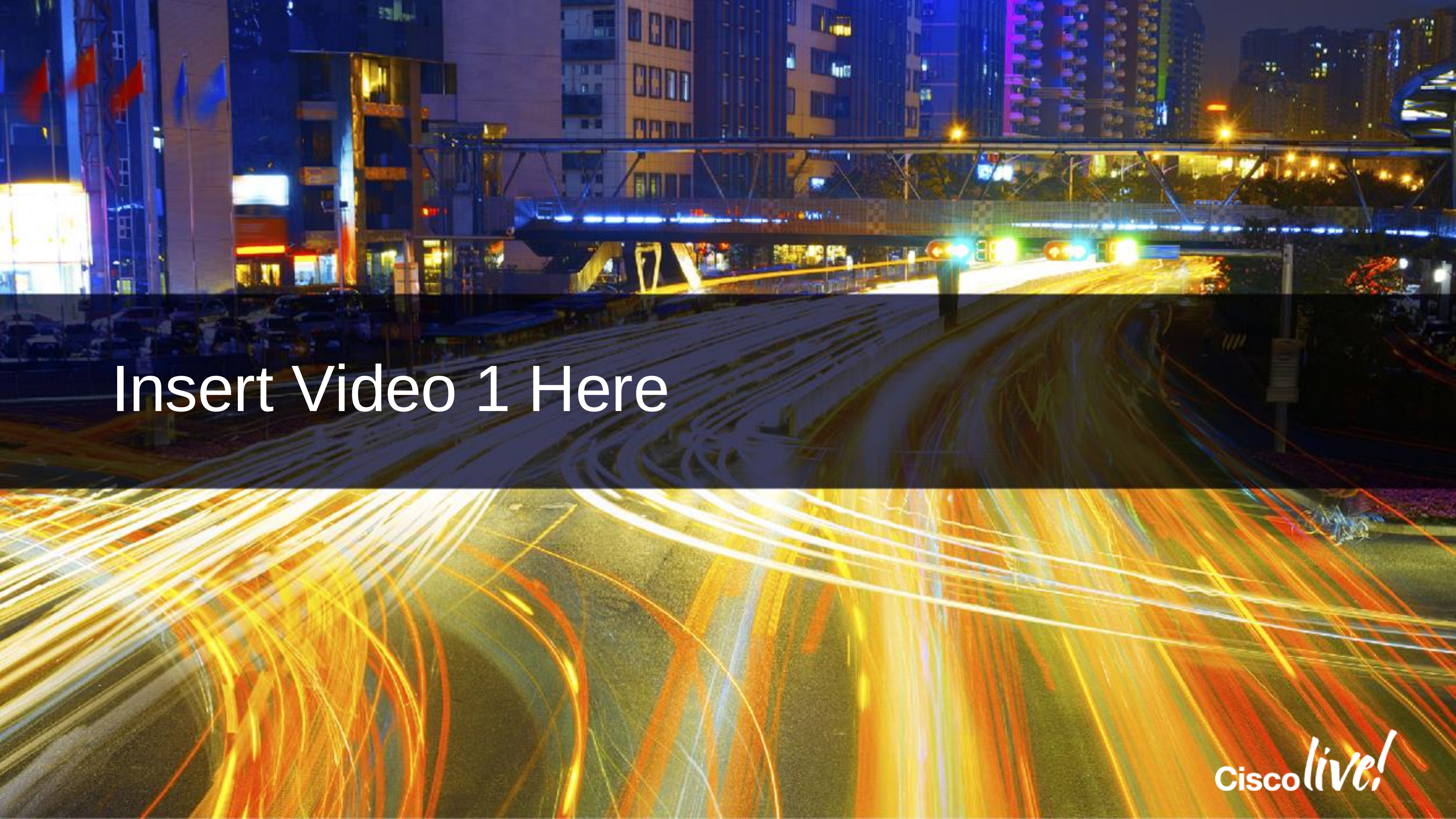
TOMORROW
starts here.

Cisco live!



Insert Video 1 Here

Enterprise QoS - The Most Widely Deployed Feature To Any Enterprise Organisation

BRKRST-2501

Rodney Thomson

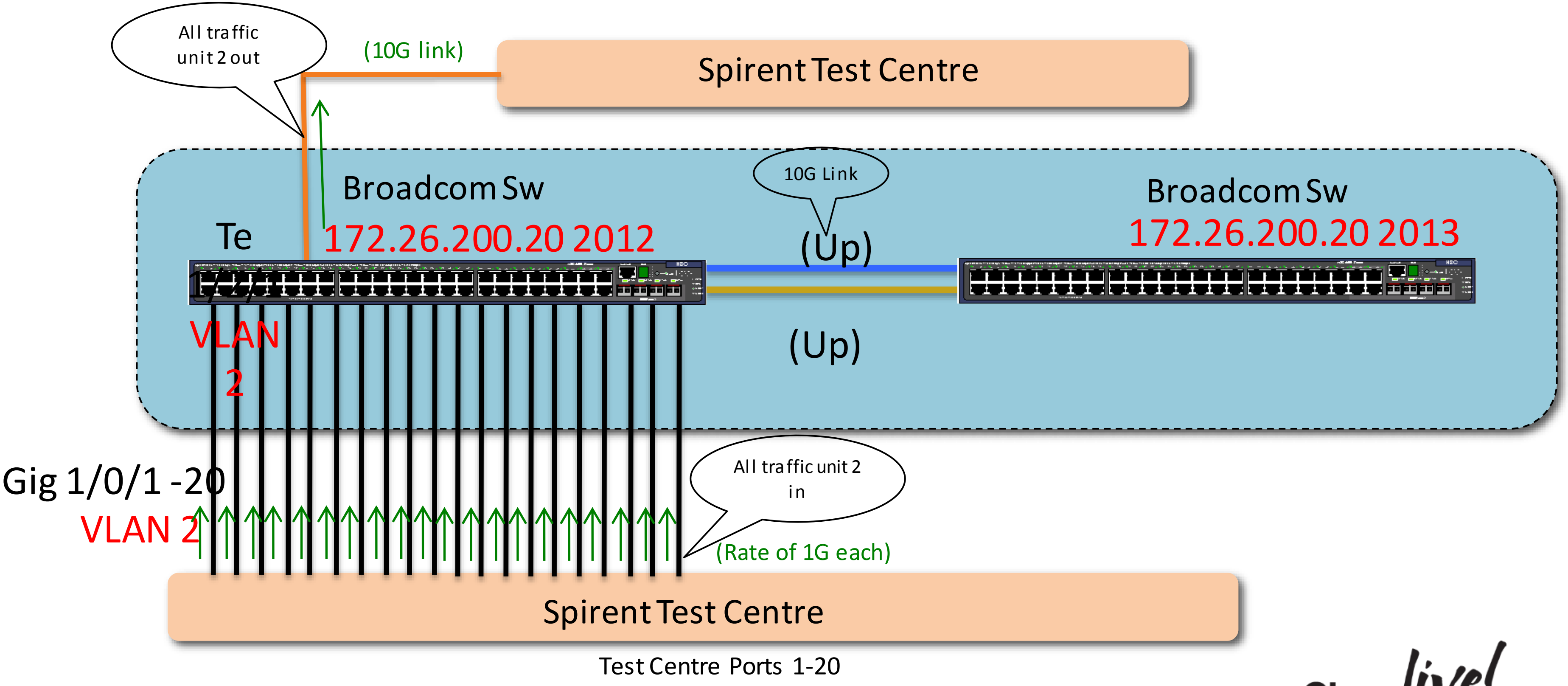
Systems Engineer

#clmel

Cisco live!

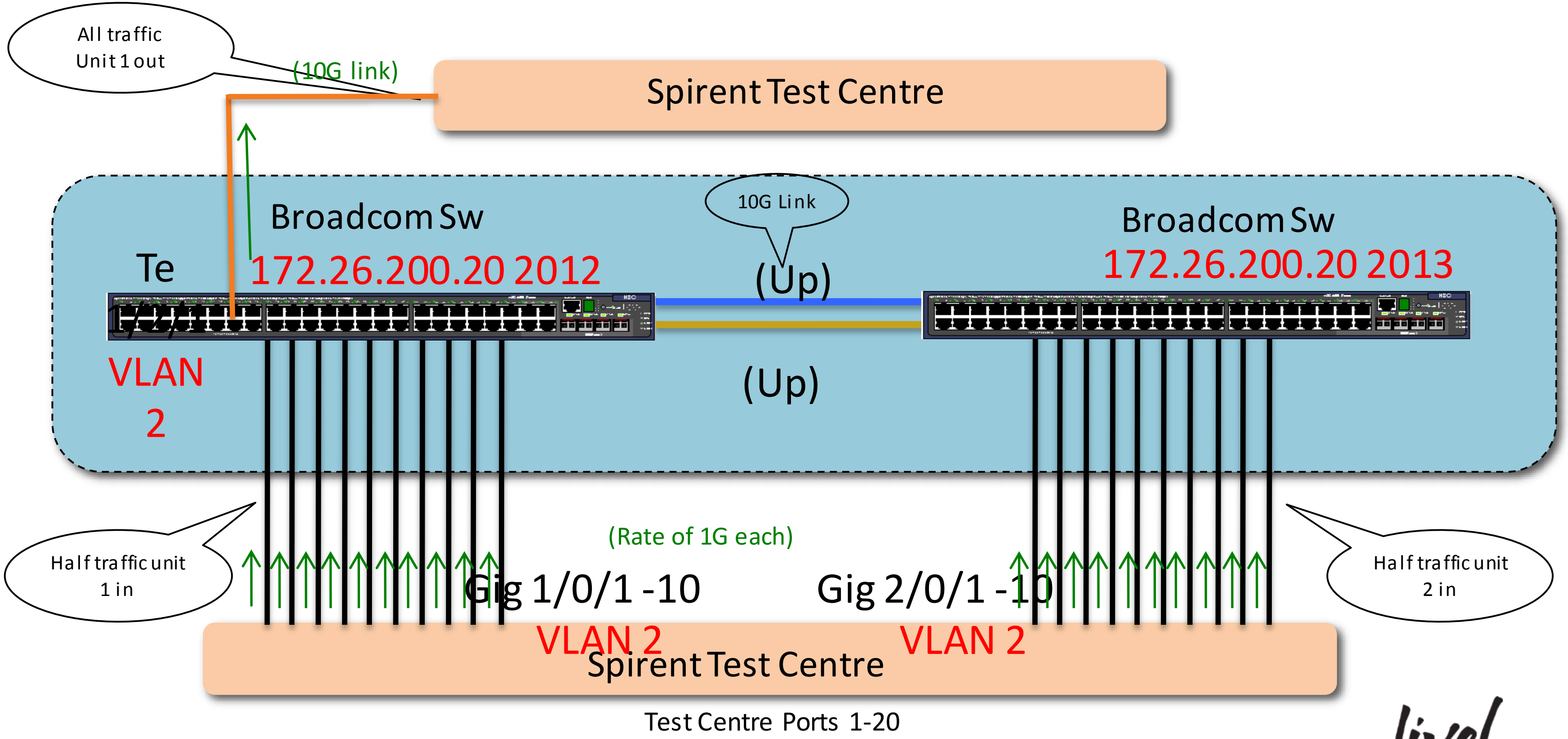
QoS Test – Based on Miercom Report Test

Topology – Scenario 1: same unit



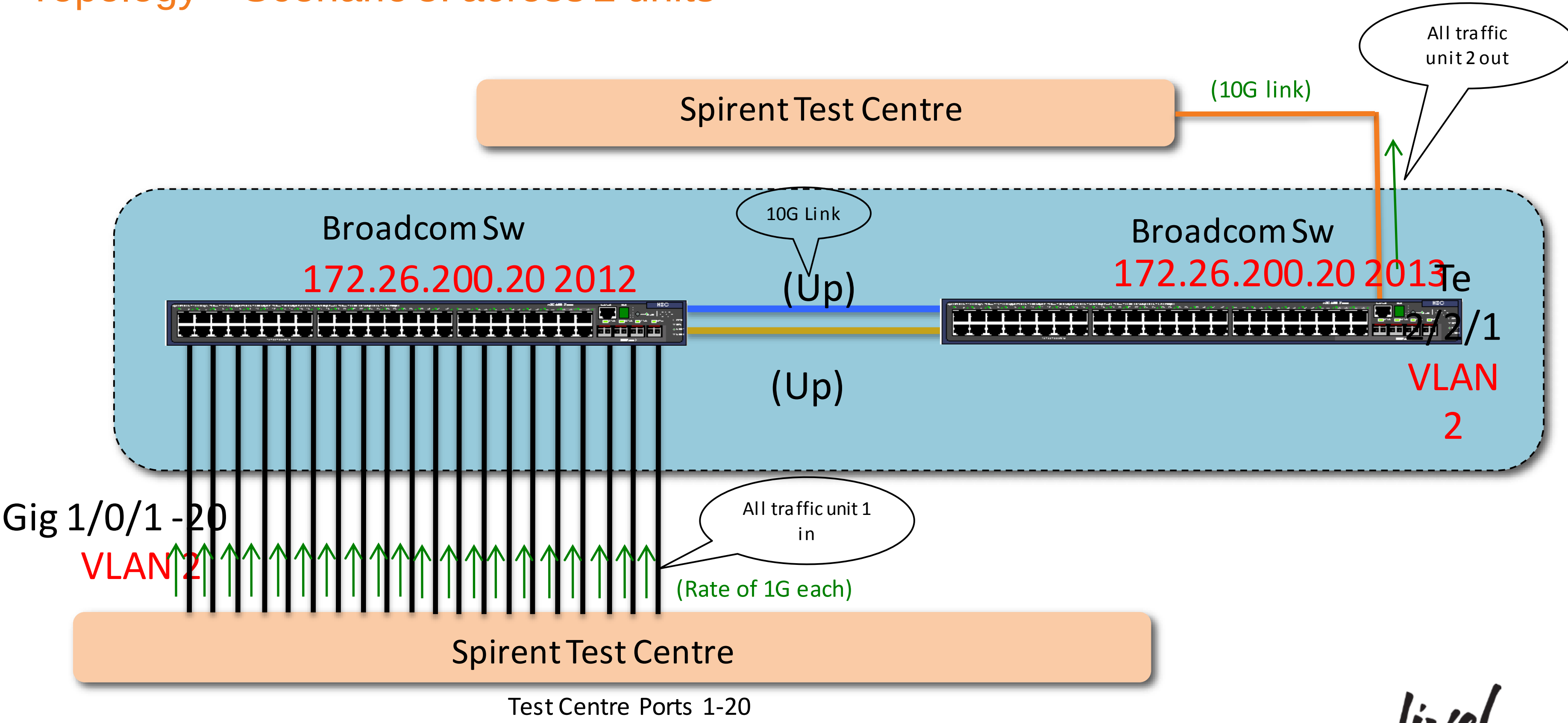
QoS Test

Topology – Scenario 2: split across 2 units



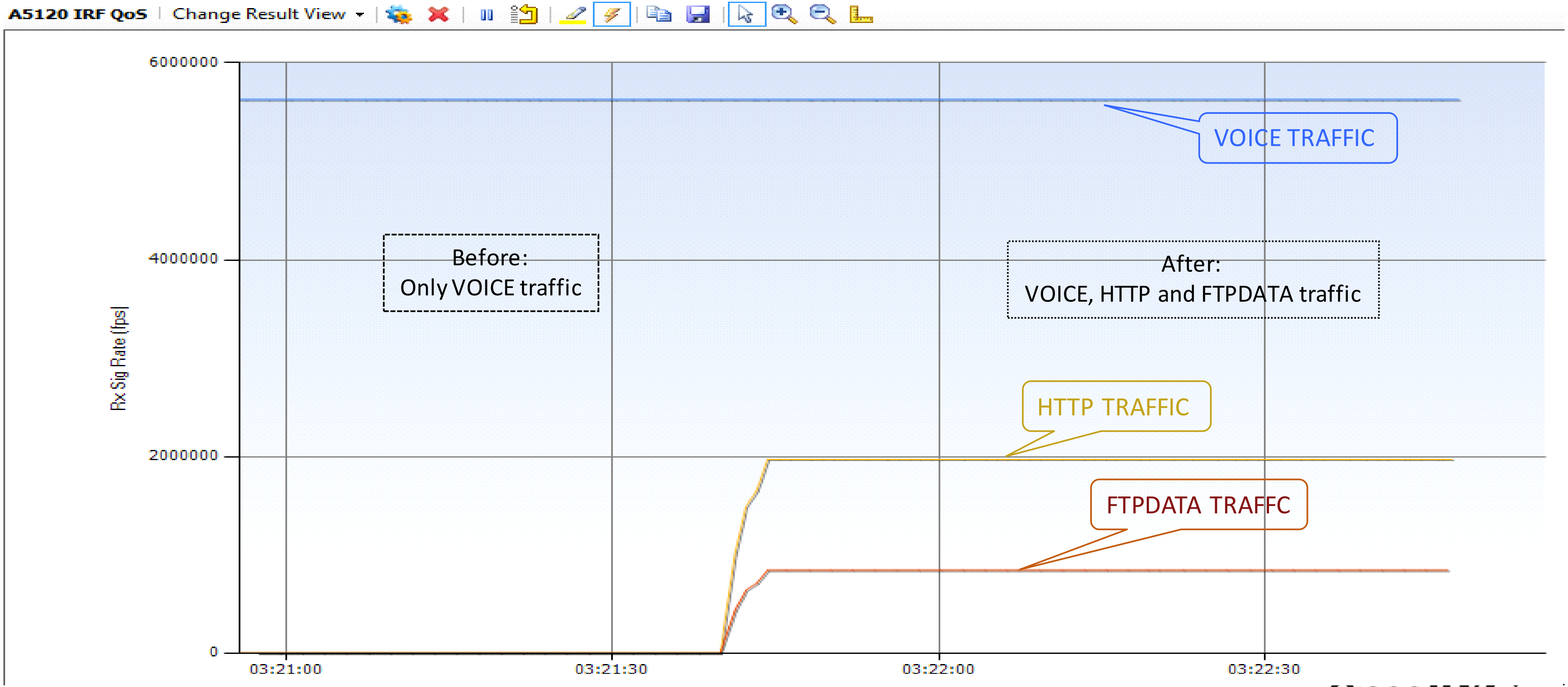
QoS Test

Topology – Scenario 3: across 2 units



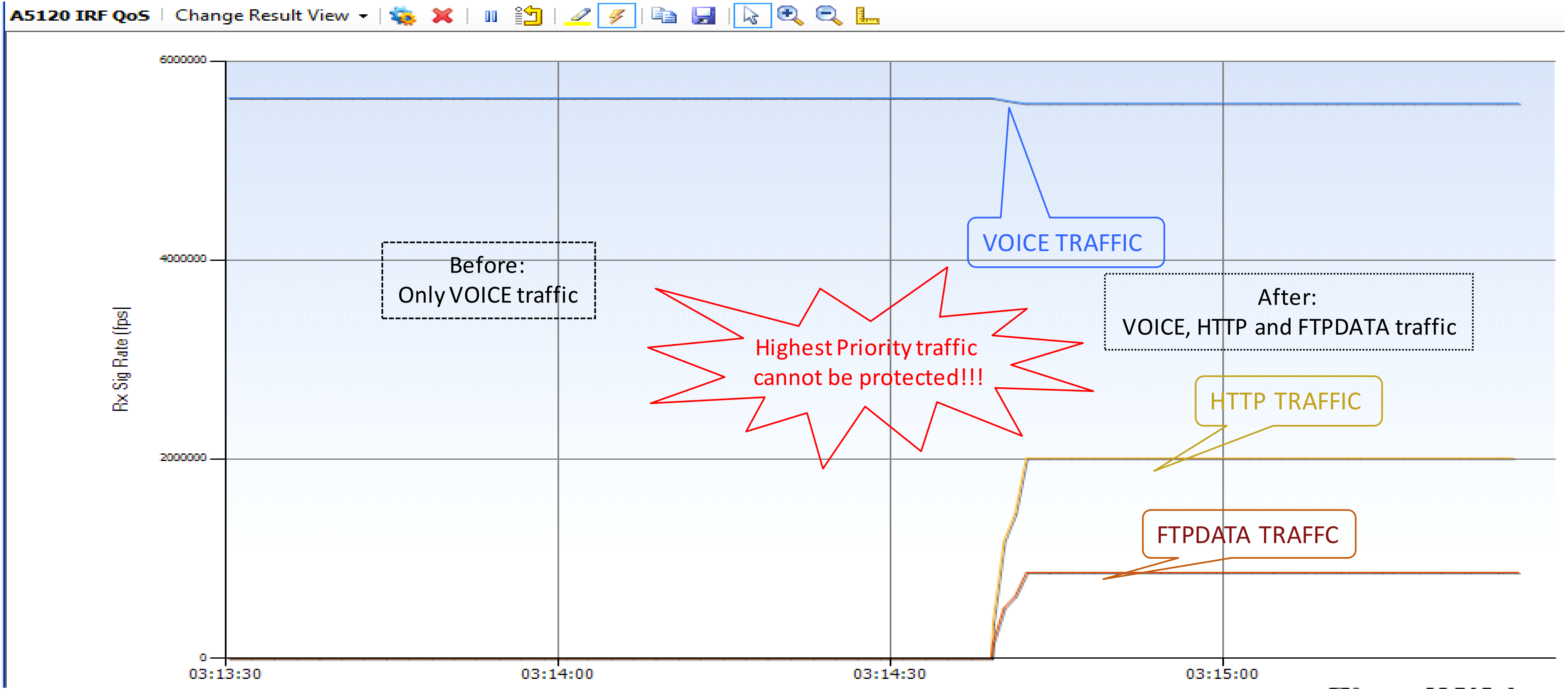
QoS Test – Other Vendor Broadcom Switch

Scenario 1: in the same unit – No DROP on VOICE Traffic



QoS Test – Other Vendor Broadcom Switch

Scenario 2: split-across the units–DROP on VOICE Traffic



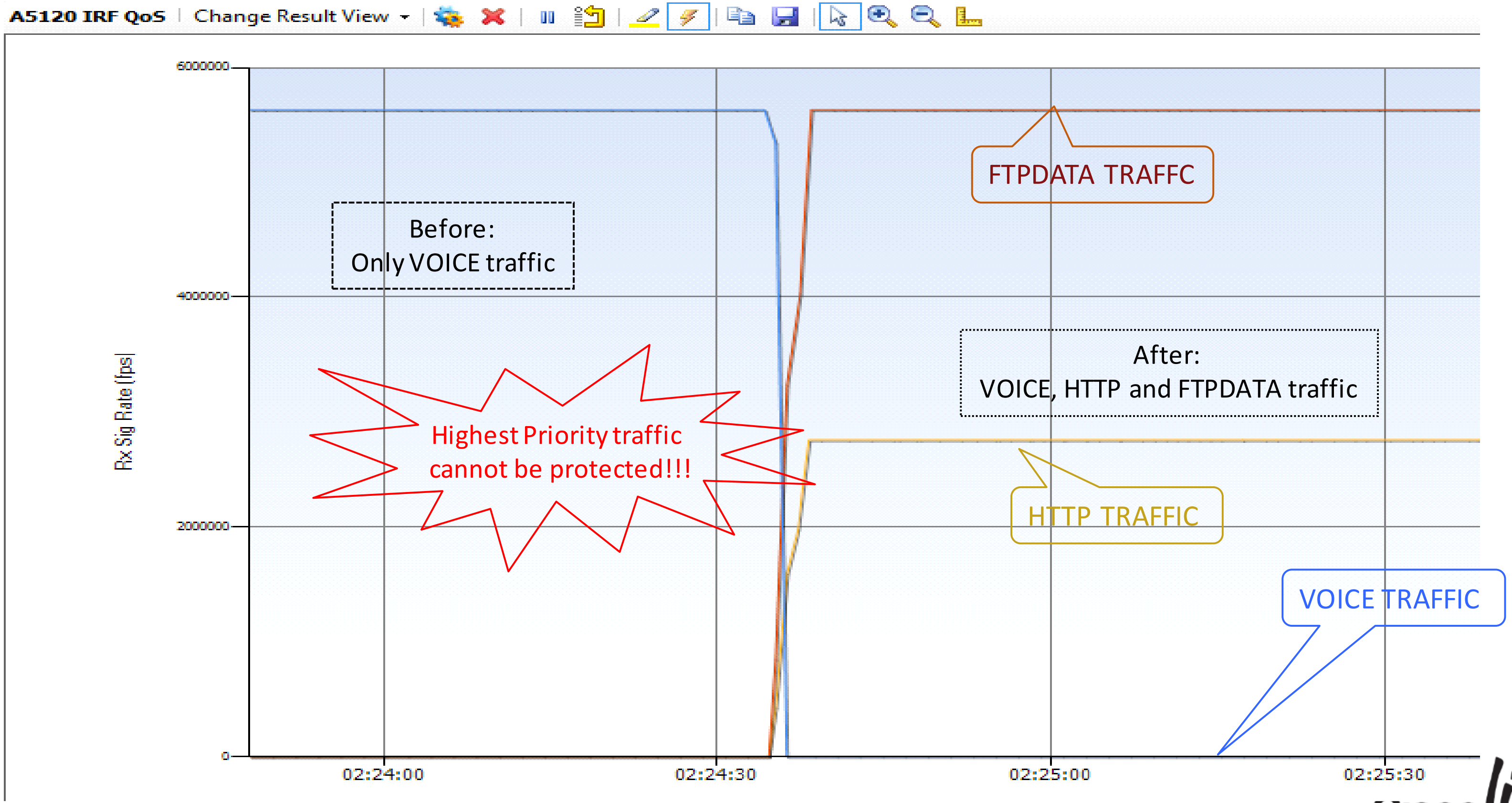
Before:
Only VOICE traffic

After:
VOICE, HTTP and FTPDATA traffic

Highest Priority traffic cannot be protected!!!

QoS Test – Other Vendor Broadcom Switch

Scenario 3: across different units – No VOICE Traffic!



Before:
Only VOICE traffic

Highest Priority traffic cannot be protected!!!

FTPDATA TRAFFC

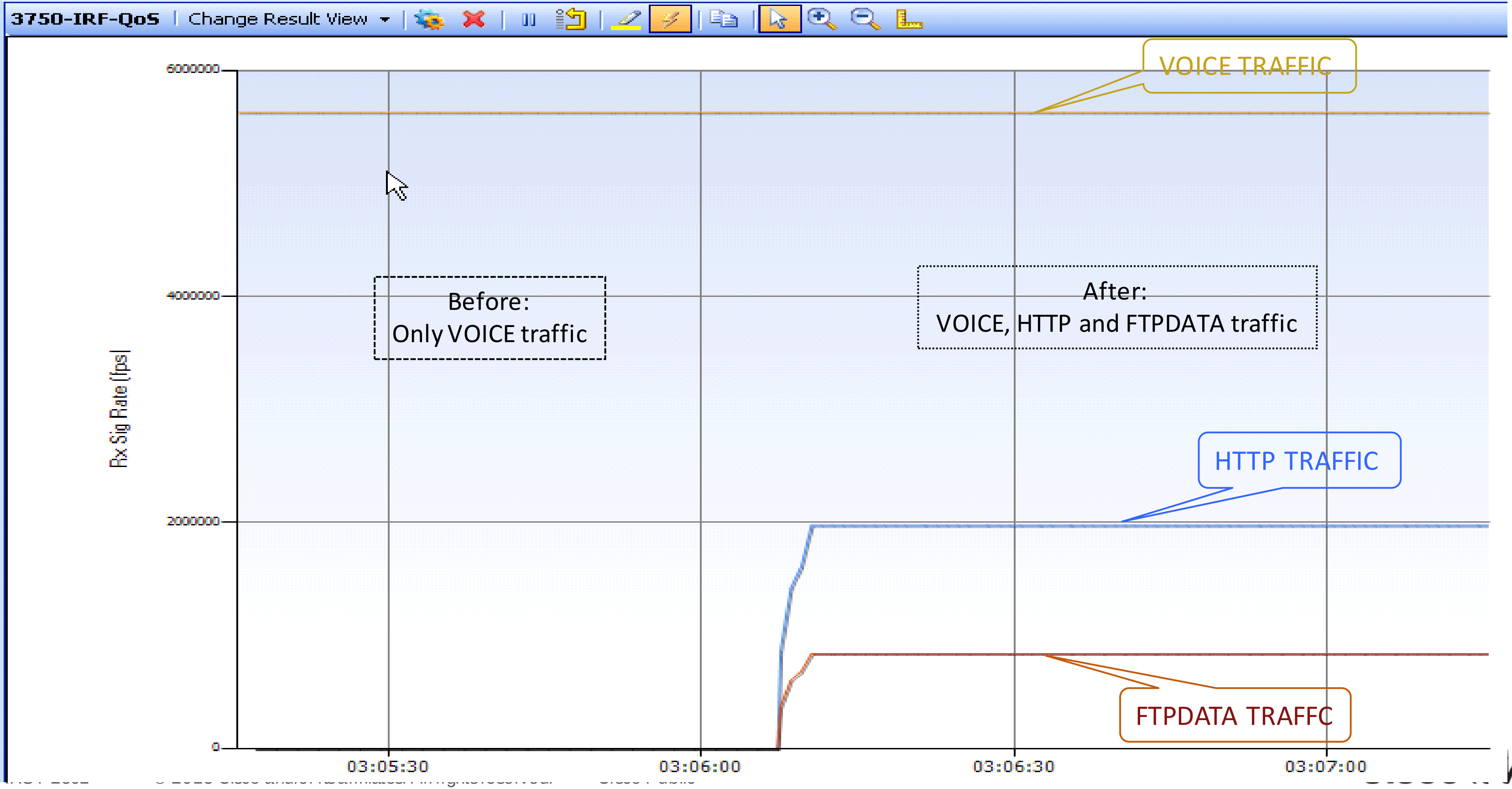
After:
VOICE, HTTP and FTPDATA traffic

HTTP TRAFFIC

VOICE TRAFFIC

QoS Test – Equivalent Cisco Switch

Scenario 1: in the same unit –NO DROP on VOICE Traffic



VOICE TRAFFIC

Before:
Only VOICE traffic

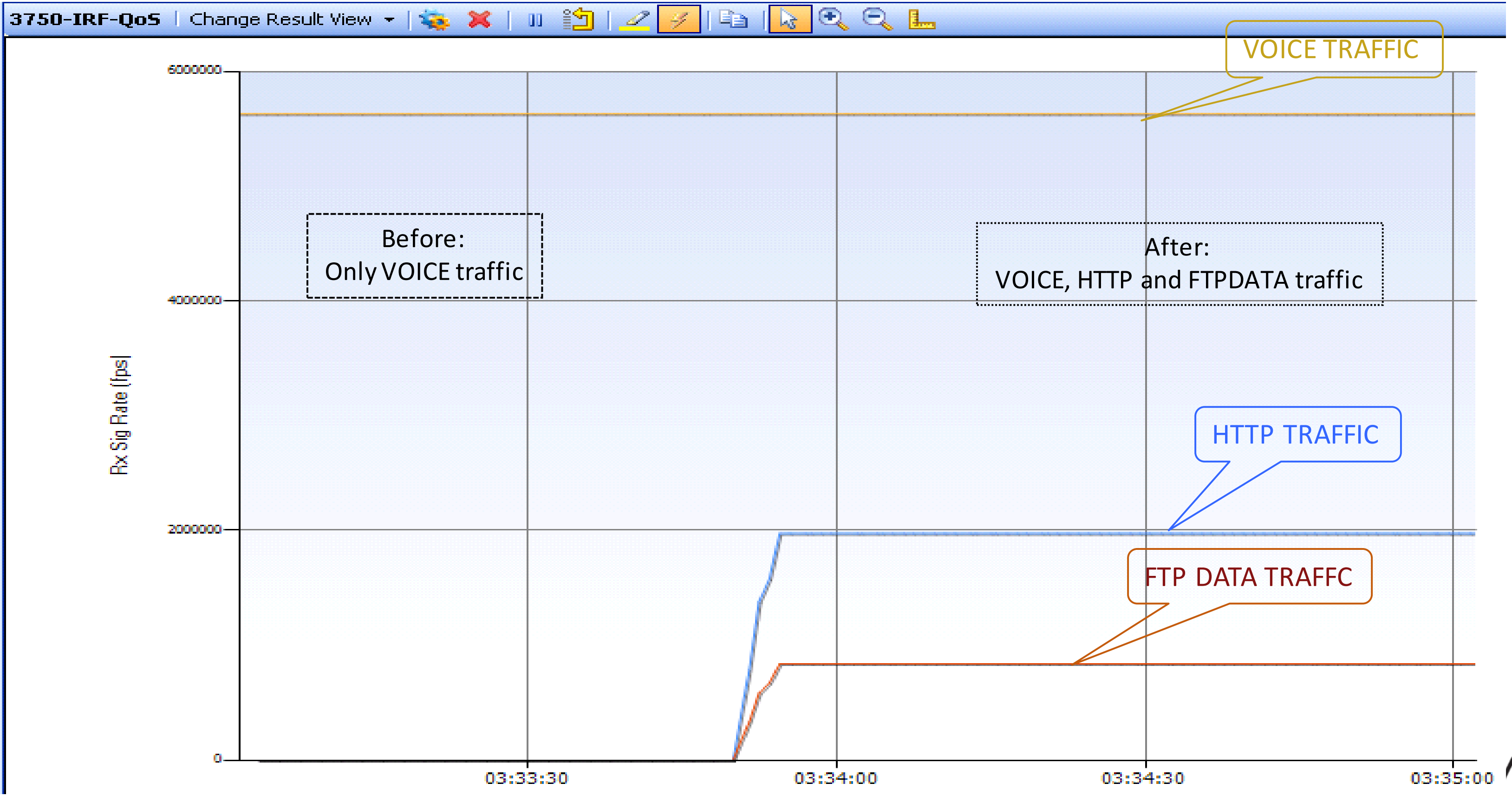
After:
VOICE, HTTP and FTPDATA traffic

HTTP TRAFFIC

FTPDATA TRAFFC

QoS Test – Equivalent Cisco Switch

Scenario 2: semi-across the units–No DROP on VOICE Traffic

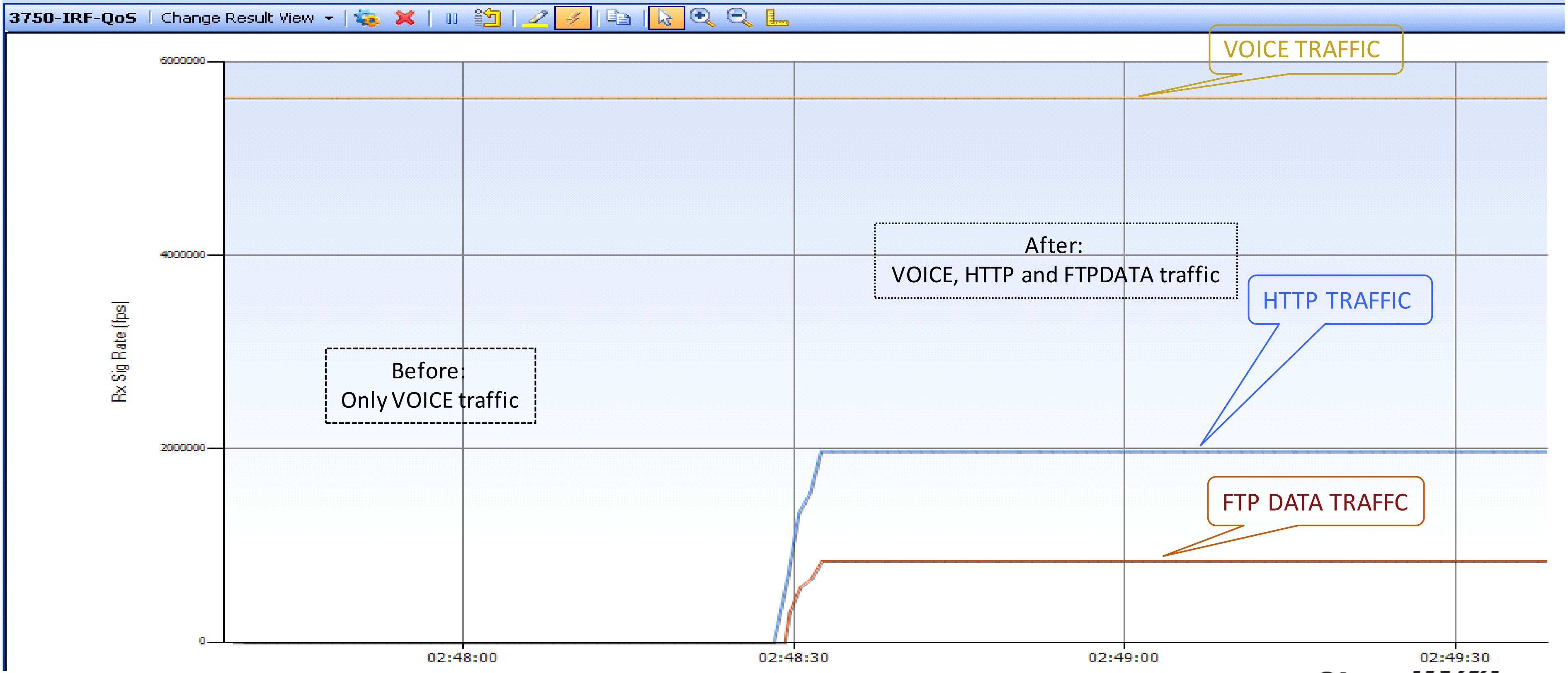


Before:
Only VOICE traffic

After:
VOICE, HTTP and FTPDATA traffic

QoS Test – Equivalent Cisco Switch

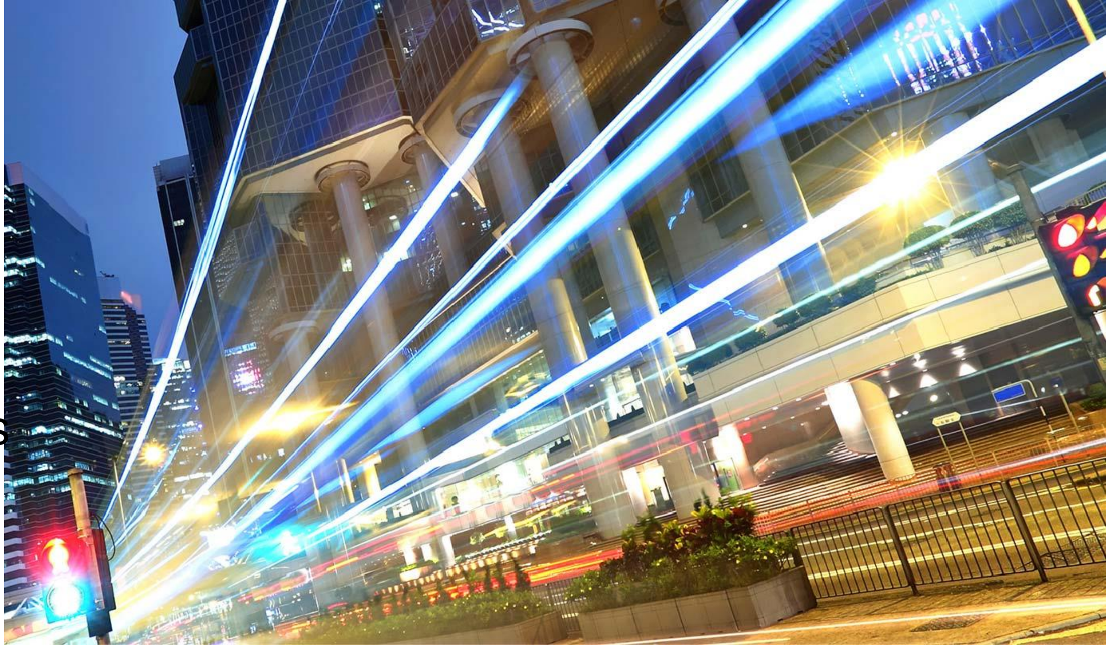
Scenario 3: across different units –No Drop on VOICE Traffic



Before:
Only VOICE traffic

After:
VOICE, HTTP and FTPDATA traffic

Agenda



- **Business and Technical Drivers**
- Components of QoS
- Design Considerations and Models
- Catalyst **QoS Design**
- Catalyst **AutoQoS**
- WAN and Branch QoS Design
- What about DC, SDN and other areas where QoS is important?

This Is What We Want To Get To…

Configuration

Classify the Traffic

```
class-map match-any VOICE_CLASS
  match  dscp ef
```

Apply a Policy to the Traffic

```
policy-map QOS_POLICY
  class VOICE_CLASS
     priority 1000
```

Apply the Policy

```
interface  GigabitEthernet0/0
   service-policy output  QOS_POLICY
```

Why Campus QoS Design is Important

Business and Technical Drivers

- New Applications and Business Requirements
  - –Explosion of Video Apps
  - –Impact of HD
  - –Blurring of Voice/Video/Data application boundaries
- Access to Standards and RFCs
  - –RFC 4594, FCoE
- New Platforms and Technologies
  - –New Switches, Routers, Supervisors, Linecards, Features, Syntax

- http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp60730

New Business Requirements

Cisco Visual Networking Index Findings

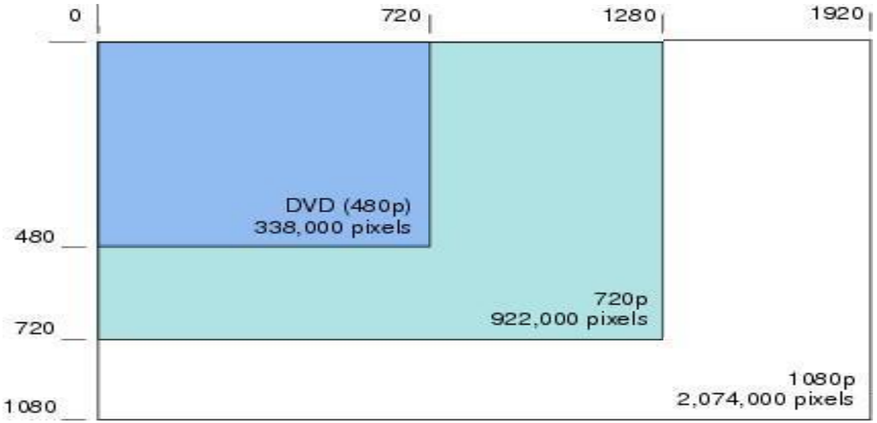
- Annual global IP traffic will surpass the zettabyte threshold (1.4 zetta bytes) by the end of 2017
- In 2017, the gigabyte equivalent of all movies ever made will cross global IP networks every 3 minutes.
- Every second, nearly a million minutes of video content will cross the network in 2017.
- The sum of all forms of video (TV, video on demand [VoD], Internet, and P2P) will be in the range of **80 to 90 percent** of global consumer traffic by 2017.
- Internet video to TV traffic will be 14 percent of consumer Internet video traffic in 2017

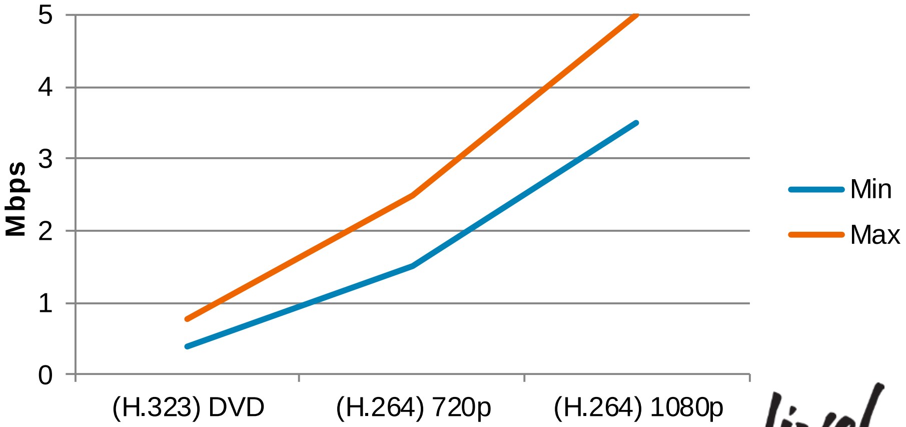
http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html

New Application Requirements

The Impact of HD on the Network

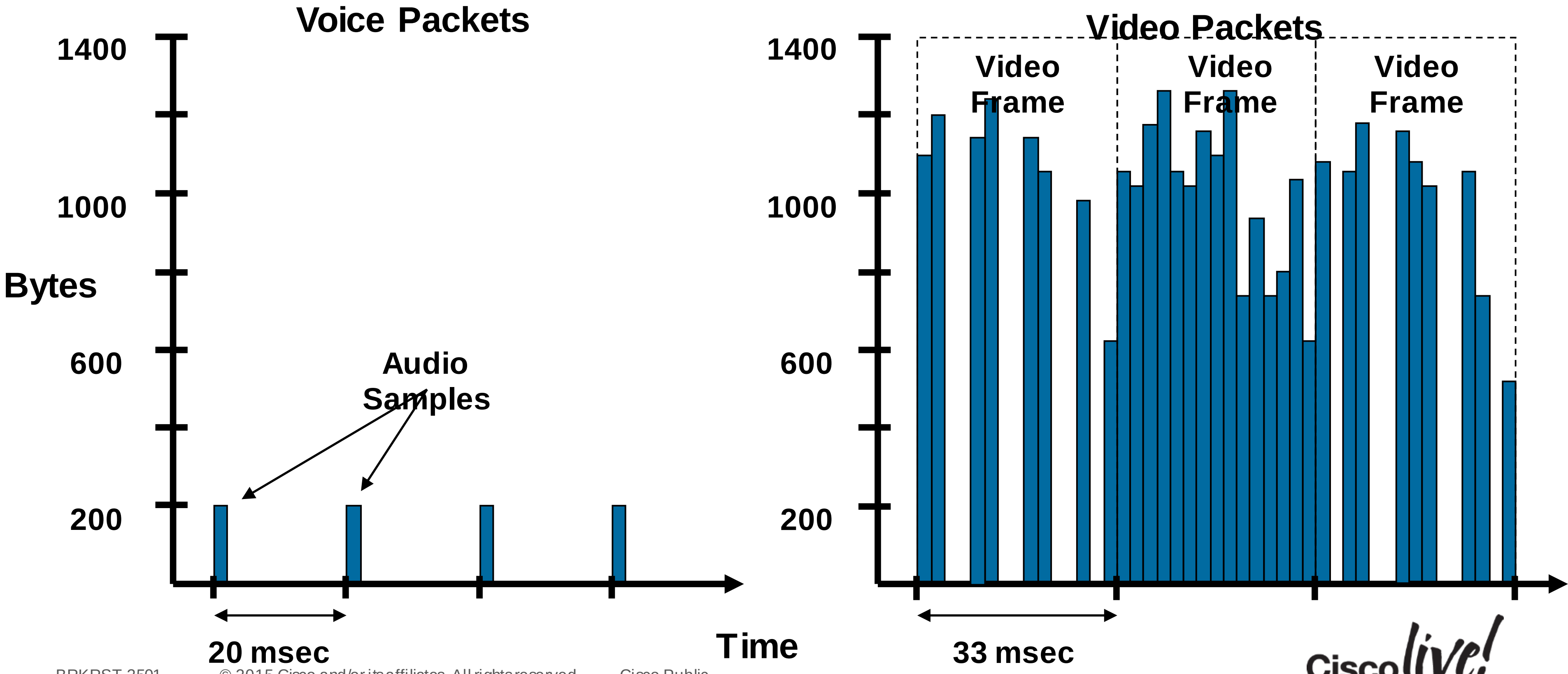
- User demand for HD video has a major impact on the network
  - –(H.264) 720p HD video requires twice as much bandwidth as (H.263) DVD
  - –(H.264) 1080p HD video requires twice as much bandwidth as (H.264) 720p
  - –Ultra HD 4320p video requires four times as much bandwidth as 1080p





New Applications Requirements

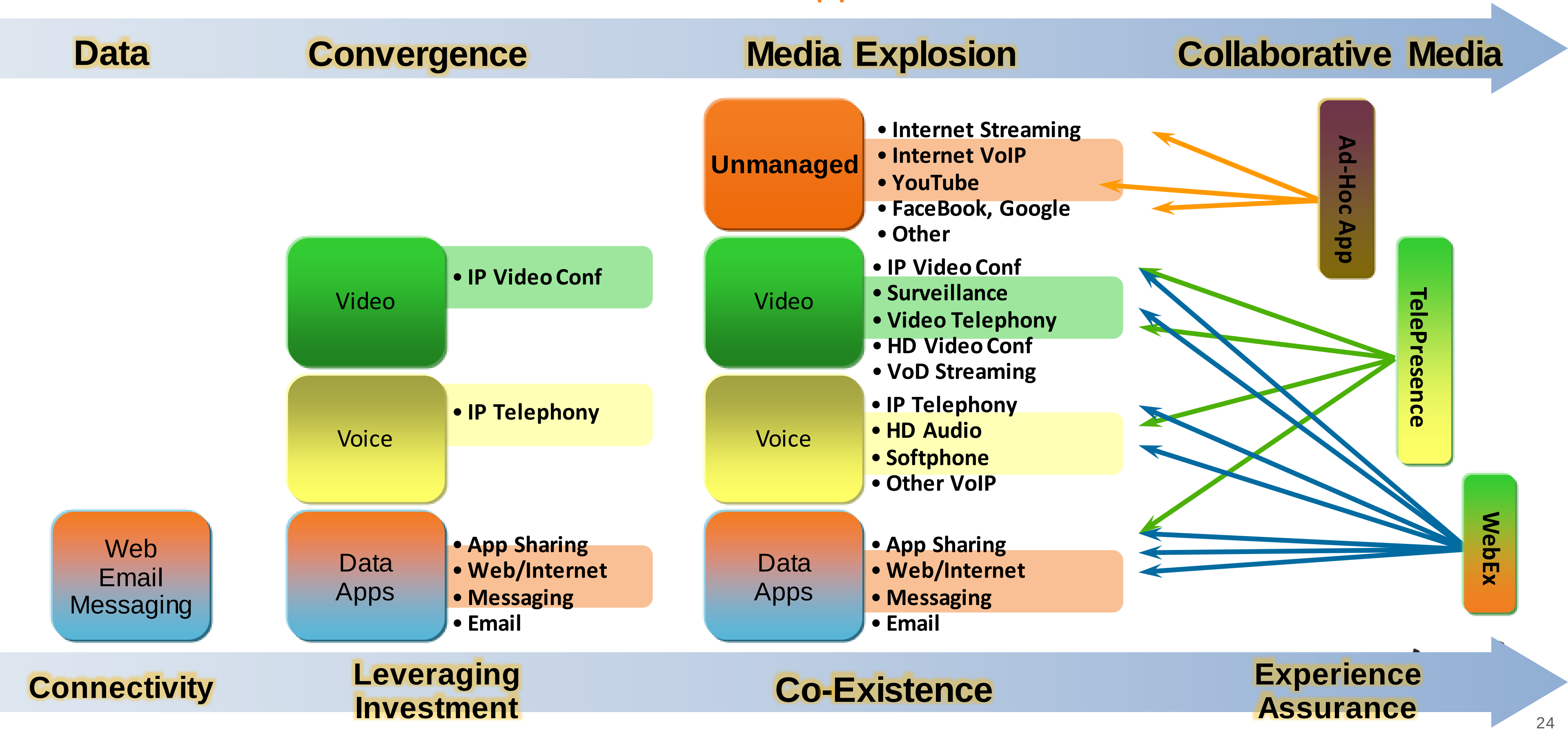
VoIP vs. HD Video—At the Packet Level



http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp60774

Medianet Application Evolution

Trends in Voice, Video and Data Media Applications



Data | Convergence | Media Explosion | Collaborative Media

Web
Email
Messaging

Video
- IP Video Conf

Voice
- IP Telephony

Data Apps
- App Sharing
- Web/Internet
- Messaging
- Email

Unmanaged
- Internet Streaming
- Internet VoIP
- YouTube
- FaceBook, Google
- Other

Video
- IP Video Conf
- Surveillance
- Video Telephony
- HD Video Conf
- VoD Streaming

Voice
- IP Telephony
- HD Audio
- Softphone
- Other VoIP

Data Apps
- App Sharing
- Web/Internet
- Messaging
- Email

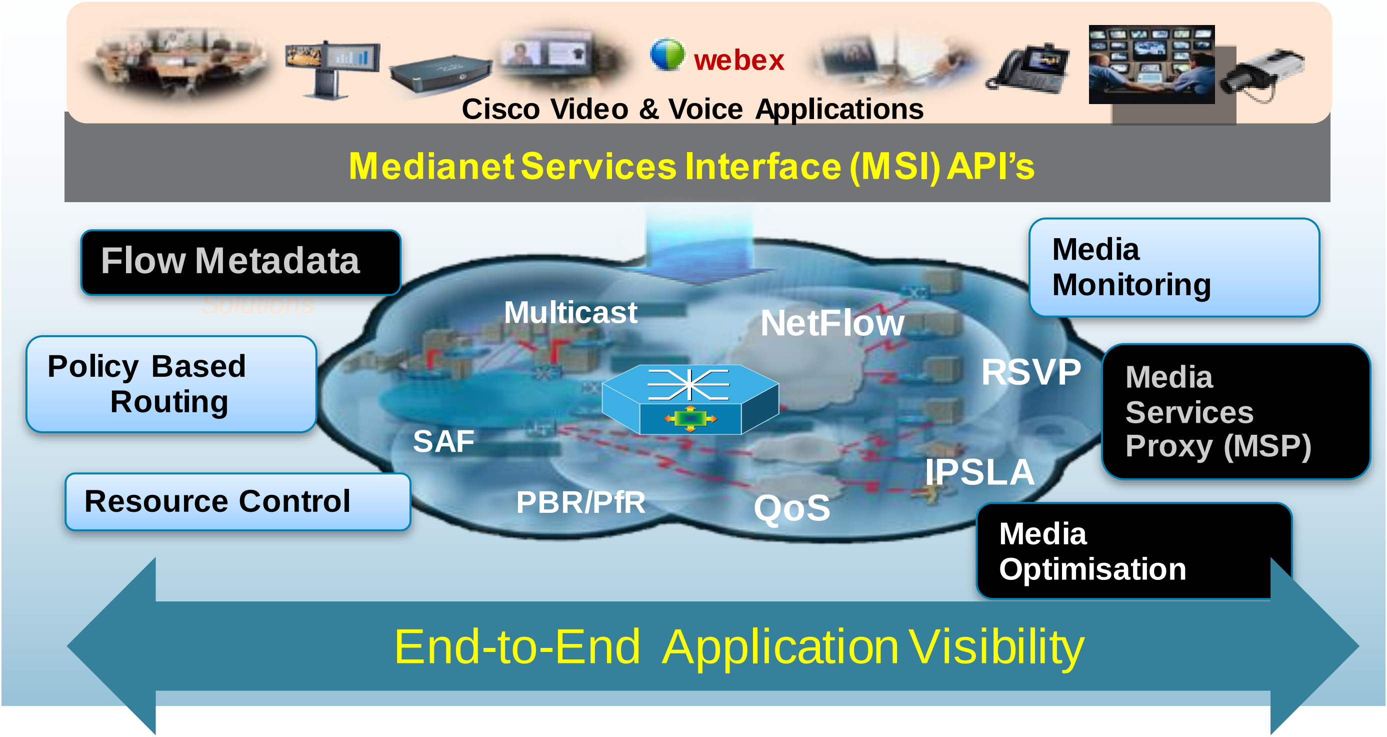
Ad-Hoc App

TelePresence

WebEx

Connectivity | Leveraging Investment | Co-Existence | Experience Assurance

Medianet Architecture

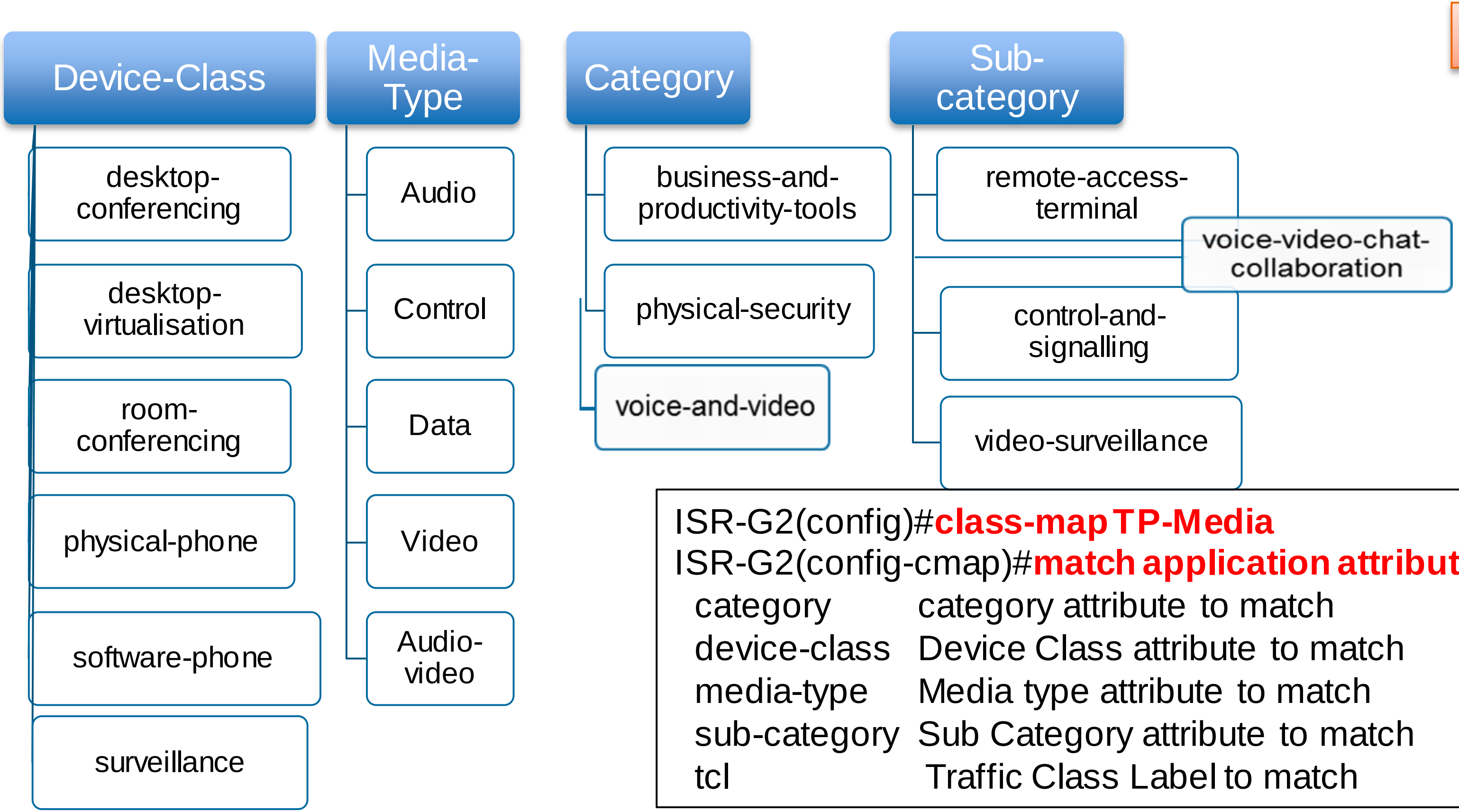


- Architectural play - Intelligent endpoints + intelligent network
- Core to Cisco's video strategy
- Multiple video & voice, business critical applications intelligently sharing the same IP Network
- Integration with key network services

Medianet is an end-to-end architecture which integrates various with Network Services and provides intelligence into the Network

Metadata Config's: Matching Application Attributes

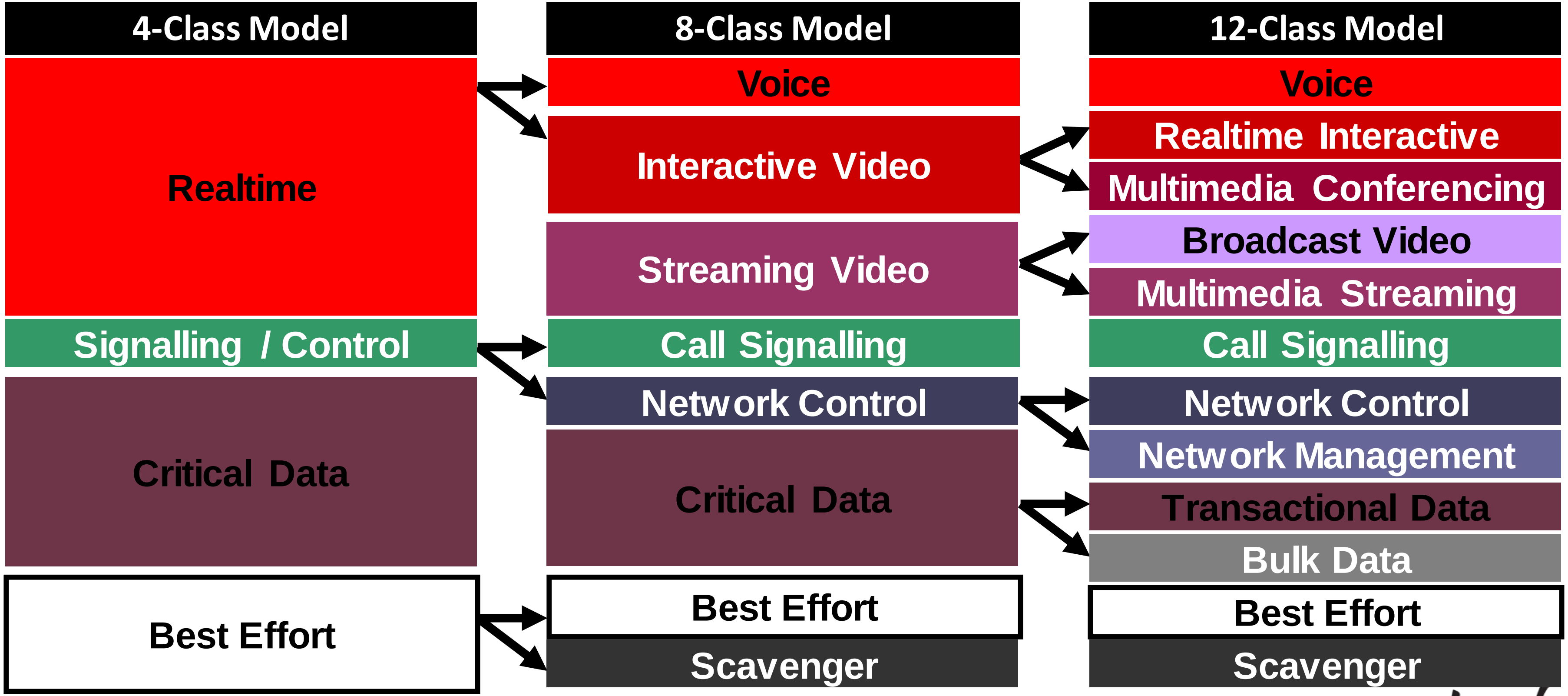
Configuration



```
ISR-G2(config)#class-map TP-Media
ISR-G2(config-cmap)#match application attribute ?
  category       category attribute to match
  device-class   Device Class attribute to match
  media-type     Media type attribute to match
  sub-category   Sub Category attribute to match
  tcl             Traffic Class Label to match
```

Evolving Business Requirements

Business Requirements Will Evolve and Expand over Time



4-Class Model

- Realtime
- Signalling / Control
- Critical Data
- Best Effort

8-Class Model

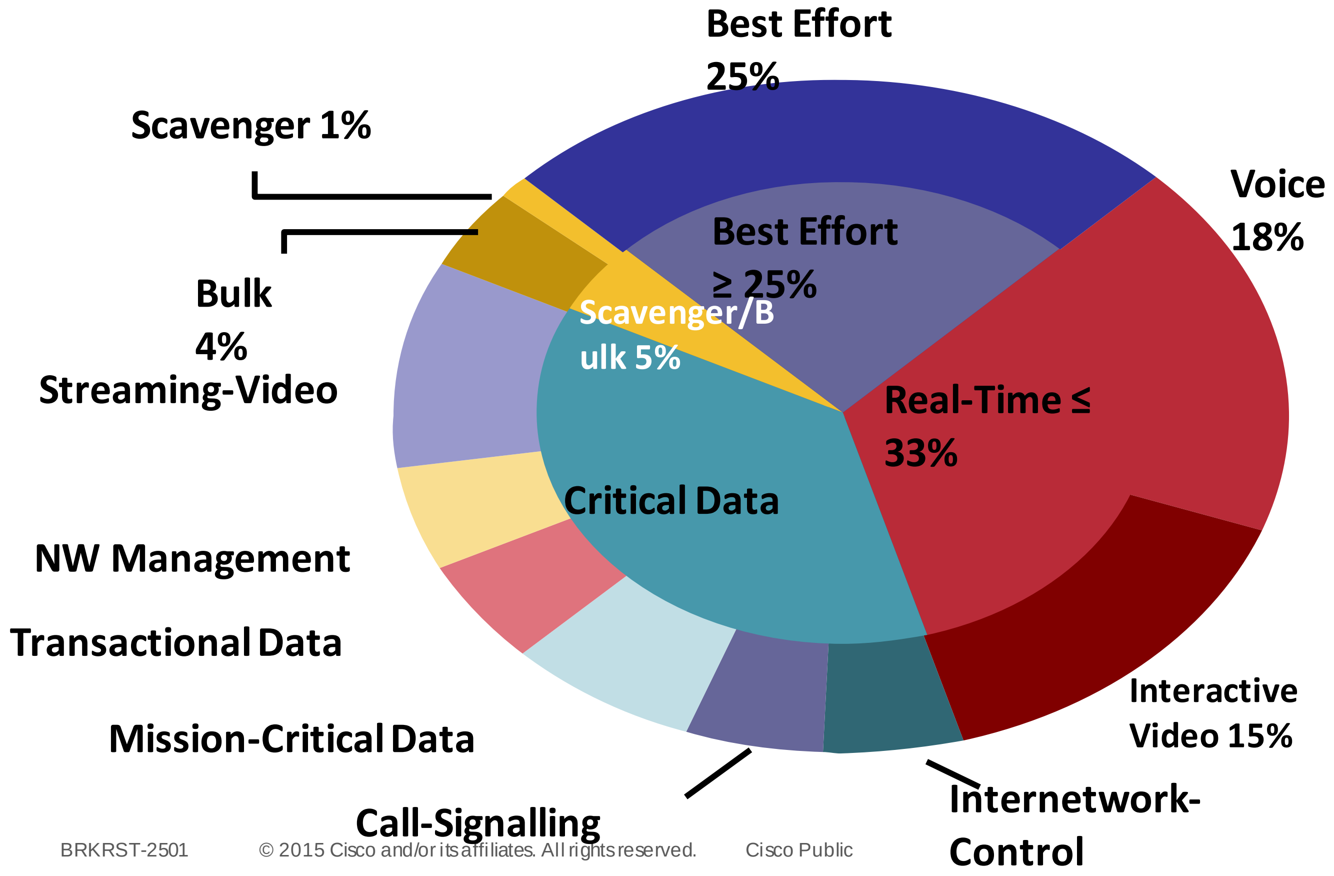
- Voice
- Interactive Video
- Streaming Video
- Call Signalling
- Network Control
- Critical Data
- Best Effort
- Scavenger

12-Class Model

- Voice
- Realtime Interactive
- Multimedia Conferencing
- Broadcast Video
- Multimedia Streaming
- Call Signalling
- Network Control
- Network Management
- Transactional Data
- Bulk Data
- Best Effort
- Scavenger

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp61135

Compatible Four-Class and Eleven-Class Queuing Models Following Realtime, Best Effort, and Scavenger Queuing Rules



Recommended Guidelines:

Best Effort (BE) Class - 25% minimum

Priority Queue (PQ) – given maximum of 33% for all LLQs

Scavenger - minimal bw allocation ~ 5% (RFC 3662) Less than best effort during congestion

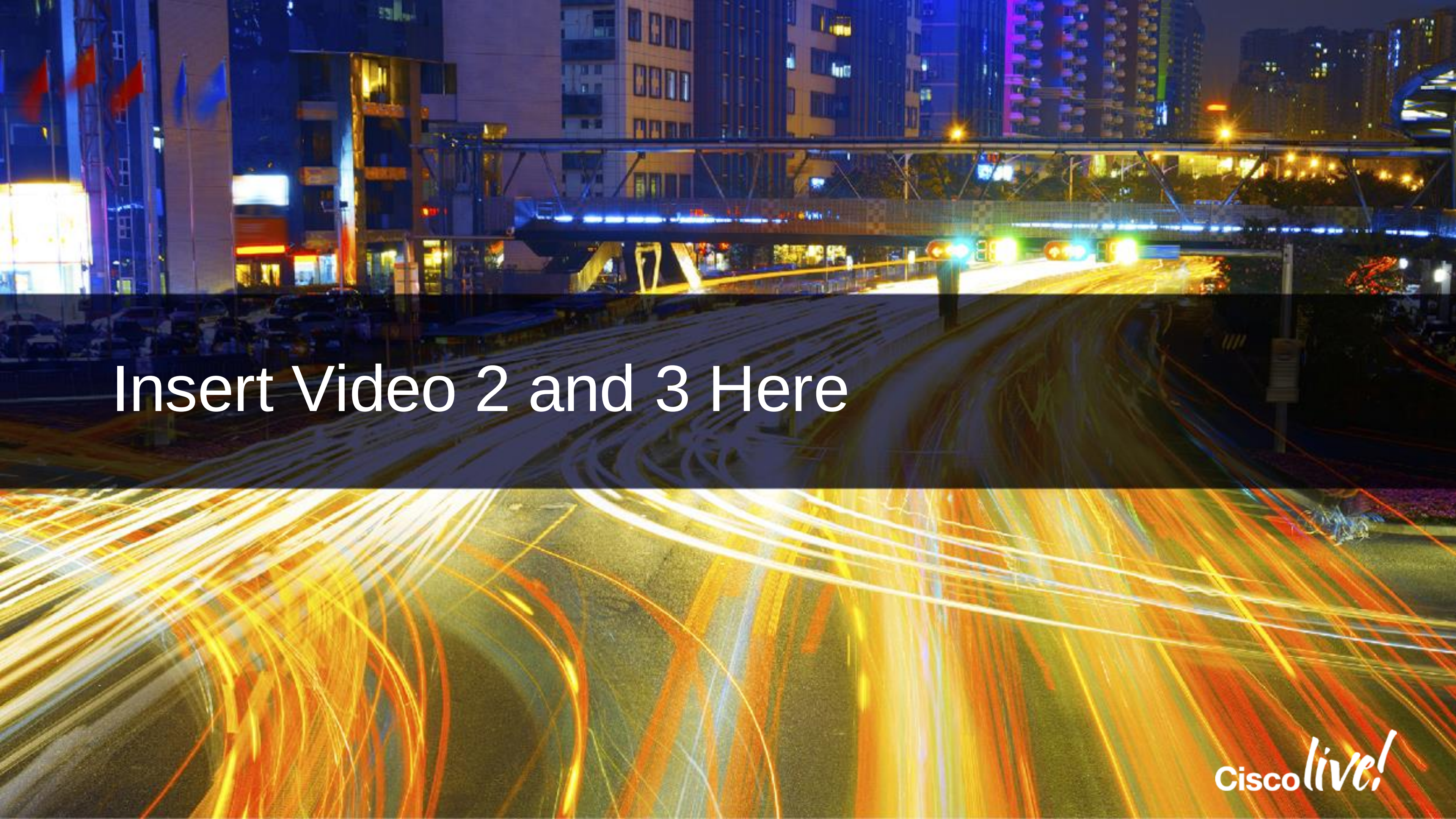
Congestion Avoidance should be enabled on select TCP flows (eg WRED, DBL)

Enterprise QoS

Agenda

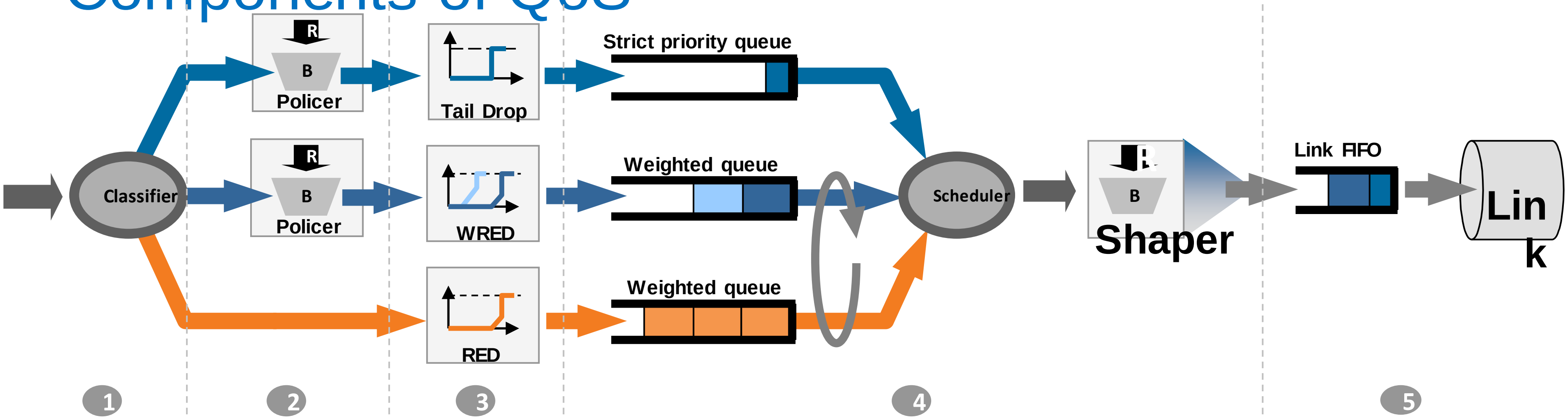
- Business and Technical Drivers for QoS Design Update
- Components of QoS
- Campus QoS Design Considerations and Models
- Catalyst QoS Design
- Catalyst AutoQoS
- WAN and Branch QoS Design
- What about DC, SDN and other areas where QoS is important?

Components of QoS



Insert Video 2 and 3 Here

Components of QoS

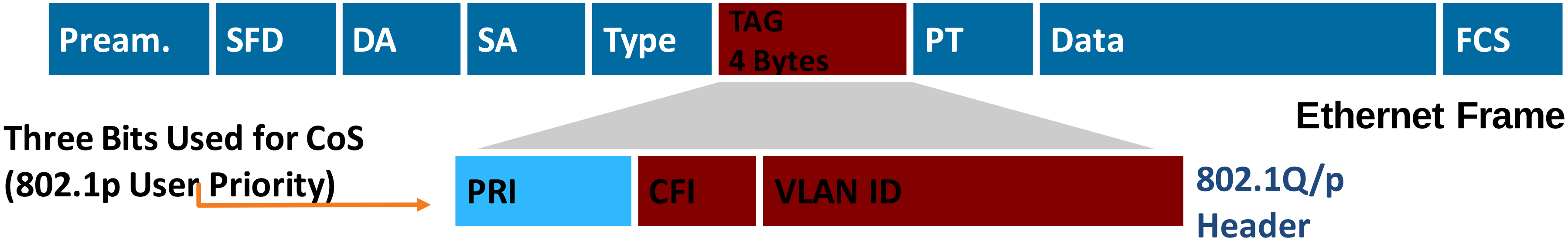


1. Classification and Marking - CoS, DSCP, Port Num, Packet Len, Protocol, VLAN etc
2. Admission Control - Local, Measurement and Resource Based (CAC and RSVP).
3. Policing - Pre Queuing includes Marking, Policing, Dropping (Tail Drop and WRED)
4. Queuing and Scheduling – Priority, Queue Length (Buffers)
5. Shaping – generally outbound, also sharing.
6. Post Queuing – Fragmenting, Interleaving, Compression

1. QoS Components - Classification

Layer 2- Ethernet 802.1Q Class of Service

DSCP is backward-compatible with IP precedence



Pream. | SFD | DA | SA | Type | TAG 4 Bytes | PT | Data | FCS

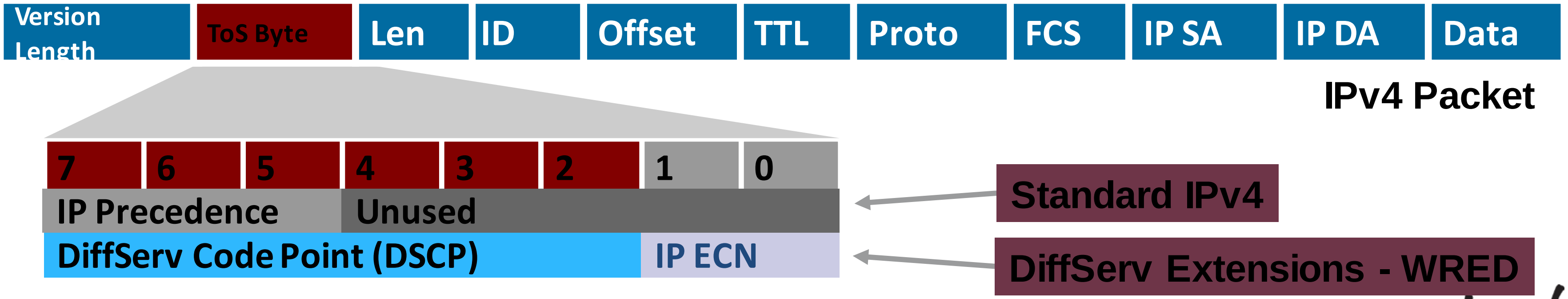
Ethernet Frame

Three Bits Used for CoS (802.1p User Priority)

PRI | CFI | VLAN ID

802.1Q/p Header

Layer 3- IP Precedence and DiffServ Code Points



Version Length | ToS Byte | Len | ID | Offset | TTL | Proto | FCS | IP SA | IP DA | Data

IPv4 Packet

7 | 6 | 5 | 4 | 3 | 2 | 1 | 0

IP Precedence | Unused

DiffServ Code Point (DSCP) | IP ECN

Standard IPv4

DiffServ Extensions - WRED

Standards and RFCs

Cisco DiffServ QoS Recommendations (RFC 4594-Based)

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

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp61104

QoS Components - Marking

Marking (a.k.a. colouring) is the process of setting the value of the DS field so that the traffic can easily be identified later, i.e. using simple classification techniques.

- **- Marking occurs at L3 or L2 e.g. 802.1D user priority field**

Traffic marking can be applied unconditionally, e.g. mark the DSCP to 34 for all traffic received on a particular interface, or as a conditional result of a policer

Conditional marking can be used to designate in- and out-of-contract traffic:

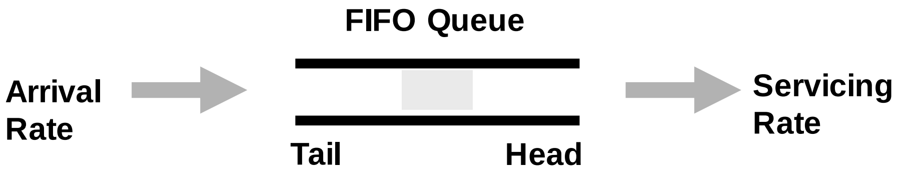
- Conform action is “mark one way”

- Exceed action is “mark another way”

Single Rate Policer has 2 states – conform or exceed.

Dual Rate Policer has 3 states – conform, exceed and violate

QoS Components - Buffers and Queues



Congestion can occur whenever there are speed mismatches (oversubscription)

When routers receive more packets than they can immediately forward, they momentarily store the packets in “buffers” (full buffers = packets dropped)

Difference between buffers and queues

- Buffers are physical memory locations where packets are temporarily stored whilst waiting to be transmitted

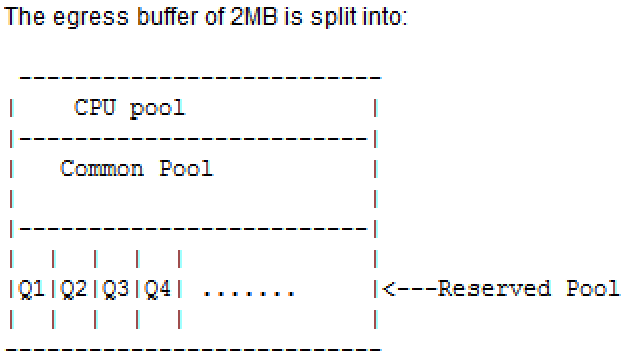
- Queues do not actually contain packets but consist of an ordered set of pointers to locations in buffer memory where packets in that particular queue are stored

- Buffer memory generally shared across different queues (so more Q’s is not necessarily better)

Routers generally use IOS-based software queuing

Catalyst switches generally use hardware queuing

QoS Components - Buffers and Queues 3750 Example



The egress buffer of 2MB is split into:

```
 ---------------------------
|    CPU pool              |
|--------------------------|
|   Common Pool            |
|                          |
|--------------------------|
|   |   |   |   |          |
|Q1 |Q2 |Q3 |Q4 | .......  |<---Reserved Pool
|   |   |   |   |          |
----------------------------
```

- The CPU and Common Pool are of fixed size.

- The Reserved Pool holds the minimum guaranteed buffer space reserved for each front-panel port and its respective queue.

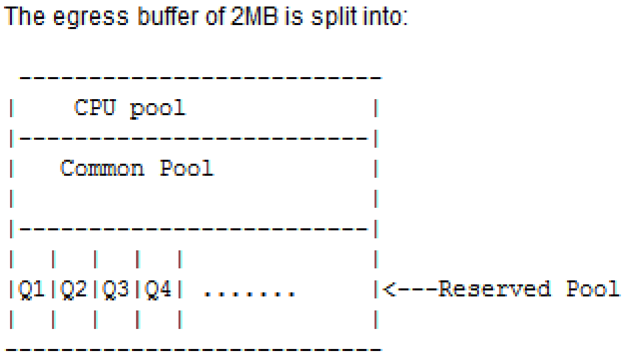
- The size of the reserved pool varies and depends on the default or user-configured settings on each of the ports (reserved-threshold).

- The common pool contains all the buffer units that are not initially reserved (minus the CPU buffer space).

http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/116102-qanda-egress-00.html

QoS Components - Buffers and Queues 3750 Example

```
Switch(config)#mls qos queue-set output 1 threshold 1 3200 3200 100 3200
```



The egress buffer of 2MB is split into:

```
  --------------------------
|    CPU pool              |
|--------------------------|
|   Common Pool            |
|                          |
|--------------------------|
|  |  |  |  |              |
|Q1|Q2|Q3|Q4|  .......     |<---Reserved Pool
|  |  |  |  |              |
 ---------------------------
```

- **3200** is the threshold percentage for WTD (Weighted Tail Drop). This number decides how many buffers to utilise from the common pool before the packets are tail dropped.

- The total available common pool for egress buffers varies from one platform to the other. They are more limited in 2960-S: 2MB for the whole system (downlink ports + uplink ports), while 3750-X has 2MB for each set of 24 downlink ports and 2MB for uplinks.

- 100 is the reserved percent of the buffers for that queue.

Dropping- Congestion Avoidance Algorithms

Queuing algorithms manage the front of the queue (Which packets get sent first)

Congestion avoidance algorithms manage the tail of the queue (Which packets get dropped first when queuing buffers fill)

Variants based on Tail Drop and RED (Random Early Discard) based on weight

Weighted Tail-drop and Weighted RED

WRED - Drops packets according to their DSCP markings

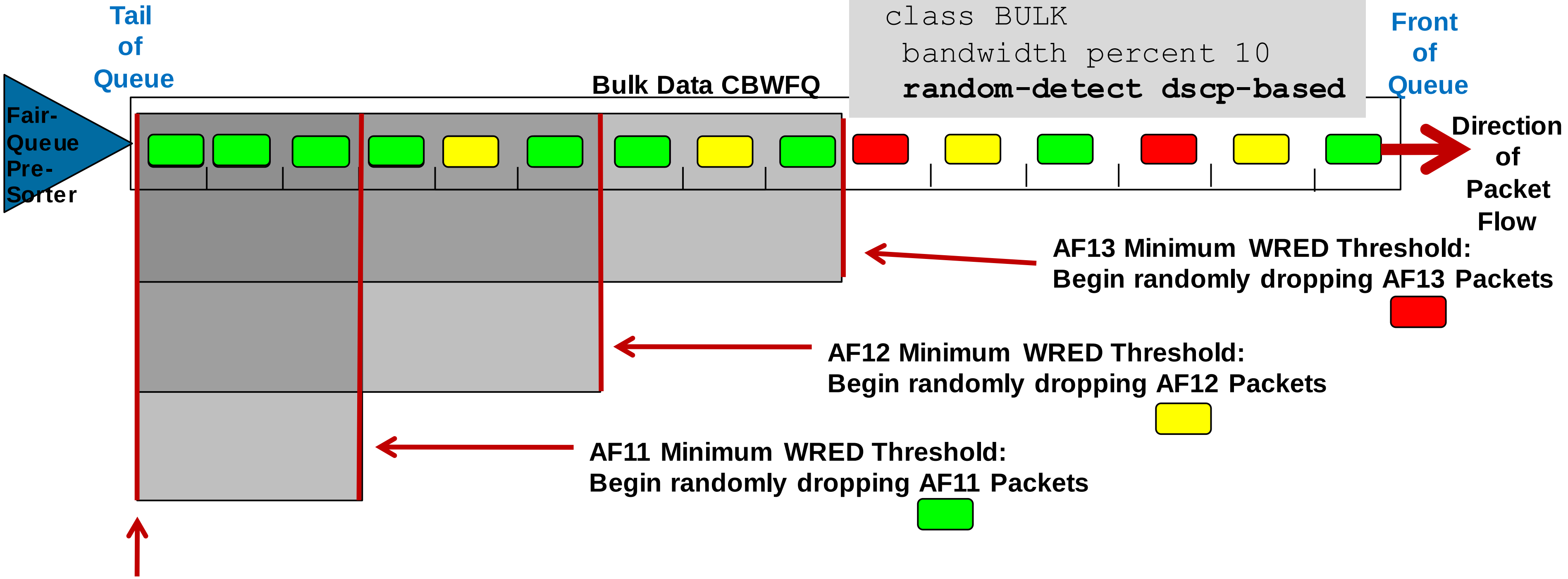
- WRED works best with TCP-based applications, like data

Congestion Avoidance helps prevent TCP Global Sync

QoS Components - Dropping

DSCP-Based WRED Operation

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



AF13 Minimum WRED Threshold: Begin randomly dropping AF13 Packets 🟥

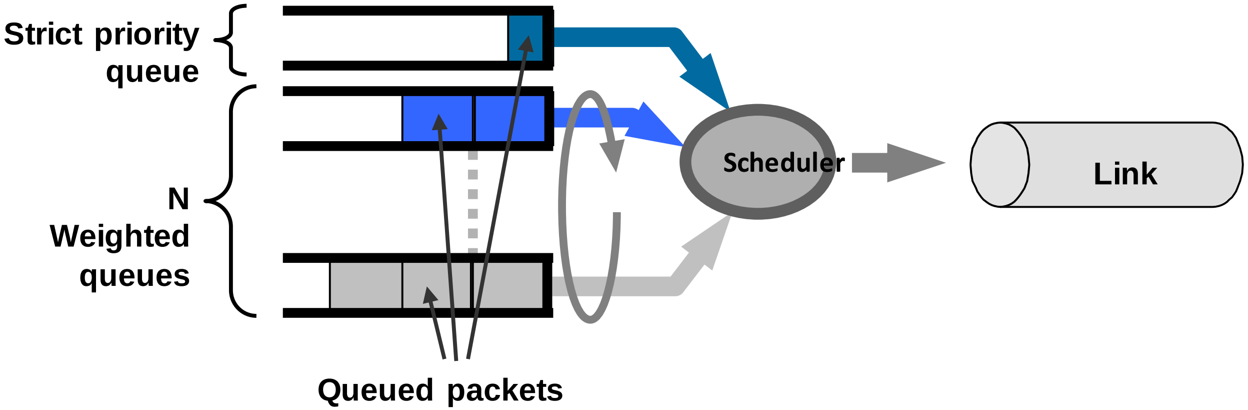
AF12 Minimum WRED Threshold: Begin randomly dropping AF12 Packets 🟨

AF11 Minimum WRED Threshold: Begin randomly dropping AF11 Packets 🟩

Maximum WRED Thresholds for AF11, AF12 and AF13 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

Queuing and Scheduling



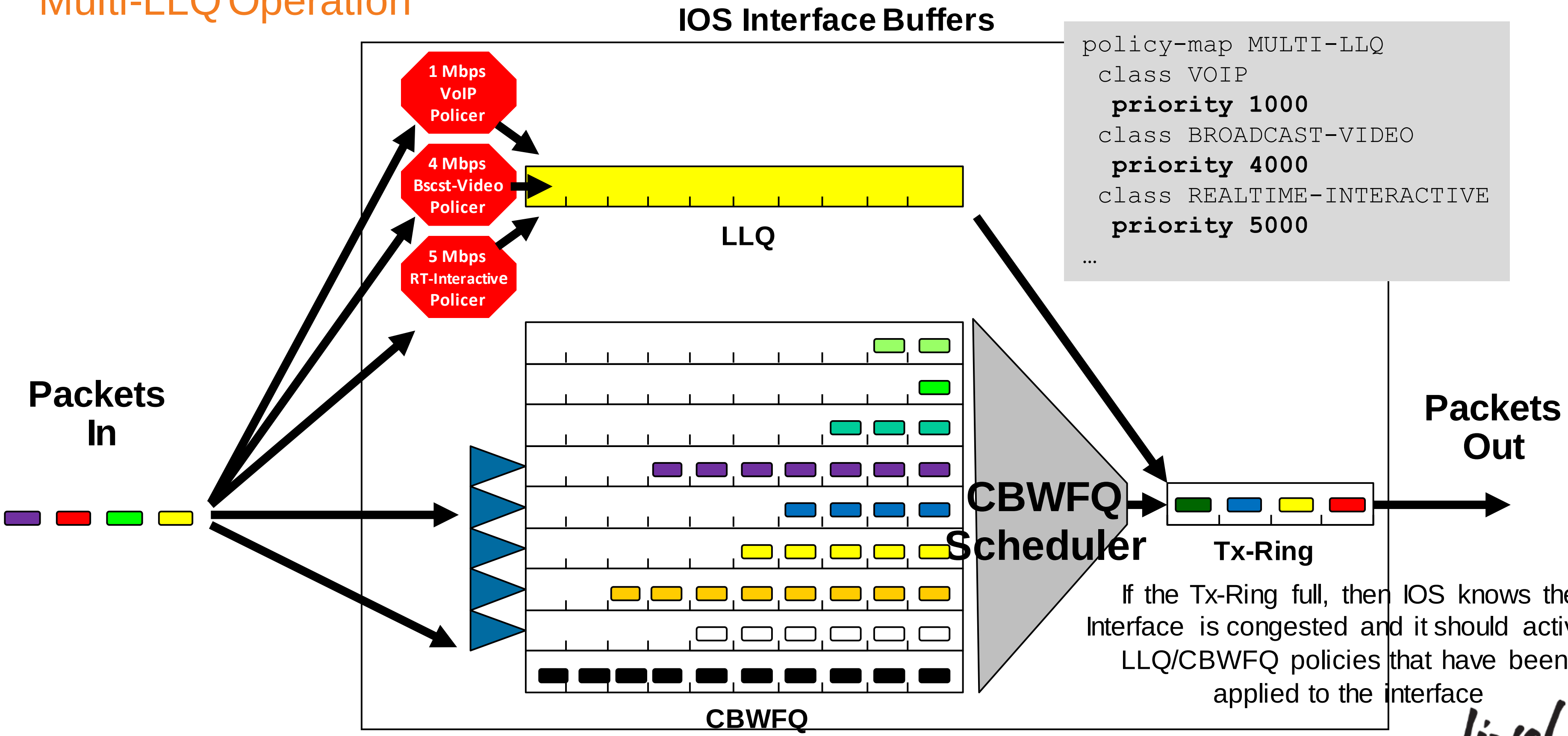
Schedulers determine which queue to service next - Different schedulers service queues in different orders

Most common types of schedulers :

- **FIFO** : is the most basic queuing type and is default when no QoS is enabled
- **Priority scheduling** – the queue is serviced if a packet is present
- **Weighted bandwidth scheduling**
- **Weighted Round Robin** (WRR), simple, each queue is weighted e.g. Custom Qing
- **Weighted Fair Queuing** e.g. (FB)WFQ, CBWFQ, LLQ (a.k.a. PQ-CBWFQ)

IOS QoS Mechanisms and Operation

Multi-LLQ Operation



```
policy-map MULTI-LLQ
 class VOIP
  priority 1000
 class BROADCAST-VIDEO
  priority 4000
 class REALTIME-INTERACTIVE
  priority 5000
…
```

If the Tx-Ring full, then IOS knows the Interface is congested and it should activate LLQ/CBWFQ policies that have been applied to the interface

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSWAN_40.html#wp129469

Policing vs. Shaping

- Policing typically drops out-of-contract traffic

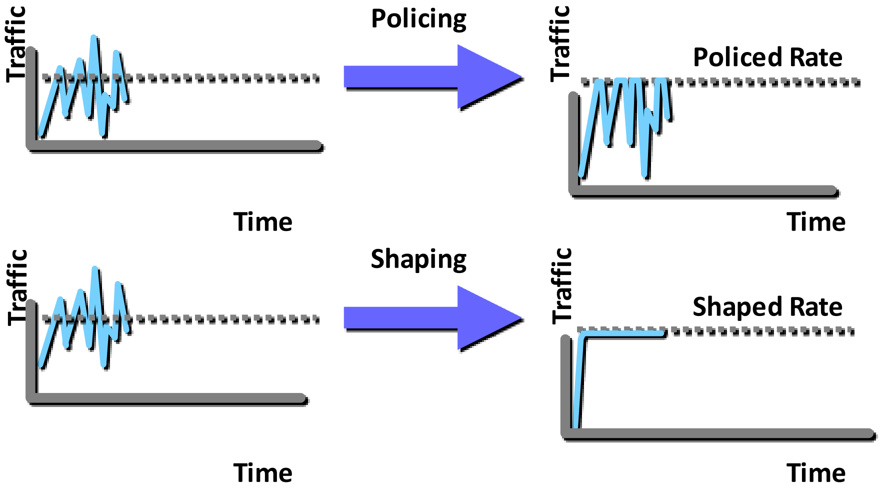
- Effectively policing acts to cut the peaks off bursty traffic

- Shaping typically delays out of contract traffic

- Shaping acts to smooth the traffic profile by delaying the peaks

- Resulting packet stream is “smoothed” and net throughput for TCP traffic is higher with shaping

- Shaping delay may have an impact on some services such as voip and video



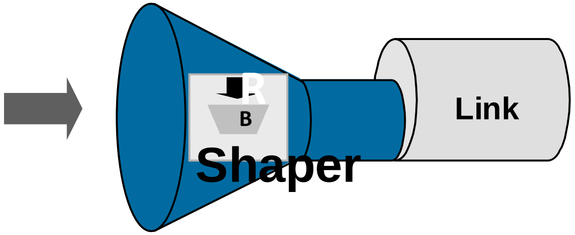
4. QoS Components - Shaping

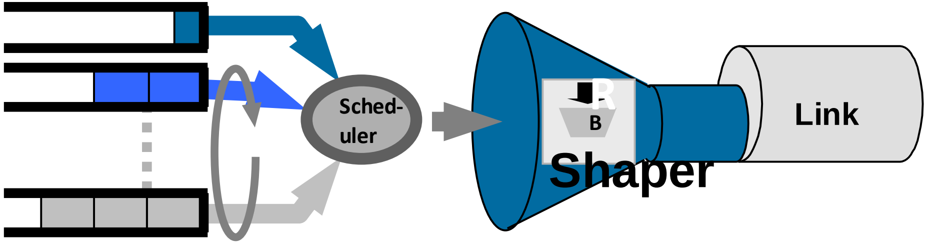
Shapers can be applied in a number of ways, e.g. :

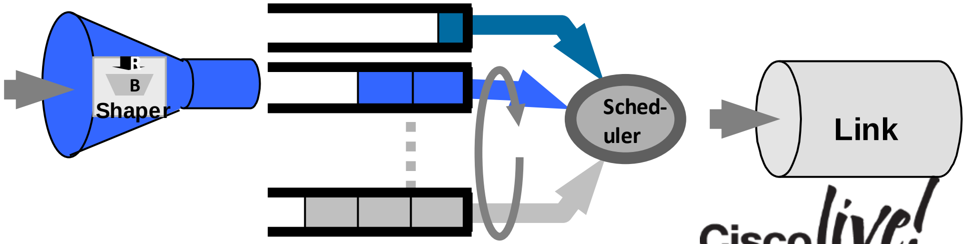
- To enforce a maximum rate across all traffic on a physical or logical interface

- To enforce a maximum rate across a number of traffic classes

- To enforce a maximum rate to an individual traffic class
- Hierarchical QoS







Enterprise QoS

Agenda

- Business and Technical Drivers for QoS Design Update
- Components of QoS
- Campus QoS Design Considerations and Models
- Catalyst QoS Design
- Catalyst AutoQoS
- WAN and Branch QoS Design
- What about DC, SDN and other areas where QoS is important?

Campus QoS Design – Considerations and Models

Campus Network Design

Infrastructure Services Required of the Campus

High Availability

- Implement strategy for sub-second failover
- Implement HA architecture with **NSF/SSO**, **VSS**, vPC etc.

Latency and Bandwidth Optimisation

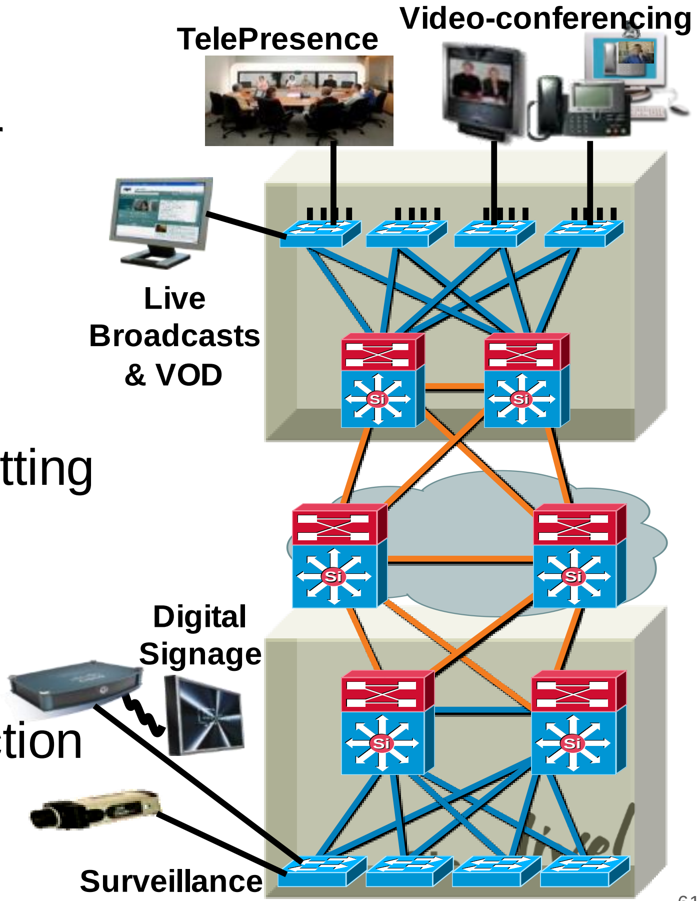
- **GigE** access
- **10GigE** distribution/core
- Implement **IP multicast** and/or stream splitting services

Confidentiality

- Authentication of endpoints and users (e.g. **802.1x**)

-Comply to security policies with data protection strategies,

-such as encryption (e.g. Cisco TrustSec)



Campus Network Design

Infrastructure Services Required of the Campus

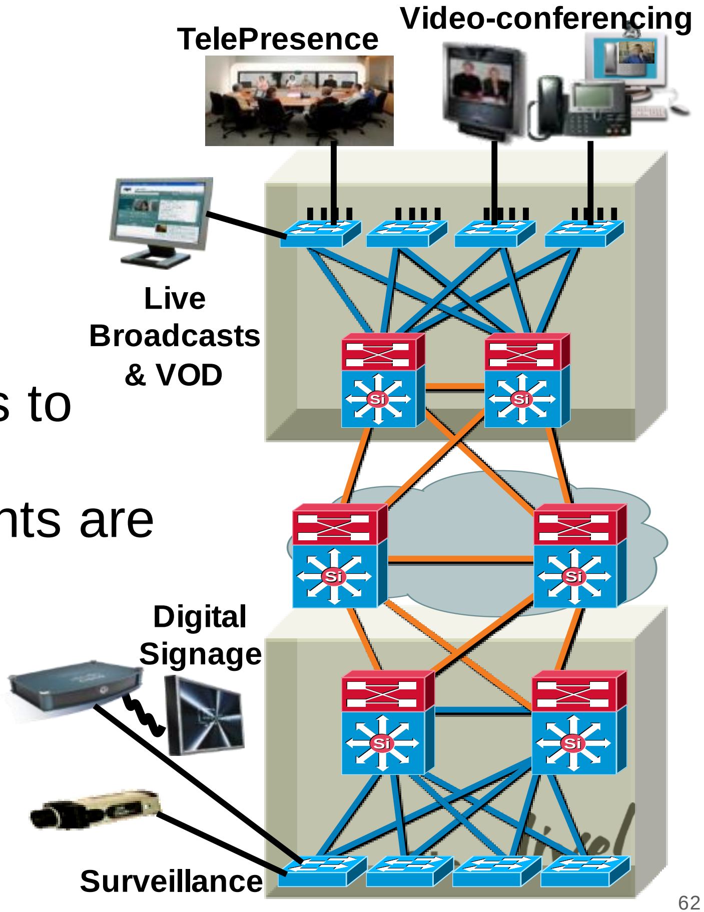
-Network Virtualisation

-Implement **VRF-Lite** (or other) Path Isolation for sensitive traffic

-video application segregation

Real-Time Application Delivery

- Implement granular **QoS** service policies to manage application service levels
- Access layer protection, ensures endpoints are fair consumers



Campus QoS Design

Strategic QoS Design Principles

- Always perform QoS in hardware rather than software when a choice exists (eg in Switches)
- Classify and mark applications as close to their sources as technically and administratively feasible
- Police unwanted traffic flows as close to their sources as possible (waste of resource)
- Enable queuing policies at every node where the potential for congestion exists (control Loss!)
- Have a QoS Policy Defined for your business

- http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1098008

Campus QoS Design

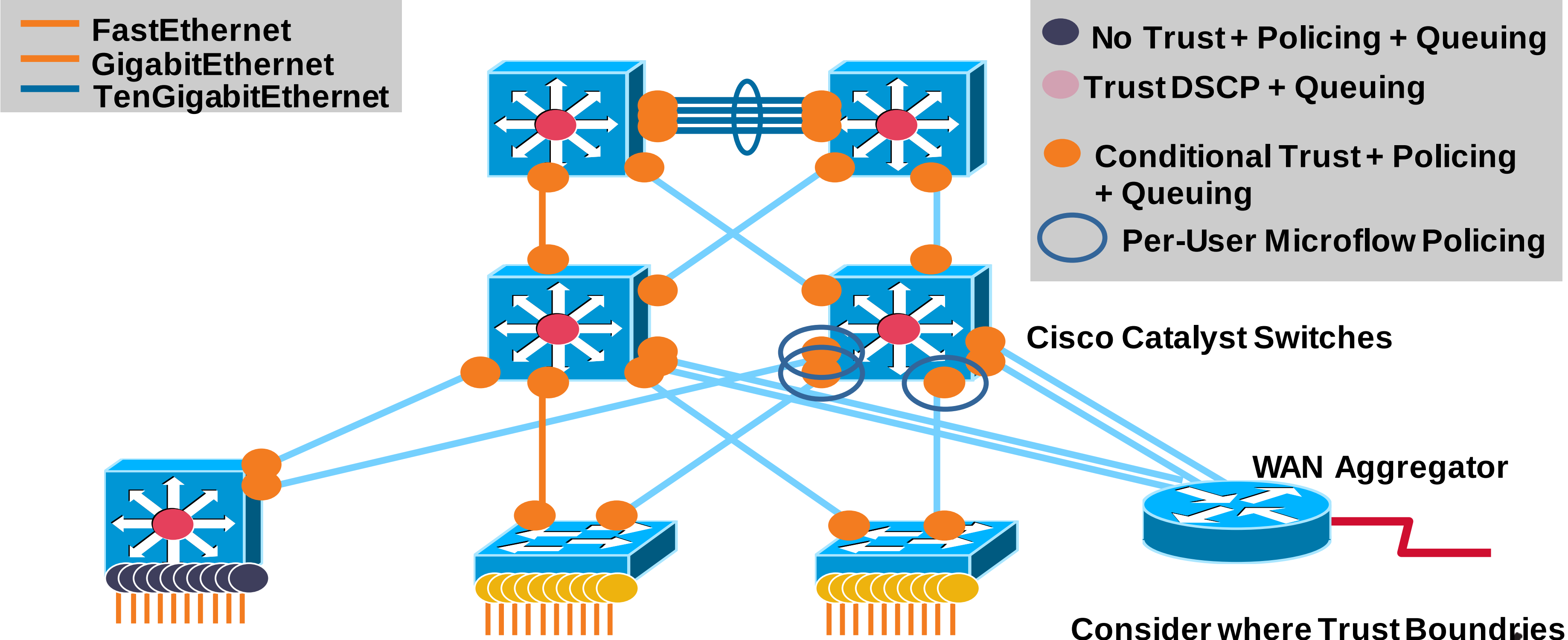
QoS Design Considerations

- Where is QoS Applied
- Internal DSCP
- Trust States and Operations
- Trust Boundaries
- Endpoint-Generated Traffic Classes
- AutoQoS

- http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1098008

Campus QoS Considerations

Where Is QoS Required Within the Campus?



— FastEthernet
— GigabitEthernet
— TenGigabitEthernet

● No Trust + Policing + Queuing
● Trust DSCP + Queuing
● Conditional Trust + Policing + Queuing
○ Per-User Microflow Policing

Cisco Catalyst Switches

WAN Aggregator

Server Farms

IP Phones + PCs

IP Phones + PCs

Consider where Trust Boundries might be extended to.

Campus QoS Design Considerations

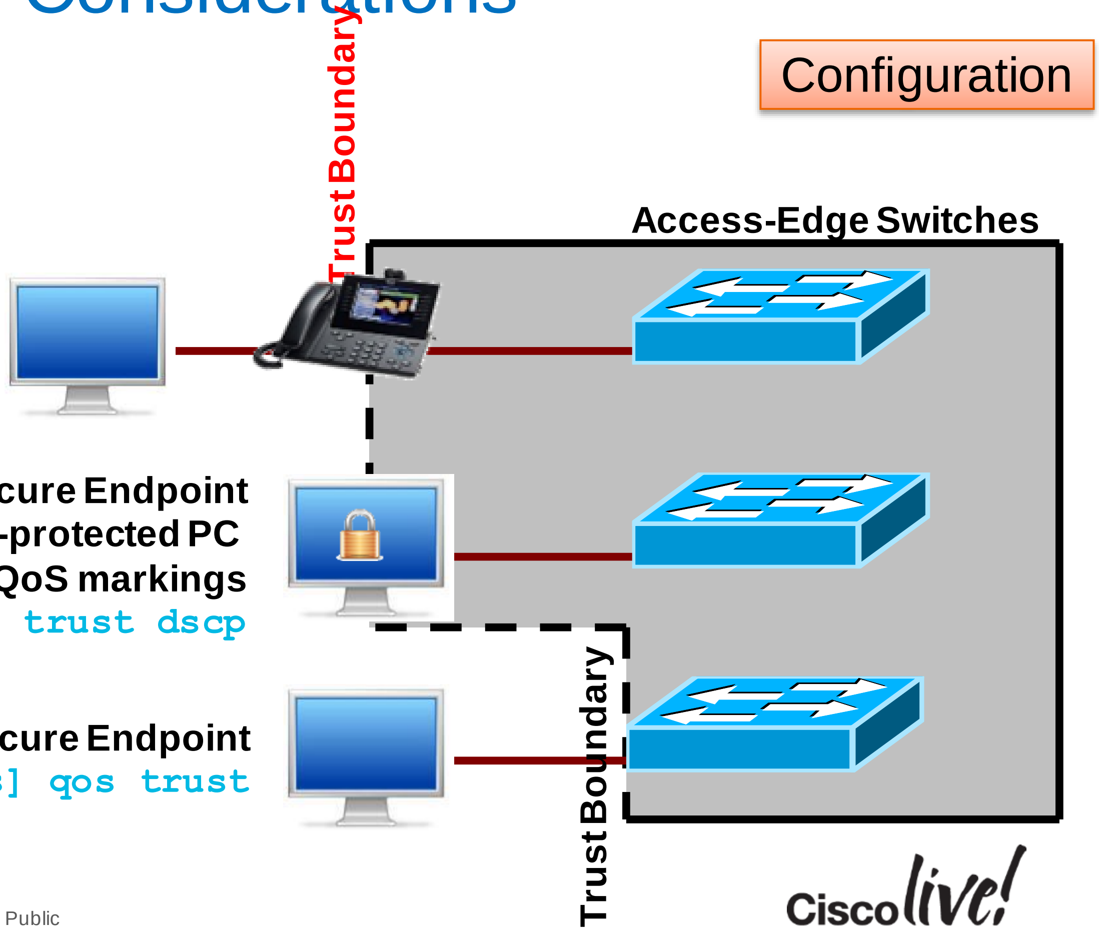
Trust Boundaries

Configuration

Conditionally Trusted Endpoints
Example: IP Phone + PC
`[mls] qos trust device cisco-phone`

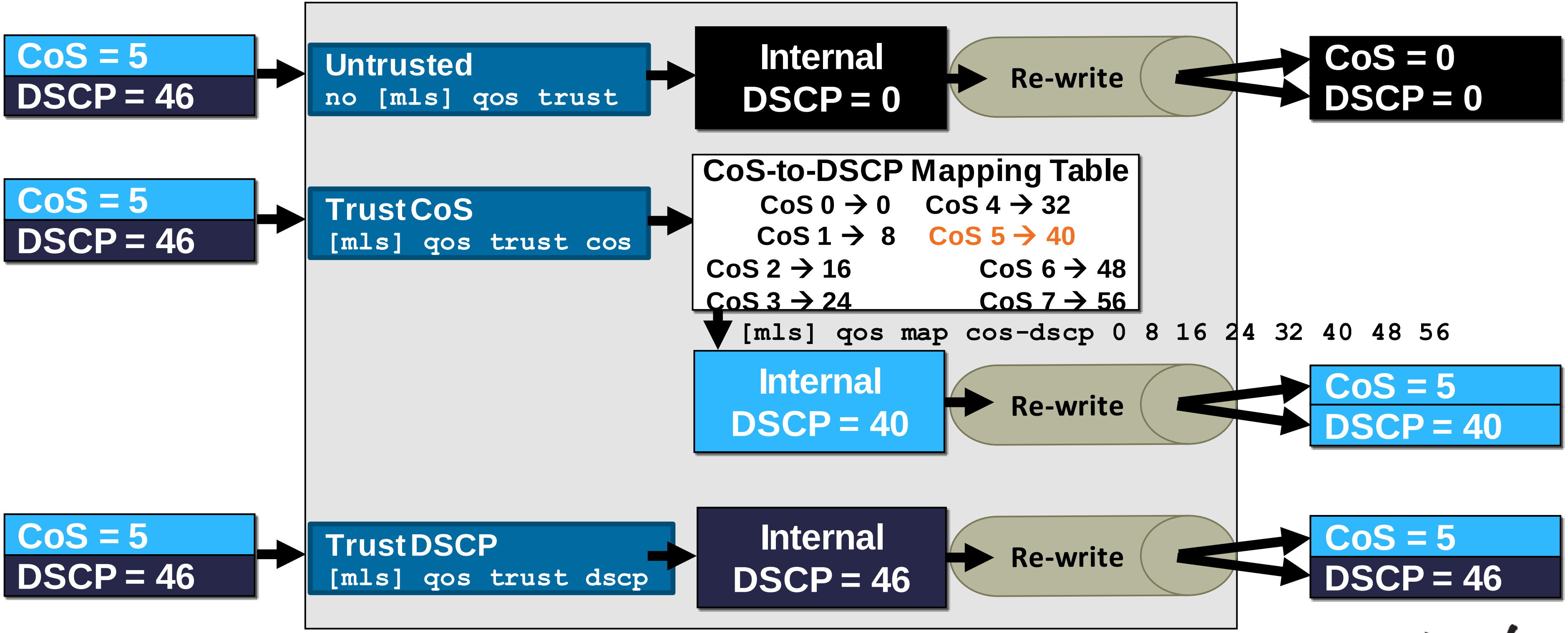
Secure Endpoint
Example: Software-protected PC
With centrally-administered QoS markings
`[mls] qos trust dscp`

Unsecure Endpoint
`no [mls] qos trust`



Campus QoS Design Considerations

Internal DSCP Derivation by Trust Options



CoS = 5
DSCP = 46

Untrusted

```
no [mls] qos trust
```

Internal
DSCP = 0

Re-write

CoS = 0
DSCP = 0

CoS = 5
DSCP = 46

Trust CoS

```
[mls] qos trust cos
```

CoS-to-DSCP Mapping Table

CoS 0 → 0	CoS 4 → 32
CoS 1 → 8	CoS 5 → 40
CoS 2 → 16	CoS 6 → 48
CoS 3 → 24	CoS 7 → 56

```
[mls] qos map cos-dscp 0 8 16 24 32 40 48 56
```

Internal
DSCP = 40

Re-write

CoS = 5
DSCP = 40

CoS = 5
DSCP = 46

Trust DSCP

```
[mls] qos trust dscp
```

Internal
DSCP = 46

Re-write

CoS = 5
DSCP = 46

Campus Egress QoS Models

Queuing and Dropping and Buffer-Sizing Recommendations

Catalyst Queuing is done in hardware and varies by platform/linecard and is expressed as: 1P*x*Q*y*T

- Example: 1P3Q8T means: 1 PQ
- 3 non-priority queues, each with
- 8 drop-thresholds per queue

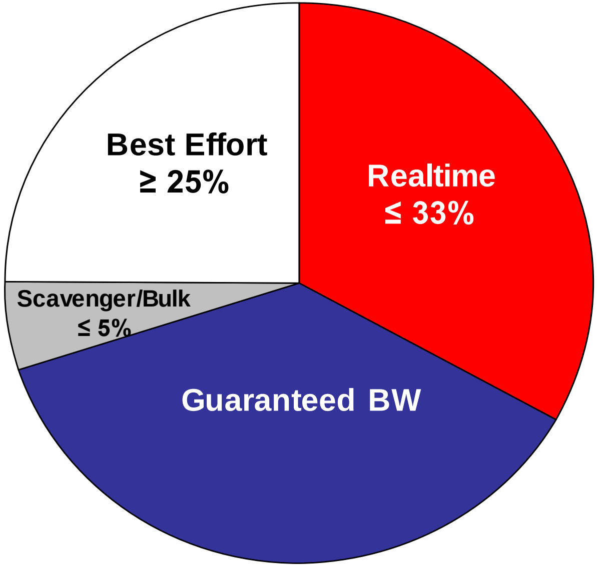
Minimum queuing capabilities for medianet is 1P3QyT

Realtime (PQ) should be less than 33% of link

Best-Effort Queue should be guaranteed at 25% of link

Scavenger/Bulk queue should be minimally provisioned

WRED is preferred congestion-avoidance mechanism



Buffers for BE and Guaranteed BW queues can be *directly* proportional to BW allocation

- Example: 25% BW for BE Queue can be matched with 25% Buffer Allocation

Buffers for PQ and Scavenger/Bulk Queue can be indirectly proportional to BW allocation

- Examples: 30% BW for PQ can be complemented with 15% Buffer Allocation
- 5% BW for Scavenger/Bulk queue can be complemented with 10%+ Buffer Allocation

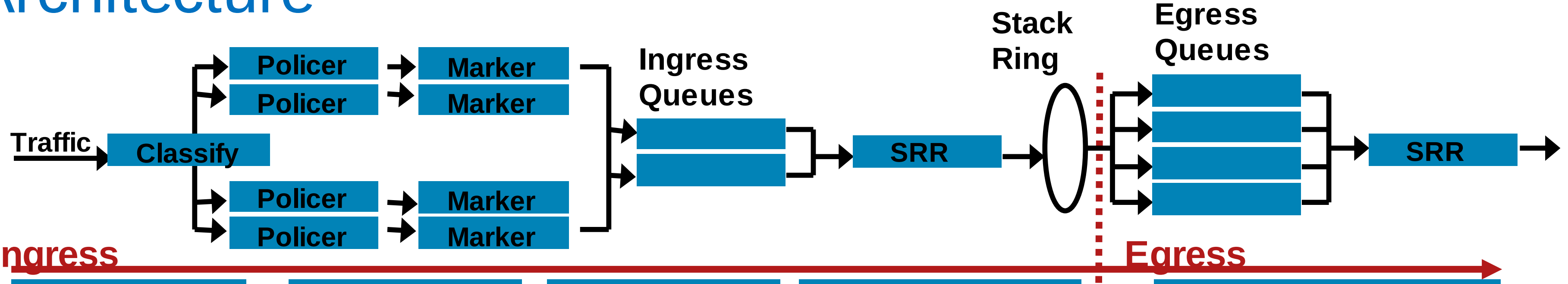
Enterprise QoS

Agenda

- Business and Technical Drivers for QoS Design Update
- Components of QoS
- Campus QoS Design Considerations and Models
- Catalyst QoS Design
- Catalyst AutoQoS
- WAN and Branch QoS Design
- What about DC, SDN and other areas where QoS is important?

Catalyst 2960/3560/3750G/E/X QoS Design

Catalyst 2960/3560/3750 G/E/X QoS Design - QoS Architecture



Classification

- Inspect incoming packets
- Based on ACLs or configuration, determine classification label

Policing

- Ensure conformance to a specified rate
- On an aggregate or individual flow basis
- Up to 256 policers per Port ASIC
- Support for rate and burst

Marking

- Act on policer decision
- Reclass or drop out-of-profile

Ingress Queue/ Schedule Congestion Control

- Two queues/port ASIC shared servicing
- One queue is configurable for strict priority servicing
- WTD for congestion control (three thresholds per queue)
- SRR is performed

Egress Queue/ Schedule Congestion Control

- Four SRR queues/port shared or shaped servicing
- One queue is configurable for strict priority servicing
- WTD for congestion control (three thresholds per queue)
- Egress queue shaping
- Egress port rate limiting

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1098508

Catalyst 2960/3560/3750 G/E/X QoS Design

Platform-Specific Considerations

- Traffic is classified on ingress, based on trust-states, access-lists, or class-maps.
- Because the total inbound bandwidth of all ports can exceed the bandwidth of the stack or internal ring, ingress queues are supported
- The Catalyst 2960 can police to a minimum rate of 1 Mbps; all other platforms within this switch product family can police to a minimum rate of 8 kbps.
- The Catalyst 3560 and 3750 support multilayer switching and as such correspondingly support per-VLAN or per-port/per-VLAN policies.
- The Catalyst 3560 and 3750 support IPv6 QoS.
- The Catalyst 3560 and 3750 support policing on 10 Gigabit Ethernet interfaces.
- The Catalyst 2960/2975/3650/3750 support Shaped Round Robin (BW limits), Shared Round Robin (shares unused BW), as well as strict priority queue scheduling
- The Catalyst 3560-E/X and 3750-E/X support SRR shaping weights on 10 GE ints

Catalyst 2960/3560/3750 Campus QoS Design

- QoS Design Steps

1. Enable QoS

2. Configure Ingress QoS Model(s):

   ❑ Trust Models
   ❑ Conditional Trust Model
   ❑ Service Policy Models

3. Configure Ingress Queuing

4. Configure Egress Queuing

Catalyst 2960/3560/3750 Campus QoS Design

- Enabling QoS and Trust Model Examples

Configuration

Enabling QoS (not enabled by default):

```
mls qos
```

```
These commands are global
```

Trust-CoS Model Example:

```
mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

```
mls qos trust cos
```

```
These commands are interface specific
```

Trust-DSCP Model Example:

```
mls qos trust dscp
```

Conditional-Trust Model Example:

```
mls qos trust device cisco-phone          [or]
mls qos trust device cts                  [or]
mls qos trust device ip-camera            [or]
mls qos trust device media-player
```

Verified with:

- `show mls qos`
- `show mls qos interface`
- `show mls qos map cos-dscp`

Catalyst 2960/3560/3750 Campus QoS Design

Configuration

- Conditional Trust to a Cisco IP Phone Example

Conditional Trust Policy to a Cisco IP Phone:

```
mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

```
These commands are global
```

```
mls qos trust device cisco-phone
mls qos trust cos
```

```
These commands are interface specific
```

Catalyst 2960/3560/3750 G/E/X QoS Design

Marking Model Example

Configuration

```
C3750-X(config-cmap)# policy-map MARKING

C3750-X(config-pmap)# class VVLAN-VOIP
C3750-X(config-pmap-c)# set dscp ef ! VoIP is marked EF

C3750-X(config-pmap-c)# class VVLAN-SIGNALING
C3750-X(config-pmap-c)#  set dscp cs3 ! Signaling (from the VVLAN) is marked CS3


C3750-X(config-pmap-c)# class BULK-DATA
C3750-X(config-pmap-c)#  set dscp af11 ! Bulk Data is marked AF11


C3750-X(config-pmap-c)# class DEFAULT
C3750-X(config-pmap-c)#  set dscp default ! An explicit class-default must be used to mark all
other IP traffic to 0 otherwise it will not be enforced.
```

Catalyst 2960/3560/3750 G/E/X QoS Design

Marking and Policing Model Example

```
mls qos map policed-dscp 0 10 18 to 8          ! Remarking DSCP is done with a global command. If these DSCP values
exceed the policers in the configuration below, they are remarked to 8

C3750-X(config-cmap)# policy-map MARKING-and-POLICING

C3750-X(config-pmap)# class VVLAN-VOIP
C3750-X(config-pmap-c)# set dscp ef ! VoIP is marked EF
C3750-X(config-pmap-c)# police 128k 8000 exceed-action drop   ! Exceeding traffic is policed

C3750-X(config-pmap-c)# class VVLAN-SIGNALING
C3750-X(config-pmap-c)#  set dscp cs3 ! Signaling (from the VVLAN) is marked CS3
C3750-X(config-pmap-c)#  police 32k 8000 exceed-action drop

C3750-X(config-pmap-c)# class SIGNALING
C3750-X(config-pmap-c)#  set dscp cs3 ! Signaling (from the DVLAN) is marked CS3
C3750-X(config-pmap-c)#  police 32k 8000 exceed-action drop

C3750-X(config-pmap-c)# class TRANSACTIONAL-DATA
C3750-X(config-pmap-c)#  set dscp af21 ! Transactional Data is marked AF21
C3750-X(config-pmap-c)#  police 10m 8000 exceed-action policed-dscp-transmit

C3750-X(config-pmap-c)# class BULK-DATA
C3750-X(config-pmap-c)#  set dscp af11 ! Bulk Data is marked AF11
C3750-X(config-pmap-c)#  police 10m 8000 exceed-action policed-dscp-transmit

C3750-X(config-pmap-c)# class SCAVENGER
C3750-X(config-pmap-c)#  set dscp cs1 ! Scavenger traffic is marked CS1

C3750-X(config-pmap-c)# class DEFAULT
C3750-X(config-pmap-c)#  set dscp default ! An explicit class-default marks all other IP traffic to 0
```

Catalyst 2960/2975/3560/3750 G/E/X QoS Design

Marking Model Example: Per-Port Application

```
C3750-X(config)#interface range GigabitEthernet 1/0/1-48
C3750-X(config-if-range)# switchport access vlan 10
C3750-X(config-if-range)# switchport voice vlan 110
C3750-X(config-if-range)# spanning-tree portfast

C3750-X(config-if-range)# mls qos trust device cisco-phone
! The interface is set to conditionally-trust Cisco IP Phones

C3750-X(config-if-range)# mls qos trust cos
! CoS-trust will be dynamically extended to Cisco IP Phones

C3750-X(config-if-range)# service-policy input MARKING-and-POLICING
! Attaches the Per-Port Marking policy to the interface(s)
```

Verified with:

- `show mls qos interface`
- `show class-map`
- `show policy-map`
- `show policy-map interface`

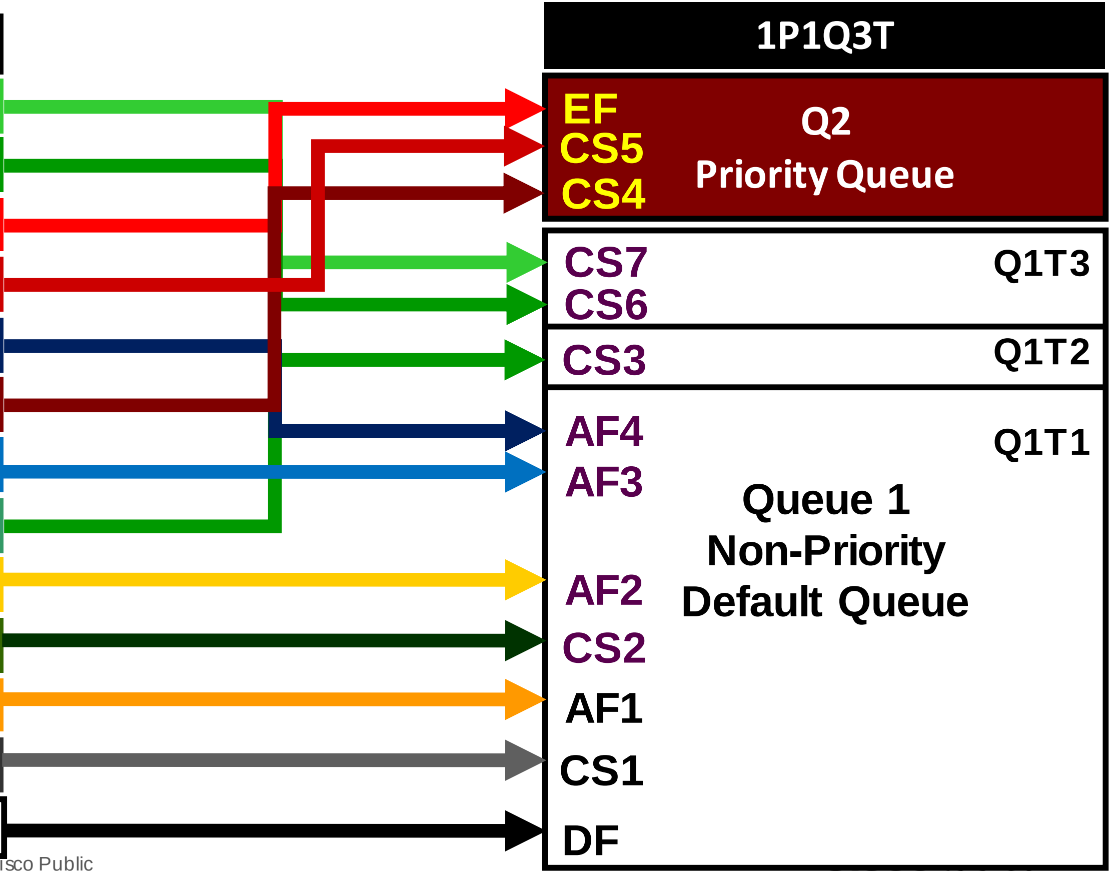
Note: While the Catalyst 3750-E MQC syntax includes an implicit class-default, any policy actions assigned to this class are not enforced. Therefore, an explicit class DEFAULT is configured in the above example to enforce a marking/remarking policy to DSCP 0 for all other IP traffic.

Note: An explicit marking command (**set dscp**) is used even for trusted application classes (like VVLAN-VOIP and VVLAN-SIGNALING) rather than a **trust** policy-map action. The use of an explicit (but seemingly redundant) explicit marking command actually improves the policy efficiency from a hardware perspective.

Catalyst 2960/2975/3560/3750 G/E/X QoS Design

1P1Q3T Ingress Queuing Model

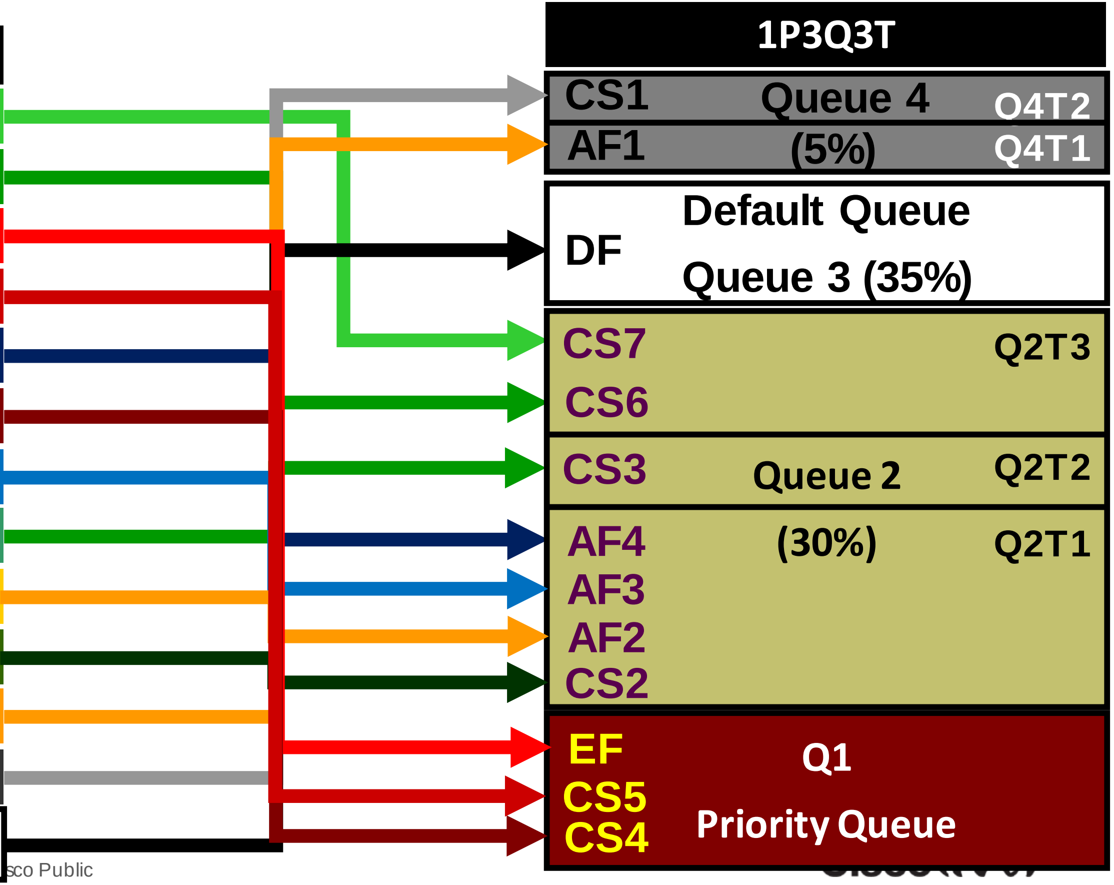
Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signalling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF



Catalyst 2960/2975/3560/3750 G/E/X QoS Design

1P3Q3T Egress Queuing Model

Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signalling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF



1P3Q3T

CS1 Queue 4 Q4T2

AF1 (5%) Q4T1

DF Default Queue

Queue 3 (35%)

CS7 Q2T3

CS6

CS3 Queue 2 Q2T2

AF4 (30%) Q2T1

AF3

AF2

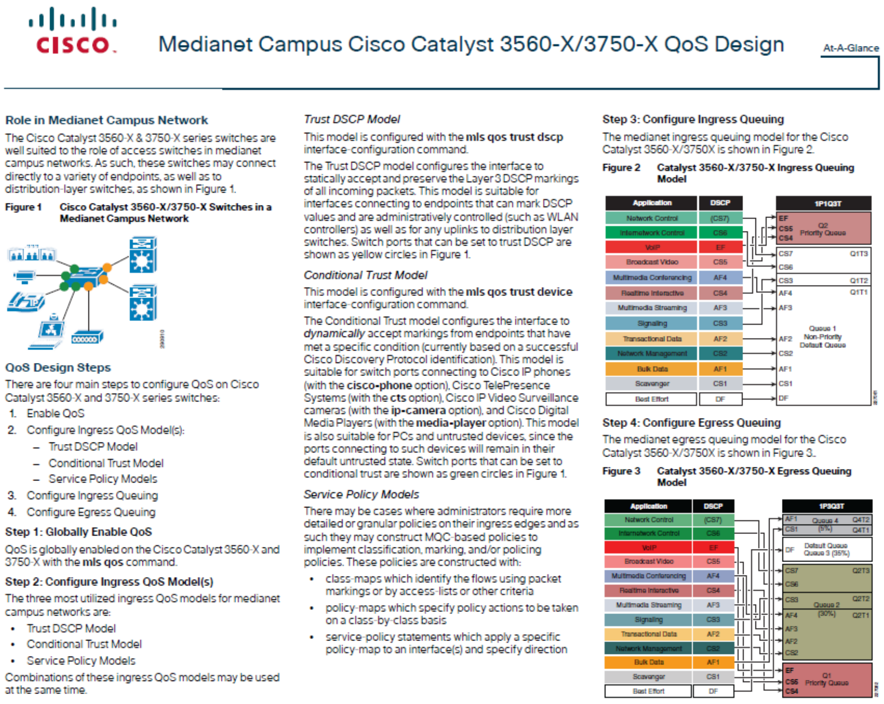
CS2

EF Q1

CS5 Priority Queue

CS4

Catalyst 2960/3560/3750 QoS Design—At-A-Glance



Medianet Campus Cisco Catalyst 3560-X/3750-X QoS Design

At-A-Glance

Role in Medianet Campus Network

The Cisco Catalyst 3560-X & 3750-X series switches are well suited to the role of access switches in medianet campus networks. As such, these switches may connect directly to a variety of endpoints, as well as to distribution-layer switches, as shown in Figure 1.

Figure 1 Cisco Catalyst 3560-X/3750-X Switches in a Medianet Campus Network

QoS Design Steps

There are four main steps to configure QoS on Cisco Catalyst 3560-X and 3750-X series switches:

1. Enable QoS
2. Configure Ingress QoS Model(s):
   - Trust DSCP Model
   - Conditional Trust Model
   - Service Policy Models
3. Configure Ingress Queuing
4. Configure Egress Queuing

Step 1: Globally Enable QoS

QoS is globally enabled on the Cisco Catalyst 3560-X and 3750-X with the **mls qos** command.

Step 2: Configure Ingress QoS Model(s)

The three most utilized ingress QoS models for medianet campus networks are:

- Trust DSCP Model
- Conditional Trust Model
- Service Policy Models

Combinations of these ingress QoS models may be used at the same time.

Trust DSCP Model

This model is configured with the **mls qos trust dscp** interface-configuration command.

The Trust DSCP model configures the interface to statically accept and preserve the Layer 3 DSCP markings of all incoming packets. This model is suitable for interfaces connecting to endpoints that can mark DSCP values and are administratively controlled (such as WLAN controllers) as well as for any uplinks to distribution layer switches. Switch ports that can be set to trust DSCP are shown as yellow circles in Figure 1.

Conditional Trust Model

This model is configured with the **mls qos trust device** interface-configuration command.

The Conditional Trust model configures the interface to *dynamically* accept markings from endpoints that have met a specific condition (currently based on a successful Cisco Discovery Protocol identification). This model is suitable for switch ports connecting to Cisco IP phones (with the **cisco-phone** option), Cisco TelePresence Systems (with the **cts** option), Cisco IP Video Surveillance cameras (with the **ip-camera** option), and Cisco Digital Media Players (with the **media-player** option). This model is also suitable for PCs and untrusted devices, since the ports connecting to such devices will remain in their default untrusted state. Switch ports that can be set to conditional trust are shown as green circles in Figure 1.

Service Policy Models

There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

- class-maps which identify the flows using packet markings or by access-lists or other criteria
- policy-maps which specify policy actions to be taken on a class-by-class basis
- service-policy statements which apply a specific policy-map to an interface(s) and specify direction

Step 3: Configure Ingress Queuing

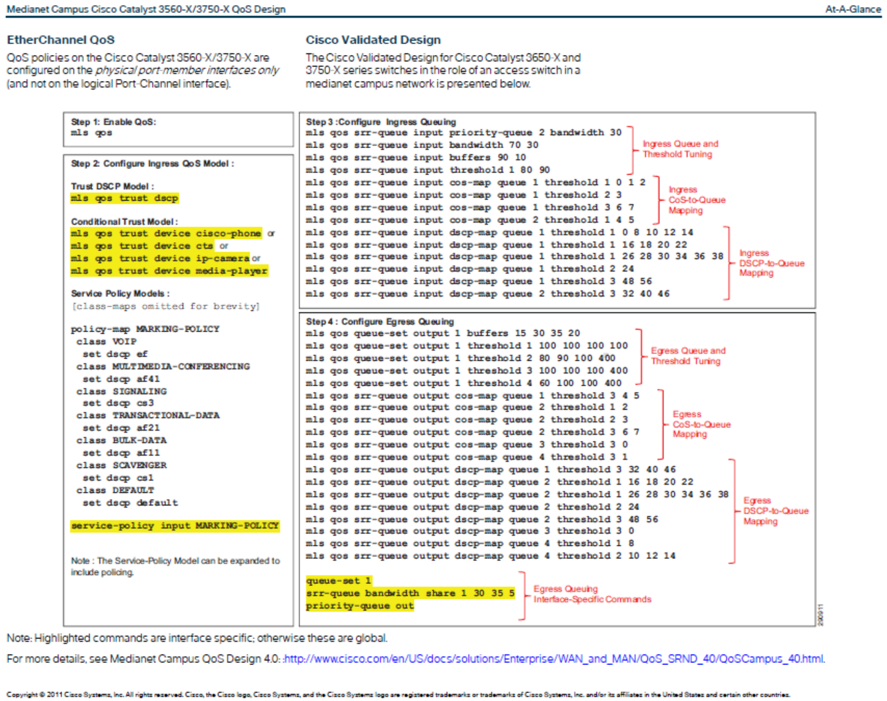
The medianet ingress queuing model for the Cisco Catalyst 3560-X/3750X is shown in Figure 2.

Figure 2 Catalyst 3560-X/3750-X Ingress Queuing Model

Step 4: Configure Egress Queuing

The medianet egress queuing model for the Cisco Catalyst 3560-X/3750X is shown in Figure 3.

Figure 3 Catalyst 3560-X/3750-X Egress Queuing Model



Medianet Campus Cisco Catalyst 3560-X/3750-X QoS Design At-A-Glance

EtherChannel QoS

QoS policies on the Cisco Catalyst 3560-X/3750-X are configured on the *physical port-member interfaces only* (and not on the logical Port-Channel interface).

Cisco Validated Design

The Cisco Validated Design for Cisco Catalyst 3650-X and 3750-X series switches in the role of an access switch in a medianet campus network is presented below.

Step 1: Enable QoS:

```
mls qos
```

Step 2: Configure Ingress QoS Model :

Trust DSCP Model :

```
mls qos trust dscp
```

Conditional Trust Model :

```
mls qos trust device cisco-phone or
mls qos trust device cts or
mls qos trust device ip-camera or
mls qos trust device media-player
```

Service Policy Models :

```
[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

service-policy input MARKING-POLICY
```

Note : The Service-Policy Model can be expanded to include policing.

Step 3 :Configure Ingress Queuing

```
mls qos srr-queue input priority-queue 2 bandwidth 30          ┐
mls qos srr-queue input bandwidth 70 30                        │ Ingress Queue and
mls qos srr-queue input buffers 90 10                          │ Threshold Tuning
mls qos srr-queue input threshold 1 80 90                      ┘
mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2         ┐ Ingress
mls qos srr-queue input cos-map queue 1 threshold 2 3             │ CoS-to-Queue
mls qos srr-queue input cos-map queue 1 threshold 3 6 7           │ Mapping
mls qos srr-queue input cos-map queue 2 threshold 1 4 5           ┘
mls qos srr-queue input dscp-map queue 1 threshold 1 0 8 10 12 14          ┐
mls qos srr-queue input dscp-map queue 1 threshold 1 16 18 20 22           │ Ingress
mls qos srr-queue input dscp-map queue 1 threshold 1 26 28 30 34 36 38     │ DSCP-to-Queue
mls qos srr-queue input dscp-map queue 1 threshold 2 24                    │ Mapping
mls qos srr-queue input dscp-map queue 1 threshold 3 48 56                 │
mls qos srr-queue input dscp-map queue 2 threshold 3 32 40 46              ┘
```

Step 4 : Configure Egress Queuing

```
mls qos queue-set output 1 buffers 15 30 35 20                  ┐
mls qos queue-set output 1 threshold 1 100 100 100 100          │ Egress Queue and
mls qos queue-set output 1 threshold 2 80 90 100 400            │ Threshold Tuning
mls qos queue-set output 1 threshold 3 100 100 100 400          │
mls qos queue-set output 1 threshold 4 60 100 100 400           ┘
mls qos srr-queue output cos-map queue 1 threshold 3 4 5           ┐
mls qos srr-queue output cos-map queue 2 threshold 1 2             │ Egress
mls qos srr-queue output cos-map queue 2 threshold 2 3             │ CoS-to-Queue
mls qos srr-queue output cos-map queue 2 threshold 3 6 7           │ Mapping
mls qos srr-queue output cos-map queue 3 threshold 3 0             │
mls qos srr-queue output cos-map queue 4 threshold 3 1             ┘
mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 46             ┐
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22          │
mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34 36 38    │ Egress
mls qos srr-queue output dscp-map queue 2 threshold 2 24                   │ DSCP-to-Queue
mls qos srr-queue output dscp-map queue 2 threshold 3 48 56                │ Mapping
mls qos srr-queue output dscp-map queue 3 threshold 3 0                    │
mls qos srr-queue output dscp-map queue 4 threshold 1 8                    │
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14             ┘

queue-set 1                                 ┐ Egress Queuing
srr-queue bandwidth share 1 30 35 5         │ Interface-Specific Commands
priority-queue out                          ┘
```

Note: Highlighted commands are interface specific; otherwise these are global.

For more details, see Medianet Campus QoS Design 4.0: :http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html.

http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/qoscampuscat3xxxaag.pdf

Enterprise QoS

Agenda

- Business and Technical Drivers for QoS Design Update
- Components of QoS
- Campus QoS Design Considerations and Models
- Catalyst QoS Design
- Catalyst AutoQoS
- WAN and Branch QoS Design
- What about DC, SDN and other areas where QoS is important?

Catalyst 2960/3560/3750G/E/X Auto QoS for Medianet

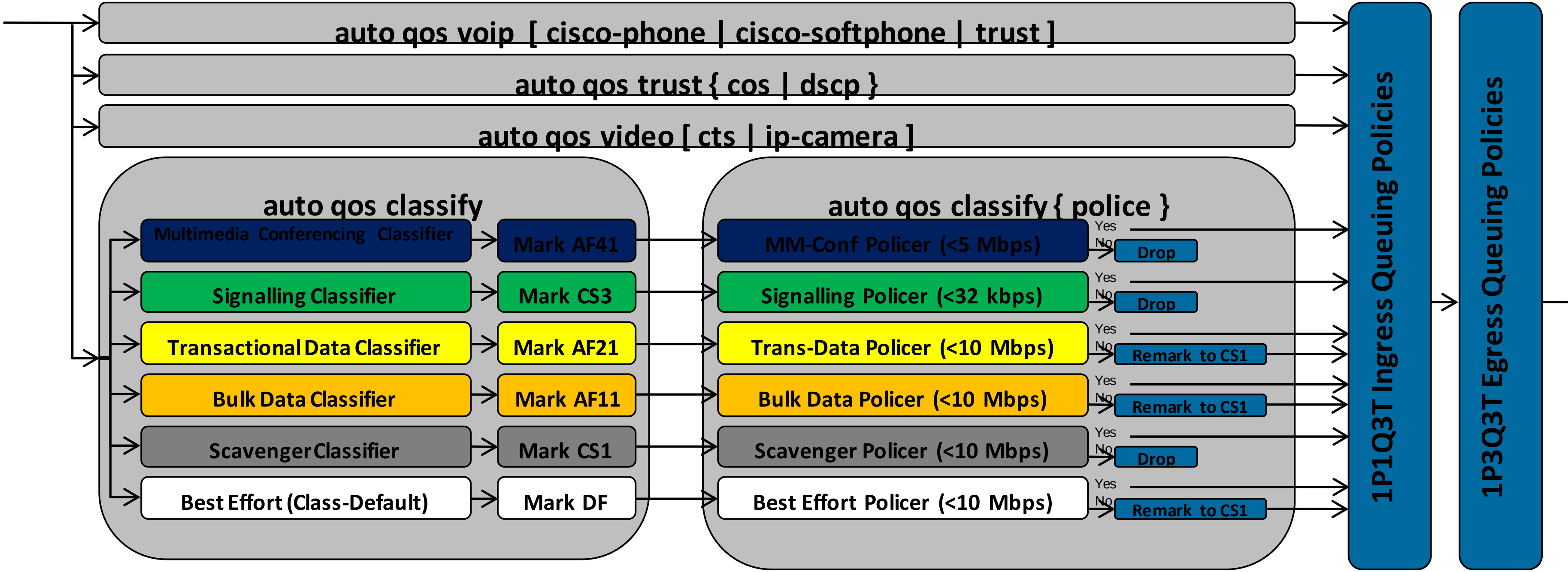
AutoQoS

- Simplifies the deployment of QoS Policies
- Uses a set of Standard configurations that can be modified
- Currently all switch platforms support AutoQoS-VoIP
  - Best practice QoS designs for IP Telephony deployments
- Catalyst 2K/3K now supports AutoQoS for Medianet
  - AutoQoS SRND4
  - Supports not only IP Phones, but also TelePresence & IPVS cameras
  - Autoprovisions ingress trust, classification, marking & policing
  - Autoprovisions ingress queuing (as applicable)
  - Autoprovisions egress queuing

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1098289

Catalyst 2960/2975/3560/3750 G/E/X QoS Design

AutoQoS SRND4 Models



auto qos voip [cisco-phone | cisco-softphone | trust]

auto qos trust { cos | dscp }

auto qos video [cts | ip-camera]

auto qos classify

Multimedia Conferencing Classifier	Mark AF41
Signalling Classifier	Mark CS3
Transactional Data Classifier	Mark AF21
Bulk Data Classifier	Mark AF11
Scavenger Classifier	Mark CS1
Best Effort (Class-Default)	Mark DF

auto qos classify { police }

MM-Conf Policer (<5 Mbps)	Yes	No	Drop
Signalling Policer (<32 kbps)	Yes	No	Drop
Trans-Data Policer (<10 Mbps)	Yes	No	Remark to CS1
Bulk Data Policer (<10 Mbps)	Yes	No	Remark to CS1
Scavenger Policer (<10 Mbps)	Yes	No	Drop
Best Effort Policer (<10 Mbps)	Yes	No	Remark to CS1

1P1Q3T Ingress Queuing Policies

1P3Q3T Egress Queuing Policies

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1144082

Catalyst 2960/3560/3750 G/E/X QoS Design

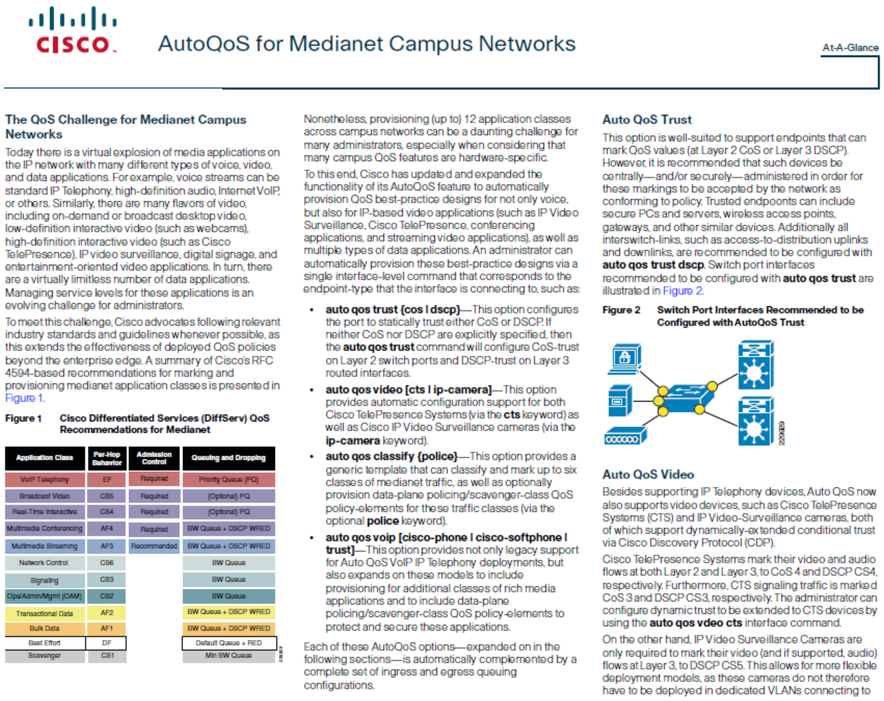
AutoQoS SRND4 – auto qos voip cisco-phone

```
C3750-X(config-if)#auto qos voip cisco-phone
```

Class-maps omitted for brevity

```
! This section defines the AutoQoS-VoIP-Cisco-Phone (SRND4) Policy-Map
policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
 class AUTOQOS_VOIP_DATA_CLASS
  set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
  ! Voice is marked to DSCP EF and policed (to remark) if exceeding 128 kbps
 class AUTOQOS_VOIP_SIGNAL_CLASS
  set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
  ! Signaling is marked to DSCP CS3 and policed (to remark) if exceeding 32 kbps
 class AUTOQOS_DEFAULT_CLASS
  set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
  ! An explicit default class marks all other IP traffic to DF
  ! and polices all other IP traffic to remark (to CS0) at 10 Mbps
!
```

AutoQoS for Medianet - At-A-Glance



AutoQoS for Medianet Campus Networks

At-A-Glance

The QoS Challenge for Medianet Campus Networks

Today there is a virtual explosion of media applications on the IP network with many different types of voice, video, and data applications. For example, voice streams can be standard IP Telephony, high-definition audio, Internet VoIP, or others. Similarly, there are many flavors of video, including on-demand or broadcast desktop video, low-definition interactive video (such as webcams), high-definition interactive video (such as Cisco TelePresence), IP video surveillance, digital signage, and entertainment-oriented video applications. In turn, there are a virtually limitless number of data applications. Managing service levels for these applications is an evolving challenge for administrators.

To meet this challenge, Cisco advocates following relevant industry standards and guidelines whenever possible, as this extends the effectiveness of deployed QoS policies beyond the enterprise edge. A summary of Cisco's RFC 4594-based recommendations for marking and provisioning medianet application classes is presented in Figure 1.

Figure 1 Cisco Differentiated Services (DiffServ) QoS Recommendations for Medianet

Application Class	Per-Hop Behavior	Admission Control	Queuing and Dropping
VoIP Telephony	EF	Required	Priority Queue (PQ)
Broadcast Video	CS5	Required	(Optional) PQ
Real-Time Interactive	CS4	Required	(Optional) PQ
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED
Network Control	CS6		BW Queue
Signaling	CS3		BW Queue
Ops/Admin/Mgmt (OAM)	CS2		BW Queue
Transactional Data	AF2		BW Queue + DSCP WRED
Bulk Data	AF1		BW Queue + DSCP WRED
Best Effort	DF		Default Queue + RED
Scavenger	CS1		Min BW Queue

Nonetheless, provisioning (up to) 12 application classes across campus networks can be a daunting challenge for many administrators, especially when considering that many campus QoS features are hardware-specific.

To this end, Cisco has updated and expanded the functionality of its AutoQoS feature to automatically provision QoS best-practice designs for not only voice, but also for IP-based video applications (such as IP Video Surveillance, Cisco TelePresence, conferencing applications, and streaming video applications), as well as multiple types of data applications. An administrator can automatically provision these best-practice designs via a single interface-level command that corresponds to the endpoint-type that the interface is connecting to, such as:

- **auto qos trust {cos l dscp}**—This option configures the port to statically trust either CoS or DSCP. If neither CoS nor DSCP are explicitly specified, then the **auto qos trust** command will configure CoS-trust on Layer 2 switch ports and DSCP-trust on Layer 3 routed interfaces.
- **auto qos video [cts l ip-camera]**—This option provides automatic configuration support for both Cisco TelePresence Systems (via the **cts** keyword) as well as Cisco IP Video Surveillance cameras (via the **ip-camera** keyword).
- **auto qos classify {police}**—This option provides a generic template that can classify and mark up to six classes of medianet traffic, as well as optionally provision data-plane policing/scavenger-class QoS policy-elements for these traffic classes (via the optional **police** keyword).
- **auto qos voip [cisco-phone l cisco-softphone l trust]**—This option provides not only legacy support for Auto QoS VoIP IP Telephony deployments, but also expands on these models to include provisioning for additional classes of rich media applications and to include data-plane policing/scavenger-class QoS policy-elements to protect and secure these applications.

Each of these AutoQoS options—expanded on in the following sections—is automatically complemented by a complete set of ingress and egress queuing configurations.

Auto QoS Trust

This option is well-suited to support endpoints that can mark QoS values (at Layer 2 CoS or Layer 3 DSCP). However, it is recommended that such devices be centrally—and/or securely—administered in order for these markings to be accepted by the network as conforming to policy. Trusted endpoonts can include secure PCs and servers, wireless access points, gateways, and other similar devices. Additionally all interswitch-links, such as access-to-distribution uplinks and downlinks, are recommended to be configured with **auto qos trust dscp**. Switch port interfaces recommended to be configured with **auto qos trust** are illustrated in Figure 2.

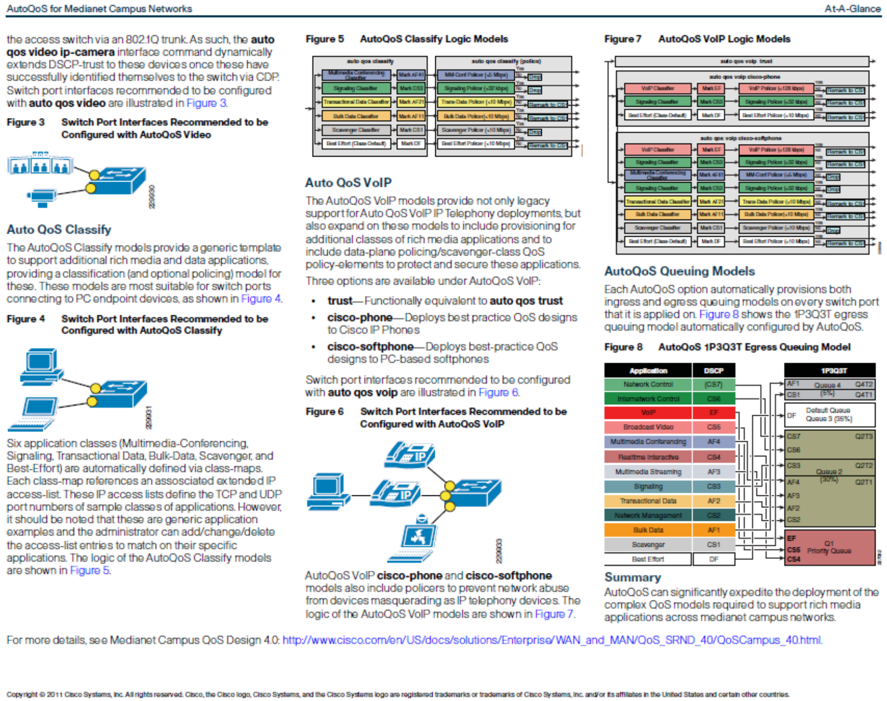
Figure 2 Switch Port Interfaces Recommended to be Configured with AutoQoS Trust

Auto QoS Video

Besides supporting IP Telephony devices, Auto QoS now also supports video devices, such as Cisco TelePresence Systems (CTS) and IP Video-Surveillance cameras, both of which support dynamically-extended conditional trust via Cisco Discovery Protocol (CDP).

Cisco TelePresence Systems mark their video and audio flows at both Layer 2 and Layer 3, to CoS 4 and DSCP CS4, respectively. Furthermore, CTS signaling traffic is marked CoS 3 and DSCP CS3, respectively. The administrator can configure dynamic trust to be extended to CTS devices by using the **auto qos vdeo cts** interface command.

On the other hand, IP Video Surveillance Cameras are only required to mark their video (and if supported, audio) flows at Layer 3, to DSCP CS5. This allows for more flexible deployment models, as these cameras do not therefore have to be deployed in dedicated VLANs connecting to



the access switch via an 802.1Q trunk. As such, the **auto qos video ip-camera** interface command dynamically extends DSCP-trust to these devices once these have successfully identified themselves to the switch via CDP. Switch port interfaces recommended to be configured with **auto qos video** are illustrated in Figure 3.

Figure 3 Switch Port Interfaces Recommended to be Configured with AutoQoS Video

Auto QoS Classify

The AutoQoS Classify models provide a generic template to support additional rich media and data applications, providing a classification (and optional policing) model for these. These models are most suitable for switch ports connecting to PC endpoint devices, as shown in Figure 4.

Figure 4 Switch Port Interfaces Recommended to be Configured with AutoQoS Classify

Six application classes (Multimedia-Conferencing, Signaling, Transactional Data, Bulk-Data, Scavenger, and Best-Effort) are automatically defined via class-maps. Each class-map references an assosciated extended IP access-list. These IP access lists define the TCP and UDP port numbers of sample classes of applications. However, it should be noted that these are generic application examples and the administrator can add/change/delete the access-list entries to match on their specific applications. The logic of the AutoQoS Classify models are shown in Figure 5.

Figure 5 AutoQoS Classify Logic Models

auto qos classify
auto qos classify (police)
Scavenger Classifier
Mark CS1
Scavenger Policer (<10 Mbps)
Drop
Best Effort (Class-Default)
Mark DF
Best Effort Policer (<10 Mbps)
Remark to CS1

Auto QoS VoIP

The AutoQoS VoIP models provide not only legacy support for Auto QoS VoIP IP Telephony deployments, but also expand on these models to include provisioning for additional classes of rich media applications and to include data-plane policing/scavenger-class QoS policy-elements to protect and secure these applications.

Three options are available under AutoQoS VoIP:

- **trust**—Functionally equivalent to **auto qos trust**
- **cisco-phone**—Deploys best practice QoS designs to Cisco IP Phones
- **cisco-softphone**—Deploys best-practice QoS designs to PC-based softphones

Switch port interfaces recommended to be configured with **auto qos voip** are illustrated in Figure 6.

Figure 6 Switch Port Interfaces Recommended to be Configured with AutoQoS VoIP

AutoQoS VoIP **cisco-phone** and **cisco-softphone** models also include policers to prevent network abuse from devices masquerading as IP telephony devices. The logic of the AutoQoS VoIP models are shown in Figure 7.

Figure 7 AutoQoS VoIP Logic Models

auto qos voip trust
auto qos voip cisco-phone
auto qos voip cisco-softphone
Bulk Data Classifier
Mark AF11
Bulk Data Policer (<10 Mbps)
Remark to CS1
Scavenger Classifier
Mark CS1
Scavenger Policer (<10 Mbps)
Drop
Best Effort (Class-Default)
Mark DF
Best Effort Policer (<10 Mbps)
Remark to CS1

AutoQoS Queuing Models

Each AutoQoS option automatically provisions both ingress and egress queuing models on every switch port that it is applied on. Figure 8 shows the 1P3Q3T egress queuing model automatically configured by AutoQoS.

Figure 8 AutoQoS 1P3Q3T Egress Queuing Model

Summary

AutoQoS can significantly expedite the deployment of the complex QoS models required to support rich media applications across medianet campus networks.

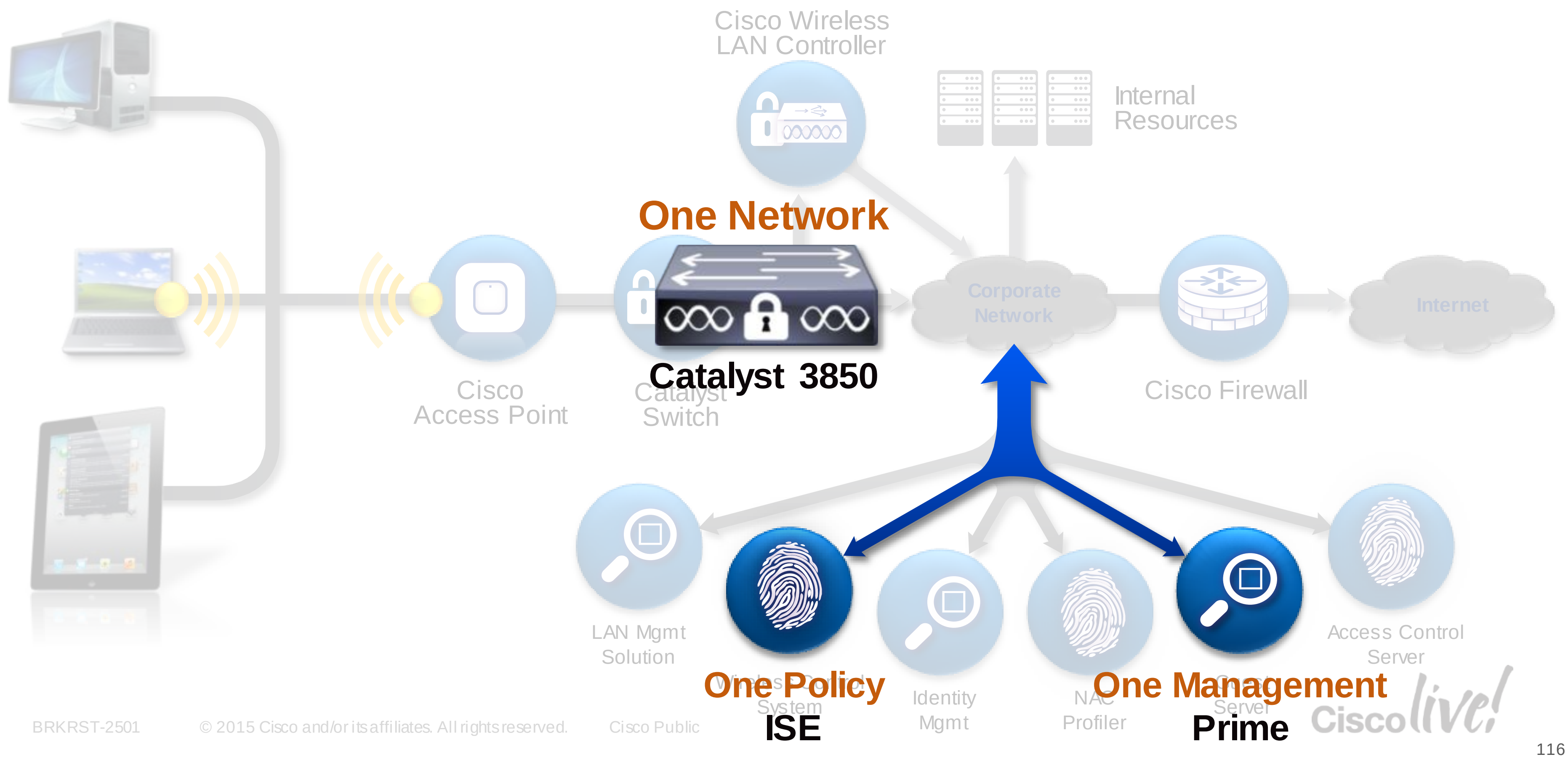
For more details, see Medianet Campus QoS Design 4.0: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html.

http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/autoqosmediacampus.pdf

Additional AutoQoS Links

- AutoQoS 1P1Q3T Ingress Queuing Policies
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1144932
- AutoQoS Egress 1P3Q3T Queuing Policies
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1144981
- AutoQoS on EtherChannel
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1145082
- Removing AutoQoS
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1145119
- AutoQoS At-A-Glance
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/autoqosmediacampus.pdf

Converged Access with the Cat 3850



Catalyst 3850 Campus QoS Design

- QoS Design Steps

1. Configure Ingress QoS Model(s):

- ❑ DSCP-Trust Model*
- ❑ Conditional Trust Models
- ❑ Service Policy Models

2. Configure Egress Queuing

*Catalyst 3850 IOS MQC will trust DSCP by default (therefore no explicit policy is required for DSCP trust)

Catalyst 3850 Campus QoS Design

Service Policy Model Example – Marking Policy

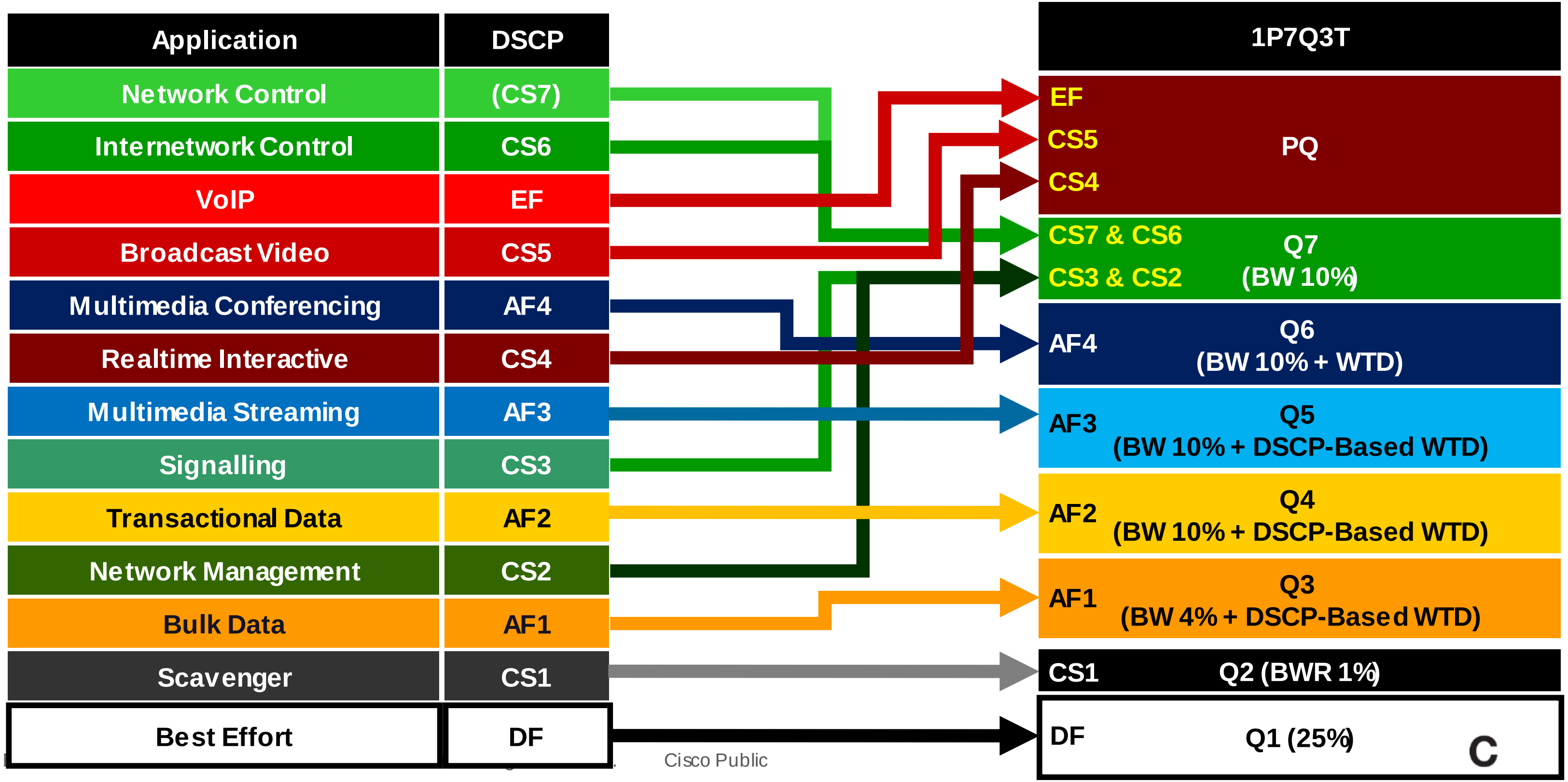
Configuration

```
[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
```

```
service-policy input MARKING-POLICY
```

Catalyst 3850 Campus QoS Design

- Egress Queuing (1P7Q3T with WTD) Model



Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signalling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

1P7Q3T

EF
CS5
CS4 — PQ

CS7 & CS6
CS3 & CS2 — Q7 (BW 10%)

AF4 — Q6 (BW 10% + WTD)

AF3 — Q5 (BW 10% + DSCP-Based WTD)

AF2 — Q4 (BW 10% + DSCP-Based WTD)

AF1 — Q3 (BW 4% + DSCP-Based WTD)

CS1 — Q2 (BWR 1%)

DF — Q1 (25%)

WTD = Weighted Tail Drop

Cisco Catalyst 4500 (Supervisor 7-E) and 4500-X QoS Design

Catalyst 6500E QoS Design

Campus QoS Design Considerations

- Catalyst 2960 / 3650 / 3750 are the last platforms to use Multilayer Switch QoS (MLS QoS) syntax
  - QoS is disabled by default and must be globally enabled with **mls qos** command
  - Once enabled, all ports are set to an untrusted port-state
- Catalyst 3850 and 4500 are using IOS Modular QoS Command Line Interface (MQC) syntax (like router platforms)
  - QoS is enabled by default
  - All ports trust at layer 2 and layer 3 by default
- Catalyst 6500 is using Cisco Common Classification Policy Language (C3PL) QoS
  - QoS is enabled by default (Sup2T) – Disabled by default (Sup720)
  - All ports trust at layer 2 and layer 3 by default
  - C3PL presents queuing policies similar to MQC

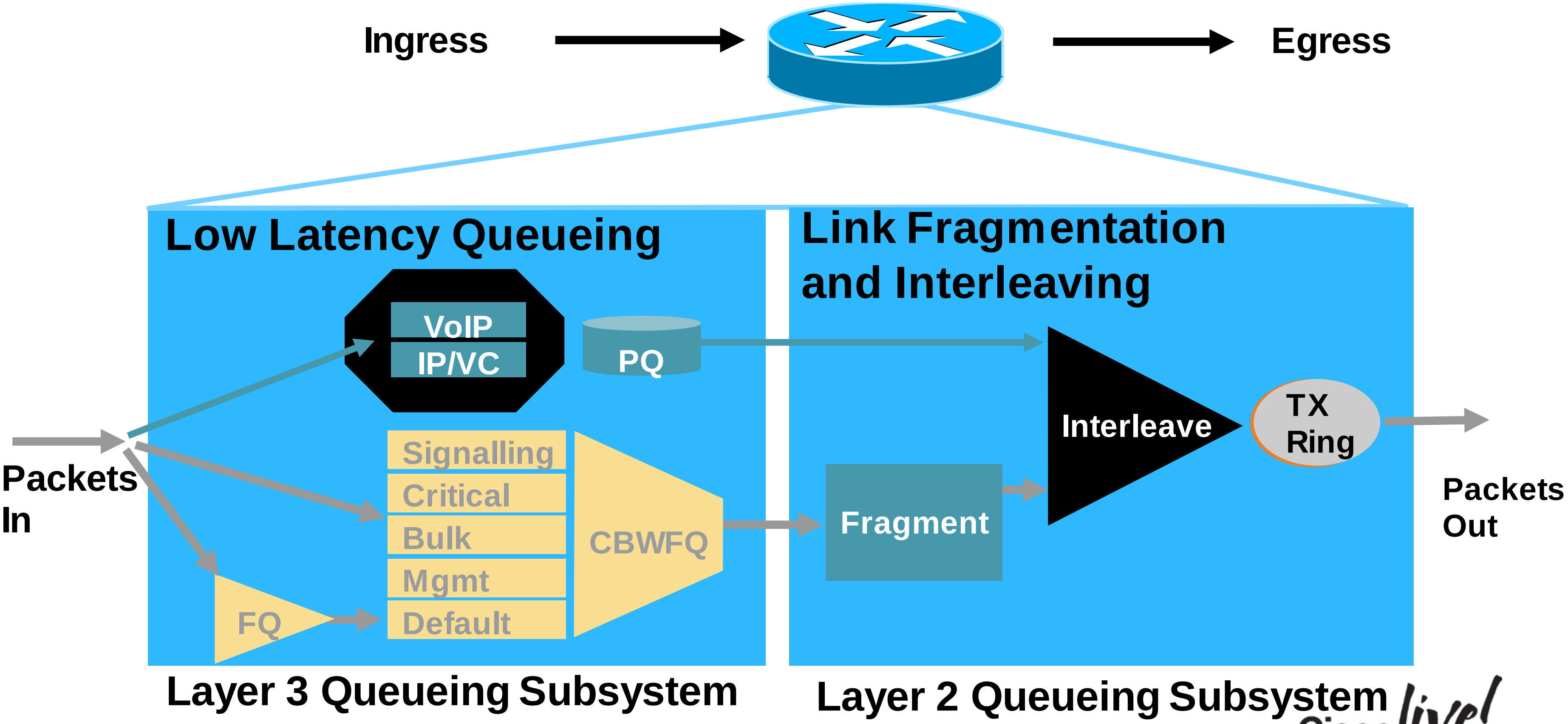
Enterprise QoS

Agenda

- Business and Technical Drivers for QoS Design Update
- Components of QoS
- Campus QoS Design Considerations and Models
- Catalyst QoS Design
- Catalyst AutoQoS
- WAN and Branch QoS Design
- What about DC, SDN and other areas where QoS is important?

WAN and Branch QoS Design

Scheduling Tools - LLQ/CBWFQ Subsystems

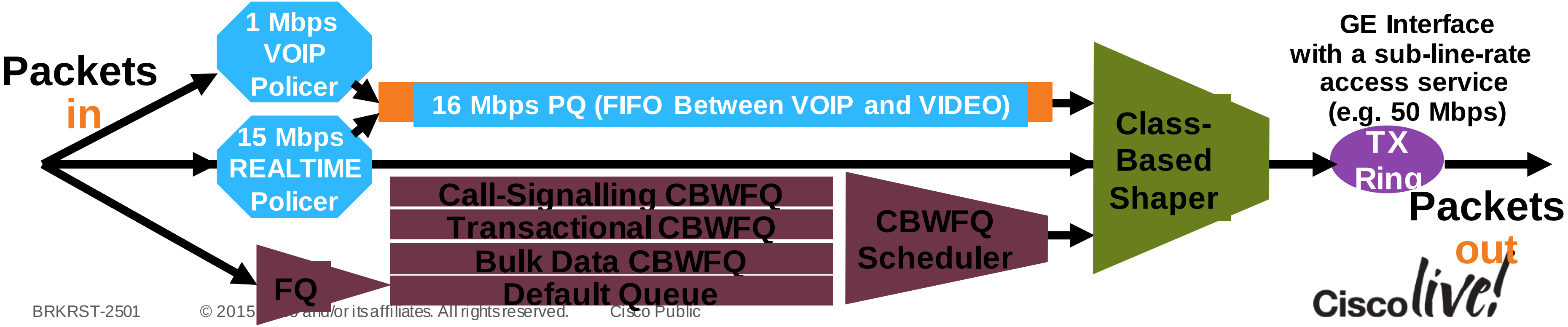


WAN/VPN QoS Mechanisms and Operation

Hierarchical QoS (Queuing & Shaping) Operation

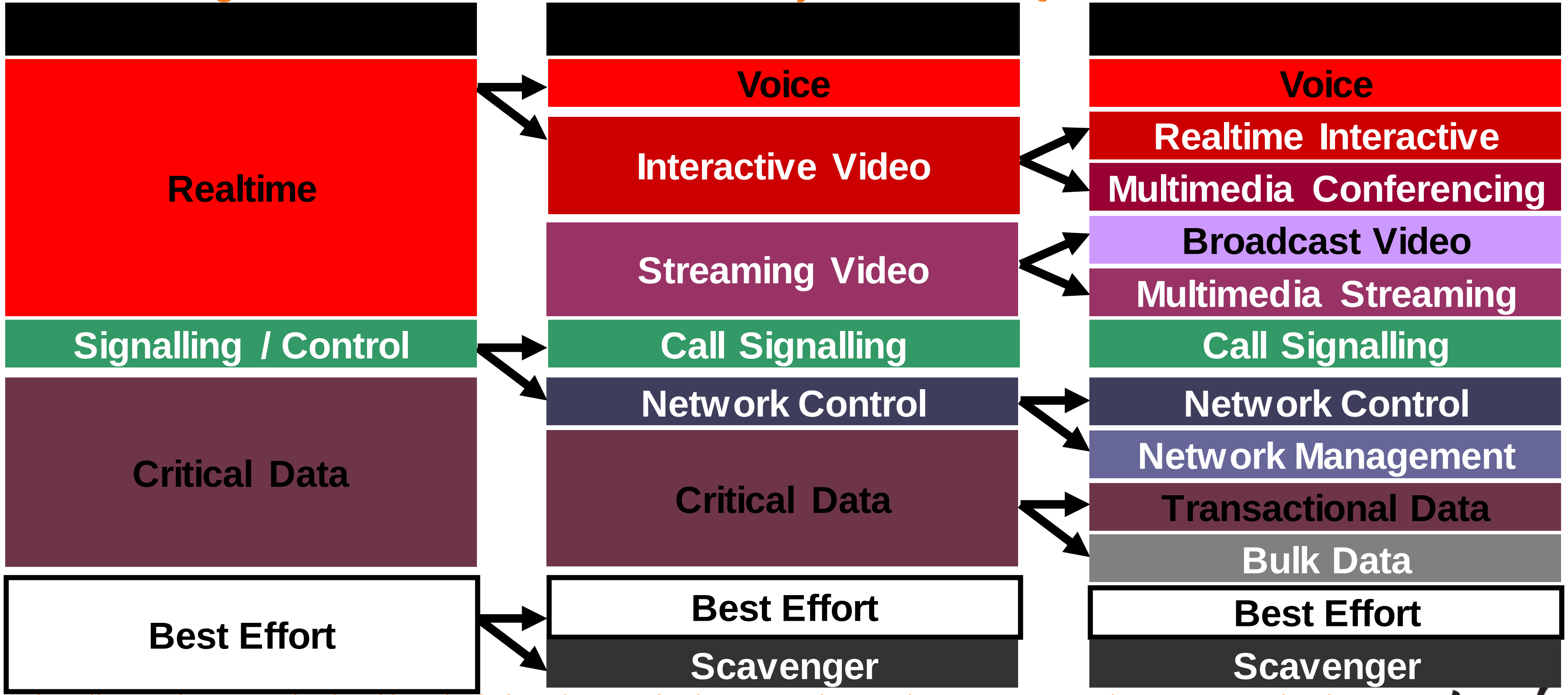
```
policy-map ACCESS-EDGE
 class VOIP
  priority 1000
 class REALTIME
  priority 15000
 class CALL-SIGNALING
  bandwidth x
 class TRANSACTIONAL
  bandwidth y
 class BULK-DATA
  bandwidth z
 class class-default
  fair-queue
```

- Queuing policies *will not* engage unless the interface is congested
- A shaper will guarantee that traffic will not exceed the contracted rate
- Traffic sharing the Priority Queue is Services on FIFO basis



Cisco Medianet WAN & Branch Design

WAN Edge Models Are Not Restricted By Hardware Queues



Realtime

Signalling / Control

Critical Data

Best Effort

Voice

Interactive Video

Streaming Video

Call Signalling

Network Control

Critical Data

Best Effort

Scavenger

Voice

Realtime Interactive

Multimedia Conferencing

Broadcast Video

Multimedia Streaming

Call Signalling

Network Control

Network Management

Transactional Data

Bulk Data

Best Effort

Scavenger

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp61135

Modular QoS and the Hierarchical Queuing Framework (HQF)

1. Traffic classification
   - "class-map"
   - identify traffic and assign to classes
2. Define the Policy
   - "policy-map"
   - Assign classes to a policy
   - Define the Treatment for each class
3. Attach the Policy to a logical/physical interface
   - "service-policy"
   - The point of application of a QOS policy

```
class-map match-any VOICE_CLASS
  match ip dscp 46
  match access-group 100
class-map match-any BUS
  match access-group 101
class-map match-all CTRL
  match access-group 103
  match access-group 104
!
policy-map QOS_POLICY
  class VOICE_CLASS
    priority
    police 64000
  class BUS
    bandwidth remaining percent 90
!
interface Gi 0/0
 ip address 192.168.2.2 255.255.255.0
 service-policy output QOS_POLICY
```

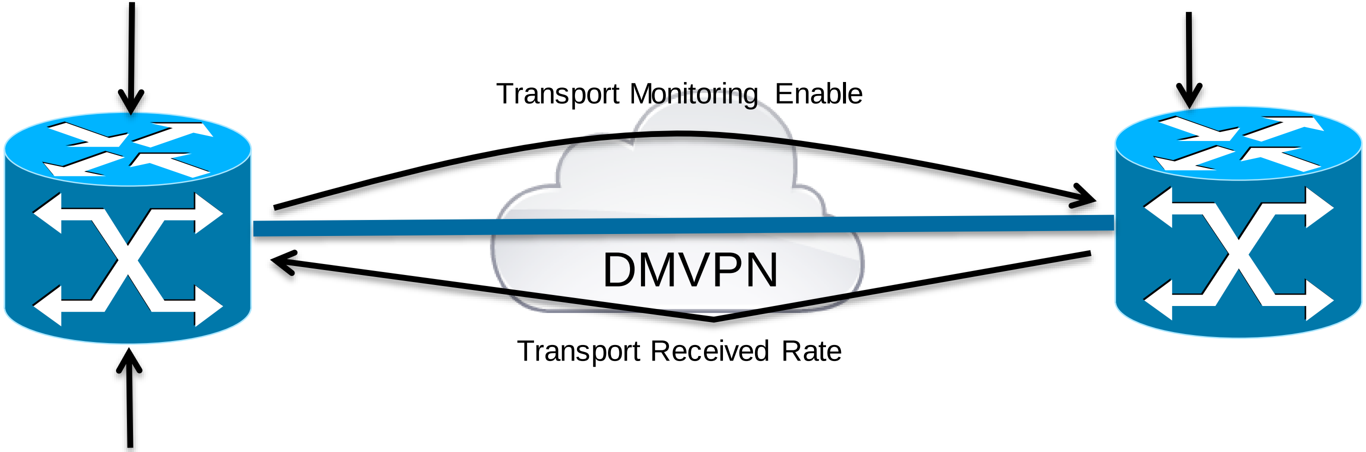
Adaptive QoS For Intelligent WAN Transport

How Does It Work?

Adapt shaping rate at the Sender based on the available bandwidth between specific Sender and Receiver (two end-points of a DMVPN tunnel)

- Configure MQC Policy with Adaptive Shaping
- Attach service-policy to nhrp-group in Egress

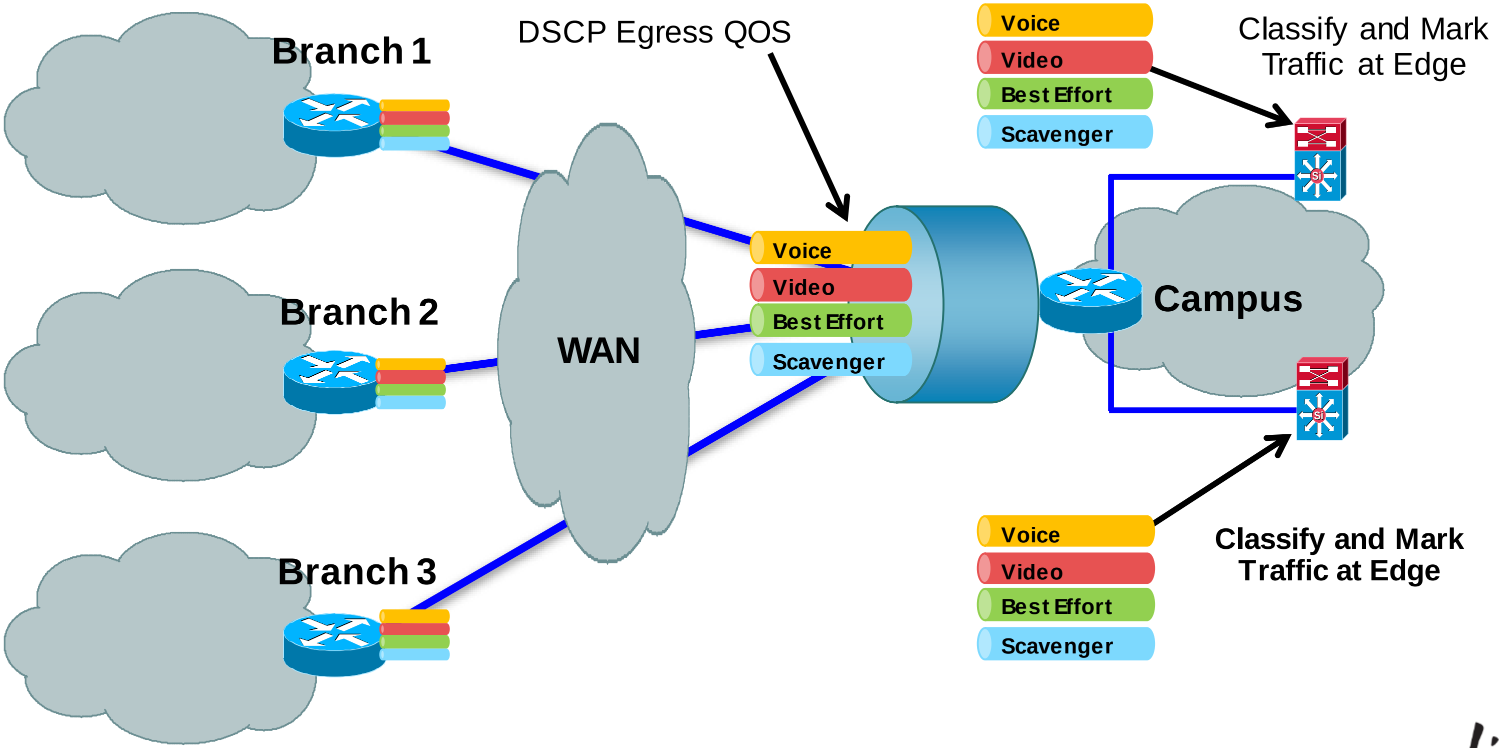
Create State for Periodic Collection of Stats on tunnel traffic received



1) Calculate Available Bandwidth in the Cloud
2) Adapt Egress Shaper to New Calculated Rate

shape adaptive upper-bound <<bps> | percent <value>>
[lower-bound <<bps> | percent <value>>]

Typical Intelligent WAN and Branch QoS Deployment



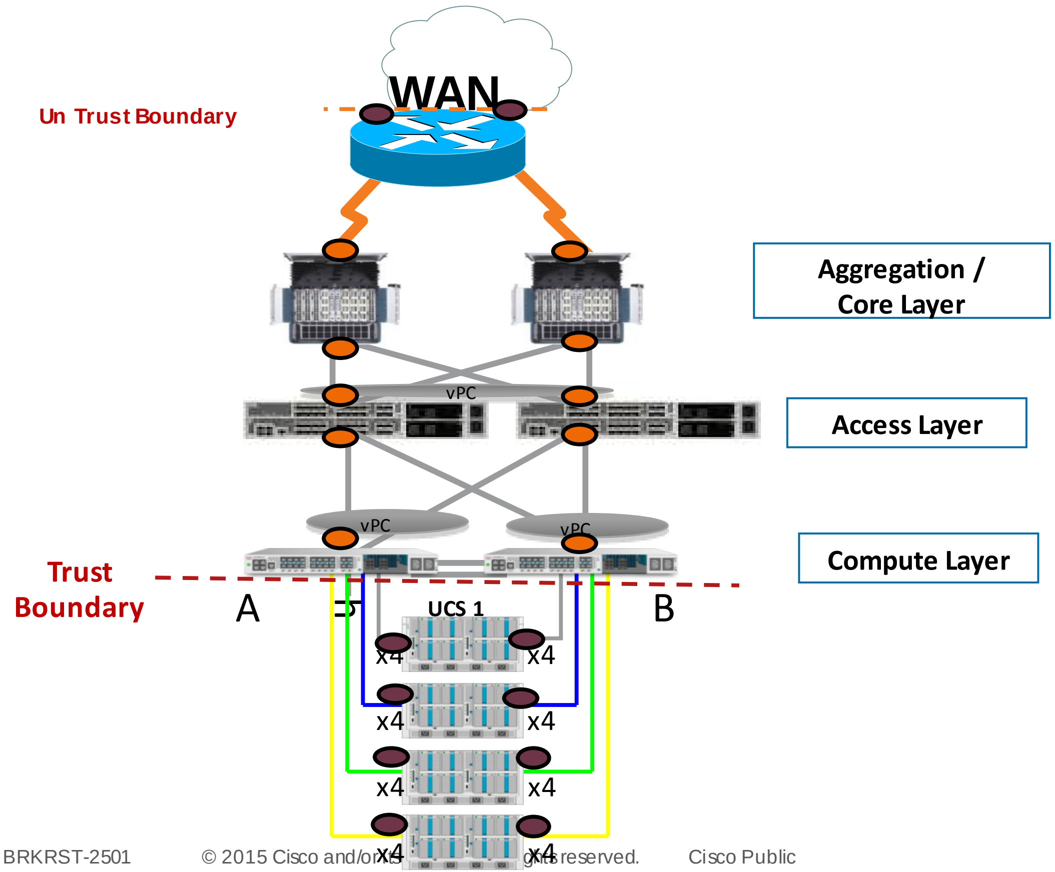
Enterprise QoS

Agenda

- Business and Technical Drivers for QoS Design Update
- Components of QoS
- Campus QoS Design Considerations and Models
- Catalyst QoS Design
- Catalyst AutoQoS
- WAN and Branch QoS Design
- What about DC, SDN and other areas where QoS is important?

Comment on DC QoS

End-to-end QoS – Similar Requirements



● Classification and initial marking

● Trust Pre-Assigned COS Markings

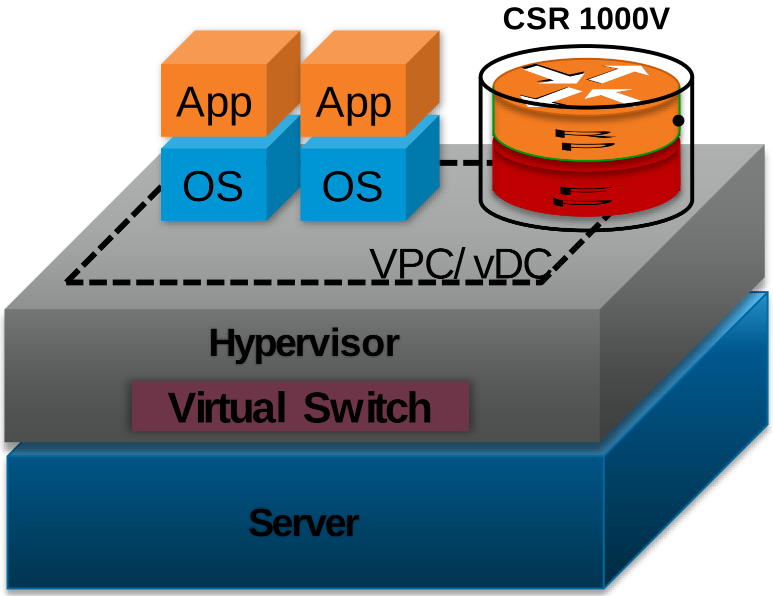
QOS Classification & Marking:
Classify and mark traffic at the compute and WAN edge layer .

QOS Trust
Subsequent points in the network can now “trust” the marked values and queue.

QOS queuing and BW guarantee:
Bandwidth based DWRR queuing on uplinks

Cisco CSR 1000V

Cisco IOS Software in Virtual Form-Factor



IOS XE Cloud Edition

- Selected Features of IOS XE for Cloud Use Cases
- MPLS CE, VPN, QoS

Infrastructure Agnostic

- Server, Switch, Hypervisor

Single-tenant WAN Gateway

- Small Footprint, Low Performance

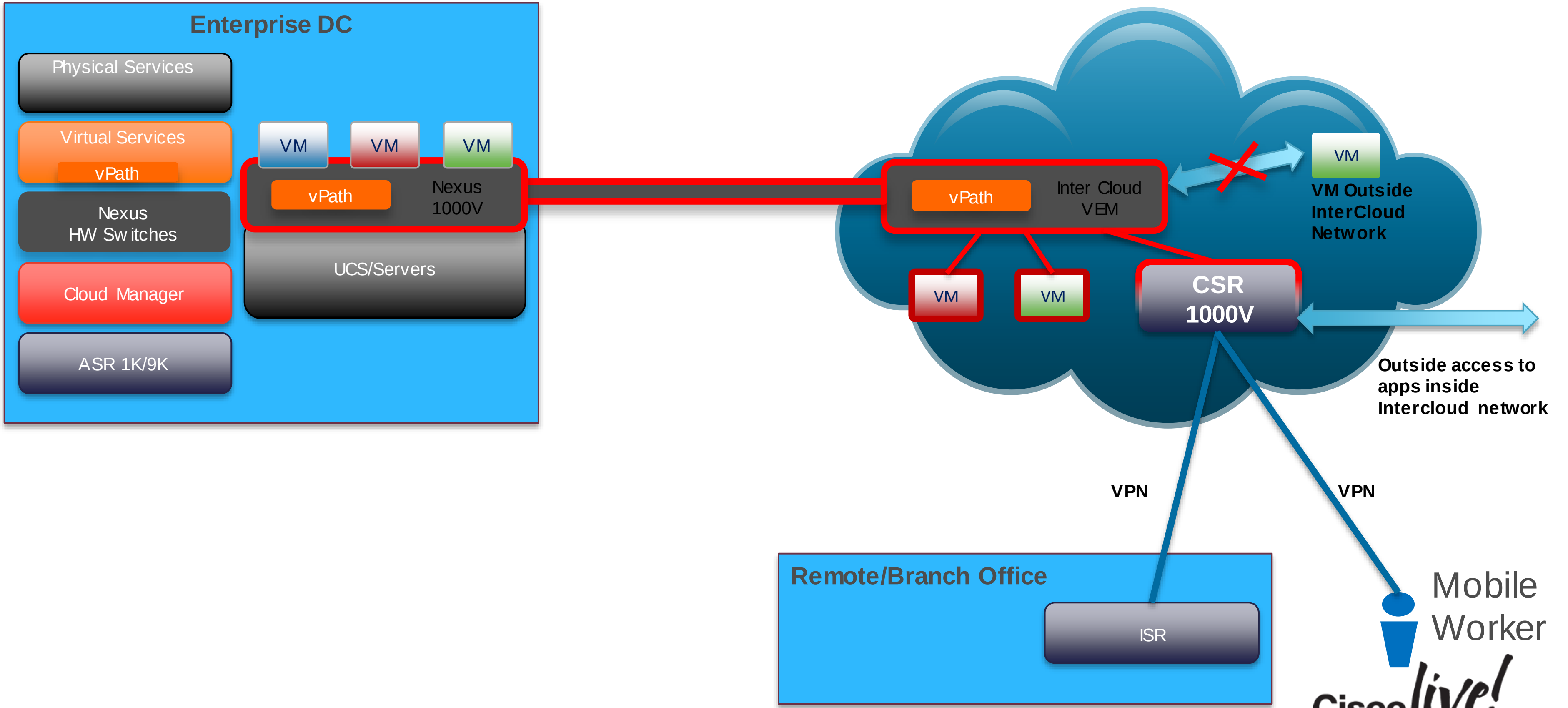
Term and Usage-based Licenses

- Elastic Capacity (Throughput, Memory)

Enterprise-class Networking with Rapid Deployment and Flexibility

CSR – Virtualised Router for QoS

Connect DC/ Branch/ Home to Cloud



Application Visibility and Control (AVC) and Software Defined Networking (SDN)

Application Visibility and Control

Growing Numbers of Apps in the Network

Range of applications in the network:

- Different traffic characteristics
- Different bandwidth requirements
- Different tolerances to delay, loss
- Different service level expectations

Existing Policies are:

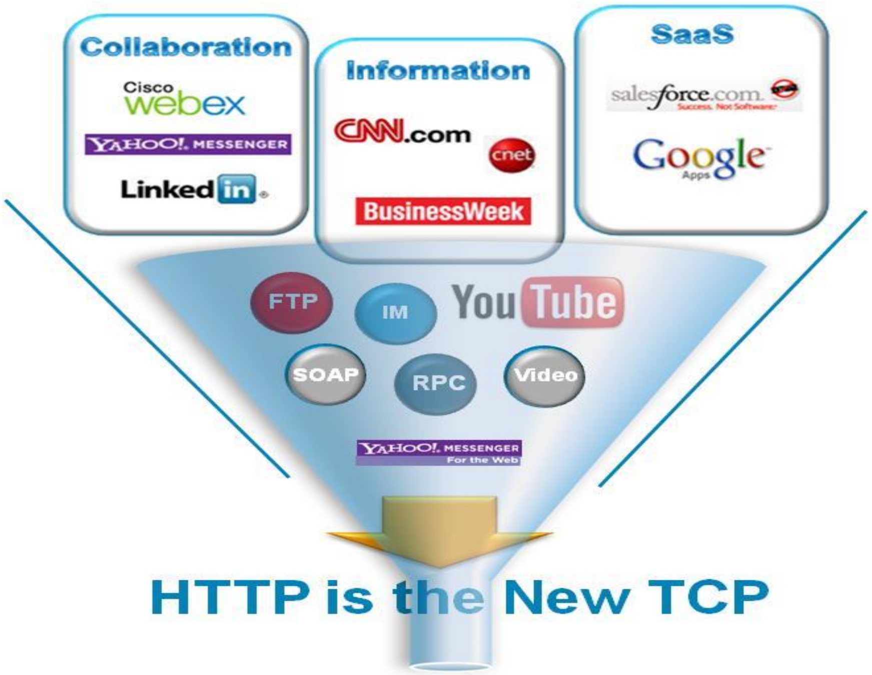
- Ports or ACL/DSCP driven
- Difficult to enforce for many Apps (port 80)
- Not scalable for big deployments (many ACEs)

AVC Provides:

- Application based policy enforcement (NBAR2/Metadata + QoS) for > 1000 apps
- Scalable, intuitive policies aligned to business logic
- Policy performance reporting (NBAR2/Metadata + QoS + FNF)
- Leverages the Identity Services Engine (ISE)

HTTP/HTTPS Ports: Open 24x7

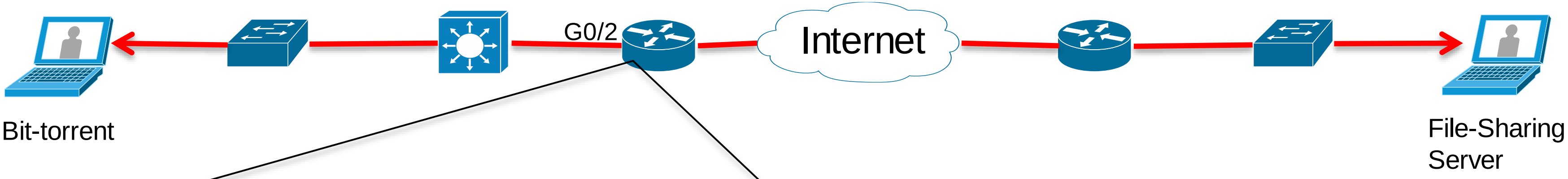
Problem: Static port classification is No Longer Sufficient



- ACL Traffic Classification doesn’t scale or match different Application characteristics
- Increasing use of Encryption (e.g HTTPS, TLS)
- User Experience sessions are composites of multiple application flows (e.g Webex Video, Voice, Data)
- IPv4 and IPv6 transition techniques proliferation

Configuration

Application Awareness with NBAR



```
class-map match-all Low-Priority-Apps
 match protocol bittorrent
 match protocol attribute p2p-technology p2p-tech-yes
!
policy-map Police-Apps
 class Low-Priority-Apps
  police 9000 conform-action transmit exceed-action drop
!
interface GigabitEthernet 0/2
 ip nbar protocol-discovery
 service-policy input Police-Apps
```

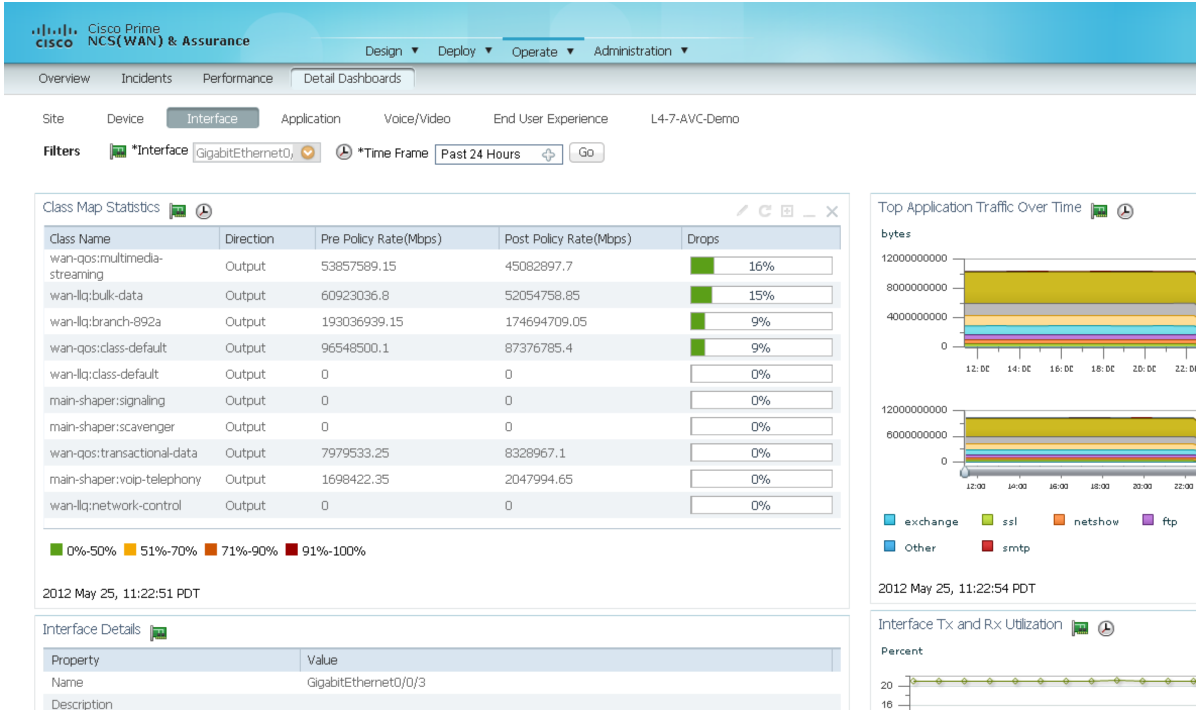
Classify Low priority App's using NBAR

Police Low priority App's

Enable NBAR protocol discovery

QoS Reporting with Cisco Prime Infrastructure (PI)

Monitor QoS Performance



Class Map Statistics

Class Name	Direction	Pre Policy Rate(Mbps)	Post Policy Rate(Mbps)	Drops
wan-qos:multimedia-streaming	Output	53857589.15	45082897.7	16%
wan-llq:bulk-data	Output	60923036.8	52054758.85	15%
wan-llq:branch-892a	Output	193036939.15	174694709.05	9%
wan-qos:class-default	Output	96548500.1	87376785.4	9%
wan-llq:class-default	Output	0	0	0%
main-shaper:signaling	Output	0	0	0%
main-shaper:scavenger	Output	0	0	0%
wan-qos:transactional-data	Output	7979533.25	8328967.1	0%
main-shaper:voip-telephony	Output	1698422.35	2047994.65	0%
wan-llq:network-control	Output	0	0	0%

🟩 0%-50% 🟨 51%-70% 🟧 71%-90% 🟥 91%-100%

2012 May 25, 11:22:51 PDT

Top Application Traffic Over Time

2012 May 25, 11:22:54 PDT

Interface Details

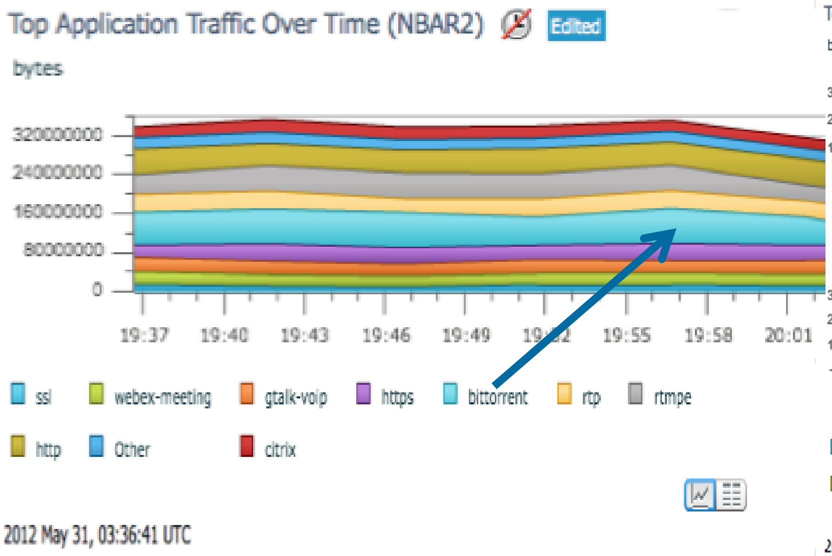
Property	Value
Name	GigabitEthernet0/0/3
Description	

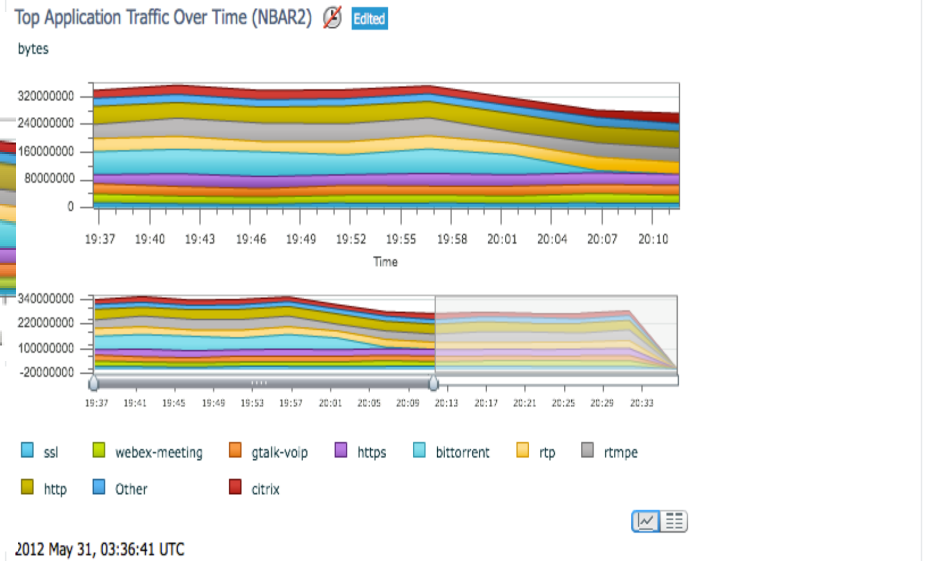
Interface Tx and Rx Utilization

QoS Reports with Cisco PI today:

- Top Application over Time (various filters: site level, end point level, global reports etc)
- QoS Class Map Statistics, Queue Drops, Pre/Post Traffic Rate, from CBQoS MIB
- New QoS features planned for PI 2.x

Validate Application Performance





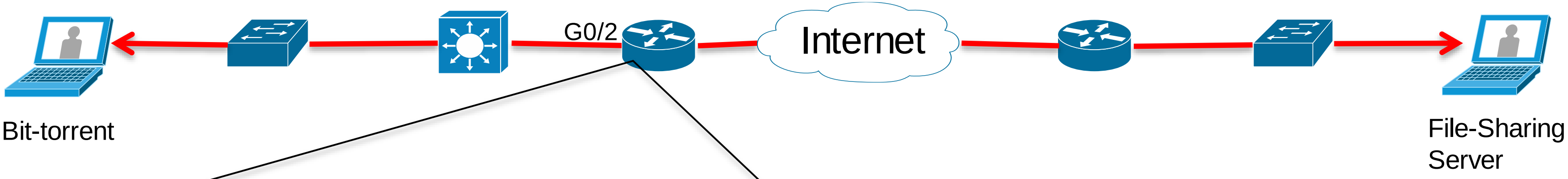
BEFORE QoS POLICY

AFTER QoS POLICY

QoS Policy applied from Cisco PI has policed the torrent traffic, thereby creating more room for business critical traffic on the WAN Interface

Configuration

Media Awareness with NBAR



```
class-map match-all Low-Priority-Apps
 match protocol bittorrent
 match protocol attribute p2p-technology p2p-tech-yes
!
policy-map Police-Apps
 class Low-Priority-Apps
   police 9000 conform-action transmit exceed-action drop
!
interface GigabitEthernet 0/2
  ip nbar protocol-discovery
  service-policy input Police-Apps
```

Classify Low priority App's using NBAR

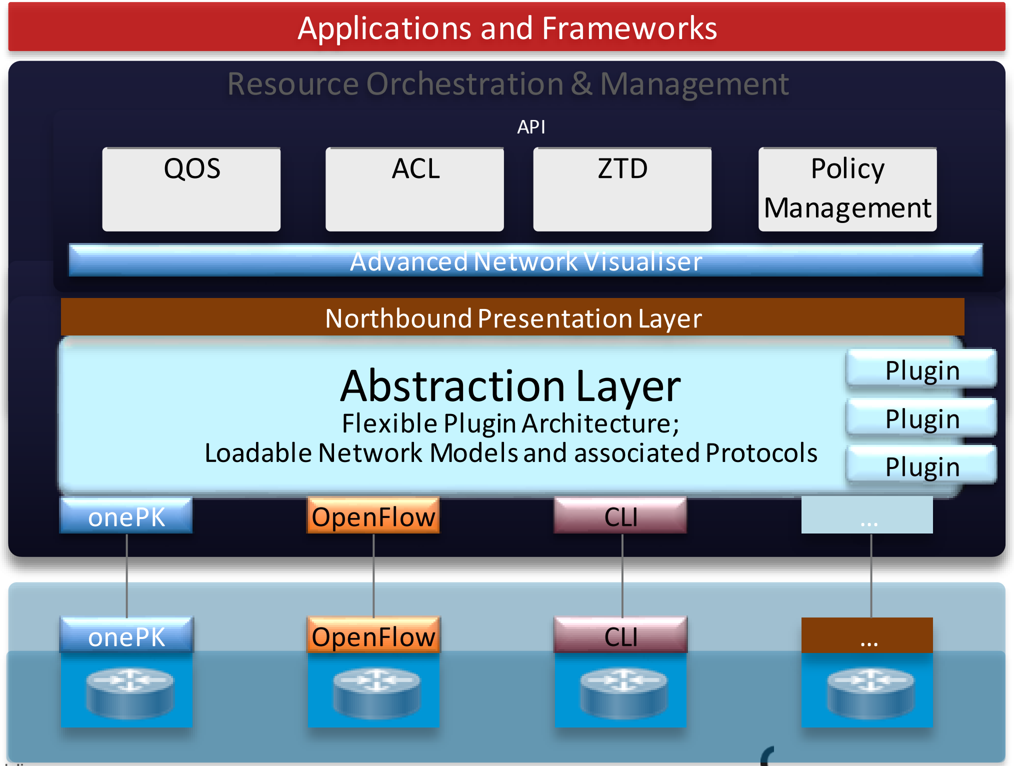
Police Low priority App's

Enable NBAR protocol discovery

SDN - Elementary Infrastructure Functions and beyond

- APIC Enterprise (Application Programming Interface Controller)

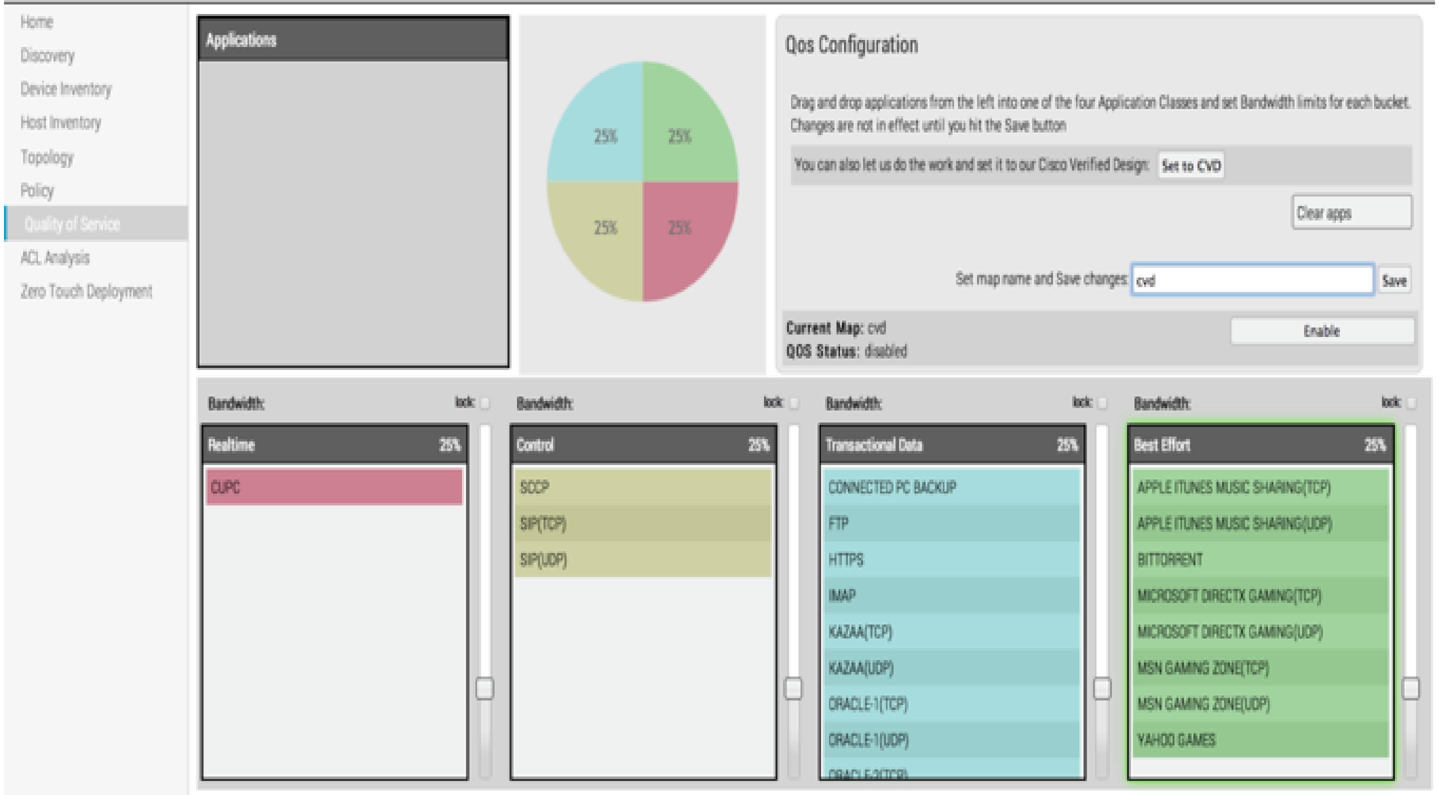
- Launched February 2014
- Enterprise specific set of “turn-key” solutions, focusing
  - Ease of Operations / Simplicity
  - Consistent Network Behaviour
  - Brownfield and Greenfield
  - Application Visibility and Control
- Examples
  - Inventory/Topology:
  - ACL Management
  - easyQoS


Applications and Frameworks
Resource Orchestration & Management
API
QOS
ACL
ZTD
Policy Management
Advanced Network Visualiser
Northbound Presentation Layer
Abstraction Layer
Flexible Plugin Architecture;
Loadable Network Models and associated Protocols
Plugin
Plugin
Plugin
onePK
OpenFlow
CLI
...
onePK
OpenFlow
CLI
...

Orchestration, Control, Management

Example: APIC Enterprise - EasyQoS

- Apps
- Wide range of product support
- Can demo 4 Classes now
- Mapping
  - CVD
  - Custom



Qos Configuration

Drag and drop applications from the left into one of the four Application Classes and set Bandwidth limits for each bucket. Changes are not in effect until you hit the Save button

You can also let us do the work and set it to our Cisco Verified Design: Set to CVD

Clear apps

Set map name and Save changes: cvd Save

Current Map: cvd
QOS Status: disabled

Enable

Bandwidth: lock: □

Realtime 25%
- CUPC

Bandwidth: lock: □

Control 25%
- SCCP
- SIP(TCP)
- SIP(UDP)

Bandwidth: lock: □

Transactional Data 25%
- CONNECTED PC BACKUP
- FTP
- HTTPS
- IMAP
- KAZAA(TCP)
- KAZAA(UDP)
- ORACLE-1(TCP)
- ORACLE-1(UDP)
- ORACLE-2(TCP)

Bandwidth: lock: □

Best Effort 25%
- APPLE ITUNES MUSIC SHARING(TCP)
- APPLE ITUNES MUSIC SHARING(UDP)
- BITTORRENT
- MICROSOFT DIRECTX GAMING(TCP)
- MICROSOFT DIRECTX GAMING(UDP)
- MSN GAMING ZONE(TCP)
- MSN GAMING ZONE(UDP)
- YAHOO GAMES

Campus QoS Design for Medianet References

Cisco Business Video Solutions
http://www.cisco.com/en/US/netsol/ns813/networking_solutions_solution_segment_home.html

Cisco Visual Networking Index
http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html

Overview of a Medianet Architecture
http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/vrn.html

Enterprise Medianet Quality of Service Design 4.0
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html

Medianet Campus QoS Design 4.0
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html

This Is What We Got To…

Classify the Traffic

```
class-map match-any VOICE_CLASS
  match  dscp ef
```

Apply a Policy to the Traffic

```
policy-map QOS_POLICY
  class VOICE_CLASS
    priority 1000
```

Apply the Policy

```
interface  GigabitEthernet0/0
  service-policy output  QOS_POLICY
```

Why Do We Need QoS?

- QoS is necessary where ever there is the possibility of congestion
- Explosion of video and rich-media applications are requiring a re-engineering of network QoS policies
- Keep it simple

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-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 http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 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

Thank you.

cisco