Интегрированные функции безопасности и унифицированных коммуникаций. Лучшие практики и рекомендации по настройке. Часть 2

Юрий Дышлевой
Системный инженер, CCIE

22.04.2021

cisco Live!

cisco

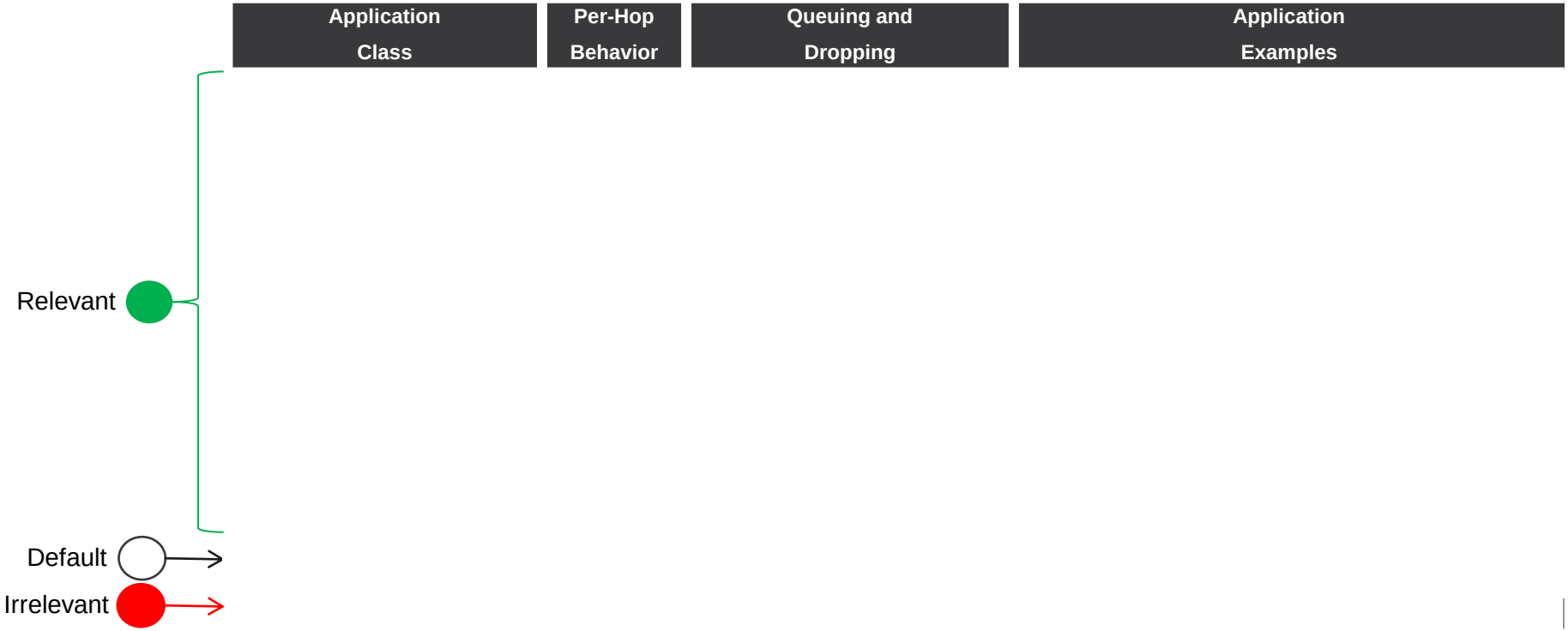
Agenda

- **WAN / VPN QoS Design**
- Integrated Voice. CUBE


Introduction to
Strategic QoS Design

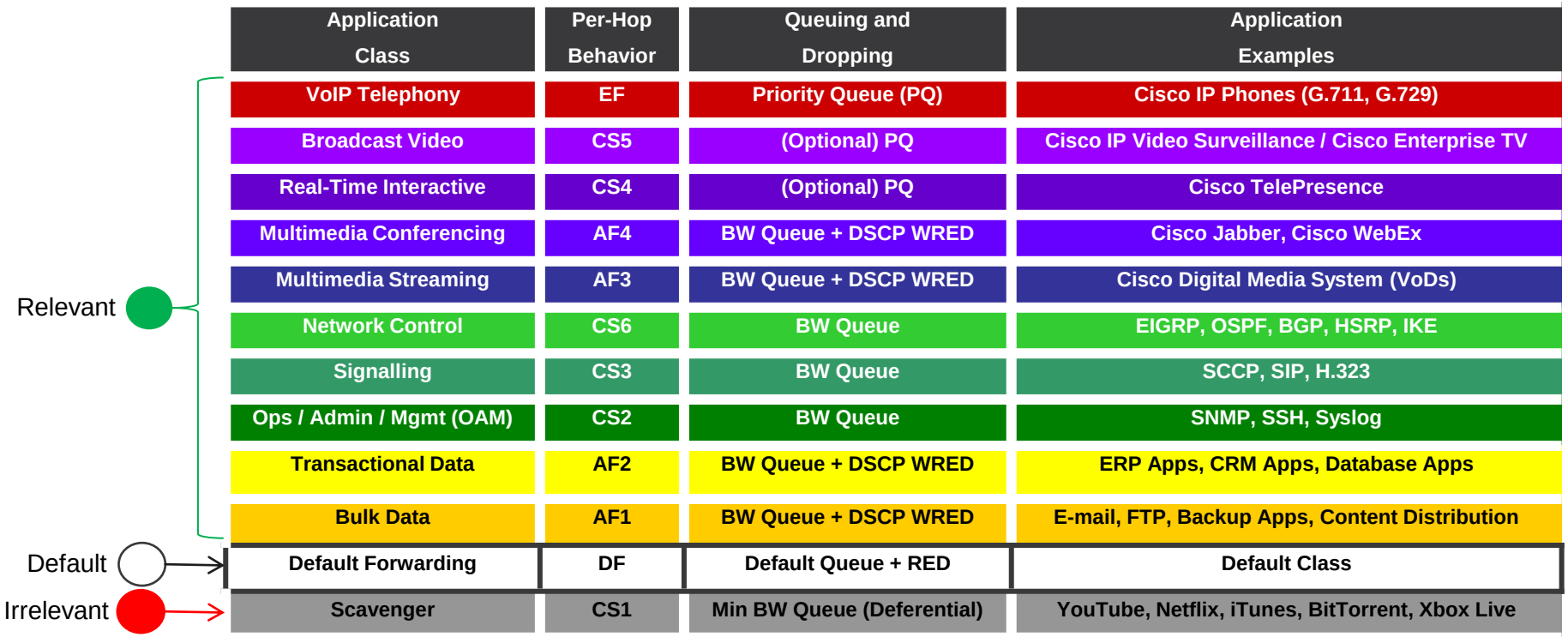
Translating Business-Relevance to QoS Treatments

Apply RFC 4594-based Marking / Queuing / Dropping Treatments



Translating Business-Relevance to QoS Treatments

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

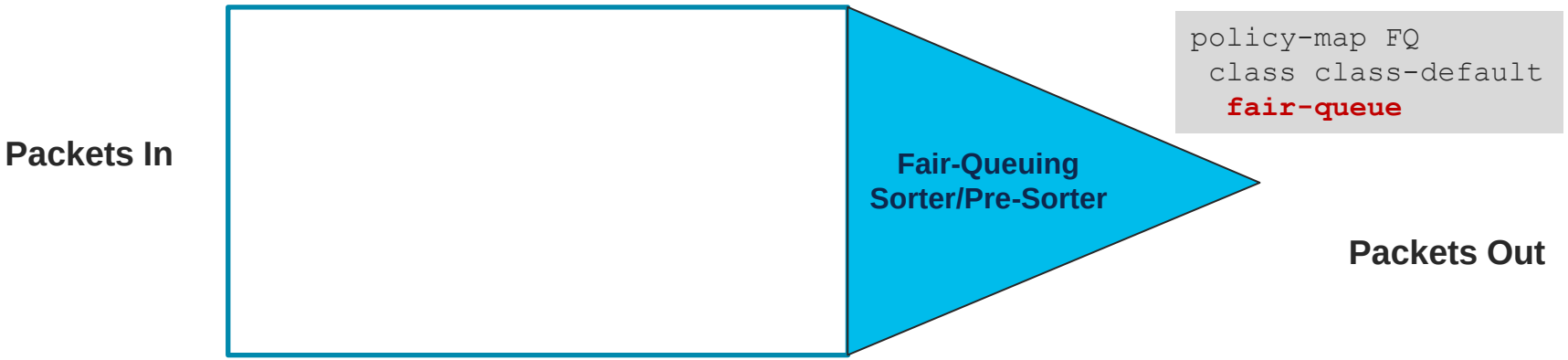


Application Class	Per-Hop Behavior	Queuing and Dropping	Application Examples
VoIP Telephony	EF	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Real-Time Interactive	CS4	(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	AF4	BW Queue + DSCP WRED	Cisco Jabber, Cisco WebEx
Multimedia Streaming	AF3	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6	BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
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
Default Forwarding	DF	Default Queue + RED	Default Class
Scavenger	CS1	Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

WAN Edge QoS Design

QoS Tools Review: Queuing and Dropping Tools

(Flow-Based) Fair-Queuing

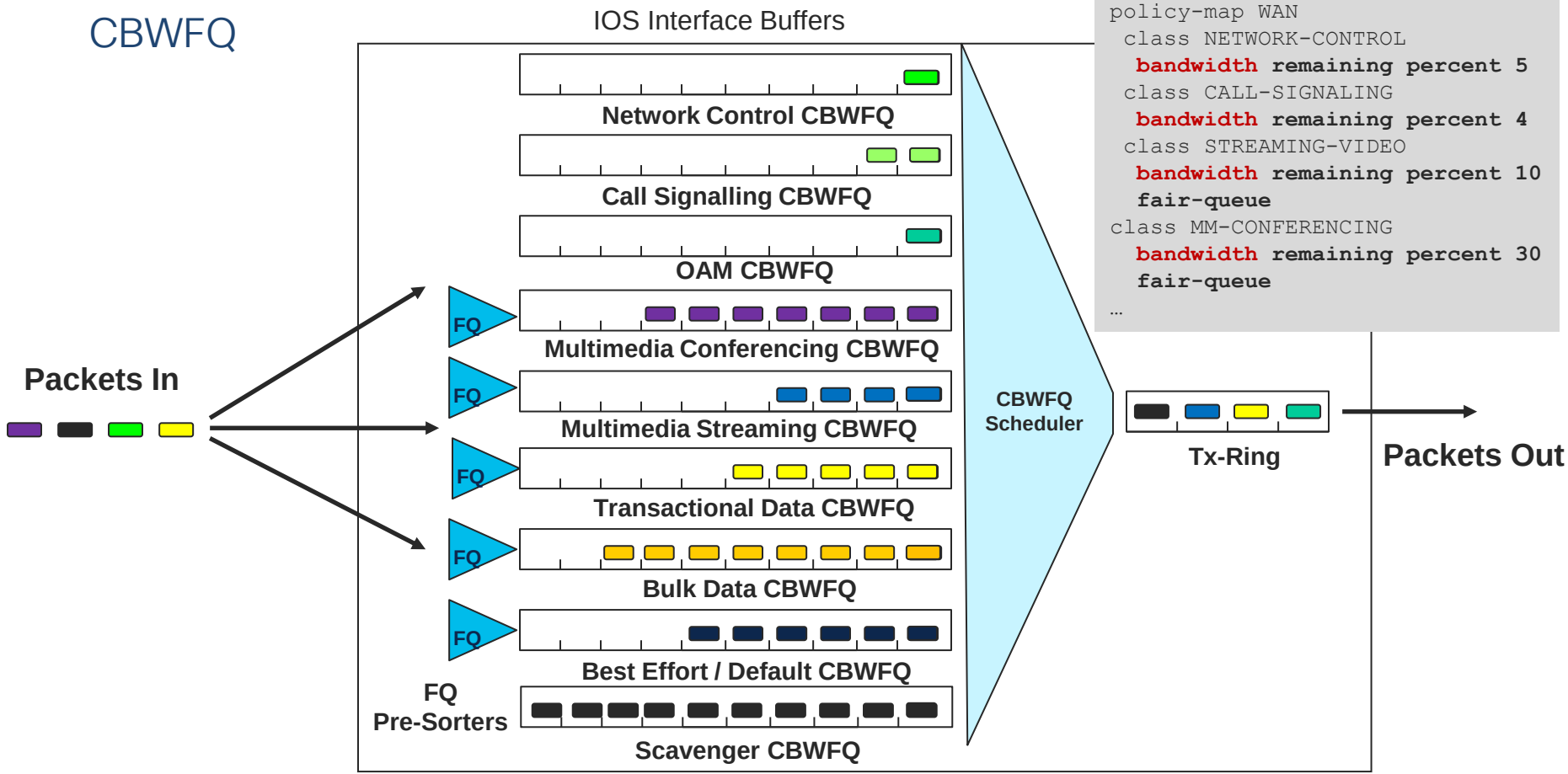



```
policy-map FQ
 class class-default
  fair-queue
```

A flow is defined by five matching tuples:
Source Address + Source Port
Destination Address + Destination Port
Layer 4 Protocol (TCP or UDP)

QoS Tools Review: Queuing and Dropping Tools

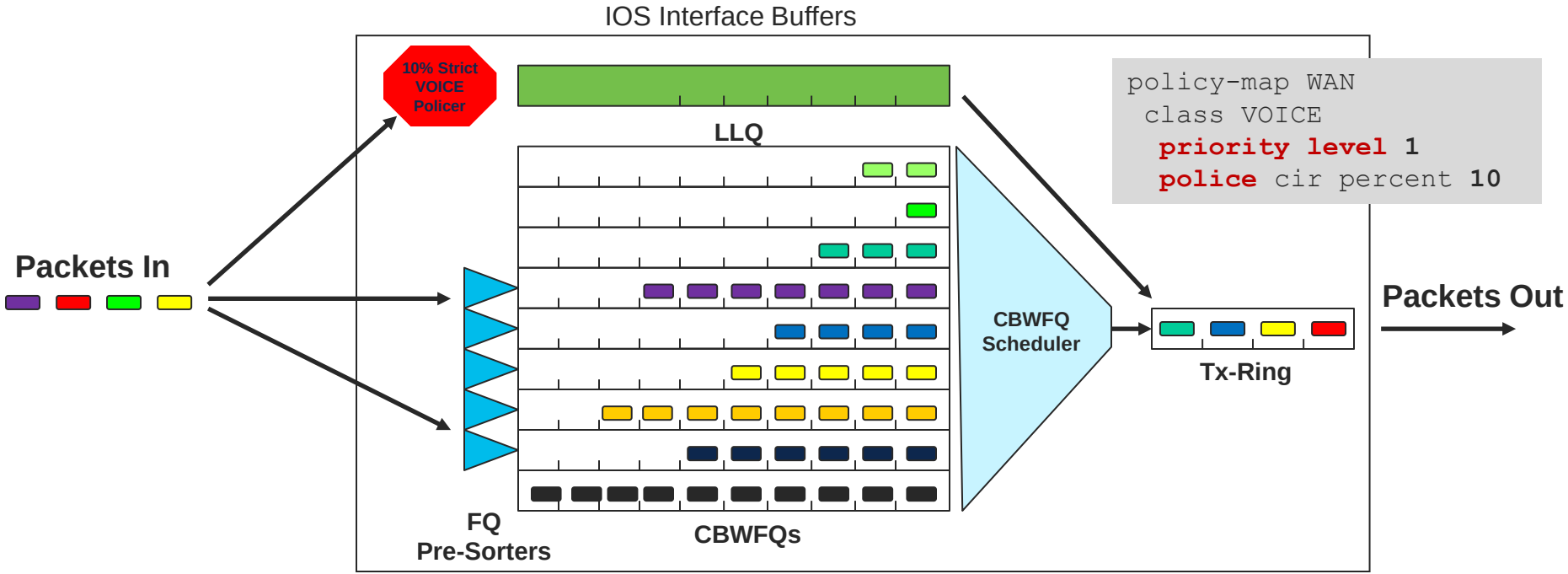
CBWFQ




```
policy-map WAN
 class NETWORK-CONTROL
  bandwidth remaining percent 5
 class CALL-SIGNALING
  bandwidth remaining percent 4
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  fair-queue
class MM-CONFERENCING
  bandwidth remaining percent 30
  fair-queue
…
```

QoS Tools Review: Queuing and Dropping Tools

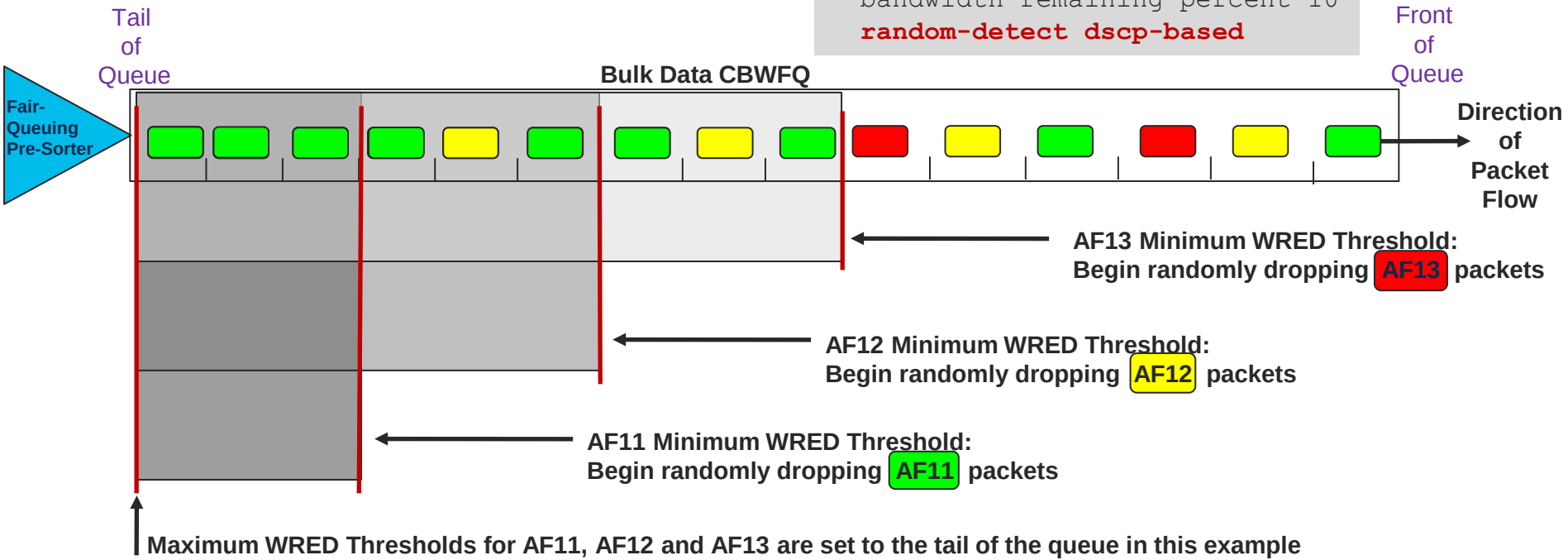
LLQ: Single-LLQ Operation and Configuration



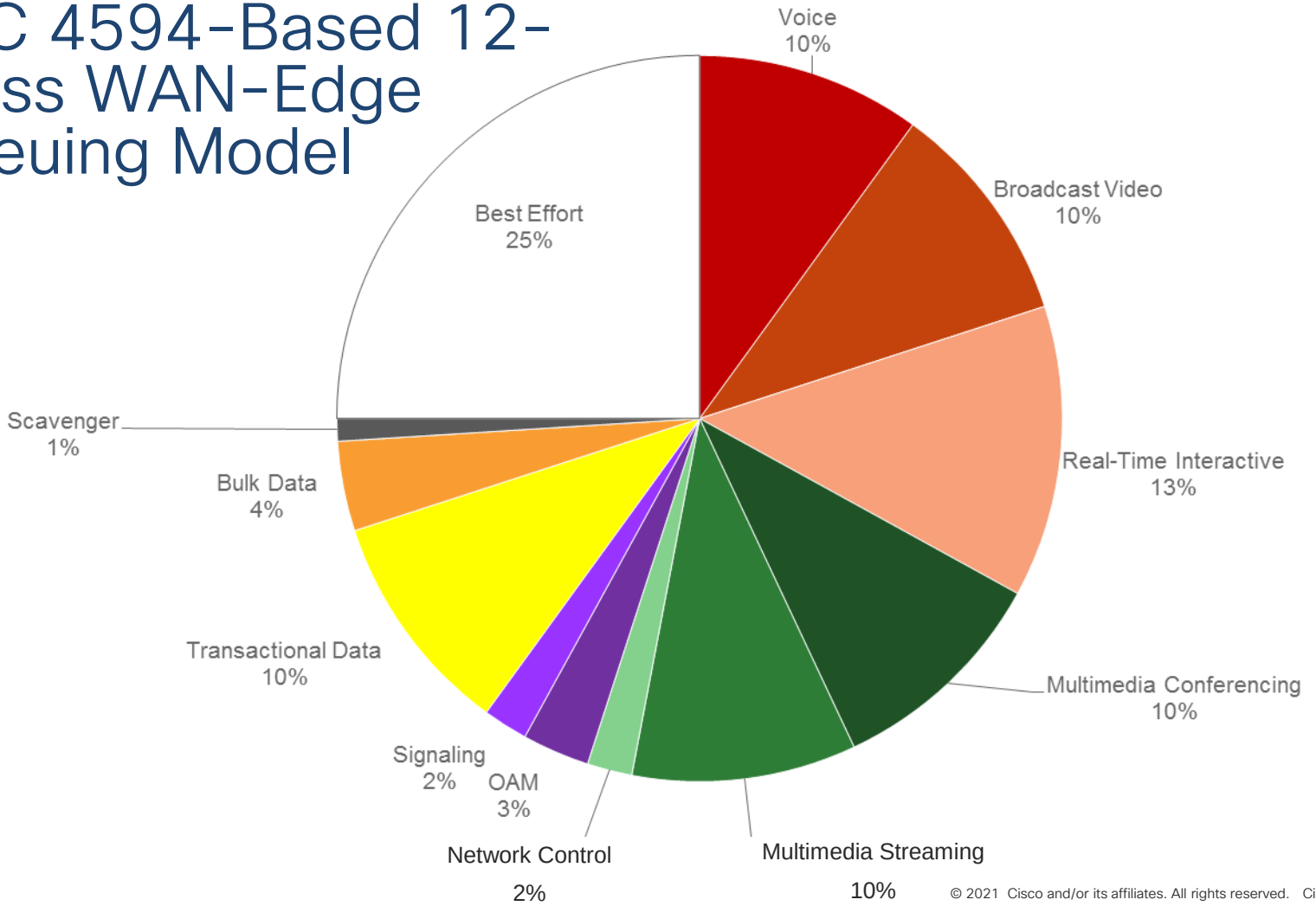
QoS Tools Review: Queuing and Dropping Tools

DSCP-Based WRED

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



RFC 4594-Based 12-Class WAN-Edge Queuing Model



RFC 4594-Based 12-Class Queuing Model Configuration

```
class-map match-all VOICE-DSCP
   match dscp ef
class-map match-all BROADCAST_VIDEO-DSCP
   match dscp cs5
class-map match-all REALTIME_INTERACTIVE-DSCP
   match dscp cs4
class-map match-all NETWORK-CONTROL-DSCP
   match cs6
class-map match-all SIGNALING-DSCP
   match cs3
class-map match-all OAM-DSCP
   match cs2
class-map match-all MULTIMEDIA_CONFERENCING-DSCP
   match dscp af41
class-map match-all MULTIMEDIA_STREAMING-DSCP
   match dscp af31
class-map match-all TRANSACTIONAL-DATA-DSCP
   match dscp af21
class-map match-all BULK-DATA-DSCP
   match dscp af11
class-map match-all SCAVENGER-DSCP
   match dscp cs1
```

Note: Appending “-DSCP” to the class-map names distinguishes WAN-Edge egress-queuing class-maps (matching on DSCP values) from the LAN-Edge ingress class-maps (matching via NBAR2).

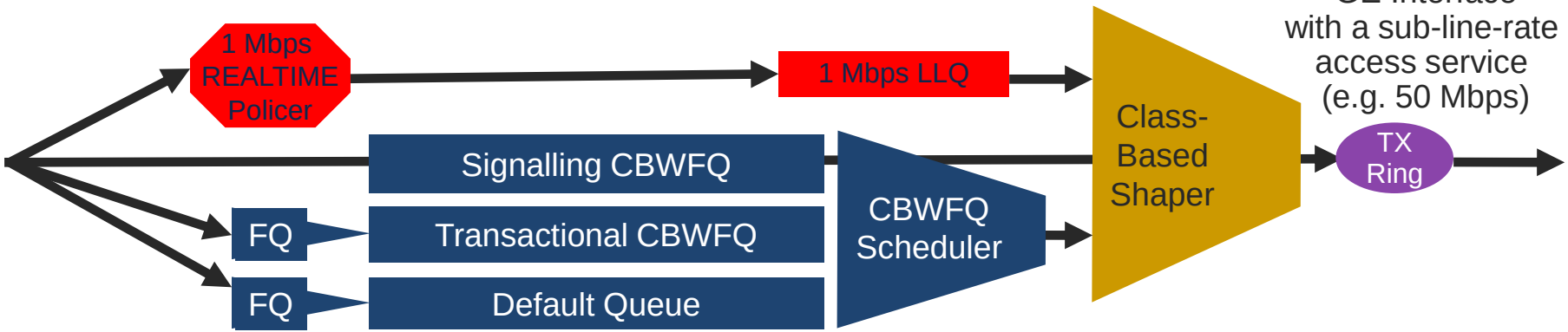
```
policy-map WAN_EDGE-QUEUING
 class VOICE-DSCP
  priority percent 10
 class BROADCAST_VIDEO-DSCP
  priority percent 10
 class REALTIME_INTERACTIVE-DSCP
  priority percent 13
 class NETWORK-CONTROL-DSCP
  bandwidth percent 2
 class SIGNALING-DSCP
  bandwidth percent 2
 class OAM-DSCP
  bandwidth percent 3
 class MULTIMEDIA_CONFERENCING-DSCP
  bandwidth percent 10
  fair-queue
  random-detect dscp-based
 class MULTIMEDIA_STREAMING-DSCP
  bandwidth percent 10
  fair-queue
  random-detect dscp-based
class TRANSACTIONAL-DATA-DSCP
  bandwidth percent 10
  fair-queue
  random-detect dscp-based
class BULK-DATA-DSCP
  bandwidth percent 4
  fair-queue
  random-detect dscp-based
class SCAVENGER-DSCP
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  fair-queue
  random-detect dscp-based
```

What Changes for Sub-Line-Rate Interfaces?

```
policy-map QUEUING
 class REALTIME
  priority 1000
 class SIGNALING
  bandwidth x
 class TRANSACTIONAL
  bandwidth y…
class class-default
  fair-queue
```

```
policy-map HQoS-50MBPS
 class class-default
  shape average 50000000
  service-policy QUEUING
```

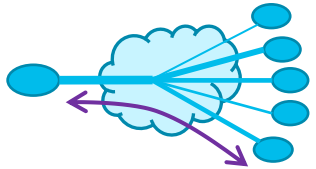
- Queuing policies *will not* engage unless the interface is congested
- A shaper will guarantee that traffic will not exceed the contracted rate
- A nested queuing policy will force queuing to engage at the contracted sub-line-rate to prioritise packets prior to shaping



VPN QoS Design

Aggregate Priority Load

IPSec VPN Design Recommendation

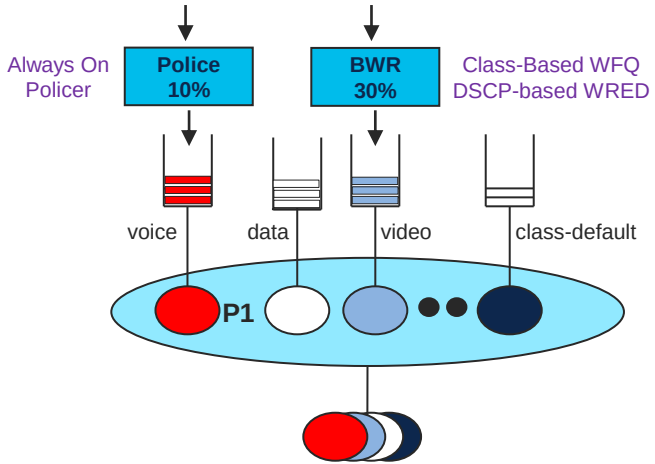


- For Voice, use an Always On policer, rather than a Conditional policer

```
class VOICE
 priority level 1
 police cir percent 10
```

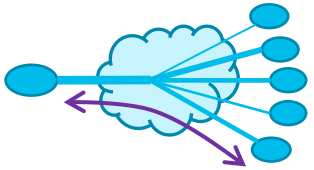
- For Video, use a Bandwidth Remaining Percent (BWR) queue with DSCP-based WRED, rather than a level 2 Priority queue

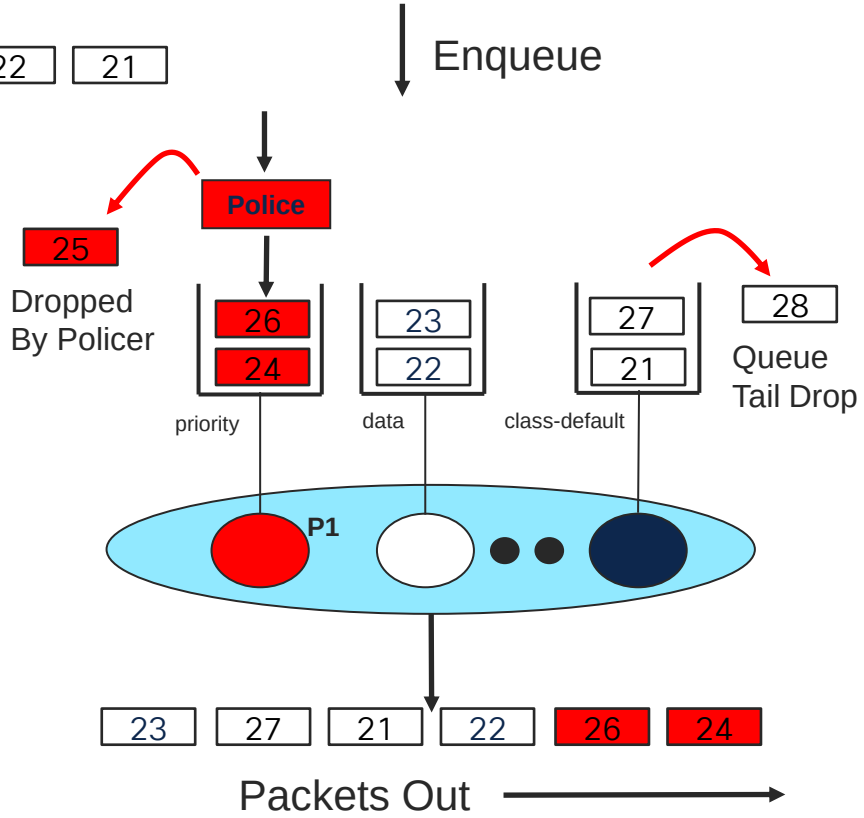
```
class INTERACTIVE-VIDEO
 bandwidth remaining percent 30
 random-detect dscp-based
```



IPsec Anti-Replay and QoS

IPSec VPN Design Recommendation





- On a congested interface, a low-priority packet may be delayed by queuing, and then, arrive at the next router after the anti-replay window has been exceeded
- Also, if an encrypted packet arrives out of sequence by the window size (default is 64 packets), the packet is dropped
- Increasing the anti-replay window size has no impact on throughput or security
- The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed

Use the maximum replay window-size of 1024 for each supported platform

```
crypto ipsec security-association replay window-size 1024
```

IPSec VPN Egress QoS Models

Example: Combining 12 Classes into an 8-Class Model

Application	DSCP
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF41
Real-Time Interactive	CS4
Multimedia Streaming	AF31
Signalling	CS3
Transactional Data	AF21
Network Management (OAM)	CS2
Bulk Data	AF11
Scavenger	CS1
Best Effort	DF

8-Class Model
VOICE PQ-10%
NET-CTRL 5% BWR
INTERACTIVE-VIDEO 30% BWR
STREAMING-VIDEO 10% BWR
CALL-SIGNALLING 4% BWR
CRITICAL-DATA 25% BWR
SCAVENGER—1% BWR
DEFAULT 25% BWR

PQ = Priority Queue
BWR = Bandwidth Remaining

Note: Bandwidth Remaining Percentages must equal 100%

IPSec VPN 8-Class Egress Queuing Model

Child Queuing Policy

8-Class Queuing Model Class-Maps

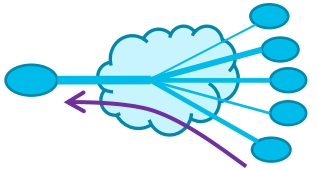
```
class-map match-any VOICE-DSCP
 match dscp ef
class-map match-any INTERACTIVE-VIDEO-DSCP
 match dscp cs4 af41 af42 af43
class-map match-any STREAMING-VIDEO-DSCP
 match dscp cs5 af31 af32 af33
class-map match-any NETWORK-CONTROL-DSCP
 match dscp cs6
class-map match-any SIGNALING-DSCP
 match dscp cs3
class-map match-any CRITICAL-DATA-DSCP
 match dscp cs2 af11 af12 af13 af21 af22 af23
class-map match-any SCAVENGER-DSCP
 match dscp cs1
```

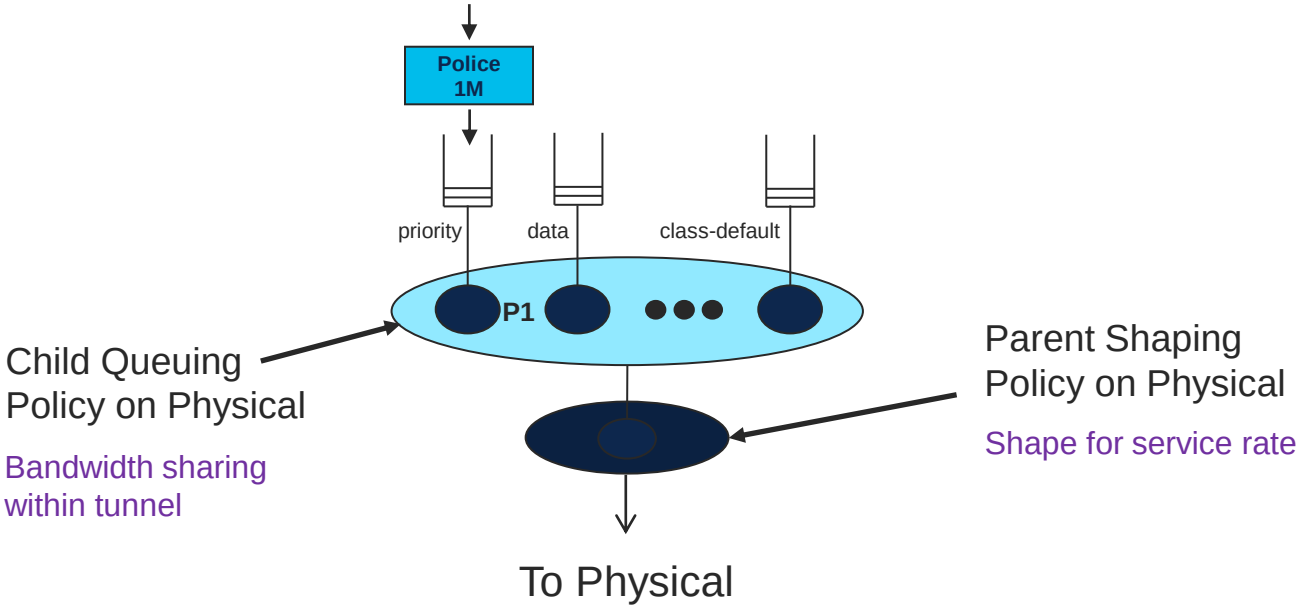
8-Class Queuing Policy-Map

```
policy-map EDGE-QUEUING
 class VOICE-DSCP
  priority level 1
  police cir percent 10
 class INTERACTIVE-VIDEO-DSCP
  bandwidth remaining percent 30
  random-detect dscp-based
 class STREAMING-VIDEO-DSCP
  bandwidth remaining percent 10
  random-detect dscp-based
 class NETWORK-CONTROL-DSCP
  bandwidth remaining percent 5
 class SIGNALING-DSCP
  bandwidth remaining percent 4
 class CRITICAL-DATA-DSCP
  bandwidth remaining percent 25
  random-detect dscp-based
 class SCAVENGER-DSCP
  bandwidth remaining percent 1
class class-default
  bandwidth remaining percent 25
  random-detect
```

Branch QoS Scheduling Hierarchy

Two Levels: Child / Parent





Branch QoS Scheduling Hierarchy

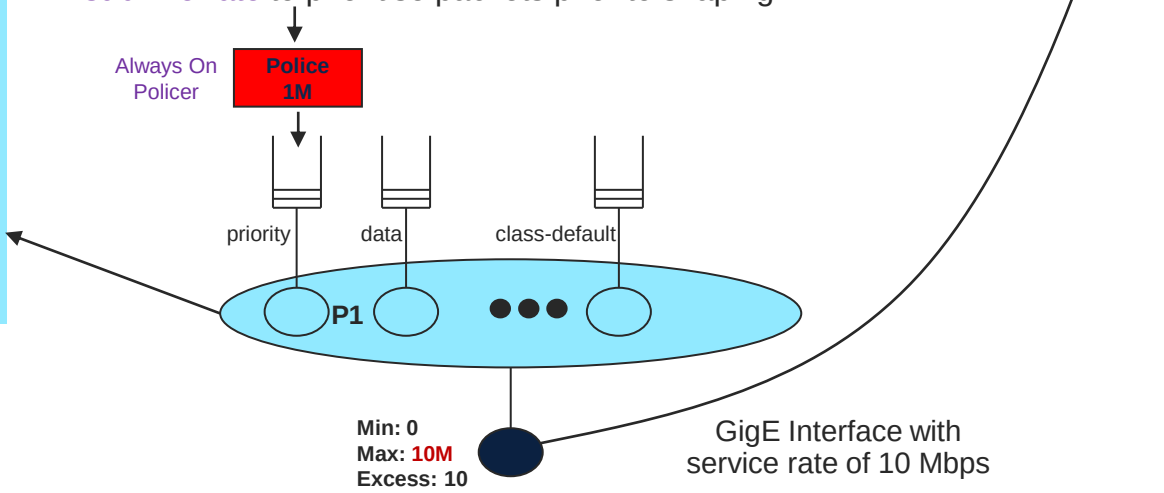
Two Levels: Child / Parent

```
policy-map EDGE-QUEUING
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
 class CALL-SIGNALING
  bandwidth remaining percent 4
 class NET-CTRL
  bandwidth remaining percent 5
 class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
 class SCAVENGER
  bandwidth remaining percent 1
 class VOICE
  priority level 1
  police cir percent 10
 class class-default
  bandwidth remaining percent 25
  random-detect
```

```
policy-map POLICY-TRANSPORT-1
 class class-default
  shape average 10 Mbps
  service-policy EDGE-QUUEING
```

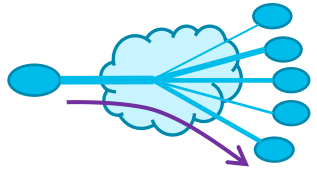
```
interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
```

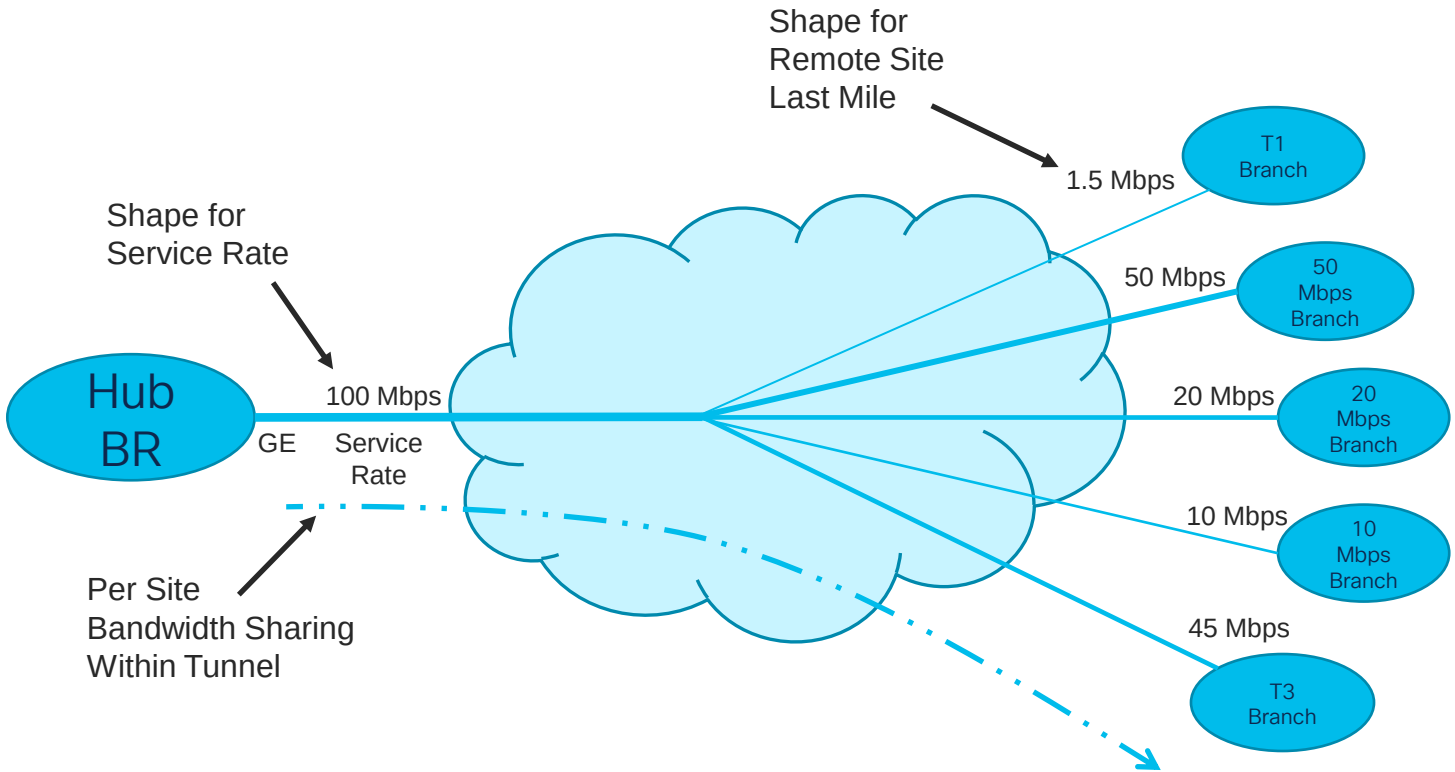
- A shaper will guarantee that traffic will not exceed the contracted rate
- A nested queuing policy will force queuing to engage at the contracted sub-line-rate to prioritise packets prior to shaping



Hub Site QoS Scheduling

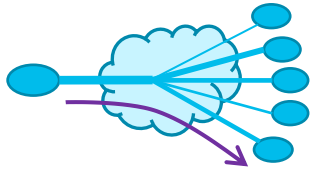
Three Levels: Child / Parent / Grandparent

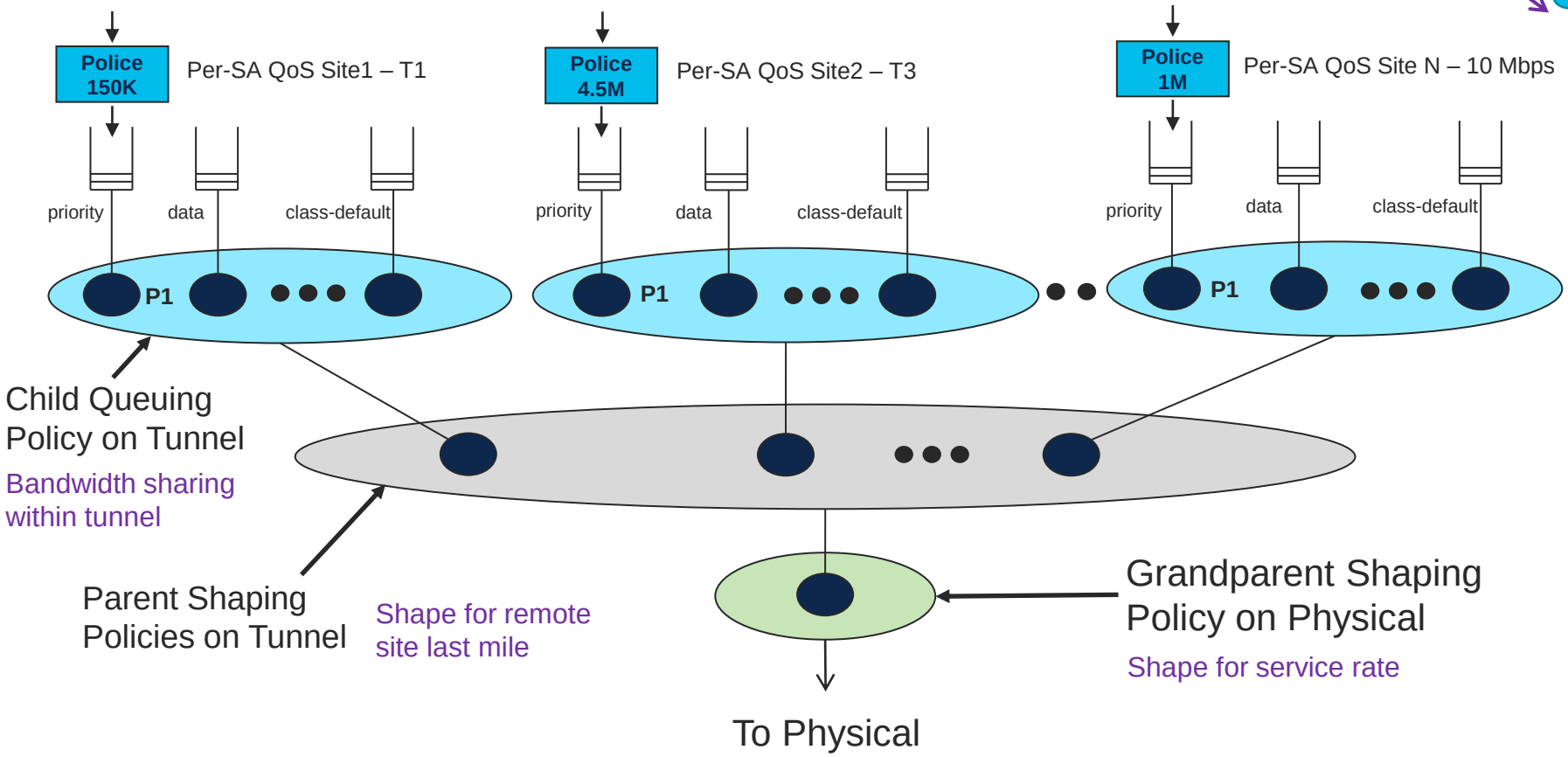




Hub Site QoS Scheduling Hierarchy

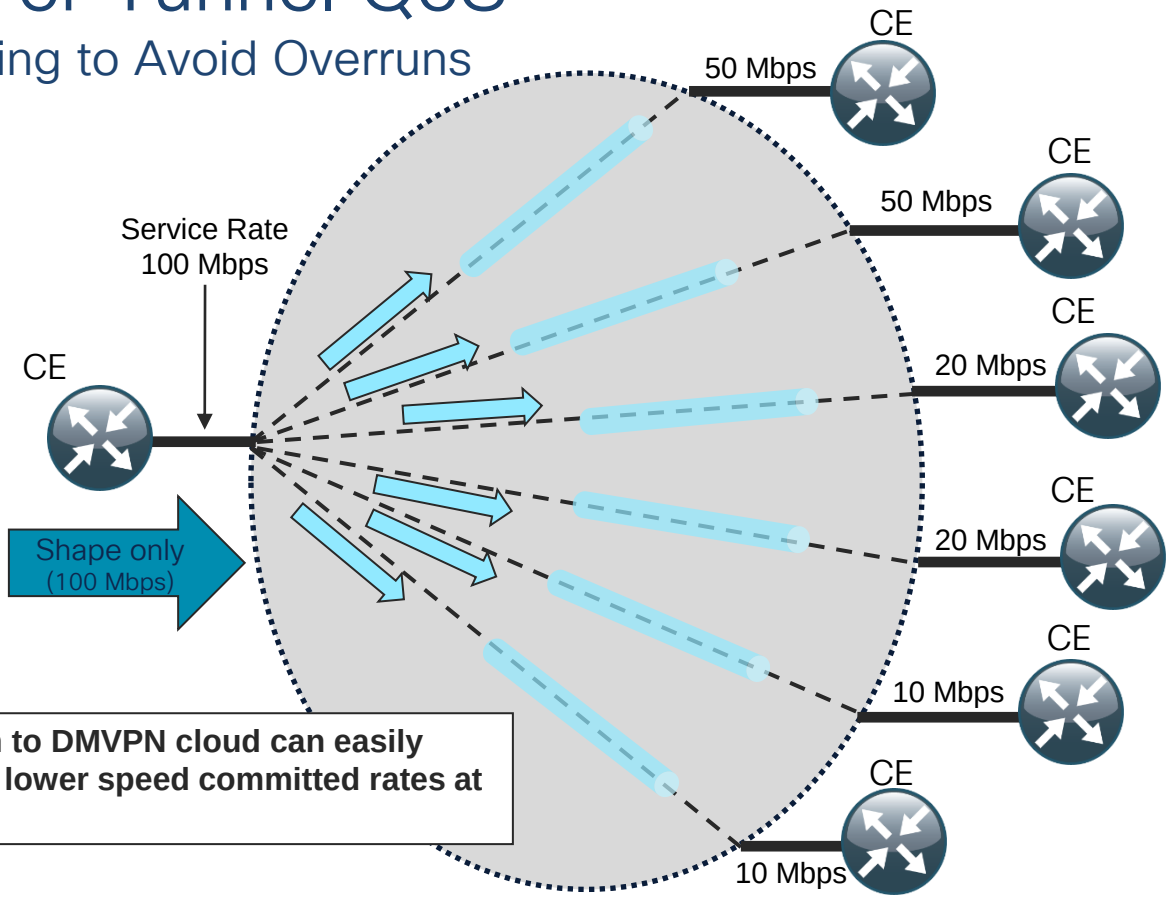
Three Levels: Child / Parent / Grandparent





DMVPN Per Tunnel QoS

Per-Site Shaping to Avoid Overruns



100 Mbps in to DMVPN cloud can easily overrun the lower speed committed rates at spoke sites

DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping

```
policy-map GROUP-50MBPS-POLICY
 class class-default
  shape average 50 Mbps
 bandwidth remaining ratio 50
  service-policy EDGE-QUEUING
```

```
policy-map GROUP-20MBPS-POLICY
 class class-default
  shape average 20 Mbps
  bandwidth remaining ratio 20
  service-policy EDGE-QUEUING
```

```
policy-map GROUP-10MBPS-POLICY
 class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy EDGE-QUEUING
```

Separate parent shaper policies for each remote-site bandwidth

```
policy-map TRANSPORT-1-SHAPE-ONLY
 class class-default
  shape average 100 Mbps
!
interface GigabitEthernet0/0/3
 bandwidth 100000
 service-policy output TRANSPORT-1-SHAPE-ONLY

interface Tunnel10
 bandwidth 100000
 nhrp map group GROUP-10MBPS service-policy output GROUP-10MBPS-POLICY
 nhrp map group GROUP-20MBPS service-policy output GROUP-20MBPS-POLICY
 nhrp map group GROUP-50MBPS service-policy output GROUP-50MBPS-POLICY
```

Signal from the spoke to the hub to use the correct policy for each remote site

Remote Site Tunnel Configurations

10 Mbps spoke

```
interface GigabitEthernet0/0
 bandwidth 100000
 service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
 bandwidth 10000
 nhrp group GROUP-10MBPS
 tunnel source GigabitEthernet0/0
 tunnel vrf TRANSPORT-1
```

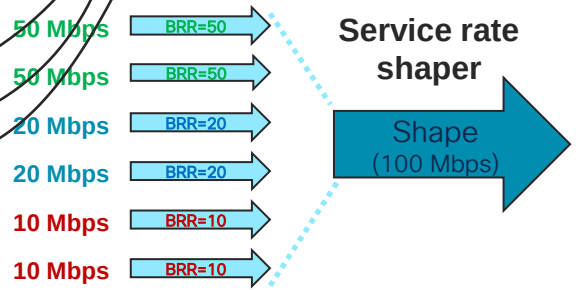
20 Mbps spoke

```
interface GigabitEthernet0/0
 bandwidth 20000
 service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
 bandwidth 20000
 nhrp group GROUP-20MBPS
 tunnel source GigabitEthernet0/0
 tunnel vrf TRANSPORT-1
```

50 Mbps spoke

```
interface GigabitEthernet0/0
 bandwidth 50000
 service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
 bandwidth 50000
 nhrp group GROUP-50MBPS
 tunnel source GigabitEthernet0/0
 tunnel vrf TRANSPORT-1
```

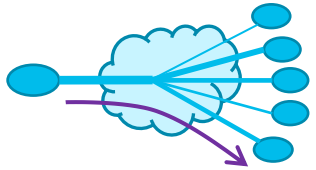
Per-Tunnel shapers



List all available policies as map groups on hub tunnel interface

Add a class-default shape-only policy on the hub physical interface for the service rate

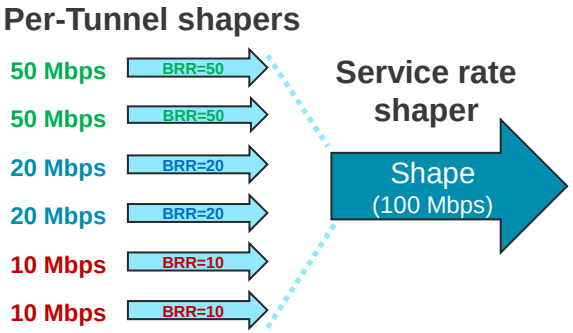
Bandwidth Remaining Ratio
Details



Bandwidth Remaining Ratio (BRR) provides proportional sharing to parent shapers during times of congestion.

If you over-subscribe your hub BR outbound bandwidth with per-tunnel policies that exceed the service rate, the BRR commands on each parent policy means they will get their "fair share" of the remaining bandwidth as compared to the other branch sites.

- If all the per-tunnel BW amounts are 5 Mbps or greater, we use a BRR value of BW / 1 Mbps. (i.e. 10 Mbps is BRR of 10, 50 Mbps is BRR of 50, etc.)
- If any of the per-tunnel BW values are less than 5 Mbps, we use a BRR value of BW / 100 Kbps. (i.e. 3 Mbps is BRR of 30, 1.5 Mbps is BRR of 15, etc.)



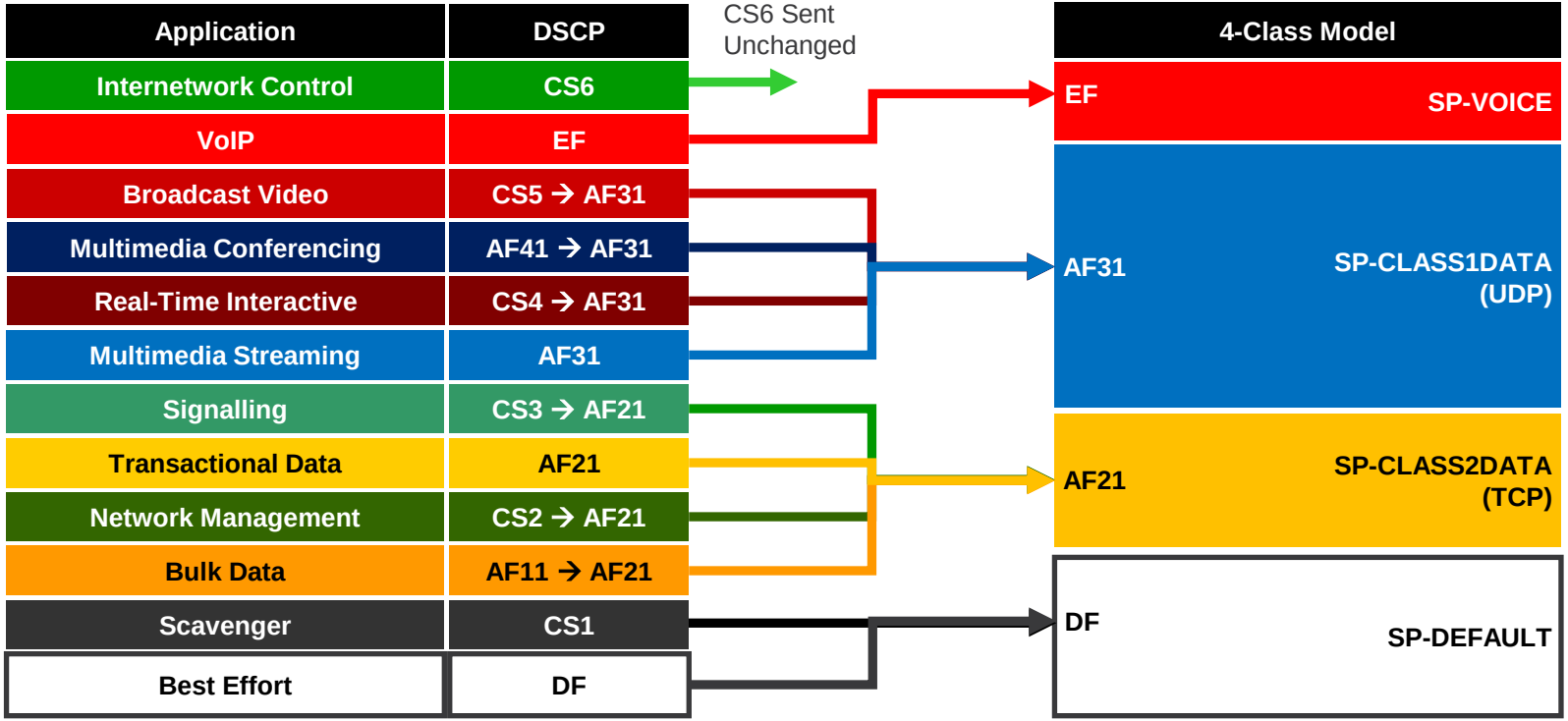
When the total bandwidth exceeds 100 Mbps, each of the per-tunnel shapers will get their fair share based on their BRR values.

Example:
50 Mbps site gets 50 / 160 or 31.25%
20 Mbps site gets 20 / 160 or 12.5%
10 Mbps site gets 10 / 160 or 6.25%

Enterprise to Service-Provider QoS Mapping

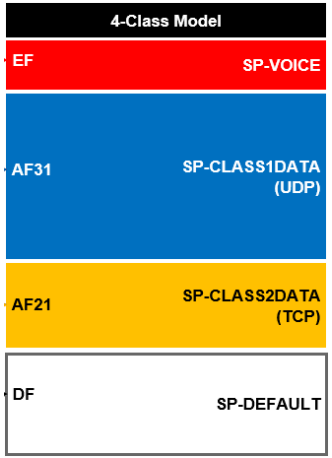
Enterprise to SP Mapping

Example: 4-Class SP Model



4-Class SP QoS Model Configuration

Non-Tunneled Traffic




```
policy-map EDGE-QUEUING
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  set dscp af31
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  set dscp af31
 class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp cs6
 class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp af21
  class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  set dscp af21
 class SCAVENGER
  bandwidth remaining percent 1
  set dscp default
 class VOICE
  priority level 1
  police cir percent 10
  set dscp ef
 class class-default
  bandwidth remaining percent 25
  random-detect
  set dscp default
```

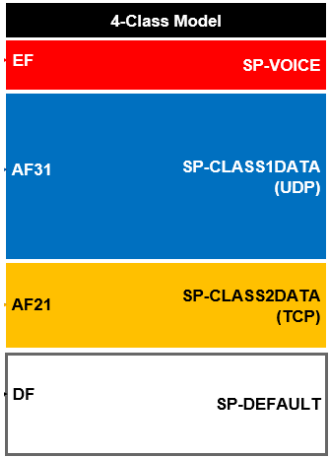
Branch Router:

```
policy-map POLICY-TRANSPORT-1
 class class-default
  shape average 10 Mbps
  service-policy EDGE-QUEUING
```

```
interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Tunneled Traffic




```
policy-map EDGE-QUEUING
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  set dscp tunnel af31
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  set dscp tunnel af31
 class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
 class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
  class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  set dscp tunnel af21
 class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel default
 class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
 class class-default
  bandwidth remaining percent 25
  random-detect
  set dscp tunnel default
```

Hub Router:

```
policy-map GROUP-10MBPS-POLICY
 class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
   service-policy EDGE-QUEUING
```

```
interface Tunnel10
 bandwidth <service-rate>
 nhrp map group GROUP-10MBPS service-policy
        output GROUP-10MBPS-POLICY
```

Branch Router:

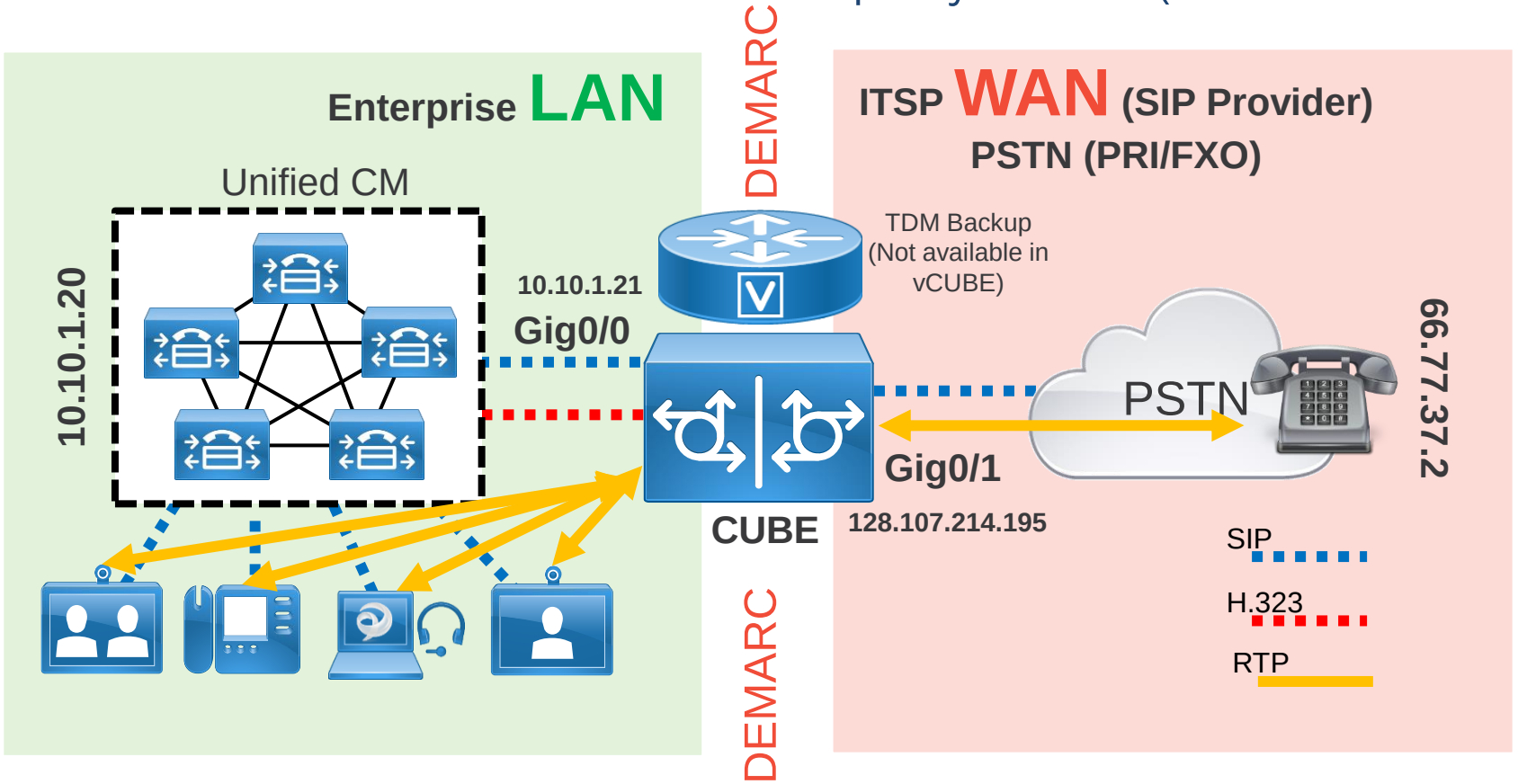
```
interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
 bandwidth 10000
 nhrp group GROUP-10MBPS
 tunnel source GigabitEthernet0/0
 tunnel vrf TRANSPORT-1
```

Agenda

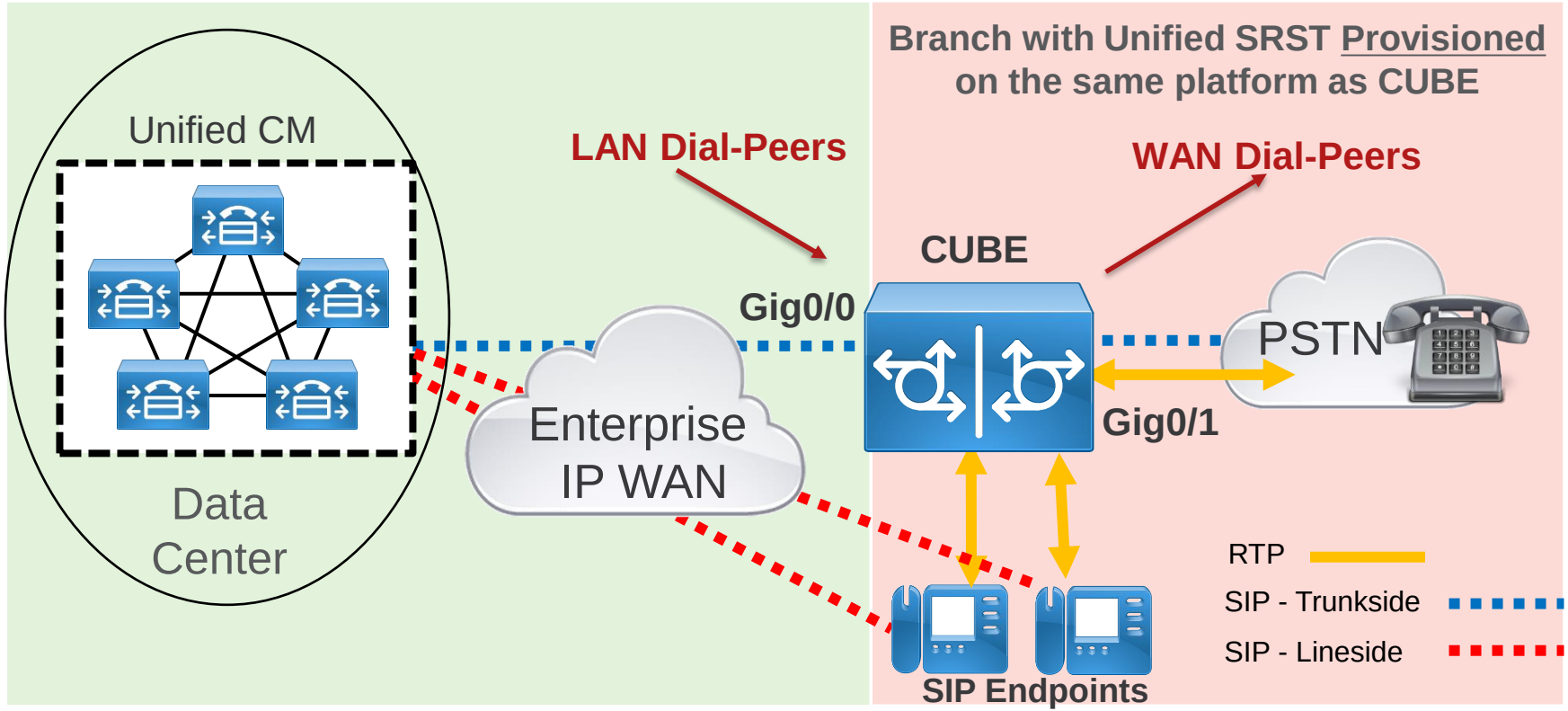
- WAN / VPN QoS Design
- Integrated Voice. CUBE

CUBE Overview and Deployments

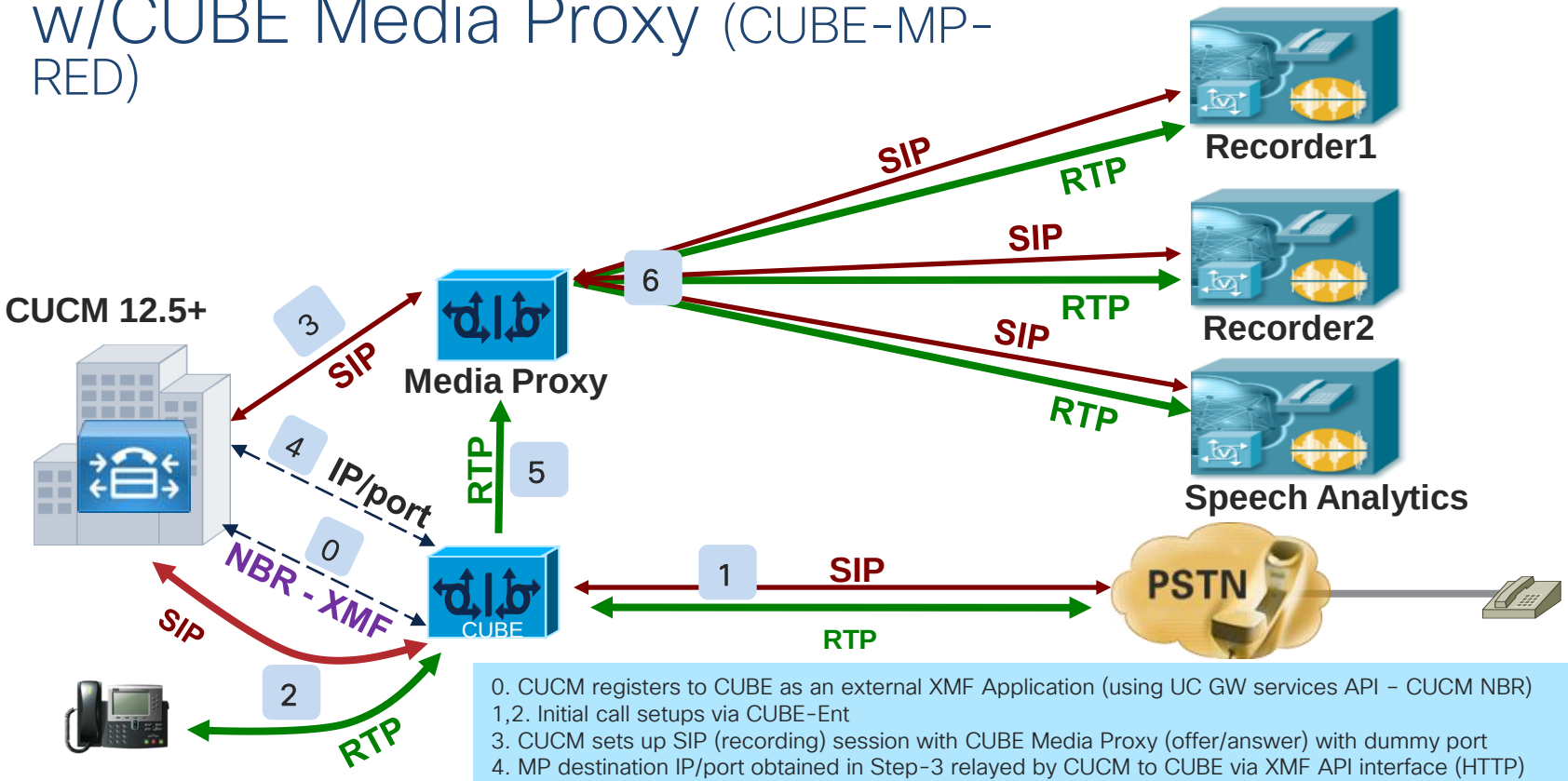
On-Prem Collaboration Deployment (CUBE-T-STD)



Branch CUBE Deployment with SRST Provisioned (CUBE-T-STD)



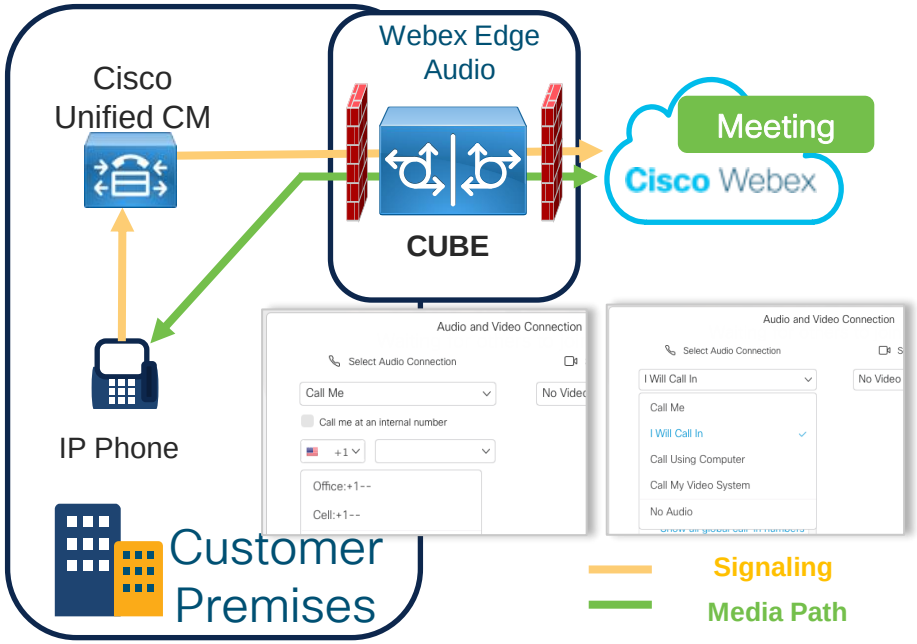
Enabling compliance recording w/CUBE Media Proxy (CUBE-MP-RED)



0. CUCM registers to CUBE as an external XMF Application (using UC GW services API – CUCM NBR)
1,2. Initial call setups via CUBE-Ent
3. CUCM sets up SIP (recording) session with CUBE Media Proxy (offer/answer) with dummy port
4. MP destination IP/port obtained in Step-3 relayed by CUCM to CUBE via XMF API interface (HTTP)
5. CUBE-Ent starts to fork media streams to the MP (target ip/port received in Step-4). MP accepts RTP because of Media latching in the inbound leg from CUCM
6. MP sets up SIP recording sessions with the 3 Recorders for multi-fork.
The ingress media stream from CUBE-Ent is then multi-forked by MP towards the 3 recorders simultaneously using the destination ip/ports as negotiated in the SIP offer/answer b/w MP and the Recorders.

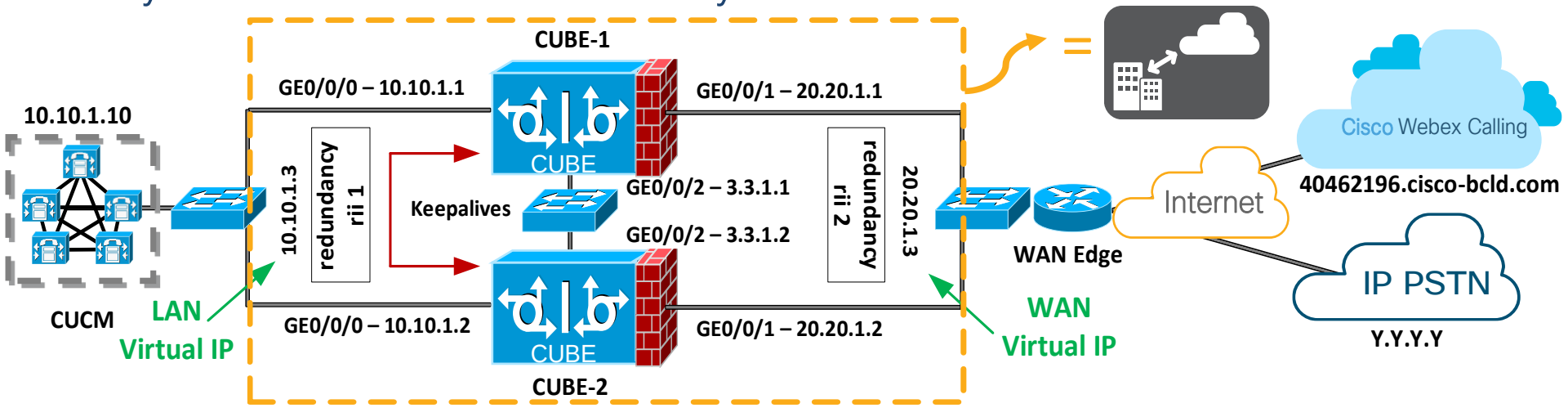
Deploying Cisco Webex Edge Audio w/CUBE

High level overview



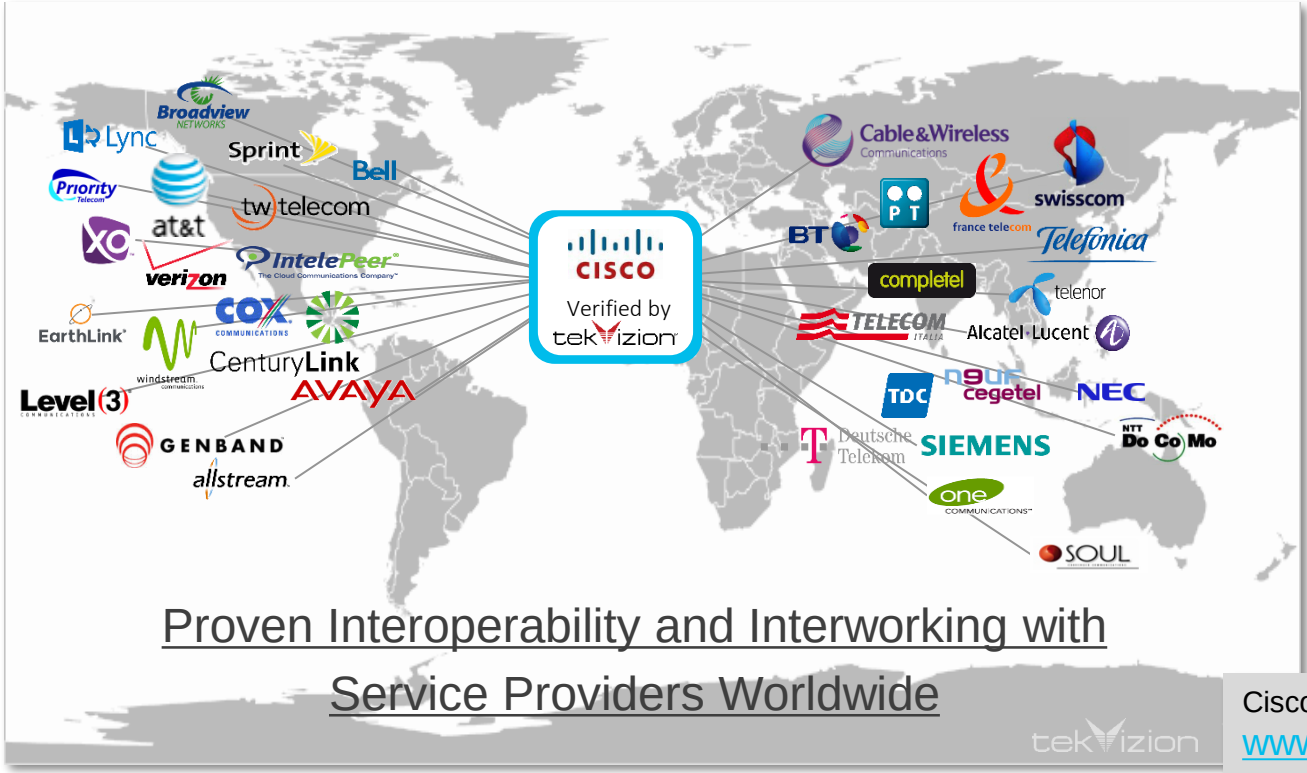
1. On-premises telephone dials the Webex meeting number or gets a call back from the Webex meeting to get connected by audio into the meeting.
2. Signaling is routed via the on-premises call control device (Unified CM) through the CUBE to Webex Meetings audio service.
3. Audio media (the sound) is routed from the Webex meeting to CUBE and then to the on-premises phone for callback and the reverse for call in.

CUBE High Availability as Local Gateway
Layer 2 box-to-box redundancy



- LGW HA solution with layer 2 box-to-box redundancy for call preservation
  - CUBE HA Active/standby model using virtual IP addresses
  - Applicable to ISR 4K and vCUBE only
  - Acts as a single Local Gateway from Webex Calling point of view
- Support for Webex Calling deployments available from IOS-XE 16.12.2
- LGW HA cannot have TDM or analog interfaces co-located

CUBE Interoperability Portal for application note

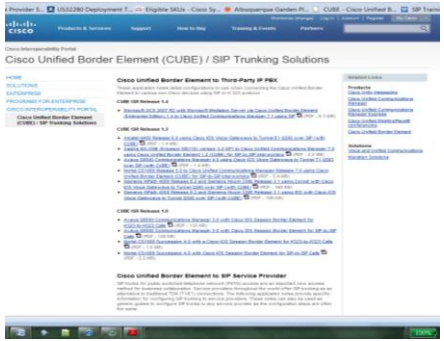


Proven Interoperability and Interworking with Service Providers Worldwide

tekVizion

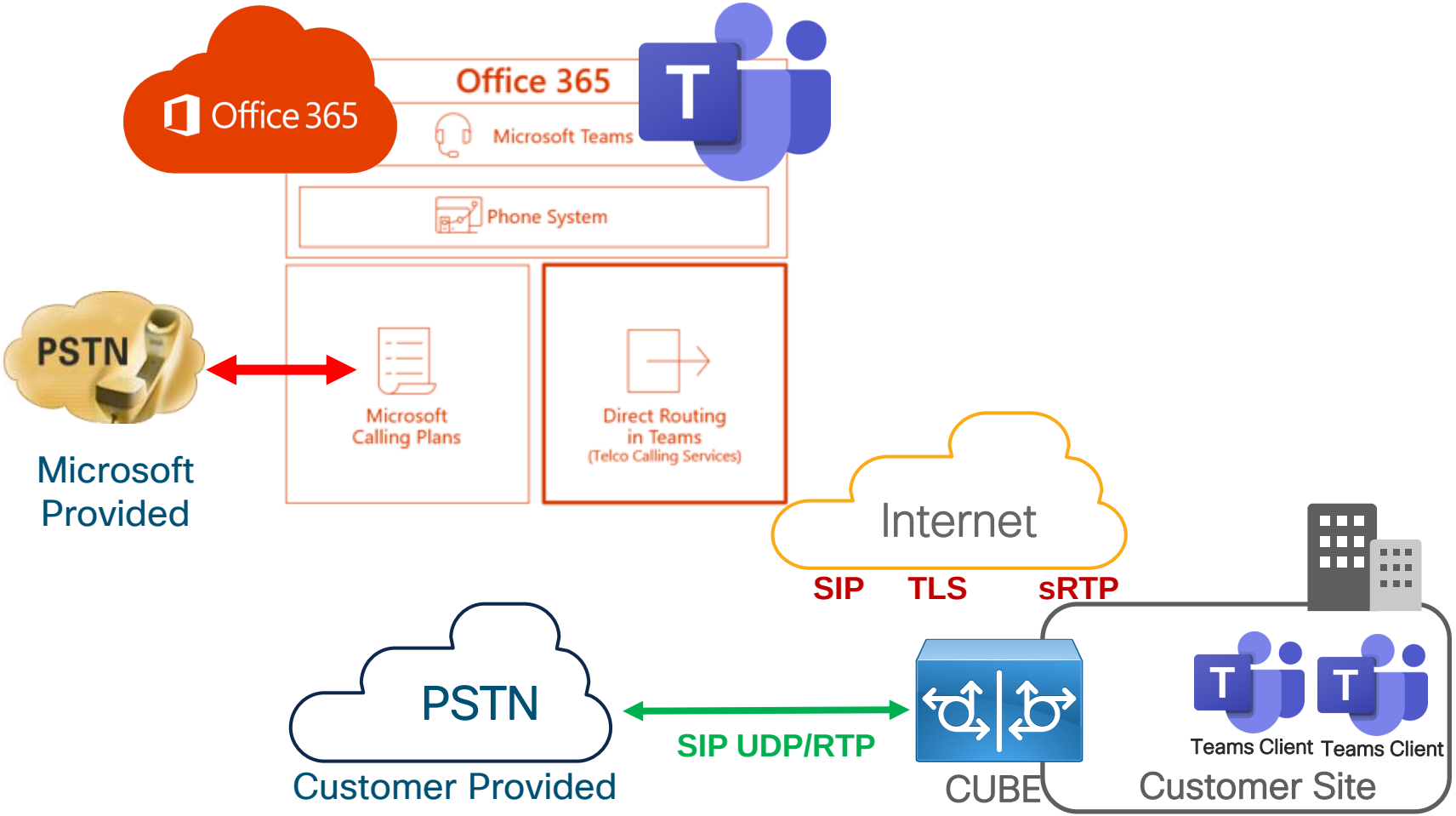
tekVizion

- Validated with Service Providers World-Wide
- Independently Tested with 3-Party PBXs in tekVizion Labs
- Standards based



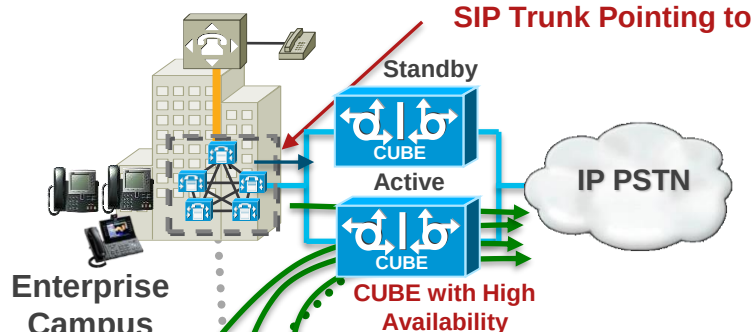
Cisco Interoperability Portal:
www.cisco.com/go/interoperability

Microsoft Teams Direct Routing – Solution Overview

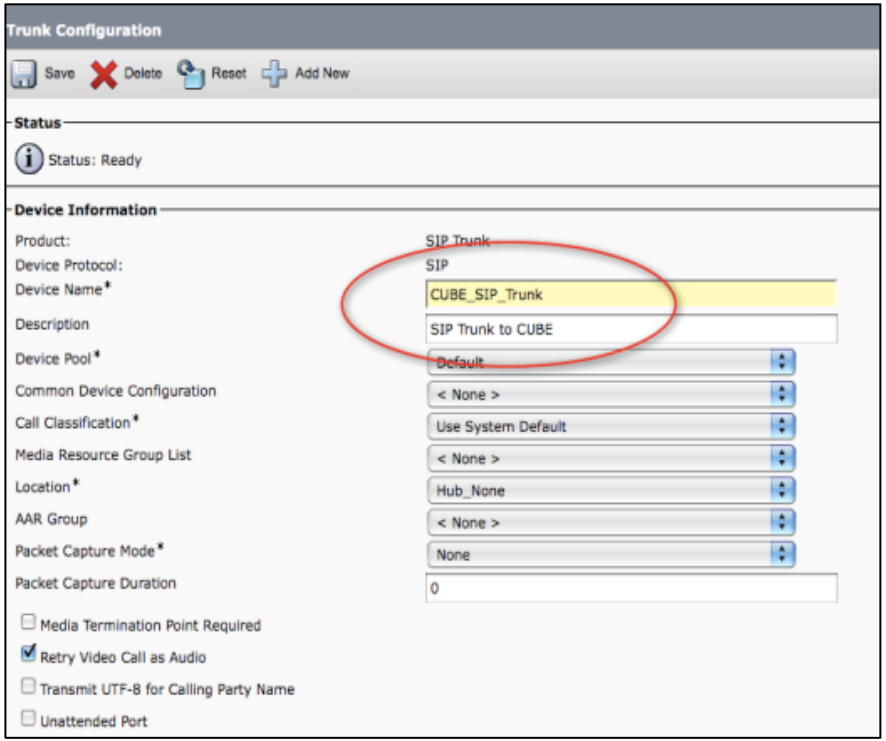


Transitioning to SIP Trunking using CUBE

Step 1:
Configure IP PBX to route calls to the edge SBC



- Configure CUCM to route all PSTN calls (central and branch) to CUBE (Gig0/0 in our slides) via a SIP trunk
- Make sure all different patterns of calls – local, long distance, international, emergency, informational etc.. are pointing to CUBE



Step 2: Get details from SIP Trunk provider

Item	SIP Trunk service provider requirement	Sample Response
1	SIP Trunk IP Address (Destination IP Address for INVITES)	**66.77.37.2** or DNS
2	SIP Trunk Port number (Destination port number for INVITES)	**5060**
3	SIP Trunk Transport Layer (UDP or TCP)	**UDP**
4	Codecs supported	**G711**, G729
5	Fax protocol support	T.38
6	DTMF signaling mechanism	**RFC2833**
7	Does the provider require SDP information in initial INVITE (Early offer required)	**Yes**
8	SBC's external IP address that is required for the SP to accept/authenticate calls (Source IP Address for INVITES)	**128.107.214.195**
9	Does SP require SIP Trunk registration for each DID? If yes, what is the username & password	No
10	Does SP require Digest Authentication?	**408-944-7700**

Step 3: Enable CUBE Application on Cisco routers

1. Enable CUBE Application

```
voice service voip
  mode border-element                    → Enables CUBE, capacity keyword has been deprecated.
  allow-connections sip to sip           → By default IOS/IOS-XE voice devices do not allow an incoming
                                           VoIP leg to go out as VoIP
```

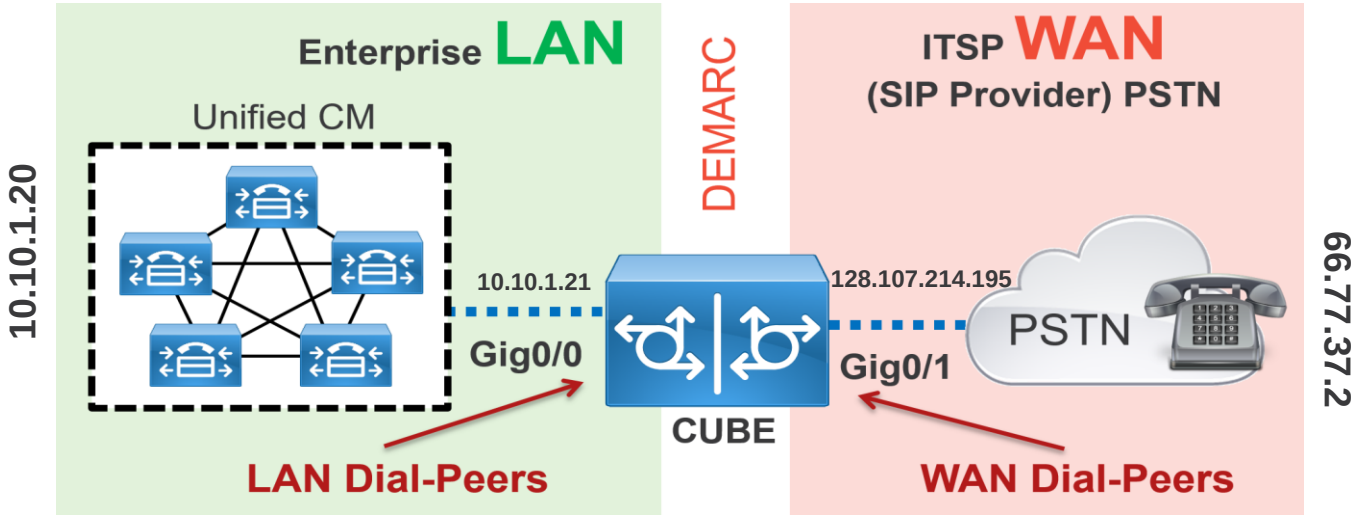
2. Configure any other global settings to meet SP's requirements

```
voice service voip
  media bulk-stats →   To increment Rx/Tx counters on IOS-XE based platforms. W/O this CLI,
                       it will show 0/0 (CPU intensive CLI)
  sip
    early-offer forced
```

3. Create a trusted list of IP addresses to prevent toll-fraud

```
voice service voip
  ip address trusted list  →        Applications initiating signaling towards CUBE, e.g. CUCM, CVP,
   ipv4 66.77.37.2   ! ITSP SIP Trunk  Service Provider's SBC. IP Addresses from dial-peers with "session target
   ipv4 10.10.1.20   ! CUCM            ip" or Server Group are trusted by default and need not be populated here
  sip
   silent-discard untrusted →       Default configuration starting XE 3.10.1 /15.3(3)M1 to mitigate TDoS Attack
```

Step 4: Configure Call routing on CUBE

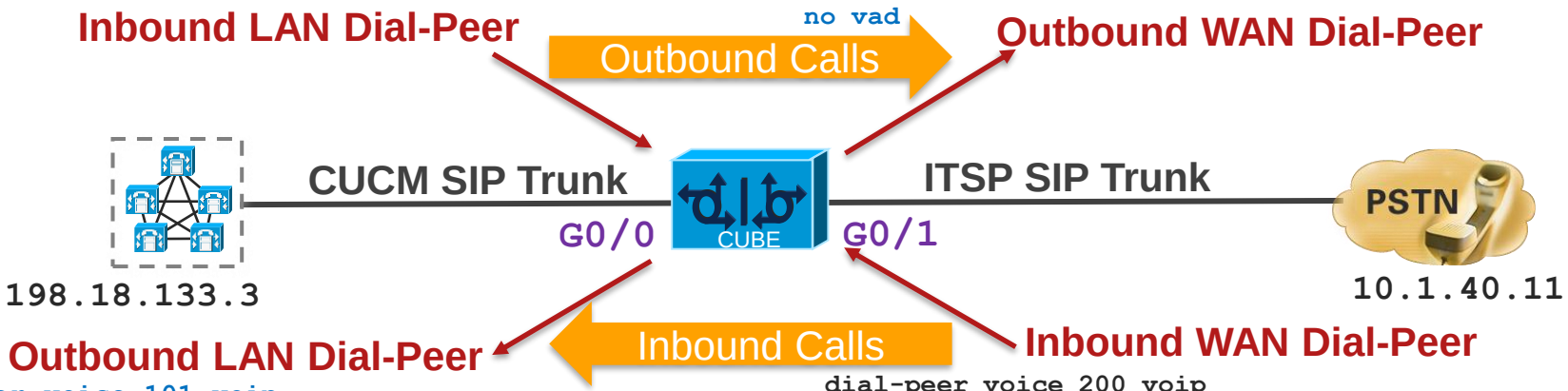


- Dial-Peer – “static routing” table mapping phone numbers to interfaces or IP addresses
- LAN Dial-Peers – Dial-peers that are facing towards the IP PBX for sending and receiving call legs to and from the PBX. Always bind LAN interface(s) on CUBE to LAN dial-peers, ensuring SIP/RTP is sourced from the intended LAN interfaces(s)
- WAN Dial-Peers – Dial-peers that are facing towards the SIP Trunk provider for sending and receiving call legs to and from the ITSP. Always bind CUBE’s WAN interface(s) to WAN dial-peer(s).


CUBE Dial-Peers
Advanced Call Routing

```
dial-peer voice 100 voip
 description *Inbound LAN dial-peer. From CUCM to CUBE*
 session protocol sipv2
 incoming called-number 8T
 voice-class sip bind control source-interface Gig0/0
 voice-class sip bind media source-interface Gig0/0
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```

```
dial-peer voice 201 voip
 description *Outbound WAN dial-peer. From CUBE to SP*
 destination-pattern 81[2-9]..[2-9]......$
 session protocol sipv2
 session target ipv4:10.1.40.11
 session transport udp
 voice-class sip bind control source-interface Gig0/1
 voice-class sip bind media source-interface Gig0/1
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```



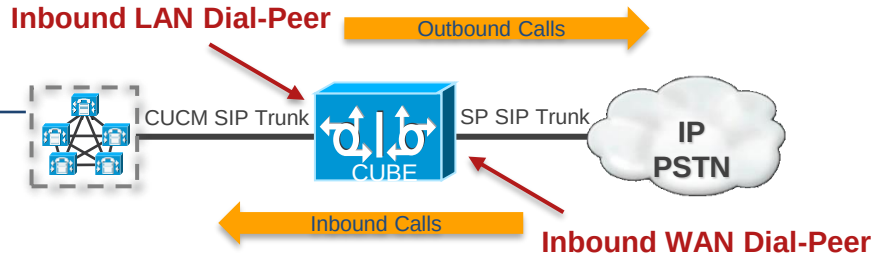

```
dial-peer voice 101 voip
 description *Outbound LAN dial-peer. From CUBE to CUCM*
 translation-profile outgoing CUBE_to_CUCM
 destination-pattern +1408944....$
 session protocol sipv2
 session target ipv4:198.18.133.3
 voice-class sip bind control source-interface Gig0/0
 voice-class sip bind media source-interface Gig0/0
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```

```
dial-peer voice 200 voip
 description *Inbound WAN dial-peer. From Provider to CUBE*
 session protocol sipv2
 incoming uri via 200
 voice-class sip bind control source-interface Gig0/1
 voice-class sip bind media source-interface Gig0/1
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad

voice class uri 200 sip
 host ipv4:10.1.40.11
```

Understanding Inbound Dial-Peer Matching Techniques

Priority

Dial-Peer Matching Rules for Inbound URI in SIP Calls		
Match Order	Cisco IOS Command	Incoming Call Parameter
1	incoming uri via	Via URI
2	incoming uri request	Request-URI
3	incoming uri to	To URI
4	incoming uri from	From URI
5	incoming called-number	Called number
6	incoming called e164-pattern-map	Called Pattern-Map-Number
7	incoming calling e164-pattern-map	Calling Pattern-Map-Number
8	answer-address	Calling number
9	destination-pattern	Calling number
10	carrier-id source	Carrier-ID associated with the call



Received:

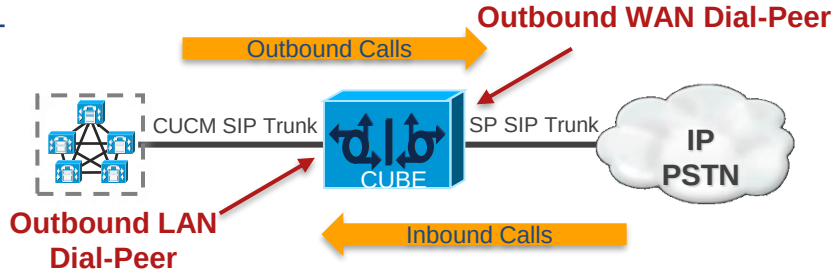
```
INVITE sip:654321@10.2.1.1 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.1:5060;x-route-
tag="cid:orange@10.1.1.1";;branch=z9hG4bK-23955-
1-0
From: "555" <sip:555@10.1.1.1:5060>;tag=1
To: ABC <sip:654321@10.2.1.1:5060>
Call-ID: 1-23955@10.1.1.1
CSeq: 1 INVITE
Contact: sip:555@10.1.1.1:5060
Supported: timer
Max-Forwards: 70
Subject: BRKUCC-2934 Session
Content-Type: application/sdp
Content-Length:   226
```

Outbound Dial-Peer Matching Criteria Summary

Priority

Dial-Peer Matching Rules for Outbound URI in SIP Calls

Match Order	Cisco IOS Command	Call Parameter
1	destination dpg <dpg-tag> (configured on inbound dial-peer)	Dial-peer Group Dial-peer
2	destination uri-from <uri-tag>	From URI
3	destination uri-to <uri-tag>	To URI
4	destination uri-via <uri-tag>	Via URI
5	destination uri-diversion <uri-tag>	Diversion URI
6	destination uri-referred-by <uri-tag>	URI-Referred-by URI
7	destination route-string <route-string-tag>	ILS Route String
8	destination uri <uri-tag> AND carrier-id target <string>	URI and Carrier-ID
9	destination-pattern <number-string> AND carrier-id target <string>	Called Number and Carrier-ID
10	destination uri <uri-tag>	URI
11	destination-pattern <DNIS-number>	Called Number
12	destination e164-pattern-map <pattern-map-number>	Called E164 Pattern Map
13	dnis-map <dnis-map-number>	Called DNIS Map
14	destination calling e164-pattern-map <pattern-map-number>	Calling E164 Pattern Map



Received:
INVITE sip:654321@10.2.1.1 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.1:5060;x-route-tag="cid:orange@10.1.1.1";;branch=z9hG4bK-23955-1-0
From: "555" <sip:555@10.1.1.1:5060>;tag=1
To: ABC <sip:654321@10.2.1.1:5060>
Call-ID: 1-23955@10.1.1.1
CSeq: 1 INVITE
Contact: sip:555@10.1.1.1:5060
Supported: timer
Max-Forwards: 70
Subject: BRKUCC-2934 Session
Content-Type: application/sdp
Content-Length: 226
.....

http://siplab.ciscolive.com/

Destination Server Group

- Supports multiple destinations (session targets) be defined in a group and applied to a single outbound dial-peer
- Once an outbound dial-peer is selected to route an outgoing call, multiple destinations within a server group will be sorted in either round robin or preference [**default**] order
- This reduces the need to configure multiple dial-peers with the same capabilities but different destinations. E.g. Multiple subscribers in a cluster

```
voice class server-group 1
 hunt-scheme {preference | round-robin}
 ipv4 1.1.1.1 preference 5
 ipv4 2.2.2.2
 ipv4 3.3.3.3 port 5065 preference 3
 ipv6 2010:AB8:0:2::1 port 5065 preference 3
 ipv6 2010:AB8:0:2::2
```

* DNS target not supported in server group

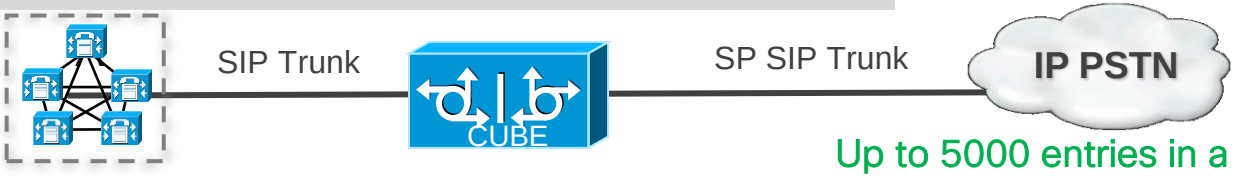
```
dial-peer voice 100 voip
 description Outbound DP
 destination-pattern 1234
 session protocol sipv2
 codec g711ulaw
 dtmf-relay rtp-nte
 session server-group 1
```

Multiple Number Patterns Under Same Incoming/Outgoing Dial-peer

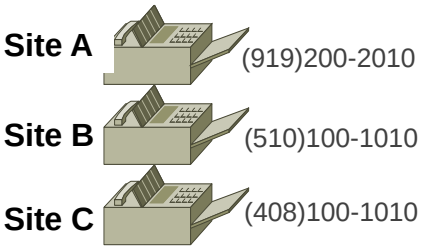
G729 Sites

```
voice class e164-pattern-map 300
  e164 200.
  e164 510100100.
  e164 408100100.

dial-peer voice 1 voip
  description Inbound DP via Calling
  incoming calling e164-pattern-map 300
  codec g729r8
```

Up to 1000 entries in a pattern map



Up to 5000 entries in a text file



G711 Sites

```
voice class e164-pattern-map 400
 url flash:e164-pattern-map.cfg

dial-peer voice 2 voip
  description Outbound DP via Called
  destination e164-pattern-map 400
  codec g711ulaw
```

```
! This is an example of the contents
    of E164 patterns text file stored
    in flash:e164-pattern-map.cfg

9192002010
5101001010
4081001010
<blank line>
```

Destination Dial-peer Group

```
voice class dpg 10000
  description Voice Class DPG for SJ
  dial-peer 1001 preference 1
  dial-peer 1002 preference 2
  dial-peer 1003
!
dial-peer voice 100 voip
 description Inbound DP
 incoming called-number 1341
 destination dpg 10000

 Received:
 INVITE sip:1341@CUBE-IP-ADDRESS:5060
 Sent:
 INVITE sip:1341@10.1.1.3:5060
```

```
dial-peer voice 1001 voip
 destination-pattern BAD
 session protocol sipv2
 session target ipv4:10.1.1.1
!
dial-peer voice 1002 voip
 destination-pattern BAD.BAD
 session protocol sipv2
 session target ipv4:10.1.1.2
!
dial-peer voice 1003 voip
 destination-pattern BAD.BAD.BAD
 session protocol sipv2
 session target ipv4:10.1.1.3
```

3. Outbound DP is selected

1. Incoming Dial-peer is first matched

2. Now the DPG associated with the INBOUND DP is selected

Call Admission Control (CAC)

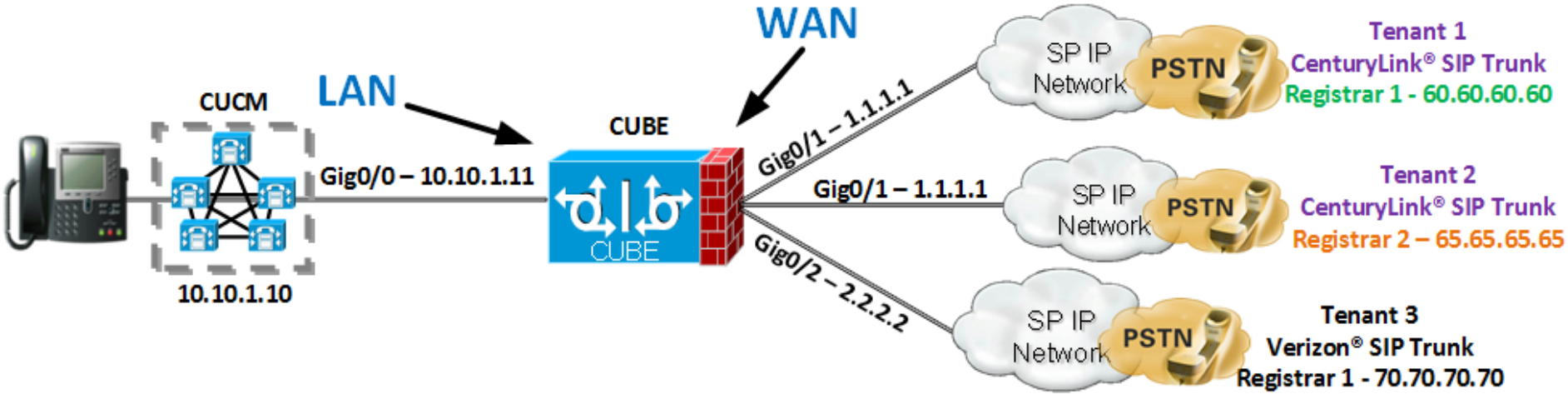
- Call processing capacity for any CUBE instance will be influenced by several considerations, including software version, features configured and the platform itself
- To ensure that calls continue to be processed reliably, configure Call Admission Control as follows to reject calls when use of system resources exceeds 80%. Refer to the CUBE Configuration Guide for further details

```
enable
conf t
 call threshold global cpu-avg low 75 high 80
 call threshold global total-mem low 75 high 80
 call treatment on
end
```

- `show call active total-calls` lists the total number of concurrent calls on a CUBE platform

Multi-Tenancy

Multiple Tenants on CUBE



- Every Registrar/User Agent/ITSP connected to CUBE can be considered a Tenant to CUBE
- Allows specific global configurations (CLI under sip-ua) for multiple tenants such as specific SIP Bind for REGISTER messages
- Allows differentiated services for different tenants

Configuring Voice Class Tenant

- Configure voice class tenant

```
voice class tenant 1
  registrar 1 ipv4:10.64.86.35:9052 expires 3600
  credentials username aaaa password 7 06070E204D realm aaaa.com
  credentials number bbbb username bbbb password 7 110B1B0715 realm bbbb.com
  bind control source-interface GigabitEthernet0/0
  bind media source-interface GigabitEthernet0/0
  copy-list 1
  outbound-proxy ipv4:10.64.86.35:9055
  early-offer forced
```

Add new voice class tenant

- Apply tenant to the desired dial-peer

```
dial-peer voice 1 voip
 destination-pattern 111
 session protocol sipv2
 session target ipv4:10.64.86.35:9051
 session transport udp
 voice-class sip tenant 1
```

Configuration Preference Order

1. dial-peer (overrides tenant and global configs)
2. tenant (overrides the global config)
3. global (voice service voip OR sip-ua)

Apply Tenant to a Dial-peer

External/PSTN Call Recording

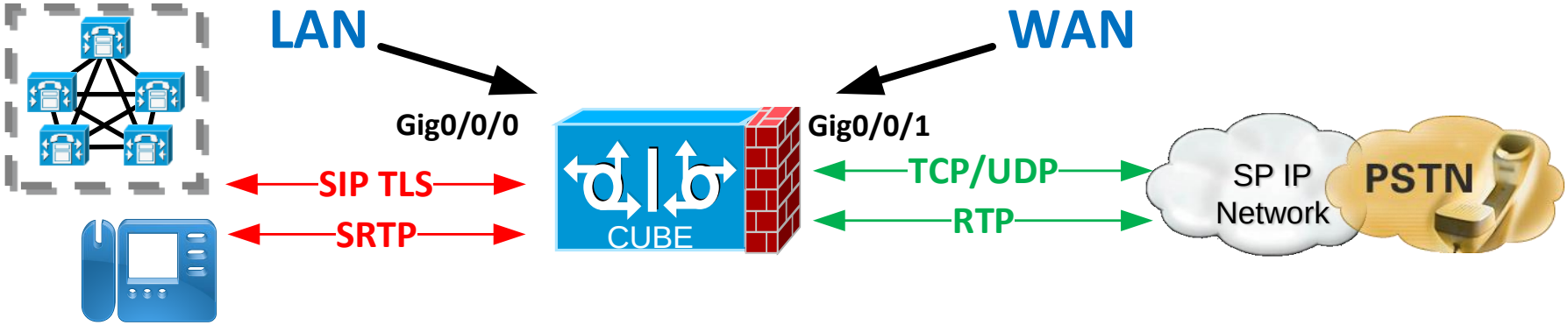
External/PSTN Call Recording Options

- CUBE Controlled (Dial-peer based SIPREC)
  - SIPREC based, CUBE sends metadata in XML format
  - Dial-peer controlled, IP-PBX independent
  - Source of recorded media (RTP only) is always CUBE (External calls only).
  - Records both audio and video calls and supported with CUBE HA

- CUCM NBR (Network Based Recording)
  - CUCM Controlled & triggered, requires UC Services API be enabled on CUBE
  - Audio calls only
  - Source of Recorded Media can be CUBE (Gateway Preferred) or Phone based (BiB)

Securing Collab deployments with CUBE

Secure SIP Trunks with CUBE



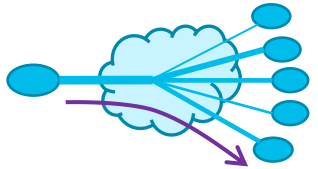
- Interworking between all three transport types is supported : UDP/TCP/TLS
- IOS-XE based platforms do not require DSPs for SRTP-RTP interworking
- TLS Exclusivity can be configured with “transport tcp tls v1.2”
- NGE Crypto supported for SRTP-SRTP (IOS-XE 16.5.2) [Crypto A – Crypto B], SRTP-RTP, SRTP pass-thru

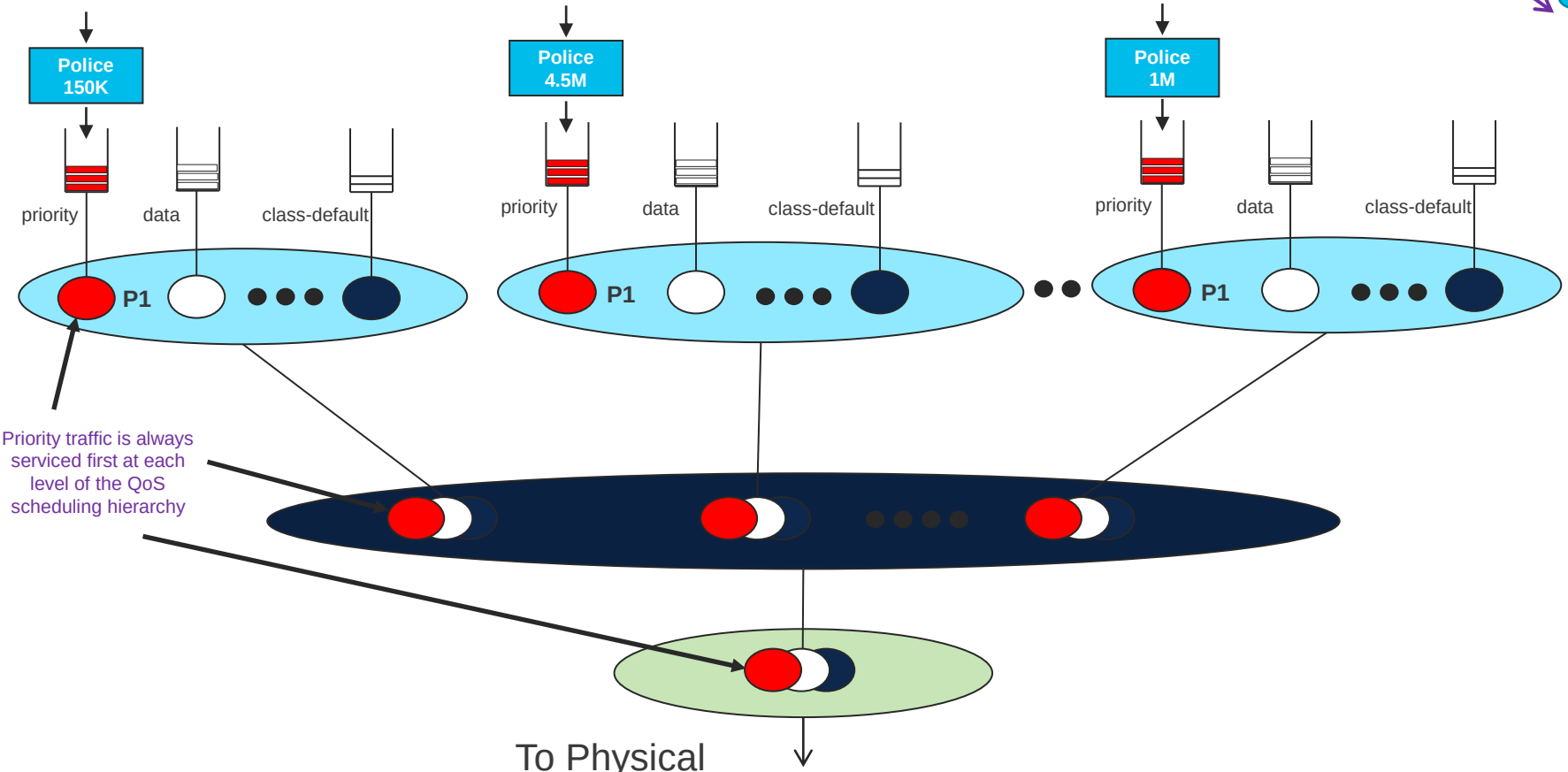
Thank you

Appendix A QoS Design

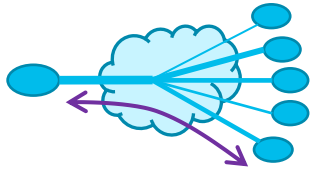
Aggregate Priority Load

Priority Propagation / Passing Lanes





Aggregate Priority Load
Conclusion

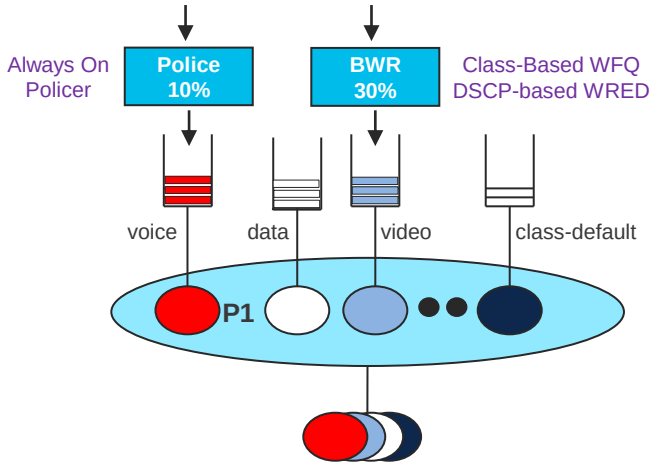


- For Voice, use an Always On policer, rather than a Conditional policer

```
class VOICE
 priority level 1
 police cir percent 10
```

- For Video, use a Bandwidth Remaining Percent (BWR) queue with DSCP-based WRED, rather than a level 2 Priority queue

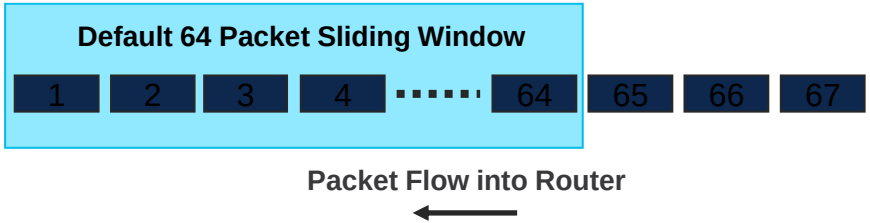
```
class INTERACTIVE-VIDEO
 bandwidth remaining percent 30
 random-detect dscp-based
```



IPsec Anti-Replay

Message Integrity

- Designed to identify packet capture/replay by 3rd party – Message Integrity
- Sender assigns sequence number per Security Association (SA) to encrypted packets
- Receiver maintains 64 packet sliding window by default

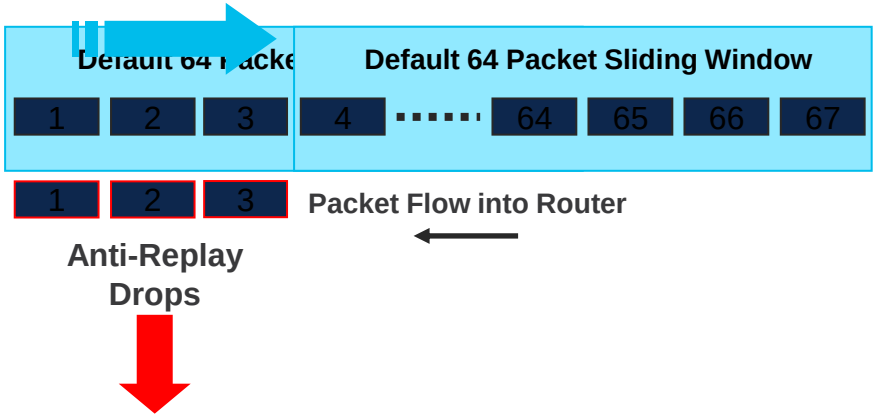


IPsec Anti-Replay

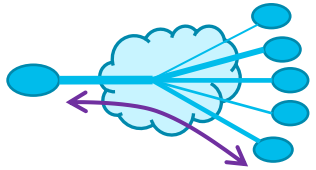
Message Integrity

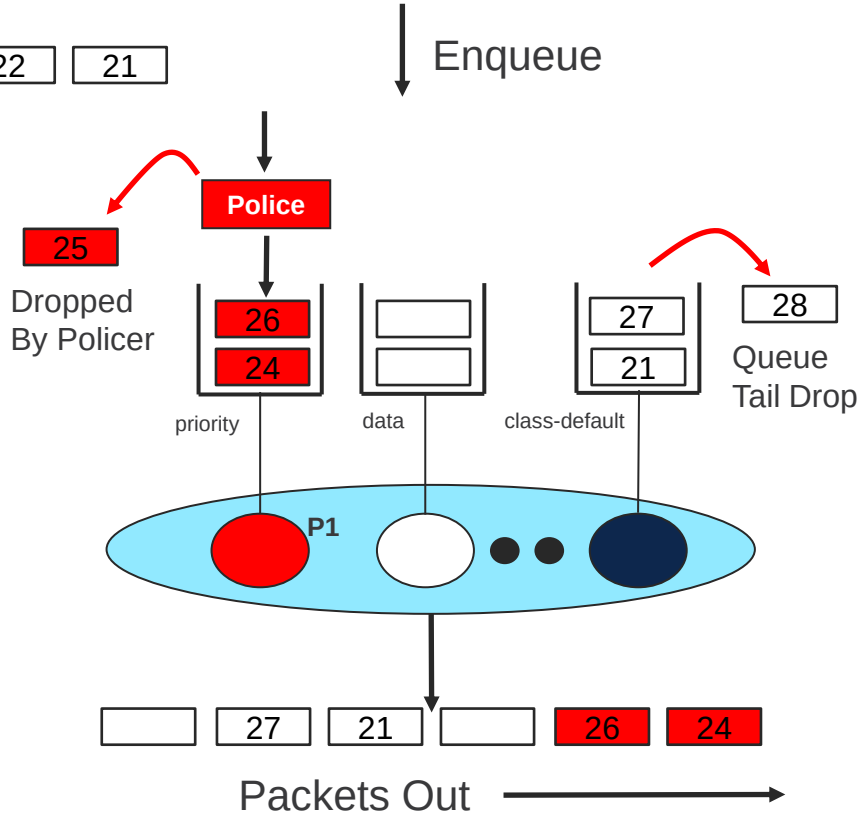
- Designed to identify packet capture/replay by 3rd party – Message Integrity
- Sender assigns sequence number per Security Association (SA) to encrypted packets
- Receiver maintains 64 packet sliding window by default

  - Window moves right to include higher sequence numbers
  - Window marks packets as received or not
  - Packets to the left of the window are dropped



IPsec Anti-Replay and QoS





- On a congested interface, a low-priority packet may be delayed by queuing, and then, arrive at the next router after the anti-replay window has been exceeded
- Also, if an encrypted packet arrives out of sequence by the window size (default is 64 packets), the packet is dropped
- Increasing the anti-replay window size has no impact on throughput or security
- The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed

Use the maximum replay window-size of 1024 for each supported platform

```
crypto ipsec security-association replay window-size 1024
```

QoS Tools Review: Queuing and Dropping Tools
Bandwidth Percent vs Bandwidth Remaining Percent

Bandwidth Percent specifies bandwidth allocation as a percentage of the value entered in the bandwidth command on the interface

- Bandwidth percentages have to take into account priority percent values
- They have to be adjusted when priority bandwidth values are changed

Bandwidth Remaining Percent specifies bandwidth allocation as a percentage of the bandwidth value that has **not** been allocated to priority classes

- Bandwidth remaining percentages must equal 100%
- The bandwidth automatically adjusts when priority bandwidth values are changed

The two features cannot be used in the same policy map

Examples:

Bandwidth Percent (BWP)

Service Rate Bandwidth = 10Mbps
Priority Queue 10% = 1 Mbps
BWP of 30% = 10 x .30 = 3.0 Mbps

→

Bandwidth Remaining Percent (BWR)

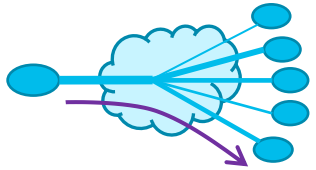
Service Rate Bandwidth = 10Mbps
Priority Queue 10% = 1 Mbps
BWR of 30% = 10 – 1 = 9 x .30 = 2.7 Mbps

→

PQ Change in Value

Service Rate Bandwidth = 10Mbps
Priority Queue 20% = 2 Mbps
BWR of 30% = 10 – 2 = 8 x .30 = 2.4 Mbps

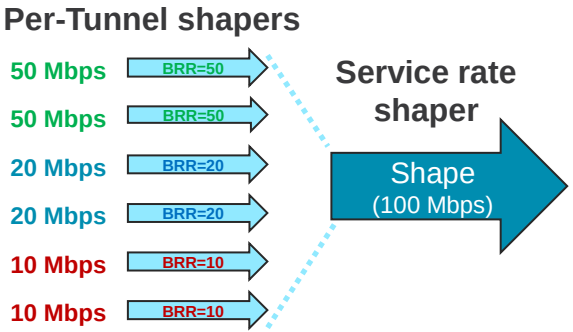
Bandwidth Remaining Ratio
Details



Bandwidth Remaining Ratio (BRR) provides proportional sharing to parent shapers during times of congestion.

If you over-subscribe your hub BR outbound bandwidth with per-tunnel policies that exceed the service rate, the BRR commands on each parent policy means they will get their "fair share" of the remaining bandwidth as compared to the other branch sites.

- If all the per-tunnel BW amounts are 5 Mbps or greater, we use a BRR value of BW / 1 Mbps. (i.e. 10 Mbps is BRR of 10, 50 Mbps is BRR of 50, etc.)
- If any of the per-tunnel BW values are less than 5 Mbps, we use a BRR value of BW / 100 Kbps. (i.e. 3 Mbps is BRR of 30, 1.5 Mbps is BRR of 15, etc.)

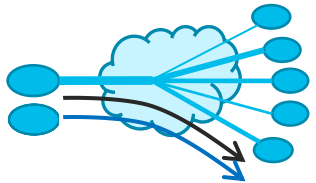


When the total bandwidth exceeds 100 Mbps, each of the per-tunnel shapers will get their fair share based on their BRR values.

Example:
50 Mbps site gets 50 / 160 or 31.25%
20 Mbps site gets 20 / 160 or 12.5%
10 Mbps site gets 10 / 160 or 6.25%

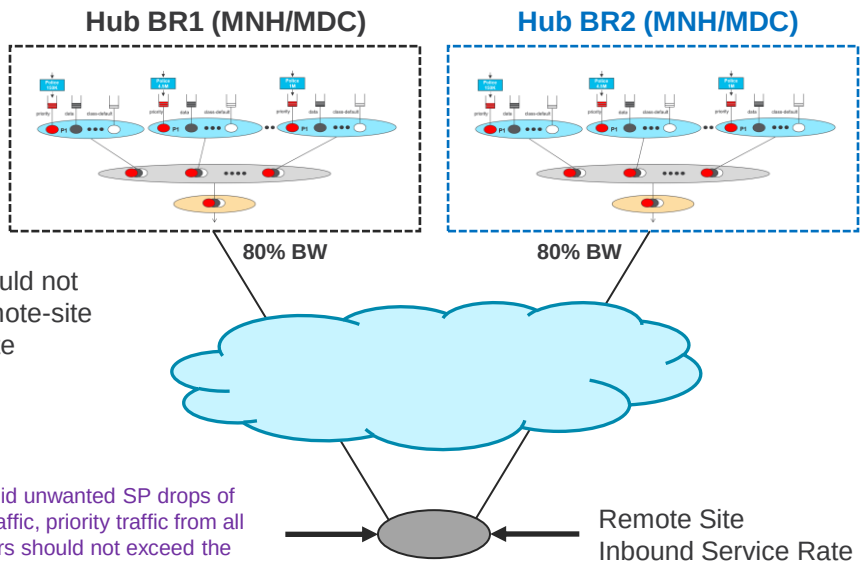
Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders



- Bandwidth can exceed 100% of the remote-site inbound Service Rate using a calculated oversubscription of ~ 1.6:1
- Bandwidth has to be divided equally due to one NHRP group
- QoS child policies do not have to be the same per Sender but DSCP markings must match for PfR TC channels to establish

- As the number of senders increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns



- Total bandwidth should not exceed 160% of remote-site inbound Service Rate

Remote Site Example:
50 Mb/s *.80 = 40 Mb/s per Hub BR

Branch Tunnel Interface

```
interface Tunnel10
 bandwidth receive 50000
 nhrp nhs 10.6.34.1 nbma 192.168.6.1 multicast
 nhrp nhs 10.6.34.2 nbma 192.168.6.41 multicast
 nhrp group RS-GROUP-50MBPS-80
```

Hub Policy

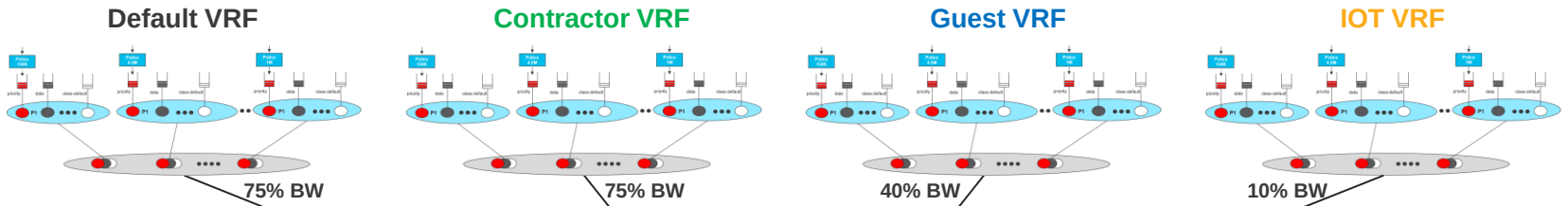
```
policy-map RS-GROUP-50MBPS-80-POLICY
 class class-default
  description 80% of 50 Mbps
  shape average 40 Mbps
  bandwidth remaining ratio 40
   service-policy WAN
```

Multiple VRF QoS for Hub Routers

Bandwidth Sharing Between Multiple VRF Tunnels

- Bandwidth can exceed 100% of the remote-site inbound Service Rate using an oversubscription ratio of ~ 2:1
- Bandwidth does not have to be divided equally between VRFs
- QoS policies do not have to be the same per VRF

- As the number of VRFs increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns



- Total bandwidth for VRFs should not exceed 200% of remote-site inbound Service Rate as oversubscription traffic will be dropped in the SP cloud
- Bandwidth for Guest traffic is normally less than non-Guest
- Bandwidth for low volume VRFs like IOT and PCI should use a much smaller percentage

Aggregate Priority Load: Priority traffic from all VRFs cannot exceed the hub BR outbound service rate

Grandparent Shaping Policy on Physical

Shape for Outbound Service Rate

To Physical

Remote Site Example:
40 Mb/s *.75 = 30 Mb/s per VRF
40 Mb/s *.40 = 16 Mb/s per VRF
40 Mb/s *.10 = 4 Mb/s per VRF

Default VRF / Contractor VRF

```
interface Tunnel101
 bandwidth receive 40000
 nhrp group RS-GROUP-40MBPS-75
```

Guest VRF

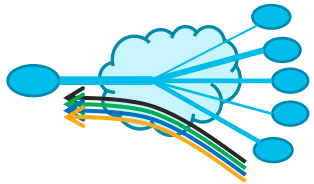
```
interface Tunnel103
 bandwidth receive 40000
 nhrp group RS-GROUP-40MBPS-40
```

IOT VRF

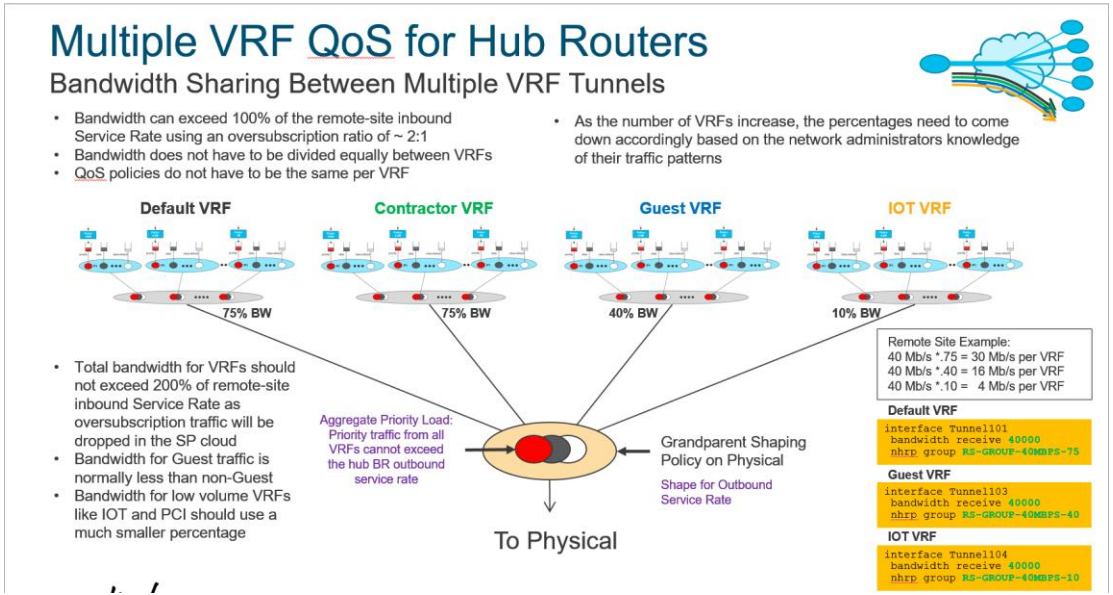
```
interface Tunnel104
 bandwidth receive 40000
 nhrp group RS-GROUP-40MBPS-10
```

VRF = Virtual Routing and Forwarding

Multiple VRF QoS for Branch



- Using normal recommendations, QoS policy is applied to the physical interface at remote site which means all VRFs share the same QoS policy by default
- If you want to use different QoS policies for each VRF, you can deploy per-tunnel QoS in the spoke to hub direction using the same tools and limitations described on the previous slide



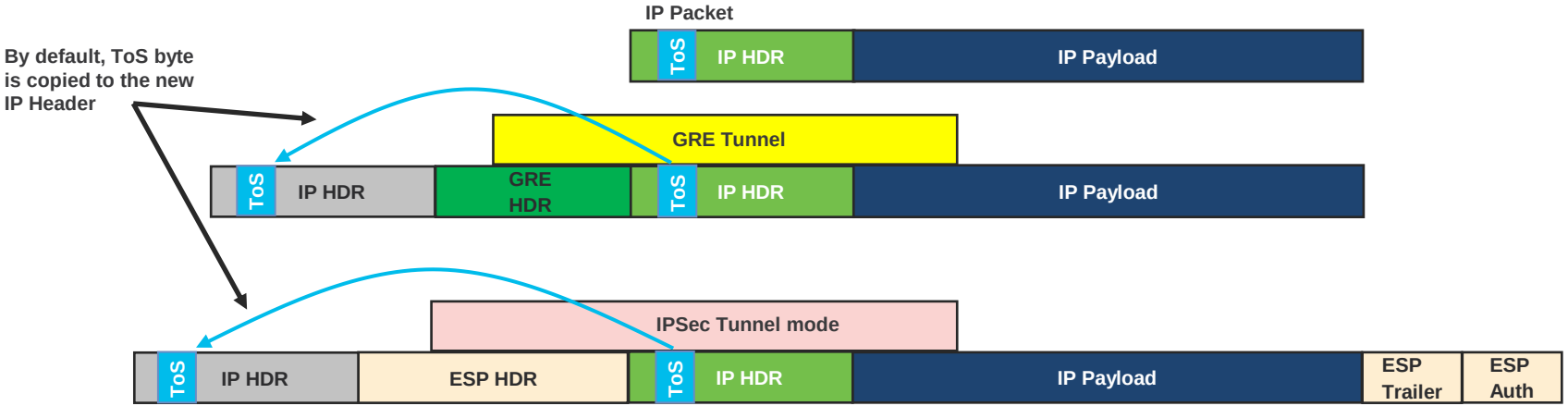
Enterprise to SP Mapping

ToS Byte Preservation

The 12-class view is preserved across the enterprise even though we treat it differently at the egress of the router and send it to different channels within the SP network

The twelve classes remain intact on the inner header and the outer tunnel header is remarked as the traffic leaves the tunnel interface

The remarked outer header is discarded after arriving at the tunnel interface on the receiving router, thus leaving the inner header marking unchanged



Enterprise to SP Mapping

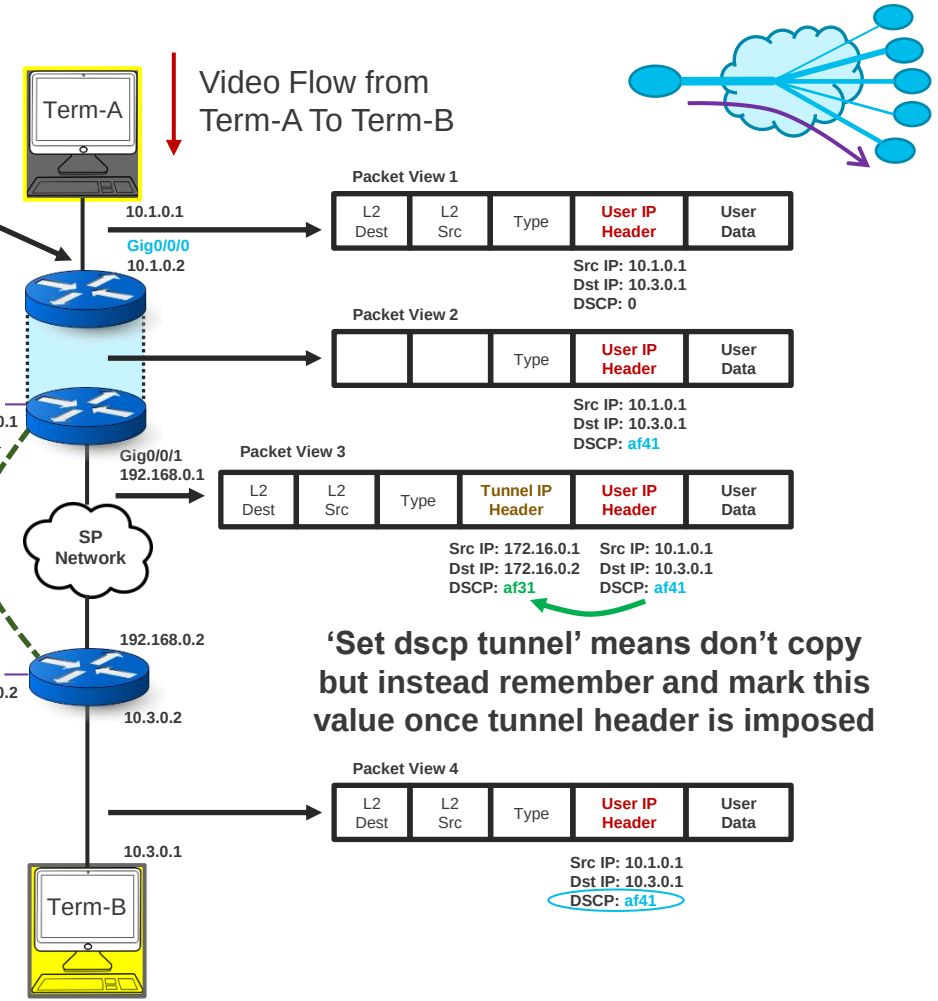
Set dscp tunnel outbound on tunnel (Hub)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
 match protocol attribute traffic-class multimedia-conferencing
 match protocol attribute business-relevance business-relevant

policy-map INGRESS-MARKING
 class MULTIMEDIA_CONFERENCING-NBAR
  set dscp af41

interface GigabitEthernet0/0/0
 service-policy input INGRESS-MARKING
```

Marking the User IP header

```
class-map INTERACTIVE-VIDEO
 match dscp af41

policy-map RS-GROUP-10MBPS-POLICY
 class INTERACTIVE-VIDEO
  set dscp tunnel af31

interface Tunnel10
 nhrp map group RS-GROUP-10MBPS service-policy
          output RS-GROUP-10MBPS-POLICY
```

Marking the Tunnel IP header



Enterprise to SP Mapping

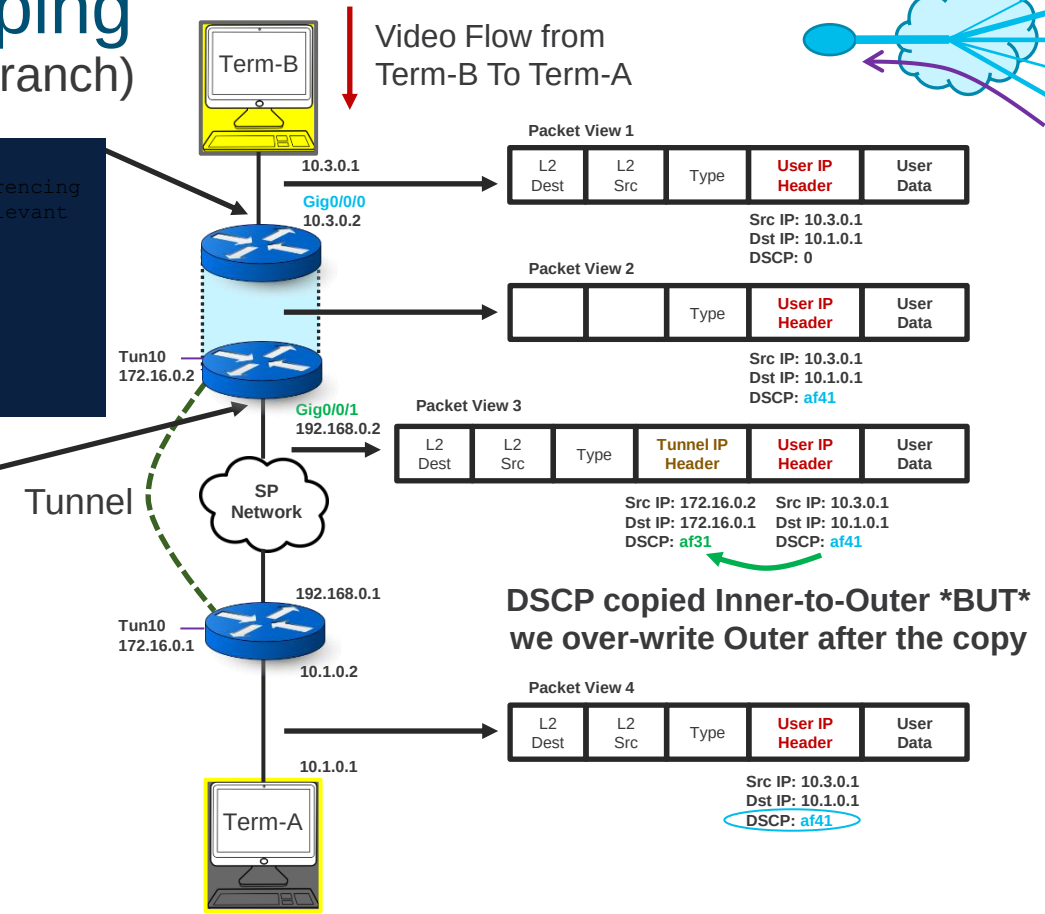
Set dscp outbound on physical (Branch)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
 match protocol attribute traffic-class multimedia-conferencing
 match protocol attribute business-relevance business-relevant

policy-map INGRESS-MARKING
 class MULTIMEDIA_CONFERENCING-NBAR
  set dscp af41

interface GigabitEthernet0/0/0
 service-policy input INGRESS-MARKING
```

Marking the **User IP header**

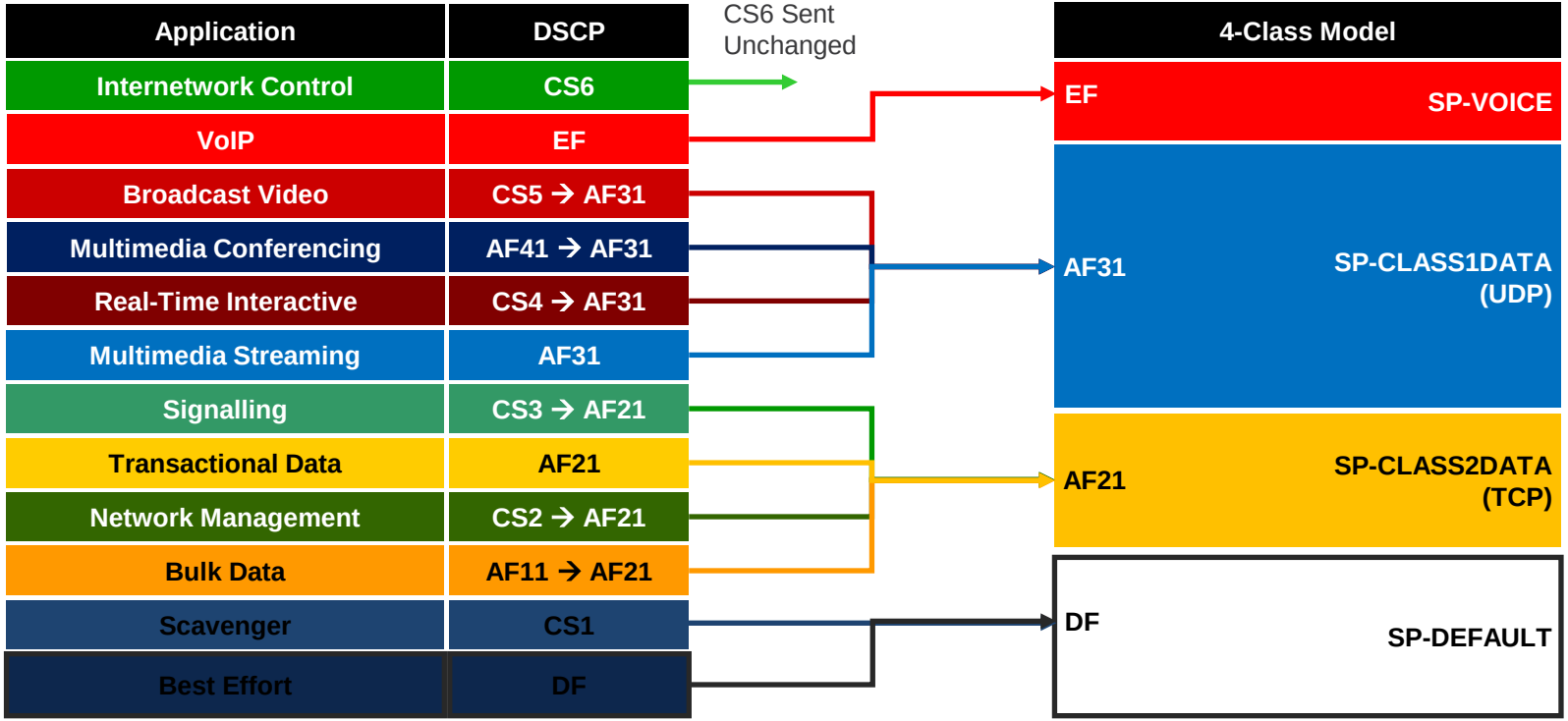
```
class-map INTERACTIVE-VIDEO
 match dscp af41

policy-map POLICY-TRANSPORT-1
 class INTERACTIVE-VIDEO
  set dscp af31

interface GigabitEthernet0/0/1
 service-policy output POLICY-TRANSPORT-1
```

Marking the **Tunnel IP header**



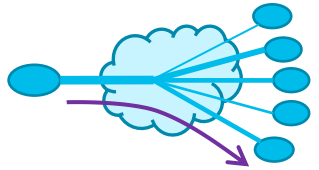
Enterprise to SP Mapping

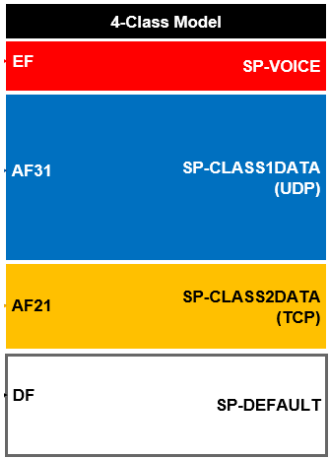
Example: 4-Class SP Model



4-Class SP QoS Model Configuration

Tunnel Interface
Hub BR






```
policy-map WAN
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
 class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
 class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
  class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
 class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel default
 class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
 class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
 class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy WAN
```

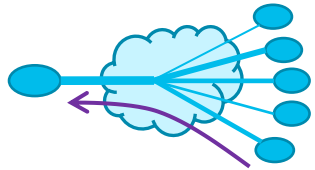
```
interface Tunnel10
 bandwidth <service-rate>
 nhrp map group RS-GROUP-10MBPS service-policy
       output RS-GROUP-10MBPS-POLICY
```

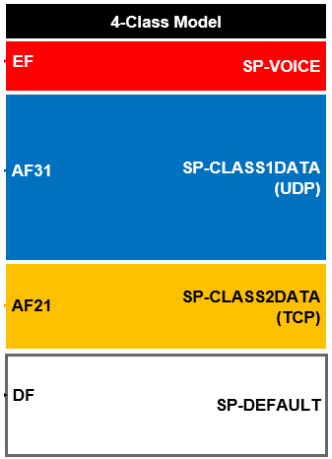
Branch Router:

```
interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
 bandwidth 10000
 nhrp group RS-GROUP-10MBPS
 tunnel source GigabitEthernet0/0
 tunnel vrf TRANSPORT-1
```

4-Class SP QoS Model Configuration

Physical Interface
Branch






```
policy-map WAN
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af31
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af31
 class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp cs6
 class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp af21
  class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af21
 class SCAVENGER
  bandwidth remaining percent 1
  set dscp default
 class VOICE
  priority level 1
  police cir percent 10
  set dscp ef
 class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp default
```

Branch Router:

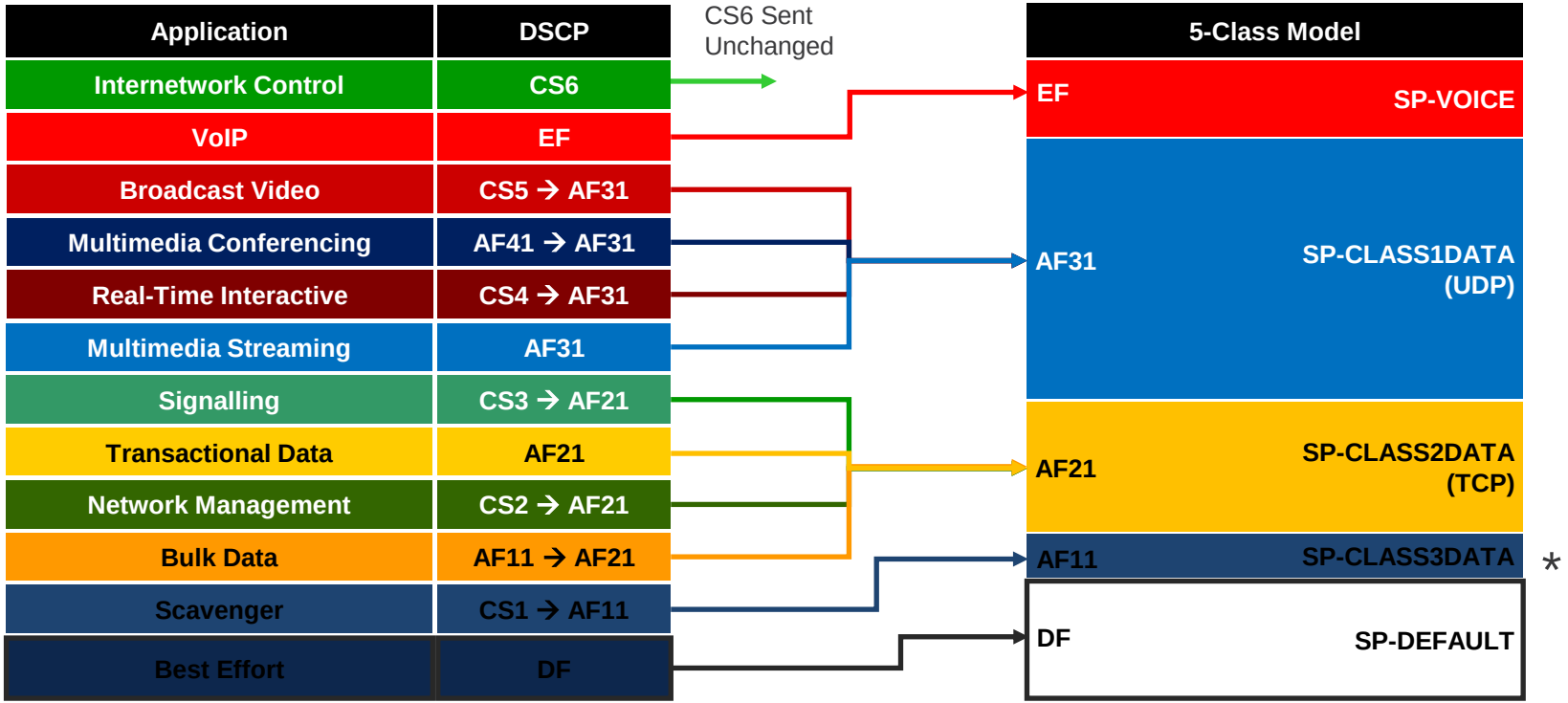
```
policy-map POLICY-TRANSPORT-1
 class class-default
  shape average 10 Mbps
  service-policy WAN

interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
```

The PfR Traffic Class channels will not establish if the DSCP values from the hub and branch routers do not match

Enterprise to SP Mapping

Example: 5-Class SP Model

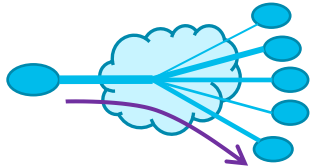
Reference

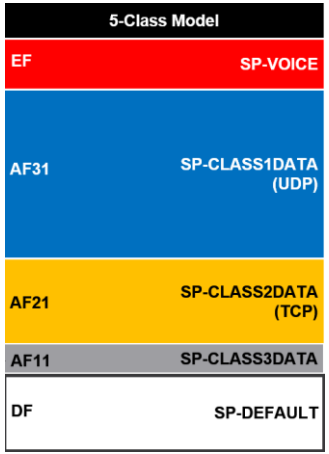


5-Class QoS Model Configuration

Tunnel Interface
Hub BR

Reference






```
policy-map WAN
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
 class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
 class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
  class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
 class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel af11
 class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
 class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
 class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
   service-policy WAN
```

```
interface Tunnel10
 bandwidth <service-rate>
 nhrp map group RS-GROUP-10MBPS service-policy
          output RS-GROUP-10MBPS-POLICY
```

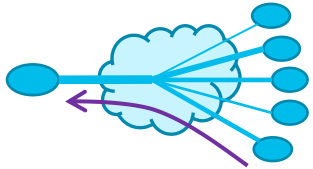
Branch Router:

```
interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
 bandwidth 10000
 nhrp group RS-GROUP-10MBPS
 tunnel source GigabitEthernet0/0
 tunnel vrf TRANSPORT-1
```

5-Class QoS Model Configuration

Physical Interface
Branch

Reference



5-Class Model	
EF	SP-VOICE
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
AF11	SP-CLASS3DATA
DF	SP-DEFAULT

```
policy-map WAN
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af31
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af31
 class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp cs6
 class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp af21
  class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af21
 class SCAVENGER
  bandwidth remaining percent 1
  set dscp af11
 class VOICE
  priority level 1
  police cir percent 10
  set dscp ef
 class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp default
```

Branch Router:

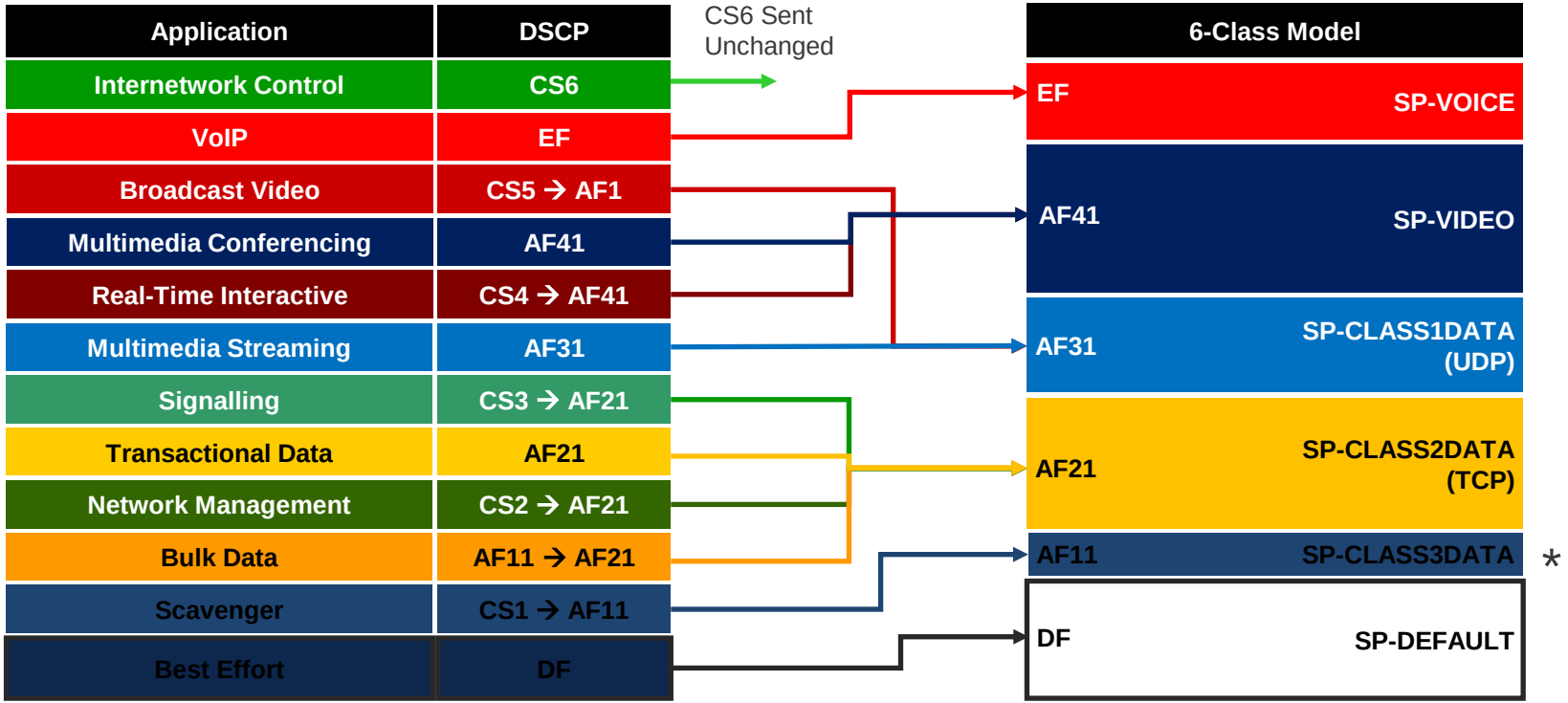
```
policy-map POLICY-TRANSPORT-1
 class class-default
  shape average 10 Mbps
  service-policy WAN
```

```
interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
```

Enterprise to SP Mapping

Example: 6-Class SP Model

Reference



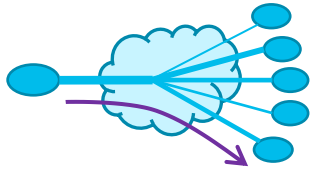
* - Specified by ISP

6-Class QoS Model Configuration

Tunnel Interface

Hub BR

Reference



6-Class Model	
EF	SP-VOICE
AF41	SP-VIDEO
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
AF11	SP-CLASS3DATA
DF	SP-DEFAULT

```
policy-map WAN
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af41
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
 class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
 class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
  class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
 class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel af11
 class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
 class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
 class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
   service-policy WAN
```

```
interface Tunnel10
 bandwidth <service-rate>
 nhrp map group RS-GROUP-10MBPS service-policy
          output RS-GROUP-10MBPS-POLICY
```

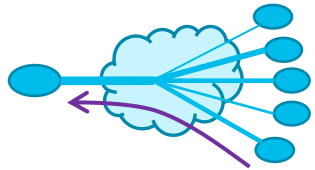
Branch Router:

```
interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
 bandwidth 10000
 nhrp group RS-GROUP-10MBPS
 tunnel source GigabitEthernet0/0
 tunnel vrf TRANSPORT-1
```

6-Class QoS Model Configuration

Physical Interface
Branch

Reference



6-Class Model	
EF	SP-VOICE
AF41	SP-VIDEO
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
AF11	SP-CLASS3DATA
DF	SP-DEFAULT

```
policy-map WAN
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af41
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af31
 class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp cs6
 class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp af21
  class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af21
 class SCAVENGER
  bandwidth remaining percent 1
  set dscp af11
 class VOICE
  priority level 1
  police cir percent 10
  set dscp ef
 class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp default
```

Branch Router:

```
policy-map POLICY-TRANSPORT-1
 class class-default
  shape average 10 Mbps
  service-policy WAN
```

```
interface GigabitEthernet0/0
 bandwidth 10000
 service-policy output POLICY-TRANSPORT-1
```