

# Framework for Signaling Flow Characteristics between Applications and the Network

Toerless Eckert, Reinaldo Penno, Amine Choukir, Charles Eckel

# Where am I?



Networked media capacity and importance exploding

New channels for creating and consuming rich media deployed at rapid pace

Pervasive video and on demand access becoming second nature to consumers

Communication applications making extensive use of rich media

All available capacity saturated at whatever rate it is added

# Where do I want to be?



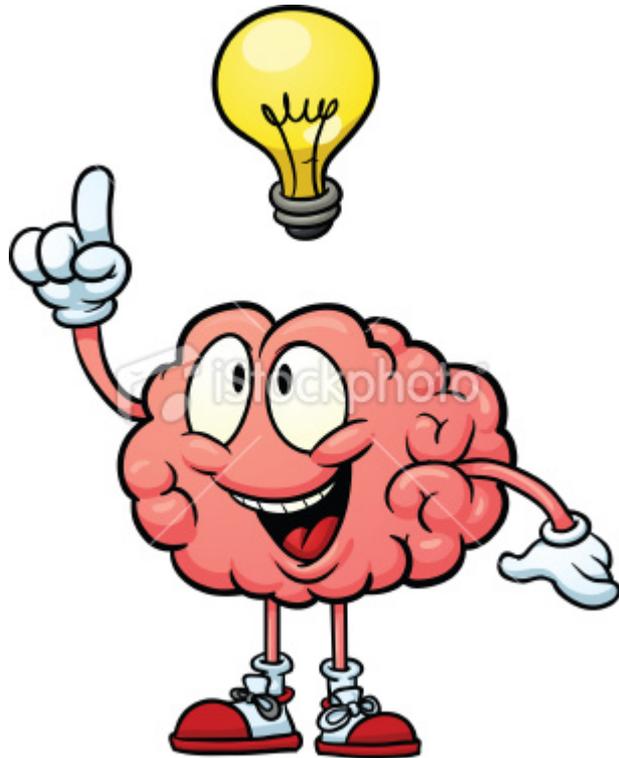
Users enjoy a consistently good experience for content that is most important to them

Operators able to add value by improving Quality of Experience (QoE) for services they provide as well as for Over-the-Top (OTT) applications

Applications coexist, sharing existing network resources predictably

Users gain visibility into network state and adapt expectations accordingly

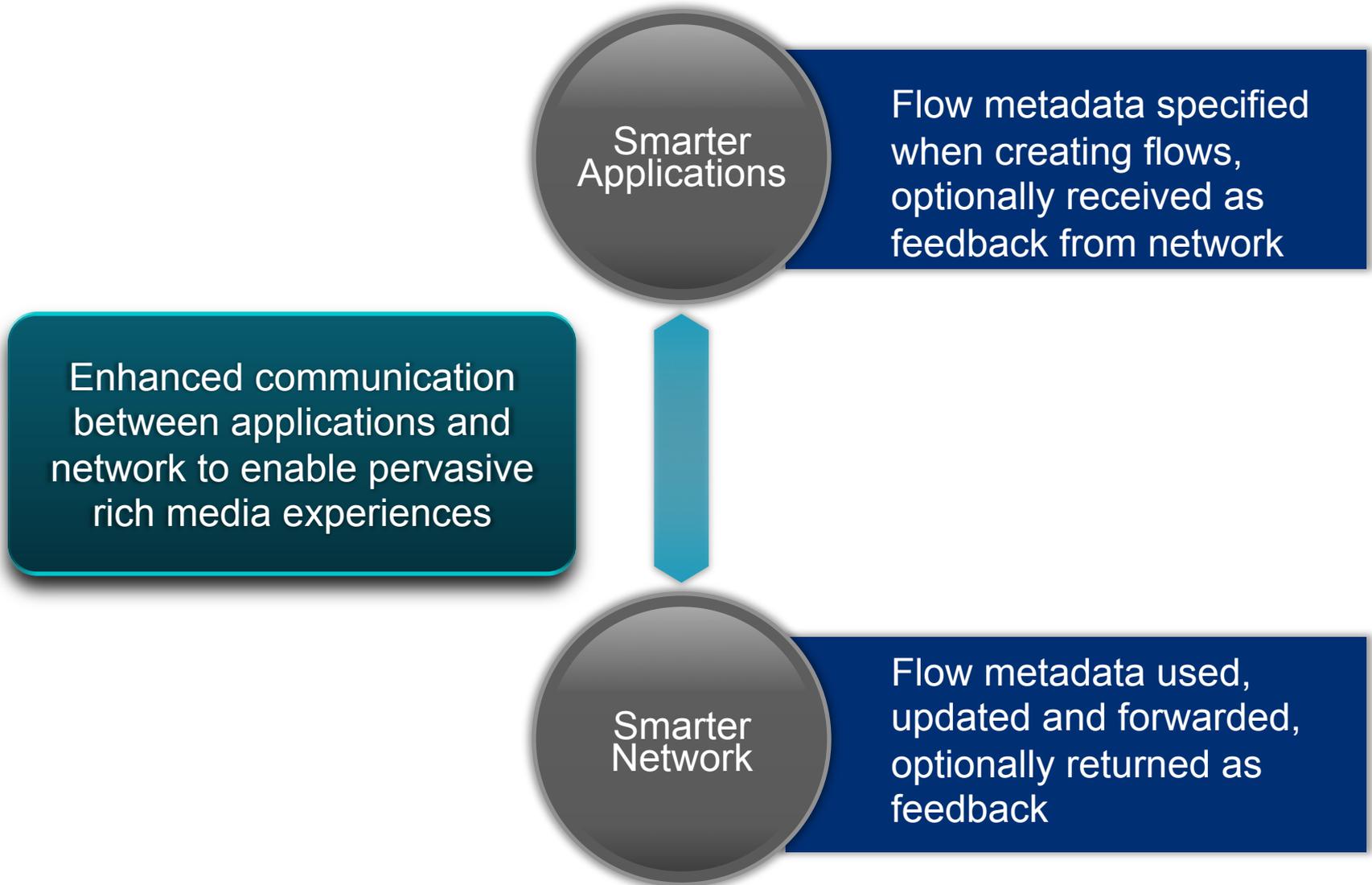
# Flow Metadata



Cooperation between applications and network infrastructure is key to improving experience and efficiency of networked media, enabling:

- applications to interact with underlying infrastructure
- infrastructure to optimize delivery of media for best possible QoE
- operational efficiency, uniform manageability, and scalability of deployments
- business models that permit networks to be recognized for entitling this differentiation

# What is a Flow Metadata?



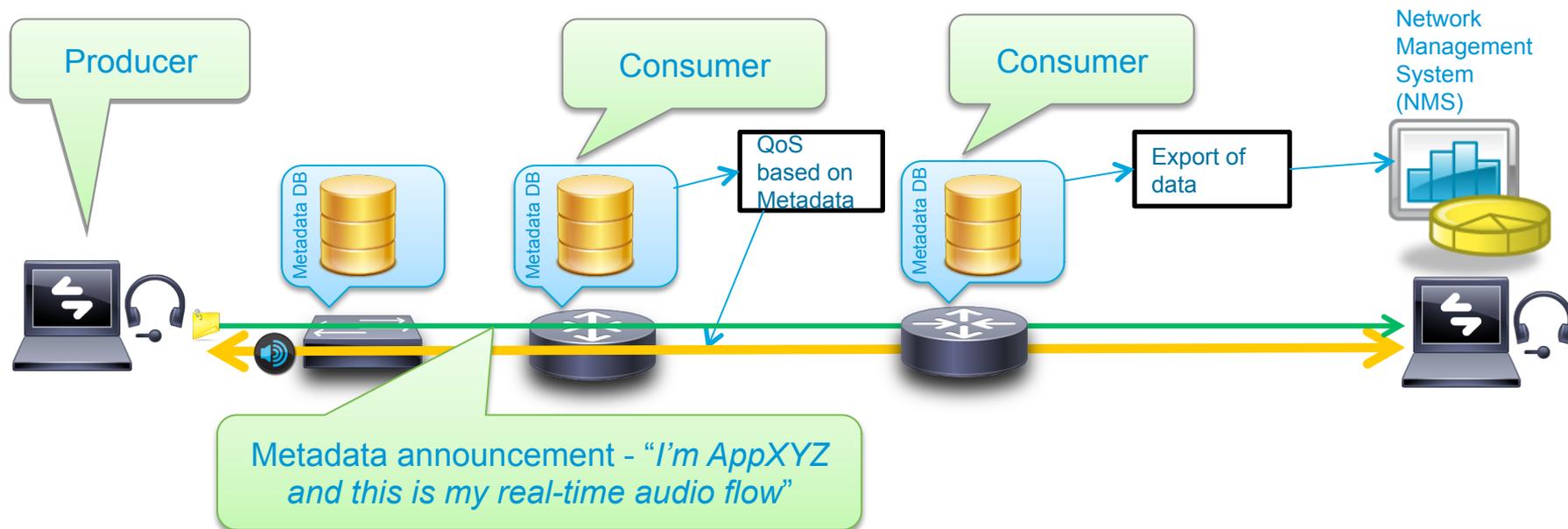
# Why Is It Needed

Visibility	How?	Mechanisms	Technologies	Considerations
Good	Network administrator configures network elements	Manual: Static configuration	Access control lists (ACL), IP address ranges, port ranges	Achieving scale, adding new devices or applications
Better	Network figures it out	Implicit: Packet and flow signatures, inspection of associated signaling	Vendor specific Deep Packet Inspection (DPI) and Application Layer Gateways (ALGs)	Encryption, application velocity, protocol changes, platform limits
<b>Best</b>	<b>Application tells network</b>	<b>Explicit: Application signals to network</b>	<b>Flow Metadata</b>	<b>Communicates flow attributes along path of flow</b>

# Flow Metadata Example

## Enterprise QoS and Enhanced Manageability

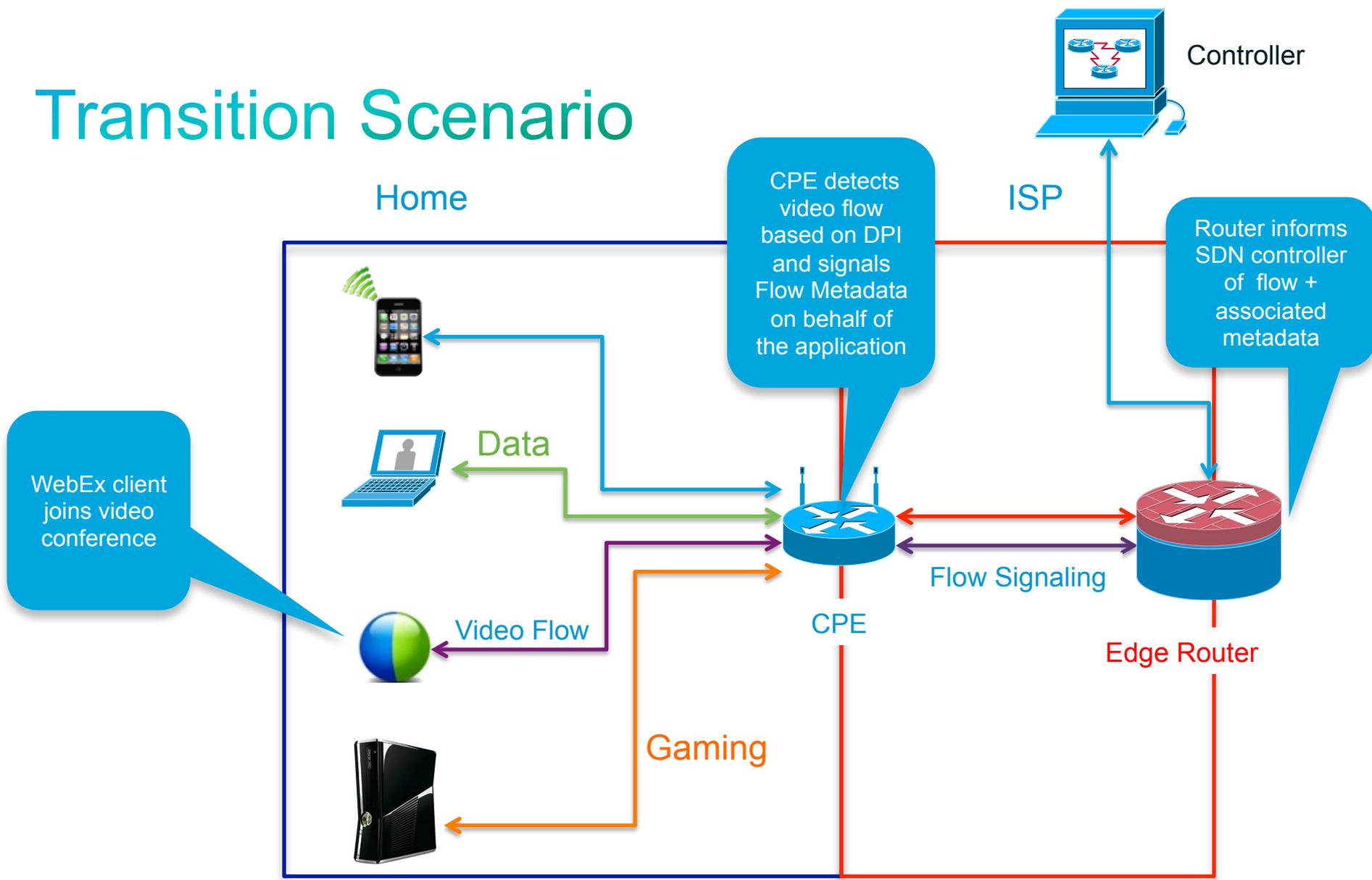
- Producer: creates flow metadata
- Consumer: utilizes flow metadata
- Flow DataBase: maintains flow attribute information



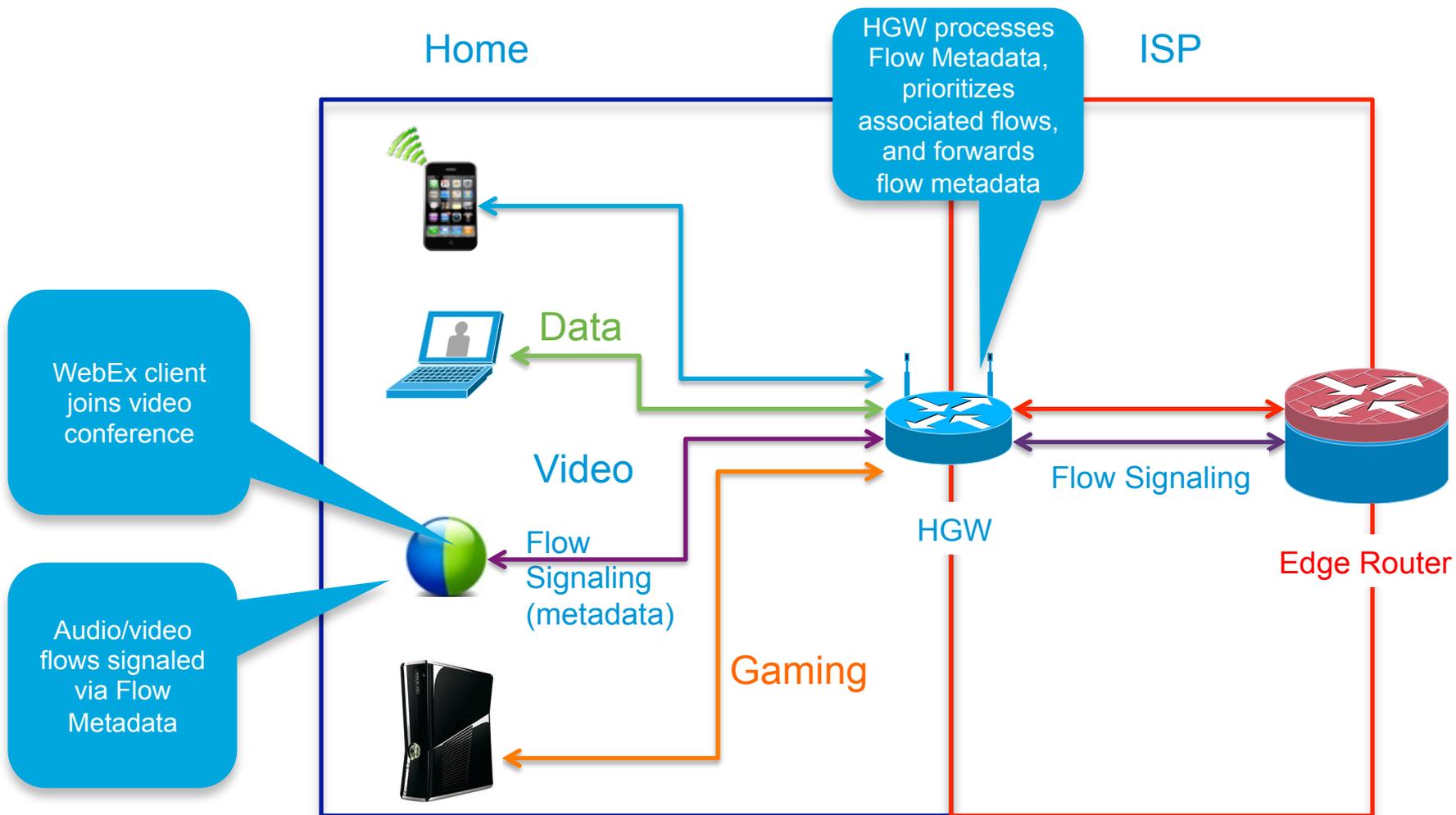
# Transition Scenario & Incremental value

- While applications do not support Flow Metadata, CPE and other Flow Metadata enabled devices can signal the network on behalf on those applications.
- Immediate incremental value for endpoints and applications: If a CPE is upgraded, applications could signal flow characteristics on both directions requesting traffic prioritization, firewall pinholes and other services without changing the rest of the network.

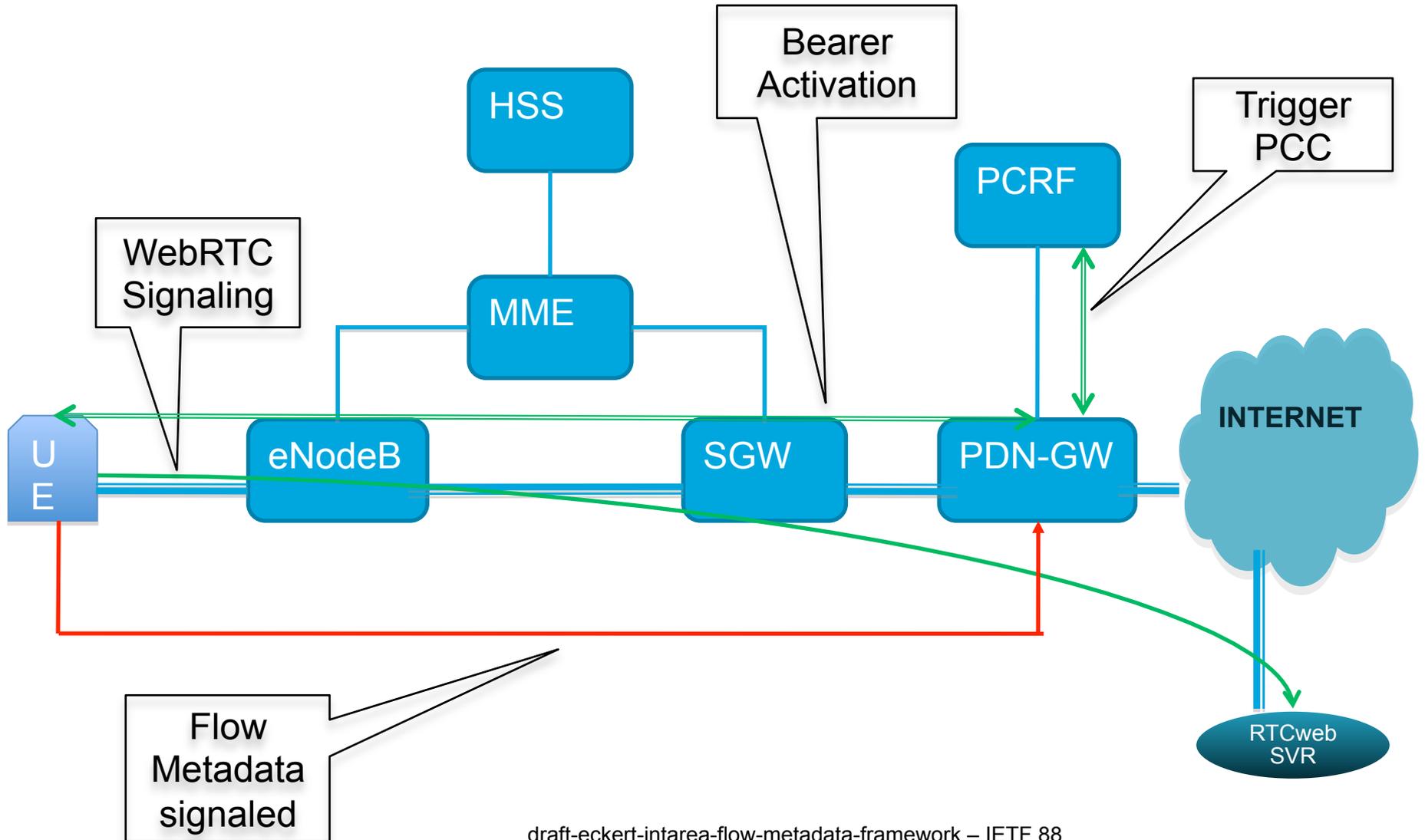
# Transition Scenario



# Incremental Value



# Flow Metadata in Mobile Network for OTT



# Security Considerations

Security is considered at two levels:

## 1. Encoding Level

- Provided as part of the encoding of the flow metadata
- E.g. Security token mechanism in: [draft-choukir-tsvwg-flow-metadata-encoding](#)

## 2. Protocol Level

- Provided by the protocol used to transport the flow metadata
- PCP provides some inherent security properties, and drafts exist proposing additional authentication mechanisms
- STUN provides short term and long term credential mechanisms

Encoding specific and protocol specific security mechanisms may be used in combination to achieve required level of security

# IETF Drafts

- [draft-eckert-intarea-flow-metadata-framework](#) provides:
  - framework to communicate information elements (a.k.a. metadata) in consistent manner between apps and network
- [draft-choukir-tsvwg-flow-metadata-encoding](#) describes a protocol independent encoding for flow metadata
- Various signaling protocols used to transport flow metadata:
  - PCP ([draft-wing-pcp-flowdata](#))
  - RSVP ([draft-zamfir-tsvwg-flow-metadata-rsvp](#))
  - STUN ([draft-martinsen-mmusic-malice](#))
  - Others ...