
SCTE®
CABLE-TEC EXPO®
FAST FORWARD 2021
ATLANTA, GA
OCTOBER 11-14
SCTE
a subsidiary of CableLabs®
UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
2021 Fall Technical Forum
SCTE® • NCTA • CABLELABS®

SCTE
a subsidiary of CableLabs®

Wireline Access Network

Configuring and Deploying Low Latency DOCSIS Networks

Greg White

Distinguished Technologist
CableLabs

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

SCTE CABLE-TEC EXPO FAST FORWARD 2021
VIRTUAL EXPERIENCE
OCTOBER 11-14

Introduction

Low Latency DOCSIS (LLD) is a recent update to DOCSIS 3.1 technology

Can be deployed as a firmware upgrade to existing DOCSIS 3.1 equipment (CM & CMTS)

Significantly Reduces:

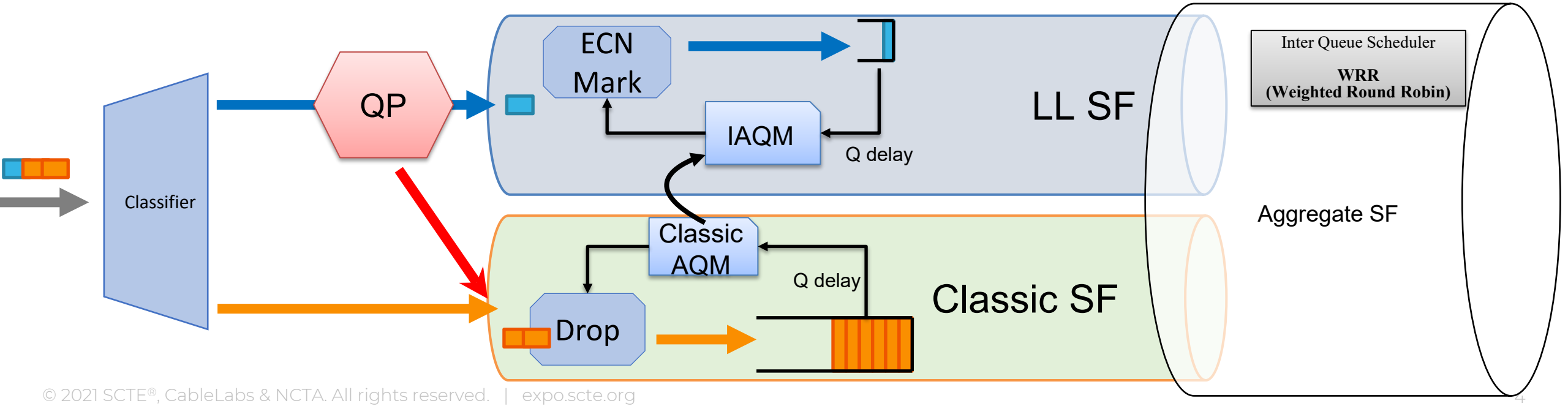
- Average Packet Latency
- Latency Variation (jitter)
- Packet Loss

Nearing deployment:

- Multiple CMTS and Certified CM implementations available
- Lab testing underway at multiple MSOs

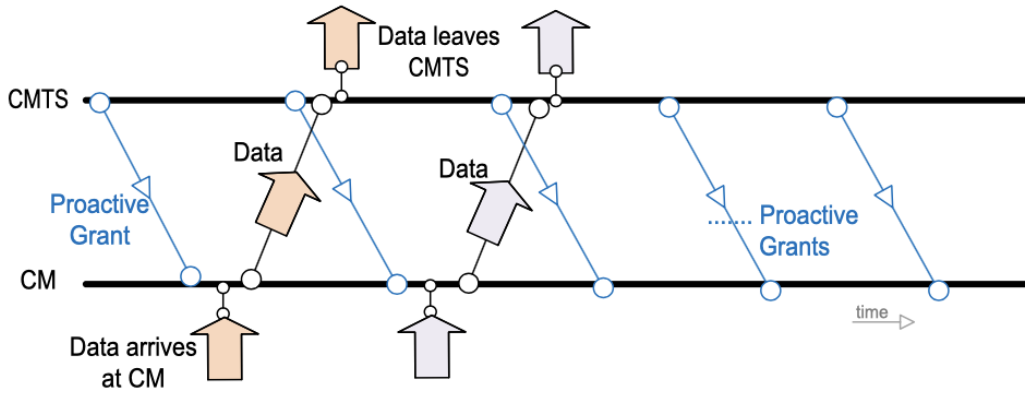
Low Latency Technology

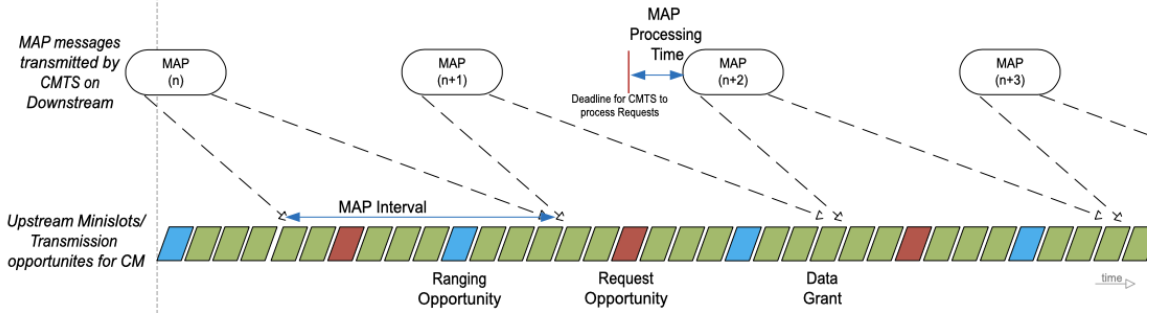
- Dual Queue (ASF)
- Classifiers
- Queue Protection
- IAQM
- Classic AQM (Coupled)
- WRR Scheduler



Low Latency Technology (2)

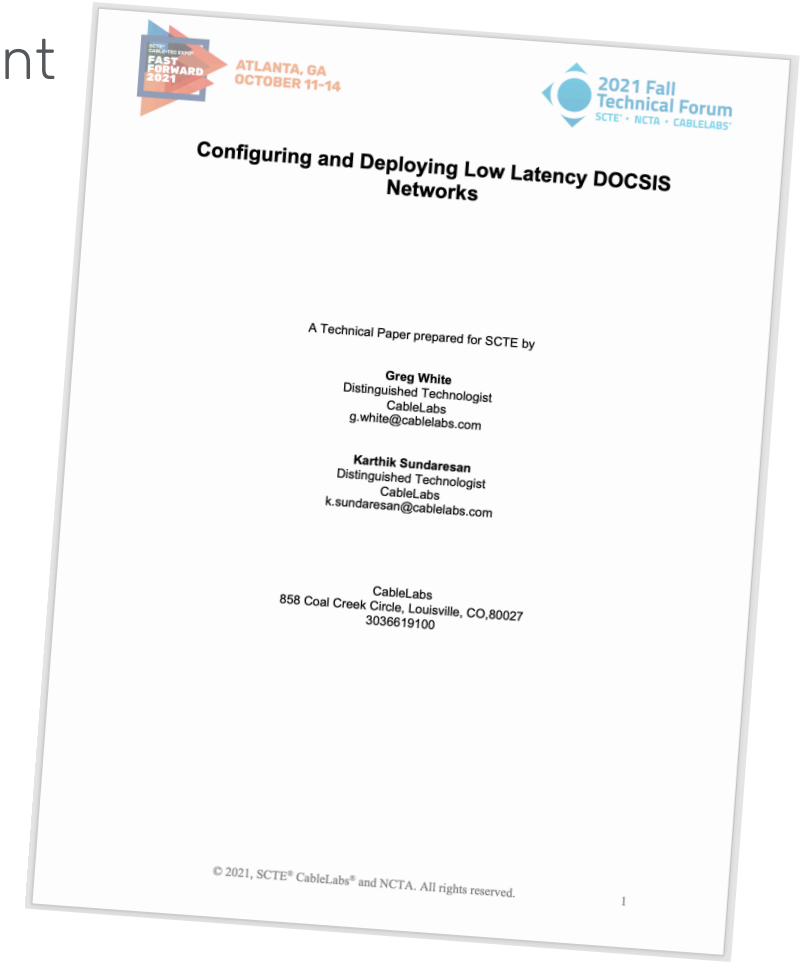
- Proactive Grant Service (PGS)
- MAP interval
  - MAP processing time
- Channel Configuration
  - Upstream: OFDMA frame size or SC-QAM Minislot size
  - Downstream: OFDM Interleaving or SC-QAM Interleaving





Guide to configuring & deploying LLD

- Meant as a reference for engineers planning LLD deployment
- Covering:
  - All of the LLD features
  - What the configuration options are
  - Recommendations
  - Configuration methods
  - How to monitor performance



ATLANTA, GA
OCTOBER 11-14

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

Configuring and Deploying Low Latency DOCSIS Networks

A Technical Paper prepared for SCTE by

Greg White
Distinguished Technologist
CableLabs
g.white@cablelabs.com

Karthik Sundaresan
Distinguished Technologist
CableLabs
k.sundaresan@cablelabs.com

CableLabs
858 Coal Creek Circle, Louisville, CO,80027
3036619100

Brief overview of Pre-LLD latency features (Chapter 2)

Describes Latency Management Features that Pre-date LLD

- Buffer Control (D3.0/D3.1)
- AQM (D3.1)

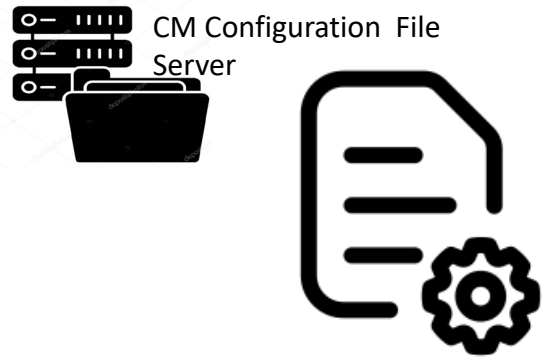
Low Latency Service Configuration (Chapter 4)

- Provides details on configuration options and recommendations for each feature
  - Aggregate Service Flow service rate
  - Low Latency Classifiers & DSCP Overwrite
  - Queue Protection
  - Immediate AQM and Coupled AQM
  - Classic AQM
  - Scheduling Weight
  - Buffer Sizing
  - Proactive Grant Service
  - CMTS MAP Interval

LLD Configuration Mechanisms (Chapter 5)

Covers the available configuration mechanisms :

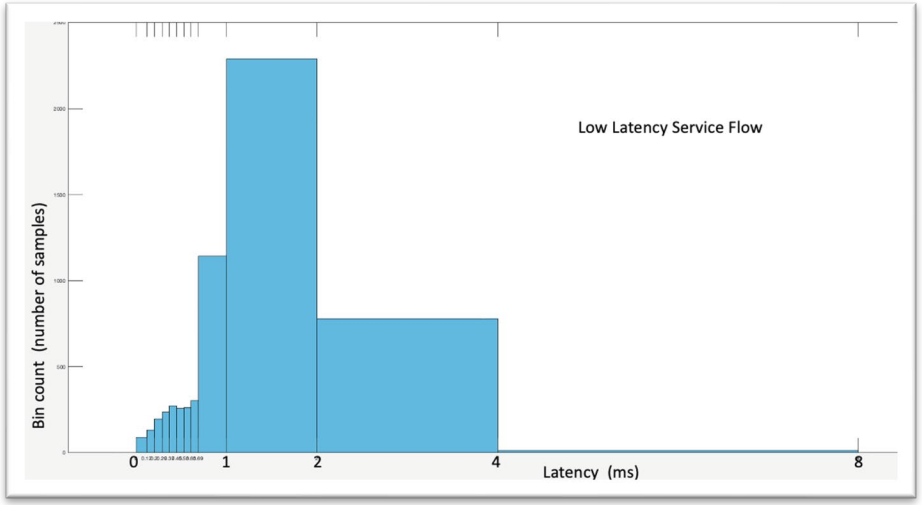
- Aggregate QoS Profile (AQP) Table
- Using existing CM config files & Service Class Name expansion
- Options for new CM config files
  - Using Aggregate QoS Profiles
  - Explicit config file TLVs
- Overriding AQP table parameters
- Classifier Merge Operation
- Primary Service Flows
- Device Capabilities
- Compatibility with pre-LLD CMs
- IPDR Ramifications



Performance Monitoring (Chapter 6)

- New Service Flow Stats counters

- Latency Histograms
  - How to enable histogram calculation on CM and CMTS
  - How to retrieve histogram data
    - SNMP
    - TFTP file upload
  - Examples of using histograms



Two Great Queues

"Classic" Queue and "Low Latency" Queue

Not High Priority / Low Priority

Both queues are optimized for the type of traffic they are designed to carry

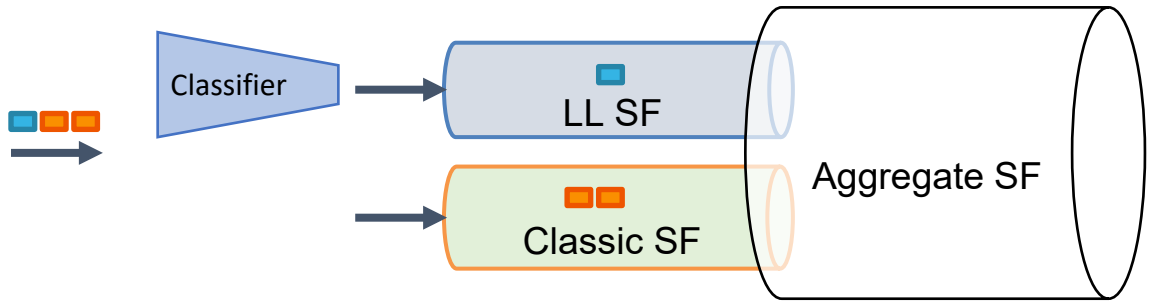
- "Queue Building" flows (HTTP, video streaming, downloads, bulk data) will prefer the classic queue
- "Non Queue Building" flows (latency sensitive apps) will prefer the low latency queue

Classification of Traffic

The application decides which queue would work better for it

LLD Classifier identifies non-queue-building traffic based on packet marking

- For low data-rate flows, use “DSCP” (“Differentiated Services Code Point”) in the IP packet header per IETF "Non-Queue-Building" definition
- For high data-rate flows, use emerging IETF standard - “L4S” (“Low Latency, Low Loss, Scalable Throughput”)



NQB and DSCP marking

"Non-Queue-Building" application flows:

- Send packets at a smooth rate, less than the available capacity
- Sender marks traffic with known DSCP

"NQB" DSCP:

- Given same priority as Best Effort (default) traffic
- In bottleneck links (e.g. DOCSIS, WiFi) provide a separate queue from Best Effort
- Defined in IETF Draft: draft-ietf-tsvwg-nqb

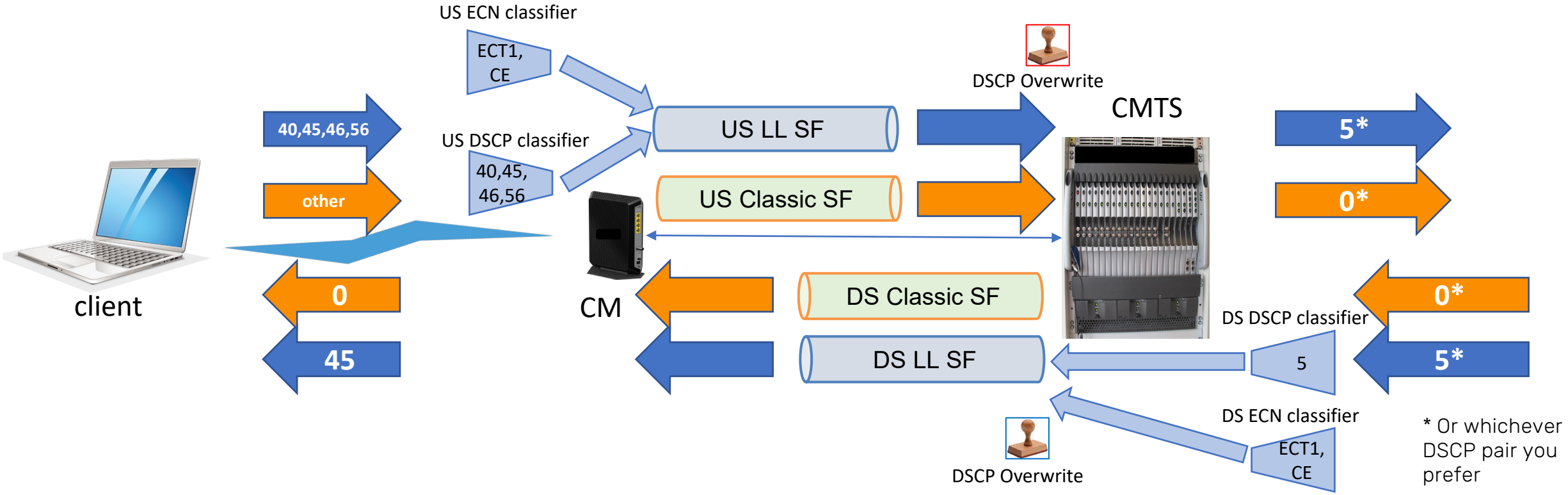
DSCP Usage Today

Recommended to be classified into LL queue

DSCP	WMM	Usage
AF21 (18)	Bckgrnd	Teams Screen Sharing
AF41 (34)	Video	Teams Video Webex Prioritized Video FaceTime Video
AF42 (36)	Video	Webex Opportunistic Video
CS5 (40)	Video	Windows10 ExcellentEffort & AudioVideo Zoom Video & Signaling Several Multiplayer Online Games CableLabs Recommended DSCP for gaming/NQB
NQB (45)	Video	Future IANA & CL Recommended DSCP
EF (46)	Video	Teams Audio Webex Audio Vonage Audio FaceTime Audio
CS7 (56)	Voice	Windows10 Voice & Control Zoom Audio

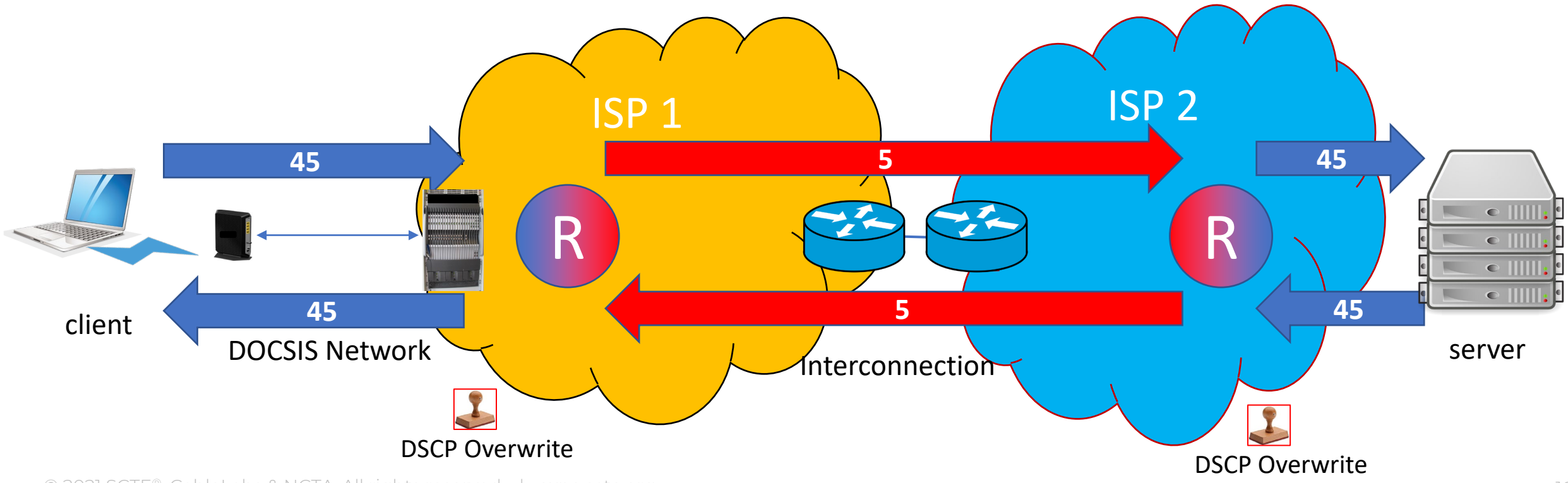
Classifier & Overwrite Recommendations

Configure *both* LL SF and Classic SF to overwrite DSCP in both directions



Classifier & Overwrite Recommendations

NQB DSCP changes through the network



What is “L4S”?

“Low-Latency Low-Loss Scalable” Throughput

- Architecture to enable new congestion control for capacity-seeking applications
- Can be utilized by TCP & QUIC, or by Real-Time Applications
- Solves TCP scalability problem: a single flow can fully utilize a multi-Gbps link
- Solves TCP buffering & delay problem: Can maintain sub-millisecond queuing delay, without causing packet loss
- Can coexist with “classic” TCP via “DualQ-Coupled AQM” or flow-queuing AQM

Defined by IETF & Supported by LLD

Perfect for applications that want high data rates, consistent ultra-low latency, and near-zero packet loss

L4S – How does it work?

Requires support in sender, receiver and network bottleneck

- Sender support
  - A congestion controller built against the “Prague requirements”, e.g.:
    - TCP Prague, QUIC Prague, BBRv2 (TCP/QUIC), SCReAM (UDP/RTC)
  - Marking IP packets as “ECT1” in the Explicit Congestion Notification field
- Bottleneck link support
  - Provide immediate feedback as to level of queuing delay using Explicit Congestion Notification marking
    - Sender no longer needs to infer congestion based on RTT variation or loss
    - Disambiguates congestion from other delay sources
  - Two implementations
    - Dual-Q Coupled AQM (e.g. LLD)
    - fq_codel+iaqm
- Receiver support
  - “Accurate ECN” feedback

ECN Traversal

ECN field MUST NOT be bleached

- Per RFC3168 & RFC8311, the only allowed transitions by a network are:

Received as:	Allowed to send as:
NotECT (00)	NotECT (00)
ECT1 (01)	ECT1 (01) or CE (11)
ECT0 (10)	ECT0 (10) or CE (11)
CE (11)	CE (11)

DOCSIS ToS Overwrite has the power to overwrite ECN

- some MSOs have incorrectly configured it!

At interconnection, some MSOs are bleaching ECN!

ECN Traversal Probe Network

CableLabs has launched a network of probes to help MSOs identify routers that are bleaching ECN

Two target probe locations:

- In the “cloud” (e.g. AWS, Azure, GoogleCloud)
- Behind customer broadband (DOCSIS) links

Seeking volunteers to create probes in additional locations

- Buy a Raspberry Pi, install the software, plug it in to your home network
- Create an Ubuntu VM

Contact me if you’d like more info!

- g.white@cablelabs.com

Via this network, we’ve already found a bug that affects ISP routers that use a particular 10 Tbps NPU

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs

Thank You!

Greg White

Distinguished Technologist
CableLabs
g.white@cablelabs.com

Karthik Sundaresan

Distinguished Technologist
CableLabs