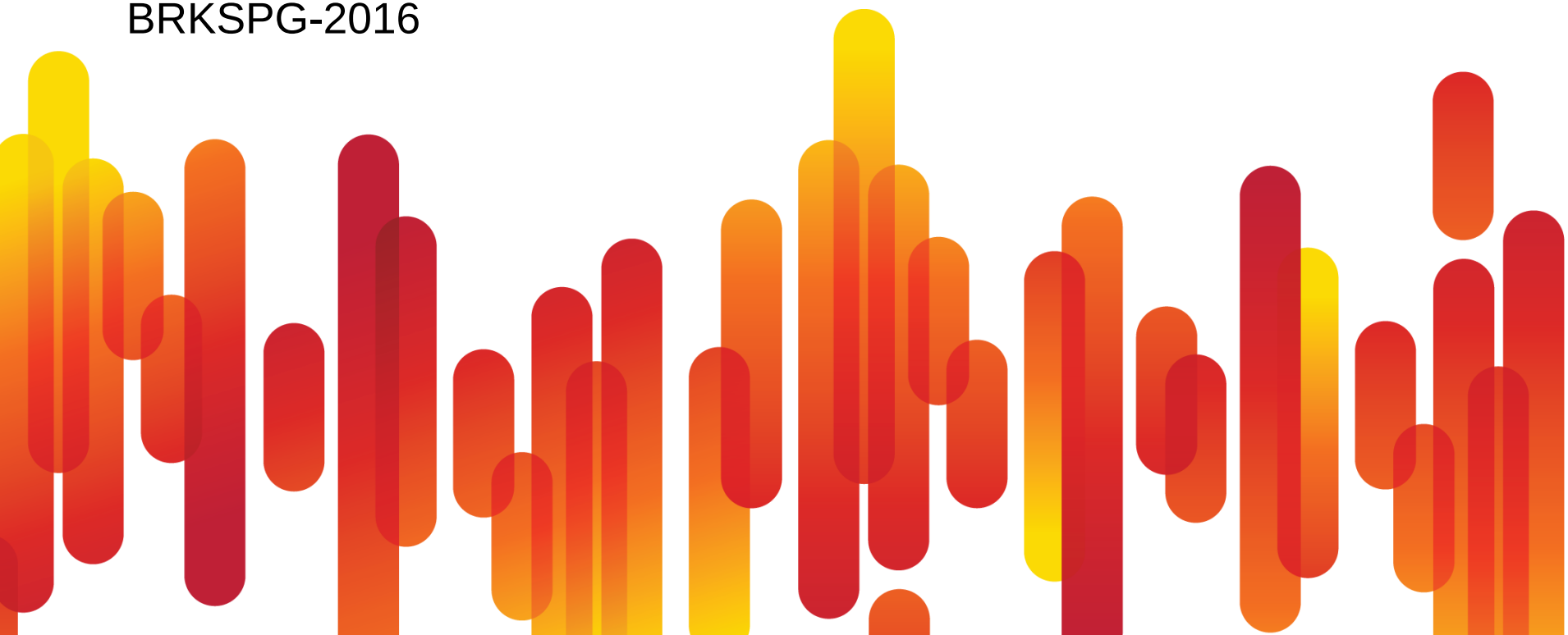
Architectures for new services over Cable

BRKSPG-2016



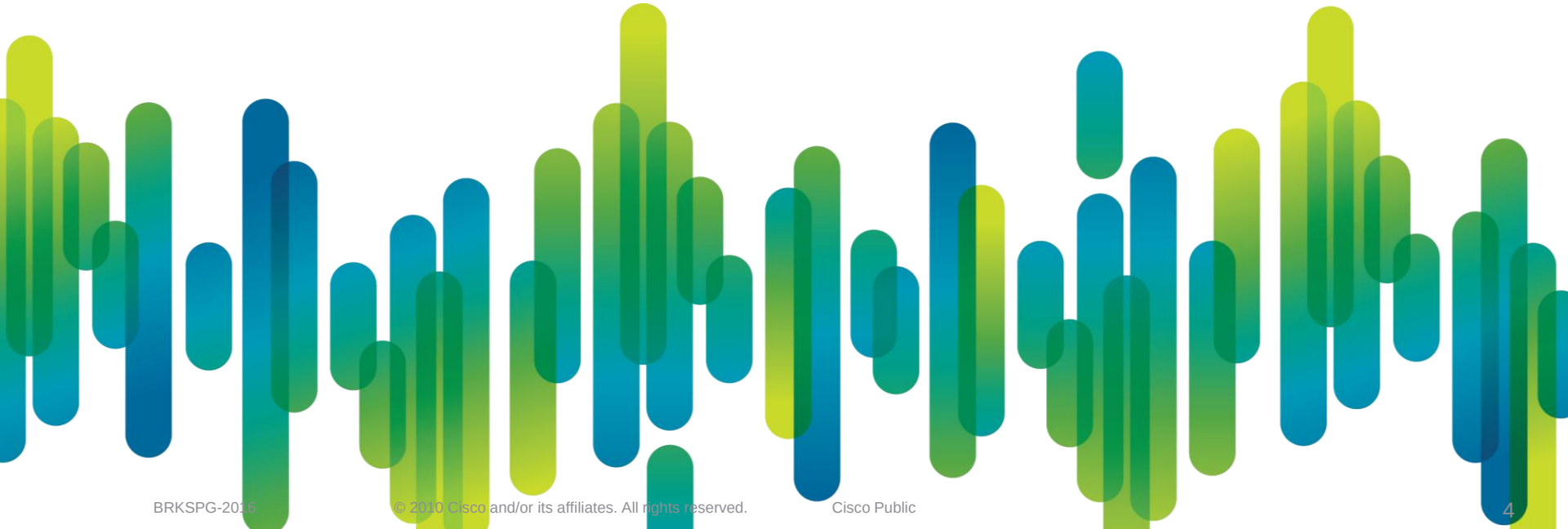
Abstract

- This session will describe the key advantages and possible solutions and architectures to enable Cable MSO's to deploy new advanced services such as broadcast video and VOD (VDOC), business services (BSoD) along with HSD and Voice services, incorporating the DOCSIS 3.0 specifications, IPv6, Multicast, Security and QOS.
- This session is targeted to Cable operators wishing to develop next generation services over Cable.
- A minimum understanding of current DOCSIS 1.0 or DOCSIS 1.1 is required.

Agenda

- EuroDOCSIS 3.0 Overview
- The Case for Next Generation Services over DOCSIS
- Video Over DOCSIS deployment models
- Carrier Ethernet Business Services
  - L2VPN over DOCSIS Deployment Models
    - CPE-Based L2VPN
    - Transparent LAN Services over DOCSIS
    - Dot1Q-Based Business Services over DOCSIS
    - MPLS-Based Business Services over DOCSIS
- Architectural Deployment considerations
  - Scaling to IPv6
  - Network QoS requirements
  - Network security
- Summary

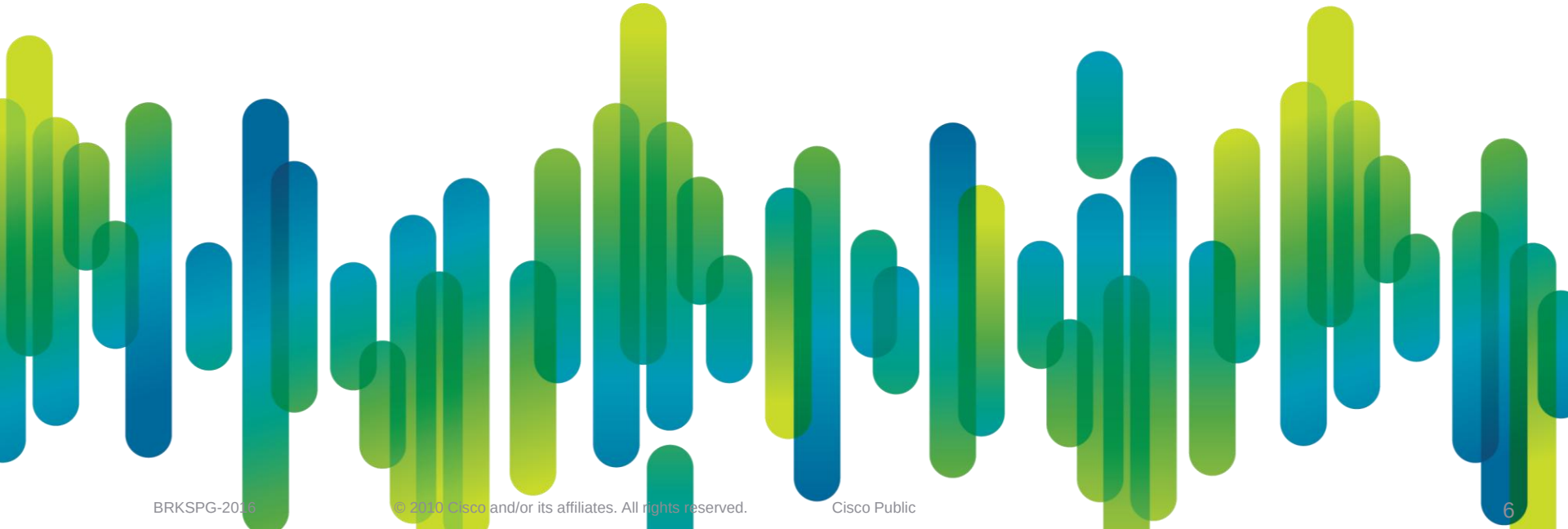
DOCSIS 3.0 Overview



DOCSIS 3.0 Features

- Channel Bonding
  - Upstream Channel Bonding
  - Downstream Channel Bonding
- MAC Layer
  - Topology and ambiguity resolution
  - Latency and Skew measurements
  - CM Status and Control
- Security
  - Enhanced Traffic Encryption
  - Enhanced Provisioning Security
- Network Management
  - CM Diagnostic Log
  - Enhanced Signal Quality Monitoring
  - IPDR Service Statistics Reporting
  - Capacity Management
- IPv6
  - IPv6 Provisioning & Management of CMs
  - Alternative Provisioning Mode & Dual-stack Management Modes for CMs
  - IPv6 Connectivity for CPEs
- IP Multicast
  - Source Specific Multicast (SSM)
  - PHS, QoS, and Authorization
  - IGMPv3/MLDv2
- Physical Layer
  - Extended US/DS Freq Range
  - S-CDMA Active Code Selection
- Business Services over DOCSIS
  - Layer 2 Virtual Private Networks
  - Support for T1/E1 Emulation

The Case for Next Generation Services Over DOCSIS



Video 2.0
Shaping the Network

Content is driving massive bandwidth demand…beyond current HFC plant capacity

- More HD channels
- Ethnic programming tiers
- "Long tail" & user-generated content

Ethnic Content

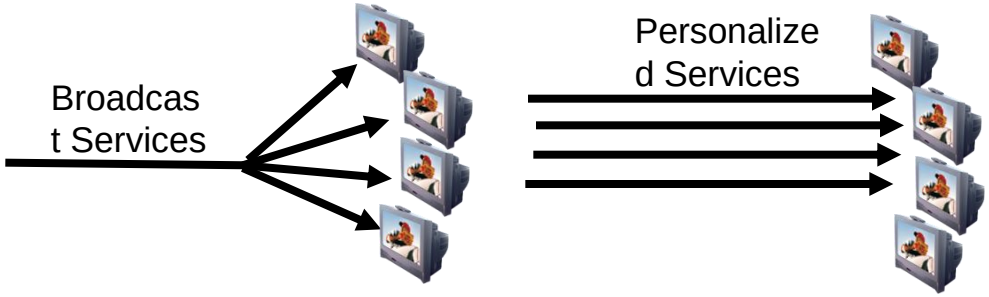
Long Tail Content

Consumers are demanding content anywhere, anytime, on any device

- Inside and outside the home
- Need QoS assurances on "shared" networks
- Network must adapt content to screen size, bitrate, codec, etc.

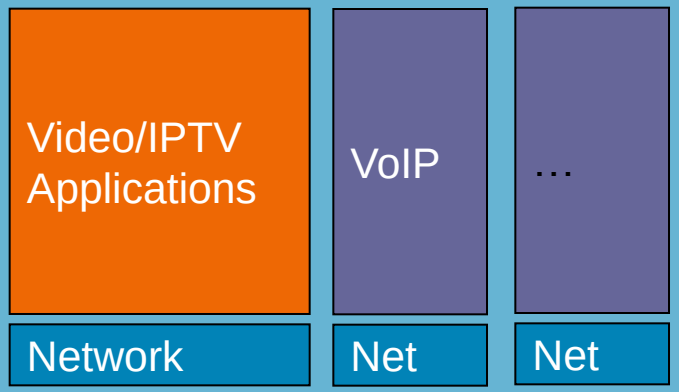
Video 2.0 means a transition from mainly broadcast to more personalized services

- Huge bandwidth increase: one to many -> one to one
- Traffic flows unpredictable; network must dynamically adapt
- Larger content libraries, more users, greater concurrency
- Personalization required



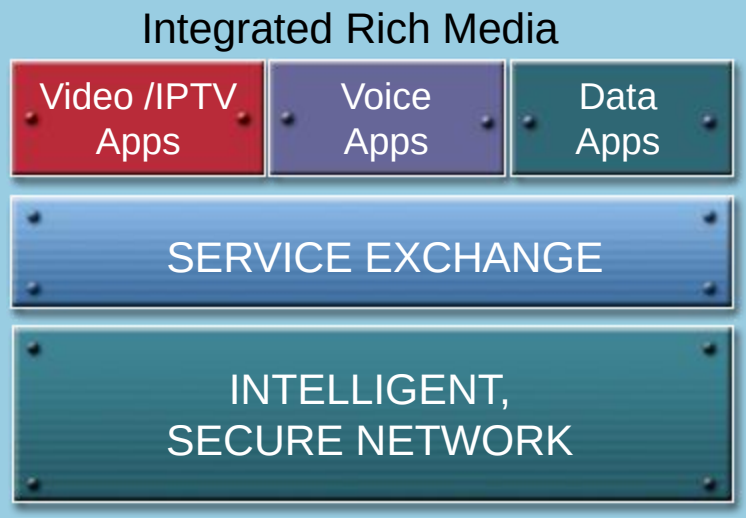
Moving to all IP Networks

Traditional Approach



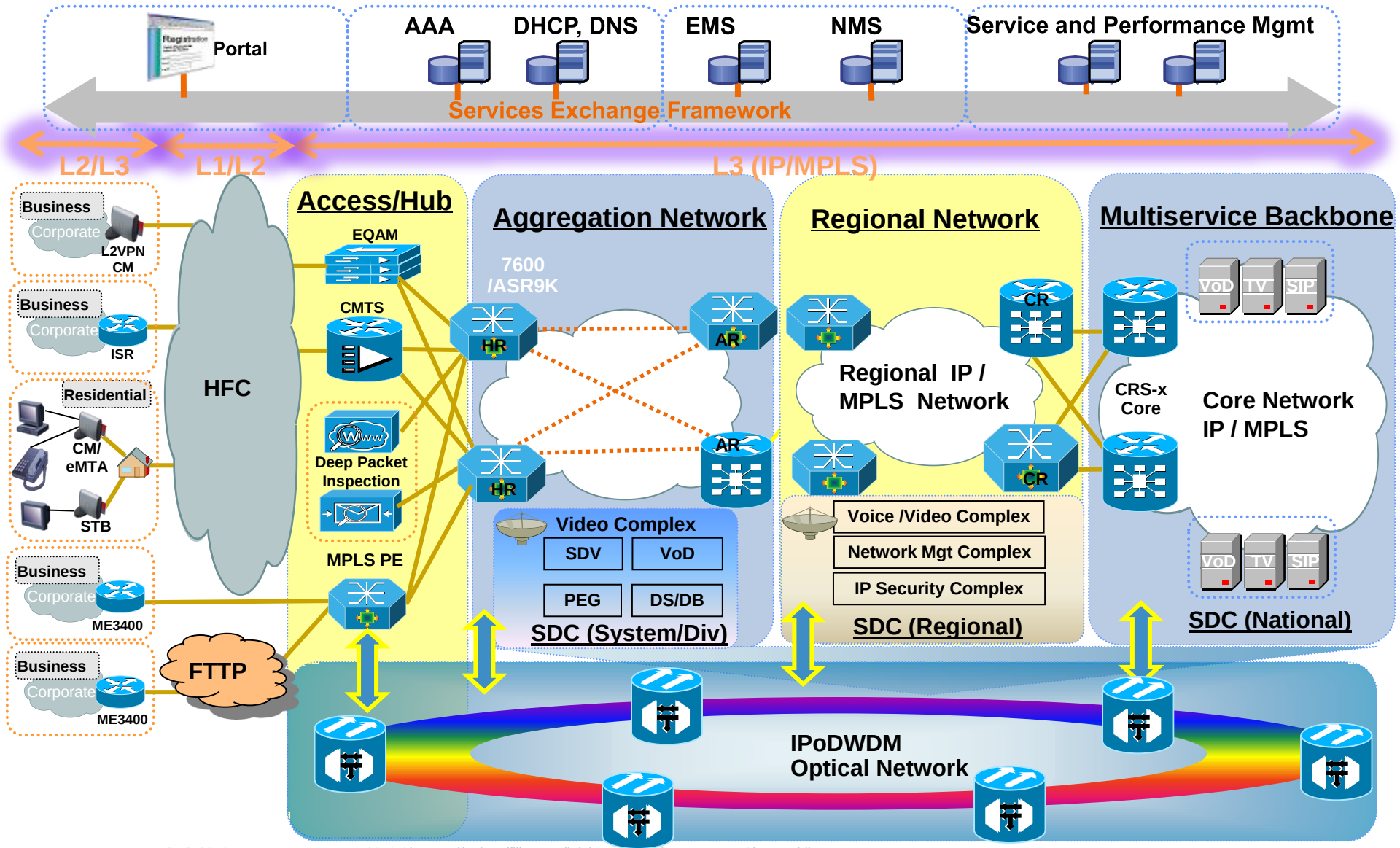
- Network/Service Silos
- Scale/Scope Challenges
- Closed Architecture
- Limited Network Linkages

IP NGN Approach



- Service Integration Enabling
- Application/Network Coupling
- Layered, Modular, Standards
- Intelligent Delivery Platform

Cable Multi-Service Networks



Why Ethernet Services?

The Basics

1. Mature and Widely Deployed

Long History of Deployment

De-facto LAN Technology

2. Resilient and Versatile

Can Terminate Fiber and Copper Effectively

Ethernet over DOCSIS adds a new paradigm

3. Cost Effective

Not as Expensive as Other WAN Technologies

IT Staff Already Trained in Ethernet

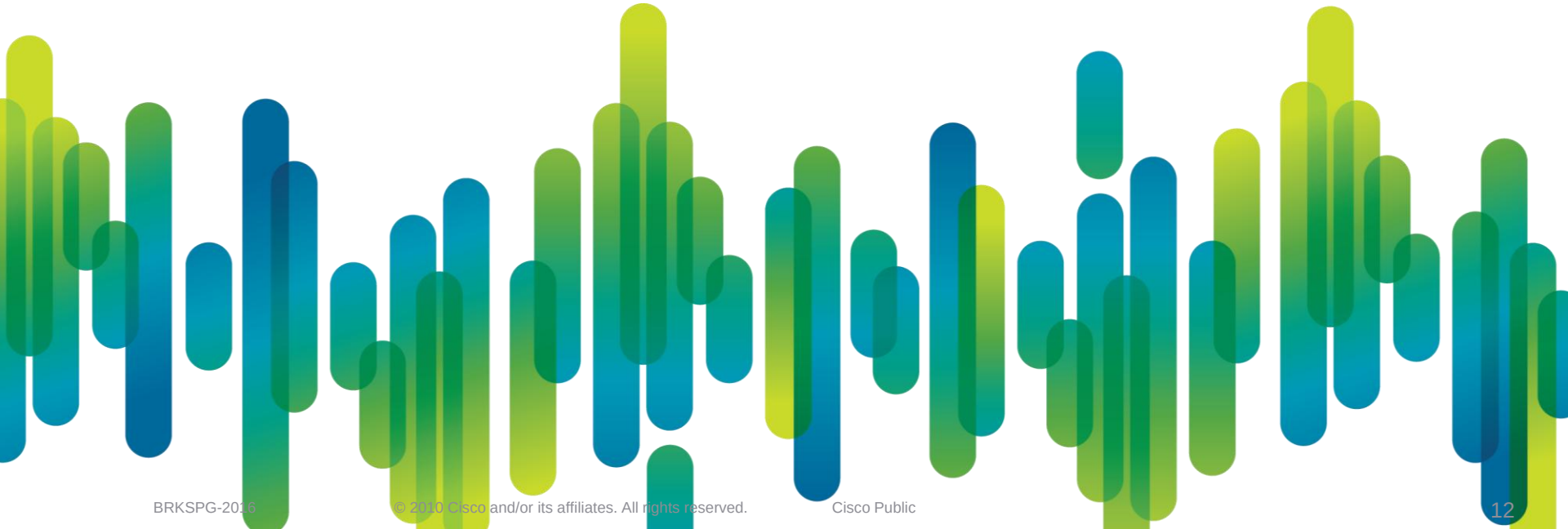
4. Constantly Evolving

Ethernet Has Came a Long Way Since Its Early Days

CMTS-Based Services Landscape

- Massive investment in HFC Infrastructure
- HFC and DOCSIS footprint and coverage
- Predominantly High Speed Data, Internet Access
- Voice over IP Revolution
  - New revenue stream for Cable Service providers
  - Competitive pricing for consumers
- Is this the end of line for CMTS- and HFC-based services?
- Next revenue generating service over HFC/CMTS?

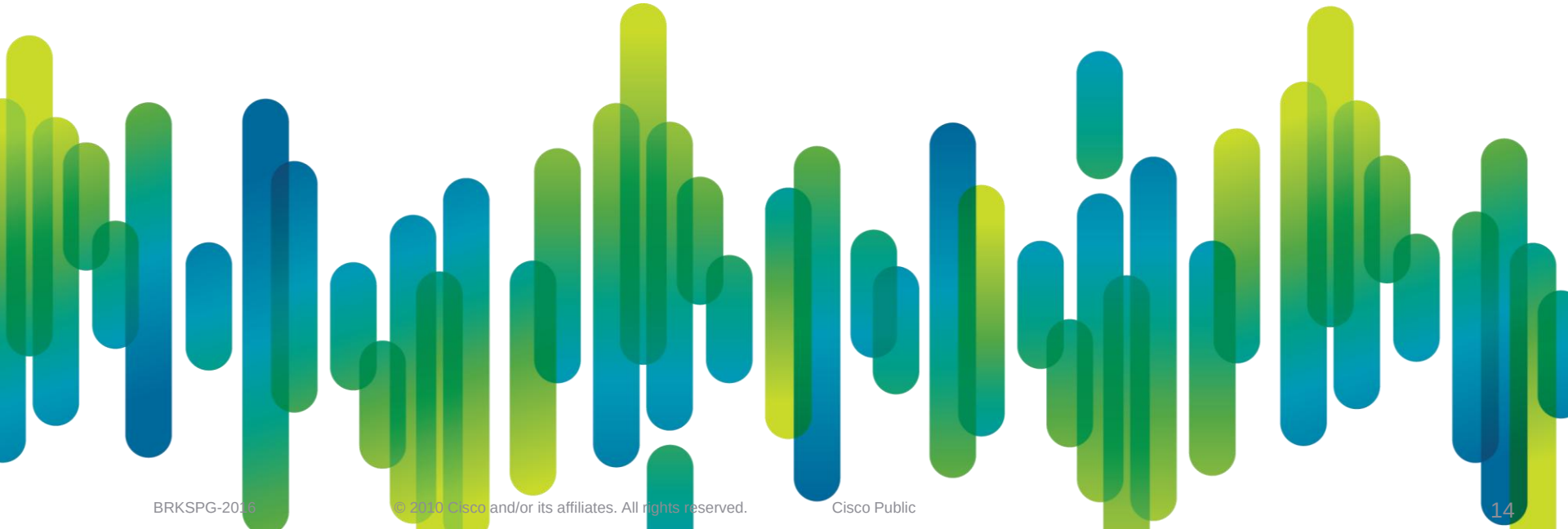
Video Over DOCSIS (VDOC)



Video Over DOCSIS

- What is it ?
  - Solution for the delivery of managed IPTV services over a DOCSIS network
  - Broadcast TV and VoD services
  - TV, PC, and other devices in the home
  - Provide user experience subscribers expect from their cable operator

VDOC Technology Overview



CMTS Features for VDOC

- DOCSIS 3.0 channel bonding
- Dynamic bandwidth sharing
- DOCSIS 3.0 multicast
- RF spanning
- Admission control and QoS
- VBR video and IP statmuxing

DOCSIS 3.0 Multicast Features

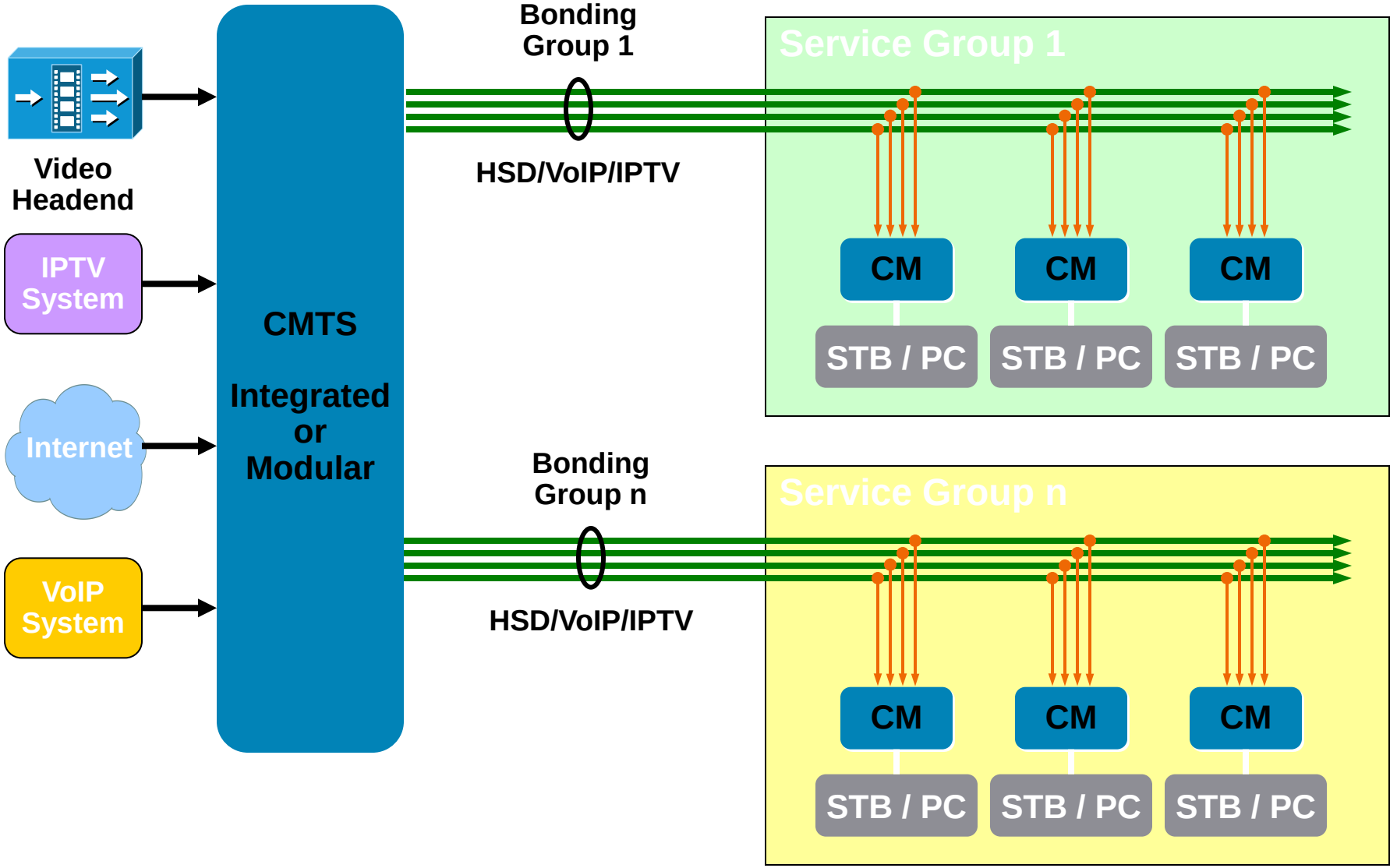
- SSM and IGMPv3
- IPv6 multicast support
- Multicast QoS
- Support for bonded multicast
- Non-IGMP based multicast
- Support for multicast authorization
- Multicast encryption
- Backward compatibility with legacy DOCSIS devices
- Explicit tracking of multicast listeners

VDOC Network Design Critical Factors

- IPTV service take rate
- Video codec and encode rate
- Popular vs long-tail linear services
- VoD service concurrency
- Service group size
- HSD/VoIP services
- Connected Home solution
- CM receive channels
- CMTS scalability and performance

DOCSIS 3.0 Channel Bonding

DS bonding group shared by all services

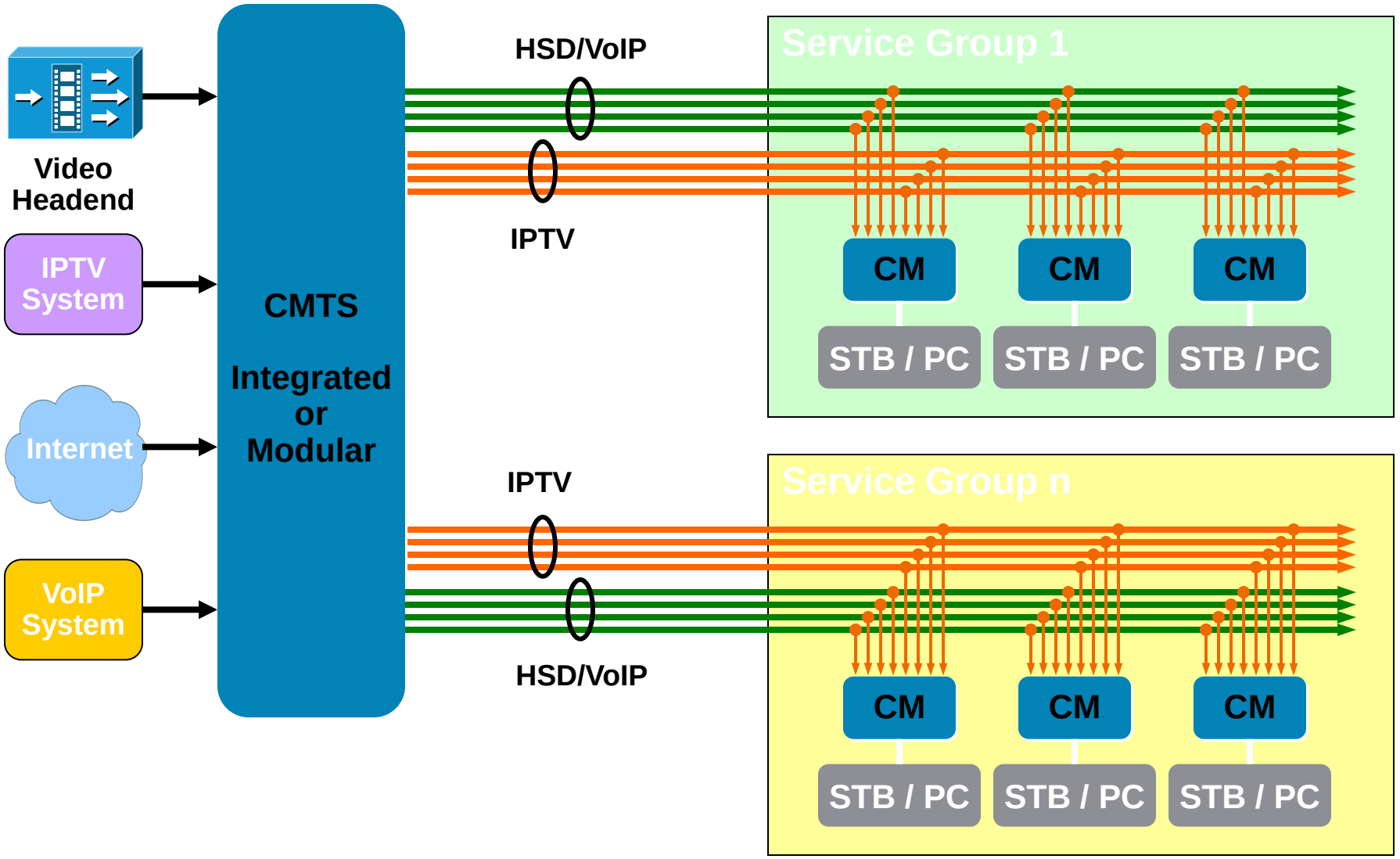


Bonding Group Selection

- A CM can receive traffic from multiple BGs
- Operator can steer flows to particular BGs by configuring Service Flow attributes for each BG
  - CMTS uses SF-attributes when selecting BG for a flow
- Operator could choose to set aside a BG for Cable IPTV and a separate BG for HSD/VoIP

DOCSIS 3.0 Channel Bonding

Separate DS bonding groups for HSD/Voice and IPTV



Dynamic Bandwidth Sharing

- Bonding Groups may overlap across a set of downstreams

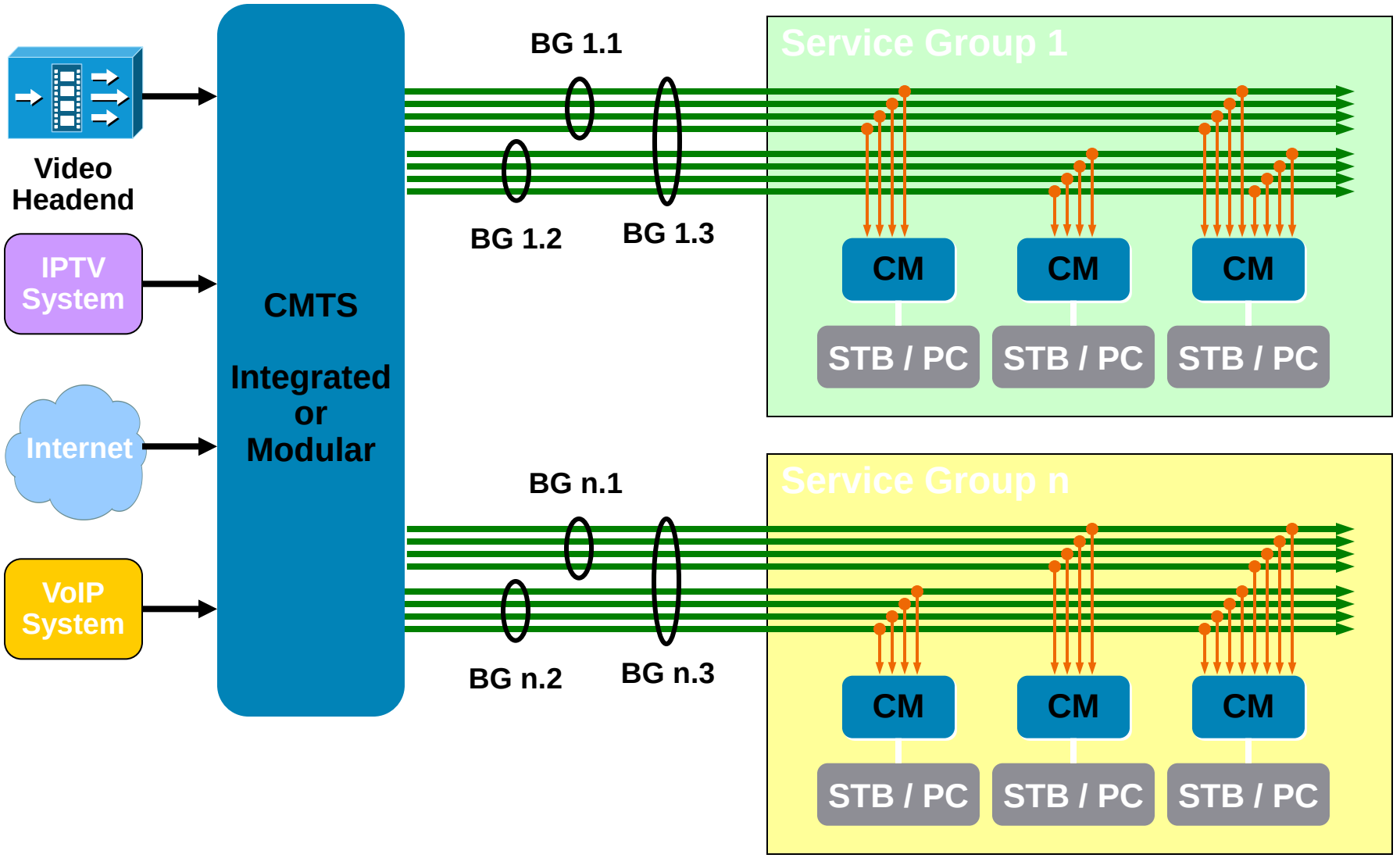
  For overlapping BGs, a portion of the BW of each downstream is allocated to each BG via configuration

- CMTS is capable of dynamically sharing bandwidth across overlapping bonding groups based on the services consumed by the CMs receiving the BGs

- Enables the deployment of a mix of CMs with different number of receive channels

  Example: Deployment of 8-channel CMs doesn't require separate set of RF channels from those used for 4-channel CMs.

Dynamic Bandwidth Sharing with Overlapping Bonding Groups

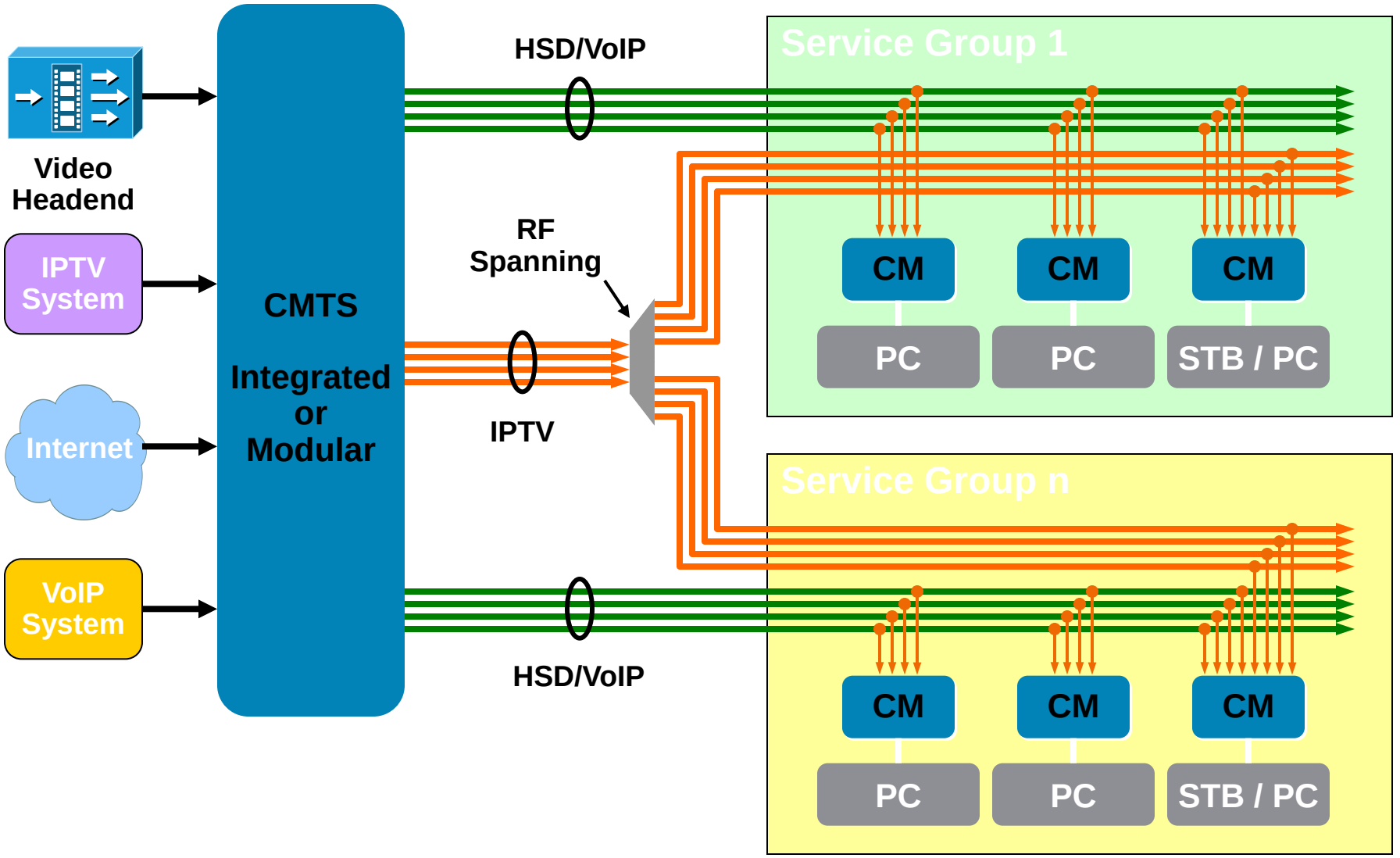


RF Spanning

- A set of downstreams can be split to multiple/all SGs served by the CMTS
  - Similar to broadcast QAMs, but limited to CMs served by a CMTS
  - Downstreams use same RF frequencies in each SG
- Useful for initial deployments where penetration rate may be low
  - IPTV clients may be lightly distributed across multiple SGs
  - Operator can deploy a handful of downstreams to start IPTV service
- When combined with static multicast, can replicate a broadcast style architecture

RF Spanning

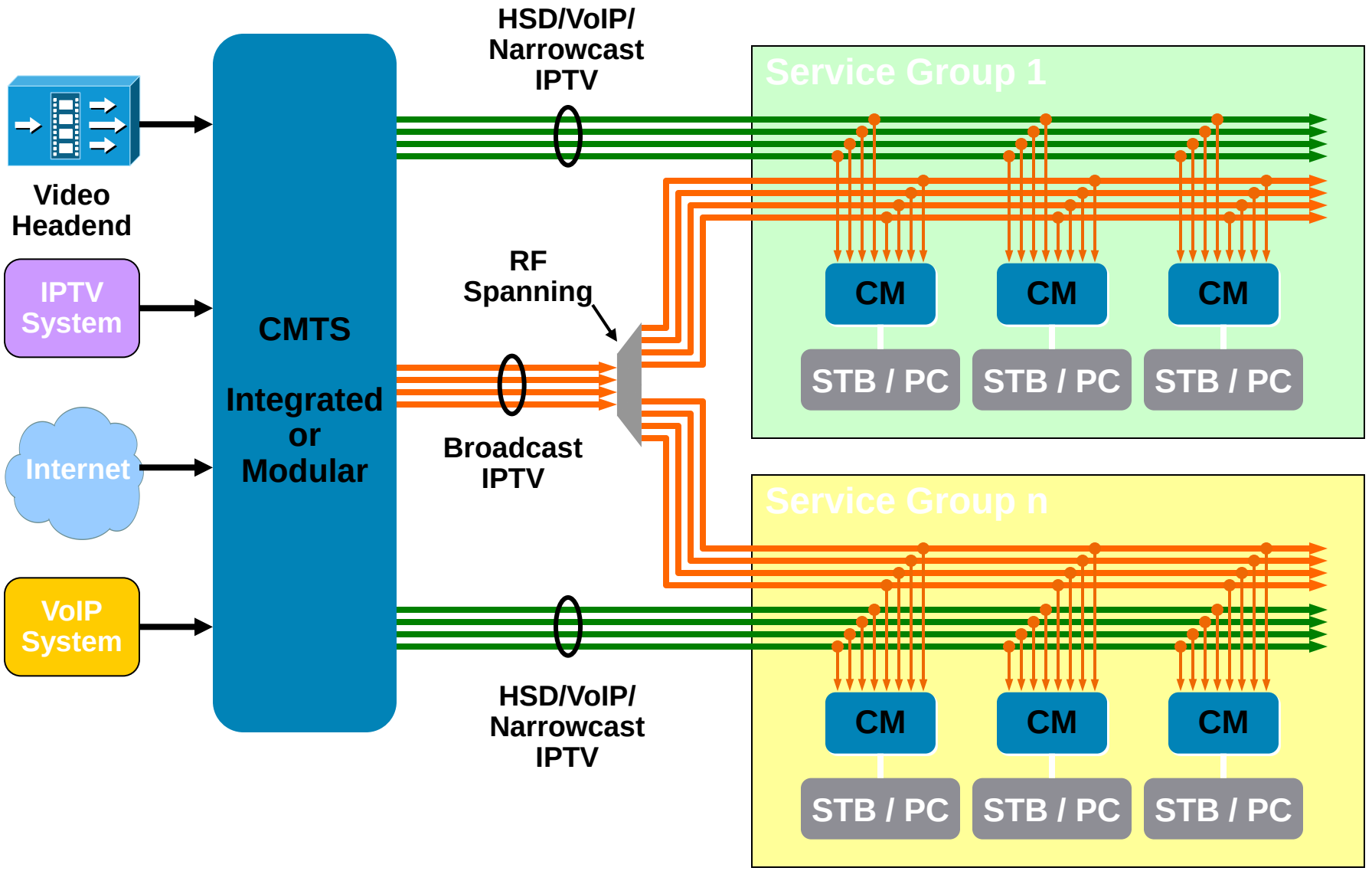
Initial low-penetration IPTV deployments



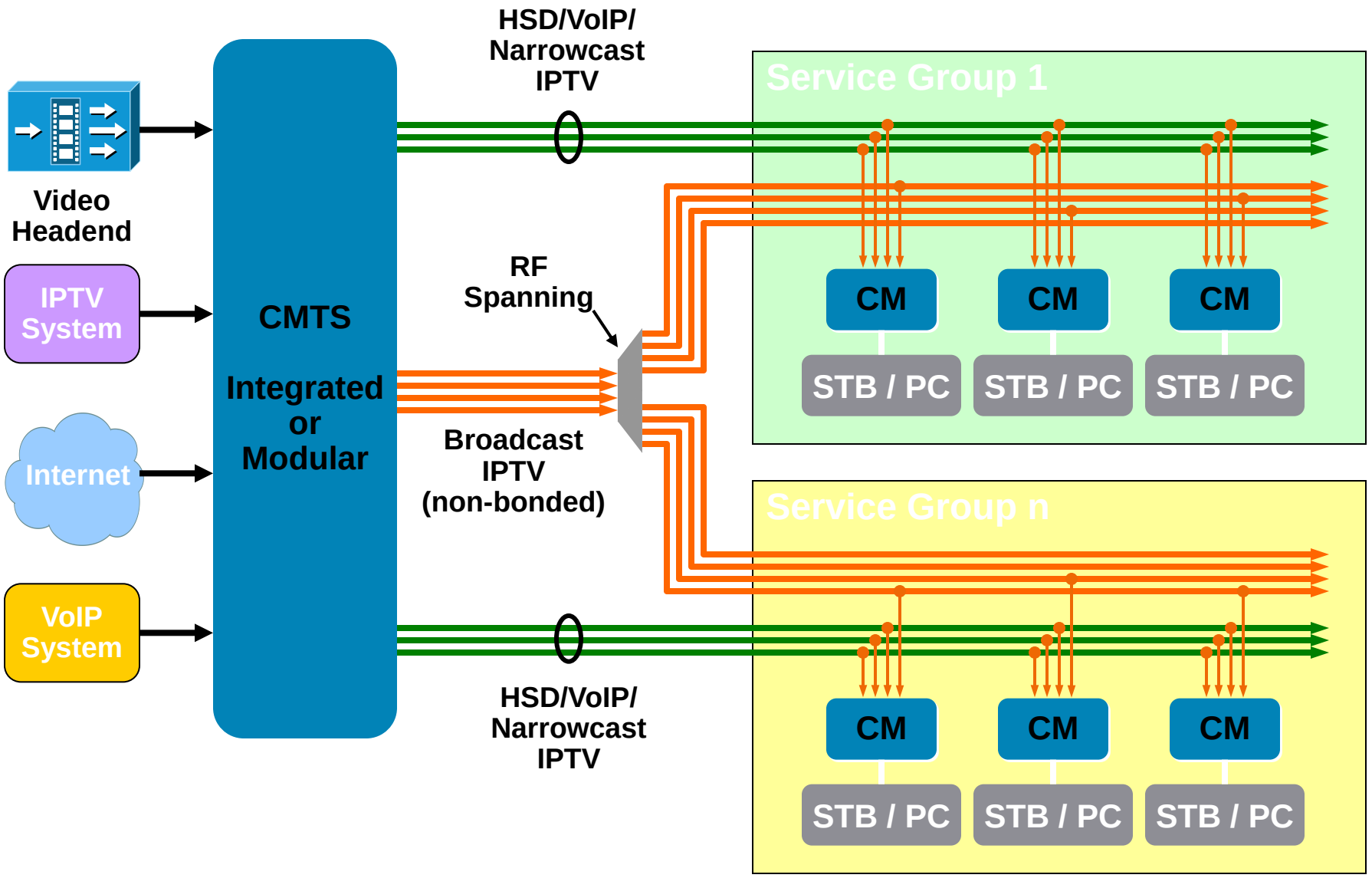
Bonded Static Multicast

- A BG is RF-spanned to all SGs and carries multicast IPTV streams
  - IPTV streams are delivered at all times as static multicast flows – regardless of viewership
  - Most popular content can be carried in a 4-channel BG
  - Long-tail content is carried over narrowcast BGs
- Subset of receive channels on CM are statically tuned to this RF-spanned BG to receive multicast IPTV streams
- Trade-offs
  - Less spectrum efficient than narrowcast BGs if all static multicast IPTV streams are not viewed by at least one CM in each SG at all times
  - Requires CMs with additional receive channels
  - The number of video streams that can be carried in such fashion is dependent on number of receive channels available on CM and spectrum availability

Bonded Static Multicast

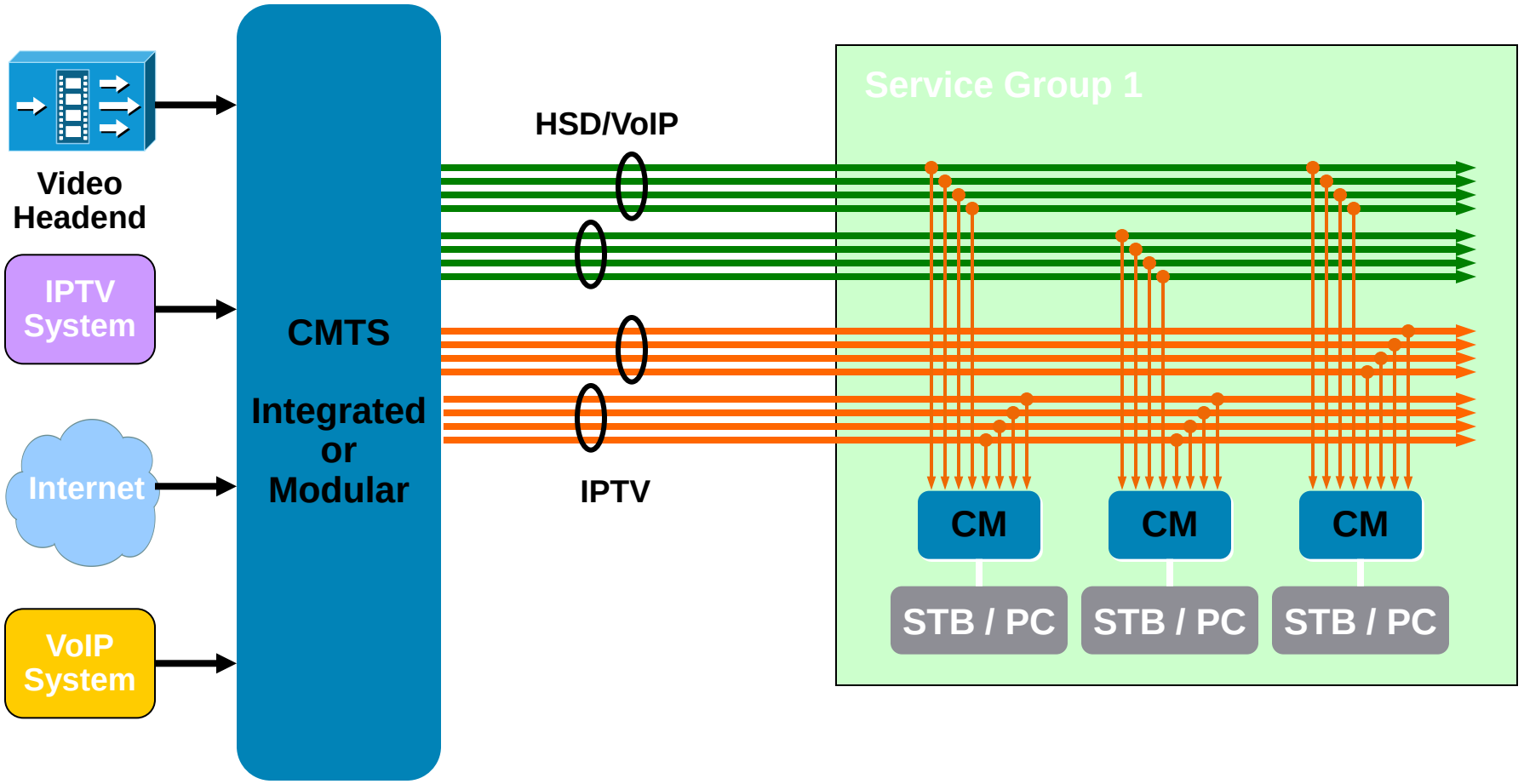


Static Multicast with CM Tuning



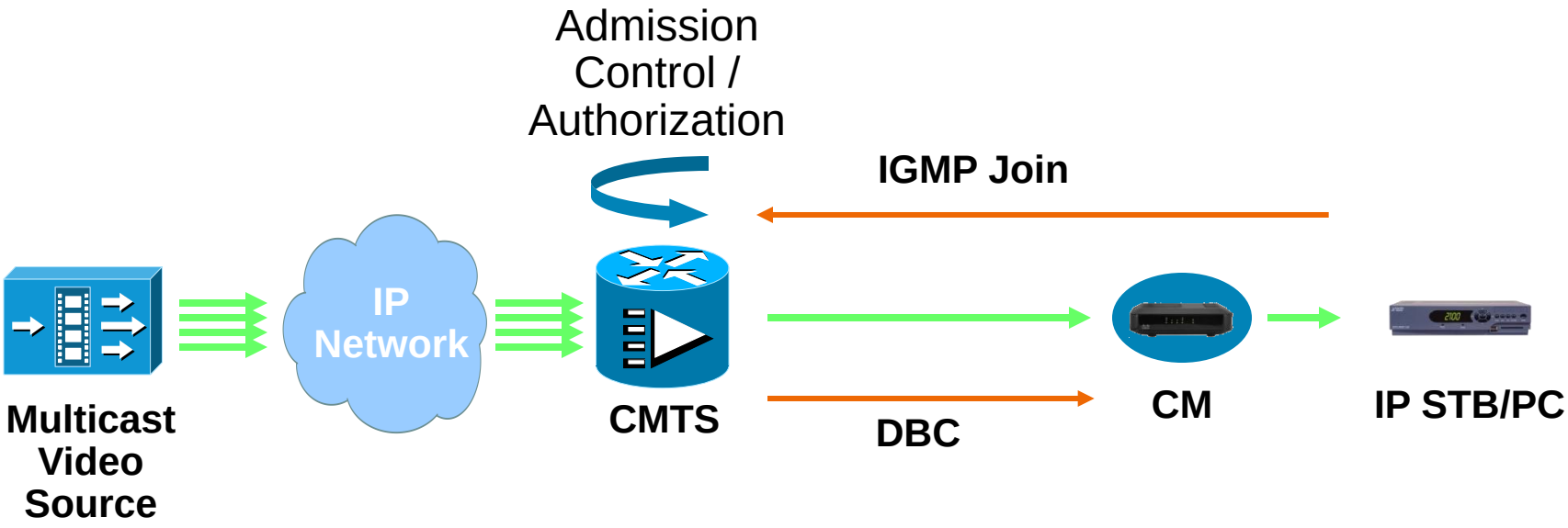
Static Multicast with DBC

Separate sets of downstreams for IPTV



Admission Control and QoS

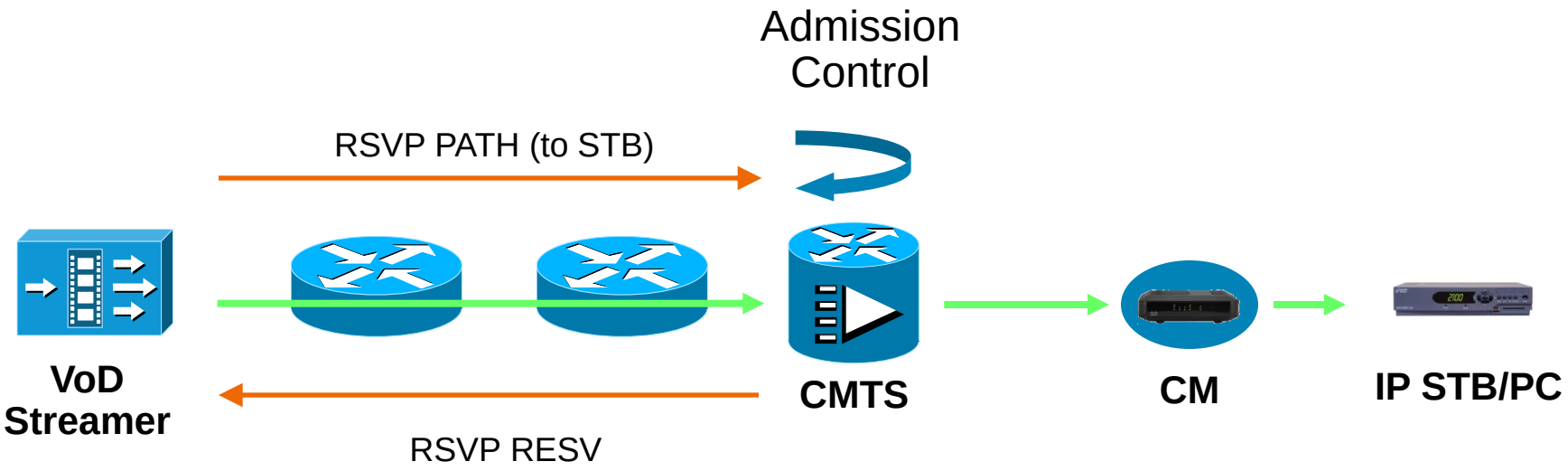
Multicast: IGMP



- CMTS forwards multicast video streams based on IGMP traffic from STB/PC
- CMTS pre-configured with video service class
  - CMTS is configured with service-class per multicast group address
- CMTS performs admission control
  - CMTS can perform multicast authorization

Admission Control and QoS

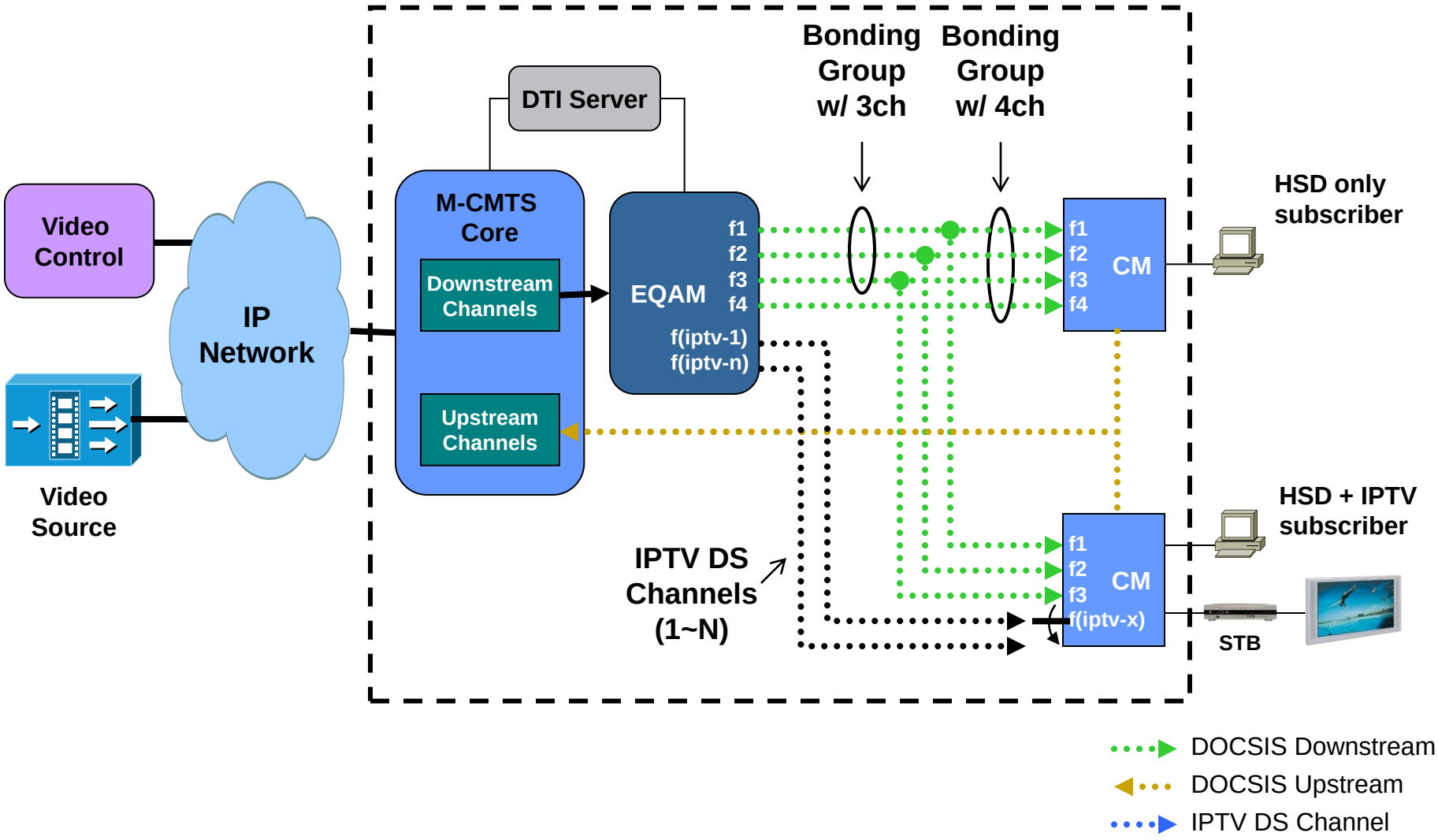
VoD: RSVP



Notes:

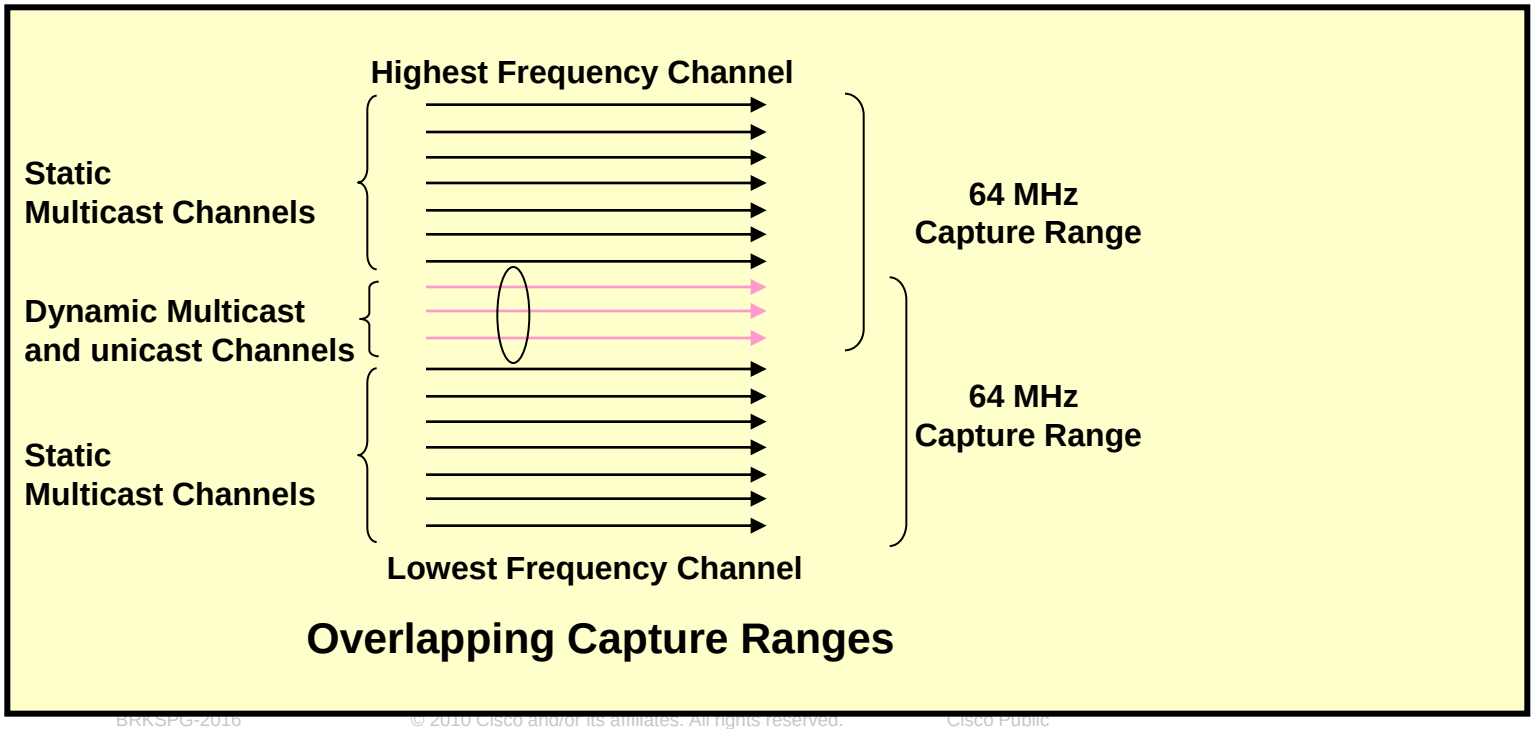
- Entitlement performed prior to initiating the above sequence
- CMTS pre-configured with video service class
    - Flexible forwarding to cable interface based on service flow attributes
- Upon receipt of RSVP, CMTS creates classifier and service flow and reserves BW

DOCSIS Transport Design

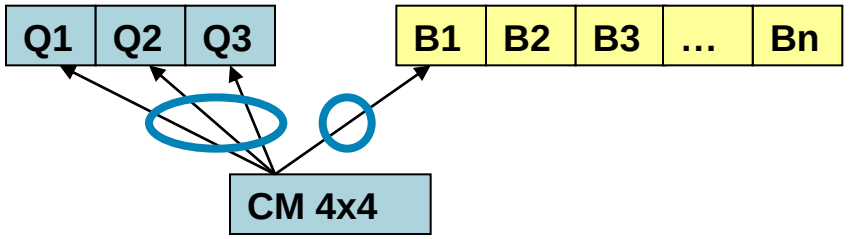


Spectrum Design with 4x4 CM

- Multicast and unicast service flows must fit modem tuner capture window.
- 14 unbonded multicast channels and 3 bonded unicast channels max
  - -- 245 SD channels (Annex B) / 315 SD channels (Annex A)
  - -- 2Mbps SD and 10% overhead
- Dynamic Bonding Change (DBC) is used to tune to different multicast channels
- One broadcast channel per CM



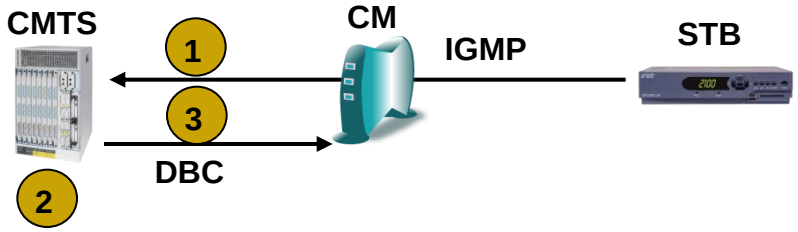
Dynamic Bonding Change (DBC)



Receiving Channel Configuration (RCC) for CM

- **Q1/Q2/Q3/B1**
- **Q1/Q2/Q3/B2**

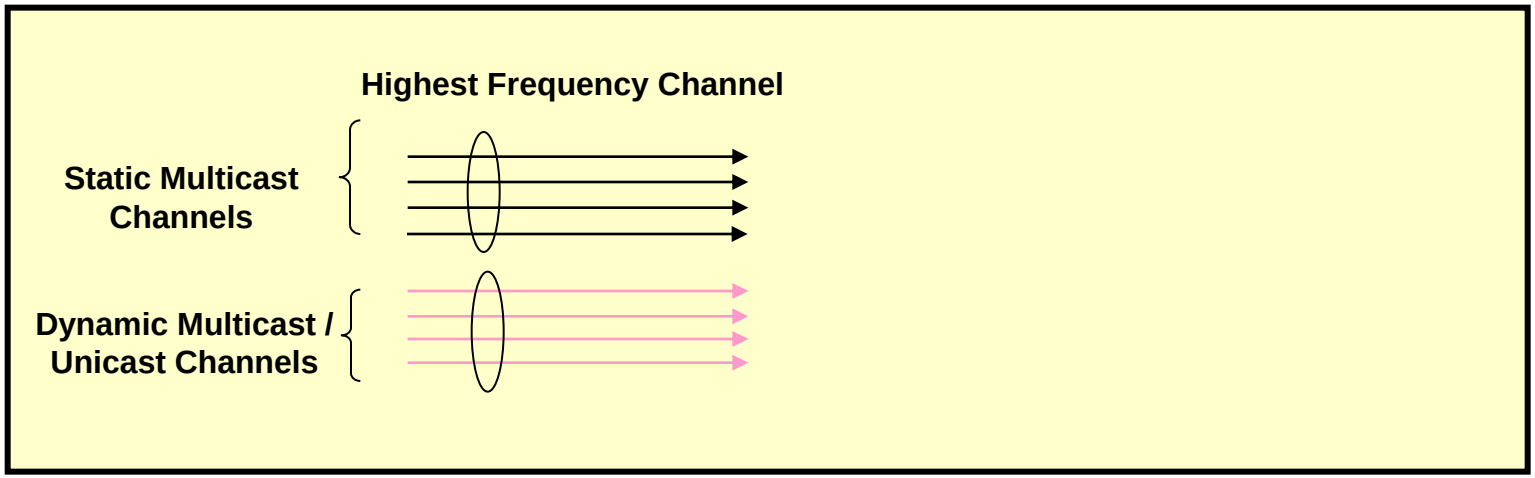
…



- **Broadcast channels are delivered by the CMTS to broadcast QAMs B1… Bn**
- **RCCs are configured on CMTS for a specific CM type**
- **The STB sends IGMP to the CMTS to tune to a broadcast channel**
- **The CMTS lookup the multicast address and finds out the broadcast QAM that carries the channel**
- **The CMTS sends the DBC message to CM and gives the RCC to STB for tuning**
- **The CM tunes to the RCC and the media flows to the STB**

Spectrum Design with 8x4 CM w. Dyanmic Multicast

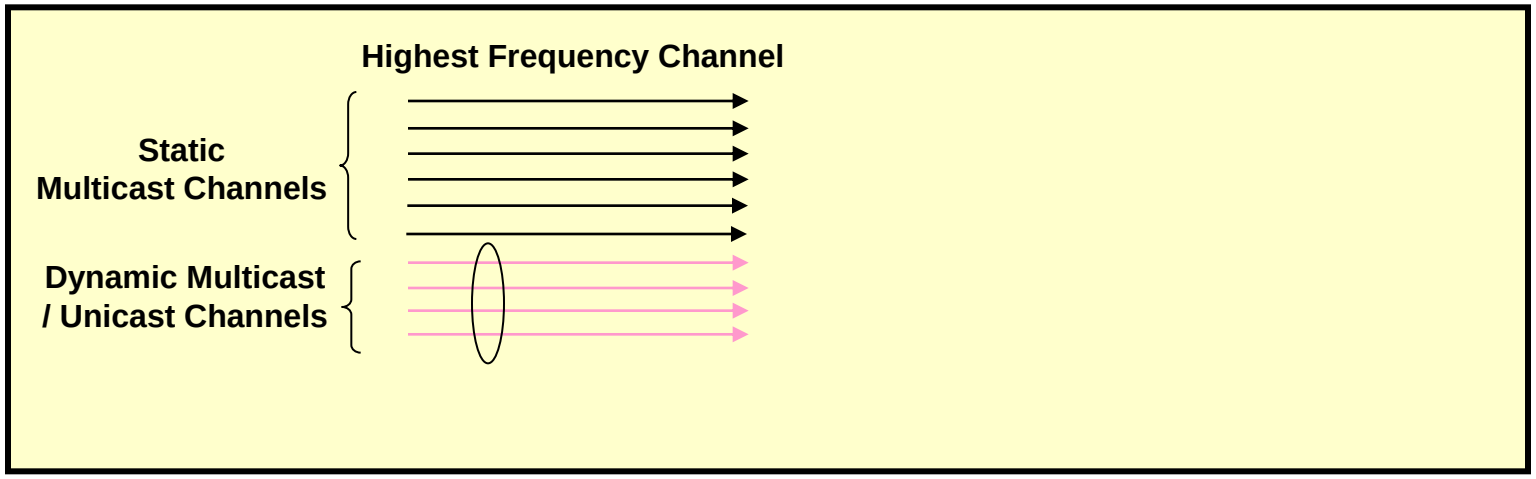
- 4 channel bonded multicast and 4 channel bonded unicast
  - -- static multicast and RF spanning
  - -- two independent tuner blocks, 32MHz each



- One 4-channel bonding group for static multicast
  - -- 70 or 98 (w. 40% statmux gain) SD channels (Annex B)
  - -- 90 or 126 SD channels (Annex A)
- One 4-channel bonding group for dynamic multicast and unicast

Spectrum Design with 8x4 CM (static multicast only)

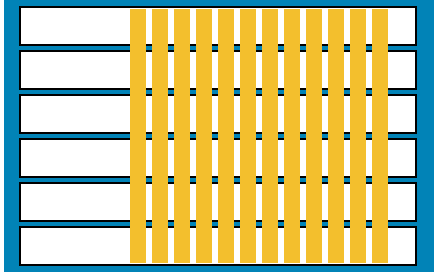
- N unbonded static multicast and 4 channel bonded unicast
  - -- static multicast and RF spanning
  - -- two independent tuner blocks
- Dynamic Bonding Change (DBC) is used to tune to different multicast channels
- Limited simultaneous broadcast channels per CM



Delivering VBR Video over DOCSIS Networks

Fat Pipe

DOCSIS 3.0 Channel Bonding



Law of large numbers

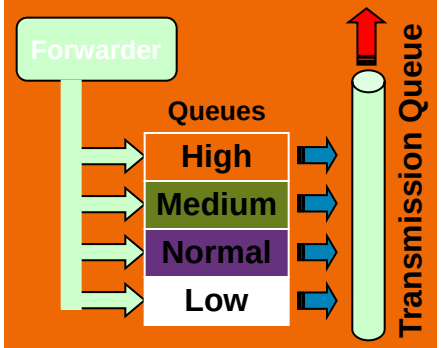
Asynchronous

100ms CPE Jitter Tolerance

60ms CMTS jitter

CMTS QoS

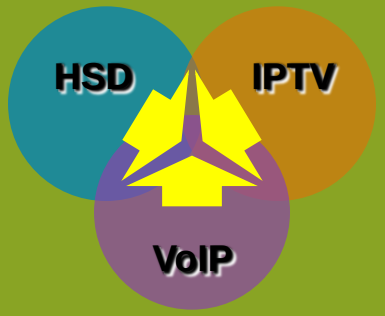
Shaping Priority



No transrating

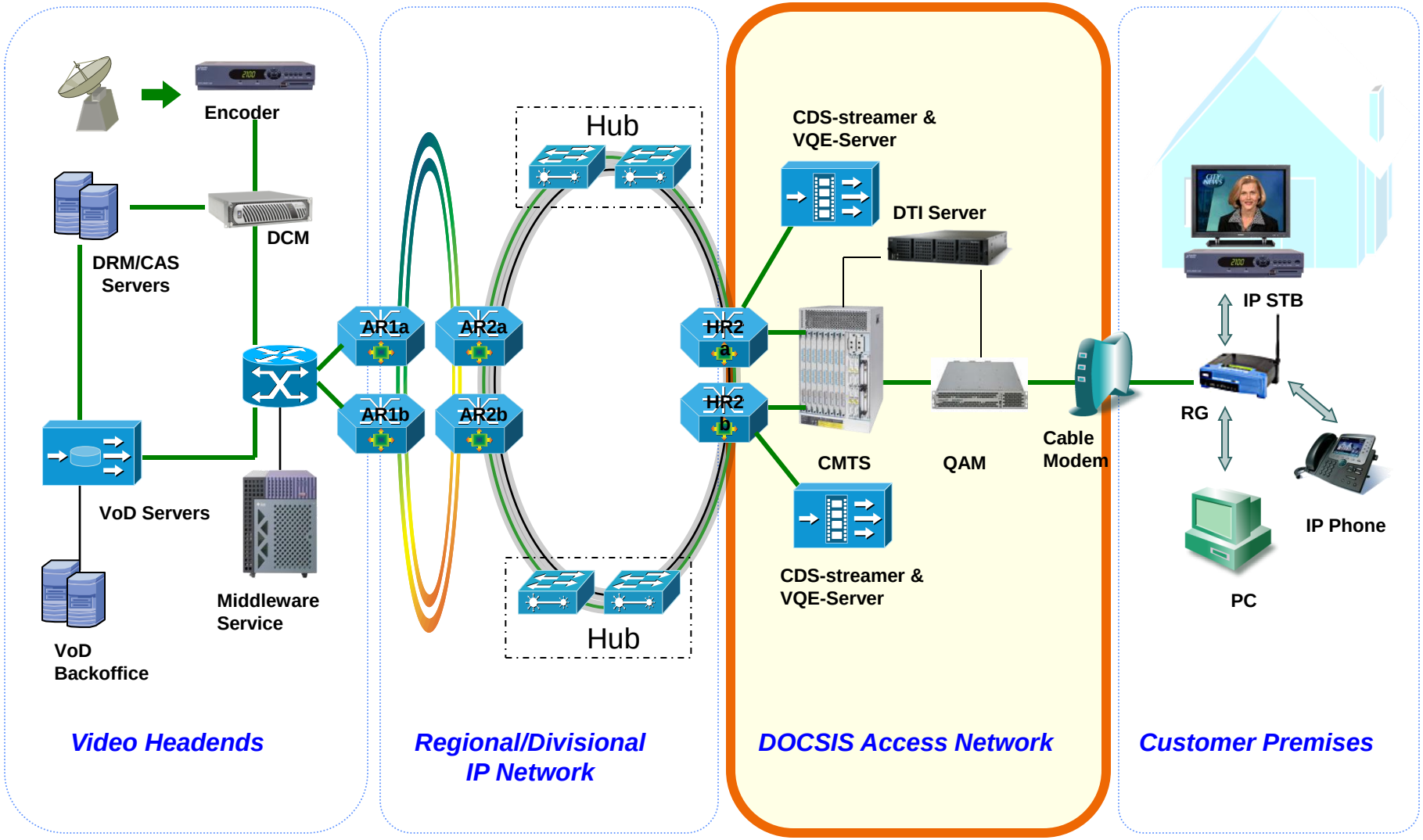
Convergence

Service / Device

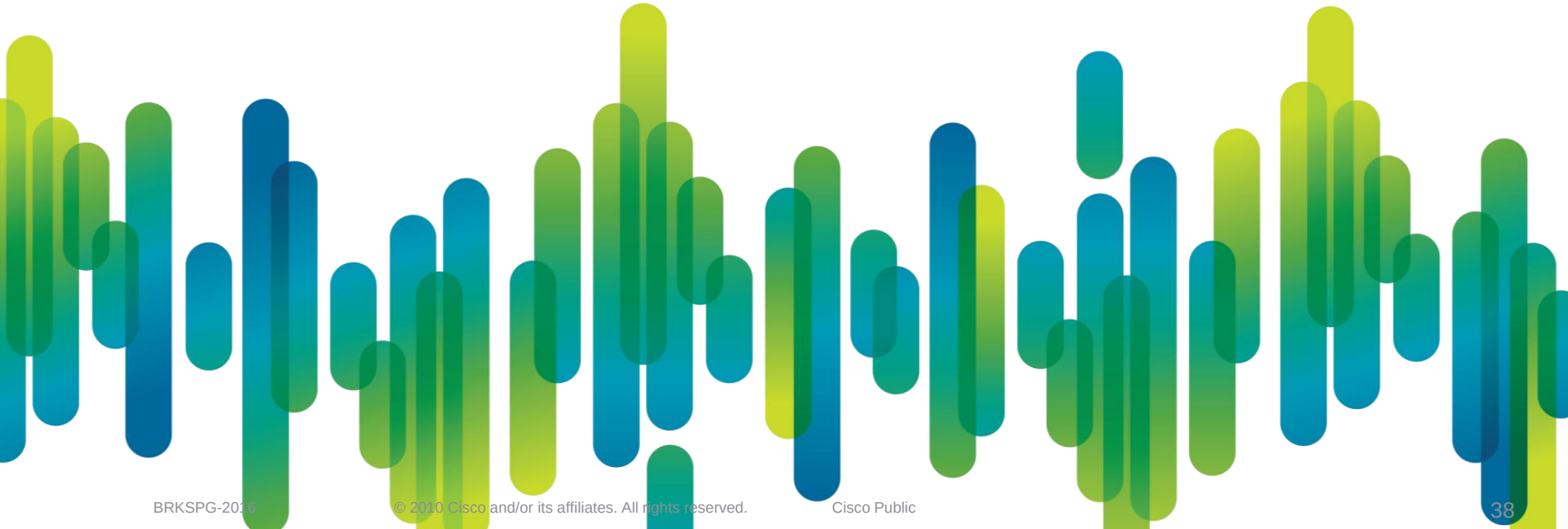


100% BW utilization

Cable IPTV System Reference Architecture



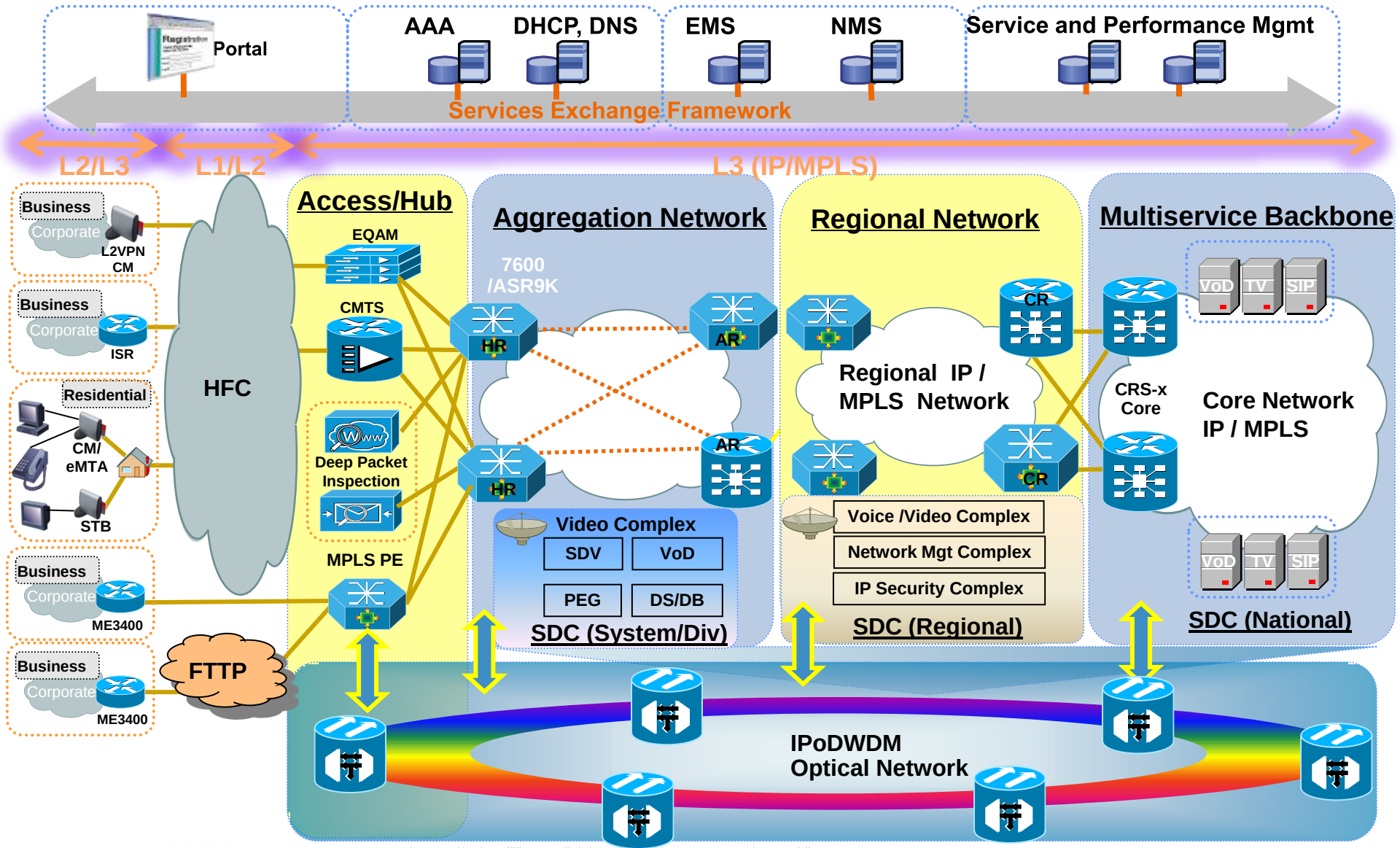
Business Services Over DOCSIS (BSoD)



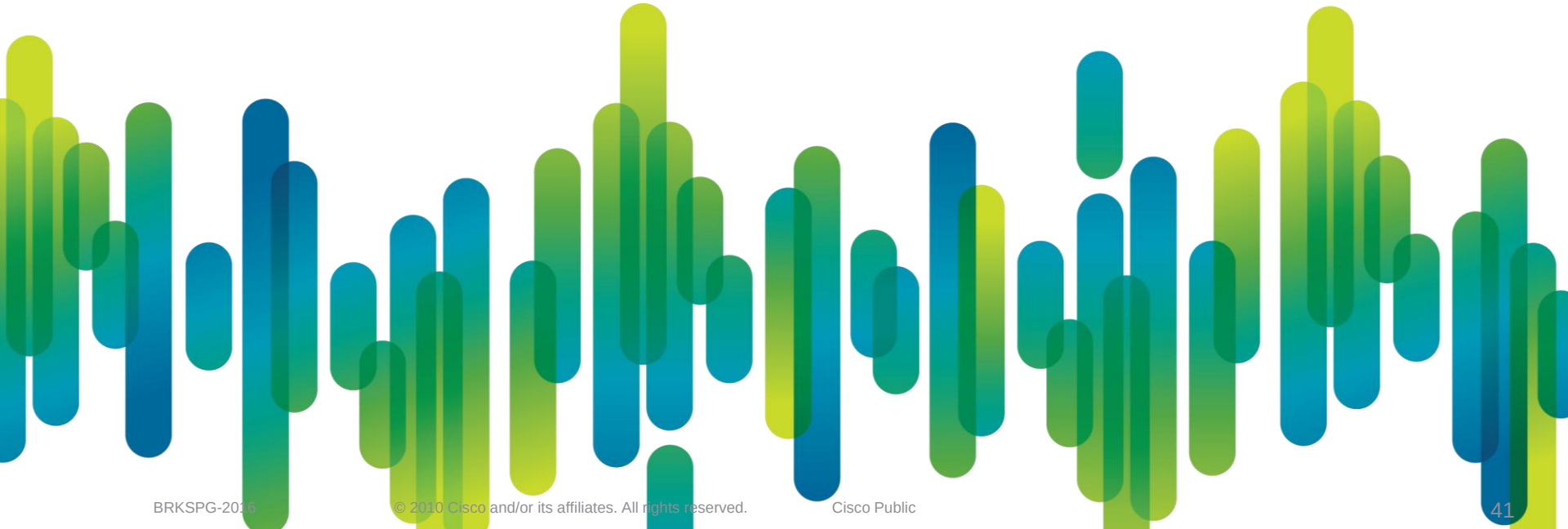
The Next Wave of Evolution—BSoD

- Long history of VPN services over Fiber
- HFC plant under-utilized in Business hours
  - Dual purpose HFC networks
- Business Services over DOCSIS – BSoD
- No additional cost in most cases
- Same HFC network, additional services
- Zero touch CMTS provisioning
- Standardized service offerings

Cable Multi-Service Networks



Carrier Ethernet Business Services



What VPN Services?

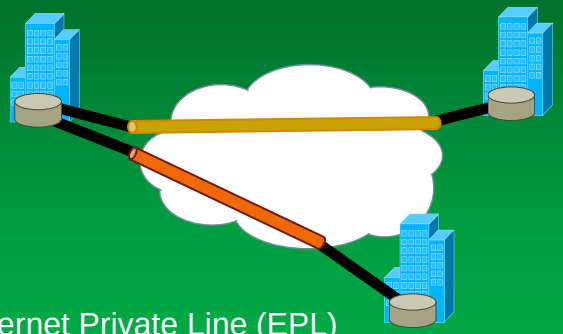
- Mass scale Carrier Ethernet Services adoption
- MPLS-based L3 VPN and L2 VPN services
- Advantages of L2 VPN services over L3 VPN:
  - Protocol Agnostic
  - No protocol sharing between SP and Customer
  - More customer control over their network
  - Simpler to deploy
- Standardized Carrier Ethernet L2VPN Services

Carrier Ethernet L2VPN Services

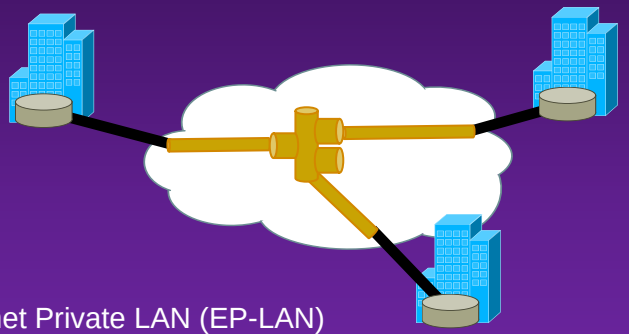
E-LINE Services

E-LAN Services

Port-based

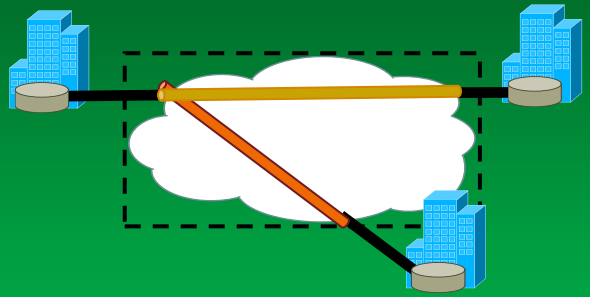


Ethernet Private Line (EPL)
Replaces a TDM private line
Dedicated UNIs for point-to-point connections
Single Ethernet Virtual Connection (EVC) per UNI
The most popular Ethernet service due to its simplicity

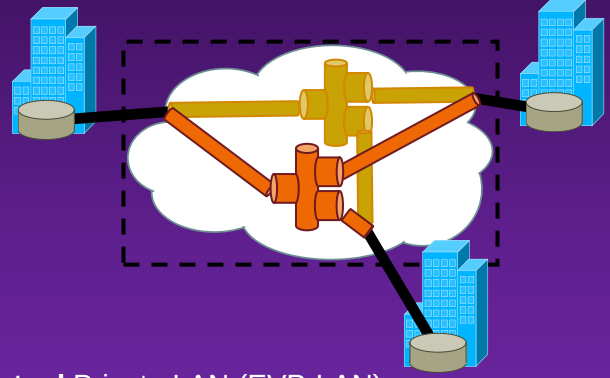


Ethernet Private LAN (EP-LAN)
Supports dedicated UNIs
Supports transparent LAN services
Supports multipoint Layer 2 VPNs

VLAN-based



Ethernet **Virtual** Private Line (EVPL)
Replaces Frame Relay or ATM services
Supports service multiplexed UNIs (i.e., multiple EVCs per UNI)
Allows single physical connection (UNI) to customer premise equipment for multiple virtual connections



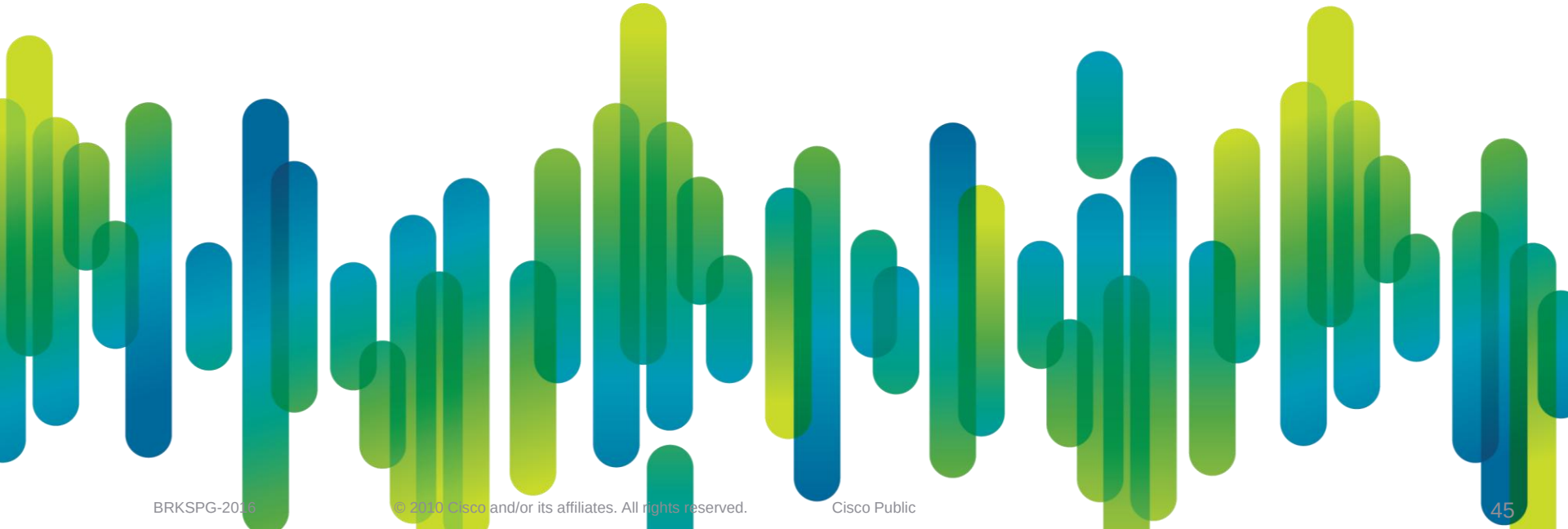
Ethernet **Virtual** Private LAN (EVP-LAN)
Supports service-multiplexed UNIs
Supports multipoint Layer 2 VPNs

Business Services Over DOCSIS

- Builds on standard defined by MEF
- Competitive advantage for Cable SPs due to HFC reach
- Cable Labs specs available* for L2VPNs
- DOCSIS 3.0 offer new opportunities for BSOD
  - Higher speed with Channel bonding
  - Effective Competition against T1, leased line and in some cases, fiber

Link here for Cable Labs L2 VPN link

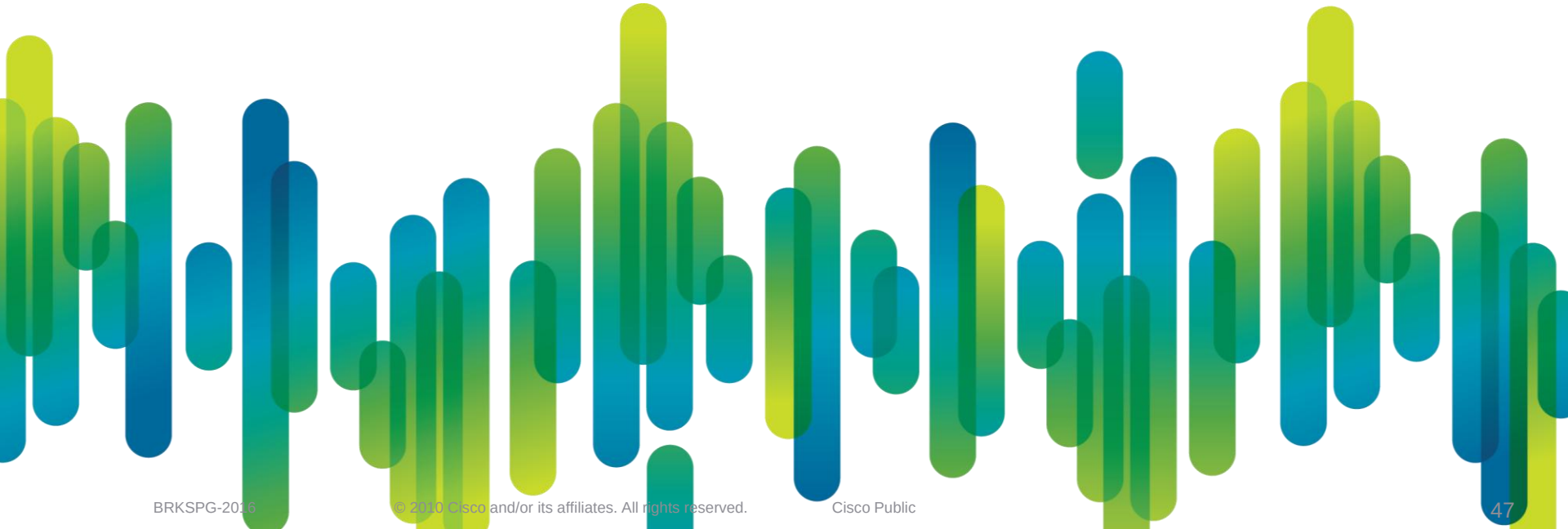
Business Services Over DOCSIS Deployment Models



BSoD L2VPN Deployment Models

- Two distinct deployment models
  - CPE-Based L2VPN
    - Minor adjustments over established HSIA services
    - Layer 2 Tunnel established between CM Routers
  - Network-Based L2VPN
    - True L2 service through CMTS
    - Layer2 tunnel established within Cable SP Network
    - Multiple variations available
      - Transparent LAN Services over DOSCIS
      - Dot1Q-based BSoD
      - MPLS-based BSoD

CPE-Based L2VPN Services

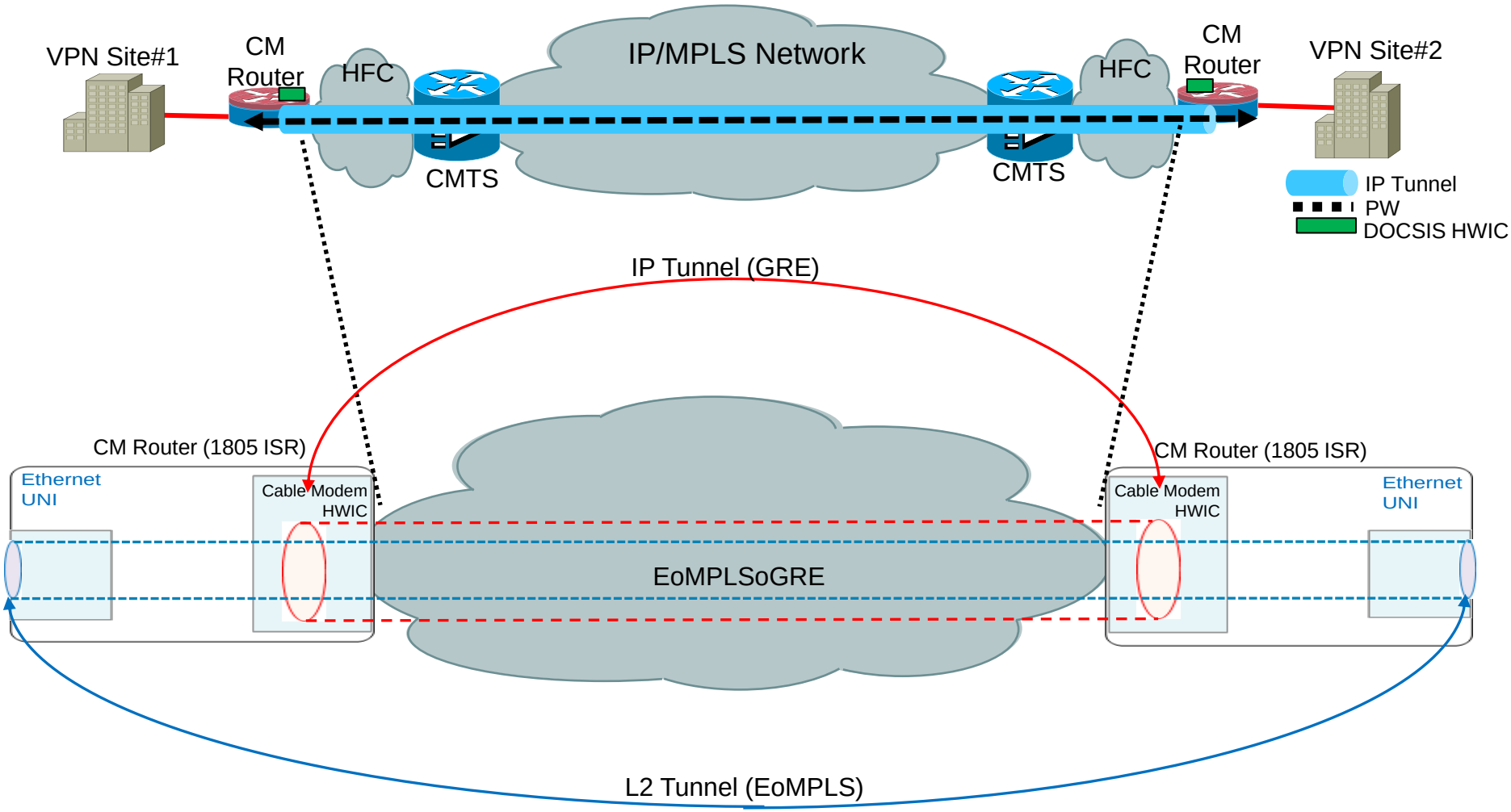


CPE-Based L2VPNs

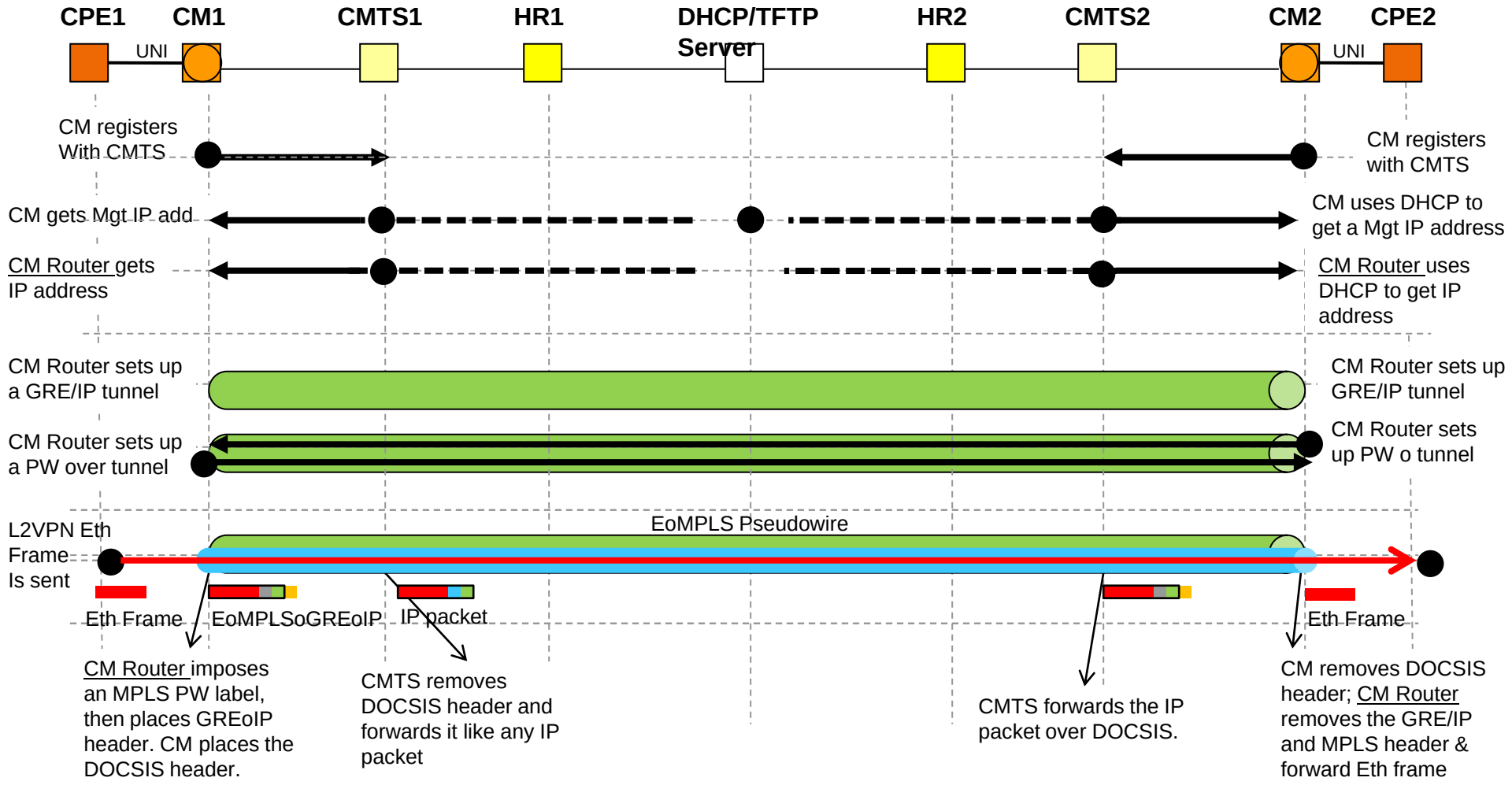
- “Over The Top” approach
- IP Tunnel created by CM router over HSIA Traffic
  - GRE or L2TPv3 Tunnel
- CM Router establishes EoMPLS over IP Tunnel
  - EoMPLSoGRE
  - EoMPLSoL2TPv3
- Cable SP see regular L3 traffic from customer
- Fragmentation may be a concern
- Simple, easy deployment, no changes to SP infrastructure

CPE-Based L2VPNs

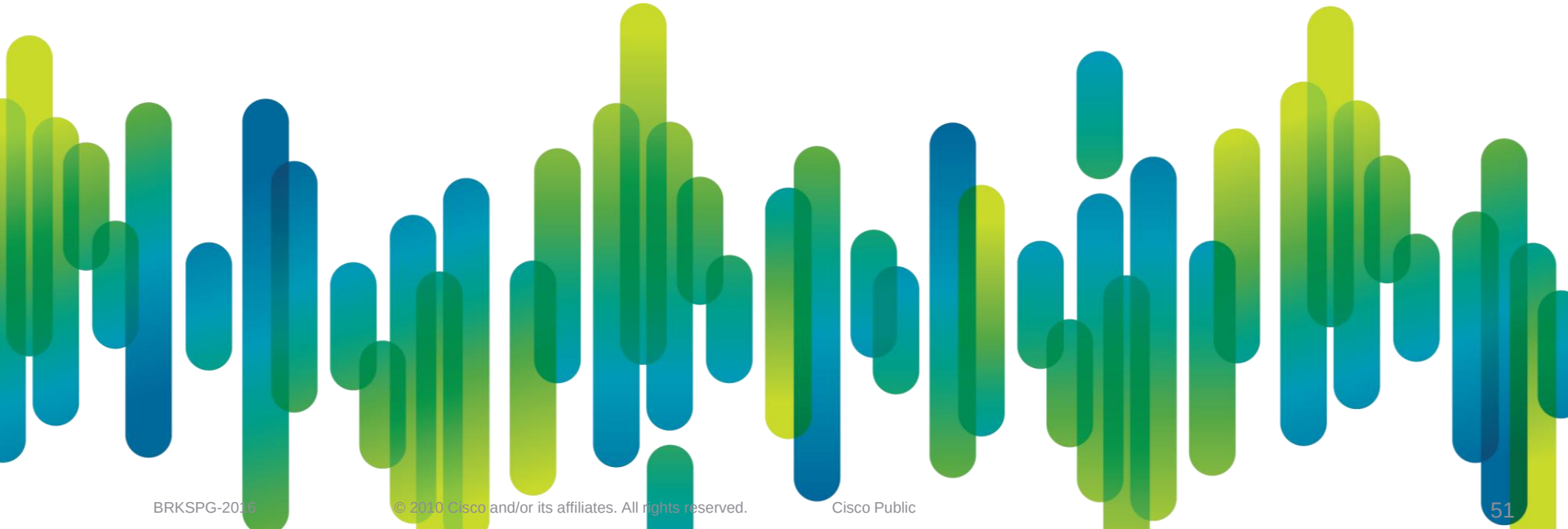
How It Works?



CPE-Based L2VPN
Control Plane and Data Plane Flow



Network-Based L2VPN Services
TLS over DOCSIS



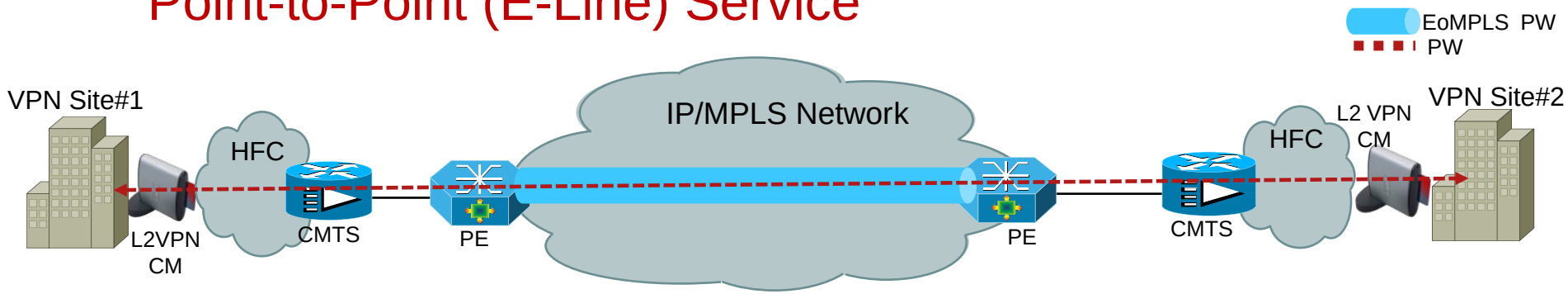
Transparent LAN Services(TLS) Over DOCSIS

How It Works?

- Cisco Proprietary Layer 2 Tunneling mechanism
- Precursor to Cable Labs specs on BSoD
- All CM traffic encapsulated in a VLAN on CMTS
- Upstream router implement EoMPLS or VPLS
- Each L2VPN site (CM) statically configured on CMTS
- No Multiplexed (EVPL, EVPLAN) Services

TLS Over DOCSIS

Point-to-Point (E-Line) Service



CMTS

```
Cable l2-vpn-service xconnect nsi dot1q

cable dot1q-vc-map 0022.3a61.7bcf Gig3/1/0 25 TLSoDOCSIS
```

- CM MAC Address
- Forwarding Interface (NSI)
- VLAN
- Customer Name (Optional)

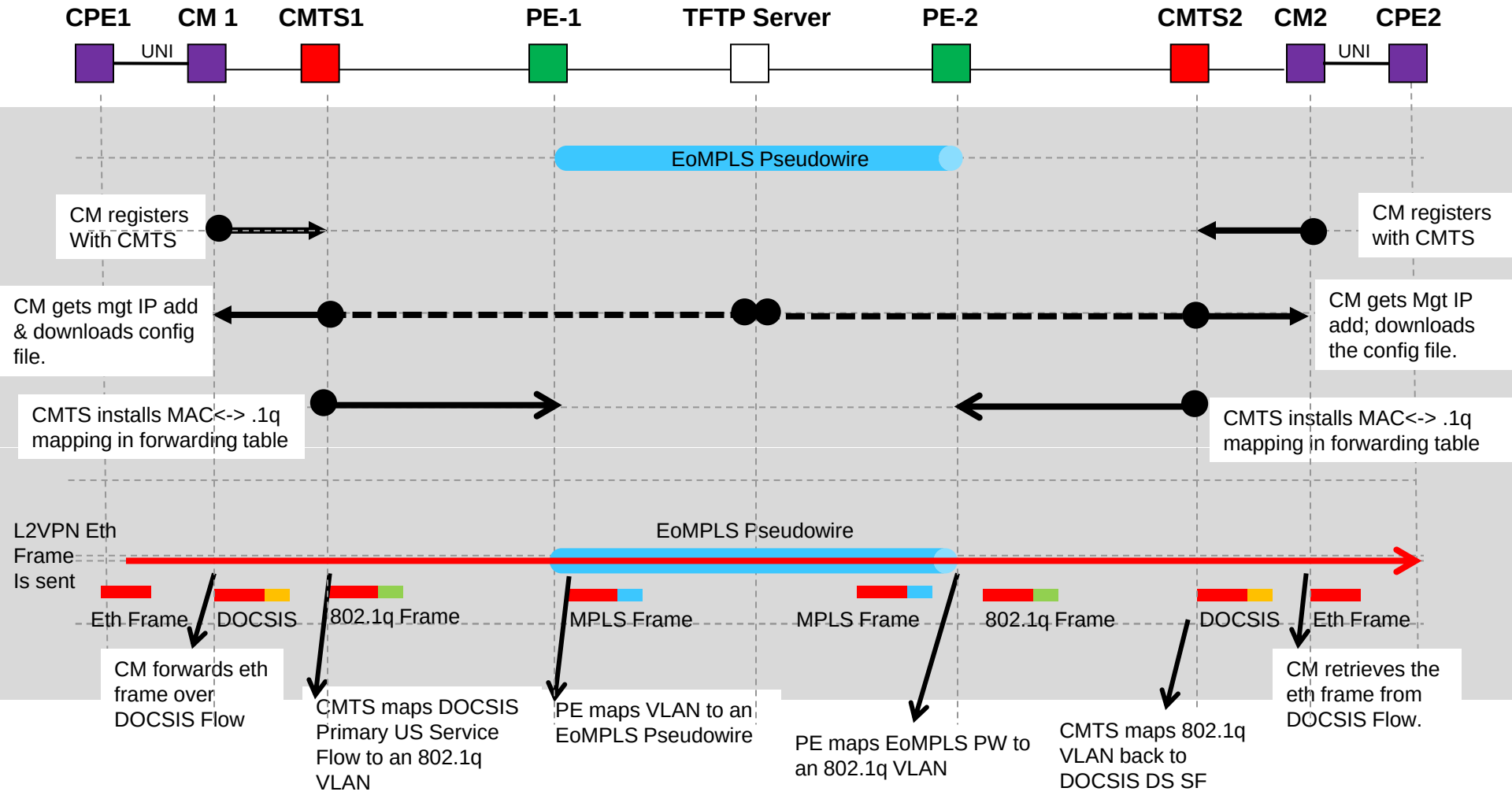
MPLS PE

```
interface GigabitEthernet1/23.25
 encapsulation dot1Q 25
 xconnect 99.1.1.21 50 encapsulation mpls
```

- VLAN encapsulated from CMTS
- EoMPLS VC ID

TLS Over DOCSIS

Control Plane and Data Plane Flow



TLS Over DOCSIS Service Verification

- Verify CM online

```
H1-10K#scm
Load for five secs: 0%/0%; one minute: 1%; five minutes: 0%
Time source is NTP, 17:18:54.122 EDT Mon Mar 22 2010

                                                                        D
MAC Address    IP Address     I/F          MAC             Prim RxPwr  Timing Num I
                                           State           Sid  (dBmv) Offset CPE P
0022.3a61.7bcf 17.101.75.100  C5/1/0/U0    online(pt)      187  17.00  1186   0   N
```

- Verify CM is online as TLS o DOCSIS

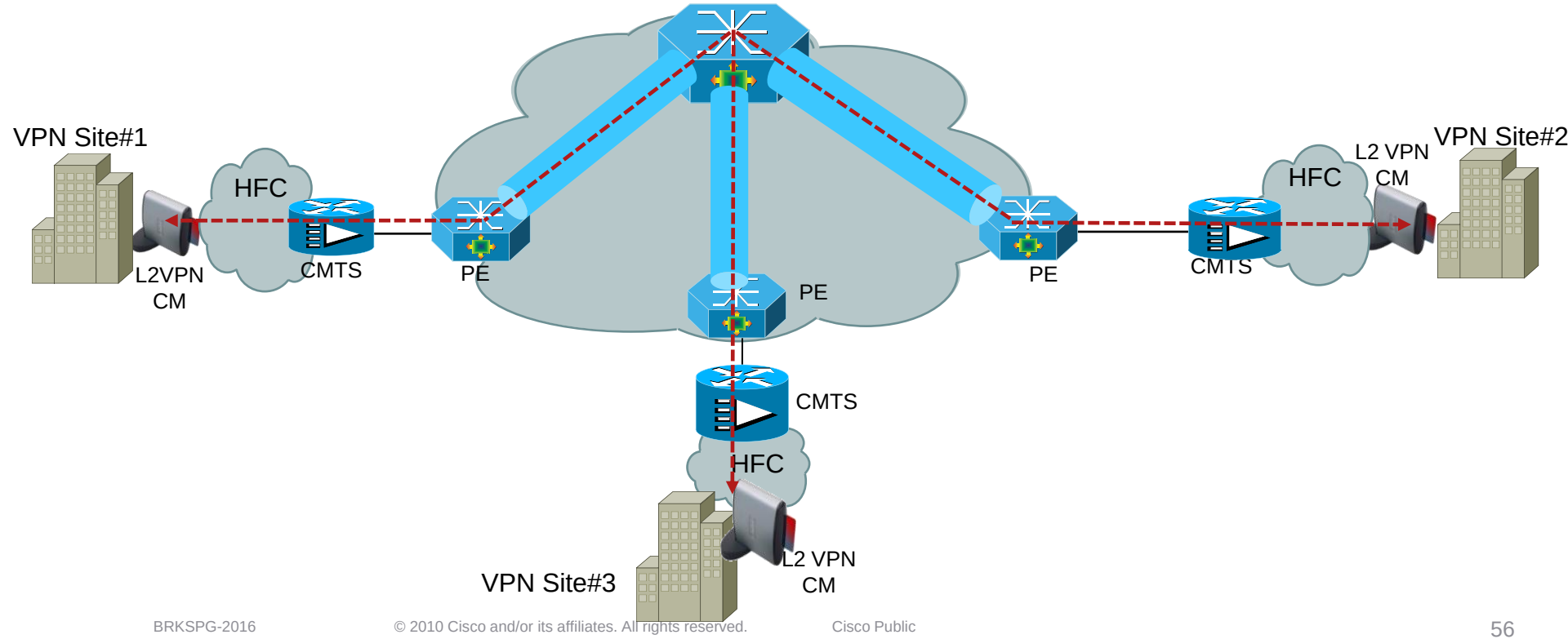
```
H1-10K#sh cable l2-vpn xconnect dot1q-vc-map 0022.3a61.7bcf verbose
Load for five secs: 1%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 17:23:02.633 EDT Mon Mar 22 2010

MAC Address                    : 0022.3a61.7bcf
Customer Name                  : TLSoDOCSIS
Prim Sid                       : 187
Cable Interface                : Cable5/1/0
Ethernet Interface             : GigabitEthernet3/1/0
DOT1Q VLAN ID                  : 25
Total US pkts                  : 0
Total US bytes                 : 0
Total DS pkts                  : 0
Total DS bytes                 : 0
```

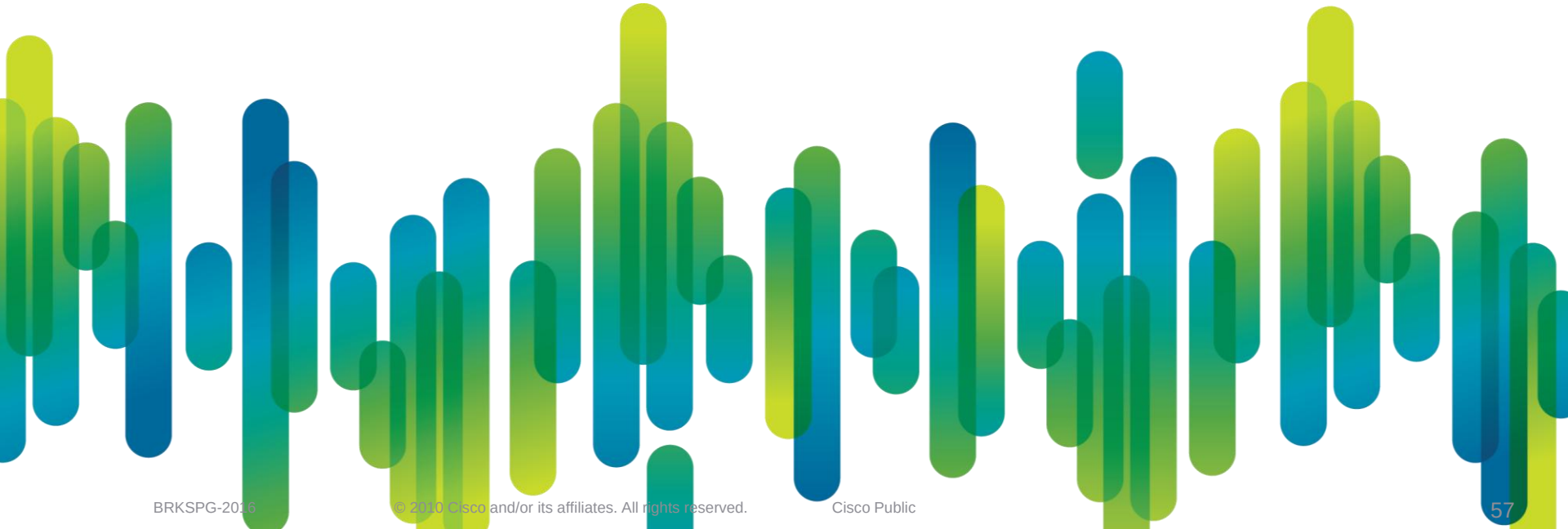
TLS Over DOCSIS

Multipoint (E-LAN) Service

- Upstream routers implements the multipoint aspect
- Full mesh VPLS may be used
- H-VPLS recommended for better scaling



Dot1Q-Based BSoD



Dot1Q-Based BSoD Overview

- Standardized by CableLabs
- Requires DOCSIS 2.0+
- Zero touch CMTS provisioning
  - No per site CMTS configuration required
  - Unique CM config file per L2VPN CM
- Up to 4 L2VPN's per CM based on service flow classification
  - Multiplexed (EVPL/EVPLAN) and non-multiplexed (EPL/EPLAN) services

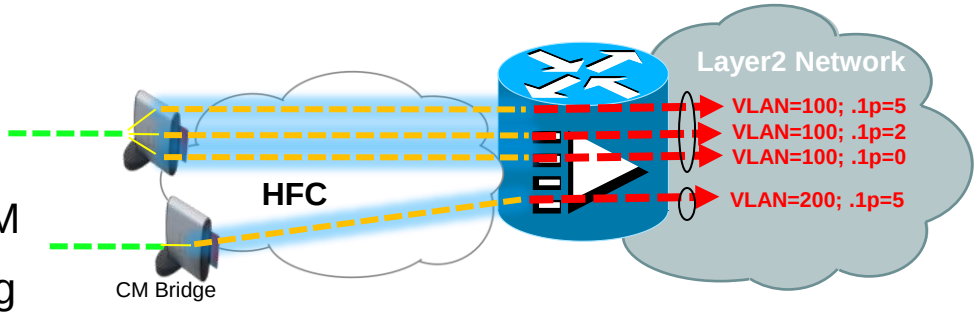
Dot1Q-Based BSoD Architecture

- CMTS implements L2 “Network Service Interface”—NSI
  - Statically defined NSI Interface
- NSI encapsulation is set to Dot1Q
- Individual DOCSIS service flow map to a VLAN
  - Mapping is defined by CM via CM config file
  - VLAN tagged frames forwarded on NSI
  - CMTS send/receive IP/MPLS and L2 traffic on same NSI
- Upstream PE router implements EoMPLS or H-VPLS

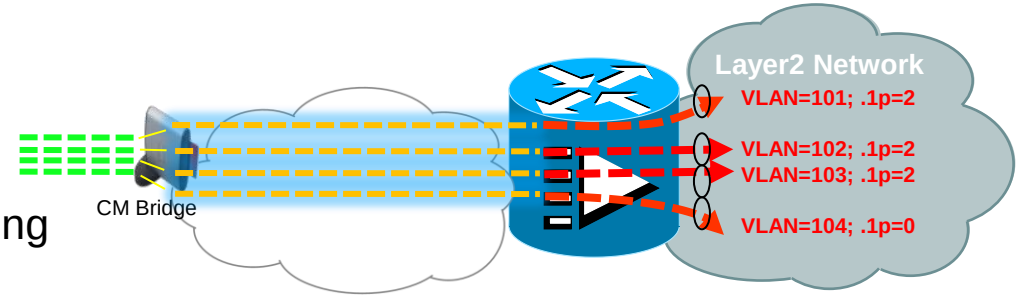
Dot1Q-Based BSoD Services

Service Multiplexing

- Service multiplexing on CM allowed by CableLabs
  - Allows for more services than TLS over DOCSIS
- Many US SFs to One VLAN
  - EPL type services
  - One VLAN for all traffic from CM
  - May use per SF 802.1p marking
  - Up to 8 US SFs

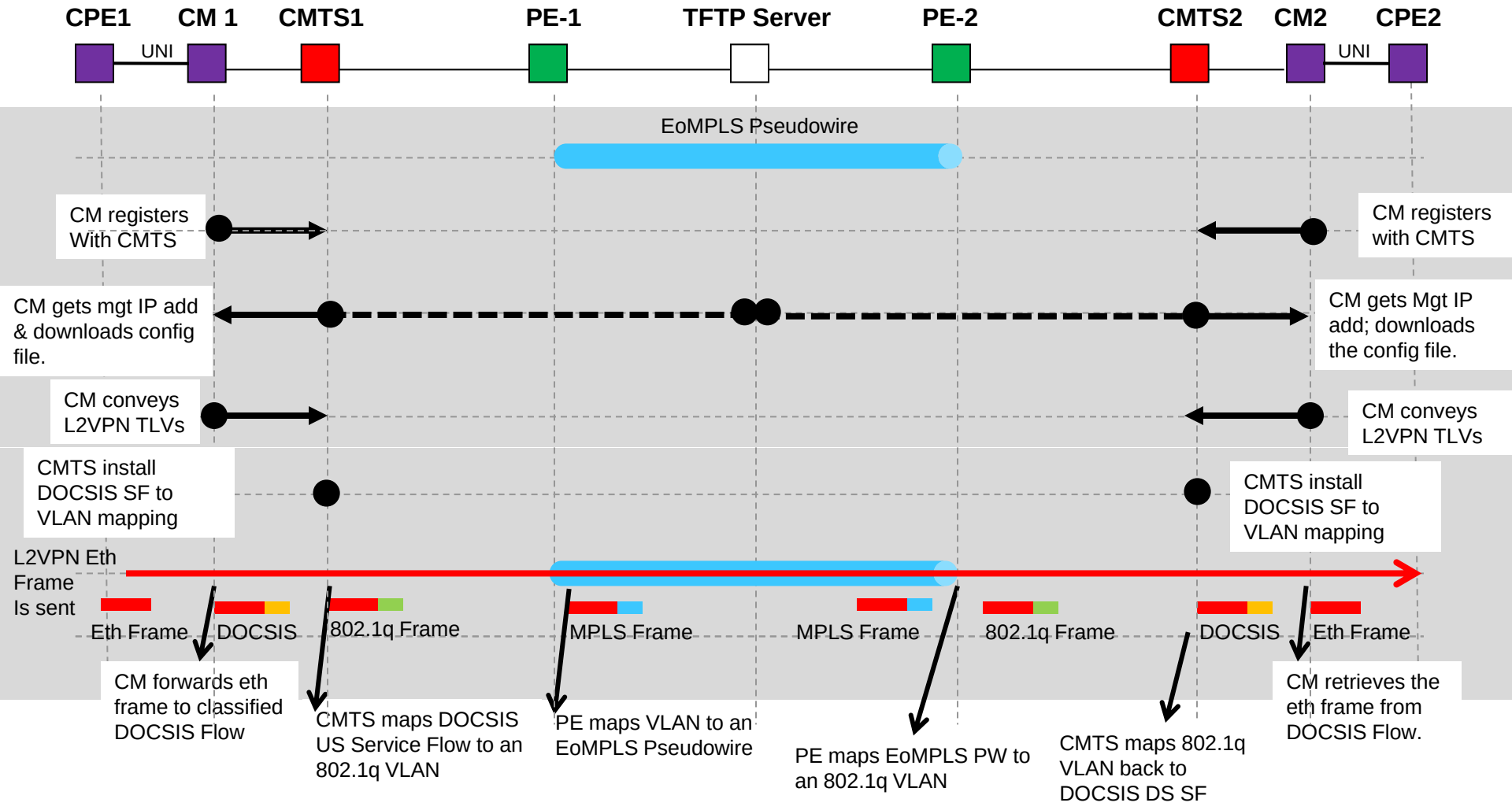


- One US SFs to One VLAN
  - EVPL type services
  - Up to 4 VLAN for a single CM
  - May use per SF 802.1p marking
  - Up to 8 US SFs total

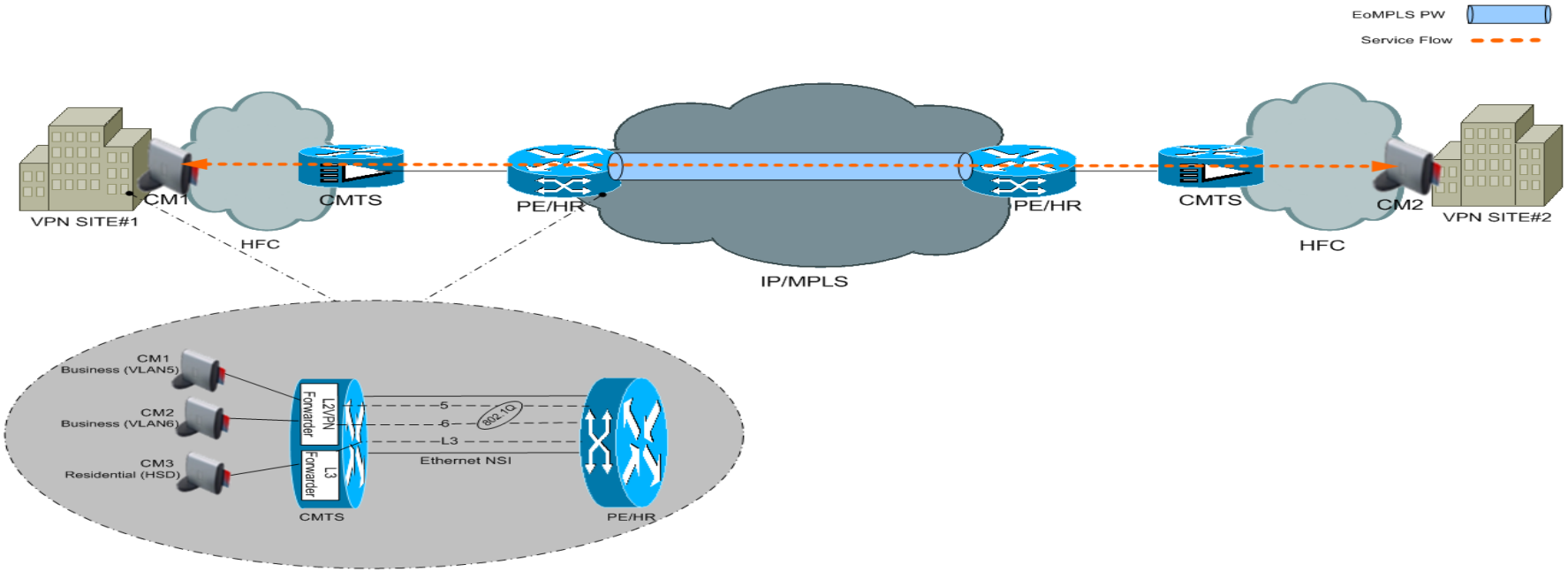


Dot1Q Based BSoD

Control Plane and Data Plane Flow



End-to-End Dot1Q-Based BSoD Service



CMTS

```
Cable l2-vpn-service xconnect nsi dot1q

cable l2-vpn-service xconnect nsi dot1q interface
Gig1/1/0
```

Designated NSI Interface

NSI Encapsulation

MPLS PE

```
interface GigabitEthernet1/23.100
 encapsulation dot1Q 100
 xconnect 99.1.1.21 50 encapsulation mpls
```

Dot1Q-Based BSoD Configuration

CM Config File Requirements

```
3,NetworkAccess,1,1
18,MaxCPE,1,0
24,UsServiceFlow
              1,ServiceFlowRef,2,1
              6,QosParamSetType,1,07
              43,VendorSpecificSubtype
                8,VendorIdentifier,3,FF FF FF
                5,L2VPNEncoding
                1,L2VPNIdentifier,9, DOT1Q BSoD
                8,IngressUserPriority,1,04
25,DsServiceFlow
              1,ServiceFlowRef,2,3
              6,QosParamSetType,1,07
29,GlobalPrivacyEnable,1,1
45,DUTFiltering
              1,DUTControl,1,01
43,GeneralExtensionInformation
              8,VendorIdentifier,3,FF FF FF
              5,L2VPNEncoding
                1,L2VPNIdentifier,9, DOT1Q BSoD
                2,NSIEncapsulation
                           2,IEEE802.1Q,2,100
```

Vendor specific subtype for L2VPN.

Vendor ID for GEI

L2VPN Id=DOT1Q BSoD must be the same as what's specified in L2VPN Encoding.

.1p bits = 4 to be imposed by CMTS

L2VPN Id=MPLS BSoD must be the same as what's specified in L2VPN Encoding.

100 is 802.1q VLAN id to be imposed by CMTS

```
CMTS-10K#
!
Cable l2-vpn-service xconnect nsi dot1q

cable l2-vpn-service xconnect nsi dot1q interface Gig1/1/0
!
```

One-time config needed on CMTS.

Dot1Q-Based BSoD Service Verification

- Verify CM is online as Dot1Q BSoD

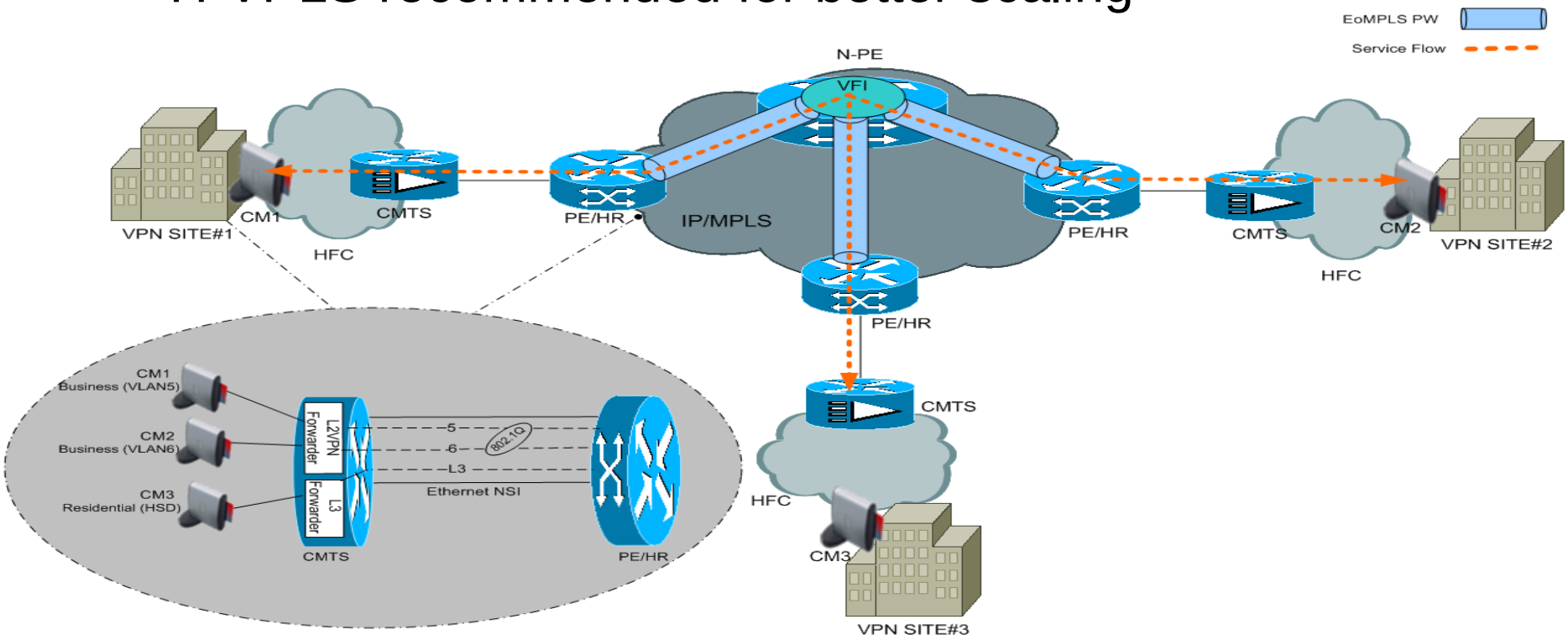
```
CMTS-uBR10k#sh cable l2-vpn xconnect dot1q-vc-map 0022.3a61.7bcf verbose

MAC Address             : 0022.3a61.7bcf
Prim Sid                : 17
Cable Interface         : Cable5/1/0
L2VPNs provisioned      : 1
DUT Control/CMIM        : Enable/0x8000FFFF
VPN ID                  : DOT1Q BSoD
L2VPN SAID              : 12302
Upstream SFID Summary   : 29
Upstream SFID [29   ]   : SID 17   UserPrio 4
Downstream CFRID[SFID]: Primary SF
CMIM                    : 0x60
Ethernet Interface      : GigabitEthernet3/1/0
DOT1Q VLAN ID           : 100
Total US pkts           : 0
Total US bytes          : 0
Total US pkt Discards   : 0
Total US byte Discards: 0
Total DS pkts           : 0
Total DS bytes          : 0
Total DS pkt Discards   : 0
Total DS byte Discards: 0
```

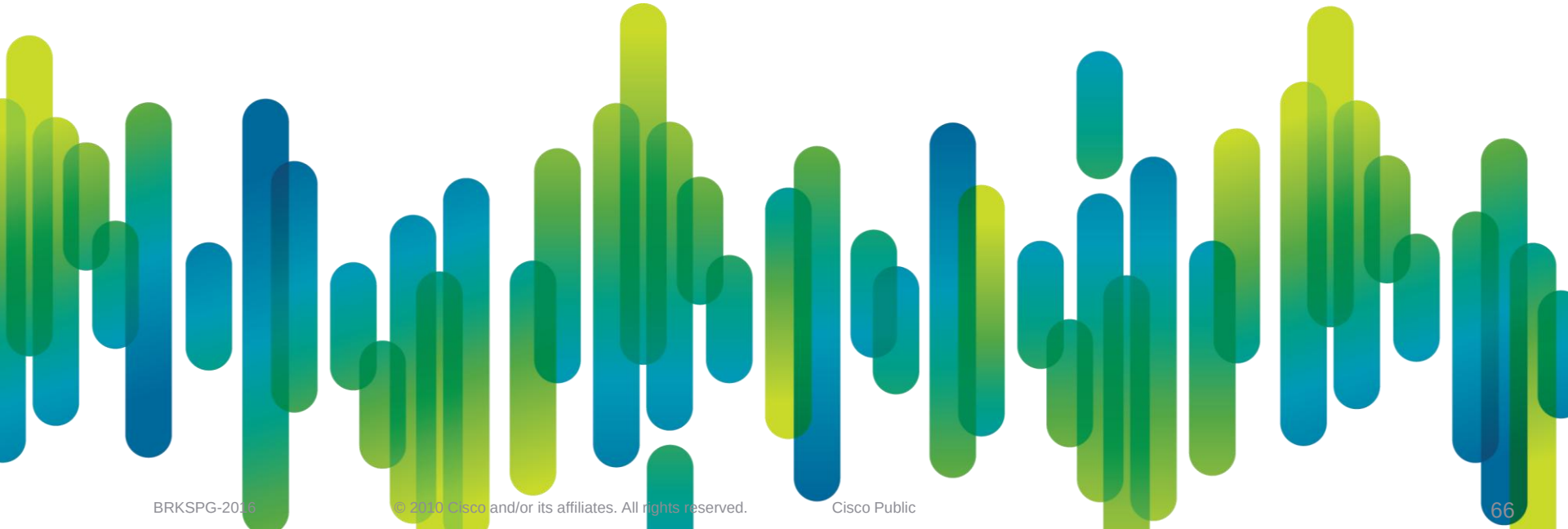
Dot1Q-Based BSoD

Multipoint (E-LAN) Service

- Upstream routers implements the multipoint aspect
- H-VPLS recommended for better scaling



MPLS-Based BSoD Services



MPLS-Based BSoD Services

- Why settle for VLAN encapsulation on CMTS for BSoD?
- Evolution of Dot1Q-Based BSoD Services
- EoMPLS on CMTS !!!

  Supported on CMTS 12.2(33)SCC and later
- No need for upstream PE device
- Better scaling (no more 4000 VLAN limit)
- Upstream redundancy and load-balancing

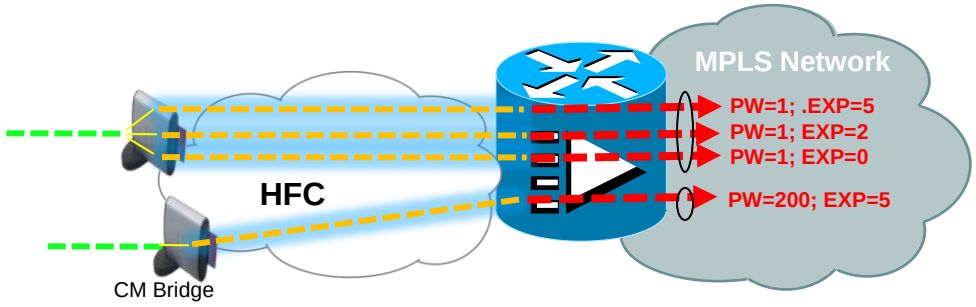
MPLS-Based BSoD Architecture

- NSI encapsulation is set to MPLS on CMTS
- CM maps Ethernet UNI to a DOCIS service flow
- DOCSIS service flow map to an EoMPLS PW
  - Mapping is defined by CM via CM config file
  - EoMPLS frames forwarded on any available MPLS uplink
- Zero Touch CMTS provisioning possible
  - Cable modem config file define PW parameters
- QoS provided through MPLS EXP bits

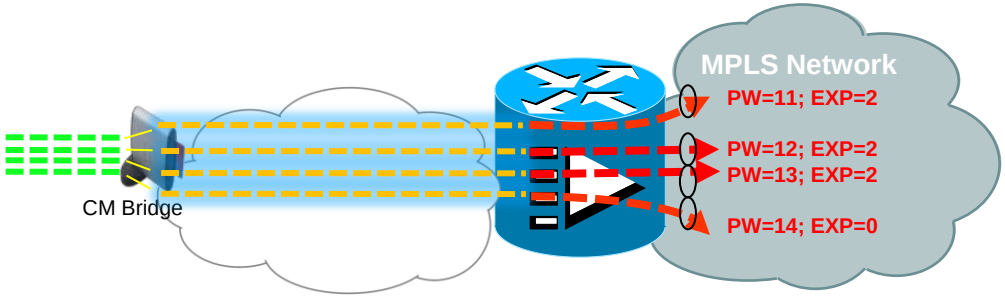
MPLS-Based BSoD Services

Service Multiplexing

- Service multiplexing on CM allowed by CableLabs
  - Allows for more services than TLS over DOCSIS
- Many US SFs to One PW
  - EPL type services
  - One PW for all traffic from CM
  - May use per SF EXP marking
  - Up to 8 US SFs

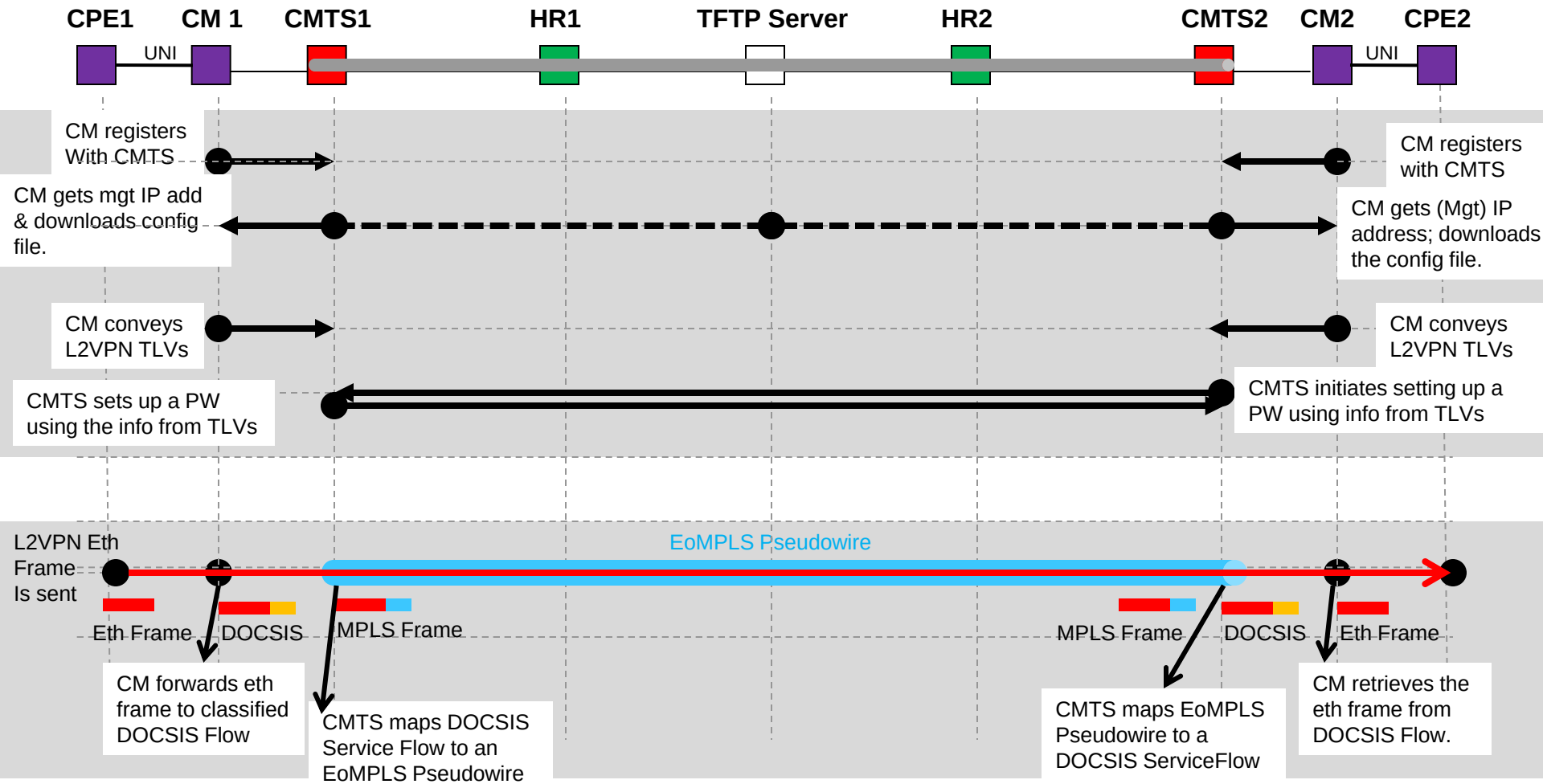


- One US SFs to One PW
  - EVPL type services
  - Up to 4 PW for a single CM
  - May use per SF EXP marking
  - Up to 8 US SFs total

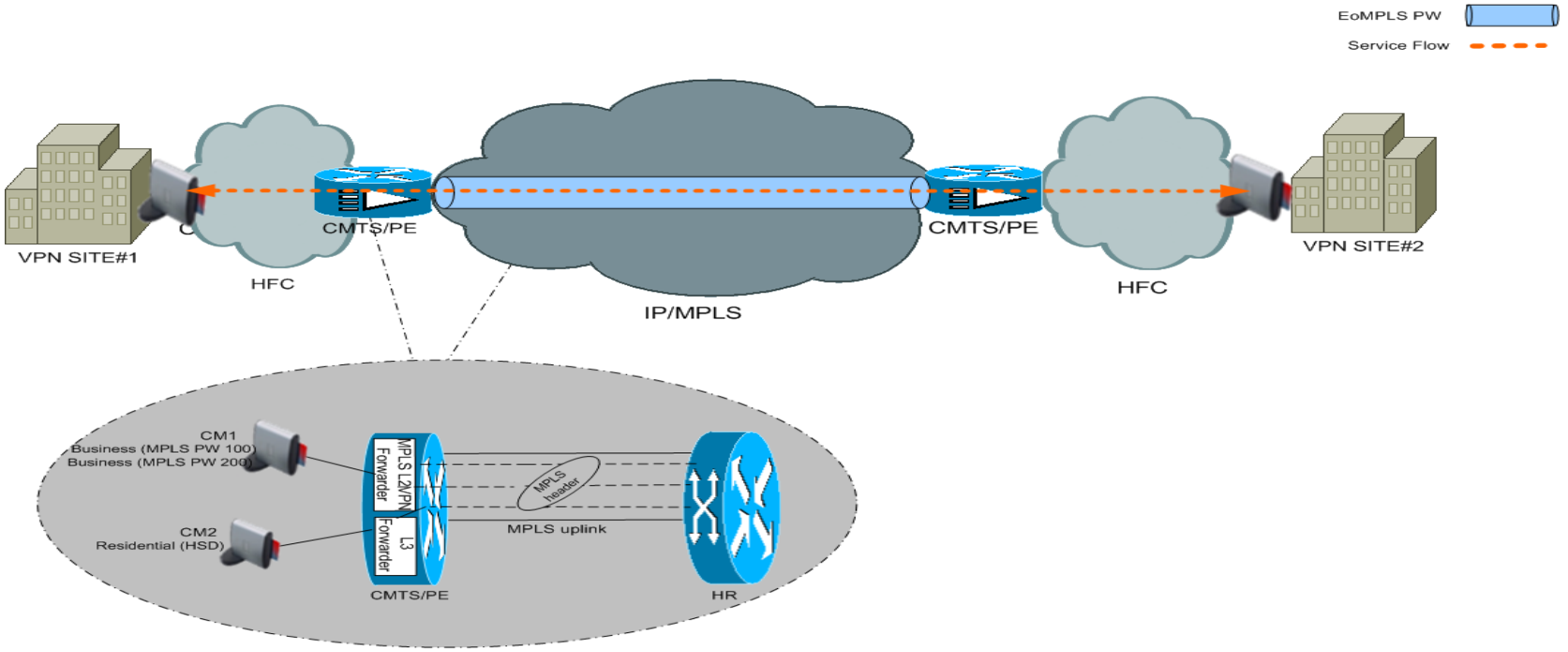


MPLS-Based BSoD

Control Plane and Data Plane Flow



End-to-End MPLS-Based BSoD Service



CMTS

```
cable l2-vpn-service xconnect nsi mpls
```

NSI Encapsulation

MPLS-Based BSoD Configuration

CM Config File Requirements

```
3,NetworkAccess,1,1
18,MaxCPE,1,16
24,UsServiceFlow
            1,ServiceFlowRef,2,1
            6,QosParamSetType,1,07
            43,VendorSpecificSubtype
              8,VendorIdentifier,3,FF FF FF
              5,L2VPNEncoding
              1,L2VPNIdentifier,9, MPLS BSoD
              8,IngressUserPriority,1,04
25,DsServiceFlow
            1,ServiceFlowRef,2,3
            6,QosParamSetType,1,07
29,GlobalPrivacyEnable,1,1
45,DUTFiltering
            1,DUTControl,1,01
43,GeneralExtensionInformation
            8,VendorIdentifier,3,FF FF FF
            5,L2VPNEncoding
              1,L2VPNIdentifier,9, MPLS BSoD
              2,NSIEncapsulation
                        4,MPLSIPv4Peer,5,1.99.1.1.22
                        5,AttachmentGroupID,4,55 55 55 55
                        6,SourceAttachmentIndividualID,4,00 00 07 d1
                        7,TargetAttachmentIndividualID,4,00 00 07 d1
```

```
CMTS-10K#
!
cable l2-vpn-service xconnect nsi mpls
!
```

Optional: Vendor specific subtype for L2VPN.

Vendor ID for GEI

L2VPN Id=MPLS BSoD must be the same as what's specified in L2VPN Encoding.

MPLS EXP=4 to be imposed by CMTS

L2VPN Id=MPLS BSoD must be the same as what's specified in L2VPN Encoding.

99.1.1.22 is peer PE's IP address.*

2001 is used as the PW-id.

Source AII and Target AII must be the same.

One-time config needed on CMTS.

* Peer PE address may not be needed in the future.

MPLS-Based BSoD Service Verification

- Verify CM is online as MPLS BSOD

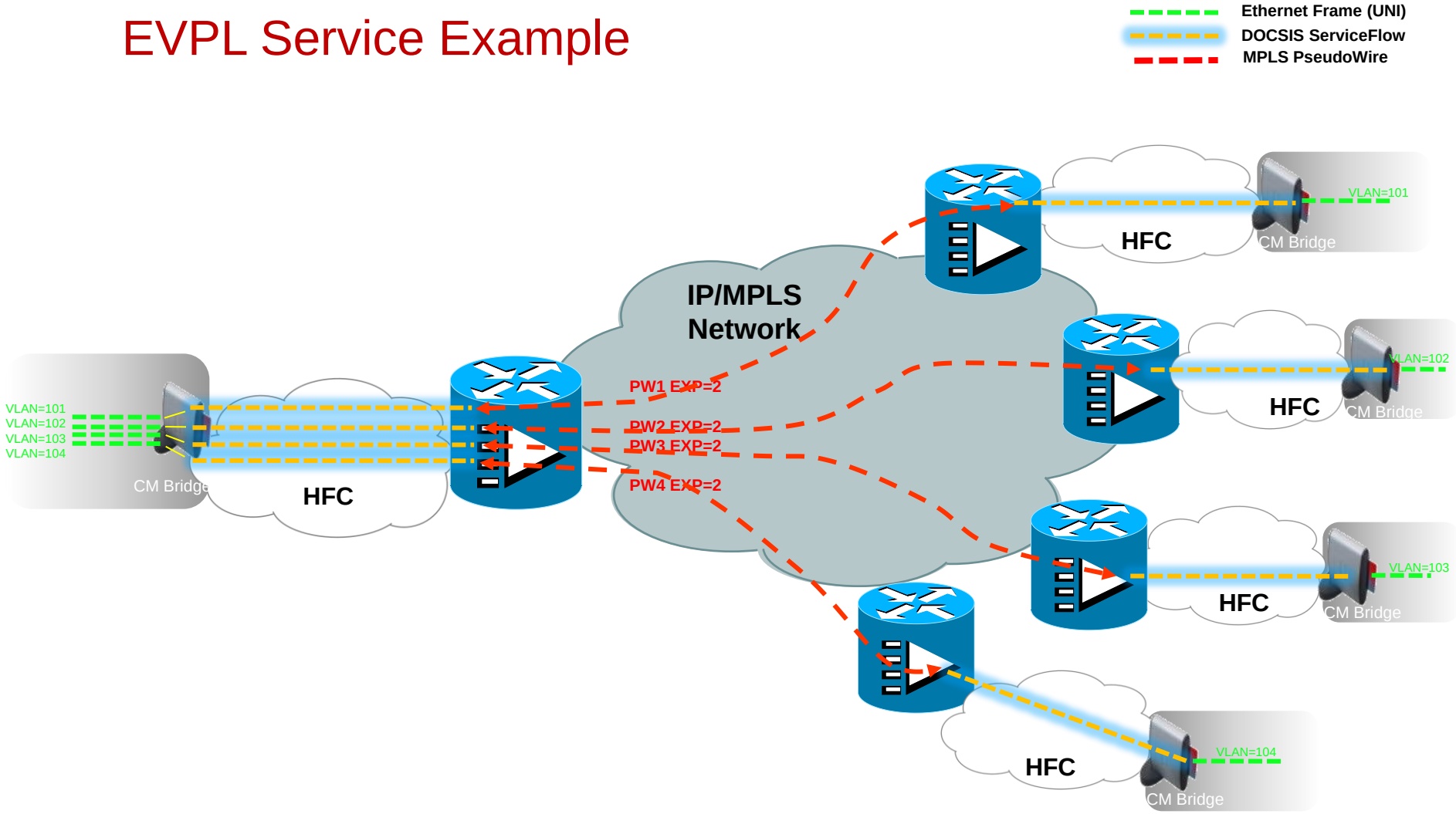
```
CMTS-uBR10k# sh cable l2-vpn xconnect mpls-vc-map 0022.3a61.7bcf verbose
MAC Address            : 0022.3a61.7bcf
Prim Sid               : 16
Cable Interface        : Cable5/1/0
L2VPNs provisioned     : 1
DUT Control/CMIM       : Enable/0x8000FFFF
VPN ID                 : MPLS EPL1
L2VPN SAID             : 12296
SAII                   : 000007D1
TAII                   : 000007D1
Upstream SFID Summary  : 27
Upstream SFID [27   ]  : SID 16   MPLS-EXP 4
Downstream CFRID[SFID] Summary: Primary SF
CMIM                   : 0x60
MPLS PEER IpAddress    : 99.1.1.22
MPLS PW VCID           : 2001
MPLS PW TYPE           : Ethernet
MPLS PW Circuit ID     : Bu254:2001
MPLS PW Remote State   : Up
MPLS PW Local  State   : UP
Total US pkts          : 0
Total US bytes         : 0
Total US pkt Discards  : 0
Total US byte Discards: 0
Total DS pkts          : 0
Total DS bytes         : 0
Total DS pkt Discards  : 0
Total DS byte Discards: 0
```

- Verify the Xconnect is up

```
CMTS-uBR10k#sh mpls l2transport vc 2001
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Bu254          DOCSIS 2001                99.1.1.22       2001       Up
```

MPLS-Based BSoD Service

EVPL Service Example



MPL-Based BSoD

Cable Modem Config File for EVPL

```
24,UsServiceFlow
            1,ServiceFlowRef,2,1
            6,QosParamSetType,1,07
            43,VendorSpecificSubtype
              8,VendorIdentifier,3,FF FF FF
              5,L2VPNEncoding
              1,L2VPNIdentifer,9,MPLS EVPL1
              8,IngressUserPriority,1,04
24,UsServiceFlow
            1,ServiceFlowRef,2,2
            6,QosParamSetType,1,07
            43,VendorSpecificSubtype
              8,VendorIdentifier,3,FF FF FF
              5,L2VPNEncoding
              1,L2VPNIdentifer,9,MPLS EVPL2
              8,IngressUserPriority,1,05
22,UsPacketClassifer
            1,ClassifierRef,1,1
            3,ServiceFlowRef,2,1
            11,IEEE802Classifier
              2, VlanID 100
22,UsPacketClassifer
            1,ClassifierRef,1,2
            3,ServiceFlowRef,2,2
            11,IEEE802Classifier
              2, VlanID 200
25,DsServiceFlow
            1,ServiceFlowRef,2,5
            6,QosParamSetType,1,07
25,DsServiceFlow
            1,ServiceFlowRef,2,6
            6,QosParamSetType,1,07
```

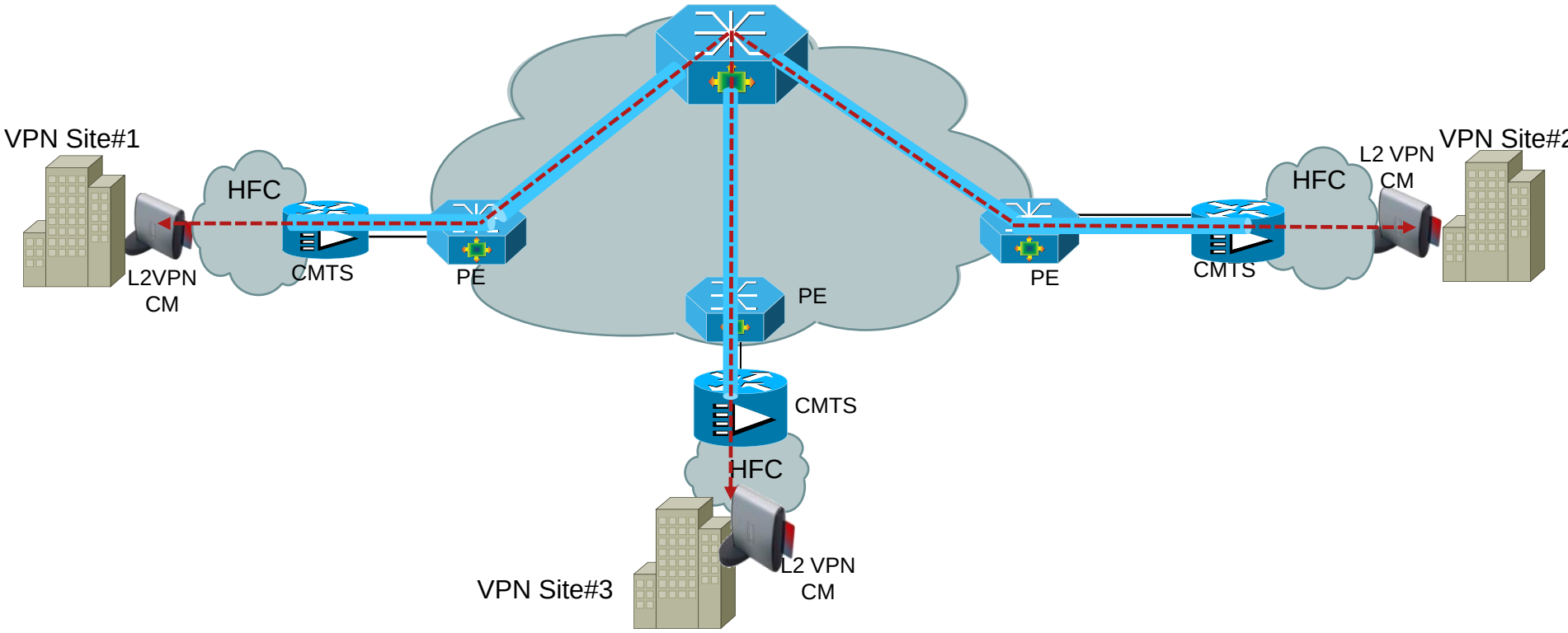
```
43,GeneralExtensionInformation
            8,VendorIdentifier,3,FF FF FF
            5,L2VPNEncoding
            1,L2VPNIdentifier,9, MPLS EVPL1
              2,NSIEncapsulation
                 4,MPLSIPv4Peer,5,1.99.1.1.22
                 5,AttachmentGroupID,4,55 55 55 55
                 6,SourceAttachmentIndividualID,4,00 00 07 d1
                 7,TargetAttachmentIndividualID,4,00 00 07 d1
43,GeneralExtensionInformation
            8,VendorIdentifier,3,FF FF FF
            5,L2VPNEncoding
            1,L2VPNIdentifier,9, MPLS EVPL2
              2,NSIEncapsulation
                 4,MPLSIPv4Peer,5,1.99.1.1.23
                 5,AttachmentGroupID,4,45 45 45 45
                 6,SourceAttachmentIndividualID,4,00 00 07 d2
                 7,TargetAttachmentIndividualID,4,00 00 07 d2
45,DUTFiltering
            1,DUTControl,1,01
```

```
CMTS-10K#
!
cable l2-vpn-service xconnect nsi mpls
!
```

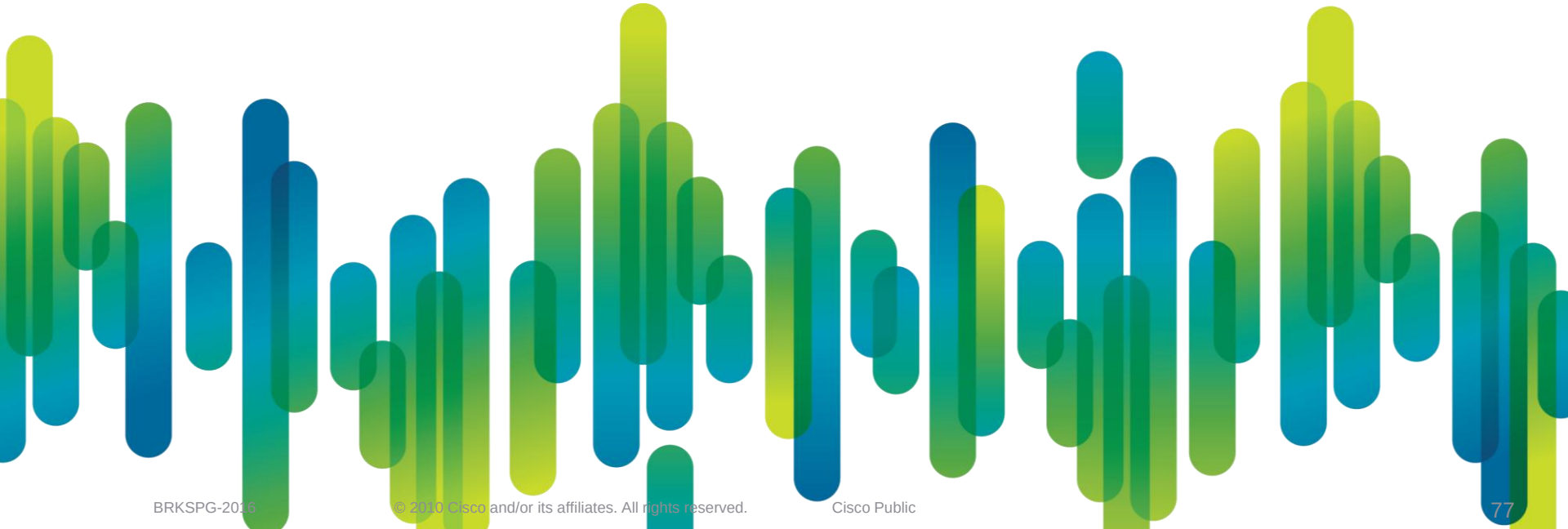
MPLS-Based BSoD

Multipoint (E-LAN) Service

- Dedicated N-PE with H-VPLS



Selecting a BSoD Deployment Model



Which BSoD Model to Use?

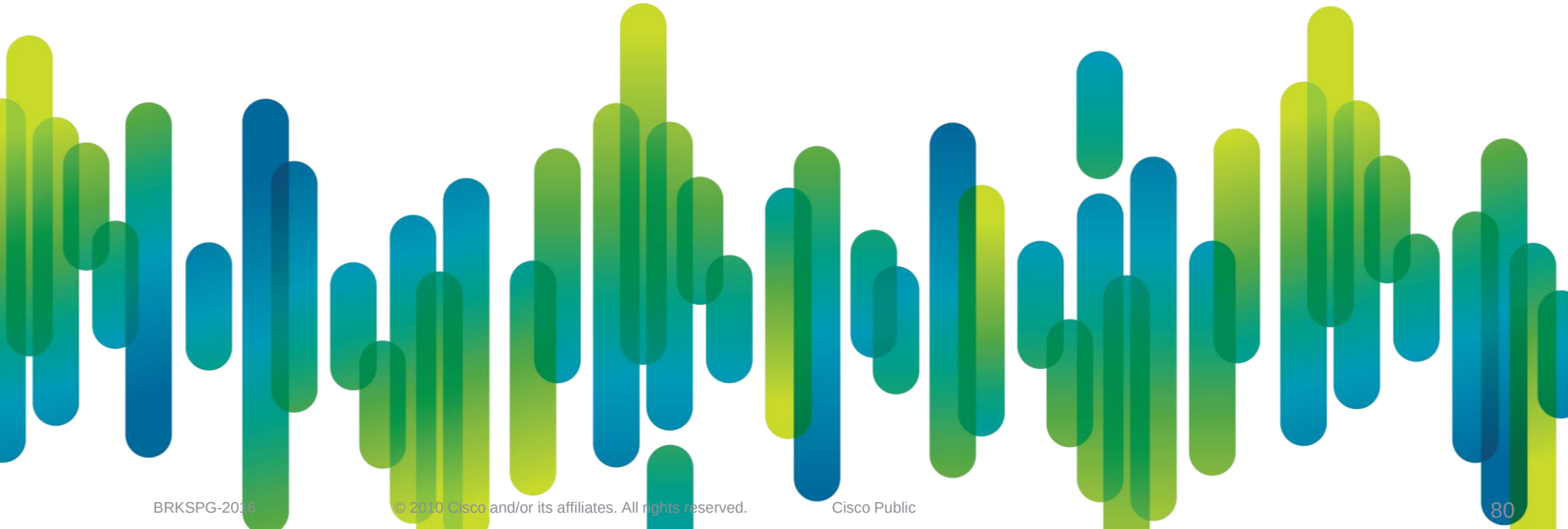
- No “One Size Fits All” answer
- Decision a function of various factors
- Technical Factors:
  - Scale and Performance
  - Fragmentation and Overhead
  - High Availability
  - Interworking with Fiber Access
- Operational Factors
  - CPE Cost
  - Ease of Deployment
  - CMTS Software and Configuration Changes

BSoD Comparison Matrix

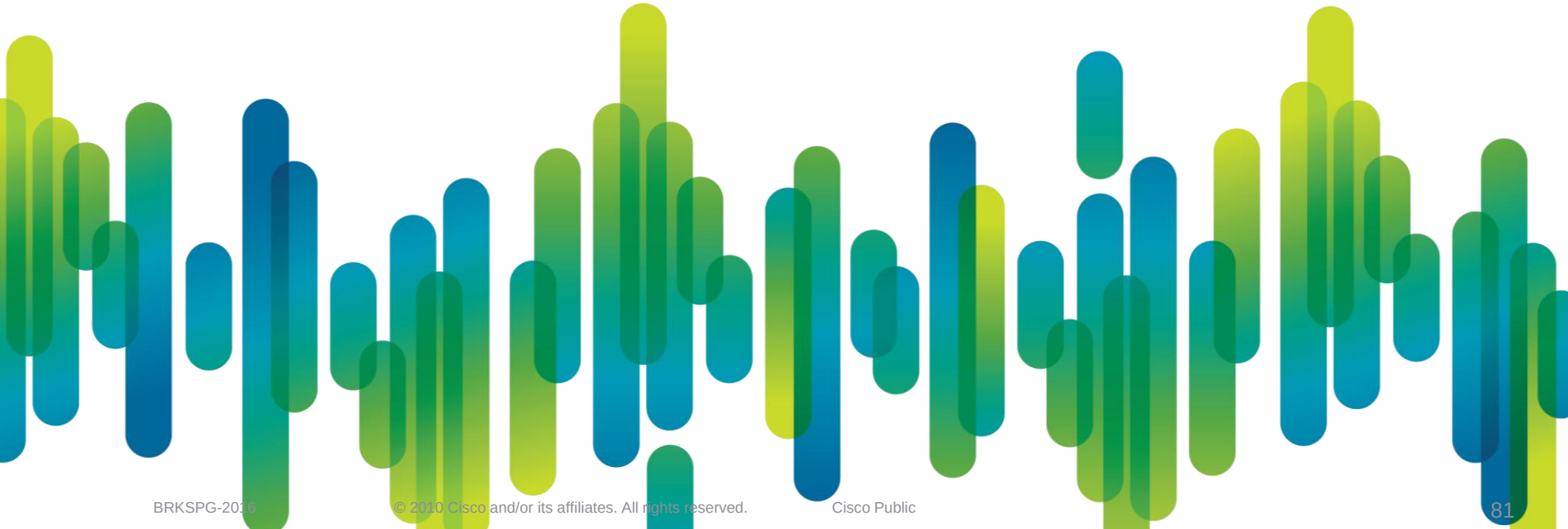
Deployment Consideration	CPE-Based L2VPN	TLS over DOCSIS	Dot1Q-Based BSOD	MPLS-Based BSoD
Scale	CPE Capability	4000	4000	16000 (uBR10K)
Fragmentation & Overhead	👎	👍	👍	👍
CMTS Uplink High Availability	👍	👎	👎	👍
Separate PE Required?	👍	👎	👎	👍
Fiber Interworking	Limited	👍	👍	👍
CPE Cost	👎	👍	👍	👍
DOCSIS Backend Changes	👍	👍	👎	👎 👍 *
CMTS Config Changes	No	Per L2VP Site	One Time	One Time *

* For time to market, Per Site L2VPN configuration on CMTS can be done via CLI, thus bypassing the DOCSIS backend changes requirement

Architectural Deployment Models



Considerations for deploying DOCSIS 3.0



Considerations for deploying DOCSIS 3.0

- Before deploying DOCSIS 3.0 services it is always useful to take some of the following into account
- What services are we planning to deploy ?

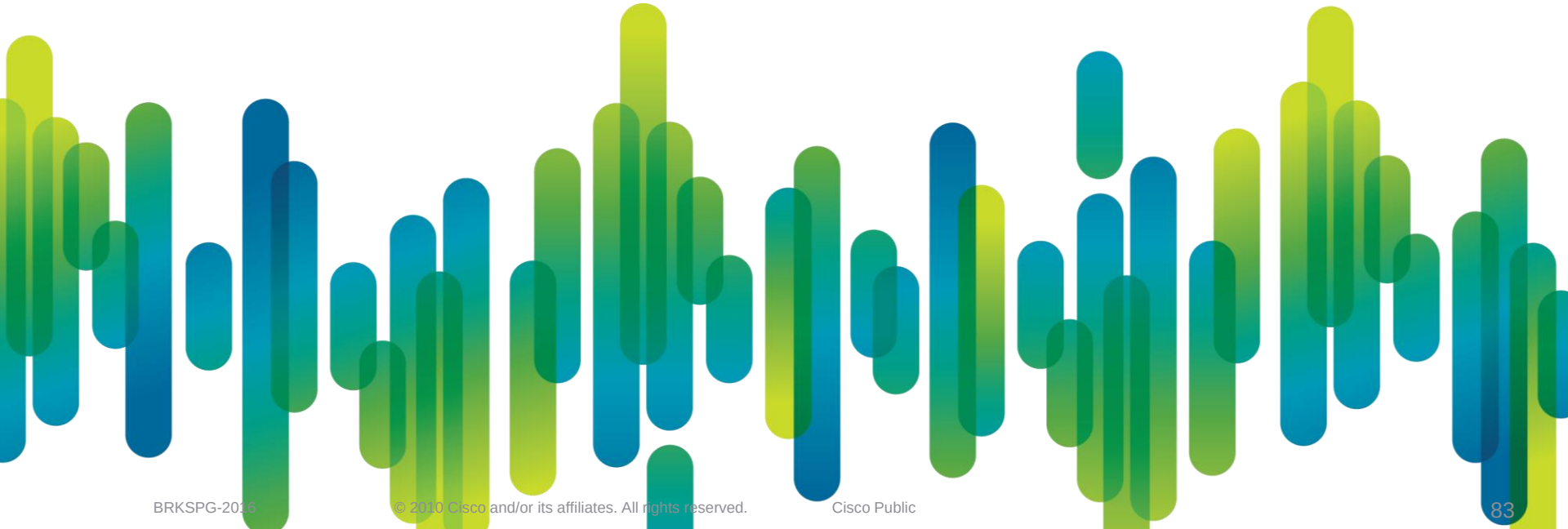
  For example: HSD (over 100Mbps Downstream),

  Video (VOD&BCAST),

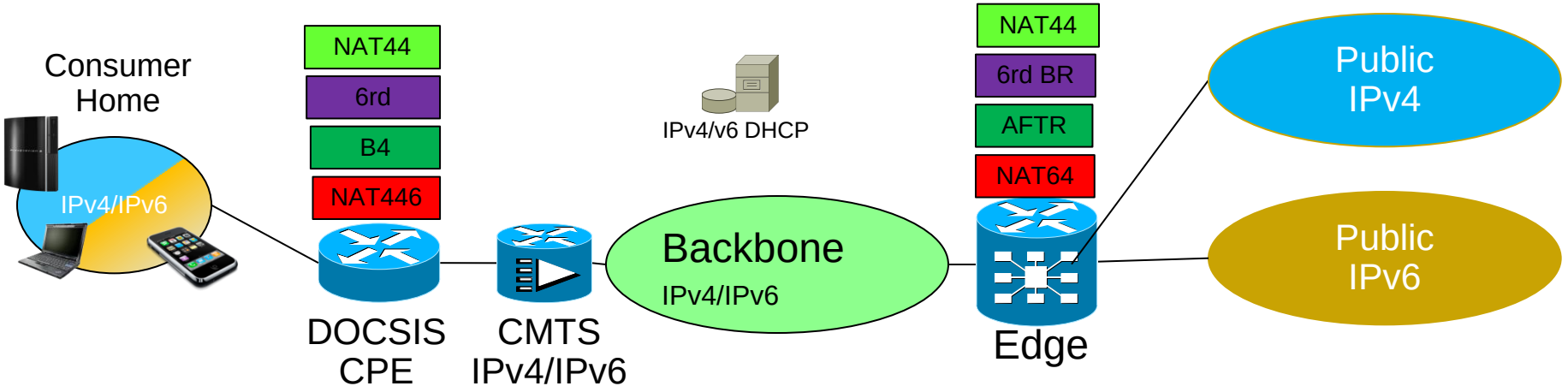
  Business services
- What DOCSIS 3.0 features are required to get these services?
- How do we run these services with the existing DOCSIS services in the HFC network ?
- How can we implement these services on the HFC network with as little change and as much flexibility as possible ?
- How do I manage these new services ?
- How do we ensure that the services that we deploy will be scalable for the future ?

ALL of these are **VALID** and **NEED** to be addressed!!

Scaling to IPv6

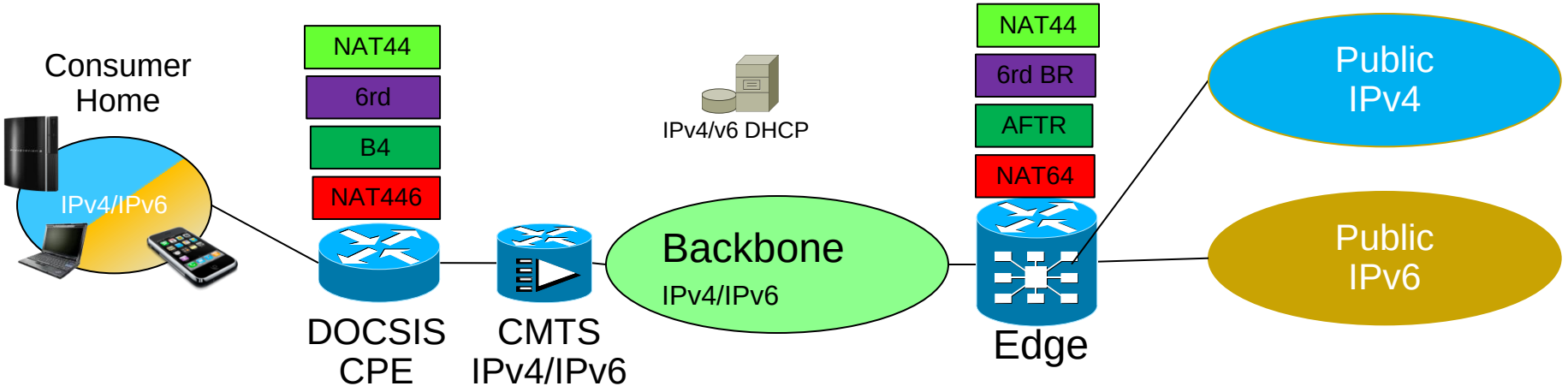


IPv6 in Cable Access Network



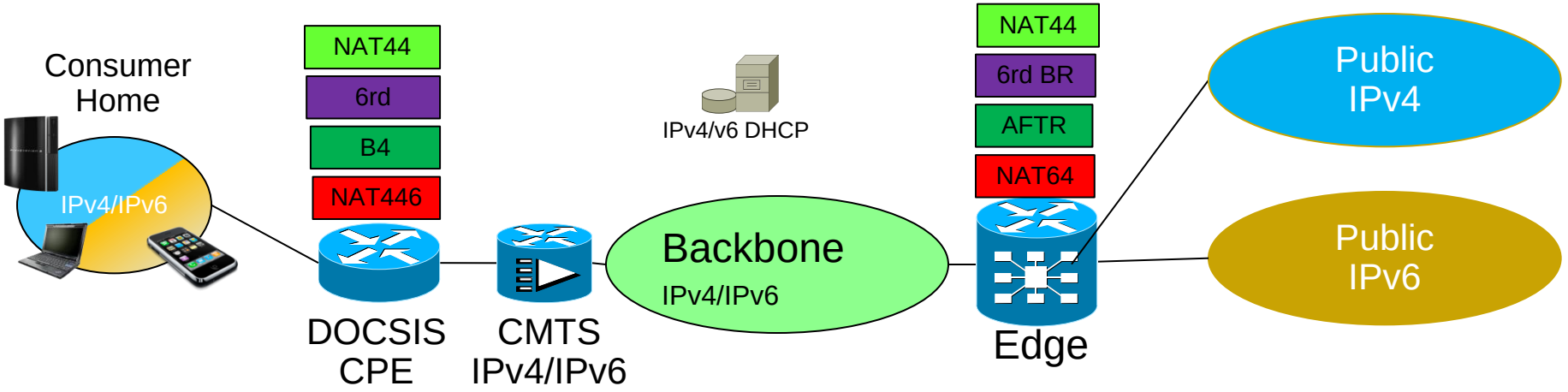
- SPs facing IPv4 exhaust and (also/because of that) want to introduce IPv6
  - Assumption is that v4/v6 internets will co-exist in mid/long-term
- Consumer CPE may be v4, v4/v6 or v6 while 1st hop router must be v4/v6
  - 1st hop router = CMTS (bridged DOCSIS CPE) or DOCSIS Gateway LAN Side
  - Bridged (legacy) DOCSIS CPE may limit the introduction of IPv6
  - We will not focus on CPE-based transition mechanisms e.g. 6to4 initiated on CPE
- CMTS and backbone network can be v4, v4/v6 or v6 (incl. 6PE/6VPE)
  - It affects transition techniques choice; that allows different connection patterns
  - Trivial fact; if CMTS+backbone is v6-only, v4 traffic must be tunneled or translated
- Edge of the network must be v4/v6 aware (to connect to both clouds)

IPv6 in Cable Access Network



- Provisioning system must be enhanced
  - Support DHCPv6 or support provisioning extensions for various transition techniques
- v4/v6 connection patterns may require different transition mechanisms
  - v4-only host ⇔ v4 Internet: native (v4 backbone) and tunneled or translated (v6 backbone)
  - v6-only host ⇔ v6 Internet: native (IPv6 backbone) and tunneled (IPv4 backbone)
    - translation is challenging since we would need to map bigger set to smaller set
  - Dual-stack host ⇔ v4/v6 Internet (depending on DNS response and availability)
  - v6-only host ⇔ v4-only Internet: NAT64/DNS64.
    - Allowing for incoming connections has some additional implications
  - v4-only host ⇔ v6-only Internet: ?possible i.e. how to map v6 Internet space to v4?

IPv6 in Cable Access Network



- Transition techniques are mostly between 1st hop router over the edge

  Main goal is to allow for different connection patterns over the existing CMTS and backbone infrastructure

  Transition mechanism is combination of tunneling (v4/v6, v6/v4), address family translation (v4 ⇔ v6), NAT44 (either on the gateway or LSN44) and native v4/v6 forwarding.

- Migration to v6 in internal ecosystem

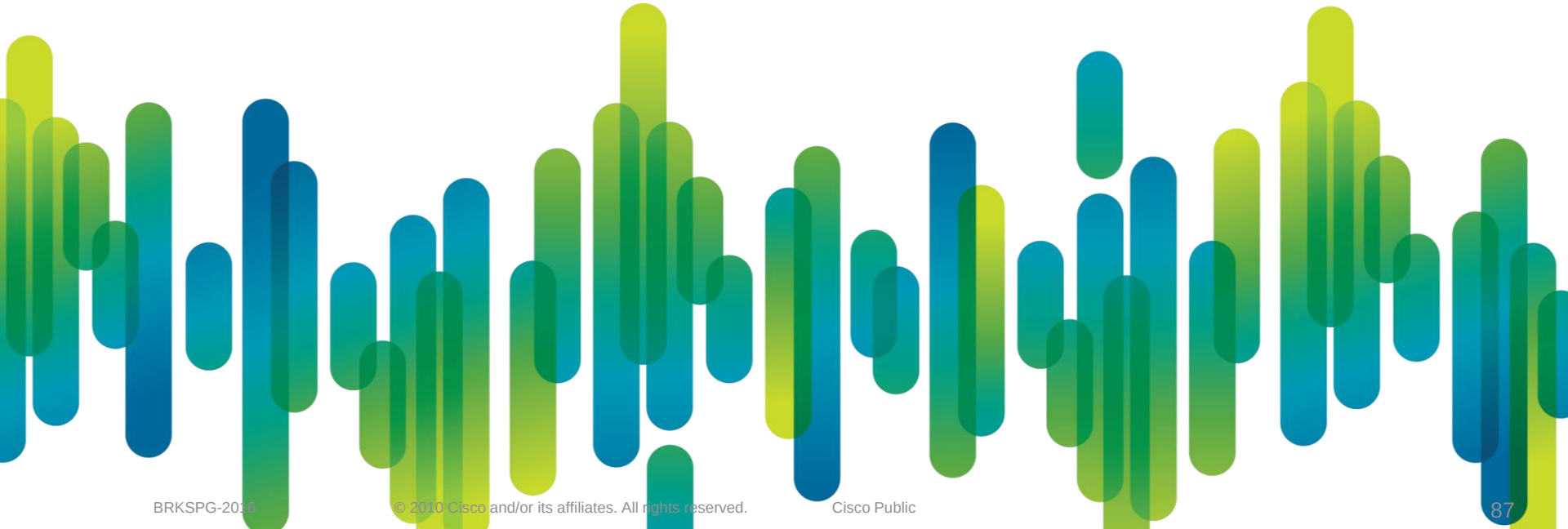
  DOCSIS CPE provisioning and management with IPv6: is not just IP addressing change

  Moving to IPv6 VoIP may have significant impact on the overall voice solution

  NMS systems

  IPTV, VoD

Network Quality of Service



Network Congestion Management and Avoidance

- Within the multi-play service provider network there may be links carrying all services and others carrying a subset of the services.
- For example, a link could carrying the following services and sample bandwidth percentages:
  - Residential/Commercial Voice (2-3 percent)
  - Video conferencing, Telepresence (1 percent)
  - Broadcast Video (10 percent)
  - Video on Demand (5-30 percent)
  - Business Services (EoMPLS, H-VPLS, L3VPN, IP-Services) (10 percent)
  - High Speed Internet (10 - 20 percent)
- In addition to the services above, the network may need to support the following:
  - Internal business applications (1-5 percent)
  - Control-plane traffic (<2 percent)

Network Congestion Management and Avoidance

- Congestion management and avoidance techniques are applied egress on all core interfaces.
- A queue model should be implemented to allow explicit allocation of bandwidth for revenue generating services with varying SLA requirements and protect the network.
- **Weighted random early detection** can be implemented for traffic classes with adaptive flows
- **Tail drop** can be implemented for real-time video
- **Strict priority queue** can be implemented for voice and video conferencing applications.

Network Congestion Management and Avoidance

Network Based QOS

Traffic Class	Traffic Type (DSCP/EXP)	Congestion Management
Priority	VoIP bearer (EF/5)	Policed strict priority
	Video conferencing bearer (CS5/5)	
	VoIP/Video conferencing signaling (CS3/5)	
Control-Plane	Network Control Plane (CS6/6)	WRED
Video	Broadcast Video (AF41/4)	Tail Drop
	VoD (AF42/3)	
	Streaming TV (AF43/3)	
Commercial Services	H-VPLS, L3VPN (EXP=1)	WRED
Business Critical	Service Provisioning, Control and Mgmt. (CS2/2)	WRED
	Ad Traffic (AF31/2)	
	Prioritized Data Services (AF21/2)	
	Network Management (CS2/2)	
Default	HSI (0/0)	WRED
	Content Distribution (AF11/0)	
	Gaming (0/0)	
	IP Services (0/0)	

Network Congestion Management and Avoidance Example

Example 4 Queue Model

Queue	Bandwidth Allocation	Service Marking (DSCP/EXP)	Congestion Treatment
Priority	10%	Voice/Video Bearer (EF/5) Signalling (CS3/5)	Policed
Video	55%	Multicast Video (AF41/4)[1]	Tail Drop at 100 ms
		Unicast Video (AF42/3)	Tail Drop at 50 ms
Business Services	20%	EoMPLS, H-VPLS, VPLS, L3VPN (Transparent/1)[2] IP-Services (CS1/1)	RED Min/Max 50/100 ms
Default	15%	High Speed Internet (0/0)	RED Min/Max 50/100 ms
		Internal Business (CS2/2)	RED Min/Max 100/150 ms
		Control-Plane (CS6/6)	RED Min/Max 150/200 ms

Network Congestion Management and Avoidance Example

Example 5 Queue Model

Queue	Bandwidth Allocation	Service Marking (DSCP/EXP)	Congestion Treatment
Priority	10%	Voice/Video Bearer (EF/5) Signalling (CS3/5)	Policed
Video	55%	Multicast Video (AF41/4)[1]	Tail Drop at 100 ms
		Unicast Video (AF42/3)	Tail Drop at 50 ms
Business Services	20%	EoMPLS, H-VPLS, VPLS, L3VPN (Transparent/1)[2] IP-Services (CS1/1)	RED Min/Max 50/100 ms
Business Critical	5%	Internal Business (CS2/2)	RED Min/Max 50/100 ms
		Control-Plane (CS6/6)	RED Min/Max 100/150 ms
Default	10%	High Speed Internet (0/0)	RED Min/Max 50/100 ms

Network Congestion Management and Avoidance Example

Example 6 Queue Model

Queue	Bandwidth Allocation	Service Marking (DSCP/EXP)	Congestion Treatment
Priority	10%	Voice/Video Bearer (EF/5) Signalling (CS3/5)	Policed
Video	55%	Multicast Video (AF41/4)[1]	Tail Drop at 100 ms
		Unicast Video (AF42/3)	Tail Drop at 50 ms
Business Services	20%	EoMPLS, H-VPLS, VPLS, L3VPN (Transparent/1)[2] IP-Services (CS1/1)	RED Min/Max 50/100 ms
Control-Plane	2%	Control-Plane (CS6/6)	RED Min/Max 50/100 ms
Business Critical	3%	Internal Business (CS2/2)	RED Min/Max 50/100 ms
Default	10%	High Speed Internet (0/0)	RED Min/Max 50/100 ms

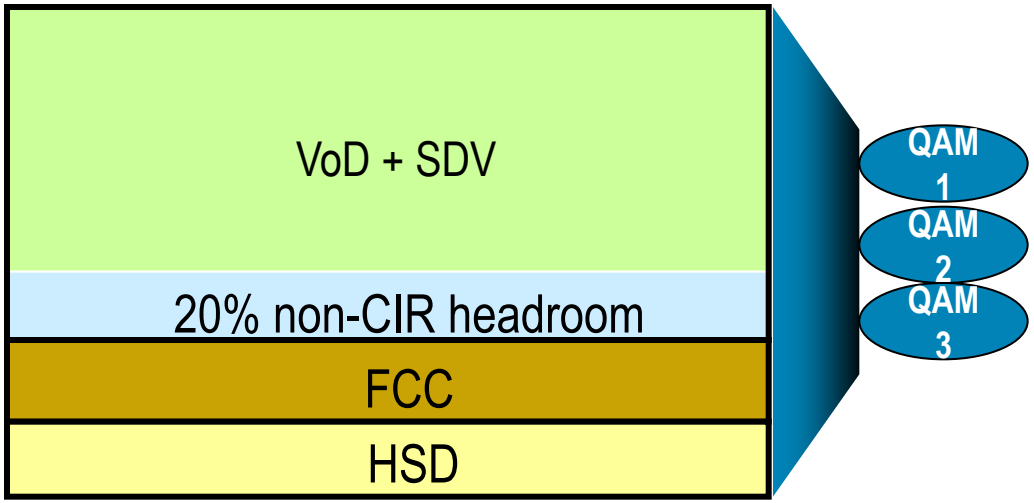
DOCSIS Quality of Service

Traffic type	DSCP	DOCSIS QoS priority	Bonding group	CIR
Interactive voice	EF	Any	HSD BD	CIR with PCMM signaling and low latency
Broadcast video	AF41	Any	Broadcast BD	Separate bonding group
Interactive video (VoD) or non-CIR best effort	AF42	Any	Video BD	CIR with PCMM for admission control
Dynamic multicast video	AF41	Any	Video BD	CIR with IGMP signaling for admission control
All control traffic	CS3	Any	Video BD	8 kbps per CM
Fast channel change	CS4	7 or 0	FCC BD	No CIR
High-speed data (Internet access)	BE	Any	HSD BD	No CIR

- DSCP marking for various traffic type
  - -- Downstream marking done at first hop routers closest to source
  - -- Upstream marking is done by the CPE/CMTS
- CIR admission control: VOD and SDV (if used)

QoS with Overlapping Bonding Groups

Dynamic bandwidth sharing among overlapping bonding groups



Bonding Group	Fixed BW (%)	Remaining ratio	Effective Guaranteed BW (%)
SDV & VoD & carousel (referenced as CIR bonding group)	90	0	72% if VoD flows are CIR 90% if VoD flows are non-CIR
FCC	5	100	23% if VoD flows are CIR 5% if VoD flows are non-CIR
HSD	5	0	5%

High Priority

Low Priority

- Attributed based forwarding is used to direct traffic to different bonding group
- Bonding group is associated with attributes
- Service flow is configured with attributes
- CMTS matches the SF attributes with bonding group attributes when directing SF

Upstream Qos

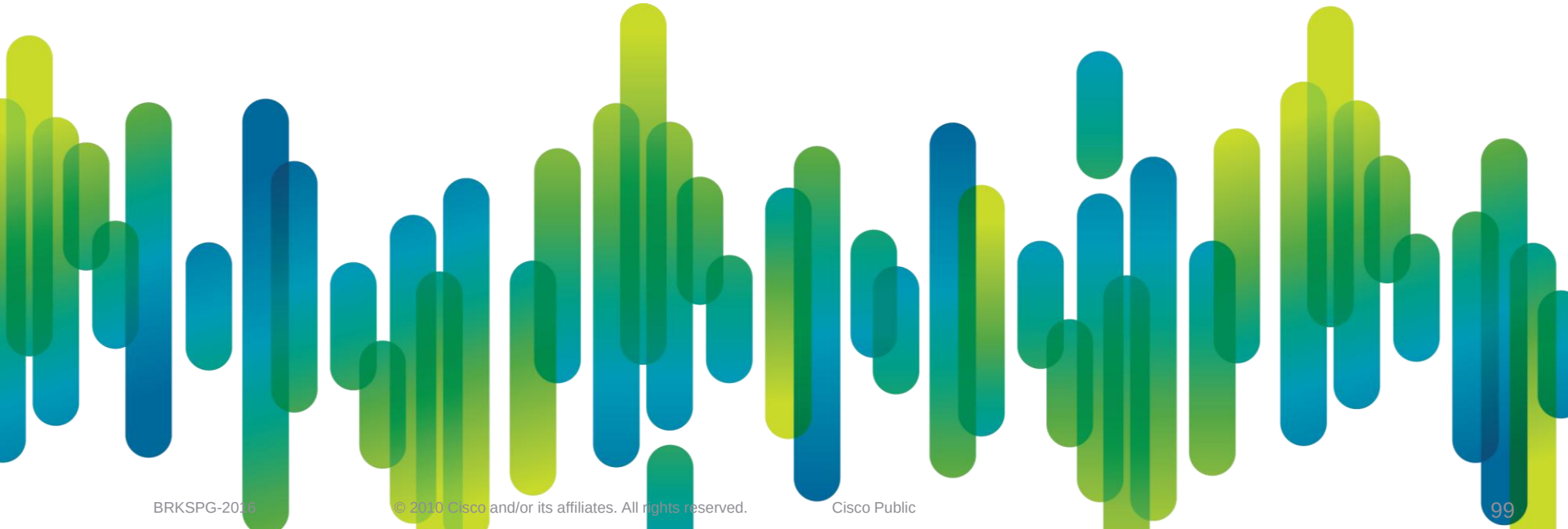
- The upstream QoS is slightly different from the downstream QoS.
- The upstream traffic is buffered at the CM; however, the scheduling and queue control are at the CMTS.
- The CMTS allocates bandwidth for each service flow. The QoS for upstream best-effort traffic uses a strict priority queue.
- At the CM, an upstream service flow can be configured with the appropriate DOCSIS priority.
- The classifier configured on the CM must match the upstream traffic going toward the ISDS and video servers.
- For IPTV applications, the upstream traffic consists mainly of the video control traffic and the TCP ACKs for streaming video

Upstream QOS

- Upstream Traffic Types, Priorities and scheduling types

Traffic type	DOCSIS QoS priority	DOCSIS scheduling type
Interactive voice	Any	Unsolicited grant service[1]
All control traffic	7	Best effort
TCP ACKs	6	Best effort
High-speed data (Internet access)	0	Best effort

Network Security



Network Security

- The focus will be on DOCSIS secutity, however general IP network security should also be ensured
  - Authentication, Authorization, and Accounting (AAA),
  - Security Server Protocols ,
  - Traffic Filtering and Firewalls,
  - IP Security and Encryption
- DOCSIS has extensive link level security
  - BPI+: Baseline Privacy
  - DES encryption
  - X.509 certificates
- Security enhancements are motivated primarily to prevent theft of service
- Secure provisioning of CMs
  - Unauthorized CMs can be prevented network access
- Encrypt data traffic between the CM and CMTS
  - Best effort / QOS Enabled IP data traffic
  - Multicast group traffic

Enhanced Security with DOCSIS 3.0

- AES required on CM and CMTS for DOCSIS 3.0

  Provides stronger traffic encryption, 128 bit Advanced Encryption Standard (AES) for user's data

  National Institute of Standards and Technology (NIST) has declared single DES as not acceptable for government applications.

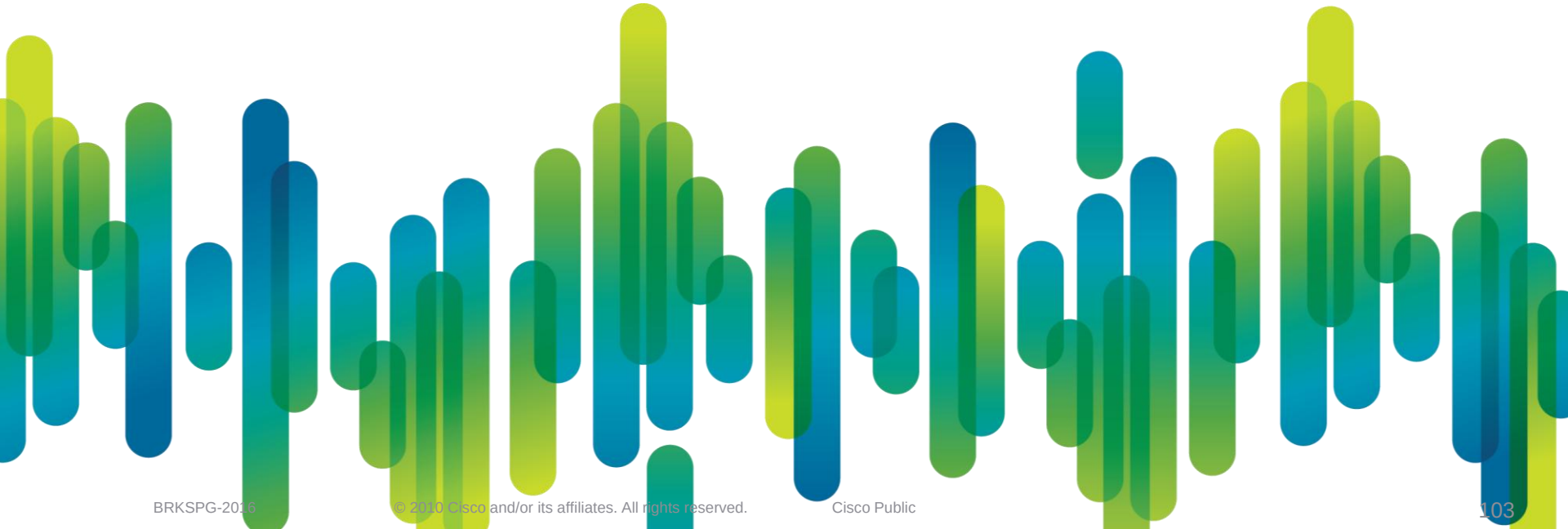
  Industry was concerned about public perception. DES is required for backwards compatibility

- Source-verify is now standardized
- ARP rate-limit
- Cert revocation: CRL + OCSP
- Enhanced software validation

Early Authentication and Encryption (EAE)

- Increases security of the CM provisioning process
  - Applies authentication before CM accesses MSO's operation support systems
  - Configuration file transfers encrypted
- MSO's have experienced:
  - Denial-of-service attacks on MSO's operation support systems
  - Hacked modems were requesting unauthorized services
- Authenticate CM after Ranging/before DHCP
  - Network admission control
  - Eliminate possibility of bypassing authentication by manipulating configuration file
- Per CM traffic: encrypted using primary SA (security association)
- Configurable
- EAE Exclusion
- Can be enabled on a per CM or per MAC domain basis

Summary



Summary

- Next Generation Services are being deployed today
- Leverage existing HFC infrastructure
- VDOC provides a cost effective and efficient architecture to deploy video services
- Business Services over DOCSIS picking up steam, already a number of European customers deploying BSoD
- Network-based BSOD provides flexibility and enhanced functionality
- Multiple decision factors for correct BSoD model
- End-to-End multiservice architectures can be deoloyed over your existing HFC infrastructure

BRKSPG-2016

Recommended Reading

Please browse on-site Cisco Store for suitable reading.

Please complete your Session Survey

- We value your feedback - don't forget to complete your online session evaluations after each session. Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Networkers 20th Anniversary t-shirt.
- All surveys can be found on our onsite portal and mobile website: www.ciscoliveeurope.com/connect/mobi/login.ww
- You can also access our mobile site and complete your evaluation from your mobile phone:
  1. Scan the Access Code
     (See http://tinyurl.com/qrmelist for software, alternatively type in the access URL)
  2. Login
  3. Complete and Submit the evaluation


CISCO