Allocated
Audio	1500k
Video	3000k
Immersive	5000k

Links Provide Bandwidth Accounting Between Locations

And Interconnect Locations

Linking Locations



Location B

BW	Allocated
Audio	Unlimited
Video	Unlimited
Immersive	Unlimited

TelePresence

IN/OUT

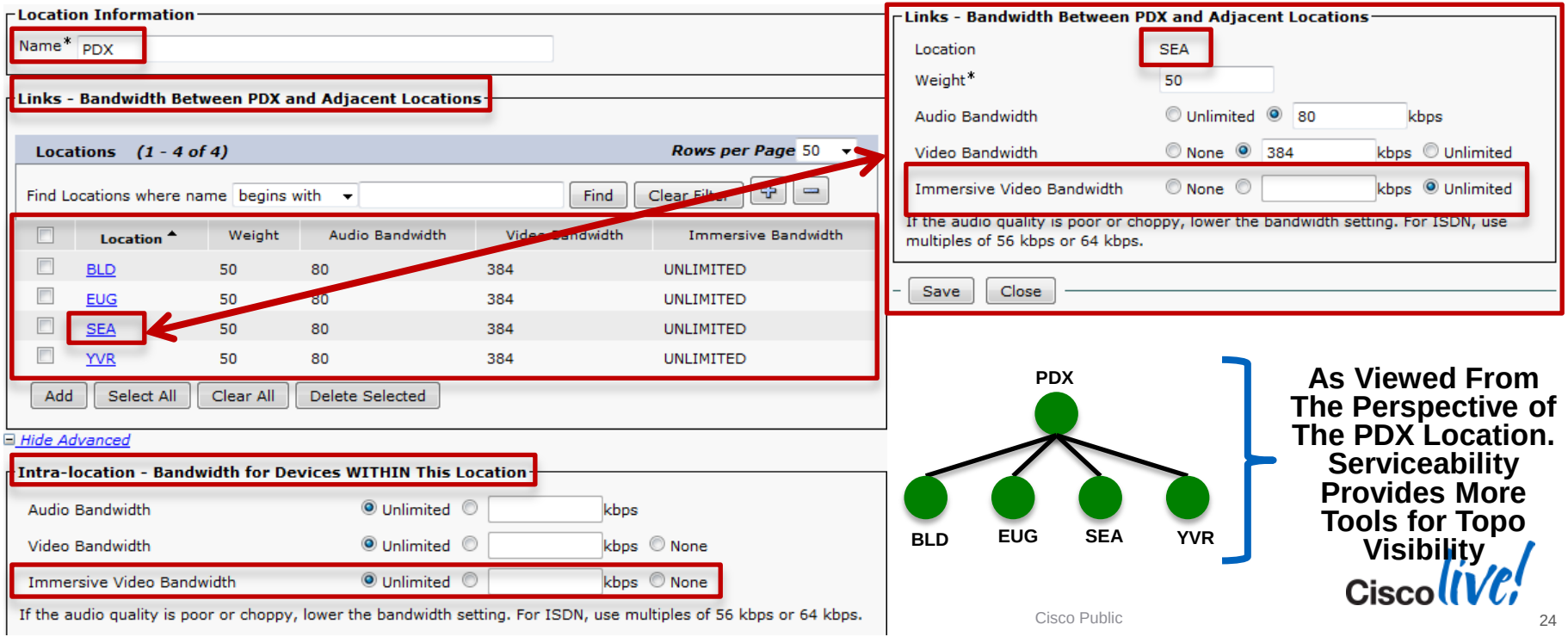
WITHIN

TelePresence and UC Video Endpoints Can Reside in the Same Location*

Network Modelling – Locations and Links

Intra-Location Bandwidth Allocation – TelePresence Immersive

- Links Interconnect Locations to Build the Topology. Bandwidth Values and Weight are Assigned to Links
- Intra-location Bandwidth Limits are Assigned to a Location to CAC ALL calls made **TO/FROM/WITHIN** the Location. Intra-location Bandwidth Values are Unlimited by Default.

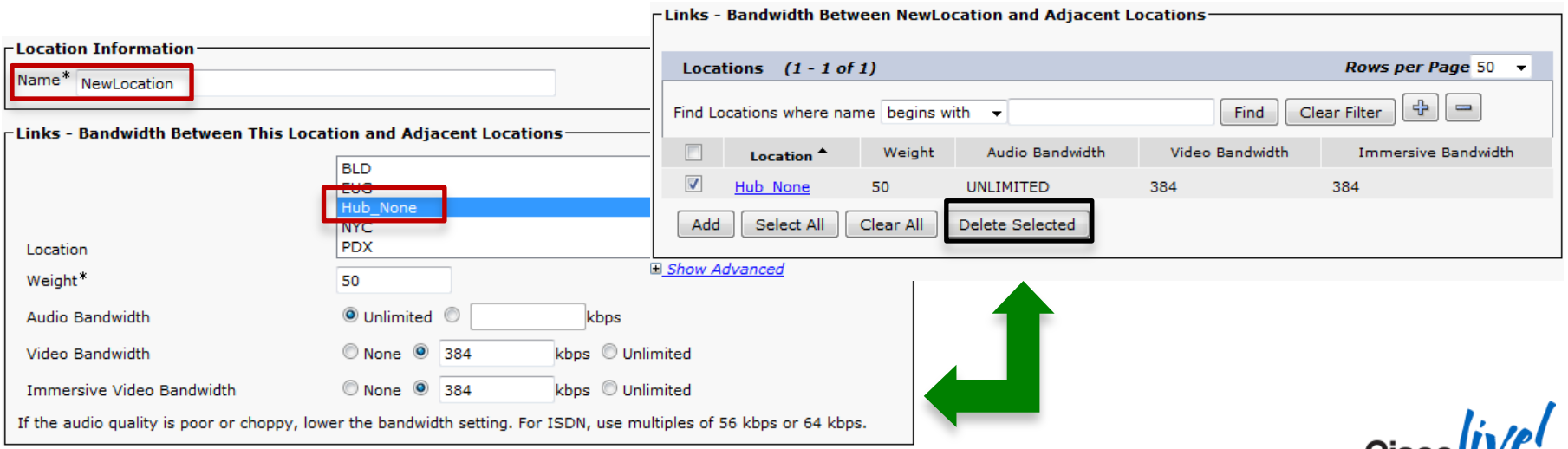


As Viewed From The Perspective of The PDX Location. Serviceability Provides More Tools for Topo Visibility

Network Modelling – Locations and Links

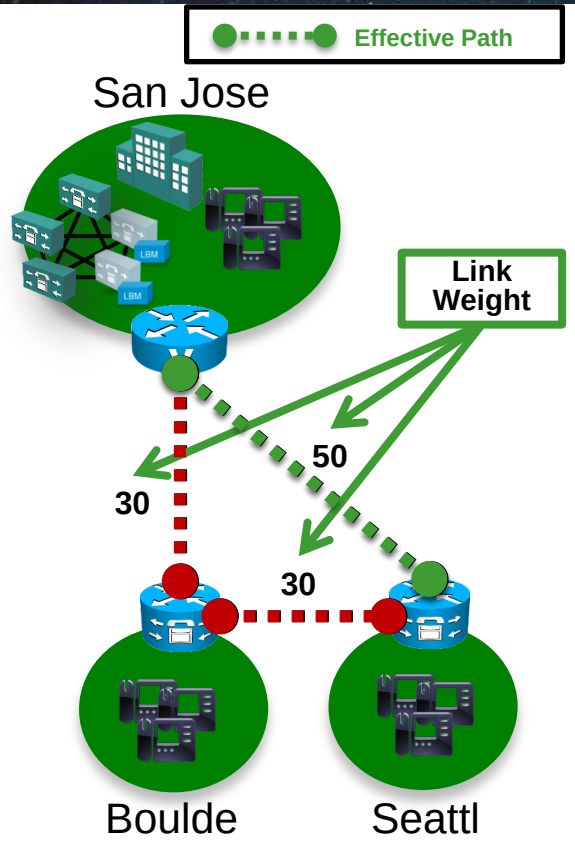
The Location Admin Page Has Been Updated To Configure Location Links

- By default when a new location is created a link to Hub. None will be added with unlimited audio bandwidth, 384 kb of both video and immersive bandwidth
- RECOMMENDATION: DELETE the link when it's not needed



Network Modelling in Locations CAC

Links, Weights and "Effective Path"



- Weight provides the ability to force a specific path choice when multiple paths between 2 locations are available
- When Multiple Paths are configured yet only 1 will be selected based on "Weight". This path is the "**Effective Path**"
- Weight is used to determine path cost, lowest weight path from source to destination is selected
- Weight is static and does not change with regards to the "effective path" from one location to another

EFFECTIVE PATH

Path 1:
San Jose > Seattle (Weight = 50 = 50)

Path 2:
San Jose > Boulder > Seattle (Weight = 30 + 30 = 60)

Network Modelling in Locations CAC
Links, Weights and "Effective Path"

- The Locations Bandwidth Manager (LBM) service computes the effective path from source location to destination location:
  - Sum weight of links across each possible path from source to destination
  - The least cost value of the path's weight determines the "Effective Path"
  - A tie break of equally weighted paths is determined by LBM based on location name
  - Once the effective path is determined, all subsequent calls that have the same source and destination locations will use the same "Effective Path"

Serviceability > Tools > Locations > Effective Path: Provides the Ability to Ascertain the "Effective Paths" Configured in the Topology

Detailed Path View

Location Name	Weight (1-100)	Audio Bandwidth (kbps)	Video Bandwidth (kbps)	Immersive Bandwidth (kbps)
PDX		Configured: Unlimited Available: Unlimited	Configured: Unlimited Available: Unlimited	Configured: **Unlimited** Available: **Unlimited**
▼	50	Configured: **160** Available: **160**	Configured: **2048** Available: **2048**	Configured: **Unlimited** Available: **Unlimited**
BLD		Configured: Unlimited Available: Unlimited	Configured: Unlimited Available: Unlimited	Configured: **Unlimited** Available: **Unlimited**
▼	50	Configured: **160** Available: **160**	Configured: **2048** Available: **2048**	Configured: **Unlimited** Available: **Unlimited**
NYC		Configured: Unlimited Available: Unlimited	Configured: Unlimited Available: Unlimited	Configured: **Unlimited** Available: **Unlimited**

Network Modelling
Key Takeaways

- Enhanced Locations CAC is a Static Model-Based CAC Mechanism
- E-LCAC is a Model of the “Routed Network” Attempting to Represent How The WAN Network Topology Routes Media
- Network Modelling is NOT Dynamic like RSVP
- The Model Needs to be Updated When the Network Topology Changes
- E-LAC is Call-Based (No Asymmetric or Unidirectional Bandwidth Deductions)
- Intra-location bandwidth assignment and deduction. The default is set to unlimited.

Locations Bandwidth Manager (LBM)



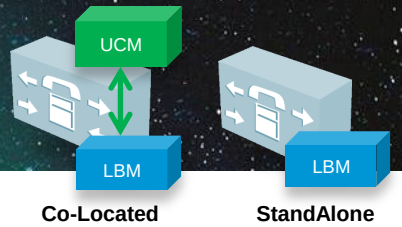

Enhanced Locations CAC Architecture

Network Modelling

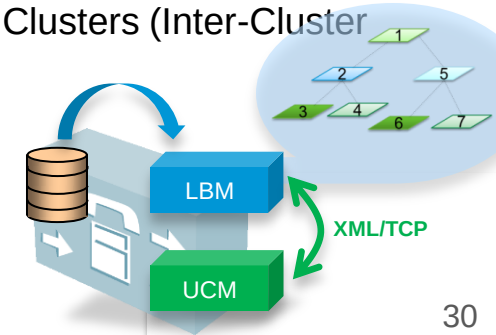
Locations Bandwidth Manager (LBM)

Inter-Cluster E-LCAC with LBM

Location Bandwidth Manager (LBM)
Service Overview

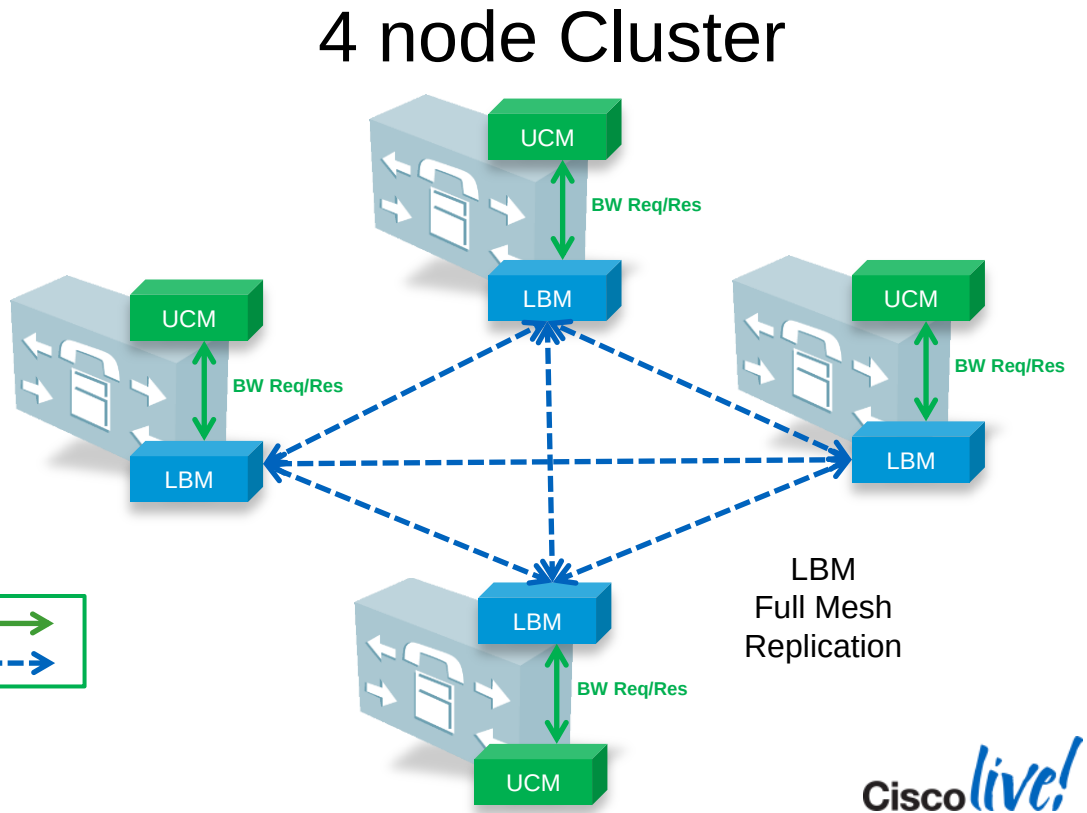


- LBM is a New Unified CM Feature Service
- LBM Service is Enabled by Default When Upgraded from a Pre-9.0 Installation
- For Fresh Installs The LBM Service Needs to be Manually Activated (like CCM service)
- LBM Can Run on Any UCM Subscriber or Standalone
- For E-LCAC to Function LBM Must Be Enabled
- Functions of LBM:
  - Location Path Assembly and Calculation
  - Servicing Bandwidth Requests from Unified CM Call Control (XML/TCP)
  - Replication of Bandwidth Information to Other LBMs Within and Between Clusters (Inter-Cluster Locations CAC)
  - Provides Configured and Dynamic information to Serviceability
  - Updates Location RTMT counters



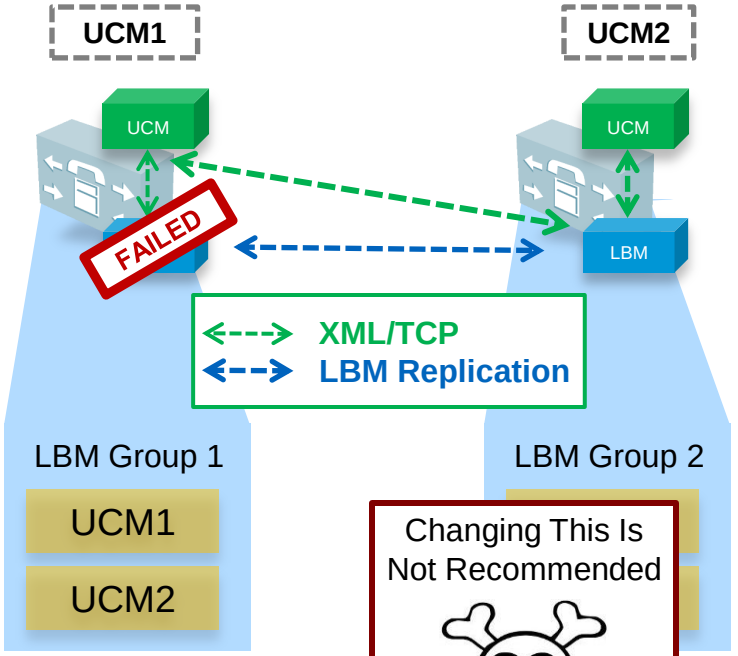
Location Bandwidth Manager Communication and LBM Replication

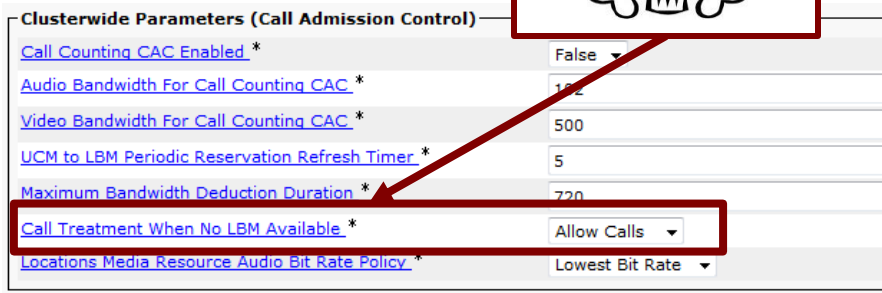
- LBM Services Within a Cluster Are Always Fully Meshed and Replicate Bandwidth Allocations
- The CallManager Service Communicates with The LOCAL LBM Service (Default)
- Recommendation:
  - Run LBM on same node as Cisco CallManager Service



LBM Redundancy
Service and Recommendations

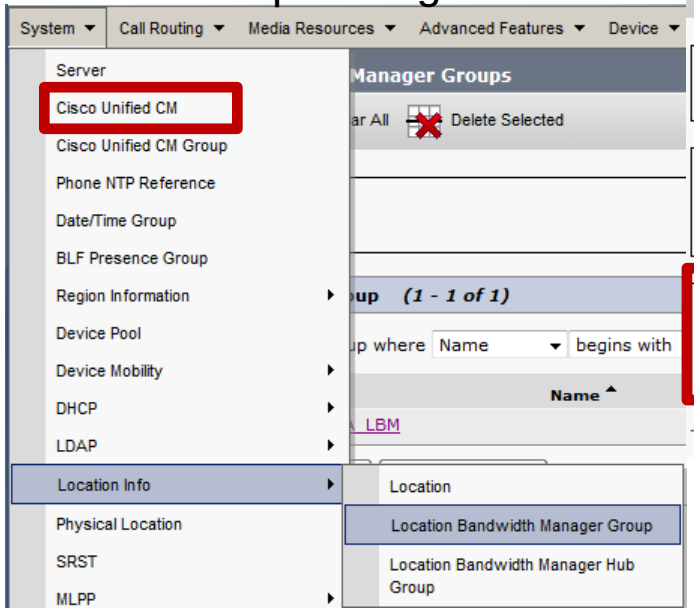
- LBM Group allows control of Active and Standby LBMs
- Provides redundancy of LBM for the UCM service during an LBM “service outage”
- **Unified CM LBM Usage Order:**
  1. LBM Group Designation (1, 2)
  2. Local LBM
  3. Service Param: “Call Treatment when no LBM available” (allow calls = Default)
- **LBM Recommendations:**
  - Run LBM on same node as Cisco CallManager Service
  - LBM Group: Co-located LBM first, LBM from local subscriber second, otherwise no redundancy.

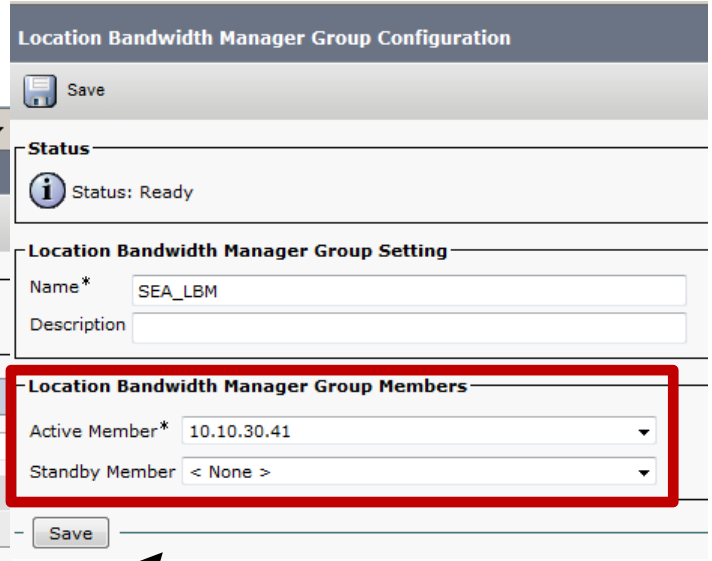


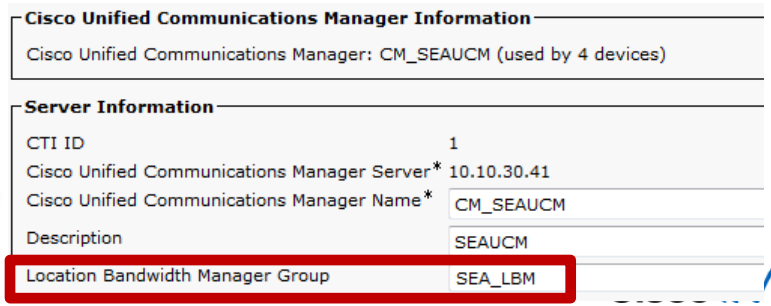


Location Bandwidth Manager (LBM)
LBM Group Configuration

LBM Group Config

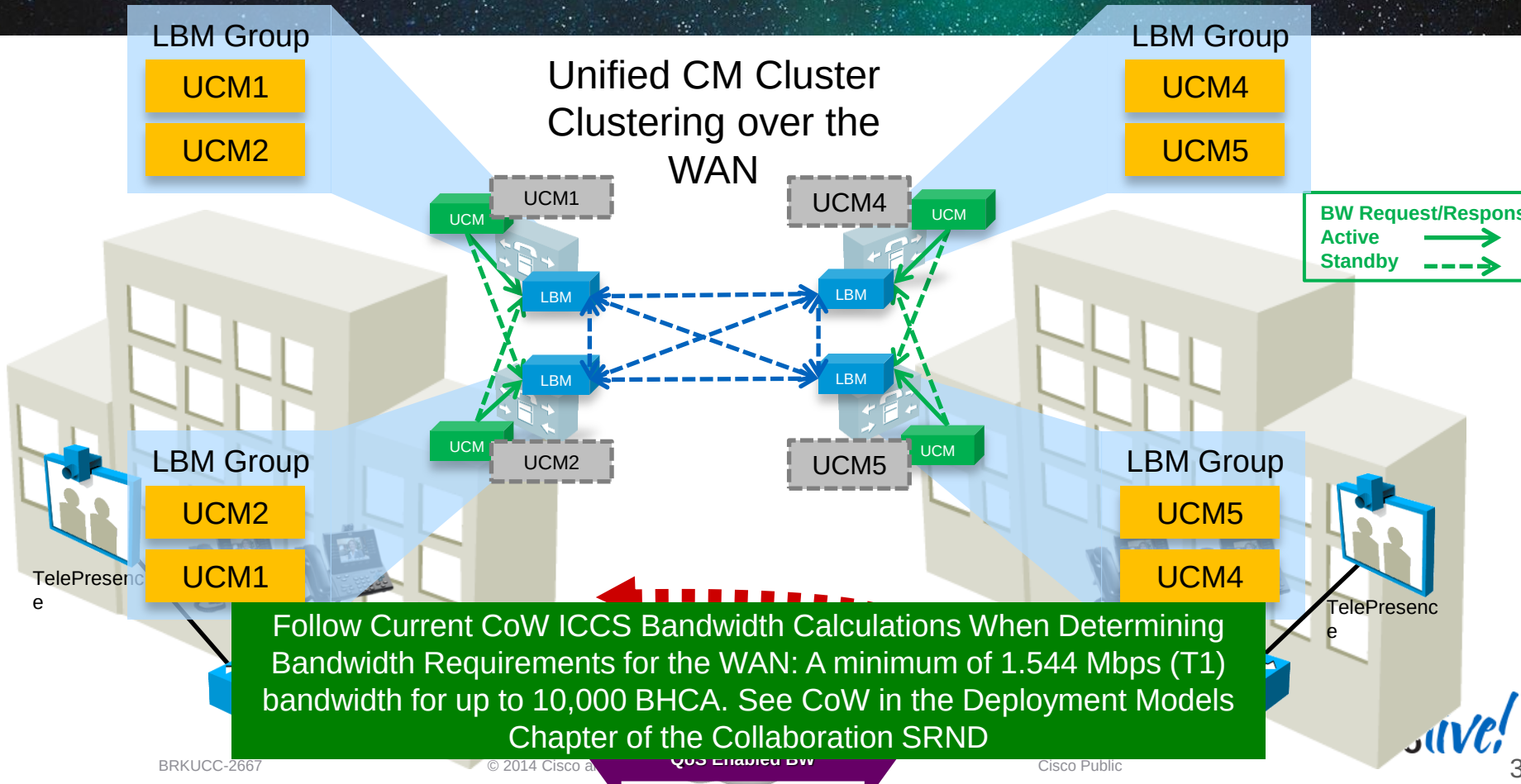






An LBM group association determines which LBMs a UCM service communicates with. In absence of an LBM group UCM communicates with the local LBM ONLY.

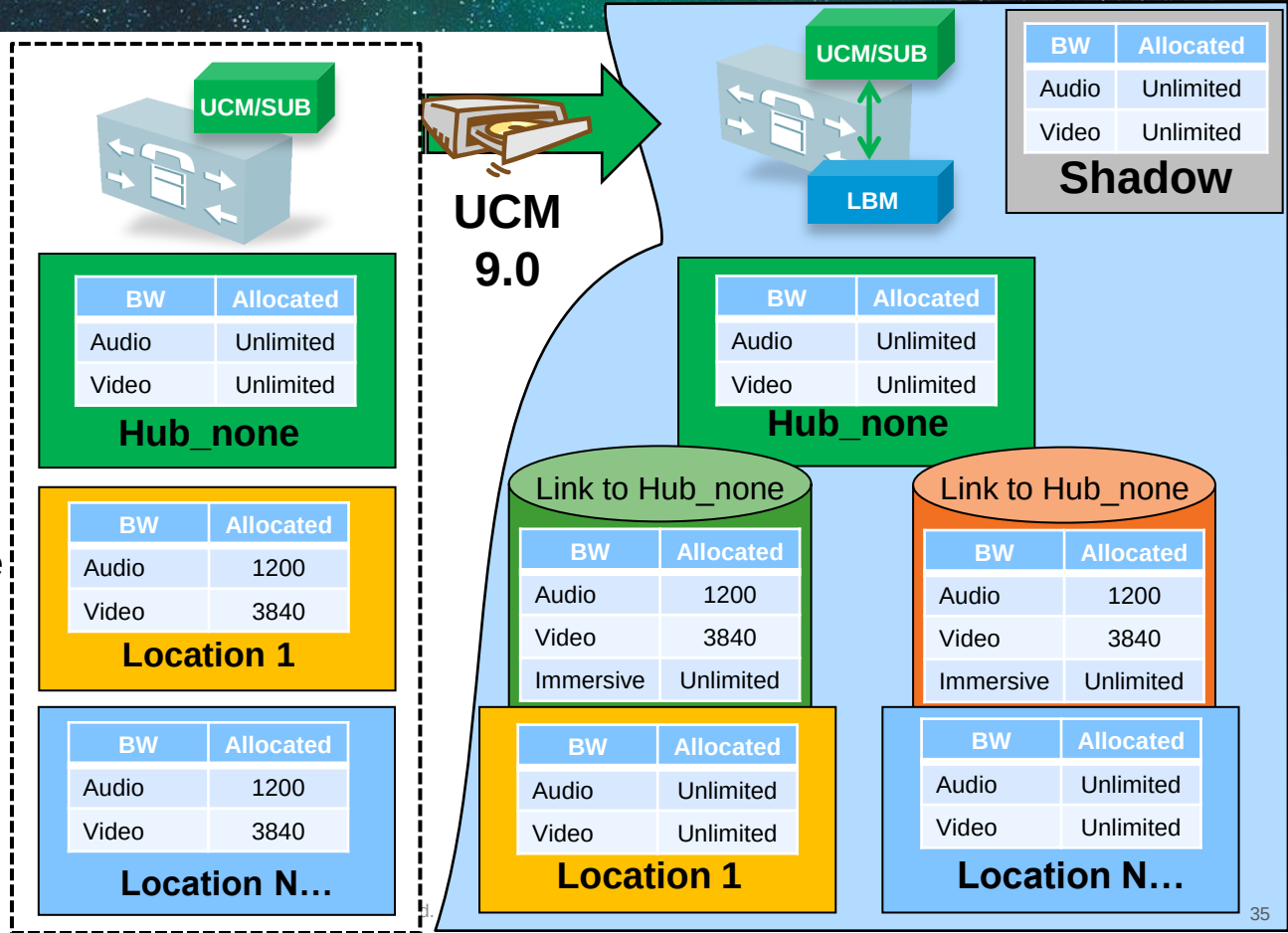
Clustering over the WAN (CoW) - LBM



Migration to Enhanced Locations CAC

Settings After An Upgrade To 9.0

- LBM is activated on each UCM subscriber
- No LBM groups or LBM hub groups
- UCM service communicates with local (on node) LBM
- Fully meshed LBM services
- No inter-cluster E-LCAC
- Intra-location bandwidth values are set to unlimited
- Location bandwidth values are migrated to a link inter-connecting the migrated location and Hub_None
- Phantom and Shadow locations have no links



Sizing and Performance

- 2000 Max Locally Configured Locations
- 8000 Max Total Replicated Locations (Globally distinct locations)
- Sizing with LBM Co-located (Cisco Sizing Tool Will Assume LBM Impact)

Key Takeaways
Summary

- LBM is a New Feature Service
- LBM is Fully Meshed Within The Cluster
- LBM is Responsible For Modeled Topology and Servicing UCM Requests
- Recommendations for LBM Group Usage
  - Run LBM on Each Unified CM Subscriber
  - Use LBM Group to create a backup LBM for the CallManager service

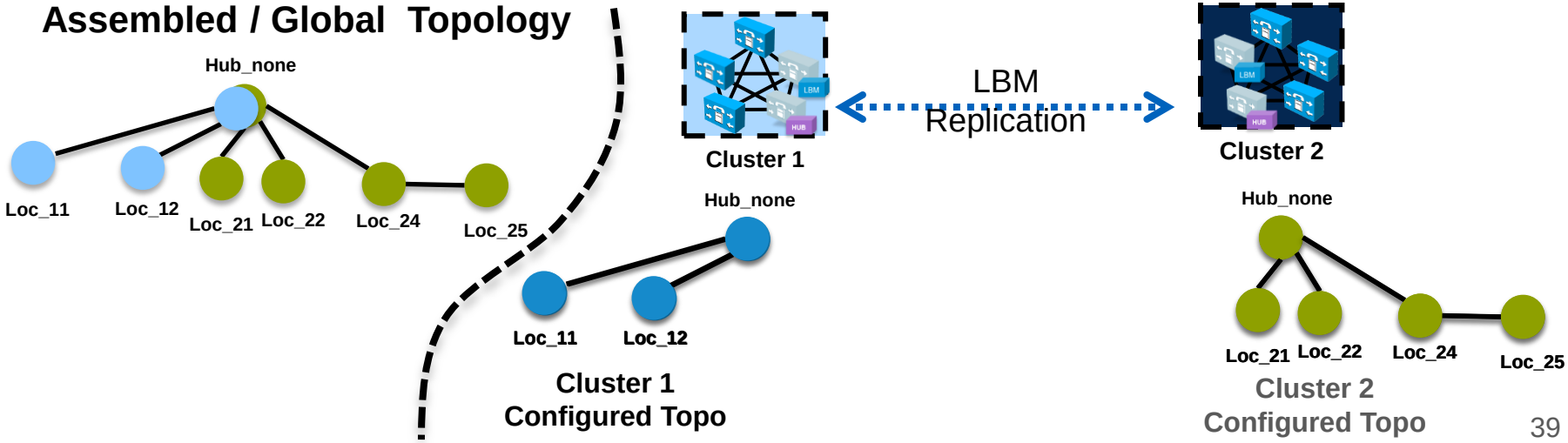
Inter-Cluster E-LCAC with LBM




Enhanced Locations CAC Architecture
- Network Modelling
- Locations Bandwidth Manager (LBM)
- **Inter-Cluster E-LCAC with LBM**

Inter-Cluster Enhanced Locations CAC

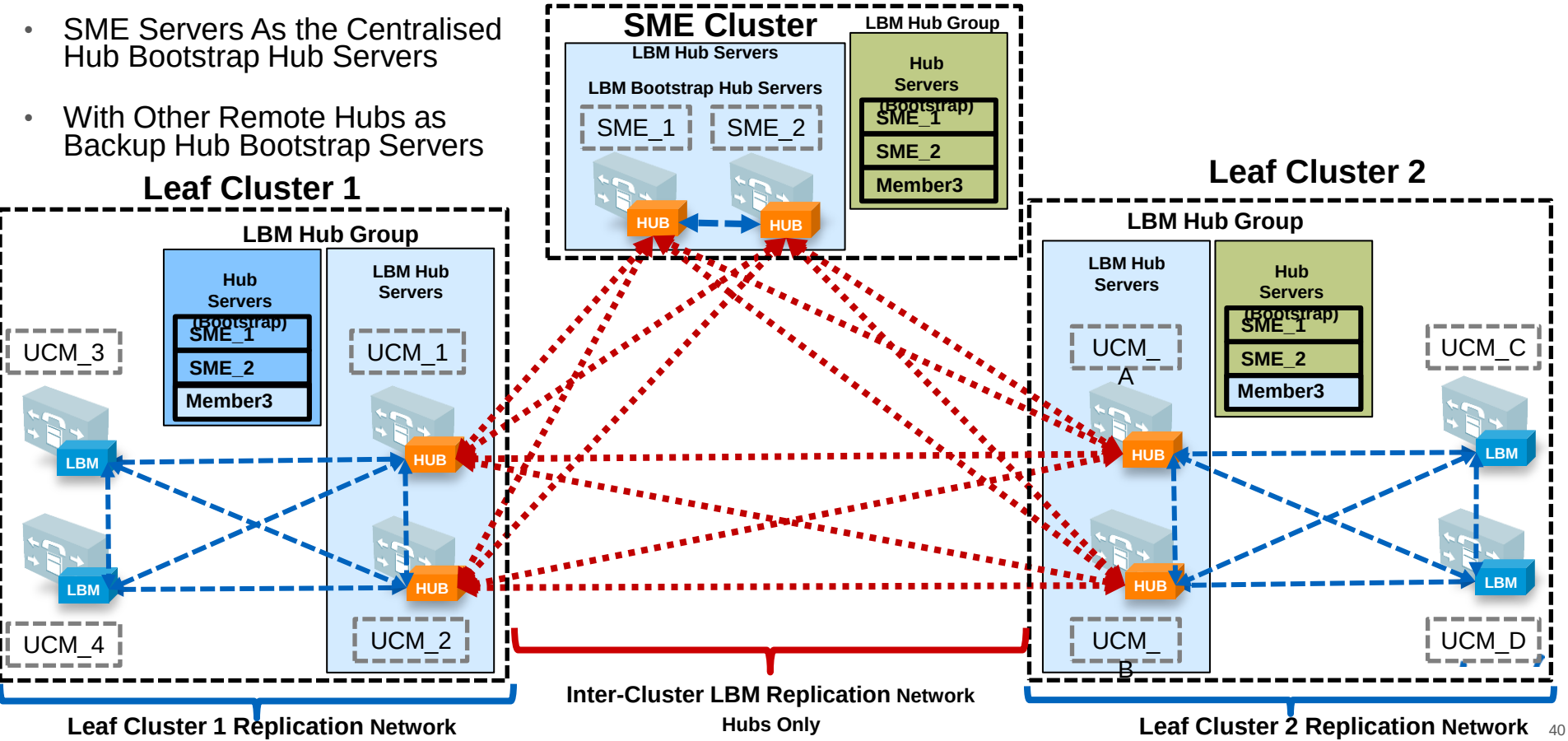
- Extends Enhanced Locations CAC Network Modelling Across Multiple Clusters
- Each Cluster Manages Its Own Topology
- Each Cluster Then Propagates Its Topology to Other Clusters Configured In the LBM Inter-Cluster Replication Network
- Each Cluster Then Creates a Global Topology (“Assembled Topology”) Piecing Together Each Clusters Replicated Topology



LBM Network – Hubs, Spokes and Hub Bootstrap

Centralised Hub Bootstrap server for the LBM replication network

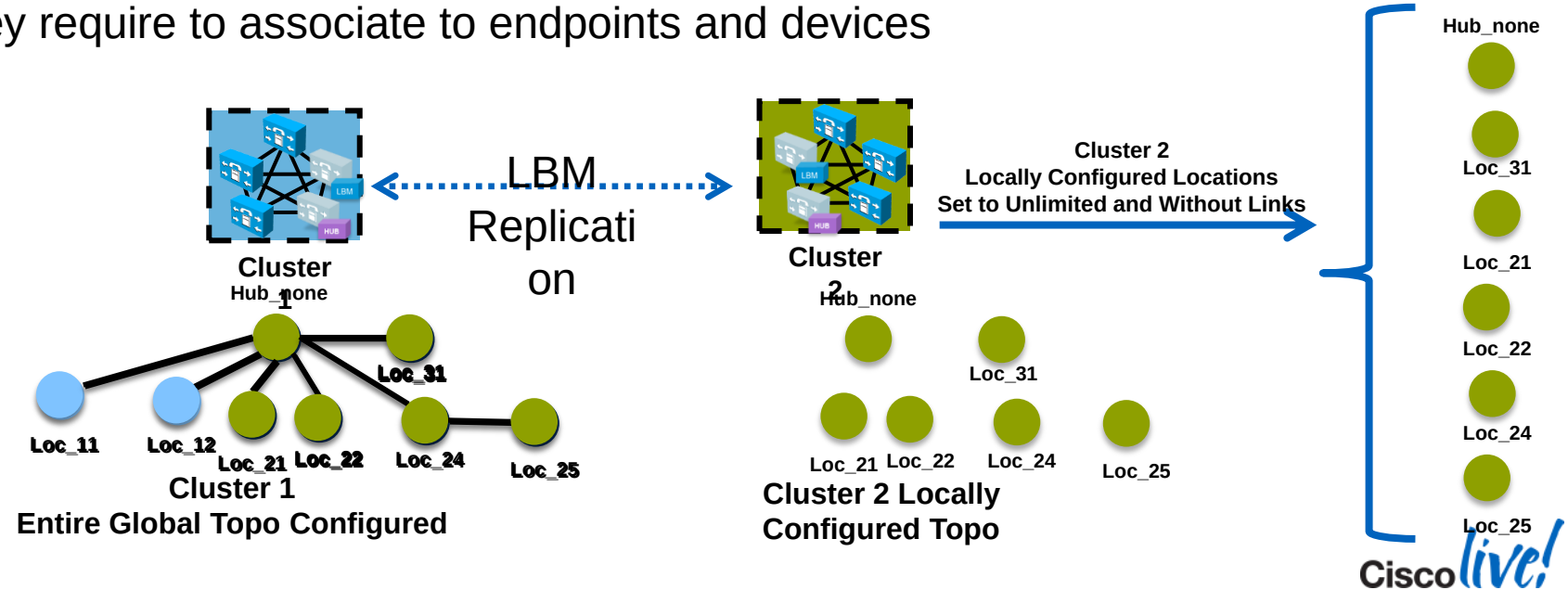
- SME Servers As the Centralised Hub Bootstrap Hub Servers
- With Other Remote Hubs as Backup Hub Bootstrap Servers



Inter-Cluster Enhanced Locations CAC

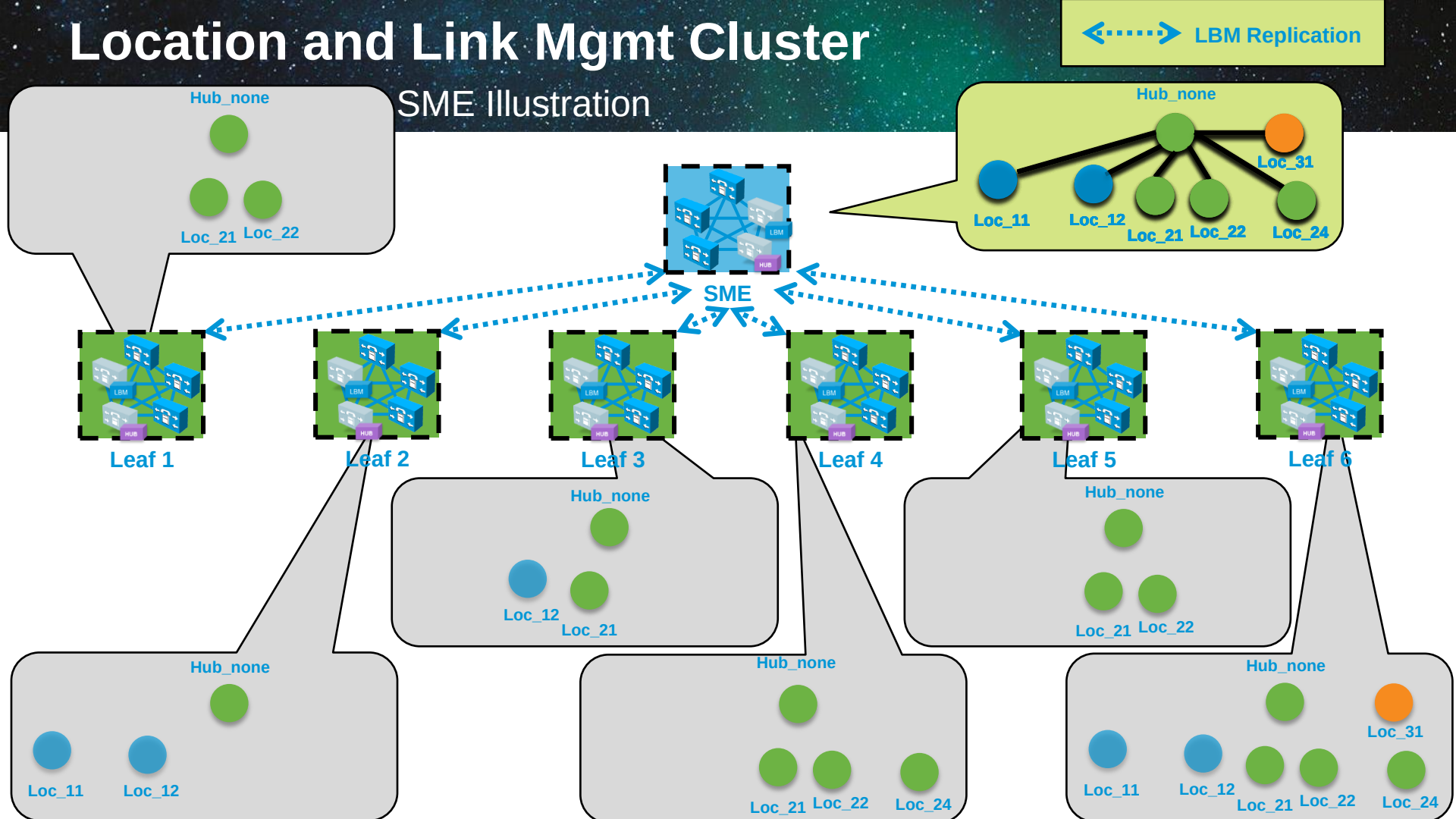
Locations and Links Management Cluster

- Single Cluster manages ALL Locations and Links for the entire Locations Replication Network
- All Other Clusters (e.g. Leaf Clusters) need only configure the Locations that they require to associate to endpoints and devices



Location and Link Mgmt Cluster

SME Illustration



Inter-cluster Enhanced Locations CAC
For Further Information

See the addendum for more information on the following:

- Inter-cluster CAC Operation and Configuration
- Inter-cluster CAC design: Location and Link Management Cluster
- TelePresence and UC Video Differentiation in Admission Control

For a complete overview of E-LCAC see Orlando Presentation and VoD
www.ciscolive365.com > BRKUCC-2343
https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=7978&backBtn=true

Audio and Video Admission Control
Considerations

No Admission Control

- Over-provision queues
- Rely on video rate adaptation and media resilience capabilities
- Audio is much easier to over-provision in pervasive video deployments
- QoS critical and rate adaption is highly beneficial for both managed/unmanaged networks
- Benefits: Simplicity

Admission Control

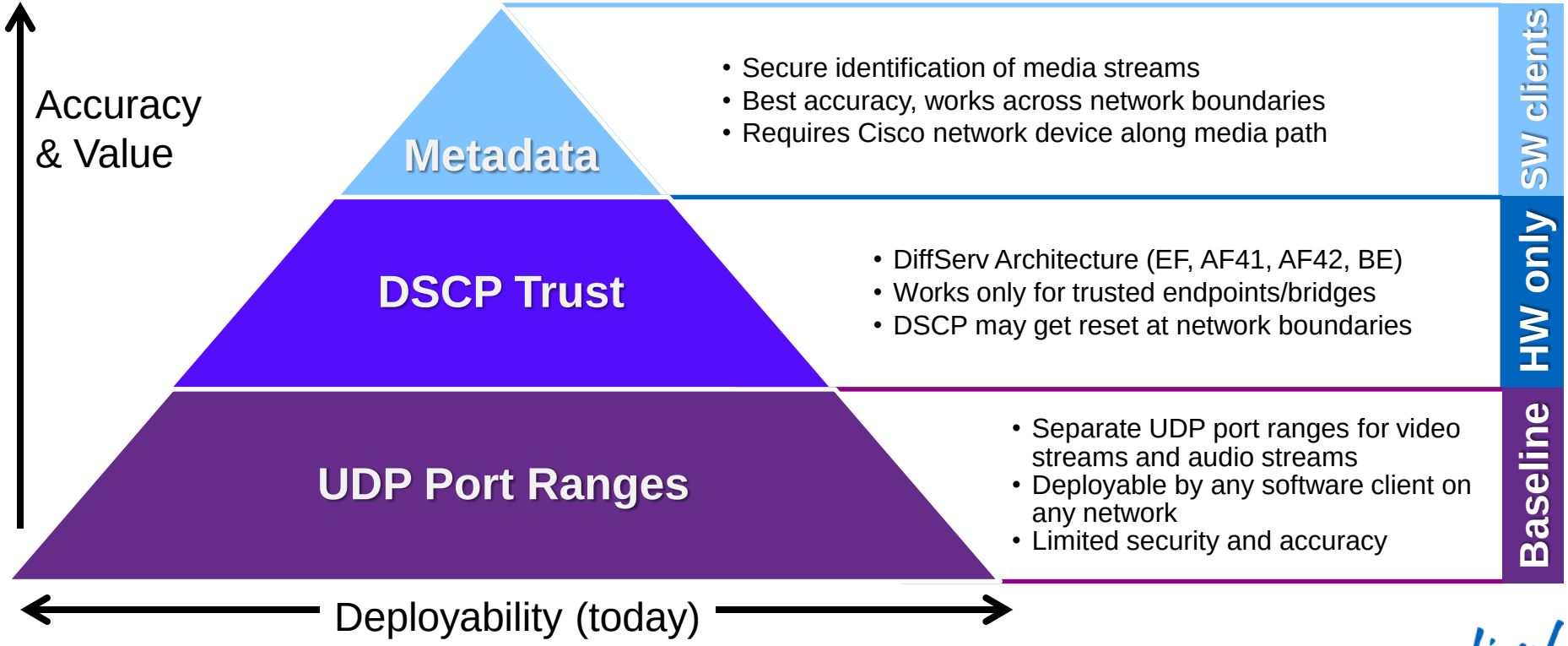
- Strict provisioning (Mapping CAC to Queuing)
- Mobility? Device Mobility feature (Add OPEX)
- Jabber? Medianet Metadata is recommended to align QoS / CAC
- Benefits:
  - Manage lower bandwidth links, use AAR for PSTN redirect
  - Ensure quality audio during the busy hour by avoiding oversubscription and packet loss
  - Safe when over-provisioning is not an option




QoS Architecture:

APPROACH OVERVIEW
IDENTIFICATION & CLASSIFICATION
QUEUING & SCHEDULING

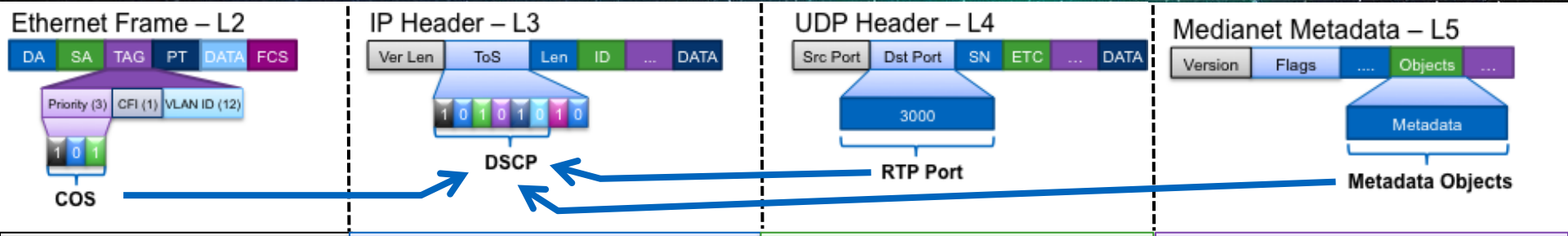
QoS Strategy
Collaboration Traffic Identification



QoS Recommendations (RFC 4594-Based)

Application Class	Per-Hop Behaviour	DSCP	Queuing & Dropping	Application Examples
VoIP Telephony	EF	46	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	40	BW Queue	Cisco IP Video Surveillance / Cisco Enterprise TV
Realtime Interactive	CS4	32	BW Queue + DSCP WRED	Cisco TelePresence
Multimedia Conferencing	AF4	34/36/38	BW Queue + DSCP WRED	Cisco Unified Personal Communicator, WebEx
Multimedia Streaming	AF3	26/28/30	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6	48	BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signalling	CS3	24	BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2	16	BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2	18/20/22	BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
Bulk Data	AF1	10/12/14	BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF	0	Default Queue + RED	Default Class
Scavenger	CS1	8	Min BW Queue (Deferential)	YouTube, iTunes, BitTorent, Xbox Live

Trust and Enforcement:
QoS Marking in the LAN and WAN



- Values 0-7
- Limited values to differentiate multiple traffic beyond 7 classes
- Goal: Use when needed in L2 environments to map to DSCP. Use DSCP when possible.

- 0-64: EF, CS5, CS4, AF4, AF3, CS6, CS3, CS2, AF2, AF1, DF, CS1, ...
- Many more values to differentiate traffic
- Goal: Get all traffic to a DSCP value

- Protocol Destination Port range.
- Difficult to differentiate Audio and Video
- Goal: Use to apply DSCP to traffic when no COS or DSCP is available.

- Large quantity of matching criteria to differentiate traffic based on signalling, media type, device models, etc....
- Requires network support
- Goal: Use to apply DSCP to traffic when no COS or DSCP is available.




QoS Architecture:

APPROACH OVERVIEW
IDENTIFICATION & CLASSIFICATION
QUEUING & SCHEDULING

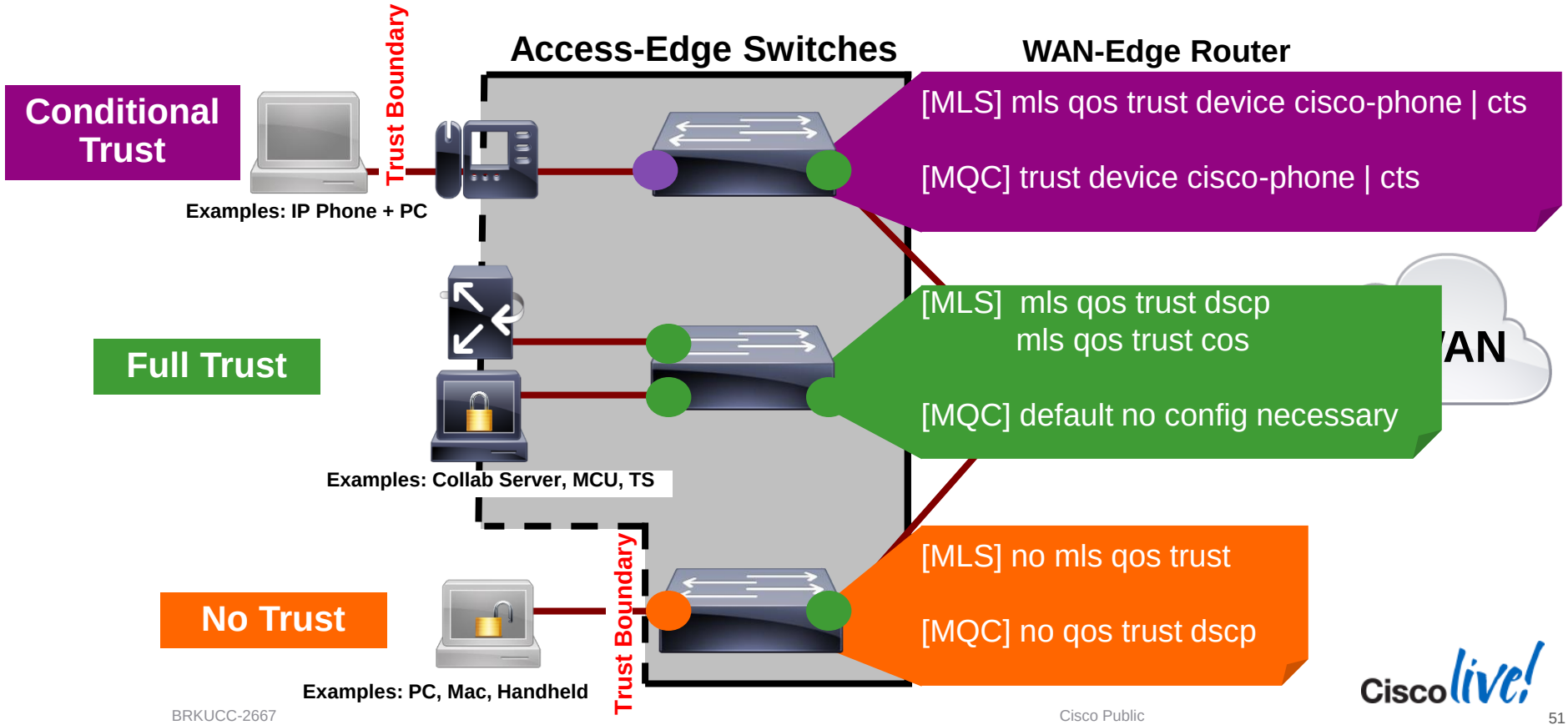
Identification and Classification Agenda

- **Trusted Devices**
- Untrusted Devices:
  - Mapping UDP/TCP Port Ranges
  - Medianet Metadata

Campus QoS Design Considerations

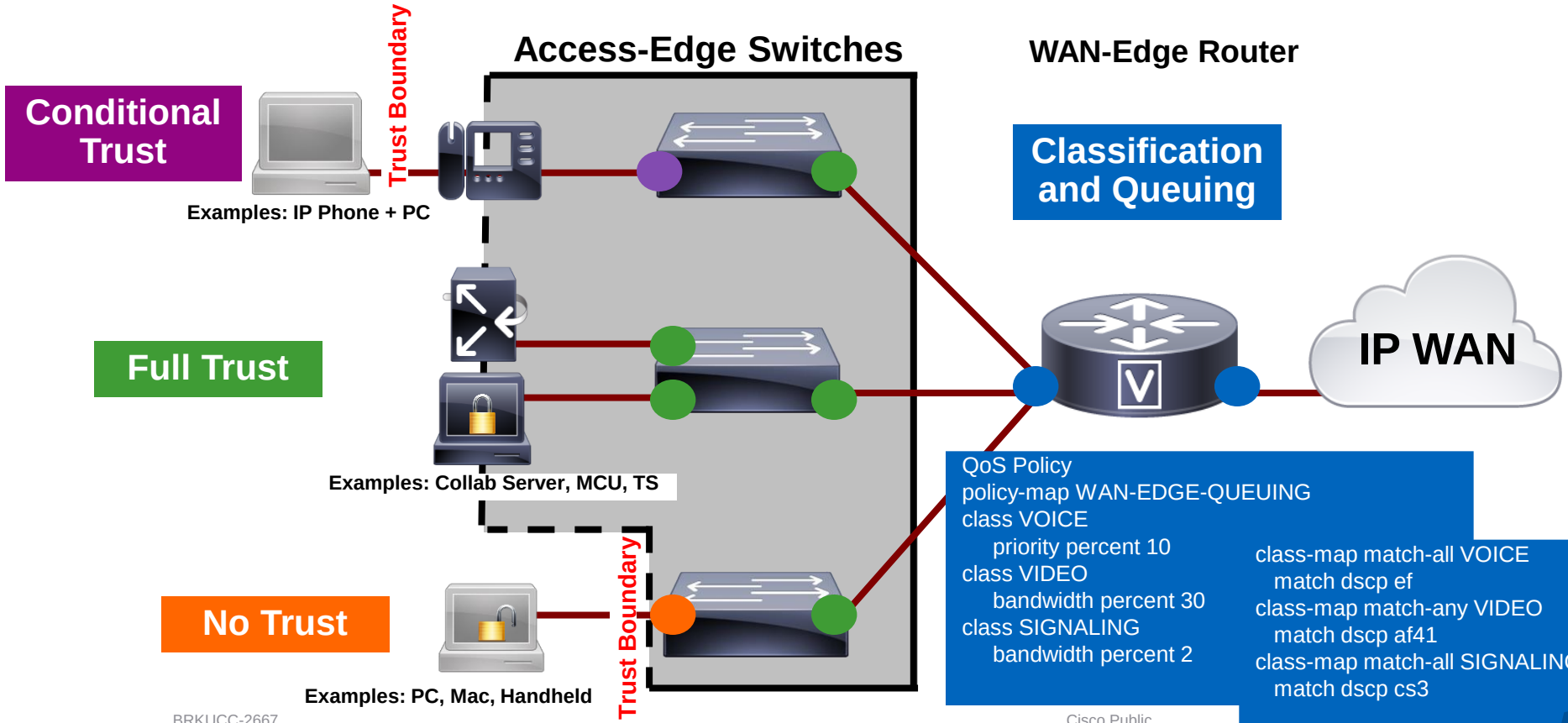
Trust Boundaries

BRKCRS-2501 Campus QoS Design Simplified

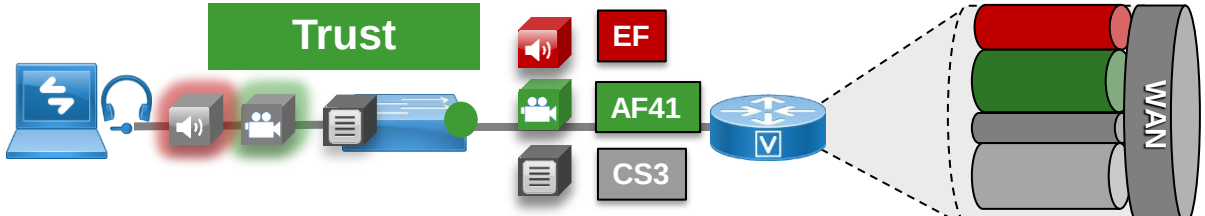


Campus QoS Design Considerations

Trust Boundaries



Egress Classification and Queuing



1

```
! This section applies the policy-map to the Interface
Router (config-if)# service-policy output EGRESS-QUEUING
 ! Attaches service policy to interface
```

```
! This section configures the bandwidth for all collab traffic
policy-map EGRESS-QUEUING
class VOICE
    priority percent 10
! Provisions 10% LLQ to VOICE class
 class VIDEO
    bandwidth percent 30
 ! Provisions 30% CBWFQ to VIDEO class
 class SIGNALING
    bandwidth percent 2
! Provisions 2% CBWFQ to SIGNALING class
...
```

2

```
! This section applies the policy-map
class-map match-all VOICE
match dscp ef
class-map match-any VIDEO
match dscp af41
match dscp af42
class-map match-all SIGNALING
 match dscp cs3
```

3

Trust and Enforcement:
Devices and Places in the Network

Conditionally-Trusted Endpoints

Immersive Endpoints

CDP Support required

IP Phones, TE, TC, TX, CTS

Mac/PC

Trusted Endpoints / Devices

PC/GPO

MAC

Handheld

WiFi AP

Untrusted Endpoints / Devices

PC

MAC

Handheld

Access

Distribution

Core

WAN Edge

IOS GW

CME

CUBE

WiFi Controller

Trusted Devices

UCM

UCx

IM&P

VCS / Expressway

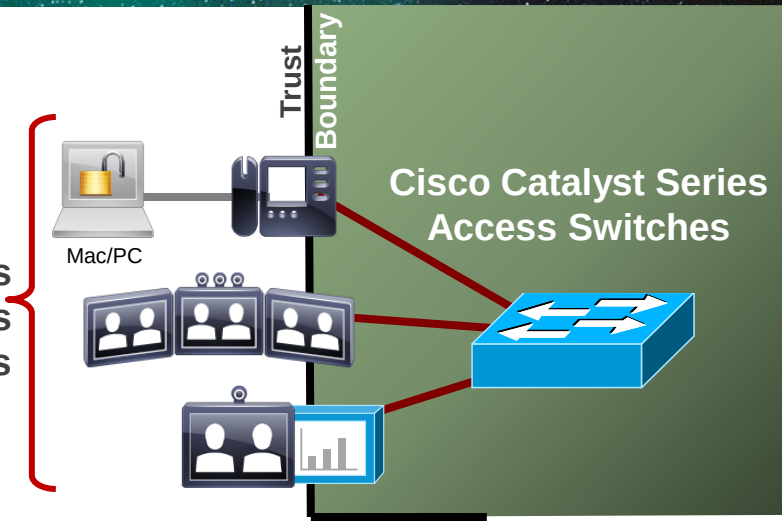
MCU/TS

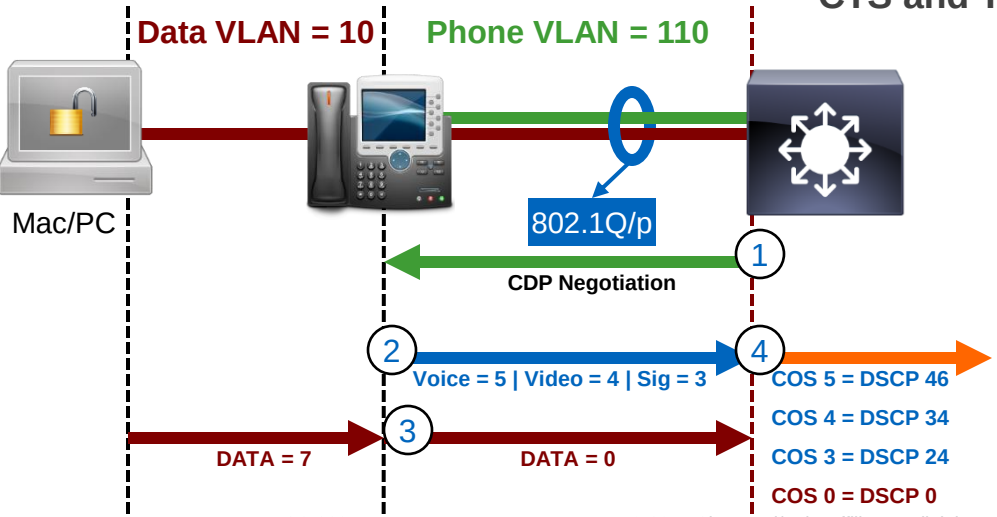
Quality of Service

CDP to Establish QoS Trust Boundary – "Conditional Trust"

1. CDP exchange, trust boundary extended to endpoint
2. Phone sets COS (audio 5, video 4, signalling 3)
3. Phone re-writes COS of Computer port traffic to 0
4. Switch trusts COS from endpoint and maps COS → DSCP

CDP:
Cisco IP Phones
TE and TC Series
CTS and TX Series





Commands:

[MLS] mls qos trust device cisco-phone | cts

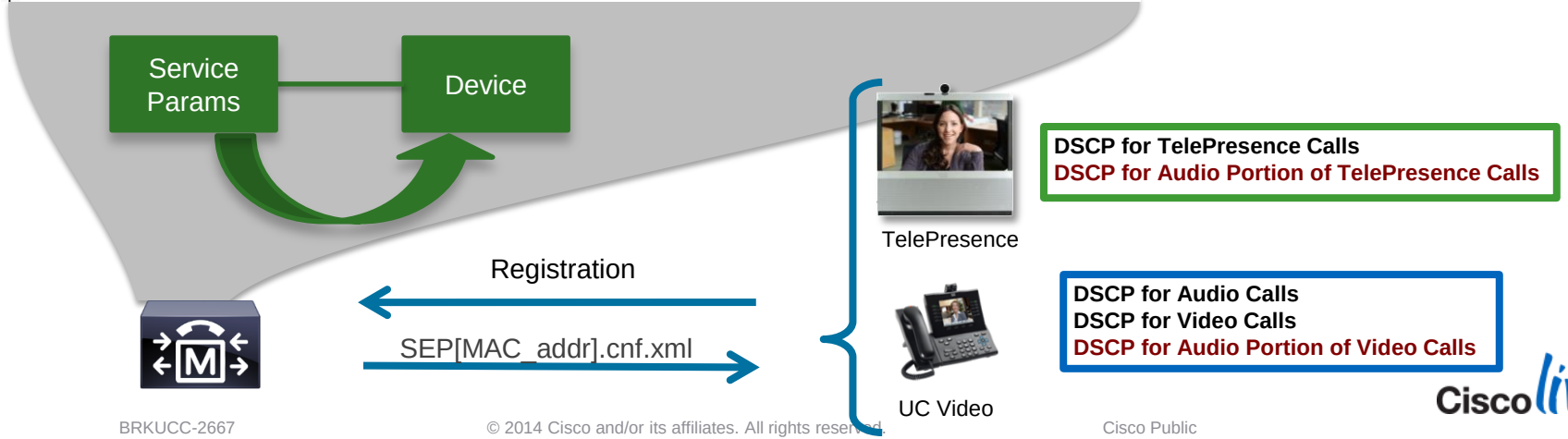
[MQC] trust device cisco-phone | cts

Quality of Service
DiffServ Configuration on Cisco Endpoints

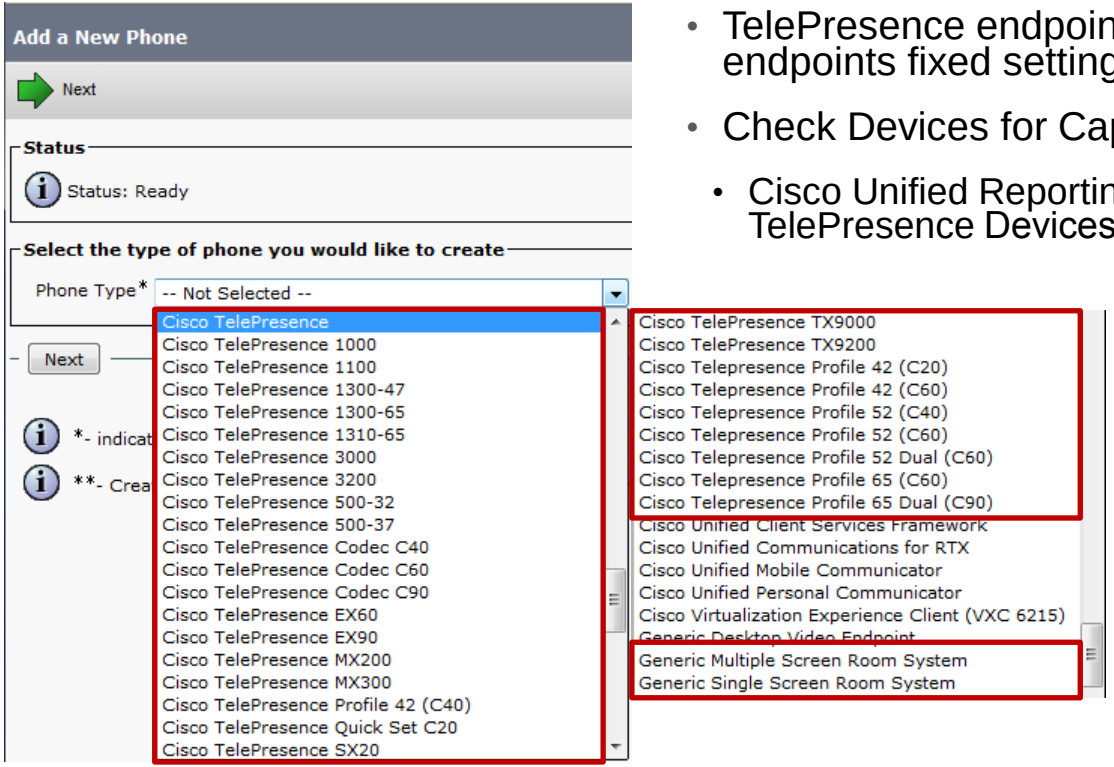
UCM Provides DSCP values via the service parameters to endpoints for media marking:

Clusterwide Parameters (System - QOS)

Priority Class *	Normal Priority	Normal Priority
DSCP for Audio Calls *	46 (101110)	46 (101110)
DSCP for Video Calls *	34 (100010)	34 (100010)
DSCP for Audio Portion of Video Calls *	34 (100010)	34 (100010)
DSCP for TelePresence Calls *	32 (100000)	32 (100000)
DSCP for Audio Portion of TelePresence Calls *	32 (100000)	32 (100000)



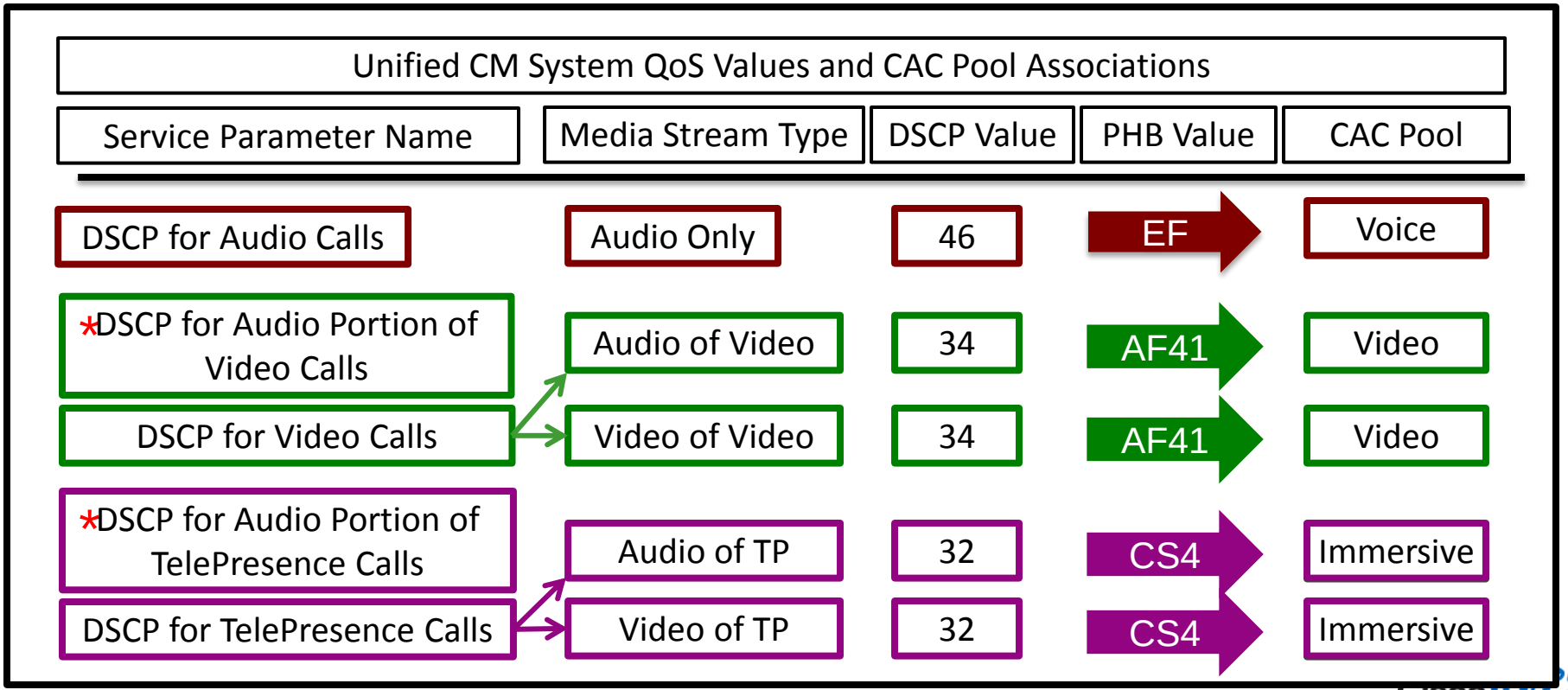
TelePresence Endpoints in Unified CM



- TelePresence endpoints are identified as immersive video endpoints fixed setting (Not Configurable)
- Check Devices for Capability:
  - Cisco Unified Reporting Tool > “Immersive Video Support for TelePresence Devices”

Unified CM QoS Classification

* New in 10.0



Trusted Devices
Summary

What we've covered:

- **Conditional trust:** Endpoints using CDP
- **Full trust:** Collab Servers, MCUs, Fully Trusted Desktop/Devices
- **Untrusted**: Desktops, Laptops, Mobile Handhelds

What's next

- **Untrusted**: Jabber Devices – Traffic identification and remarking

See Addendum for Server QoS Configurations

For more information online:

Search in www.cisco.com > Medianet Campus QoS Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html

Search in www.cisco.com > Medianet WAN Aggregation QoS Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSWAN_40.html

Breakout Sessions for more information:

BRKCRT-2501 Campus QoS Design—Simplified: Friday, Jan 31, 9:00 AM - 11:00 AM

Identification and Classification Agenda

- Trusted Devices
- **Untrusted Devices:**
  - **Mapping UDP/TCP Port Ranges**
  - Medianet Metadata

Mapping Identifiable Media and Signalling Streams

1. Identifying media and signalling streams from the client based on Layer 4 (Transport) port ranges (Protocol TCP/UDP and Ports).
   - The protocol port ranges are configured in Unified CM and are passed to the endpoint during device registration. The endpoint then uses these port ranges for signalling and media negotiation.
2. Classify the signalling and media streams and remark with a corresponding DSCP
   - Network Access Control Lists (ACL): Method consists of configuring ACLs to classify and mark DSCP based on protocol and port ranges
   - Windows Global Policy Objects (GPO): Method consists of configuring GPO's to classify and mark DSCP based on protocol, port ranges and application and relies on DSCP trust to pass through the network

Mobile Portfolio: Jabber Clients





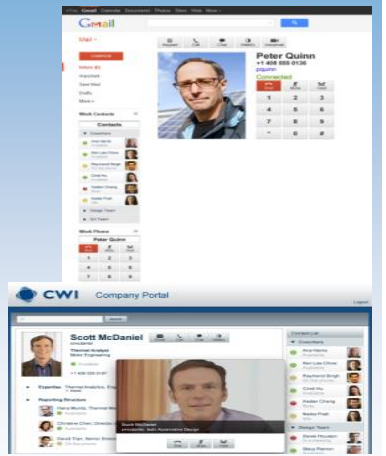


Win, Mac

Tablet

Smartphone

Web SDK

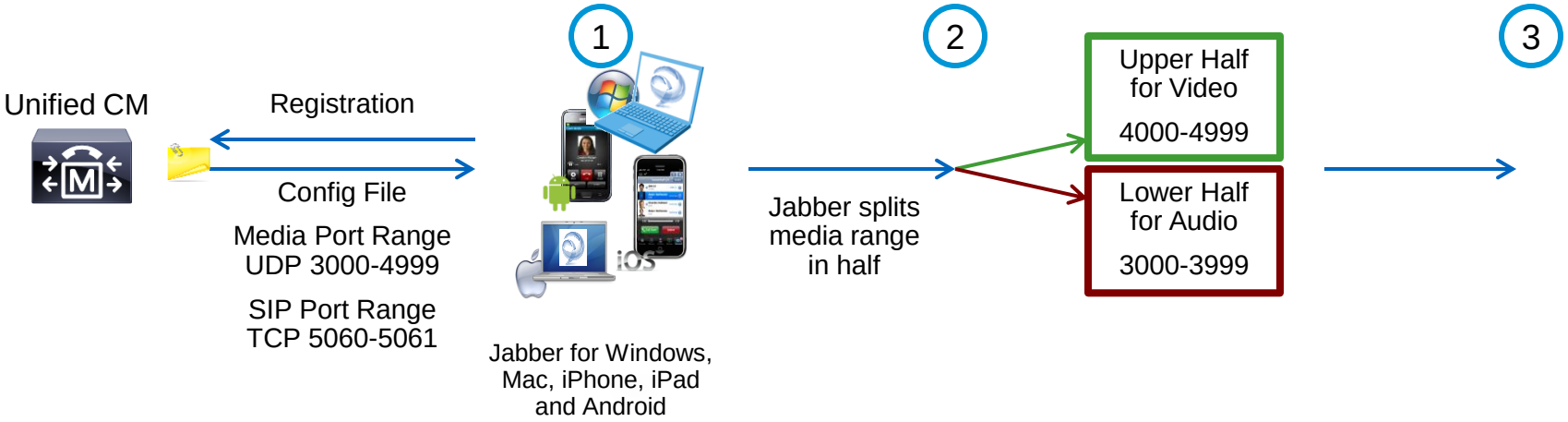


QoS Classification and Marking in Jabber Products

- **Classification in Windows 7 and 8**
  - Global Policy Objects (GPOs) which specifies Protocol, Port and Application as means of identification of traffic by which to mark QoS
- **Classification in Windows 2000 and XP**
  - Windows 2000 and XP have a different model for allowing the application to mark QoS, which is called Generic Quality of Service (GQoS). Jabber for Windows has implemented GQoS allowing the application to inform the OS to mark the desired DSCP. Turning this function on in Windows 2000 and XP is explained in the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/248611
- **Classification in Mac OSX**
  - Natively marks DSCP
- **Classification in iOS (iPhone and iPad)**
  - Natively marks DSCP
- **Classification in Android**
  - Natively marks DSCP

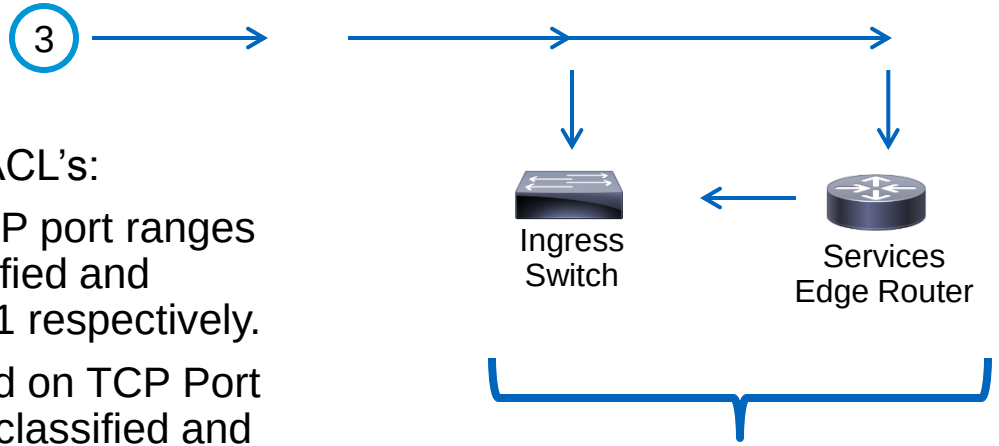
Latest Jabber Releases

Jabber's Use of UDP Port Ranges



1. Client registration, download configuration file
2. Split media port range in half, upper half for video and lower half for audio

Jabber's Use of UDP Port Ranges



3. Configure Network with ACL's:

   Media is identified on UDP port ranges 3xxx and 4xxx and classified and remarked to EF and AF41 respectively.

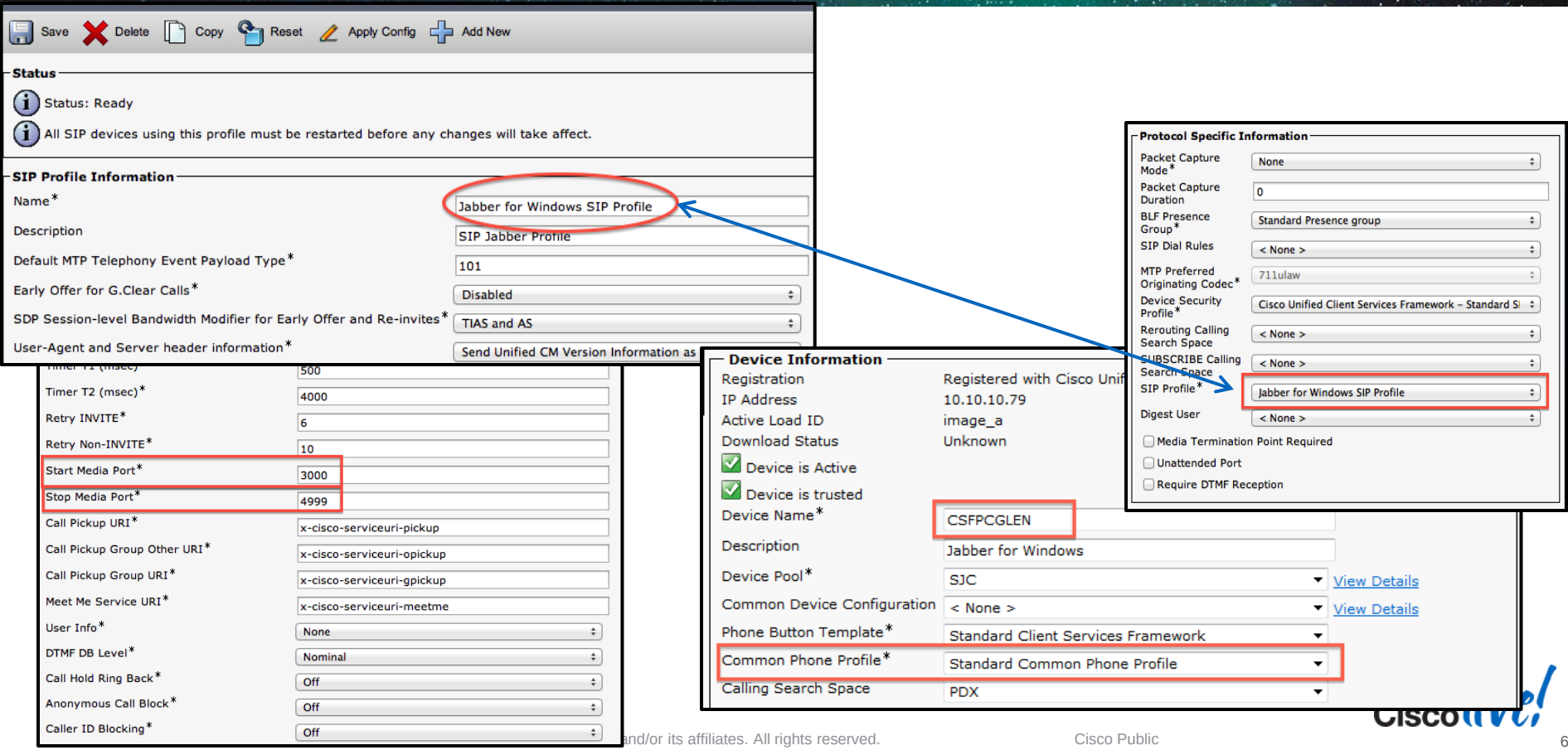
   SIP Signalling is identified on TCP Port range 5060-5061 to and classified and remarked to CS3.

Example QoS Policy for Jabber Clients:

- UDP Port Range 3xxx Mark DSCP EF
- UDP Port Range 4xxx Mark DSCP AF41
- TCP Port 5060-5061 Mark DSCP CS3

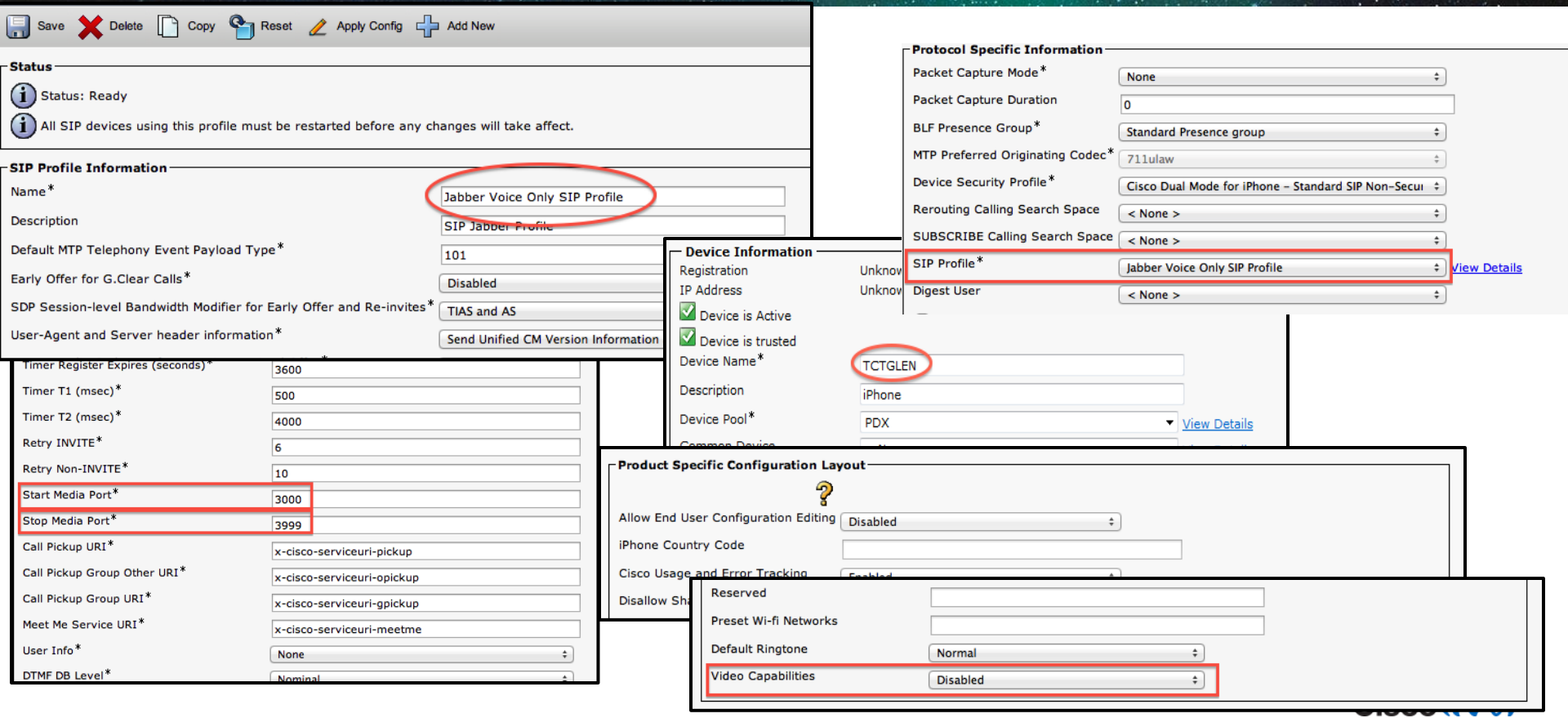
Configuring Jabber Client

Managing Media Ports: SIP Profile



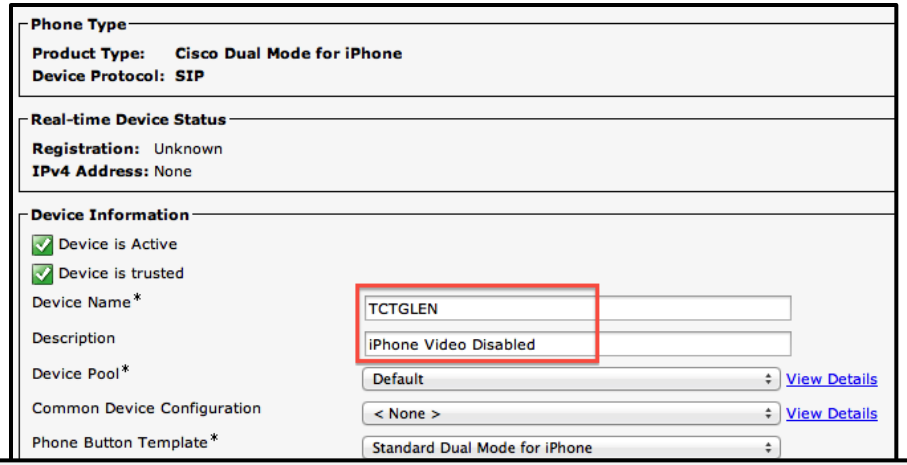
Configuring Jabber Client

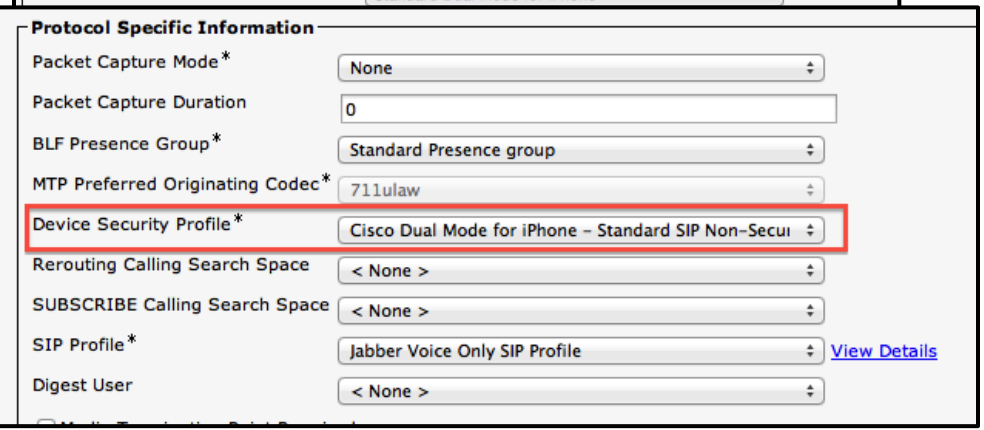
Managing Media Ports: SIP Profile / Voice Only

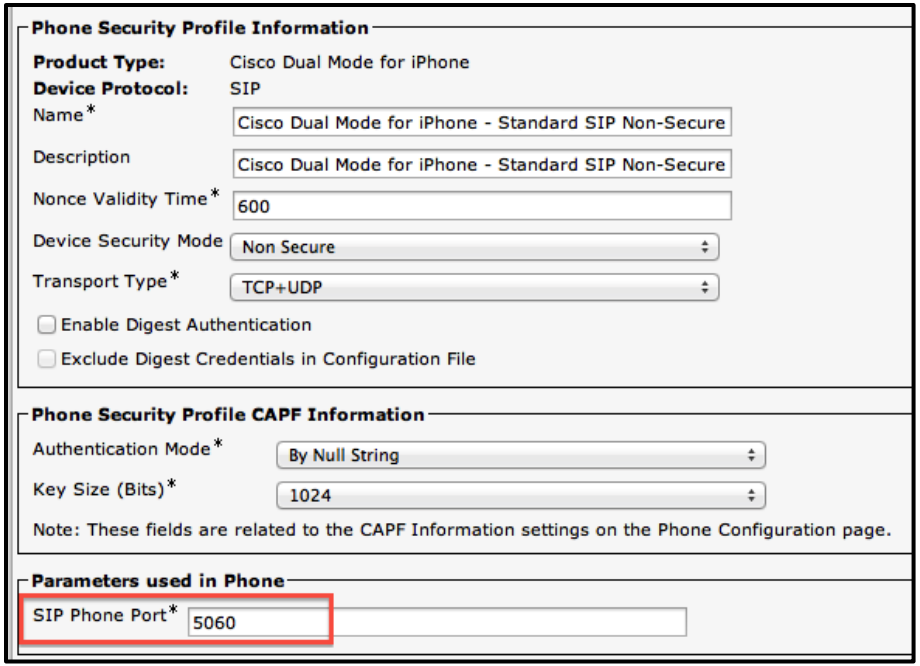


Configuring Jabber for Windows Client

Managing Signalling Port: IP Security Profile



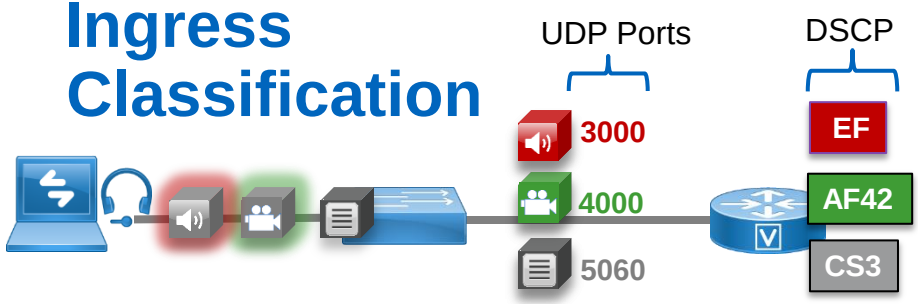




Jabber Client Summary / Best Practices

- Use the SIP Profile to configure media port range (default 16384-32766)
- Use the Sip Security Profile to configure the signalling port range (default 5060 or 5061 for secure signalling)
- If you have SCCP devices in the same network use a port range outside of 16384-32766 to avoid overlap and incorrect remarking
  - **Unified CM 9.1 expands SIP media port range to 2048-65535**
- Video Enablement:
  - Disable video if you do not want device to send or receive video
  - Video capable devices ALWAYS divide the port ranges (even if video is disabled)
  - Devices that do NOT support video (version dependent) use the entire port range for audio-only.

Ingress Classification



1

```
! This section applies the policy-map to the Interface
Router (config-if)# service-policy input INGRESS-MARKING
 ! Attaches service policy to interface
```

2

```
! This section configures the policy-map to set DSCP
 for JABBER Voice, Video and SIP Signaling on
ingress
policy-map INGRESS-MARKING
  class JABBER-VOICE
   set dscp ef
 class JABBER-VIDEO
   set dscp af42
  class JABBER-SIP
   set dscp cs3
 class class-default
```

3

```
! This section configures the classes
class-map match-all JABBER-VOICE
  match access-group 100
class-map match-all JABBER-VIDEO
  match access-group 101
class-map match-all JABBER-SIP
  match access-group 102
```

4

```
! This section configures the ACL's
access-list 100 permit udp any any range 3000 3999
access-list 101 permit udp any any range 4000 4999
access-list 102 permit tcp any any range 5060 5061
```

5

6

Egress Queuing

6

```
! This section applies the policy-map to the Interface
Router (config-if)# service-policy output EGRESS-QUEUING
 ! Attaches service policy to interface
```

```
! This section configures the bandwidth for all collab traffic
policy-map EGRESS-QUEUING
class VOICE
    priority percent 10
! Provisions 10% LLQ to VOICE class
 class VIDEO
    bandwidth percent 30
 ! Provisions 30% CBWFQ to VIDEO class
 class SIGNALING
    bandwidth percent 2
! Provisions 2% CBWFQ to SIGNALING class
...
```

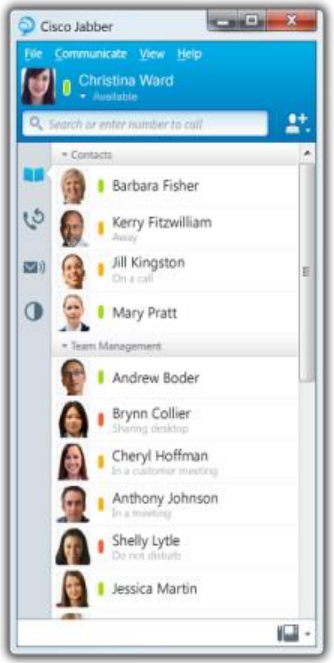
7

```
! This section applies the policy-map
class-map match-all VOICE
match dscp ef
class-map match-any VIDEO
match dscp af41
match dscp af42
class-map match-all SIGNALING
 match dscp cs3
```

8

Jabber For Windows "To Trust or Not to Trust"

Group Policy Objects



Media Port Range
(3000-4999)

QoS Group Policy

Audio Call
(Voice Stream)

Video Call
(Voice and Video Streams)

(EF)
(Ports:3000-3999)

(AF41)
(Ports:4000-4999)

EF EF EF — Voice Stream

EF EF EF — Voice Stream

AF 41 AF 41 AF 41 — Video Stream

SIP Port Range
(5060-5061)

QoS Group Policy

SIP Signalling

(CS3)
(Ports:5060-6061)

CS3 CS3 CS3 — SIP Signalling

Summary / Best Practice Recommendations

Trusted / Native Marking

- Windows 7 and 8 require GPOs set QoS
  - GPOs use TCP and UDP port ranges to set QoS
  - Cannot differentiate audio-only from audio of a video call
- Previous Windows versions allow the application to set QoS natively
- All other Jabber clients (latest versions) mark EF for audio-only, AF41 for audio and video of a video call.

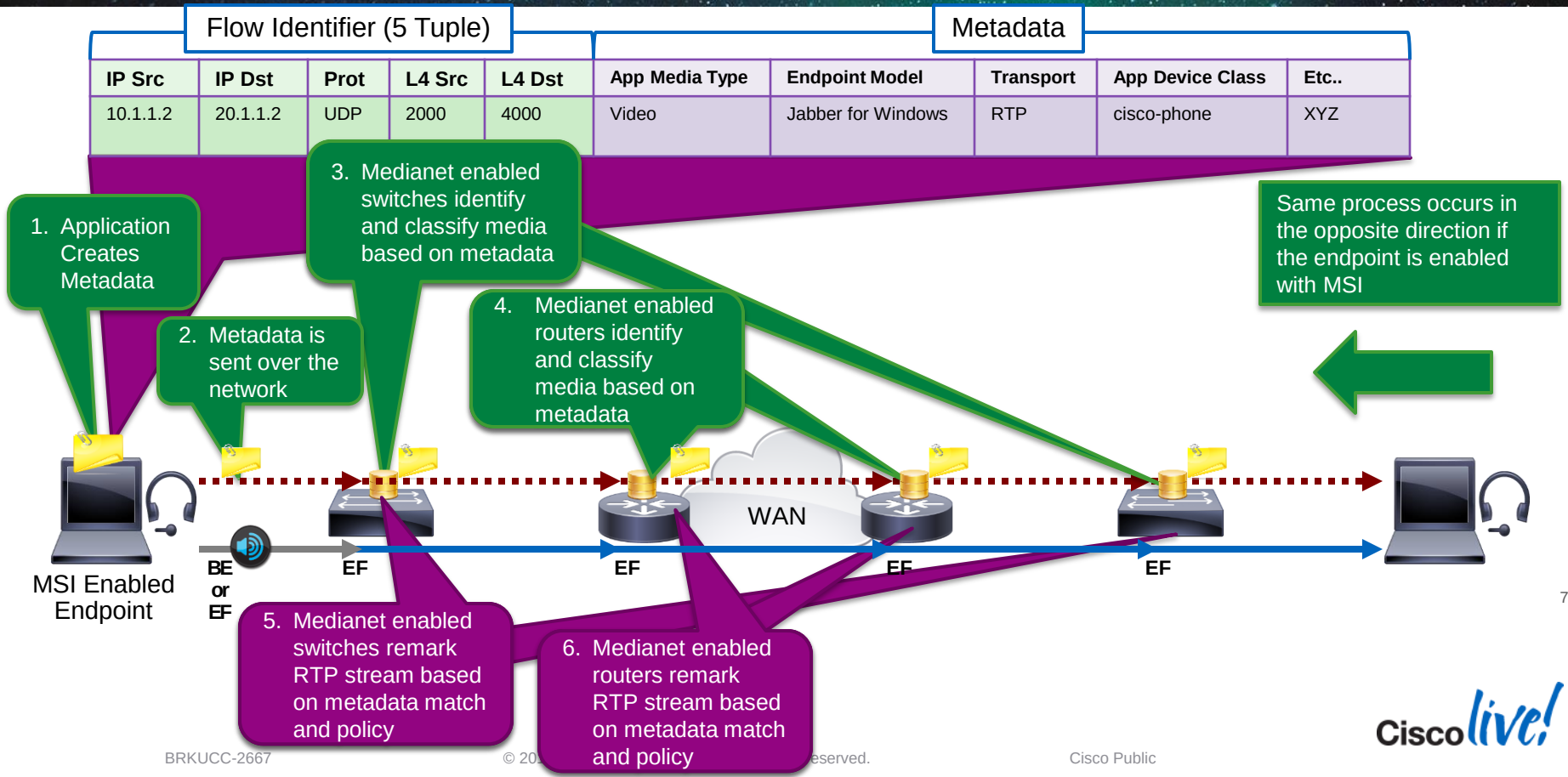
Mapping Identifiable Media and Signalling Streams (Network ACLs)

- QoS Strategies
  - Mark audio EF and Video AF41
  - Mark audio AF41 and Video AF42
  - Mark audio and video AF42
- Recommended Remarking Policy
  - Remark using UDP/TCP Port ranges OR Use MSI and Medianet Metadata (next section)

Classification and Identification Agenda

- Trusted Devices
- **Untrusted Devices:**
  - Mapping UDP/TCP Port Ranges
  - **Medianet Metadata**

Medianet Flow Metadata



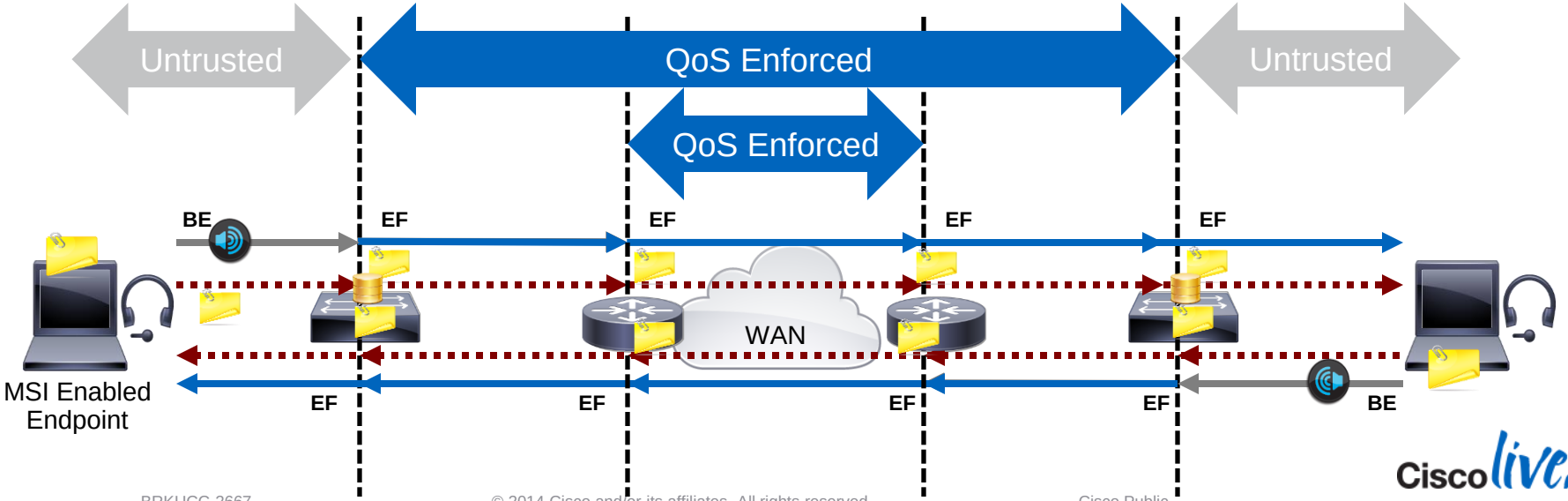
Medianet Flow Metadata
What's the Benefit?

```
(config)#metadata flow
```

```
(config)#interface g0/1
(config-interface)#metadata flow
```

- Enable metadata flow globally, or per interface
- RSVP snooping required on L2 switch

- Mark on switches and trust on routers enforcing QoS end-to-end across the network
- Mark on routers to enforce QoS on the WAN (good starting point).



Network Devices Supporting Medianet Metadata

Platform	IOS / Switch Image	Package	Medianet Feature
Cisco Catalyst 4500E Supervisor Engine 7-E and 7L-E, Cisco Catalyst 4500E Supervisor Engine 6-E, Cisco Catalyst 4500 Supervisor Engine 6L-E, Cisco Catalyst 4500X Series	XE 3.3.0SG or later 15.1.(1)SG or later	IP Base or higher	Media Awareness: • Flow Metadata • Media Services Proxy
Cisco Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F Switches	15.1(1)SG or later	IP Base or higher	Media Awareness: • Flow Metadata • Media Services Proxy
Cisco Catalyst 6500-E Series Switches Supervisor Engine 2T Cisco Catalyst 6500-E Series Switches Supervisor Engine 720	15.0(1)SY or later 15.1(2)SY or later	IP Base or higher	Media Awareness: • Flow Metadata • Media Services Proxy
Cisco 880*, 990*, 1900, 2900 and 3900 Series Integrated Services Routers	15.2(1) T	Data	Media Awareness: • Flow Metadata
	15.2(3) T, *15.2(4) M2	Data	Media Awareness: • Media Services Proxy
	15.4(1)T 15.4(1)S	Data	Reverse Flow Metadata Support
Cisco ASR 1000 Series Aggregation Services Routers	Cisco IOS XE 3.7 or later	Advanced Enterprise	Media Awareness: • Flow Metadata

Collaboration Endpoints Supporting Medianet Metadata

Collaboration Endpoints	Version
Cisco Jabber for Windows	UC 9.0(1) or later
Cisco Jabber for Mac	9.2.1 or later
Cisco Jabber for iOS and Android	Planned*
Cisco TelePresence (EX, C, MX, SX, TX, CTS 500-32, TX1300 and TX9000). MSI Included in software install	TC 6.0 or later
WebEx	WebEx (WBS28)

Current defect in TX6.3 and TC7.0! To be fixed in 7.0.2 and 6.4?

* MSI for iOS and Android support planned. Come talk to me if this is important to you!

QoS: Metadata Based Classifications

Application Identifier

- match application telepresence-media
- match application cisco-phone

Dynamic Attribute

- match application attribute media-type audio
- match application attribute media-type video
- match application attribute media-type audio-video

Audio-Only Call

Video Call

Application Group

- match application application-group webex-group
- match application application-group telepresence-group

Category

- match application attribute category voice-video
- match application attribute category business-productivity-tools

Class-map Migration for Existing Egress QoS Policy

Class-map match-all Jabber

Match access-group 110

Class-map match-any Jabber

Match application cisco-phone

Match access-group 110

Match ….

```
Class-map: Jabber (match-any)
     100198 packets, 10599254 bytes
     30 second offered rate 75000 bps
     Match:  application cisco-phone
       99535 packets, 10512016 bytes
       30 second rate 75000 bps
     Match: access-group 110
       663 packets, 87238 bytes
       30 second rate 0 bps
```

Class-map Migration for Existing Ingress QoS Policy

```
class-map match-all VOICE
  match access-group 100
class-map match-any VIDEO
  match access-group 101
class-map match-all SIGNALING
  match access-group 102
```

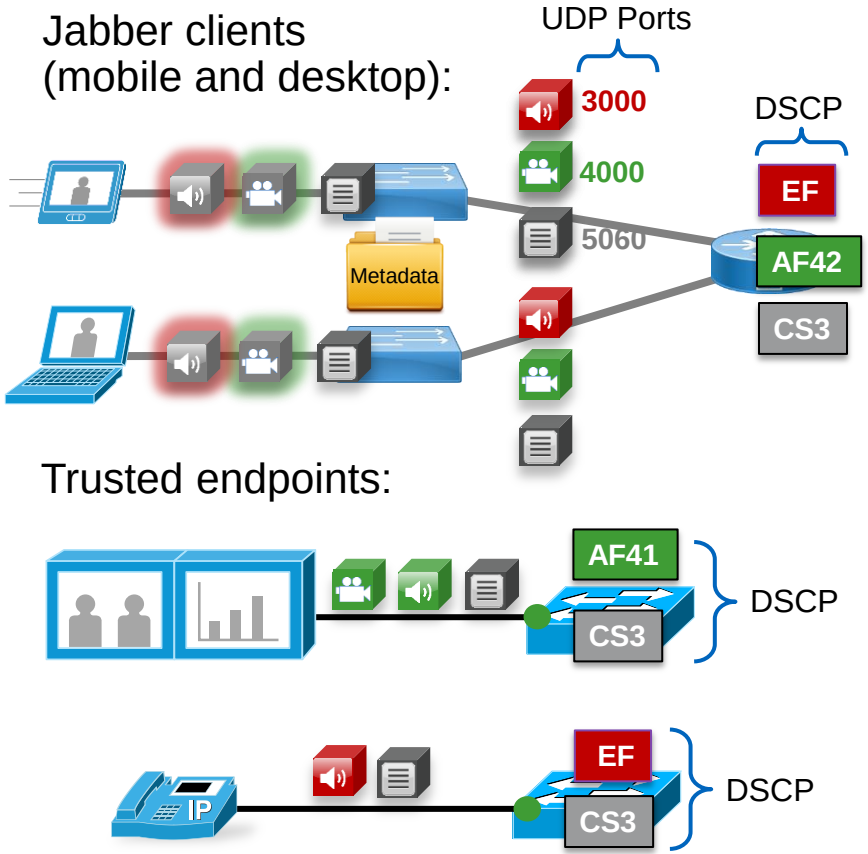
```
class-map match-any VOICE
  match application attribute media-type audio
  match access-group 100
class-map match-any VIDEO
  match application attribute media-type audio-video
  match application attribute media-type video
  match access-group 101
class-map match-any SIGNALING
  match application attribute sub-category control-and-signaling
  match access-group 102
```

```
policy-map INGRESS-MARKING
  class VOICE
    set dscp ef
Class VIDEO
    set dscp af41
 class SIGNALING
    set dscp cs3
class class-default
```

Note: No Device Type Differentiation. This policy applies to ALL metadata capable endpoints that match these attributes.

Identification and Classification

Bringing it all Together

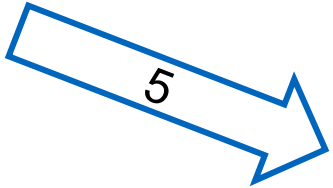


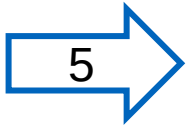
- Jabber classification based on UDP port ranges and ACL's (mobile clients) and/or metadata (desktop clients):
  - Audio of **all** Jabber calls (voice-only and video) is marked EF
  - Video of Jabber calls is marked AF42
- Video endpoint and IP phone classification based on conditional trust and CDP:
  - Audio and video streams of video calls are marked AF41
  - Voice-only calls are marked EF

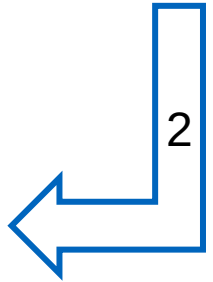
Ingress Classification
Port Ranges and Metadata

```
! This section configures the ACL's
access-list 100 permit udp any any range 3000 3999
access-list 101 permit udp any any range 4000 4999
access-list 102 permit tcp any any range 5060 5061
```

```
! This section applies the policy-map to the Interface
Router (config-if)# service-policy input INGRESS-MARKING
  ! Attaches service policy to interface
```

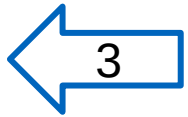


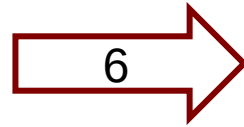




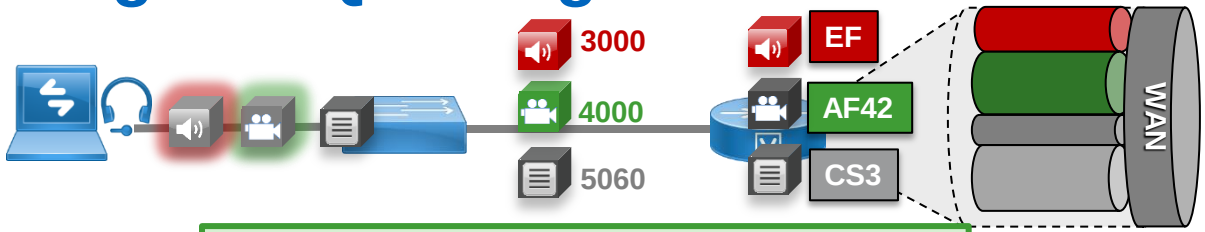

```
! This section configures the classes
class-map match-any JABBER-VOICE
  match application attribute media-type audio
  match access-group 100
class-map match-any JABBER-VIDEO
  match application attribute media-type audio-video
  match application attribute media-type video
  match access-group 101
class-map match-any JABBER-SIP
  match application attribute sub-category control-and-signaling
  match access-group 102
```

```
! This section configures the policy-map to set DSCP
 for JABBER Voice, Video and SIP Signaling on
ingress
policy-map INGRESS-MARKING
   class JABBER-VOICE
     set dscp ef
class JABBER-VIDEO
     set dscp af41
 class JABBER-SIP
     set dscp cs3
class class-default
```





Egress Queuing



Queuing on EGRESS

All marked traffic:

1. Trusted
2. Metadata
3. Port Ranges

6

```
! This section applies the policy-map to the Interface
Router (config-if)# service-policy output WAN-EDGE-QUEUING
 ! Attaches service policy to interface
```

```
! This section configures the bandwidth for all collab traffic
policy-map WAN-EDGE-QUEUING
class VOICE
    priority percent 10
! Provisions 10% LLQ to VOICE class
 class VIDEO
    bandwidth percent 30
 ! Provisions 30% CBWFQ to VIDEO class
 class SIGNALING
    bandwidth percent 2
! Provisions 2% CBWFQ to SIGNALING class
...
```

7

```
! This section applies the policy-map
class-map match-all VOICE
match dscp ef
class-map match-any VIDEO
match dscp af41
match dscp af42
class-map match-all SIGNALING
 match dscp cs3
```

8

Medianet Metadata
Benefits and Best Practices Recommendations

Benefits

- More secure!
  - Don’t have to trust the whole OS, just the application!
  - Less worries about rogue endpoints usurping TCP or UDP port range to hijack your QoS.
- Easy and safe migration from ACL port range mechanism!
  - Simply add the metadata match criteria into your already configured class-maps
  - Ensure they are the first criteria

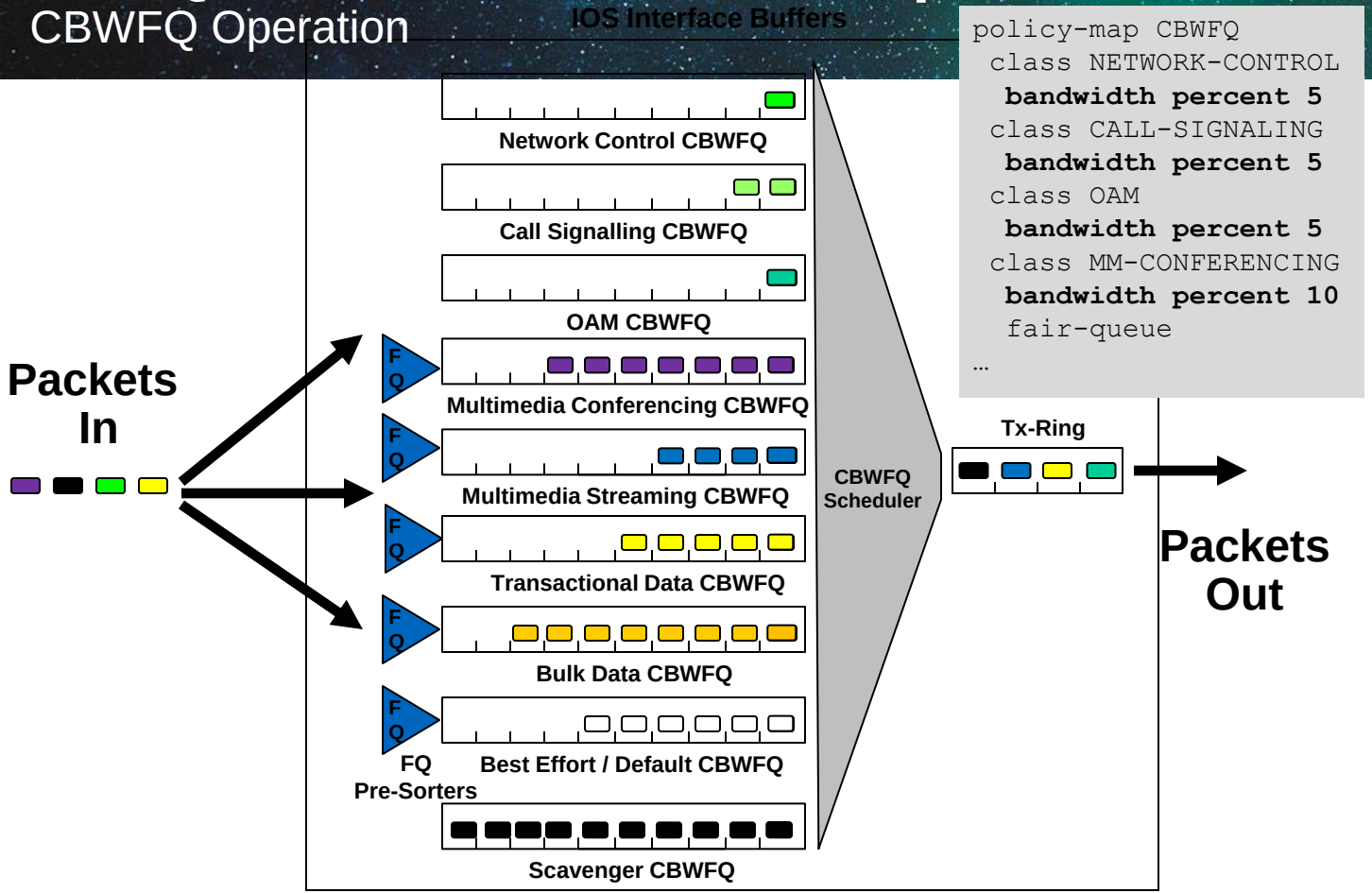



QoS Architecture:

APPROACH OVERVIEW
IDENTIFICATION & CLASSIFICATION
QUEUING & SCHEDULING

IOS QoS Mechanisms and Operation

CBWFQ Operation

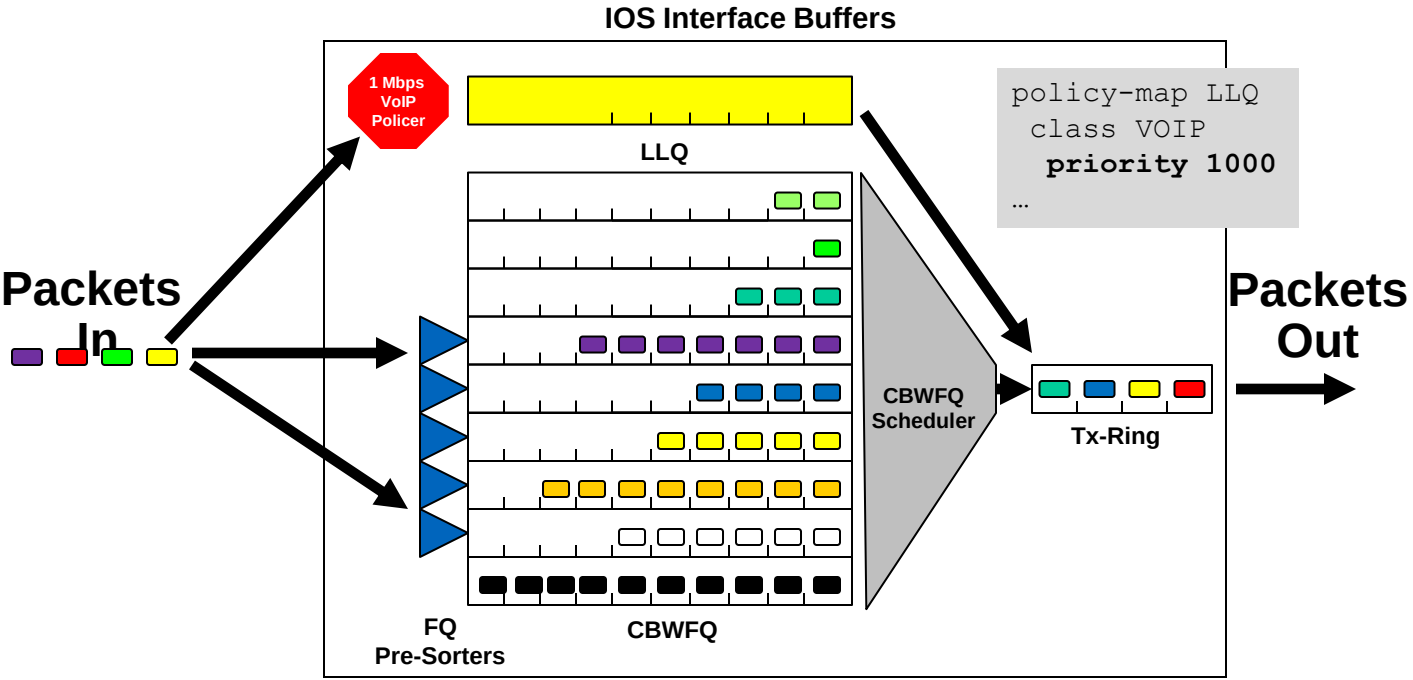



```
policy-map CBWFQ
 class NETWORK-CONTROL
  bandwidth percent 5
 class CALL-SIGNALING
  bandwidth percent 5
 class OAM
  bandwidth percent 5
 class MM-CONFERENCING
  bandwidth percent 10
  fair-queue
…
```

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSWAN_40.html#wp129419

IOS QoS Mechanisms and Operation

(Single) LLQ Operation

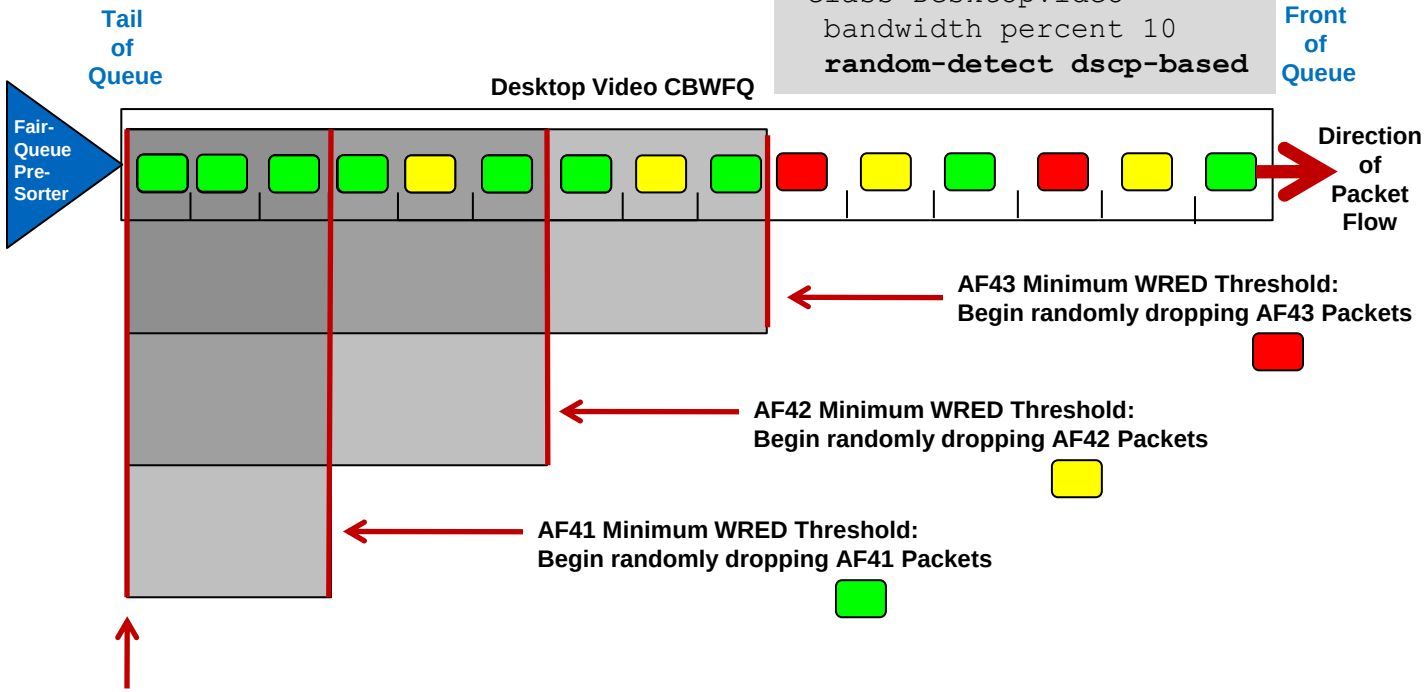


http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSWAN_40.html#wp129443

IOS QoS Mechanisms and Operation

DSCP-Based WRED Operation

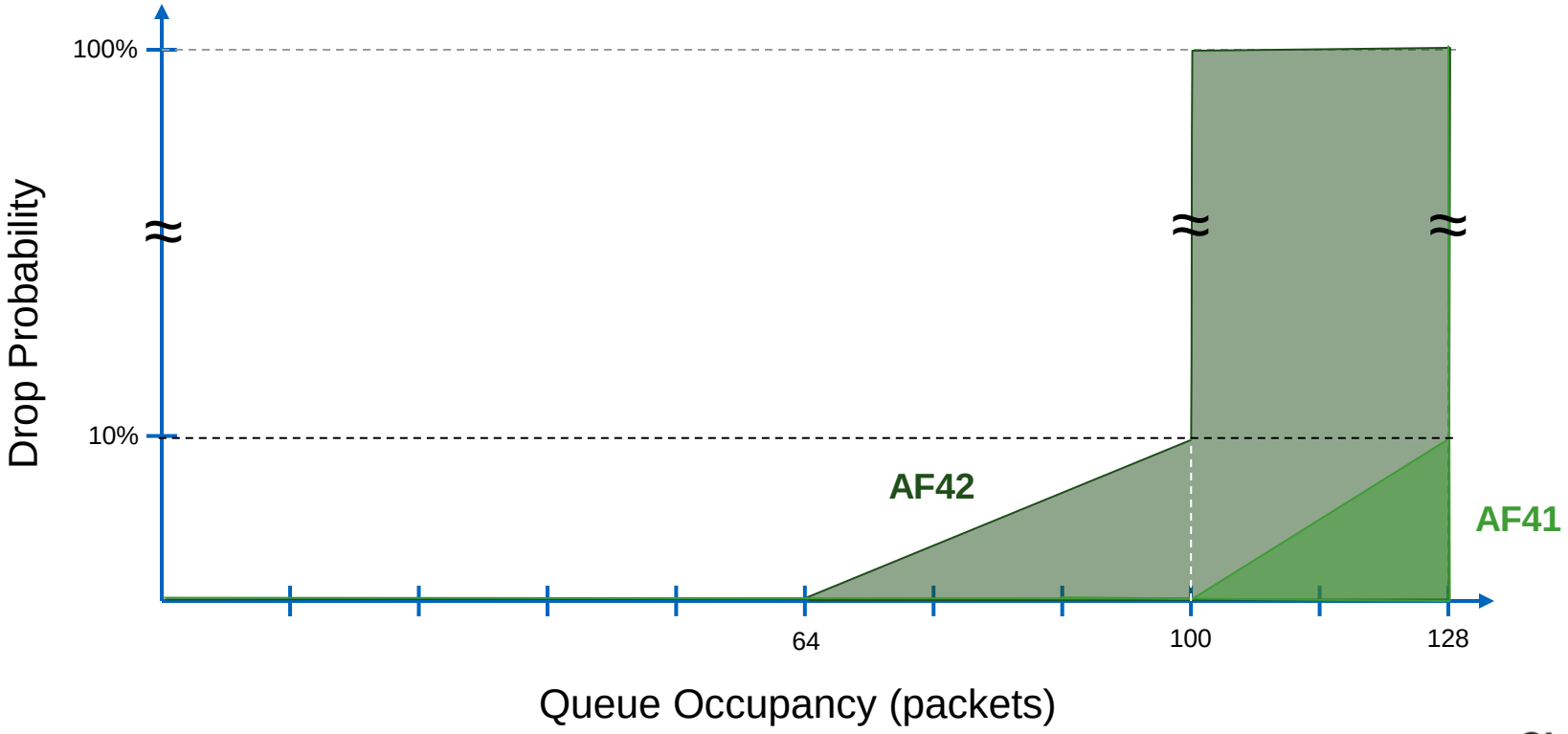
```
policy-map BULK-WRED
 class DesktopVideo
  bandwidth percent 10
  random-detect dscp-based
```



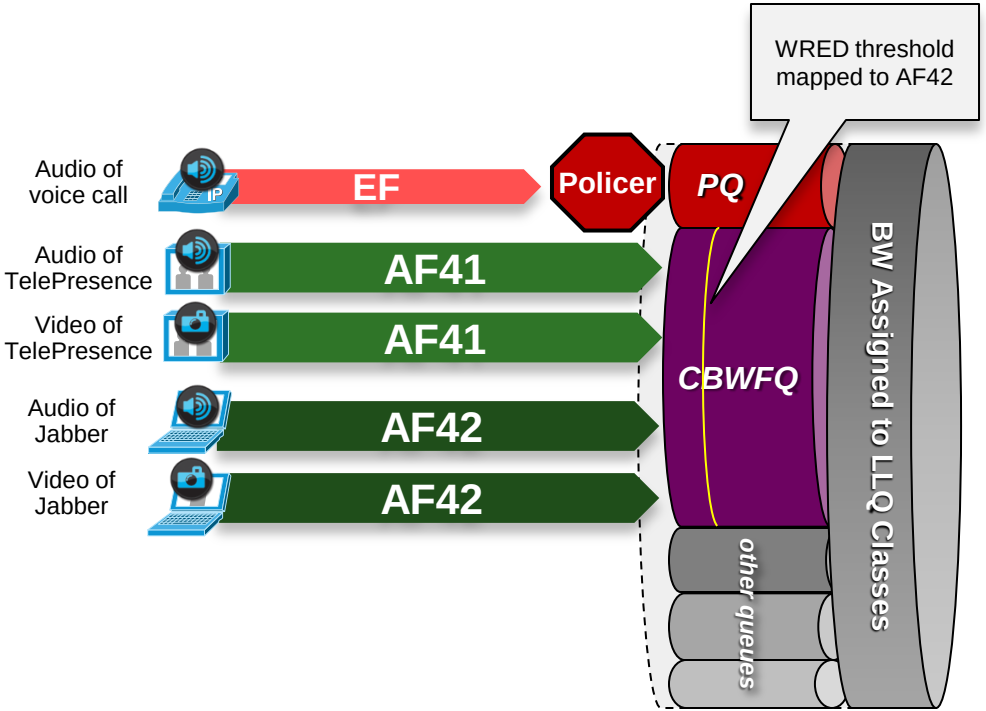
Maximum WRED Thresholds for AF41, AF42 and AF43 are set to the tail of the queue in this example

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSWAN_40.html#wp129476

WRED Thresholds



Queuing and Scheduling
Summary / Example



- Map all audio (EF) traffic to PQ
- Map all video (AF41 and AF42) to a class-based queue, in which:
  - AF41 is tail dropped
  - AF42 is mapped to a WRED threshold




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com


CISCO
TM