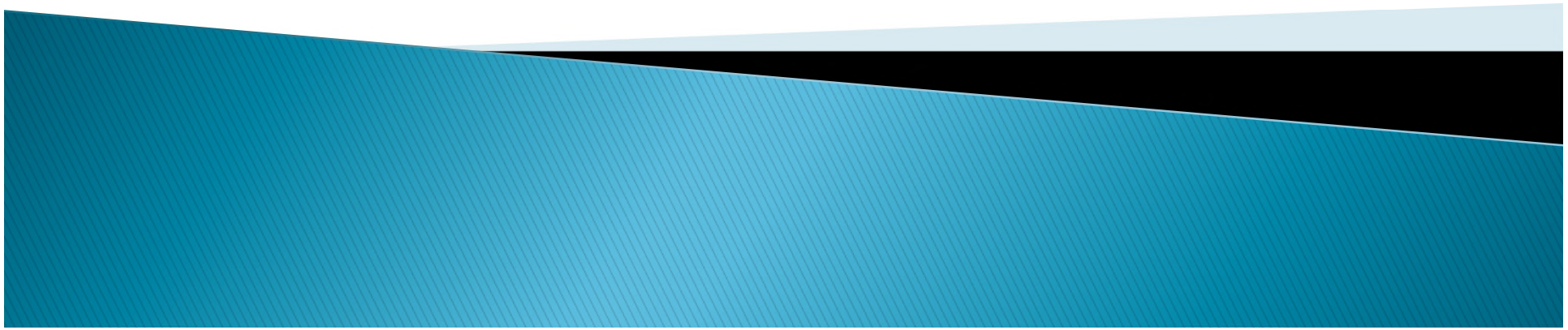
Digital Transmission Licensing Administrator

DTCP2

Presentation to CPTWG

January 27, 2016



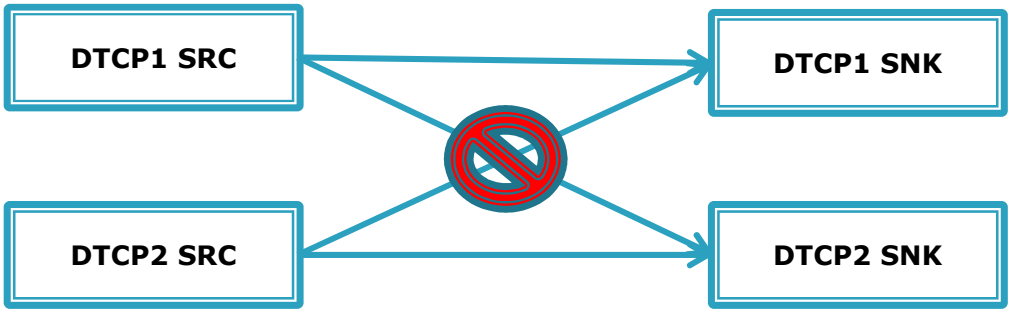
DTCP2 Protection Basics

- Robust content protection system developed for "Enhanced Image" as well as current audiovisual formats
- Stronger cryptographic elements
- Hardware root of trust
- DTCP2 Core Functions implemented in hardware
- Meets or exceeds MovieLabs requirements for link protection systems
- Security and robustness equal to or greater than HDCP 2.2

DTCP2 - Cryptographic Elements

- NIST P-256 Elliptic Curve
  - Increased cryptographic strength over existing curve
- AES-128 encryption
- SHA-256
  - Increased hash authentication over current SHA-1
- Full Authentication only
- NIST SP 800-90A Rev1 for DRNG

Distinct from DTCP-IP



DTCP-IP and DTCP2 do not interoperate as they use different sized elliptic curves.

DTCP2 – Licensing

- New DTCP2 Specification
  - Mapped initially to IP
- New Compliance and Robustness Rules for Adopter Agreement
- No changes to Content Participant Agreement
- No changes to IP Statement
  - Enables any content owner to require DTCP2 encoding without license or fee

DTCP2 - Two Levels of Compliance and Robustness Rules

- **L2** requires higher levels of robustness and output/recording protection
  - Robustness Rules require "DTCP2 Core Functions" to be implemented in hardware
  - Compliance Rules require higher output protection (e.g., HDCP2.2); analog output not permitted
- **L1** permits handling of content in a manner equivalent to current DTCP-IP

Four New CMI Flags

- "L2-Only" Flag
- "EI" Flag
- "HDR" Flag
- "SDO" (Standard Digital Output) Flag

- Flags set per upstream requirements, consistent with other outputs
  - E.g.,
    - SDO set in accordance with AACS2 Rules
    - L2-Only and HDR set upstream by content provider rules or mapped to content protection system rules

- Perpetuate protections downstream

L2-Only Flag

- Settings
  - 0 = Content may be protected using L1 or L2
    - Protected output permitted as Enhanced Image or Non-Enhanced Image
  - 1 = Content shall be protected using L2
    - May be downconverted to non-EI but must be protected using L2

- "L2" requires higher level Compliance and Robustness Rules.
- "L1" requires DTCP1 level Compliance and Robustness Rules.

Note: Both L1 and L2 permit output using current and future content protection technologies approved per change management.

EI Flag

- Settings
  - 0 = Content is Non-Enhanced Image
  - 1 = Content is Enhanced Image

  - "Enhanced Image"
    - i.e., audiovisual works with image quality surpassing "HD" audiovisual works (i.e., resolution at <=1920x1080 pixels, standard color space for HD quality (BT.709), and standard peak luminance for HD quality (100 nits)).
  - "Non-Enhanced Image"
    - i.e., image quality at or below HD audiovisual works

HDR Flag

- Settings
  - 0 = Content with HDR may be downconverted to SDR
  - 1 = Content with HDR may not be downconverted to SDR (unless permission is signaled using non-DTCP methods)
- Requires use of SDR version available to the Sink Device, to avoid problems caused by HDR-to-SDR downconversion or displays that do not support HDR

SDO Flag

- Settings
  - 0 = Content in Enhanced Image quality shall only be passed to Approved L2 protection technologies. L1 permitted if downconverted to Non-Enhanced image.
  - 1 = Content may be passed to any Approved L1 or L2 content protection technologies as Enhanced Image or Non-Enhanced Image.
- Inherits SDO as set by content owner under AACS2 rules

Logic for Flags

- Source device should apply flags consistent with other outputs permitted by upstream rules
  - i.e., upstream technology should similarly restrict the same content when passed to other technologies
- Devices should respond logically to flag combinations
  - Examples:
    - If upstream technology permits L1 output of EI content, then HDR flag should be deemed non-asserted (Don't Care)
    - If upstream technology sets SDO flag, then L2-Only flag and HDR flag should be deemed non-asserted (Don't Care)

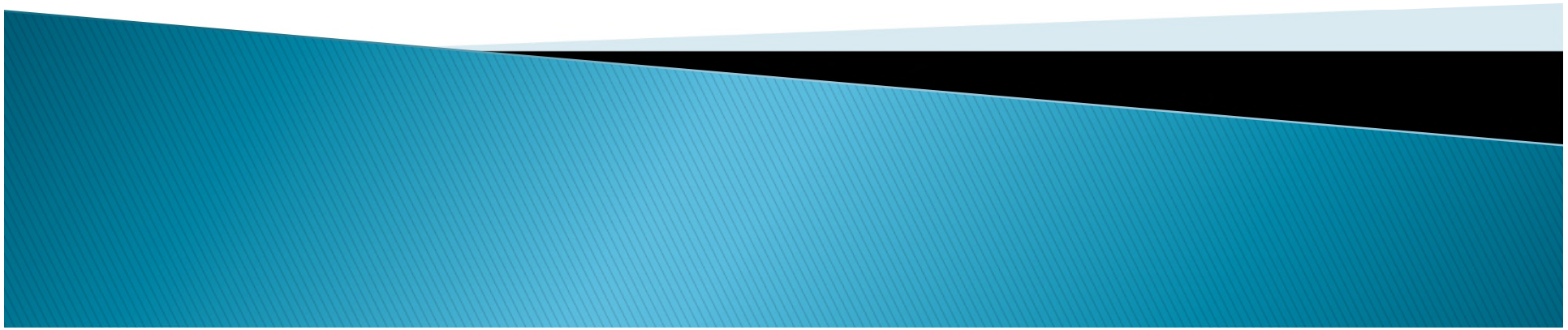
Results of Flag Combinations

L2-Only Flag	HDR Flag	SDO Flag	EI Flag	Output Results
1 (Asserted)	1 (Asserted)	0 (Not Asserted)	*Don't care*	•L2 required •No downconversion to SDR •L1 not permitted
1 (Asserted)	0 (Not Asserted)	0 (Not Asserted)	*Don't care*	•L2 required for both Enhanced Image and Non-Enhanced Image •Downconversion to SDR also permitted •L1 not permitted

Results of Flag Combinations

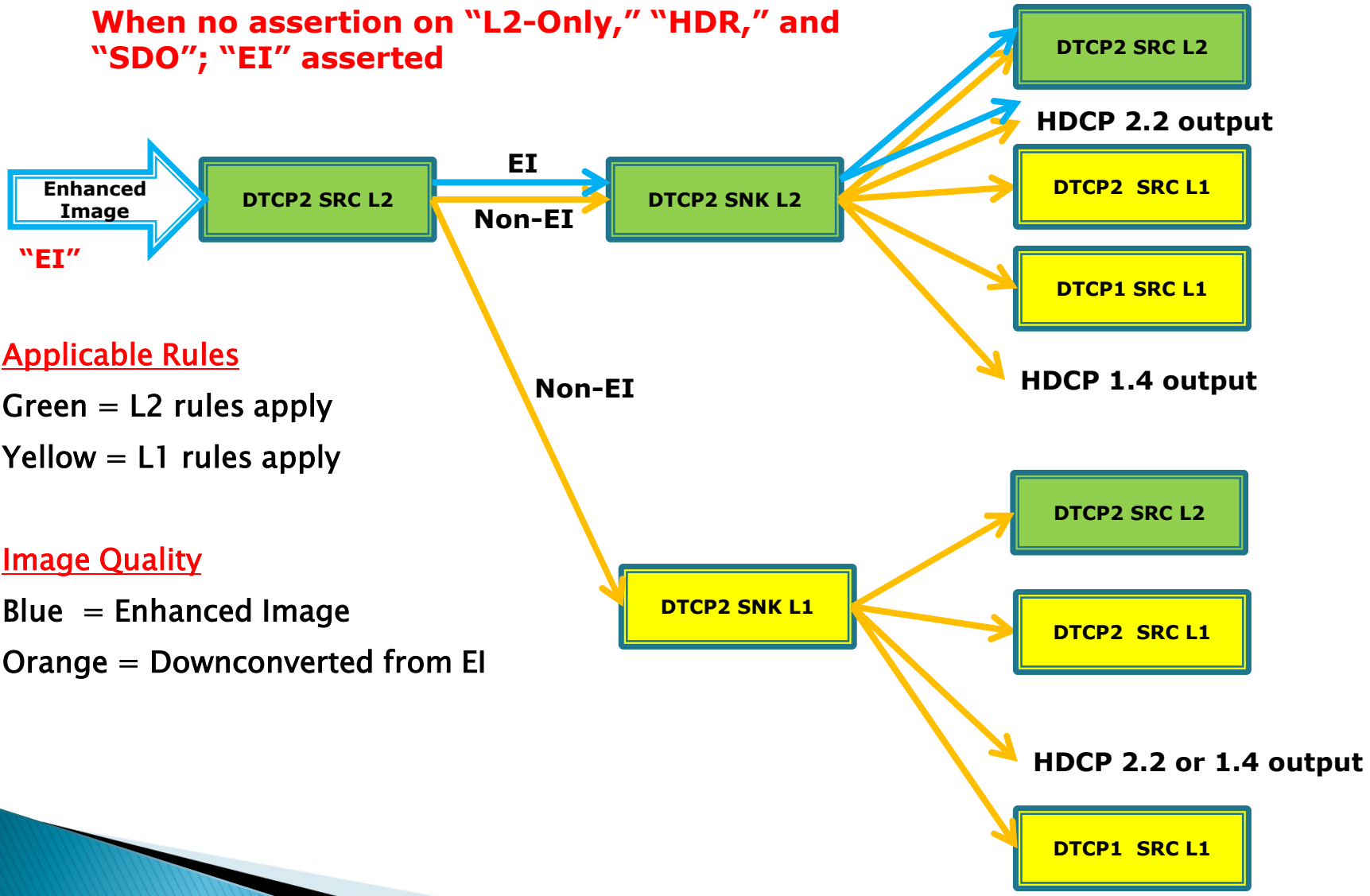
L2-Only Flag	HDR Flag	SDO Flag	EI Flag	Output Results
0 (Not Asserted)	*Don't Care*	0 (Not Asserted)	1 (Asserted)	•L2 required for Enhanced Image •L1 permitted for Non-Enhanced image downconverted from Enhanced Image; can set SDO to Asserted
0 (Not Asserted)	*Don't Care*	0 (Not Asserted)	0 (Not Asserted)	•L2 and L1 permitted; can set SDO to Asserted
Don't Care	*Don't Care*	1 (Asserted)	*Don't Care*	•L2 and L1 permitted

DTCP-2 Use Cases



Use Case 1a: Upstream = Enhanced Image

When no assertion on "L2-Only," "HDR," and "SDO"; "EI" asserted



Applicable Rules

Green = L2 rules apply

Yellow = L1 rules apply

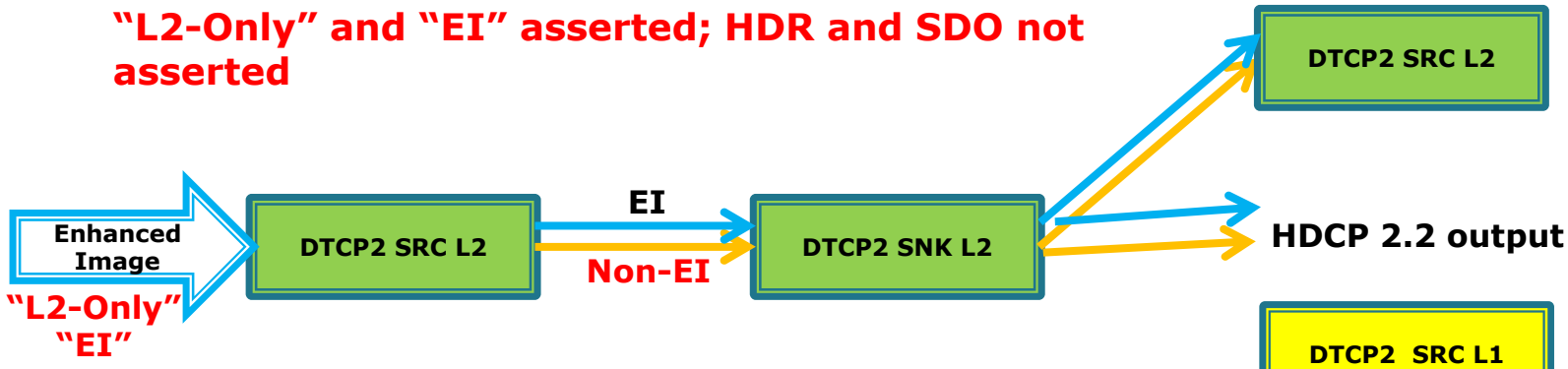
Image Quality

Blue = Enhanced Image

Orange = Downconverted from EI

Use Case 1b: Upstream = Enhanced Image

"L2-Only" and "EI" asserted; HDR and SDO not asserted



Applicable Rules

Green = L2 rules apply

Yellow = L1 rules apply

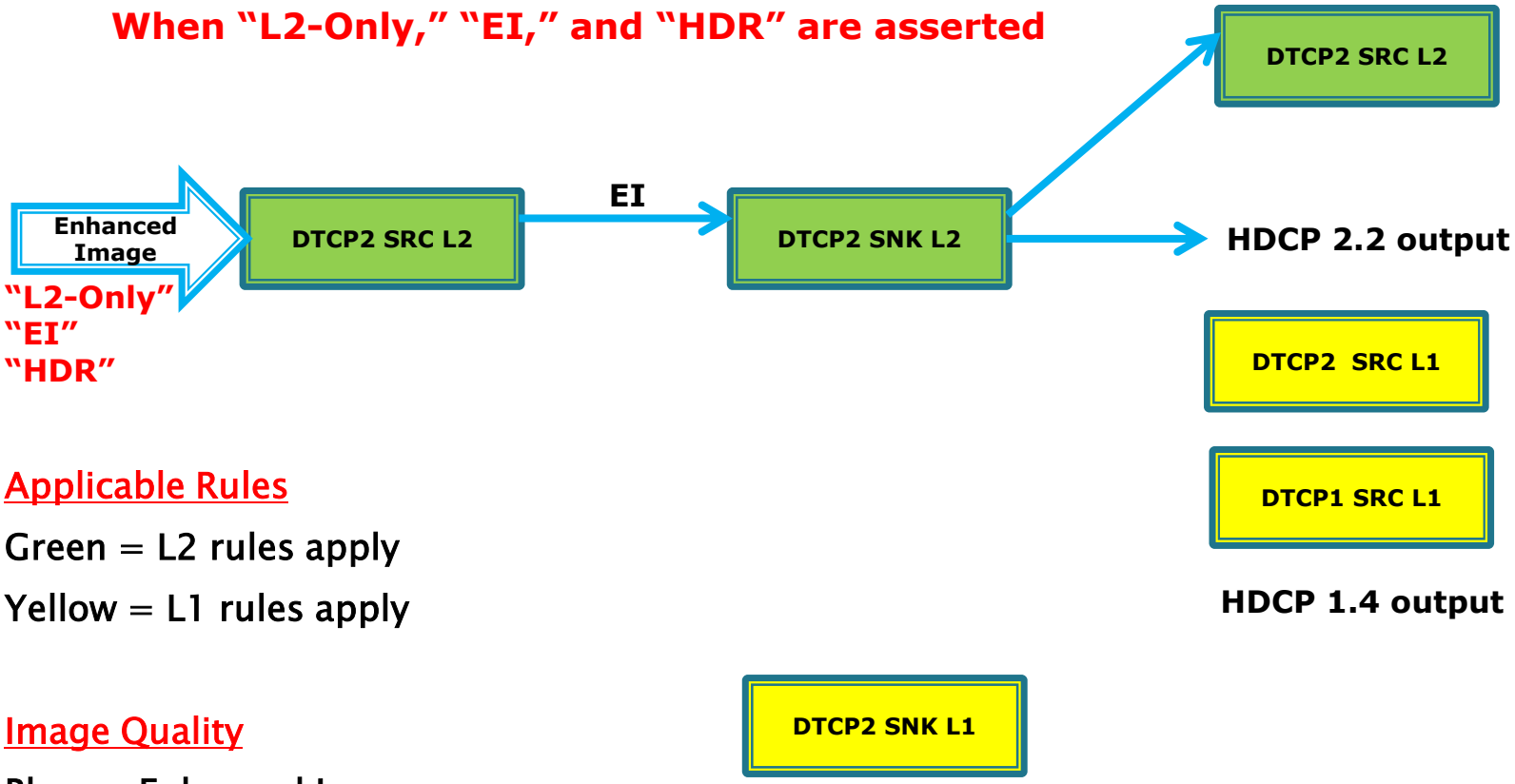
Image Quality

Blue = Enhanced Image

Orange = Downconverted EI

Use Case 1c: Upstream = Enhanced Image

When "L2-Only," "EI," and "HDR" are asserted



Applicable Rules

Green = L2 rules apply

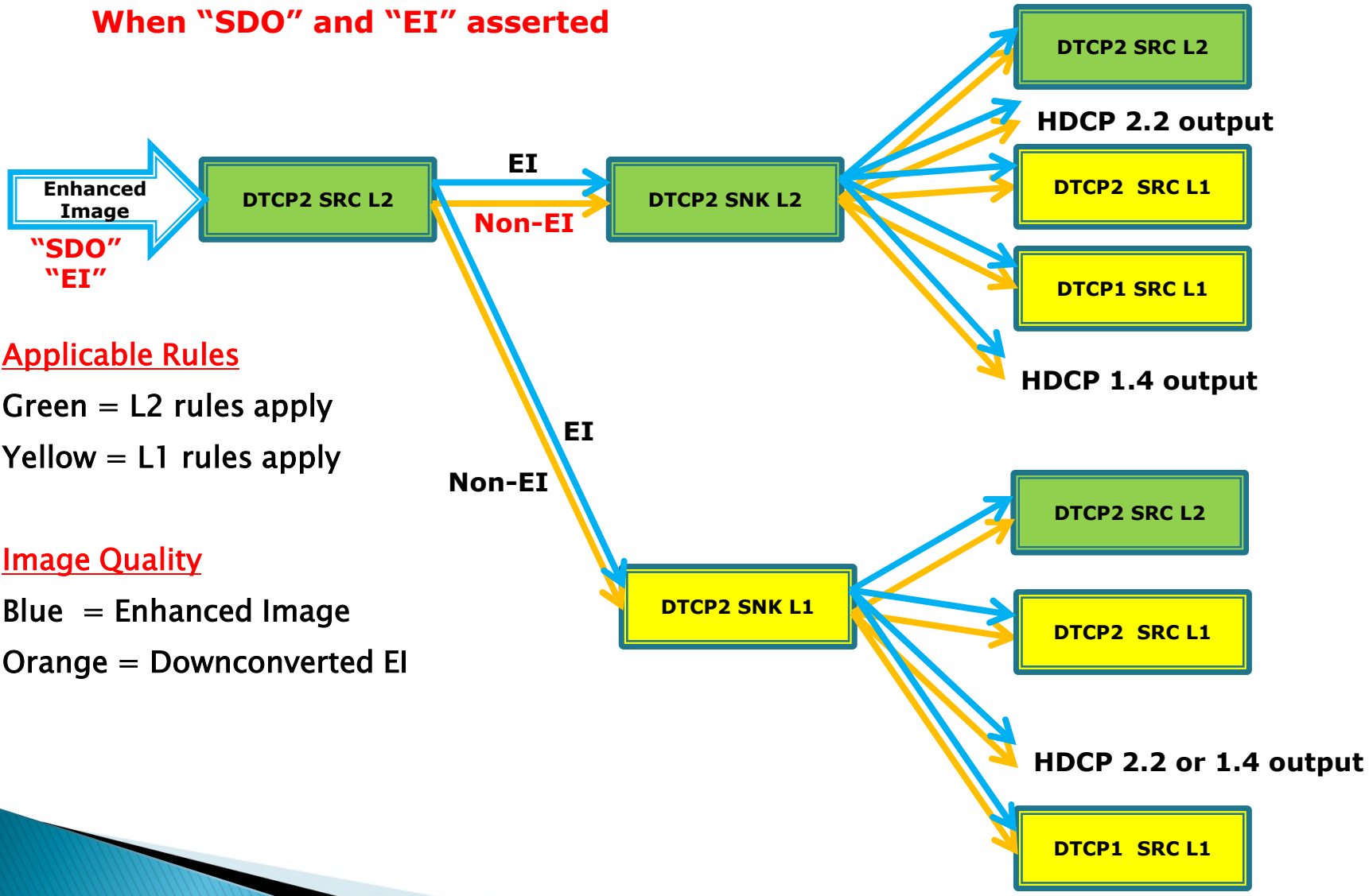
Yellow = L1 rules apply

Image Quality

Blue = Enhanced Image

Use Case 1d: Upstream = Enhanced Image

When "SDO" and "EI" asserted



Applicable Rules

Green = L2 rules apply

Yellow = L1 rules apply

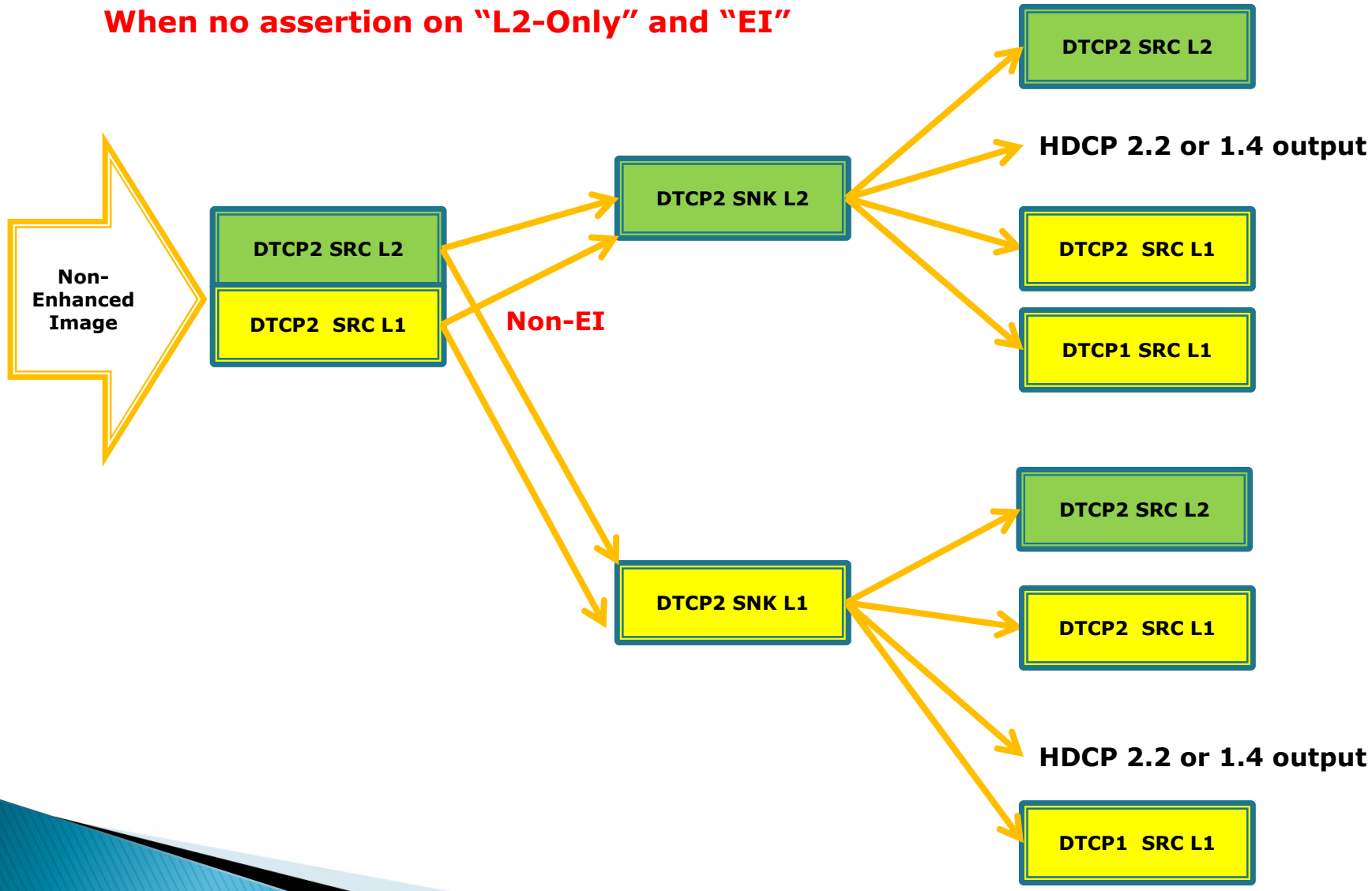
Image Quality

Blue = Enhanced Image

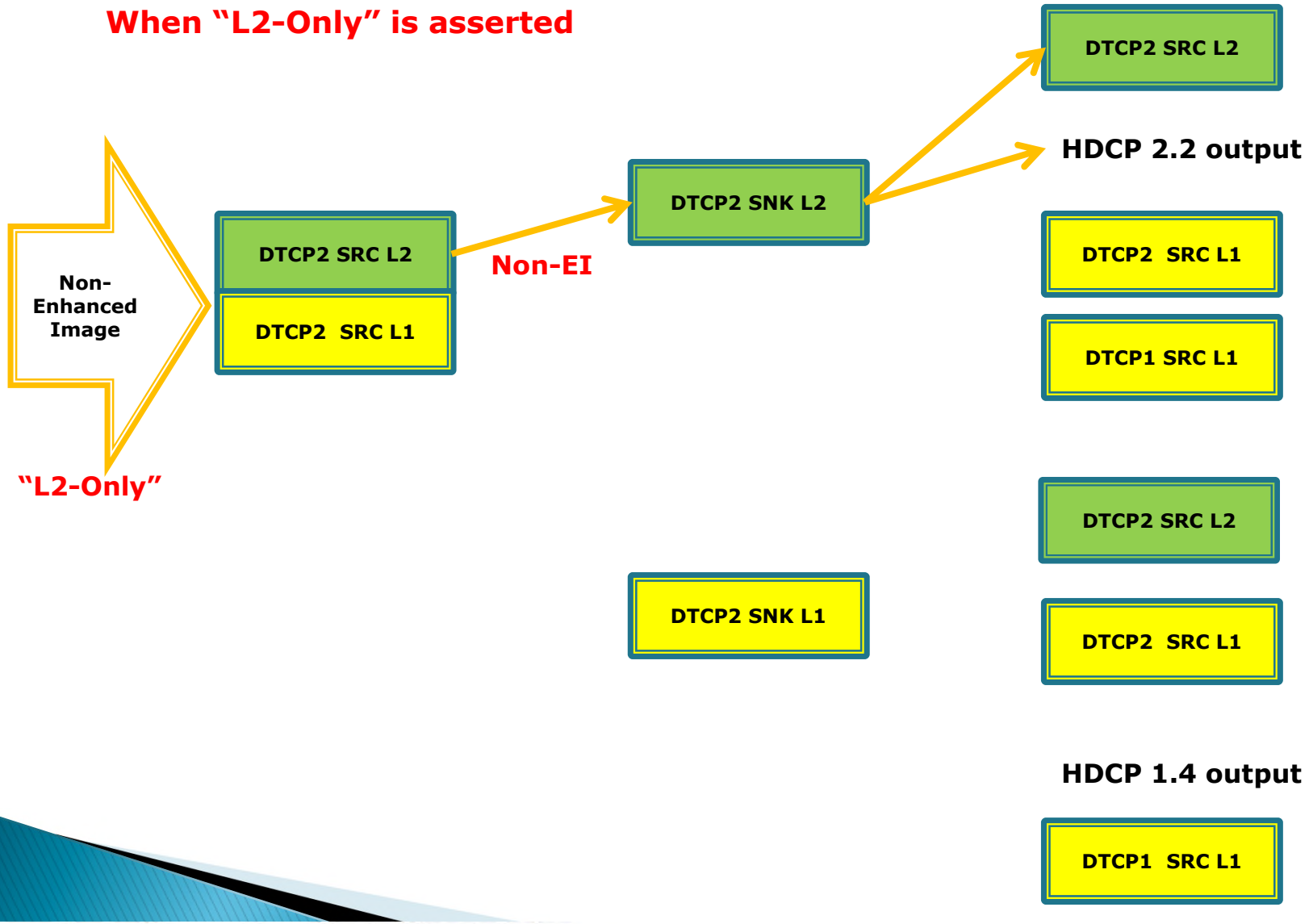
Orange = Downconverted EI

Use Case 2a: Upstream = Non-Enhanced Image

When no assertion on "L2-Only" and "EI"



Use Case 2b: Up Stream = Non-Enhanced Image



Digital Transmission Licensing Administrator

DTCP2

Questions?