Metro Ethernet CCIE Update

Monique Morrow Distinguished Consulting Engineer

Agenda

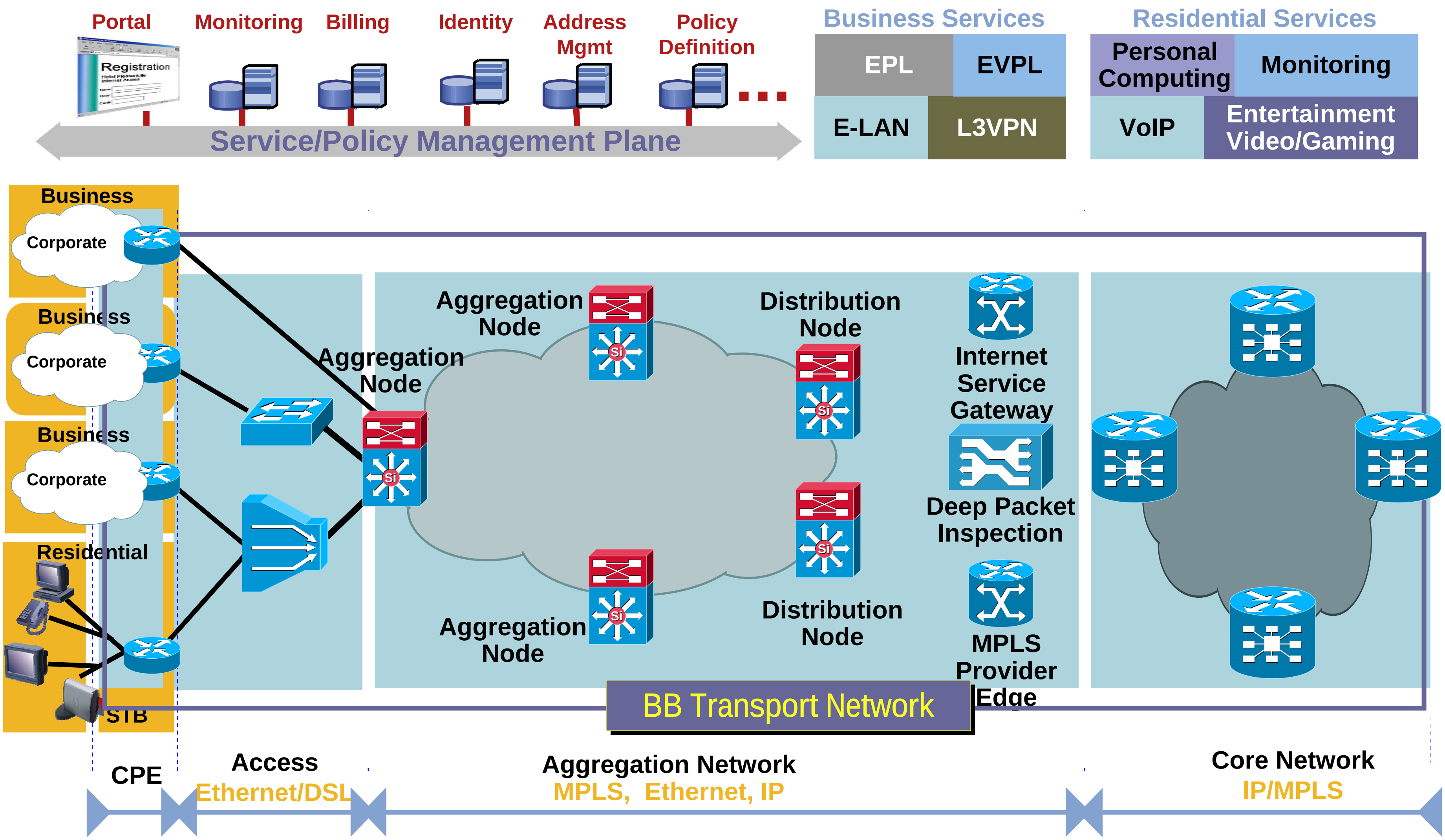
- Carrier-Class Ethernet Network Concepts
- Residential & Business Services Overview
- Broadband Transport Architecture
- Subsystems
  - Service Deployment Models
  - Service Scale & Resiliency
  - Broadcast TV and IP Multicast
  - Quality of Service
  - Security
  - Network Management
- Summary

Carrier-Class Ethernet Network Concepts

Carrier-Class Ethernet Network Concepts

- Converged network delivering residential and business service offerings
- 10GE aggregation to address massive scale requirements
- Flexible service insertion points
- Sub-second convergence for real-time application
- QoS architecture for Application & Transport SLAs
- Secured Transport, Services, & Users

Carrier-Class Ethernet Architecture



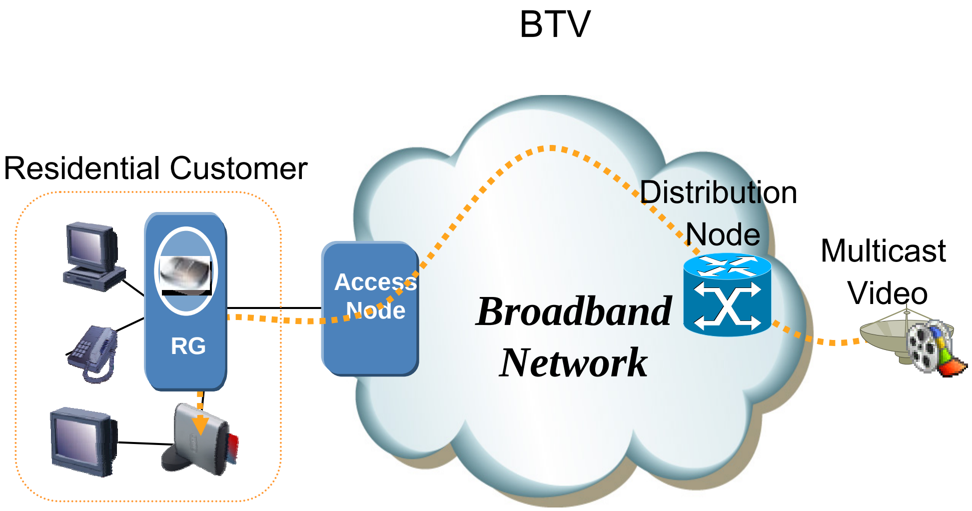
Broadband Services Overview

Broadband Service Offering

- Residential services
  - Video—Broadcast TV
  - Video—Video on demand
  - Voice—Voice over IP
  - Data—High-Speed Internet
- Business services
  - E-LINE
  - E-LAN

Broadcast Television

- Service considerations
  - User selects a broadcast channel among multiple channels (<200)
  - Service controlled by video middleware
- Application requirements
  - Real-time traffic where majority of traffic is downstream
  - Efficient method of distributing high bandwidth traffic:
  - MPEG2: 3.75M to 14M
  - Channel change time < 1500 ms
  - End-to-end delay requirement: < 100–500 ms
  - Network loss < 1E-07
  - Network jitter < 100–200ms
  - < 1s recovery in failure scenario
  - Quality Of Experience is KEY



Video on Demand (VoD)

- Service considerations

  User selects on video on demand (non-scheduled videos)

  Service controlled by video middleware

- Application requirements

  Real-time traffic where majority of traffic is downstream

  Method of call admission control for high bandwidth traffic (3.75M to 14M video streams)

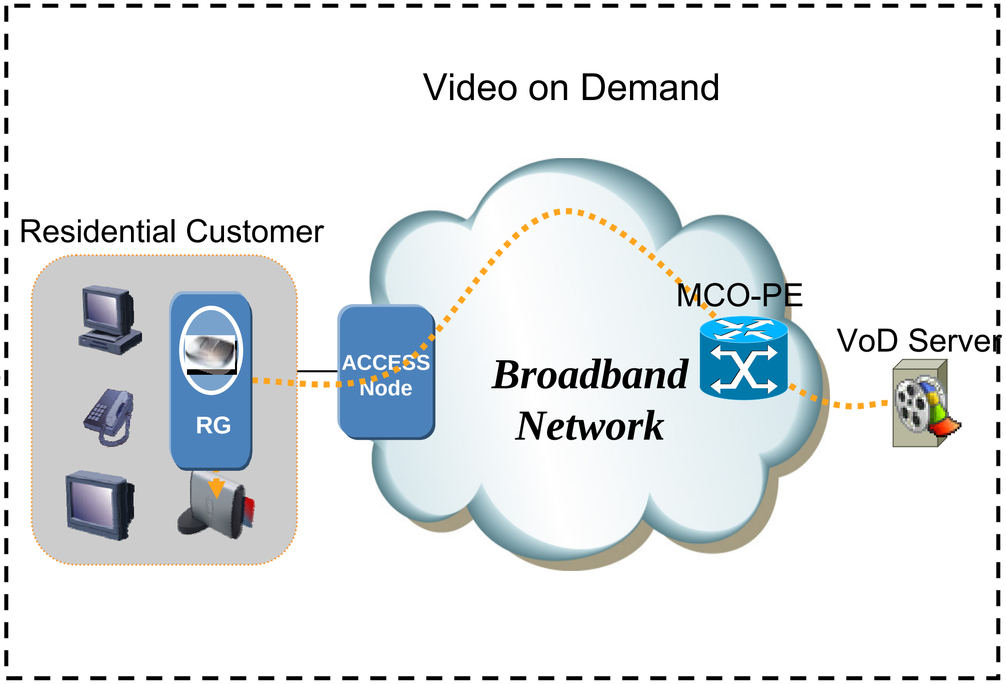
  End-to-end delay requirement: < 100–500 ms

  Network loss < 1E-07

  Network jitter < 100–200ms

  < 1s recovery in failure scenario

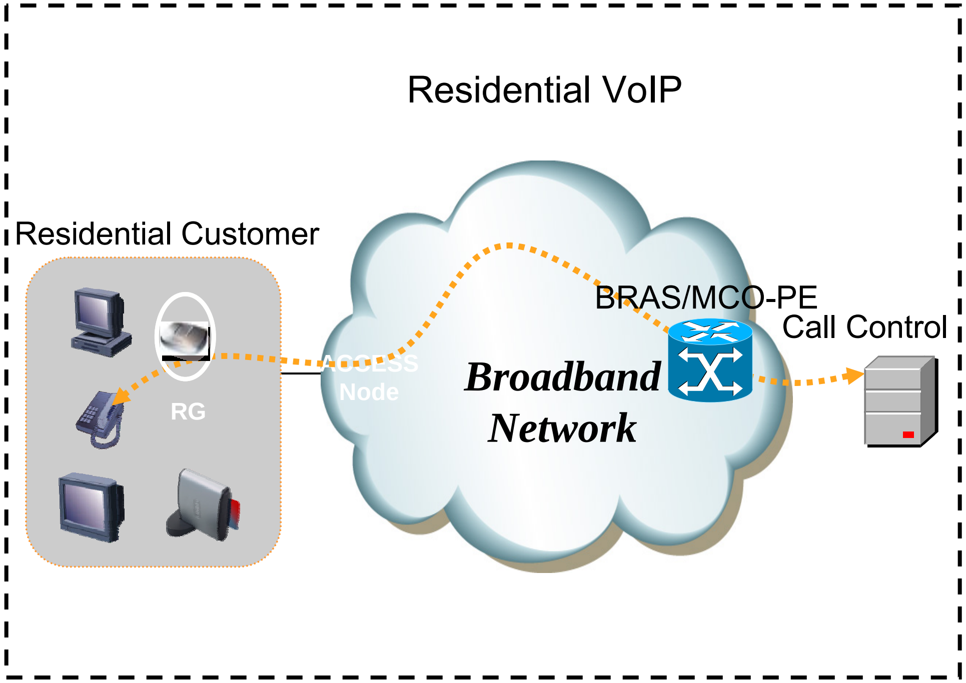
  Quality Of Experience is KEY



Residential Services

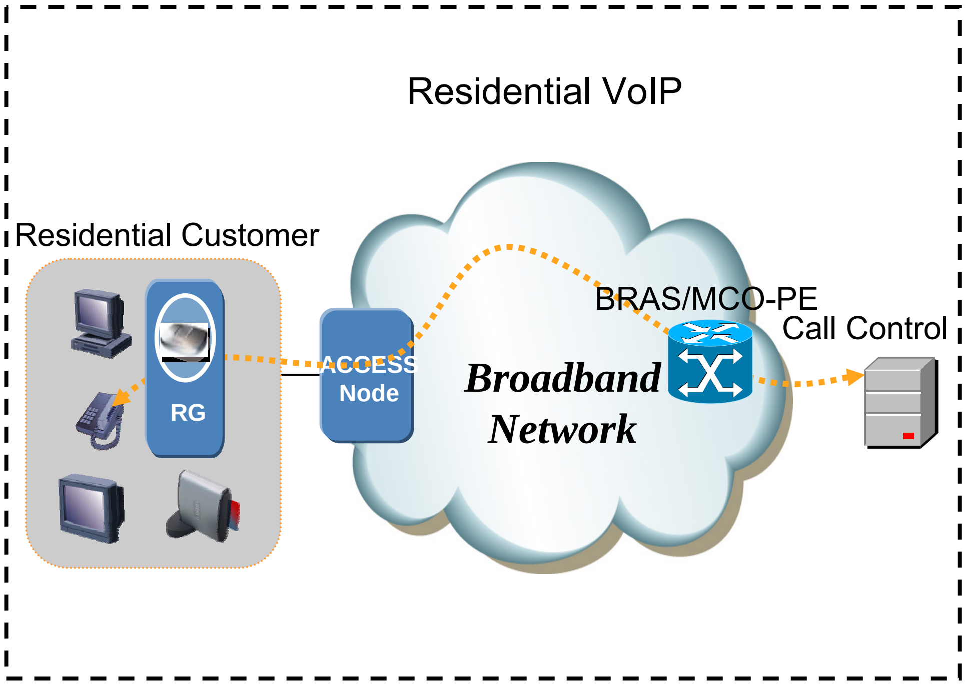
Voice over IP (VoIP)

- Service considerations
  - User makes IP, non-circuit based voice calls as alternative to traditional PSTN
  - On-net VoIP calling
  - Off-net calling (hopoff to PSTN)
- Application requirements
  - Real-time bi-directional traffic
  - End-to-end delay requirements: 150ms
  - Network loss < 1E-02
  - Network jitter < 20–30ms
  - < 1s recovery in failure scenario
  - Quality Of Experience is KEY



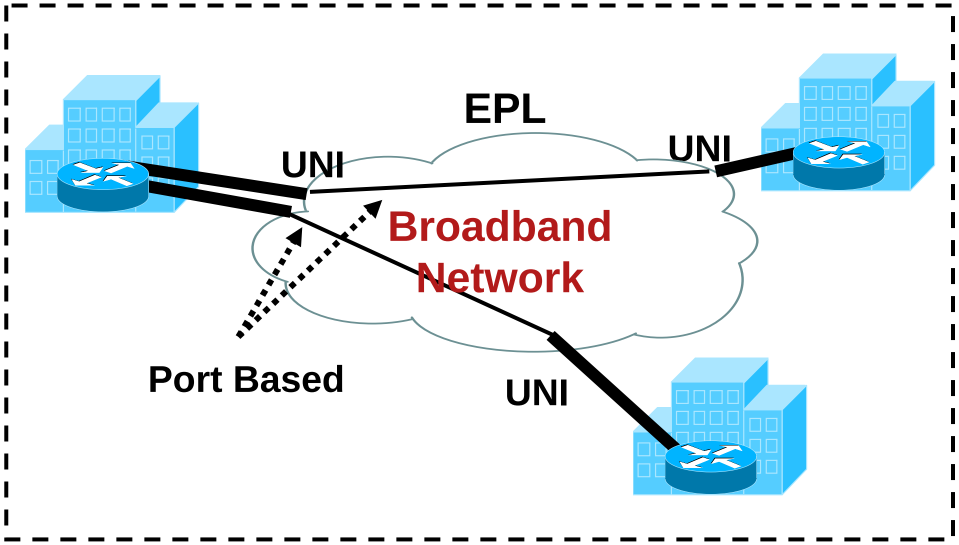
Internet Access Data

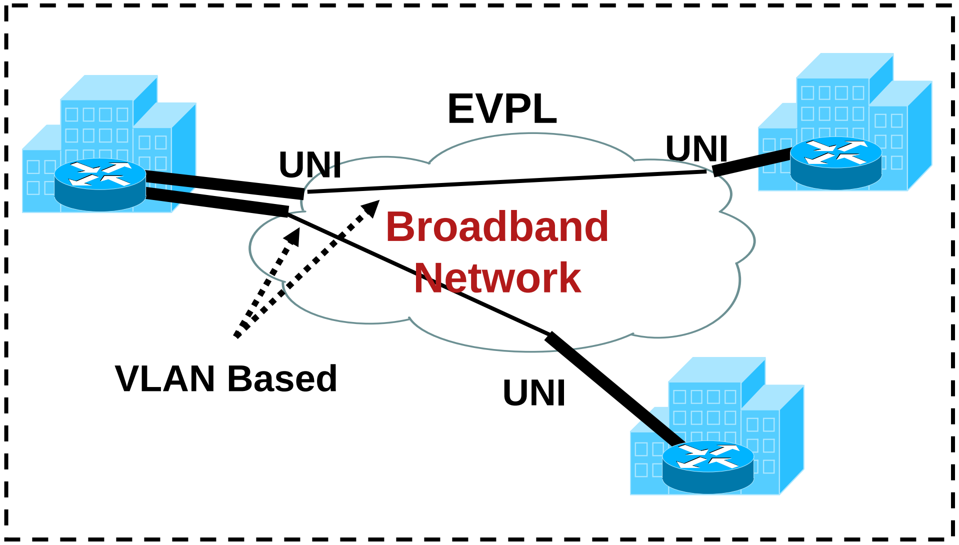
- Service considerations
  - Best effort data service (Internet, e-mail, chat rooms, gaming)
  - Bridged or PW (EoMPLS)
  - Provisioned via IP or PPPoE Internet access
- Application requirements
  - Non-real-time bi-directional traffic
  - Best effort



E-LINE

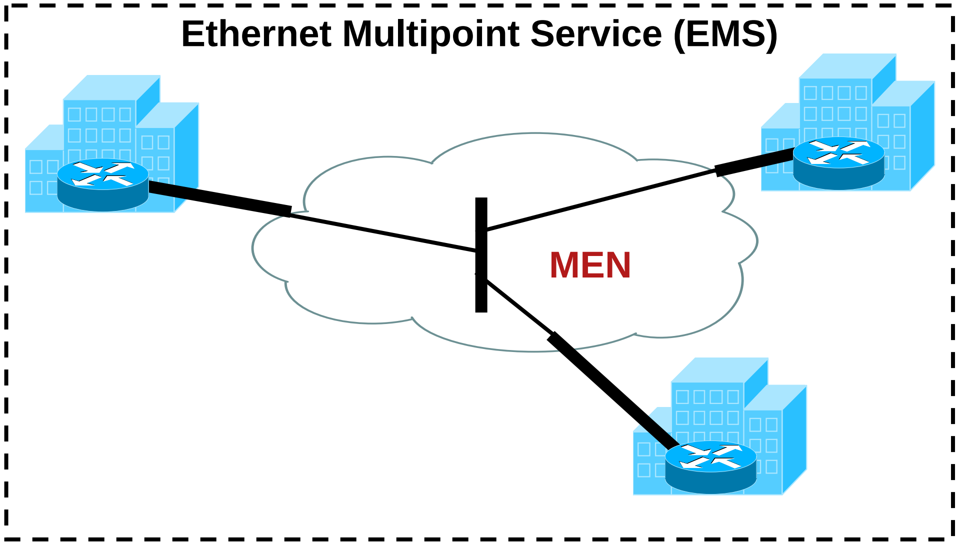
- Service considerations
  - Port/VLAN based point-to-point business service
  - Service multiplexing at UNI (VLAN)
  - High availability-protected
  - Fully transparent offering
- Service requirements
  - Scalability for large sites
  - Real-time traffic and stringent packet loss requirements
  - SLA—CIR/PIR/burst, loss

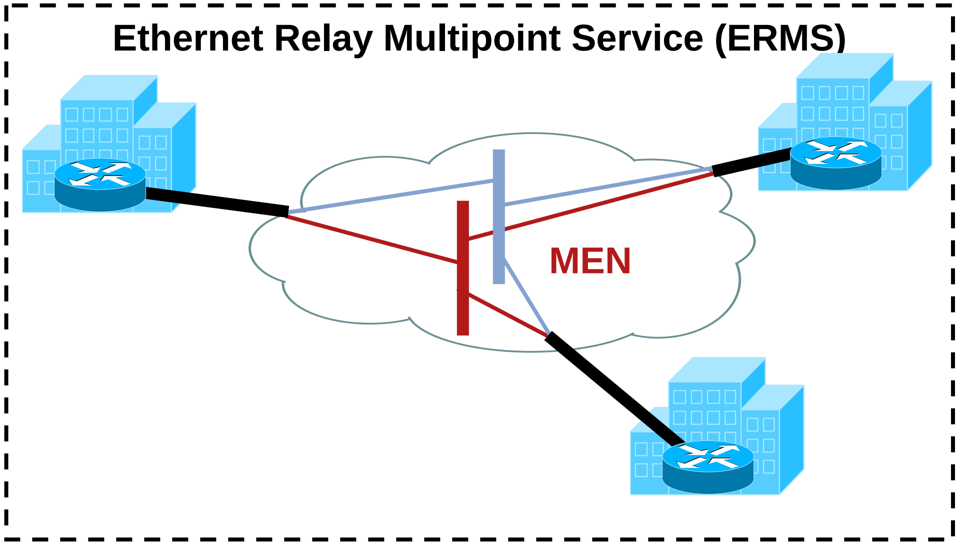




E-LAN

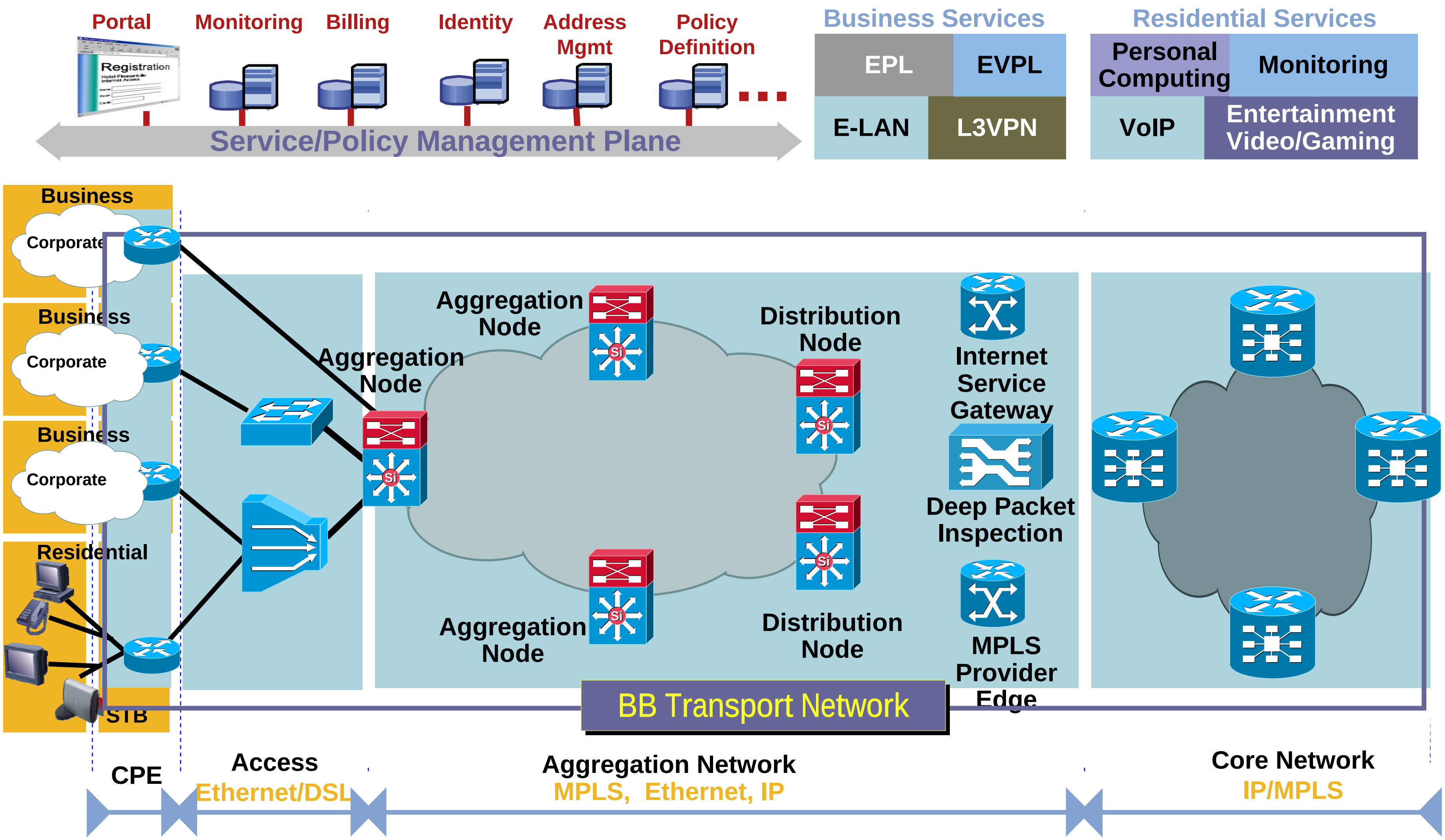
- Service considerations
  - Port/VLAN-based multipoint business service
  - Service multiplexing at UNI (ERMS)
  - High availability-protected
  - Fully transparent offering (EMS)
- Service requirements
  - Small-to-mid size multipoint connectivity
  - Corporate/campus LAN extension
  - Disaster recovery





Broadband Transport Architecture

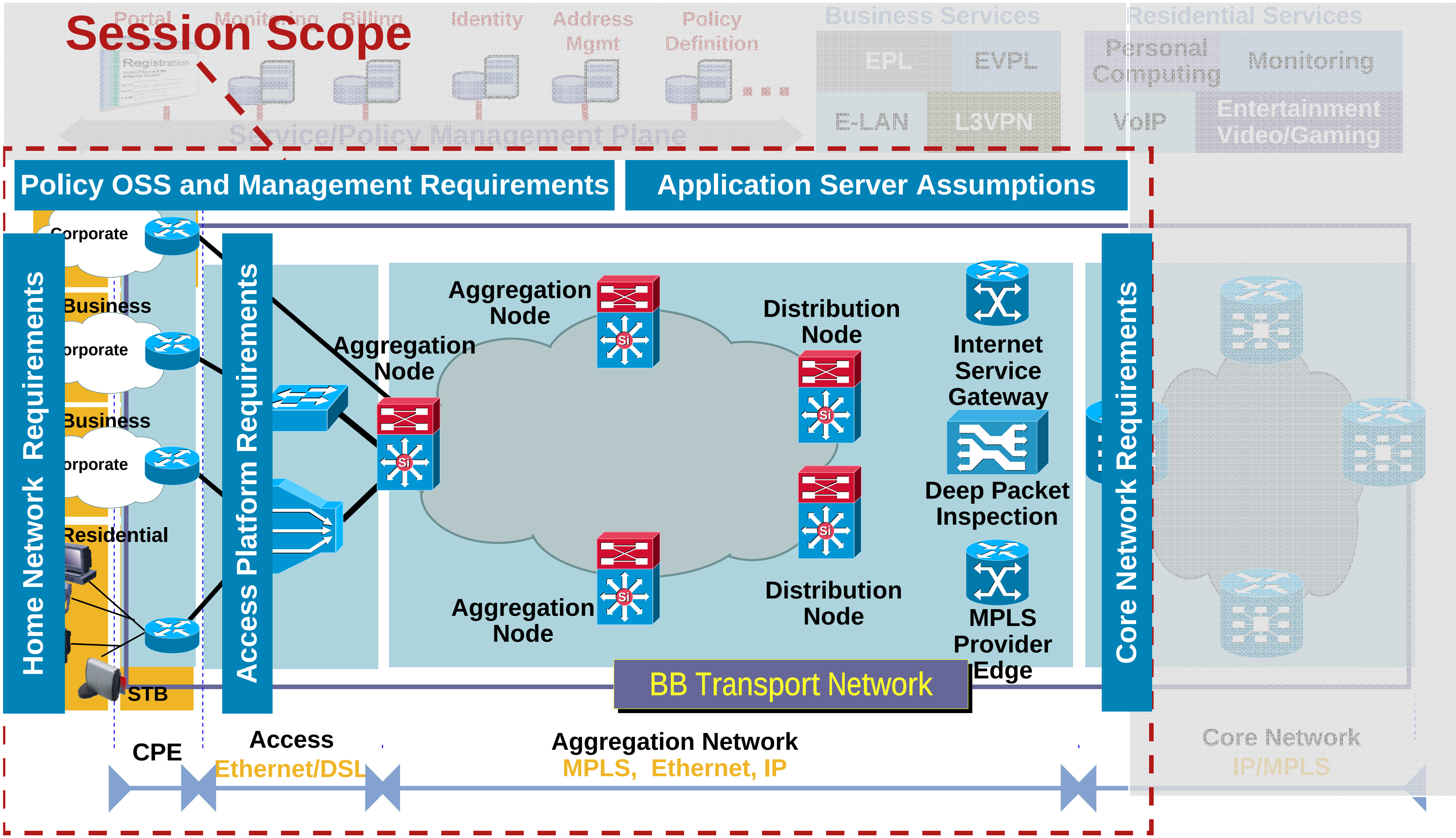
Broadband System Architecture



Next Generation Broadband Architecture Concept

- The service edge
  - Flexible choices for the service insertion points
  - Optimal balance between operations and network transport efficiency
- The aggregation network
  - Flexible transport choices: Ethernet, MPLS, IP
  - Layer 2 virtualized transport mechanisms provide service isolation
  - Support for point to point and multipoint services with centralized or distributed service edge
- The Ethernet and DSL access network
  - Ethernet UNI mapping: multiplexed or not-multiplexed
  - DSLAM (ADSL/2+, VDSL) UNI mapping: aligned with WT-101v8, multiplexing based on VCs or VLANs, routed (bridged) CPEs, ATM COS or IEEE 802.1p for service COS classification
  - DSLAM subscriber connectivity models: 1:1 for business, N:1 for residential (subscribers/VLAN)

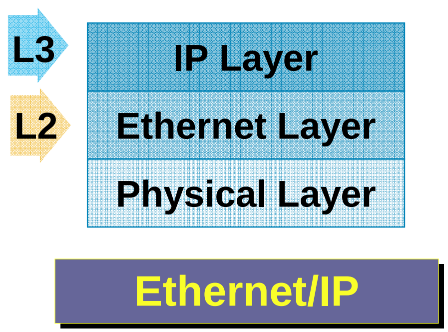
Broadband Transport Architecture

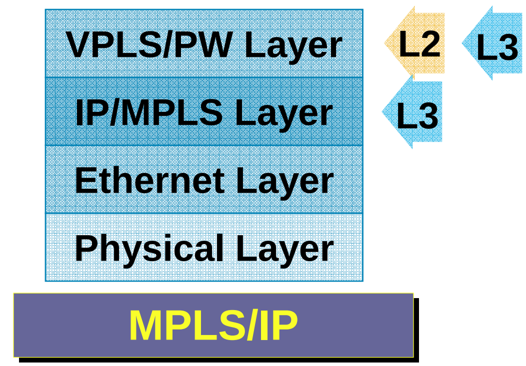


Solving Carrier Aggregation Requirements
Two Approaches/Models

L2 L2 Service: Business L2VPN

L3 L3 Service : L3VPN, High Speed Internet (HSI), IPTV, Voice over IP (VoIP)…





Virtualization happens on the Ethernet layer	Virtualization happens on MPLS overlay layers
L2 Services inserted into Ethernet Layer	L2 Services inserted on VPLS/PW Layer
L3 Services inserted into IP Layer	L3 Services inserted into IP Layer or VPLS/PW Layer

Service Deployment Models

Defining the L3 Service Edge

- L3 edge point—why is this significant?

  Access (closest to the subscriber)

  Aggregation (closer to the sub)

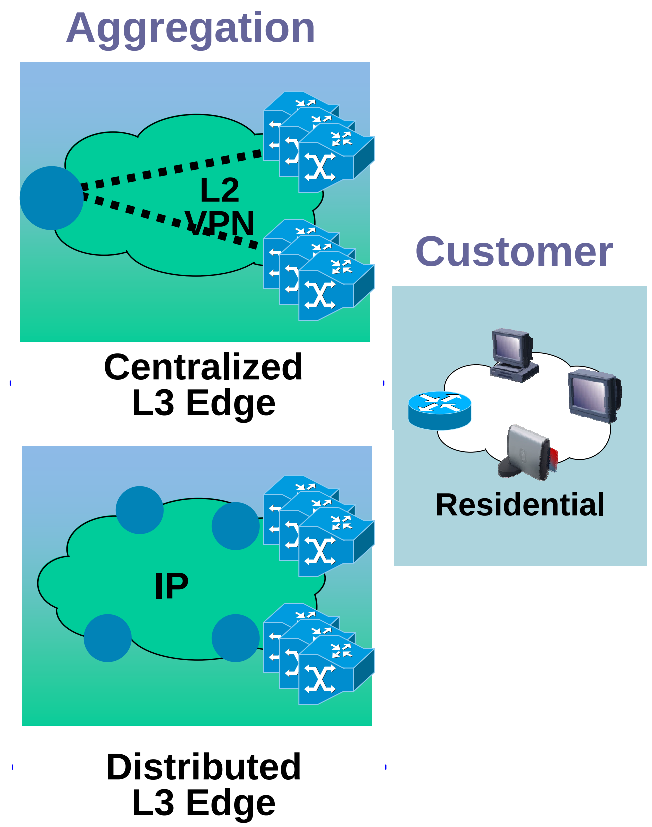
  Distribution (closer to the core)

- This influences possible architectures

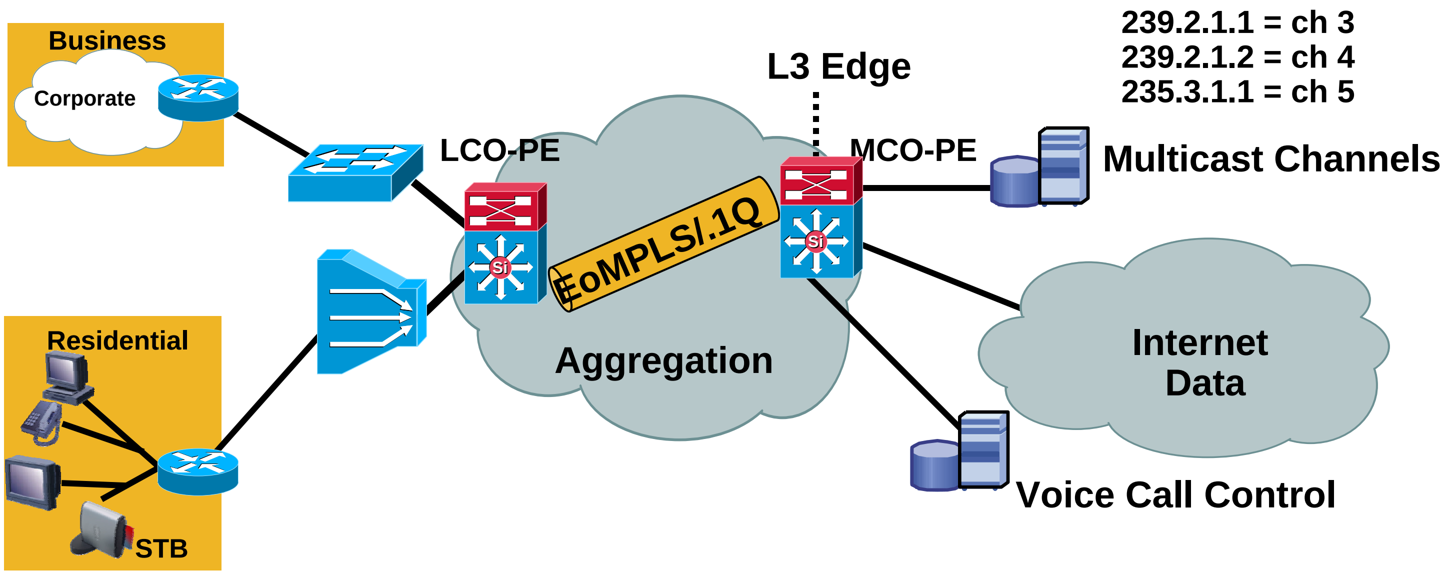
  Centralized vs. distributed L3 edge points

  Centralized = service L3 edge at a single "point"

  Distributed = service L3 edge at multiple "points"



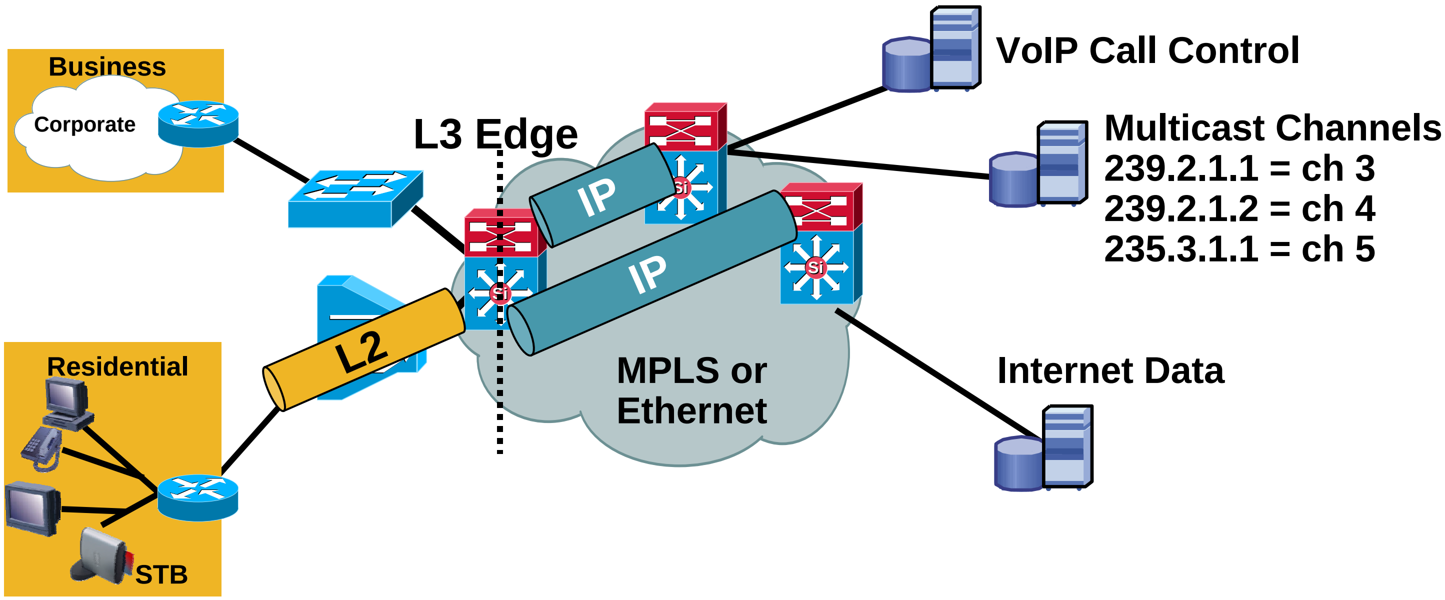
Centralized L3 Service Edge



Layer 3 Edge Point Reside at Central Location in Network

- Ethernet/IP
  - L2 service VLANs used from subscriber to MCO-PE
- MPLS/IP
  - Pseudowire used from LCO-PE to MCO-PE for L2 tunneling
  - For example, Internet access insertion point: driven by the existing service model, operational structure, traffic patterns

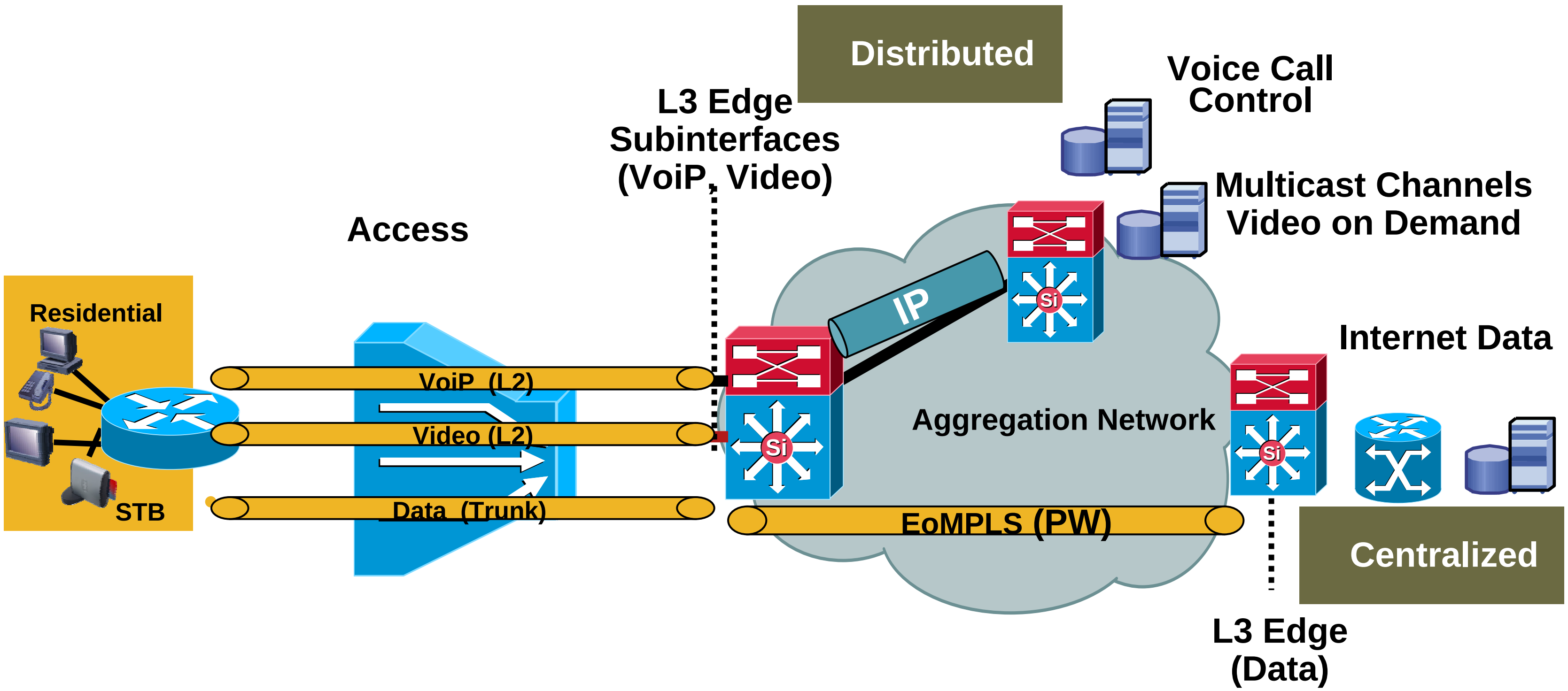
Distributed L3 Service Edge



L3 Edges Are Distributed at Different Points in the Network

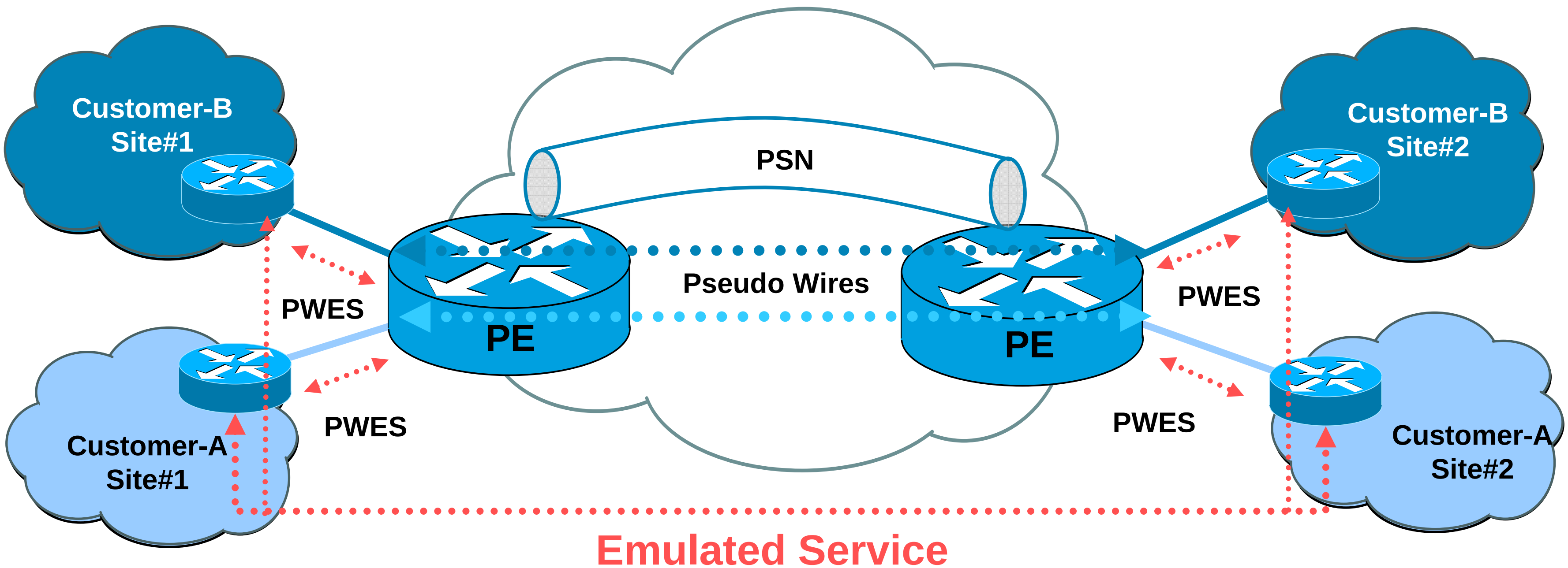
- For example, VoIP, VOD IP/TV®, broadcast IP/TV insertion point: driven by the minimal network operational needs, the simplicity and efficiency of the IP multicast transport

L3 Service Edge—Residential Hybrid Approach



- Distributed L3 edge for VoIP/IP/TV Broadcast/IP/TV VOD
  - Minimal network operational needs
    - Allows multicast channels to be distributed at closest edge to subscribers
- Centralized L3 edge for data
  - Driven by the existing service model, operational structure, traffic patterns

EoMPLS (VPWS) Reference Model

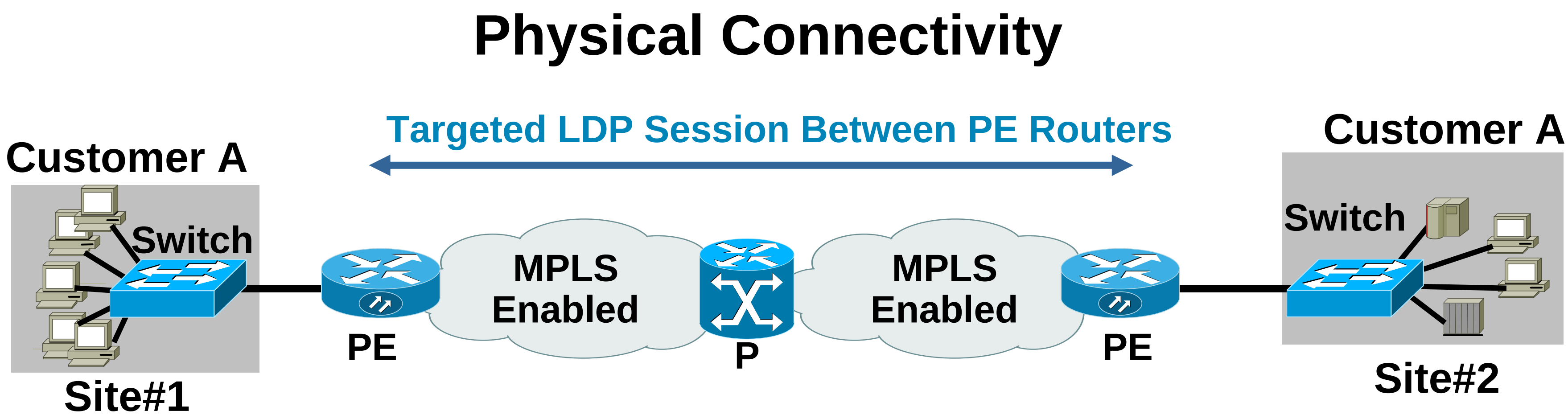


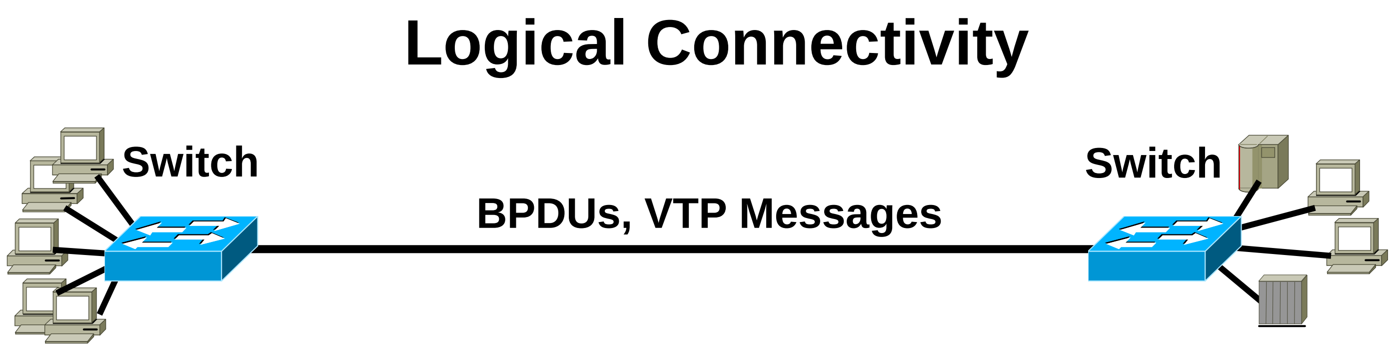
A pseudo-wire (PW) is a connection between two provider edge (PE) devices which connects two pseudo-wire end-services (PWESs) of the same type

Service Types: Ethernet, 802.1Q, ATM VC or VP, HDLC, PPP, Frame Relay VC

Any Transport over MPLS (AToM) is Cisco's implementation of VPWS for MPLS networks

EoMPLS Reference Model





Port-Based EoMPLS Configuration

UPE-1
interface loopback 0
ip address 10.10.10.10/32

mpls label protocol ldp
mpls ldp router-id loopback0

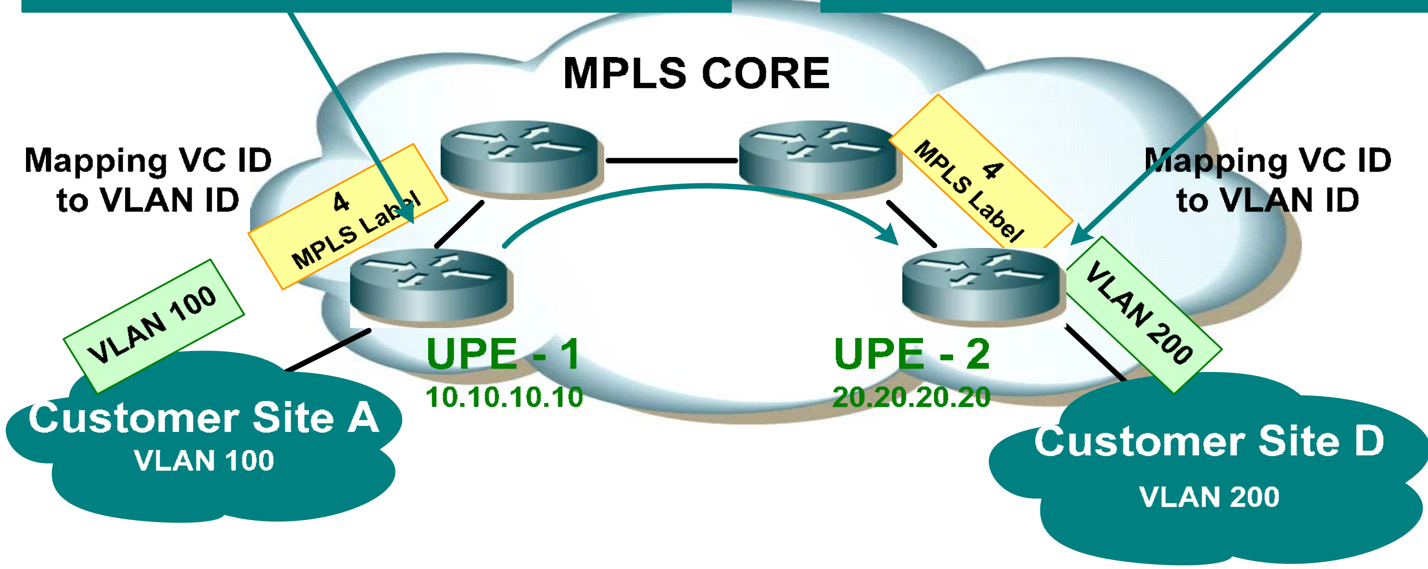
interface gigabitethernet 1/1.100
xconnect 20.20.20.20 100 encapsulation mpls

VC ID MUST MATCH & UNIQUE BETWEEN UPEs

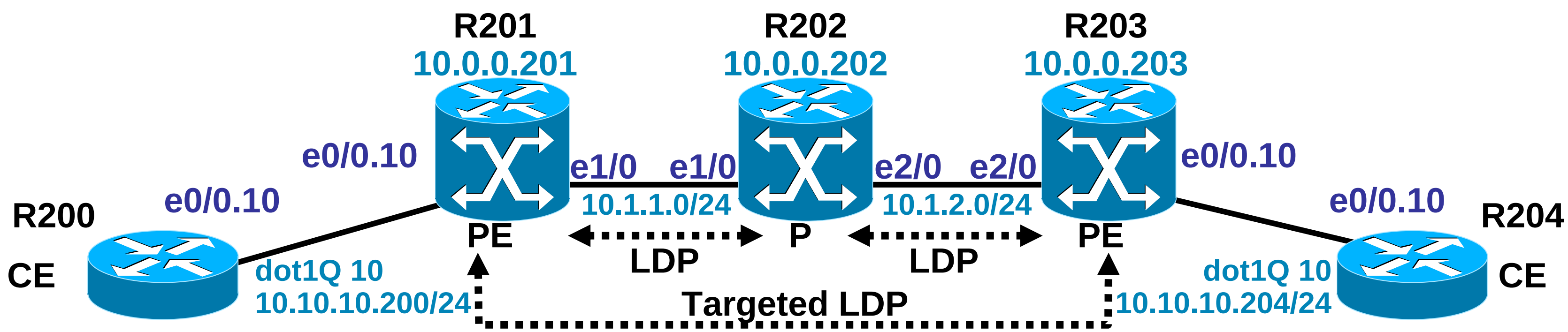
UPE-2
interface loopback 0
ip address 20.20.20.20/32

mpls label protocol ldp
mpls ldp router-id loopback0

interface gigabitethernet 2/1.200
xconnect 10.10.10.10 100 encapsulation mpls



Port-Based EoMPLS Configuration

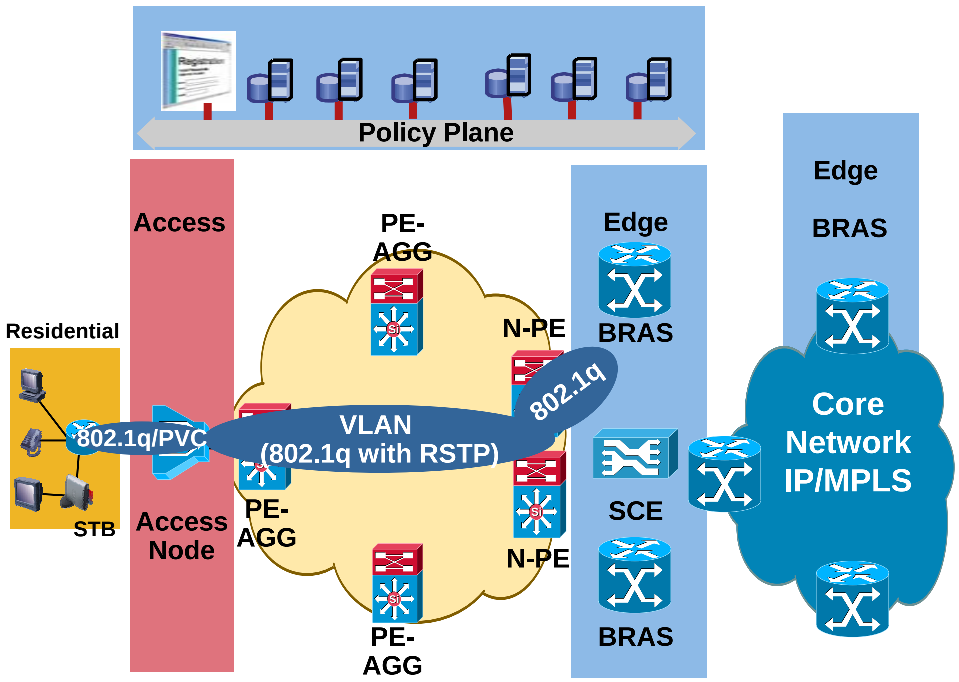



```
hostname R201
!
ip cef
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.201 255.255.255.255
!
interface Ethernet0/0.10
 description *** To R200 ***
 encapsulation dot1Q 10
 no ip directed-broadcast
 no cdp enable
 xconnect 10.0.0.203 10 encapsulation mpls
```

```
hostname R203
!
ip cef
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.203 255.255.255.255
!
pseudowire-class eompls
 encapsulation mpls
!
interface Ethernet0/0.10
 description *** To R204
 encapsulation dot1Q 10
 no ip directed-broadcast
 no cdp enable
 xconnect 10.0.0.201 10 pw-class eompls
```

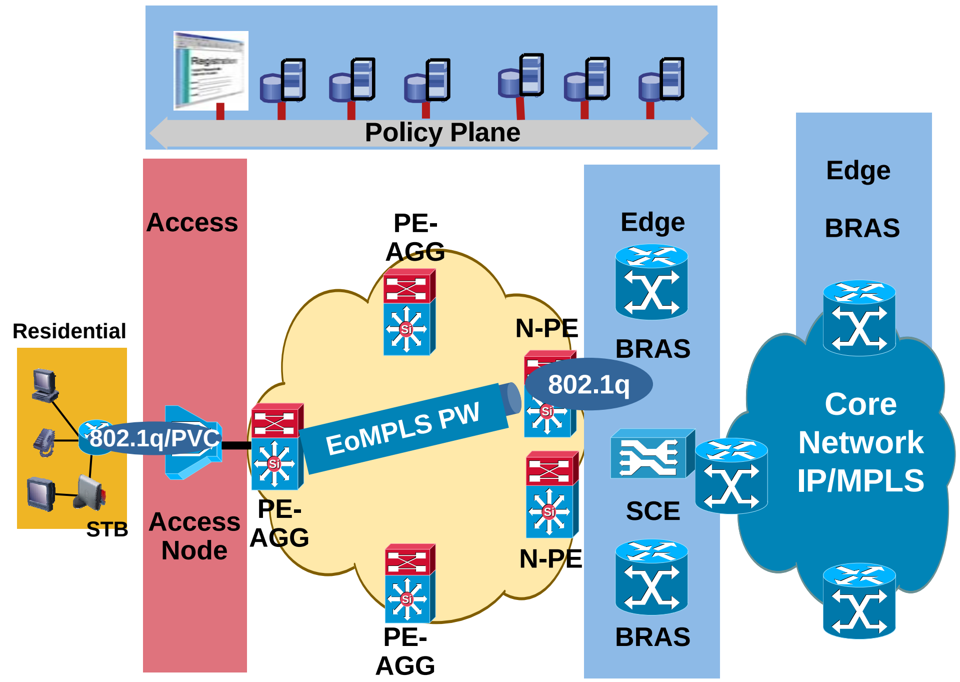
Residential Services

Centralized L3 Edge for Data



Ethernet/IP Aggregation

- PPPoE or IP subscriber sessions carried over a VLAN (802.1q) in the Ethernet/IP aggregation network
- Subscriber line identity provided by the DSL Forum PPPoE line-id VSA or DHCP Op82

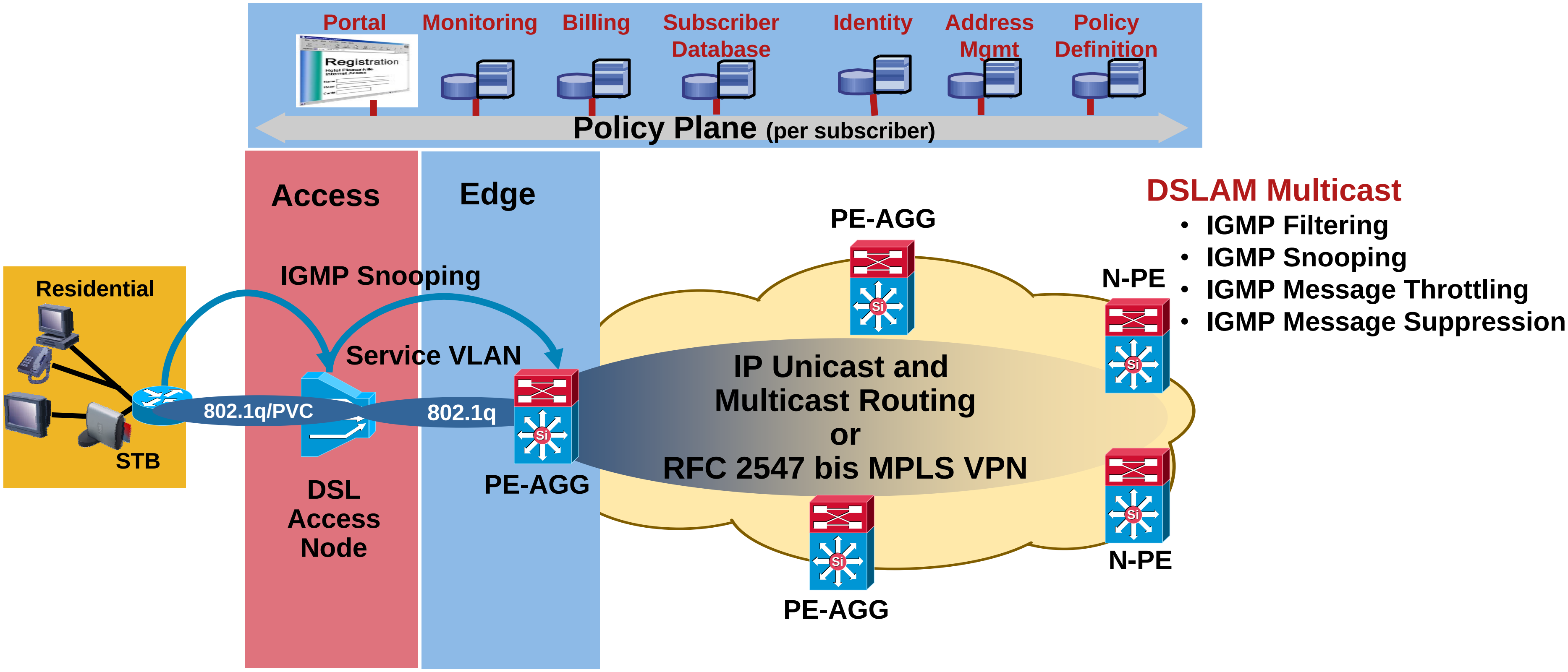


MPLS/IP Aggregation

- PPPoE or IP subscriber sessions carried over a EoMPLS PW in the MPLS/IP aggregation network
- Subscriber line identity provided by the DSL Forum PPPoE line-id VSA or DHCP Op82

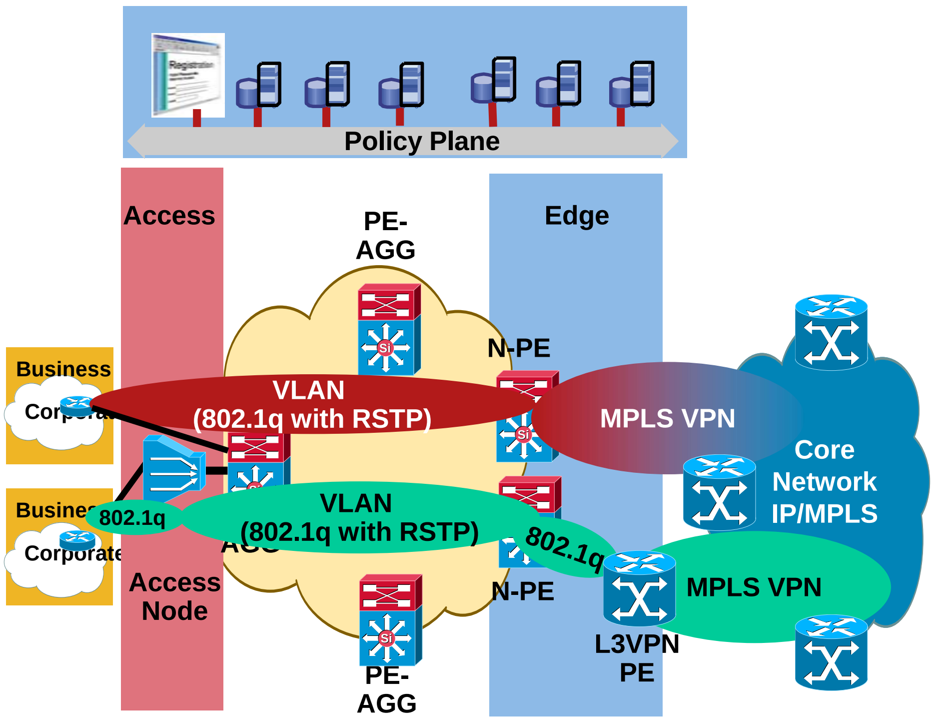
Distributed L3 Edge—VoIP, VoD and B-TV IP Aggregation

Residential Services



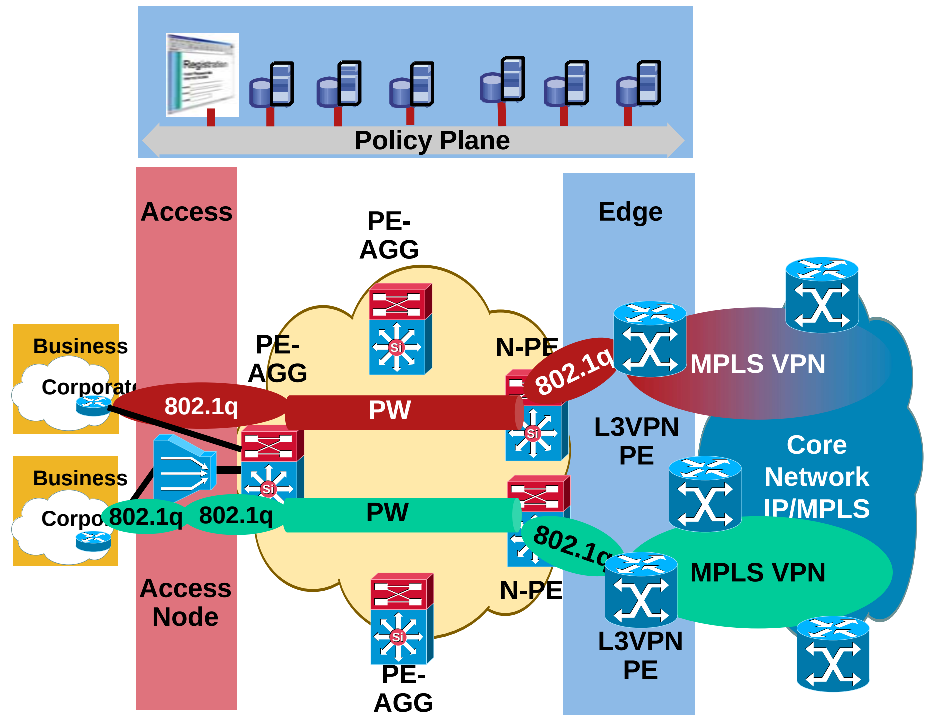
This Service Model Is Same for Both Ethernet/IP and MPLS/IP Aggregation

L3—VPN Service



Ethernet/IP Aggregation

- DSL UNI (PVC or 802.1q) 1:1 VLAN mapping in DLAM
- L3-VPN provided by a dedicated L3 VPN PE or by N-PE

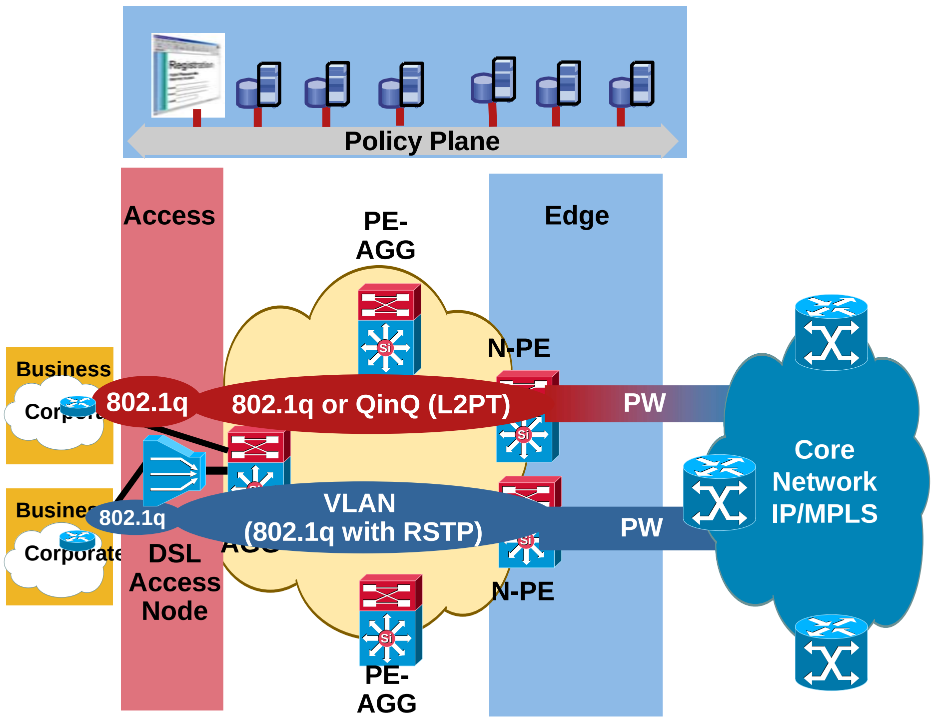


MPLS/IP Aggregation

- DSL UNI (PVC or 802.1q) 1:1 VLAN mapping in DLAM
- L3-VPN provided by a dedicated L3 VPN PE with EoMPLS tunnels from PE-AGG

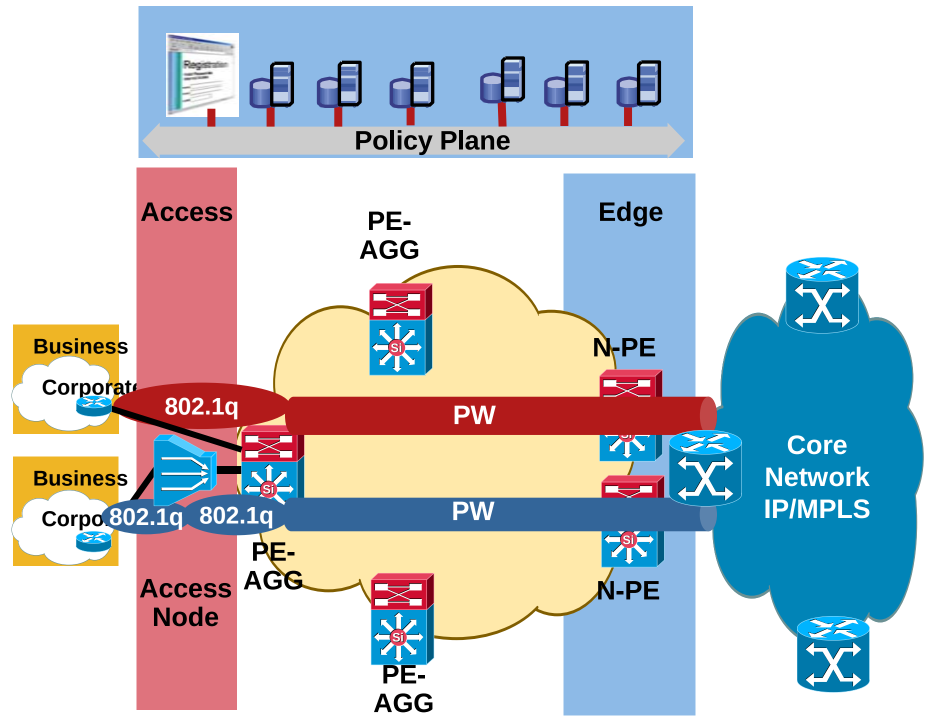
E-LINE Service (EPL and EVPL)

Business Services



Ethernet/IP Aggregation

- DSL UNI (PVC or 802.1q) 1:1 VLAN mapping in DLAM
- Ethernet VLANs in the metro Ethernet aggregation network EoMPLS pseudowires from the N-PE

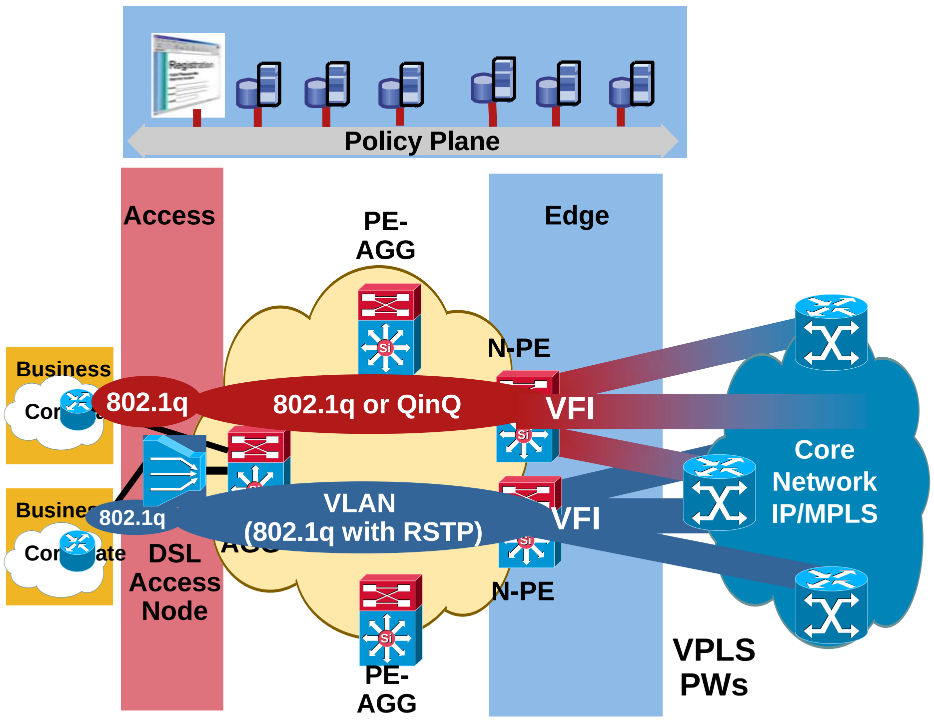


MPLS/IP Aggregation

- DSL UNI (PVC or 802.1q) 1:1 VLAN mapping in DLAM
- EoMPLS PW backhaul from PE-AGG/U-PE for ERS services for the DSL UNI and ERS/EWS for Ethernet UNI

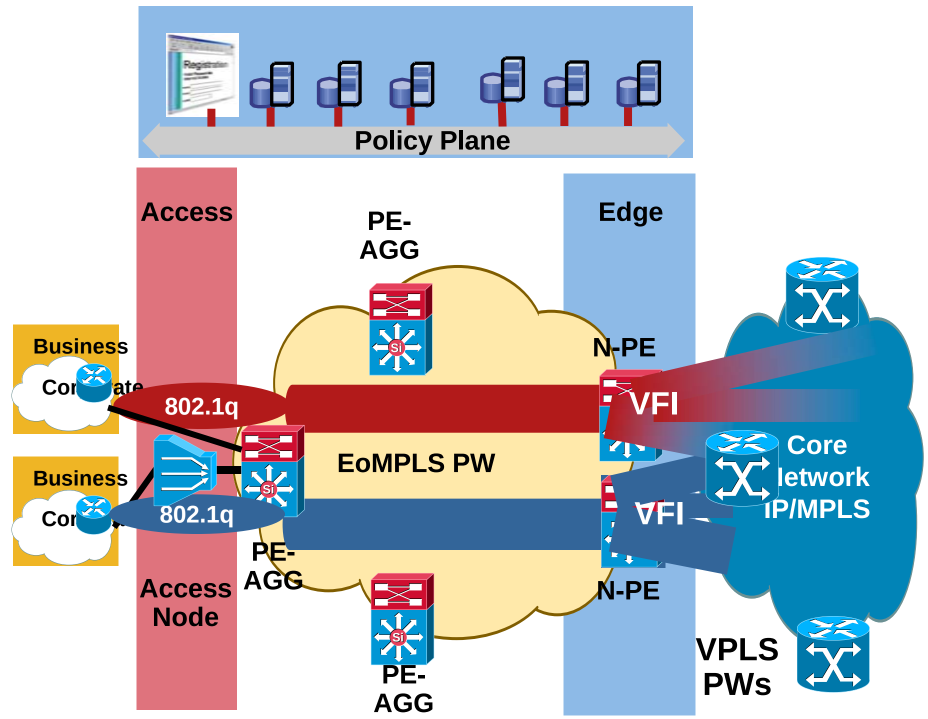
Business Services

E-LAN Services (H-VPLS)



Ethernet/IP Aggregation

- DSL UNI (PVC or 802.1q) 1:1 VLAN mapping in DLAM
- Ethernet VLANs in the metro Ethernet aggregation network VPLS from N-PE

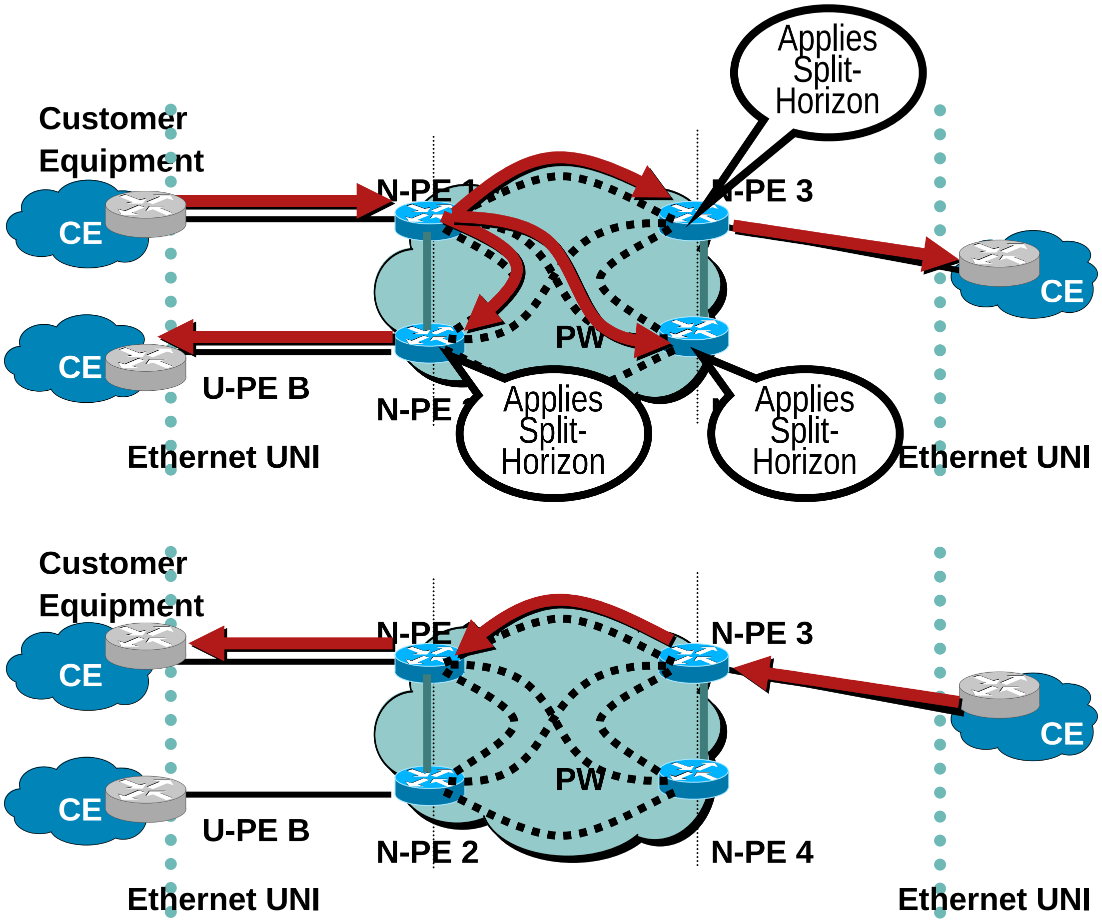


MPLS/IP Aggregation

- DSL UNI (PVC or 802.1q) 1:1 VLAN mapping in DLAM
- EoMPLS PW backhaul from PE-AGG/U-PE for ERS services for the DSL UNI and ERS/EWS for Ethernet UNI

How VPLS works...
(Almost) emulating a Bridge

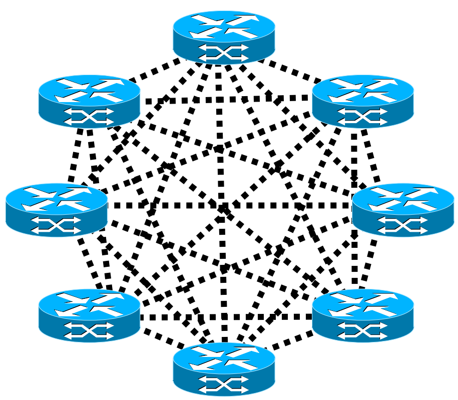
Business Services



- Flooding (Broadcast, Multicast, Unknown Unicast)
- Dynamic learning of MAC addresses on PHY and VCs
- Forwarding
  - Physical Port
  - Virtual Circuit
- VPLS uses Split-Horizon and Full-Mesh of PWs for loop-avoidance in core
  - SP does not run STP in the core

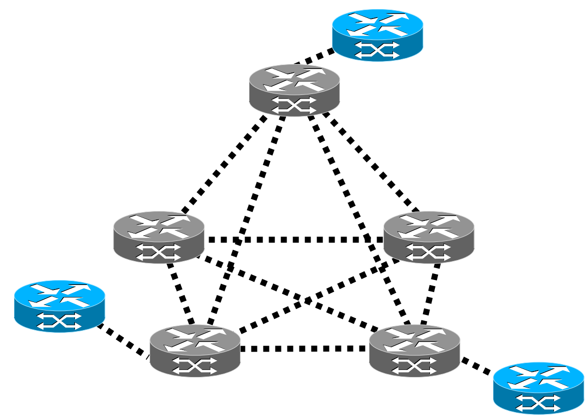
Hierarchical-VPLS: Why?

VPLS



- Potential signaling overhead
- Full PW mesh from the Edge
- Packet replication done at the Edge
- Node Discovery and Provisioning extends end-to-end

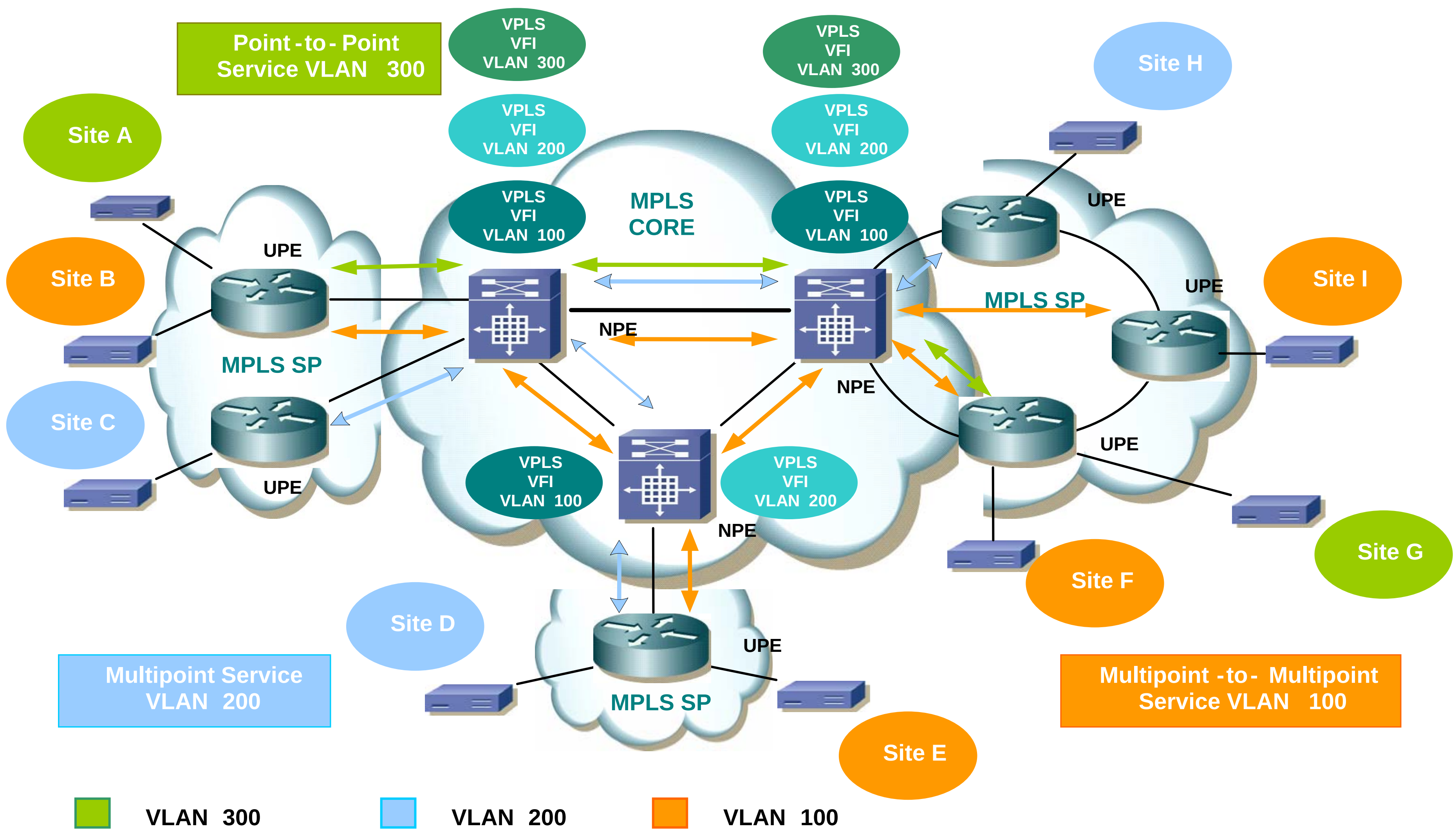
H-VPLS



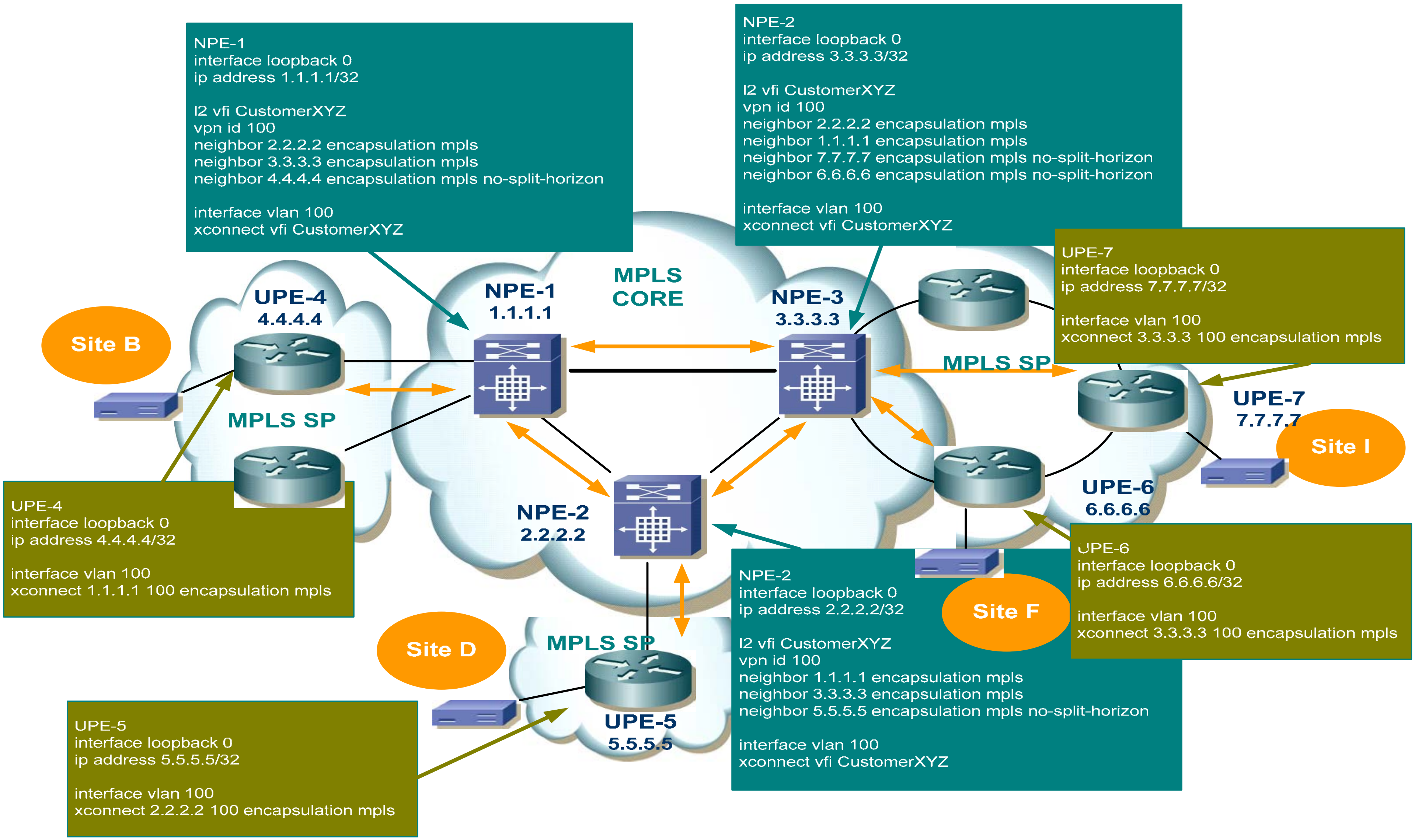
- Minimizes signaling overhead
- Full PW mesh among Core devices only
- Packet replication done the Core only
- Partitions Node Discovery process
- H-VPLS Flavors: H-VPLS with Ethernet Access & H-VPLS with MPLS Access

Business Services

H-VPLS w/ MPLS Access



H-VPLS w/ MPLS Access



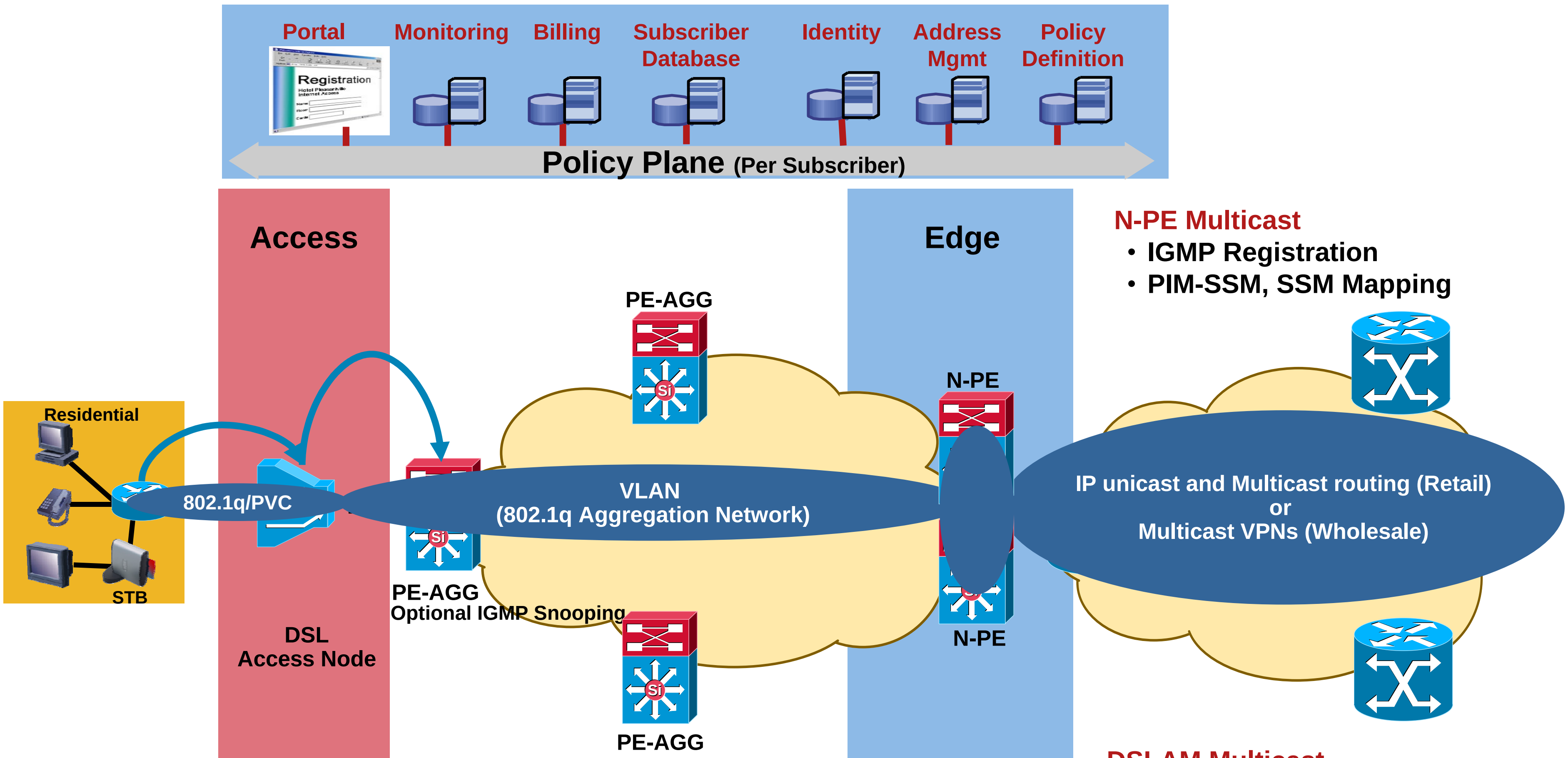
Broadcast TV and IP Multicast

B-TV Transport Options and Characteristics

	Bandwidth Efficiency	Fast Convergence	Service Separation	Extra Services
L3	**IP** **PIM SSM,** **SSM mapping**	**MPLS TE** **Fast IGP (BFD)** **Fast Multicast Convergence**	**Multi-VRF** **MPLS VPN** **Multicast VPN**	**Security** **Monitoring** **Load Balancing** **Anycast Sources**
L2	**802.1q** **IGMP Snooping**	**802.1w RSTP**	**802.1q/ 802.1ad** **VLAN**	
L2	**H-VPLS** **IGMP Snooping**	**TE-FRR (Only Link)**	**L2-VPN**	

- Transport options in the aggregation network?
  - L2—Ethernet switching
  - L2 emulated—H-VPLS
  - L3—IP multicast
- What are the main benefits of IP multicast in the aggregation network?

B-TV Delivery—L2 Aggregation



N-PE Multicast

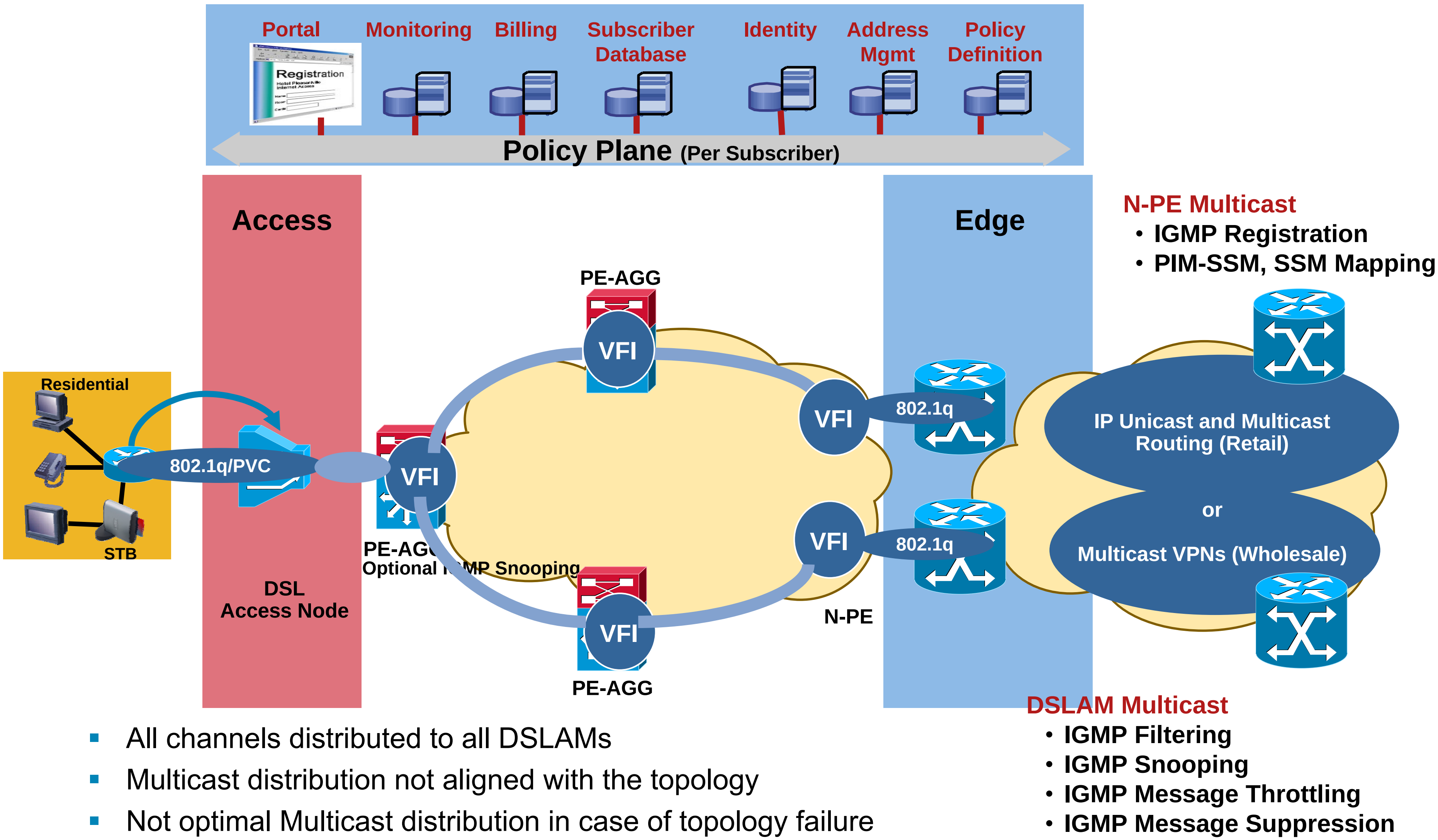
- IGMP Registration
- PIM-SSM, SSM Mapping

DSLAM Multicast

- IGMP Filtering
- IGMP Snooping
- IGMP Message Throttling
- IGMP Message Suppression

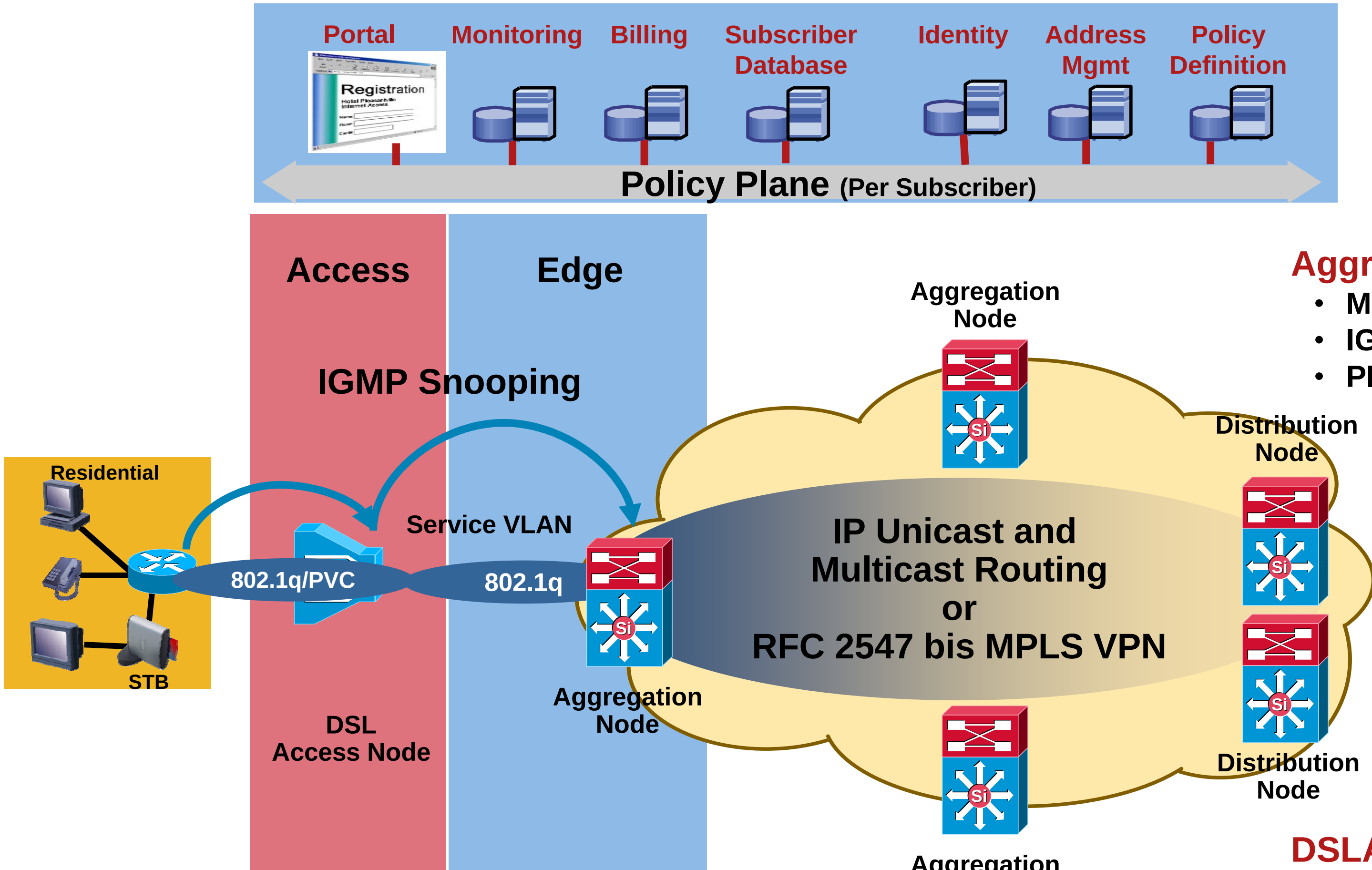
- PE-AGG IGMP snooping to optimize the multicast distribution
- Optimal multicast with any topology and in case of topology failure
- Resiliency can be provided at both L2 and L3 based on N-PE capabilities

B-TV Delivery—L2 Emulated Aggregation (H-VPLS)



- All channels distributed to all DSLAMs
- Multicast distribution not aligned with the topology
- Not optimal Multicast distribution in case of topology failure

B-TV Delivery—L3 Aggregation



Aggregation Node Multicast
- Multicast VPN
- IGMP registration
- PIM-SSM, SSM Mapping

IP Unicast Routing

DSLAM Multicast
- IGMP Filtering
- IGMP Snooping
- IGMP Message Throttling
- IGMP Message Suppression

SSM-MAP

Step 1 - Enable IP MC

```
Router# configure terminal

Router(config)# ip multicast-routing
```

Step 2 – Enable SSM-MAP

```
Router(config)# ip igmp ssm-map enable
Router(config)# no ip igmp ssm-map query dns
```

Step 3 – Create Access list

```
Router(config)#  access-list 12 permit 232.1.1.0 0.0.0.255
```

Step 4 – statically map MC source

```
Router(config)#  ip igmp ssm-map static 12 27.1.1.2
```

Step 5 – Enable PIM-SM

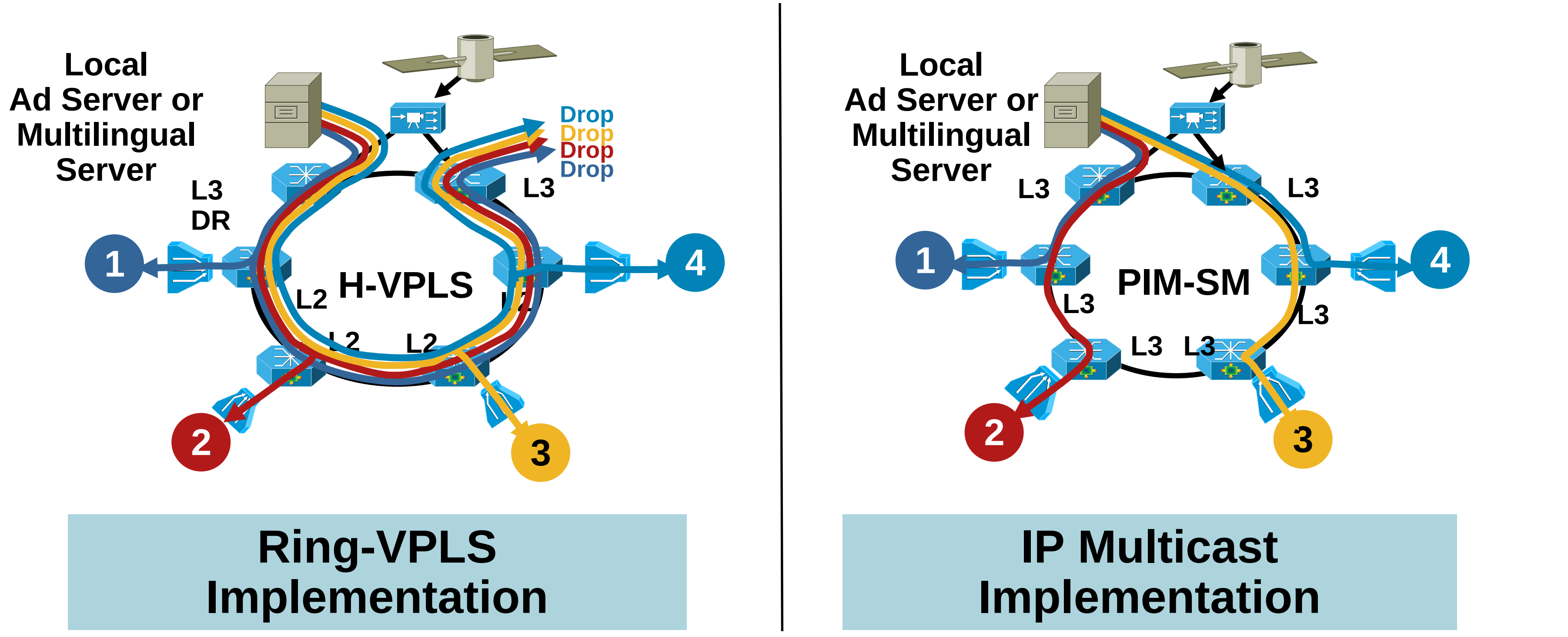
```
Router(config)# interface TenGigabitEthernet2/1

Router (config-if)# ip pim sparse-mode
```

Benefits of Distributed L3 Edge for Multicast

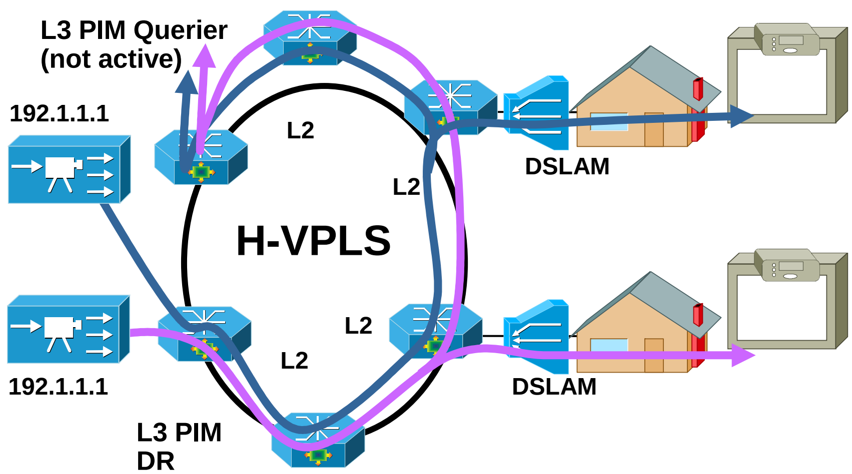
Efficient Multicast Distribution

- L3 enables shortest path to source
- L2 needs IGMP snoop, Else replicates every m'cast packet around ring
- IWasted bandwidth, less room for HSI and other services
- Extra processing stress on L2 forwarding engines



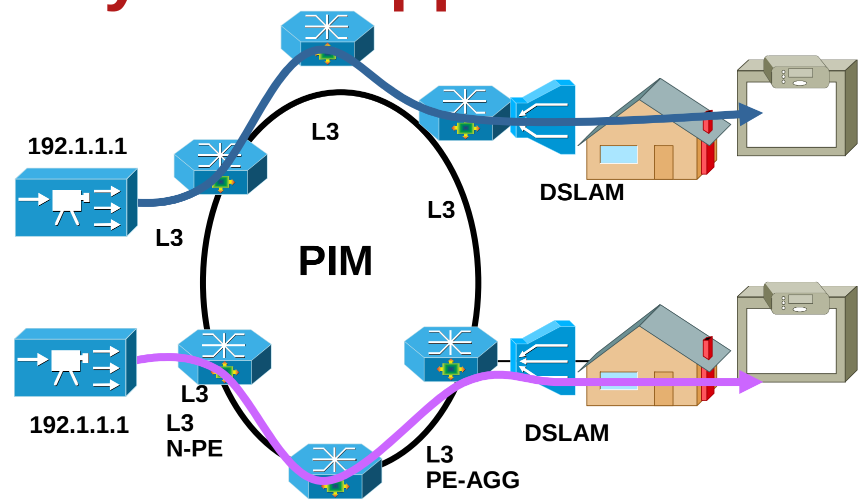
Benefits of Distributed L3 Edge for Multicast

Anycast Support



Ring-VPLS Implementation

- No anycast support in aggregation network
- No shortest-path election to the source because mcast traffic only enter through the designated router
- All of above results in inefficient distribution multicast pkts

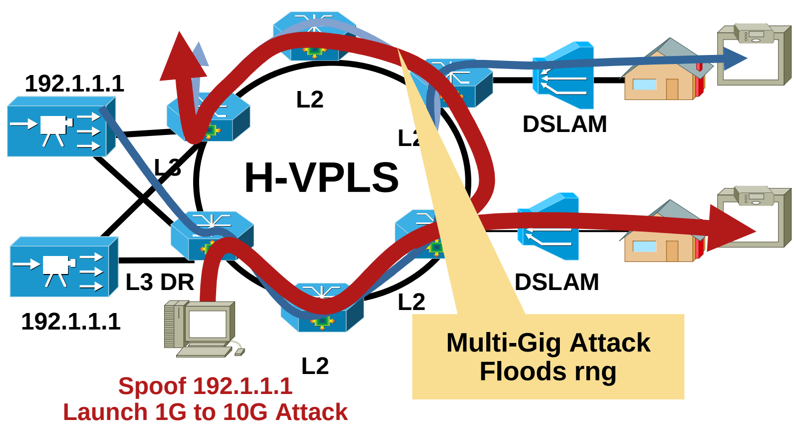


IP Multicast Implementation

- PIM-SSM inherently supports anycast
- Shortest path election through IGP
- Load sharing between multicast source
- Instantiate multiple replication tree for same multicast destination

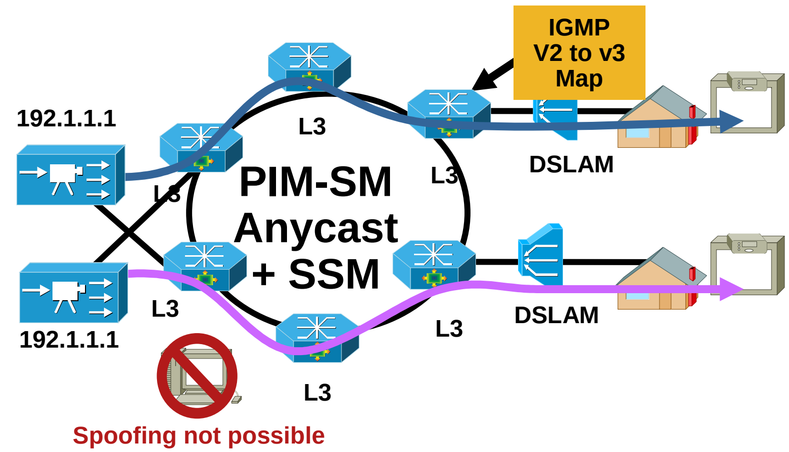
Benefits of Distributed L3 Edge for Multicast:

Source Specific Multicast (SSM) Prevents Security Threats



Ring-VPLS Implementation

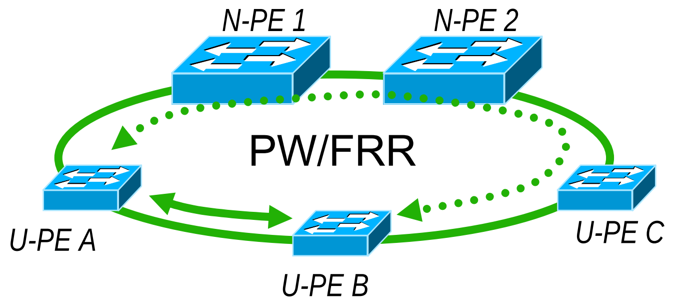
- SSM-Map not supported at the PE-AGG
- Attack launched from spoofed source address can create outage on ring
- H-VPLS aggregation network is vulnerable to spoofed sources



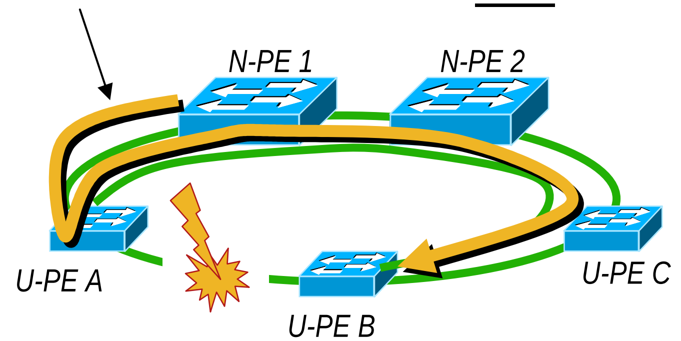
IP Multicast Implementation

- SSM enabled at the PE-AGG
- SSM-Map enforces source aware mapping
- Minimizes ability to spoof service
- Anycast works with SSM

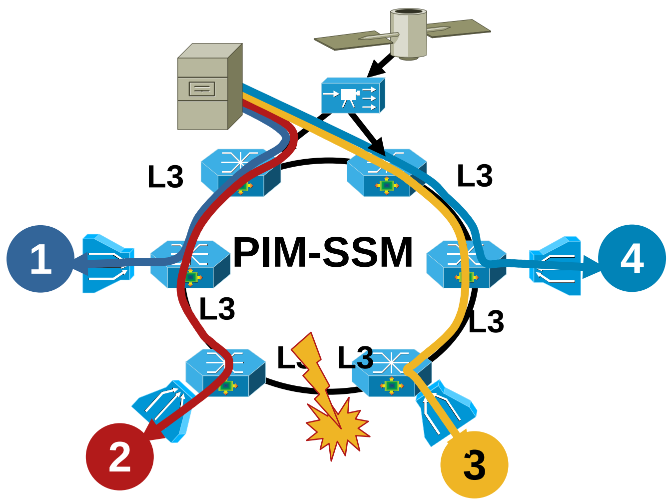
Benefits of Distributed L3 Edge for Multicast: No packet duplication



Traffic-Flow from N-PE1 to U-PE B:
Traffic traverses link twice

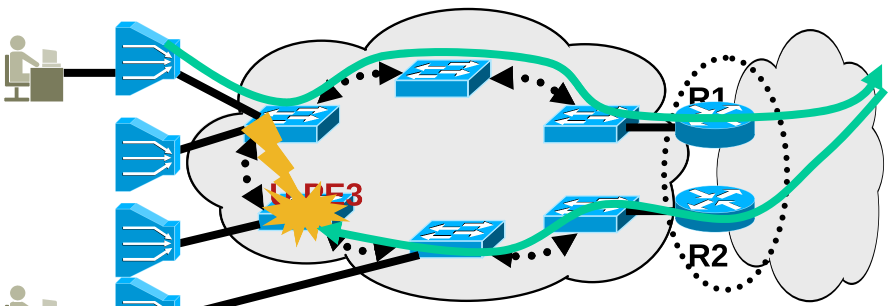


Ring-VPLS Implementation

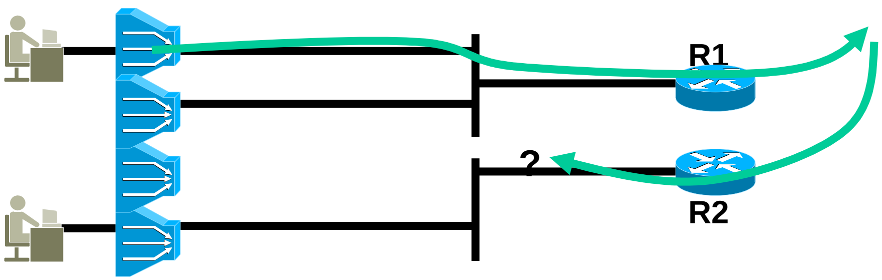


IP Multicast Implementation

Node Failure and Unicast Traffic

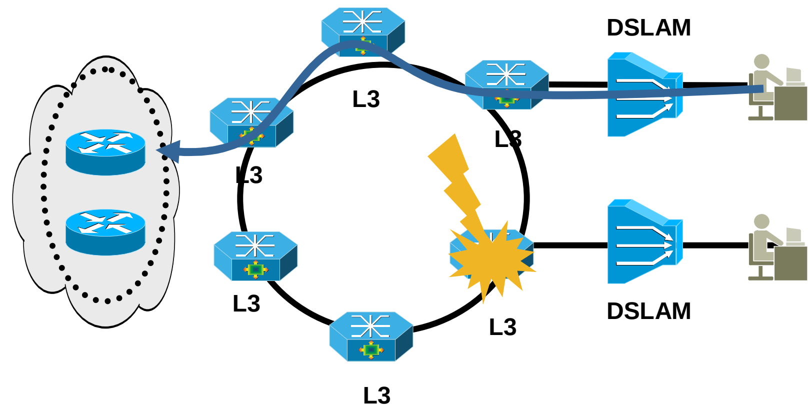


Logical View



Ring-VPLS Implementation

- L2 network segmented due to node failure
- Asymmetric routing can blackhole unicast traffic



L3 Implementation

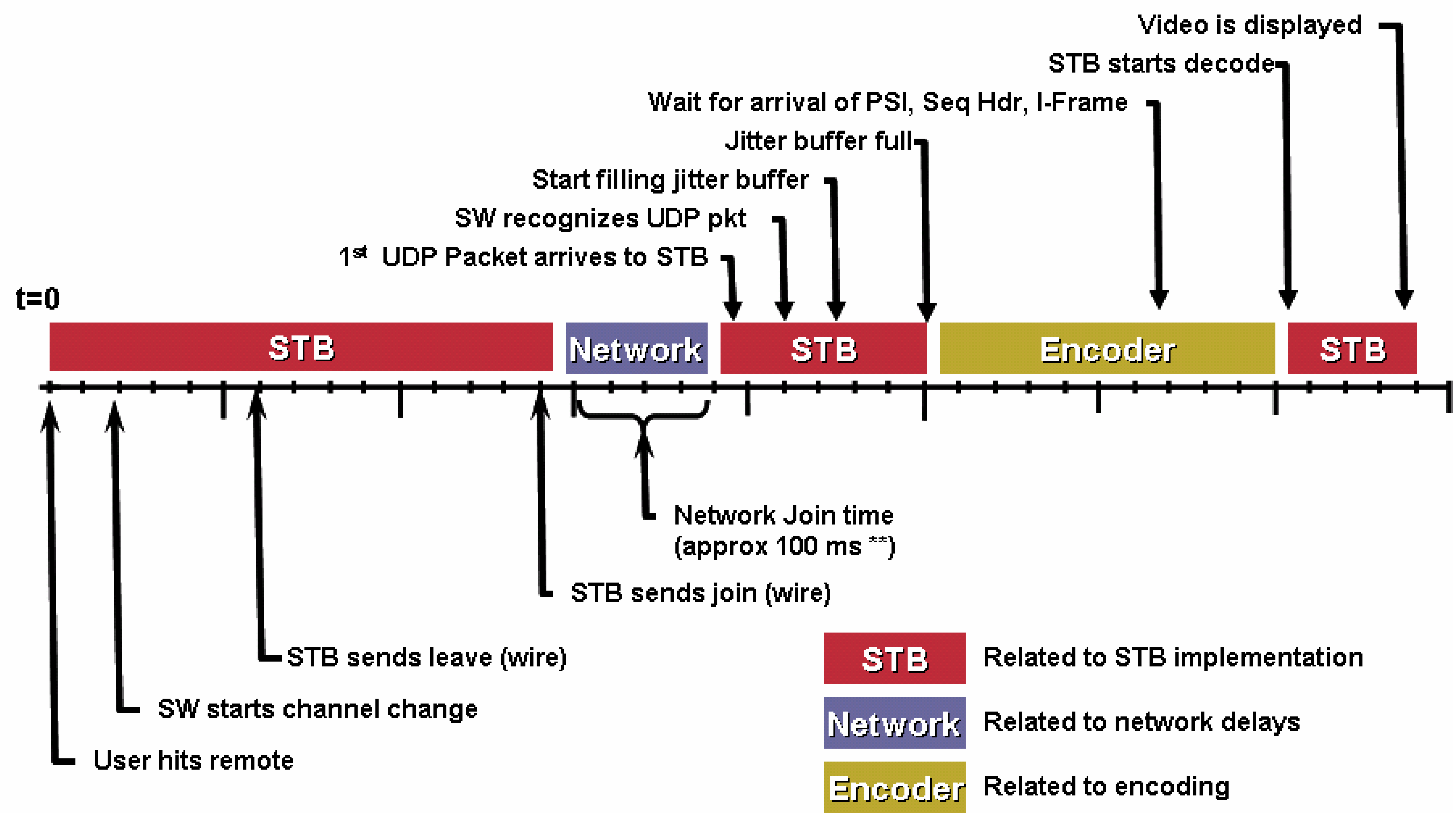
- No impact to unicast traffic. IGP converges around failed node

Channel Zapping Delay

- Common misconception is that IP multicast causes slow channel change
- Only when mcast request has to go to the regional headend is it >100ms
- Typical PE-agg router will serve thousands of subscribers and probability is that the next channel is already multicast to the PE-agg node
- The main culprit is waiting for the I-Frame—this can be solved by a frame cache approaches

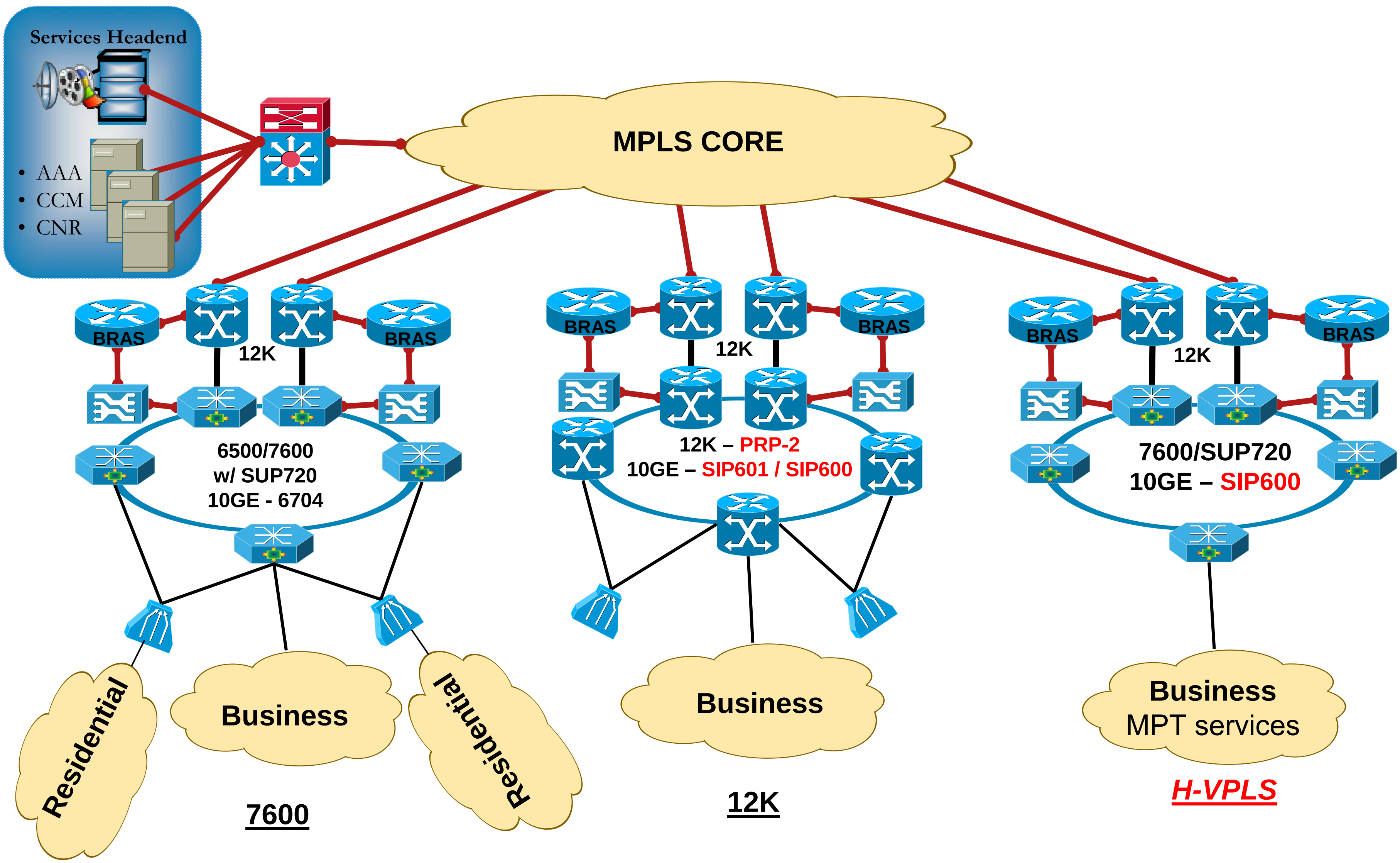
Channel Change Latency Factor	Typical Latency
Multicast Leave for old Channel	50 msec
Delay for Multicast Stream to Stop	150 msec
Multicast Join for New Channel	50 msec
Jitter Buffer Fill	150-200 msec
Conditional access delay	0 msec – 2 sec
I-Frame Delay	500 msec

Channel Zapping Delay STB, Network and Encoding Events Summary



Service Scalability & Resiliency

Validated Topologies



7600 Aggregation Architecture

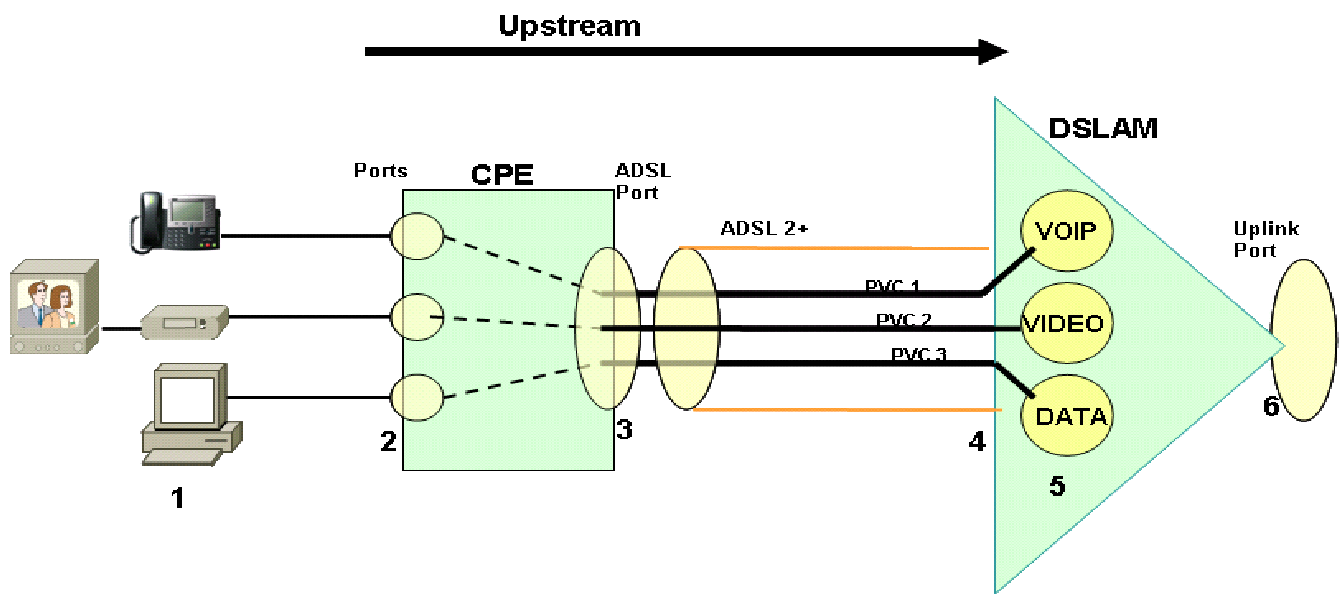
Physical Components

Broadband Transport			
H/W Component	Functional Roles	H/W Configuration	Software
Cisco 7600 Catalyst 6500	LCO-PE MCO-PE	WS-SUP720-3B/3BXL WS-X6704-10GE WS-X6748-GE WS-X6724-SFP	12.2(18)SXF

Non-Transport *	
Cisco 7200/7300/10000	BRAS
SCE 2020	SCE
Ericsson	DSLAM
Kasenna, Myrio	Middleware
Kasenna	VOD server
Ericsson, Linksys	Residential G/W
Amino, SA, Kreatel	STB
Cisco Call Manager	Voice Call Control
Cisco	IP Phones

(*) Components used in the E2E NSITE/SPSE testbeds but outside the "Transport" focus

7600 Aggregation Architecture - Highlights



- Multiple-PVC DSL UNI
- N:1 Service VLANs

  Shared VLAN per Service at DSLAM (not at the LCO-PE)
- Distributed L3 edge for VoIP/VOD/BCAST TV

  IP unicast/multicast routing used in Aggregation network
- Centralized L3 edge for DATA

  EoMPLS used in Aggregation network to backhaul traffic to BRAS

Physical Components

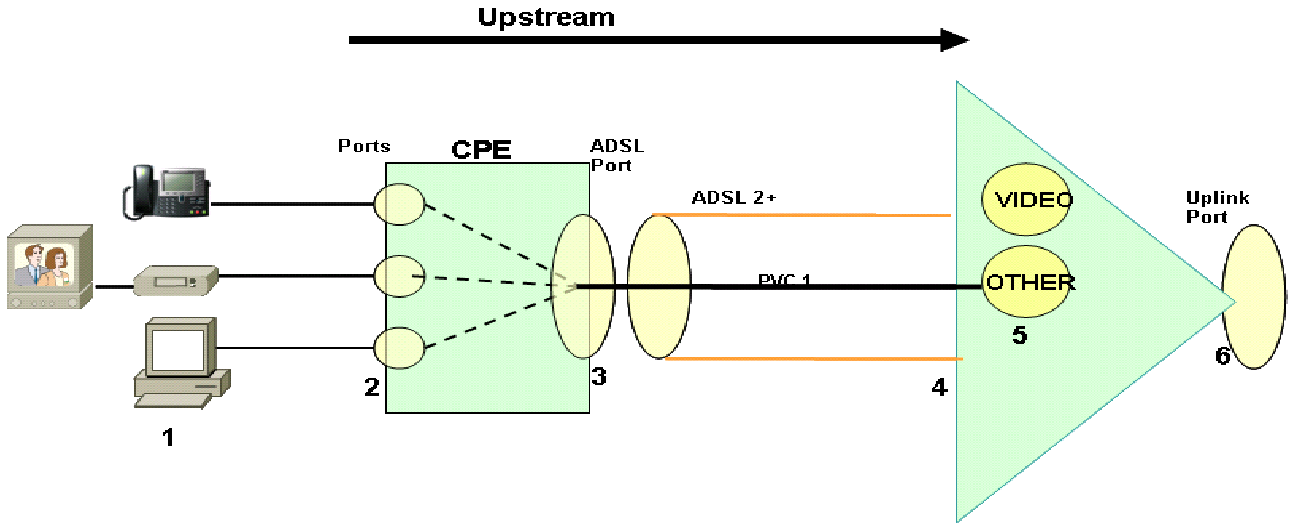
12K Aggregation Architecture

Broadband 4.0 Transport			
H/W Component	Functional Roles	H/W Configuration	Software
Cisco 12000	LCO-PE MCO-PE	12000-SIP-600 SPA-5X1GE SPA-10X1GE SPA-1XTENGE-XFP	12.0(32)S

Non-Transport *	
Cisco 7200/7300/10000	BRAS
SCE 2020	SCE
Ericsson	DSLAM
Kasenna, Myrio	Middleware
Kasenna	VOD server
Ericsson, Linksys	Residential G/W
Amino, SA, Kreatel	STB
Cisco Call Manager	Voice Call Control
Cisco	IP Phones

(*) Components used in the E2E NSITE/SPSE testbeds but outside the “Transport” focus of BB4.0

12K Aggregation Architecture - Highlights



- Single-PVC DSL UNI
  - This can be achieved with MVR-like functionality in the DSLAM
- N:1 Service VLANs
  - Shared VLAN per Service at DSLAM (not at the LCO-PE)
- Centralized L3 edge for VoIP/VOD/Data
  - EoMPLS used in Aggregation network to backhaul traffic to BRAS
- Distributed L3 edge for BCAST TV
  - IP multicast routing used in Aggregation network
- Model implemented with Cisco 12000

Traffic Profile in the Aggregation (18K Subs per 10G ring)

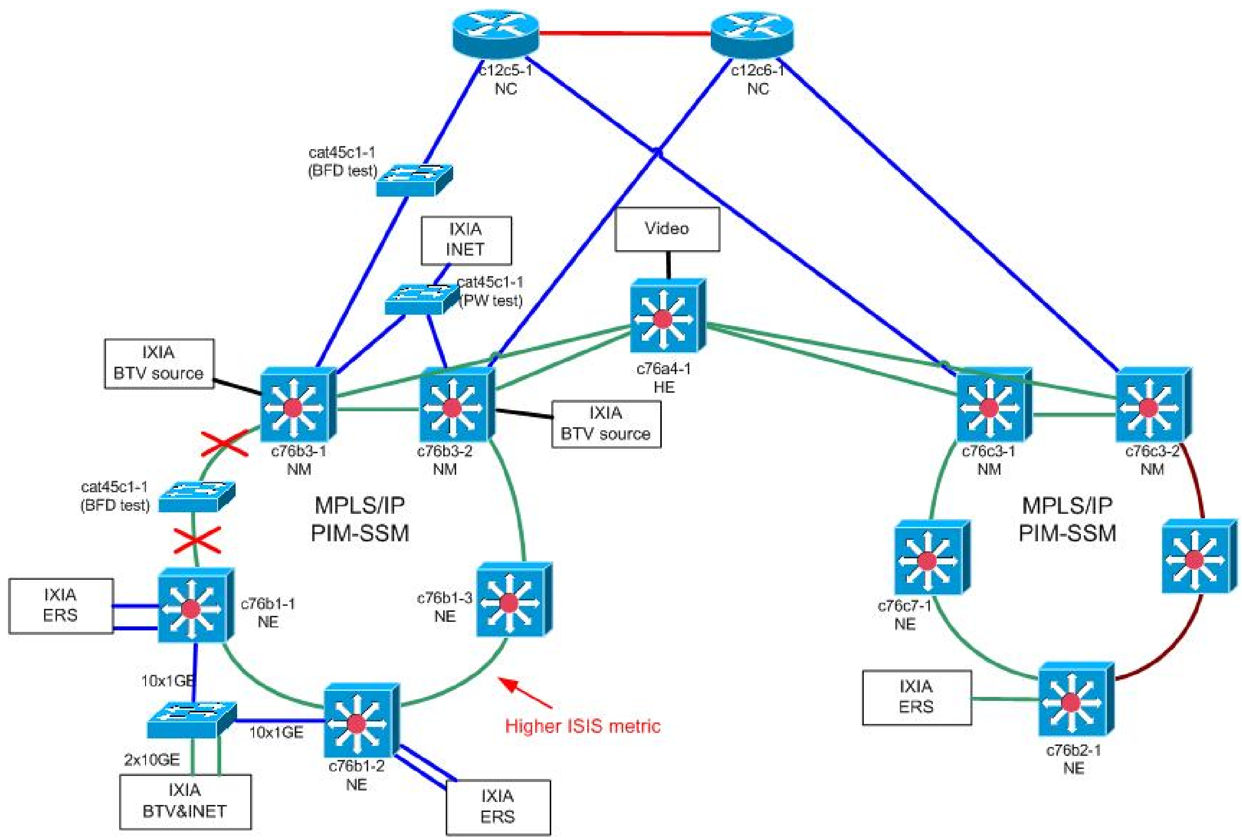
Service	Total Bandwidth per LCO	Total Bandwidth per Ring	Scaling per LCO	Scaling per Metro Pop
Residential VoIP	22 Mbps	66 Mbps	600 sustained G.729 calls @ 20msec sampling PPPoE encapsulation (36.12 kbps/call+signaling) (10% of LCO Subs)	1800 sustained G.729 calls @ 20msec sampling PPPoE encapsulation (36.12 kbps/call+signaling) (10% of Metro Pop Subs)
Residential TV	750 Mbps	750 Mbps	200 MPEG-2 Channels @ 3.75 Mbps CBR	150 MPEG-2Channels @ 5Mbps CBR
Residental VoD	750 Mbps	2.25 Gbps	200 MPEG-2 VoD Streams @ 3.75Mbps (3+% of Subs)	440 MPEG-2 VoD Streams @ 5Mbps (3% of Subs)
Residential HSD / Business PIR (Shared Bandwidth)	732 Mbps	2.3 Gbps	3000 Subscribers @ 256 Kbps (50 % of Subs)	9000 Subscribers @ 256 Kbps (50 % of Subs)
Business VoIP	4.4 Mbps	13.2 Mbps	50 sustained G.711 calls @ 20msec sampling PPPoE encapsulation (87.2 kbps/call) (25% of LCO Subs)	150 sustained G.711 calls @ 20msec sampling PPPoE encapsulation (87.2 kbps/call) (25% of Metro Pop Subs)
DSL Business 2 Mbps CIR	300 Mbps	900 Mbps	150 Business Subscribers @ 2 Mbps	450 Business Subscribers @ 2 Mbps
DSL Business 7.5 Mbps CIR	187.5 Mbps	562.5 Mbps	25 Business Subscribers @ 7.5 Mbps	75 Business Subscribers @ 7.5 Mbps
Ethernet Business 50 Mbps CIR	1.25 Gbps	3.75 Gbps	25 Business Subscribers @ 50 Mbps	75 Business Subscribers @ 50 Mbps
Total Bandwidth	~4Gbps	~10.5 Gbps	220 EoMPLS Pseudowires	640 EoMPLS Pseudowires

Service Protection Mechanism

- Network fast failure detection and protection mechanisms
  – Bidirectional Forwarding Detection for IGP
  – Fast-IGP
  – MPLS-TE FRR
  – SSO
- Service resiliency
  – GEC to DSLAM
  – PW Redundancy

BFD in the Metro Ring

- Impacted Services
  - – Residential BTV
  - – Residential HIA
  - – Business ERS
- Scaling Numbers
  - – 200 BTV streams
  - – 400 BTV receivers
  - – 20 HIA EVPL PWs
  - – 200 Bus EVPL PWs



BFD in the Metro Ring

- NM Config

```
interface TenGigabitEthernet1/3
 description c76b3-1 Ten1/3 to c76b1-1 Ten1/1
 mtu 4470
 ip address 50.1.2.13 255.255.255.252
 ip pim sparse-mode
 ip router isis 65000
 logging event link-status
 load-interval 30
 carrier-delay msec 0
 mpls ip
 bfd interval 50 min_rx 50 multiplier 3
 isis circuit-type level-1
 isis network point-to-point
 isis metric 9 level-1
 isis hello-interval 3
!
router isis 65000
 net 49.0001.0000.0000.0012.00
 is-type level-1
 metric-style wide
 set-overload-bit on-startup 300
 max-lsp-lifetime 65500
 ispf
 lsp-refresh-interval 65000
 spf-interval 1 100 110
 prc-interval 1 100 110
 no hello padding
 log-adjacency-changes
 passive-interface GigabitEthernet3/2
 passive-interface Loopback0
 passive-interface Loopback3
 bfd all-interfaces
```

- NE Config

```
interface TenGigabitEthernet1/1
 description c76b1-1 Ten1/1 to c76b3-1 Ten1/3
 mtu 4470
 ip address 50.1.2.14 255.255.255.252
 ip pim sparse-mode
 ip router isis 65000
 load-interval 30
 carrier-delay msec 0
 mpls ip
 bfd interval 50 min_rx 50 multiplier 3
 isis circuit-type level-1
 isis network point-to-point
 isis metric 9 level-1
 isis hello-interval 3
!
router isis 65000
 net 49.0001.0000.0000.0017.00
 is-type level-1
 metric-style wide
 set-overload-bit on-startup 300
 max-lsp-lifetime 65500
 lsp-refresh-interval 65000
 ispf
 spf-interval 1 100 110
 prc-interval 1 100 110
 no hello padding
 log-adjacency-changes
 redistribute static ip route-map STATIC2ISIS level-1
 passive-interface Vlan2
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 passive-interface Loopback3
 bfd all-interfaces
```

BFD in the Metro Ring

- NE<->NM LDP sessions established via failed NM1-NE1 link
  - NE1<->NM1, NE1<->NM2, NE2<->NM1, NE2<->NM2
- INET, BTV and ERS traffic via failed NM1-NE1 link
- LOS detection at NM1

		BFD on	BFD off
		Δ (Link Down & ISIS adj change)	Δ (Link Down & ISIS adj change)
Link down	NE 1	97 msec	7.317 sec (isis hello-interval 3, multiplier 3)
Link up	NE 1	1.003 sec	1.018 sec

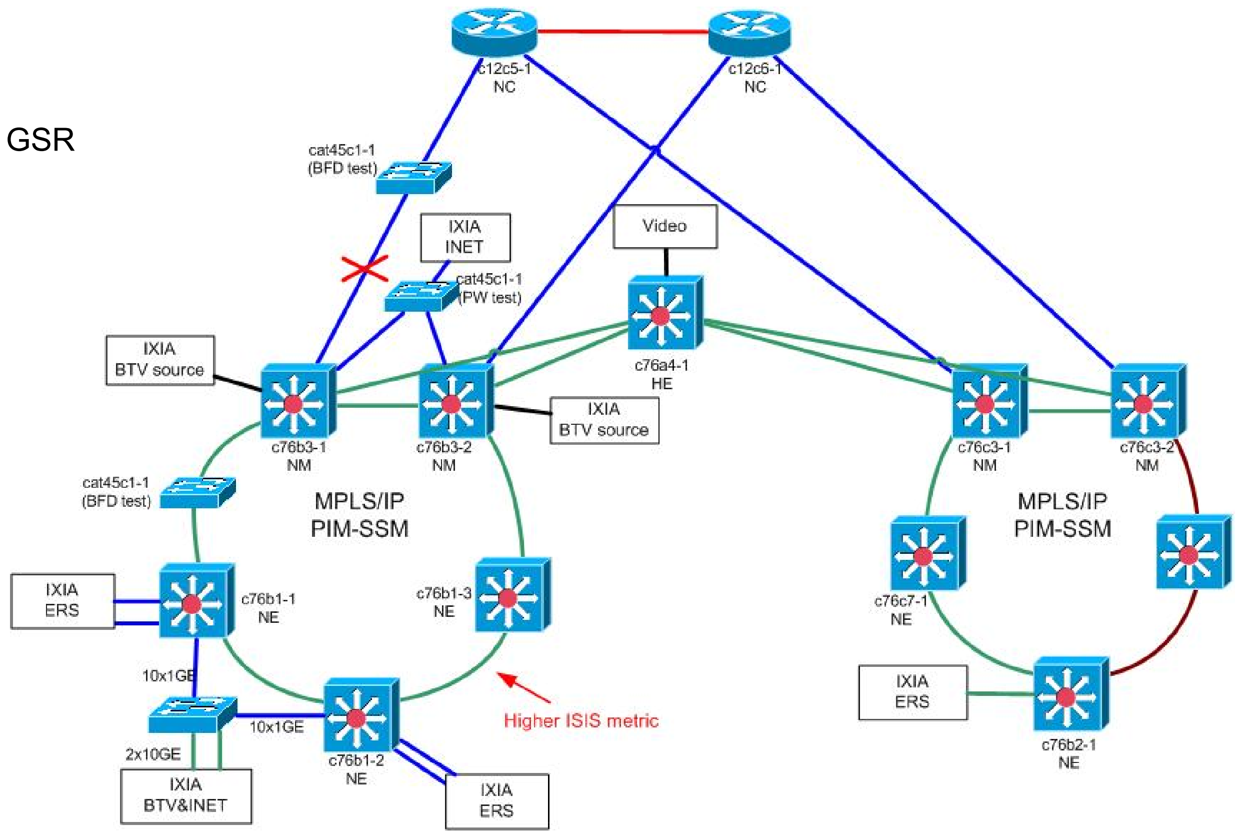
BFD in the Metro Ring

- NE<->NM LDP sessions established via failed NM1-NE1 link
  - NE1<->NM1, NE1<->NM2, NE2<->NM1, NE2<->NM2
- INET, BTV and ERS traffic via failed NM1-NE1 link
- LOS detection at NM1

		BFD on			BFD off		
		INET	BTV	ERS	INET	BTV	ERS
Link down	NE 1	337 ms up 291 ms down	580 ms	294 ms up 199 ms down	>10 sec	8-10 sec	>10 sec
	NE 2	291 ms up 290 ms down	600 ms	288 ms up 168 ms down	>10 sec	8-10 sec	>10 sec
Link up	NE 1	3.64 sec up 3.84 sec down	3.43 sec	3.61 sec up 1.48 sec down	>20 sec	18.8 sec	>20 sec
	NE 2	3.49 sec up 1.55 sec down	3. 35 sec	3.47 sec up 1.48 sec down	>20 sec	18.8 sec	>20 sec

BFD between Metro Ring and Core

- Impacted Services
  - Business ERS
- Scaling Numbers
  - 50 BFD neighbors on each GSR
  - 200 BTV streams
  - 400 BTV receivers
  - 20 HIA EVPL PWs
  - 200 Bus EVPL PWs



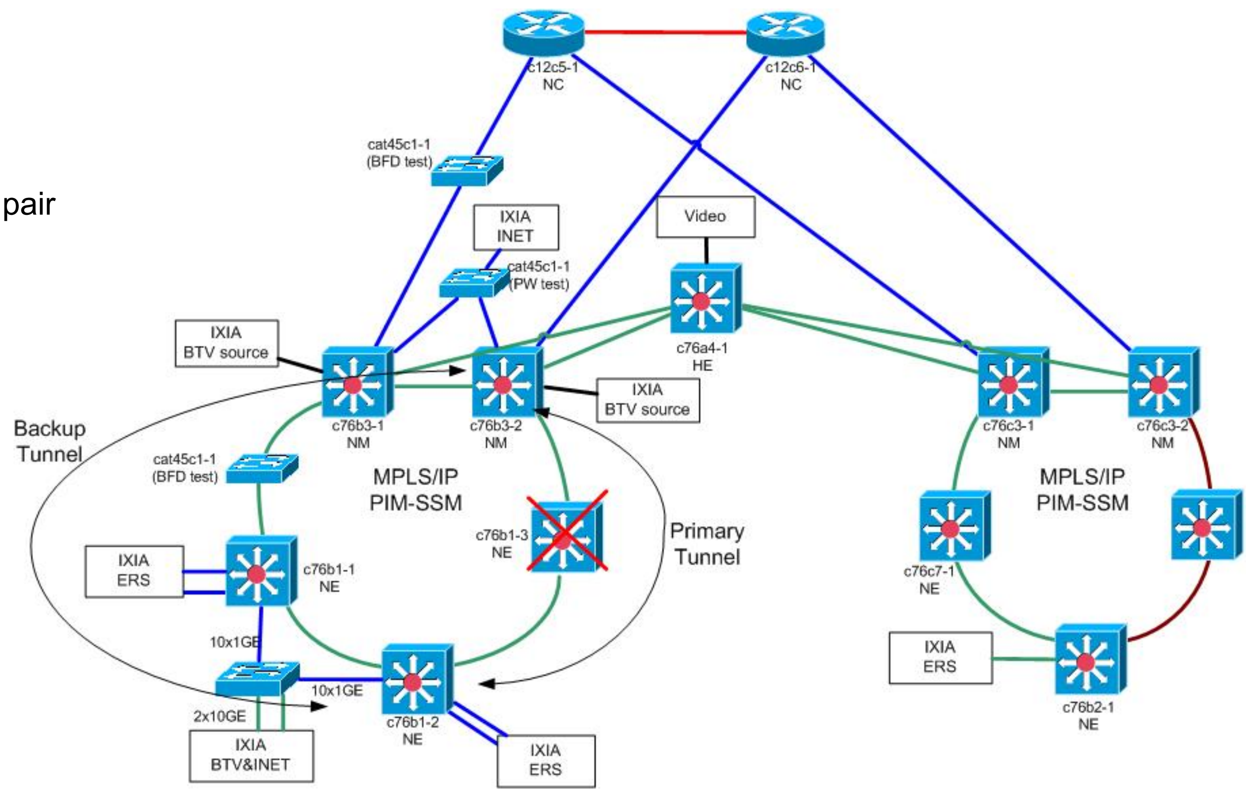
BFD between Metro Ring and Core

- NE<->NE LDP session established via failed NM1-P link
  - 200 ERS EoMPLS pseudowires
- ERS traffic via failed NM1-P link

		BFD on			BFD off		
		INET	BTV	ERS	INET	BTV	ERS
Link down	NE 1	x	x	128 ms up 200 ms down	x	x	>10 sec
	NE 2	x	x	132 ms up 203 ms down	x	x	>10 sec
Link up	NE 1	x	x	0 ms up 1 ms down	x	x	>20 sec
	NE 2	x	x	0 ms up 1 ms down	x	x	>20 sec

MPLS TE FRR Node Protection
INET traffic protected

- Impacted Services
  - Residential HIA
  - BTV from NM2 to NE2
- Scaling Numbers
  - 1 primary/backup tunnels pair
  - 200 BTV streams
  - 20 HIA EVPL PWs
  - 200 Bus EVPL PW



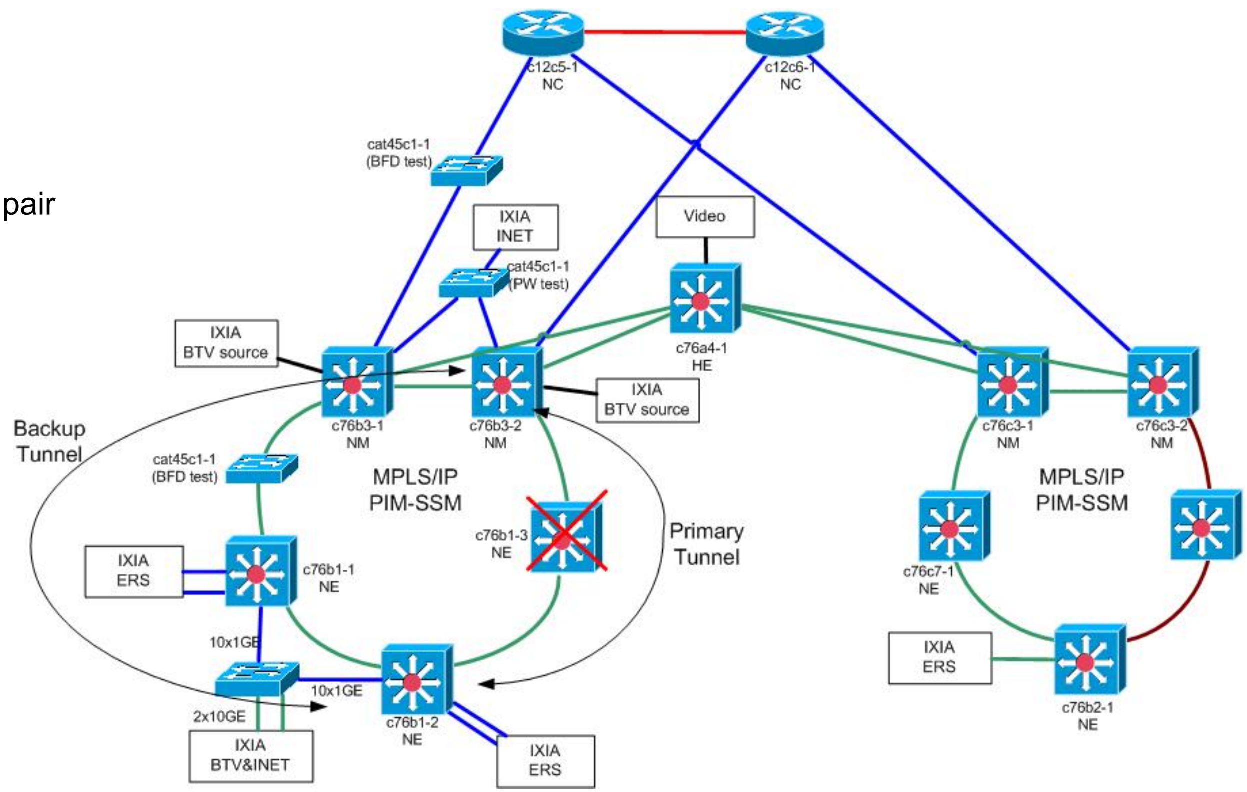
MPLS TE FRR Node Protection

- Node Protection
  - – NE2<->NE3<->NM2 primary tunnel
  - – NE2<->NE1<->NM1<->NM2 backup tunnel
- NE3 midpoint node failure
  - – 10 INET EoMPLS pseudowires from NE2 to NM2 in TE Tunnel
  - – 100 multicast streams to NE2 via failed path

		INET (TE FRR)	BTV	ERS
NE3 Pwr Off	NE 1	X	x	x
	NE 2	28 ms up 28 ms down	240 ms	x
NE3 Pwr On	NE 1	X	x	x
	NE 2	0 ms up 0 ms down	65 ms	x

MPLS TE FRR Node Protection
Business traffic Protected

- Impacted Services
  - Business Traffic
  - BTV from NM2 to NE2
- Scaling Numbers
  - 1 primary/backup tunnels pair
  - 200 BTV streams
  - 20 HIA EVPL PWs
  - 200 Bus EVPL PW

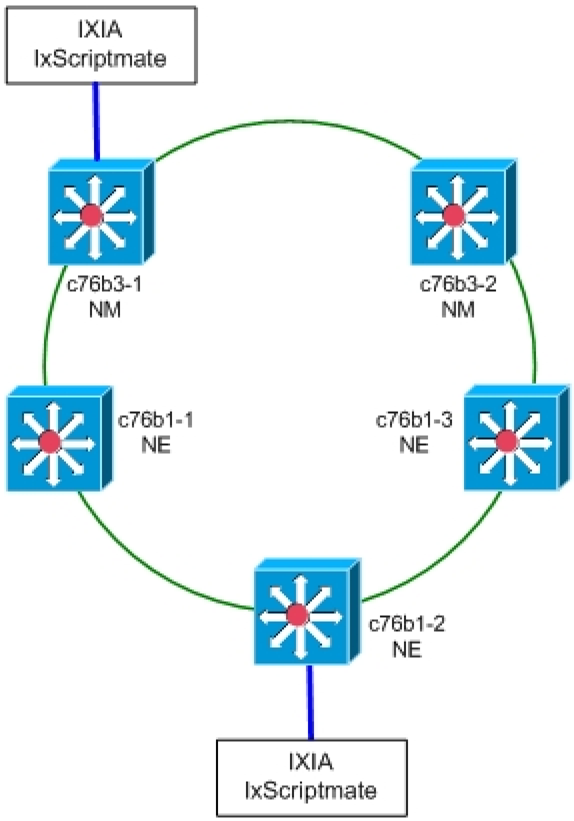


MPLS TE FRR Node Protection

- Node Protection
  - NE2<->NE3<->NM2 primary tunnel
  - NE2<->NE1<->NM1<->NM2 backup tunnel
- NE3 midpoint node failure
  - 200 ERS EoMPLS pseudowires from NE2 to NM2 in TE Tunnel

Resiliency Applied FRR-Node Protection	Test Condition	ERS (200 PWs)
NE3 Power Off	Primary Tunnel Down	123 ms
NE3 Power On	Primary Tunnel Up	0 ms

BTV - IP Multicast Group Join Delay



Group Join Delay = the elapsed time between the time a DUT receives a group of IGMP Join requests and the time the multicast clients begin receiving traffic for the groups they joined.

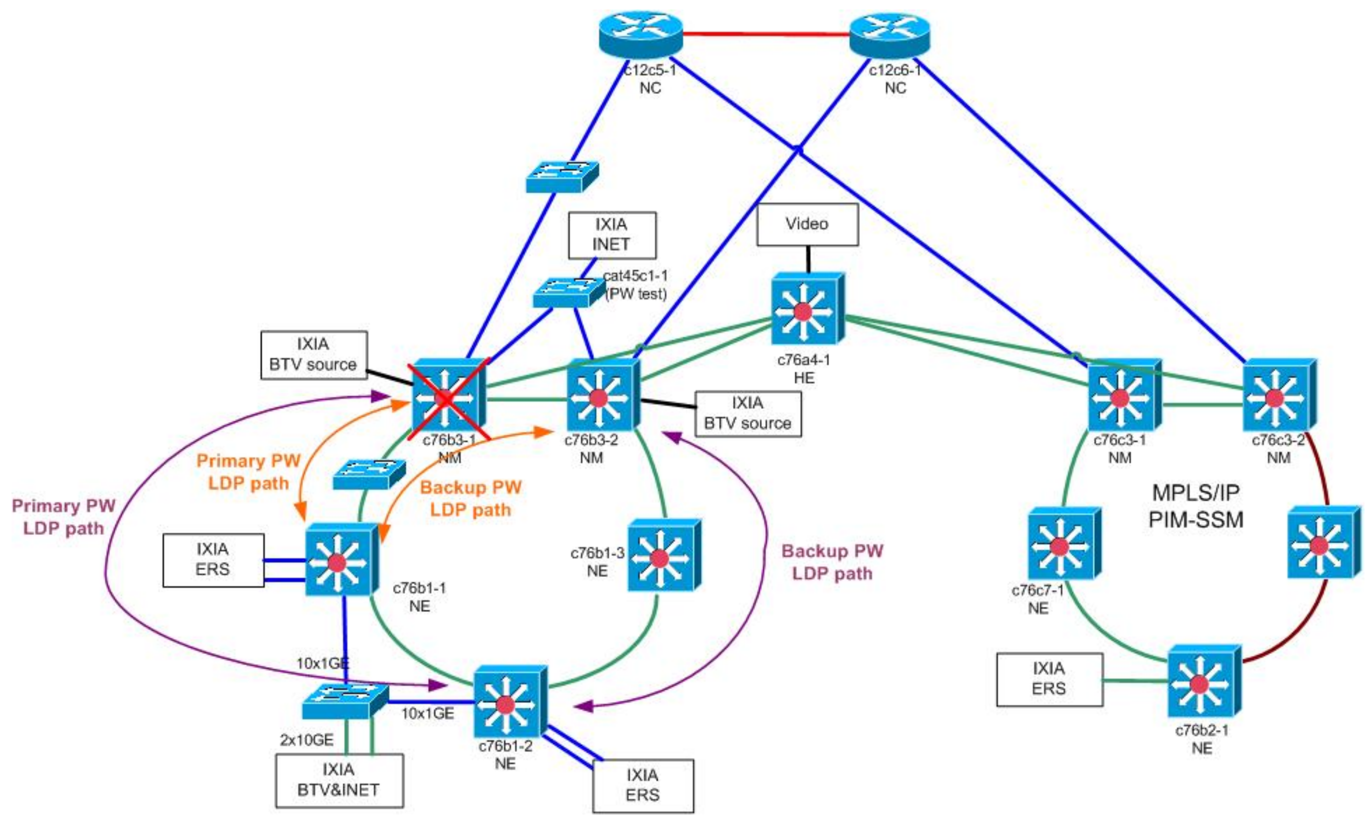
Average Group Join Delay (ms)				
Size	No Static Groups		Static Groups	
	Channels		Channels	
	100	200	100	200
512	157	264	11	20
1024	194	264	22	21
1280	160	277	18	24
1518	155	250	29	25

Note: The Group Join Delay with DNS mapping is in the same order of magnitude as with static groups (caching).

New Feature

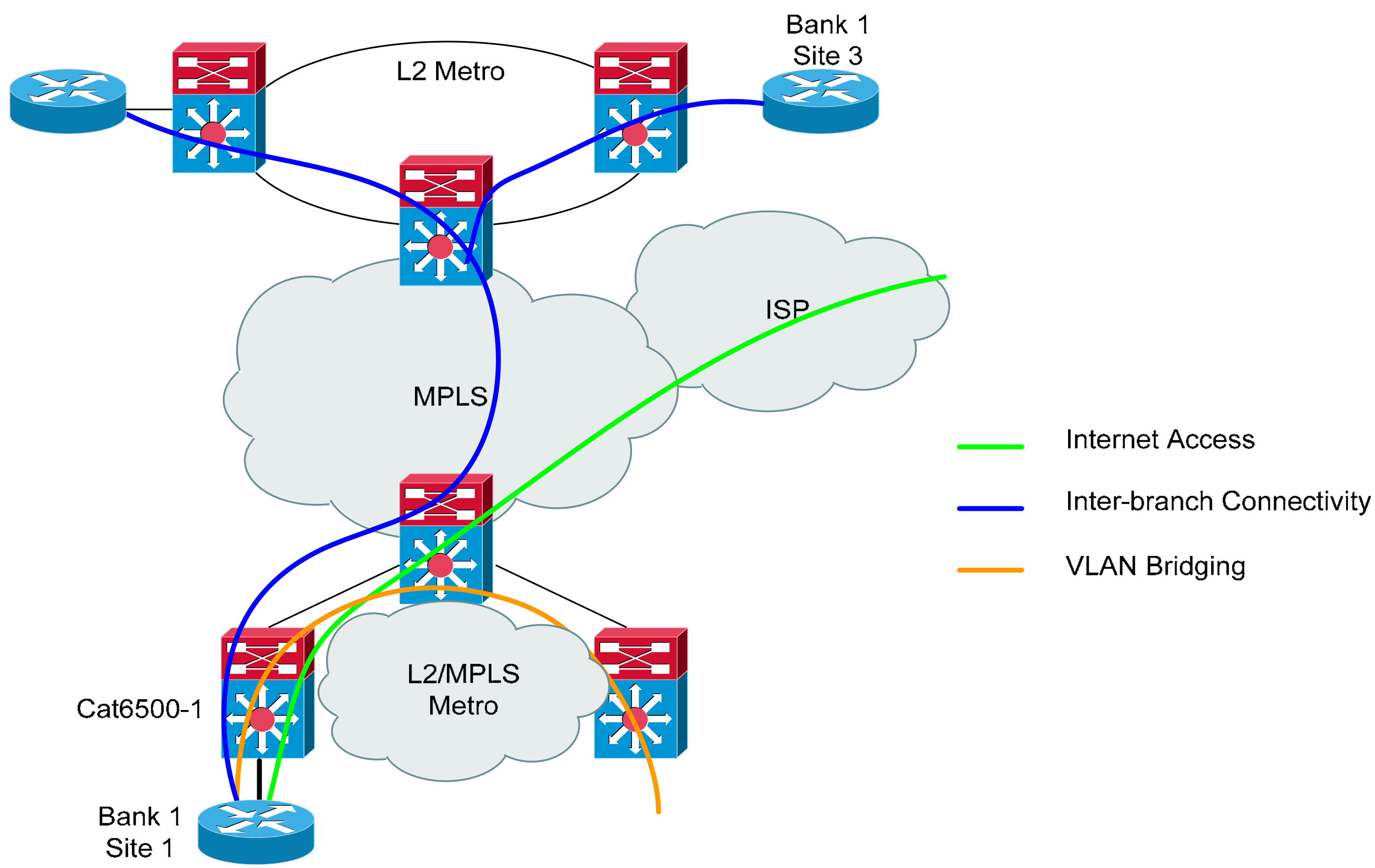
PW Redundancy – End2End HA

- Impacted Services
  - Residential BTV
  - Residential HIA
  - Business ERS
- Failure type
  - NM reload
  - NM power cycle



New Feature

L2/L3 Mux UNI



New Feature

L2/L3 MUX UNI Configuration

L2/L3 MUX UNI

```
interface GigabitEthernet3/4
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1820,1830
 switchport mode trunk
 switchport nonegotiate
 mtu 9216
 logging event link-status
 load-interval 30
 no cdp enable
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
 spanning-tree bpduguard disable
 spanning-tree guard root
!
interface GigabitEthernet3/4.1
 encapsulation dot1Q 23
 no snmp trap link-status
 xconnect 50.0.0.12 14 pw-class internet-pw
 backup peer 50.0.0.13 14 pw-class internet-pw
```

VoD VLAN

```
interface Vlan1820
 description IXIA VoD vlan
 mac-address 0018.2000.0001
 ip unnumbered Loopback4
 ip helper-address 50.1.2.34
 no ip redirects
 load-interval 30
```

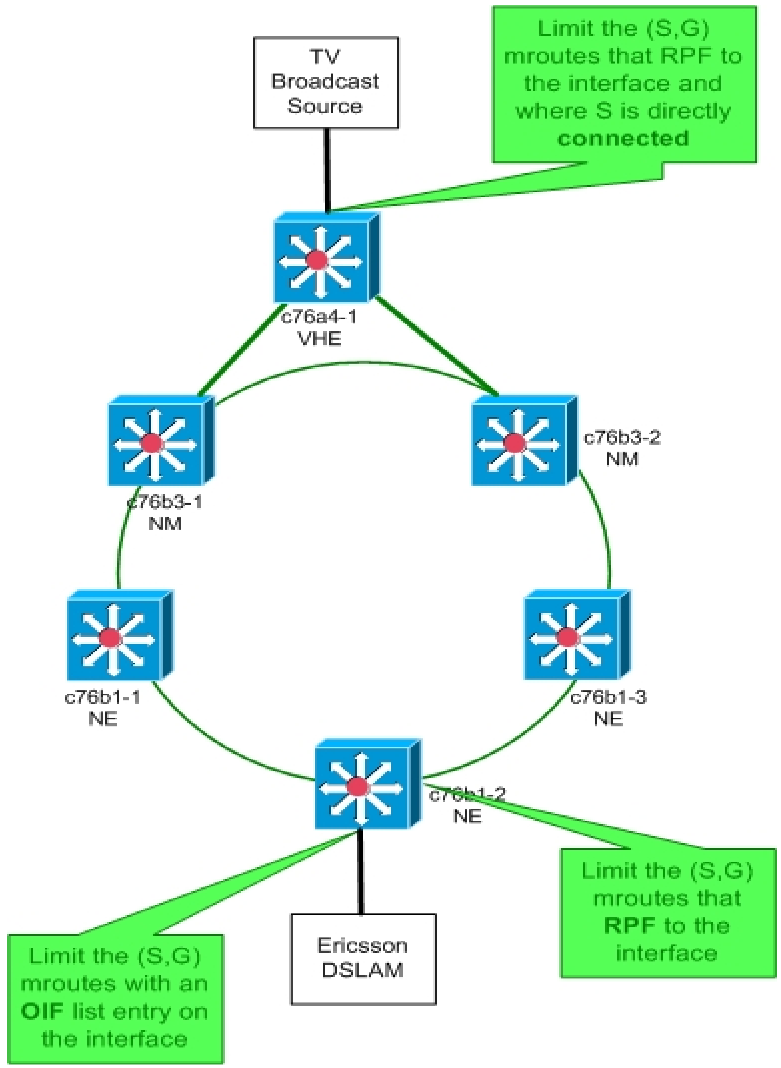
TV Broadcast VLAN

```
interface Vlan1830
 description IXIA TV_Bcast vlan
 mac-address 0018.3000.0001
 ip unnumbered Loopback5
 no ip redirects
 ip pim sparse-mode
 ip multicast limit out 11 10
 load-interval 30
```

Internet Pseudowire

New Feature

Multicast Call Admission Control



Syntax:

```
ip multicast limit [rpf|connected|out] <acl> <n>
ip multicast limit cost <acl> <cost>
```

Example:

```
c76b1-2(config)#ip multicast limit cost 11 10
…
c76b1-2(config)#interface Vlan1830
c76b1-2(config-if)#ip multicast limit out 11 100
…
c76b1-2(config)access-list 11 permit 239.12.1.0 0.0.0.255
```

Show/Debug Commands:

```
c76b1-2#show ip multicast limit
Interface Vlan1830
  Multicast Access Limits
 out acl 11 (100 = max 100) exceeded 7
 out acl 12 (0 < max 100) exceeded 0

c76b1-2#debug ip mrouting limit
Jun  7 11:46:06.039: MRL(0): IGMP add mroute (192.12.2.2,
239.12.1.11) denied for Vlan1830, limit-acl 11, cost-acl
11, cost 10, (100 = max 100)
Jun  7 11:46:06.043: %MROUTE-4-MROUTELIMIT: Exceeded
multicast limit for group 239.12.1.11, source 192.12.2.2 on
interface Vlan1830 - VRF default
-Process= "IGMP Input", ipl= 0, pid= 298
```

Aggregation Network Scale Challenges

- MPLS/IP scale considerations
  - EoMPLS PWs
  - LDP neighbours
  - ARP table

EoMPLS PW Scale Characteristics

Residential Services

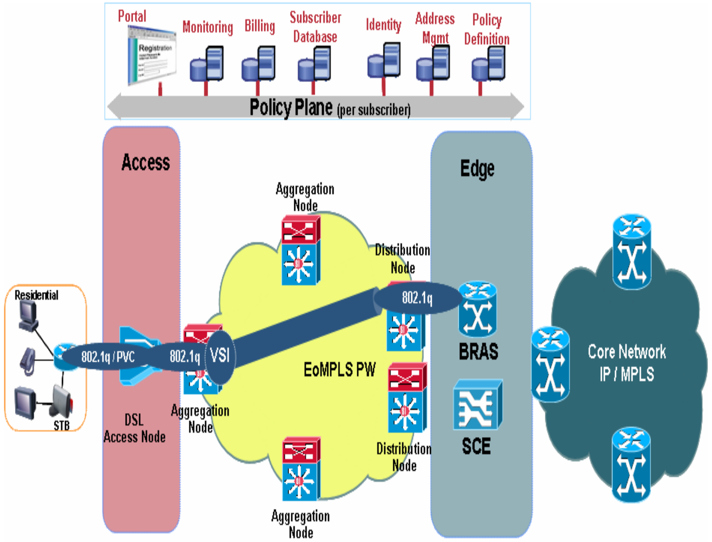
- Single PW per DSLAM; N:1 VLAN model
- No EoMPLS PW scale concerns at the aggregation node (LCO-PE); single EoMPLS PW per shared service VLAN
- No MAC learning as residential service carried over VPWS
- EoMPLS PW scale must be considered for distribution node when designing large scale network

No. PW = M * N * Y
M = number of CO's per Metro POP
N = number of DSLAMs per Local CO
Y = number of BRAS-terminated services per DSLAM

Example (Large ILEC):

M = 25
N = 40
Y = 1

TOTAL EoMPLS PW at the MCO-PE= 25*40*1=1K



LDP Scale Characteristics

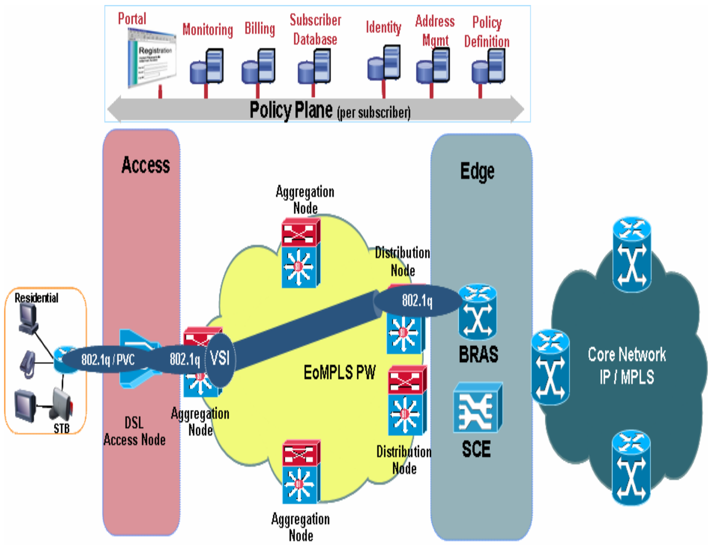
- No LDP scale concerns at the aggregation node (LCO-PE); it requires an LDP neighbor per MCO-PE that this node uses as aggregation point
- No LDP scale concerns at the distribution node (MCO-PE). It requires a directed LDP neighbor per LCO-PEs being aggregated. The LDP scale well within the platform limitation as demonstrated below.

No. LDP Neighbors = M * W
M = number of rings that aggregate at the distribution node (MCO-PE)
W = number of aggregation nodes (LCO-PE) per subtending ring

Example:

M = 10
W = 5

Required LDP Neighbours at MCO-PE = 10*5=50



ARP Scale Characteristics

- Typical 3play CPE deployment: STBs bridged and VoIP/HIA routed (NAT)
- 2x STBs and 1xRG per household
- ARP scaling should be considered at the aggregation nodes
- No ARP scaling issues at the distribution node as hosts not directly connected

Total ARP Entries = M * W * Y
M = number of DSLAMs attached to the aggregation node (LCO-PE)
W = number of subscribers per DSLAM
Y = number of devices behind CPE that routed at the LCO-PE (eg.STB/Phone)

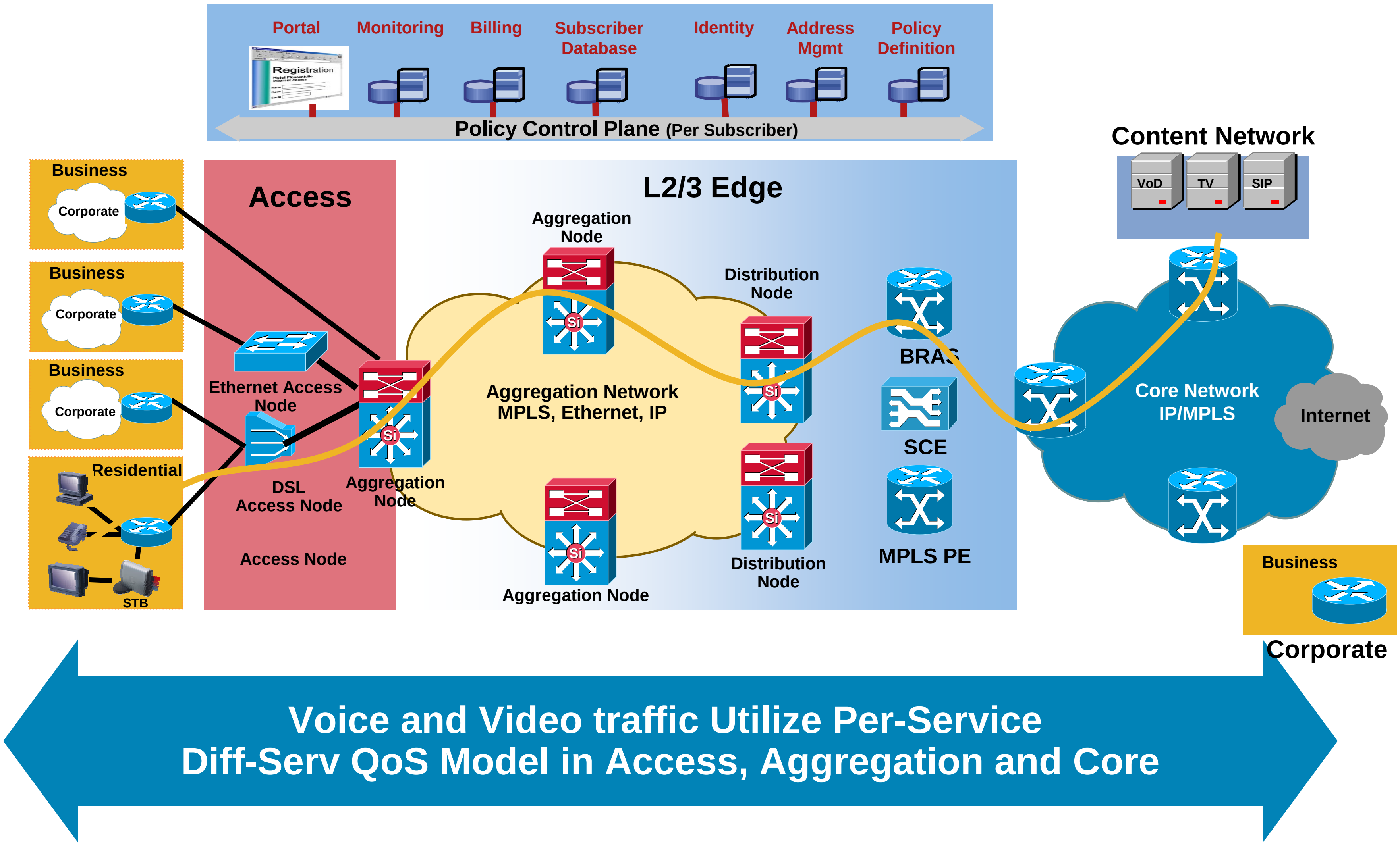
Example (Large ILEC):

M = 40
W = 300
Y = 3

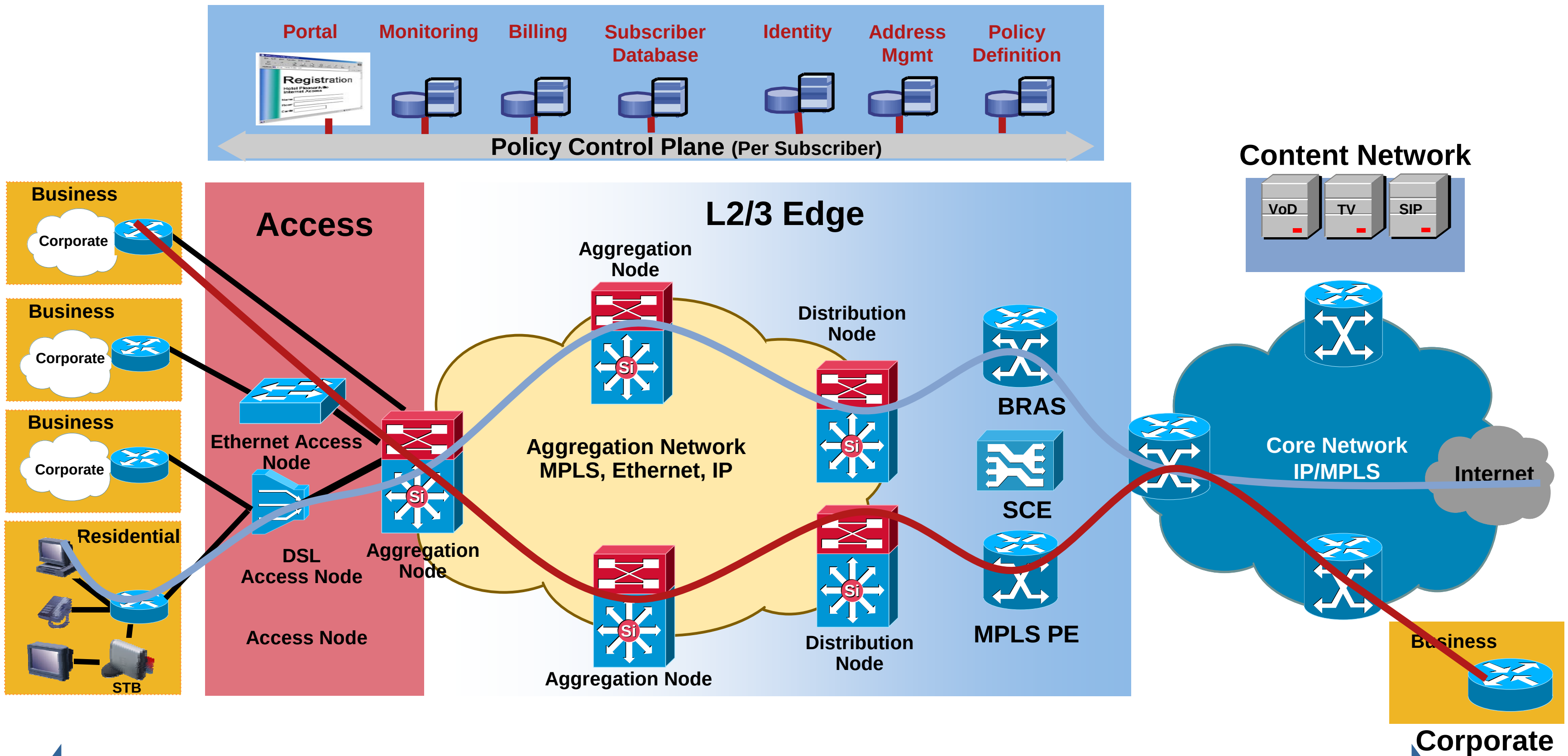
TOTAL ARP Entries in LCO-PE = 40*300*3=36K

QoS

QOS Architecture Direction

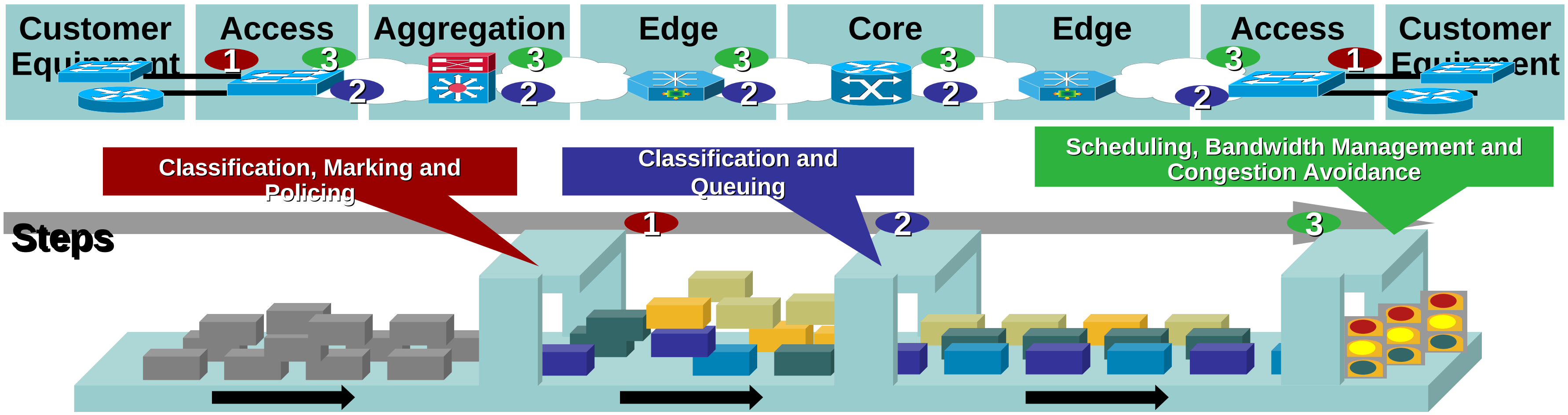


QOS Architecture Direction



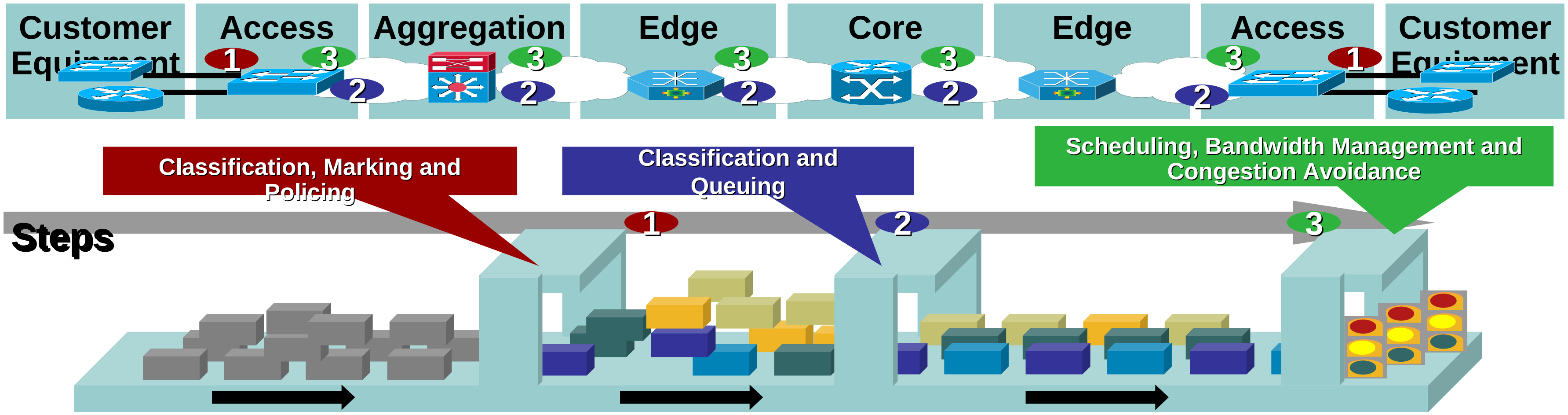
Internet and Business Traffic Utilize Per-Subscriber QoS Model in Access, Aggregation and Core

QOS Model with Ethernet/IP Aggregation



QoS Function	Residential Subscriber	Business Customer
Classification/ Marking	Classified at CPE for upstream, and at content source for downstream into Voice, Video, and INET classes. DSCP or 802.1p markings used for aggregation network, EXP for MPLS core.	Classified at LCO-PE based on customer markings to RT, BC, and BE classes. Markings mapped to 802.1p for aggregation network and to EXP for MPLS core.
Traffic Conditioning	Limited per-subscriber by rate between DSLAM and DSL CPE. Per-service aggregate rate limiting implemented on DSLAM egress/LCO-PE ingress and service injection points.	Policy implemented at LCO-PE ingress to adhere per-subscriber, per-service traffic to SLA agreement. Egress policy at LCO-PE to CPE interface possibly needed for multipoint service.
Congestion Management/ Avoidance	Traffic mapped to queues by classes. Scheduling performed by DWRR or MDRR. WRED used on INET class for congestion avoidance.	Traffic mapped to queues by classes. Scheduling performed by DWRR or MDRR. WRED used on BE and BC classes for congestion avoidance.

QOS Model with MPLS/IP Aggregation



QoS Function	Residential Subscriber	Business Customer
Classification/ Marking	Classified at CPE for upstream, and at content source for downstream into Voice, Video, and INET classes. DSCP markings used for Voice and Video traffic, EXP markings derived for INET traffic.	Classified at LCO-PE based on customer markings to RT, BC, and BE classes. Markings mapped to EXP for Aggregation network and MPLS core.
Traffic Conditioning	Limited per-subscriber by rate between DSLAM and DSL CPE. Per-service aggregate rate limiting implemented on DSLAM egress / LCO-PE ingress and service injection points.	Policy implemented at LCO-PE ingress to adhere per-subscriber, per-service traffic to SLA agreement. Egress policy at LCO-PE to CPE interface possibly needed for multipoint service.
Congestion Management/ Avoidance	Traffic mapped to queues by classes. Scheduling performed by DWRR or MDRR. WRED used on INET class for congestion avoidance.	Traffic mapped to queues by classes. Scheduling performed by DWRR or MDRR. WRED used on BE and BC classes for congestion avoidance.

Triple Play Services CAC Requirements

- VoIP telephony service
  - Subscriber line: no CAC required
    - The number of calls generally limited at the application level
  - Aggregation network: no CAC required
    - Generally provisioned with sufficient class bw to cope with peak during working and failure case
- TV broadcast service
  - Subscriber line: CAC required
  - Aggregation network: no CAC required
    - Generally provisioned with sufficient class bw to cope with peak during working and failure case
- Video on demand service
  - Subscriber line
    - For fixed number of channels per subscriber line: no CAC required
    - For variable number of channels per subscriber line/variable bandwidth cases: CAC required
  - Aggregation network: CAC required
    - Potential for congestion both in working and network failure cases

Video CAC

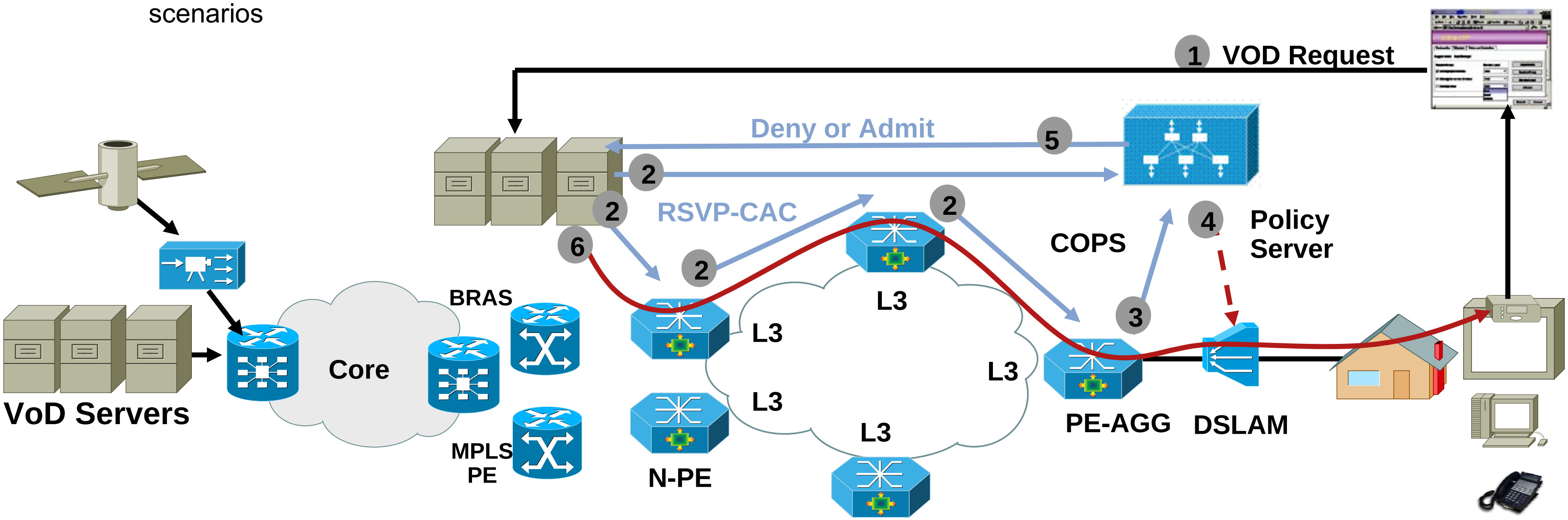
Topology-Unaware Off-Path CAC	Topology-Aware Off-Path CAC	Topology-Aware On-Path CAC
1 • Embedded within the VoD server • CAC decisions not synchronized with the network topologies	2 • CAC decision outsourced to Policy Server • Policy server interaction with the network for topology synchronization	3 • Dynamic adjustment to any topology change • Requires network level connection admission control signaling: RSVP

Integrated CAC

2 + 3

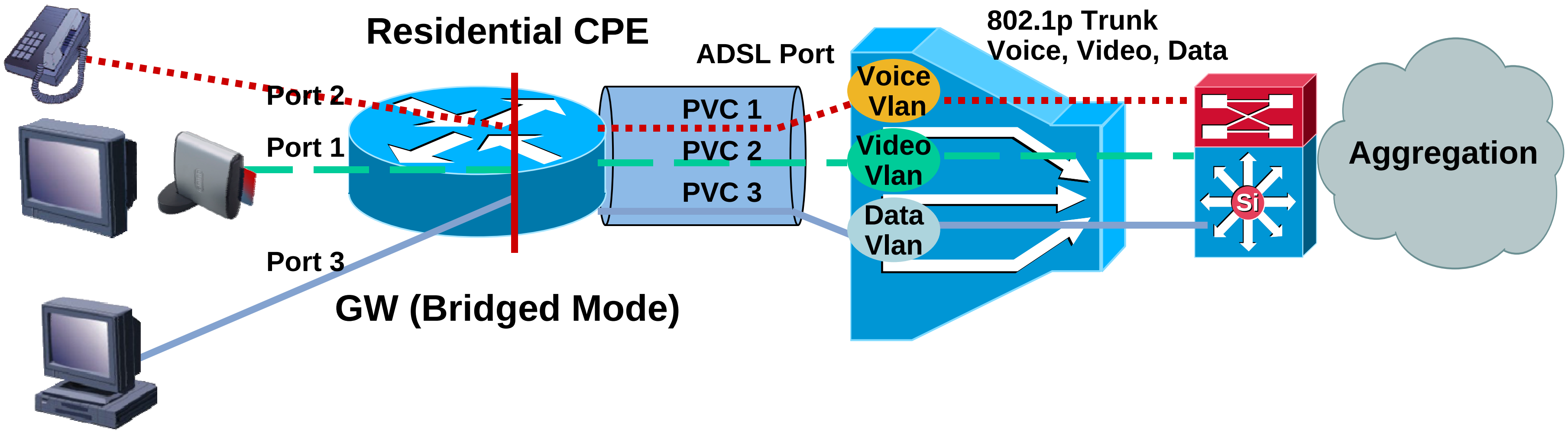
- Integrated video CAC approach combines two methods
- VOD stream will be denied if business rules of either fail
- Prioritize blocking of free VOD vs. pay VOD in network failure scenarios

COPS: Common Open Policy Server



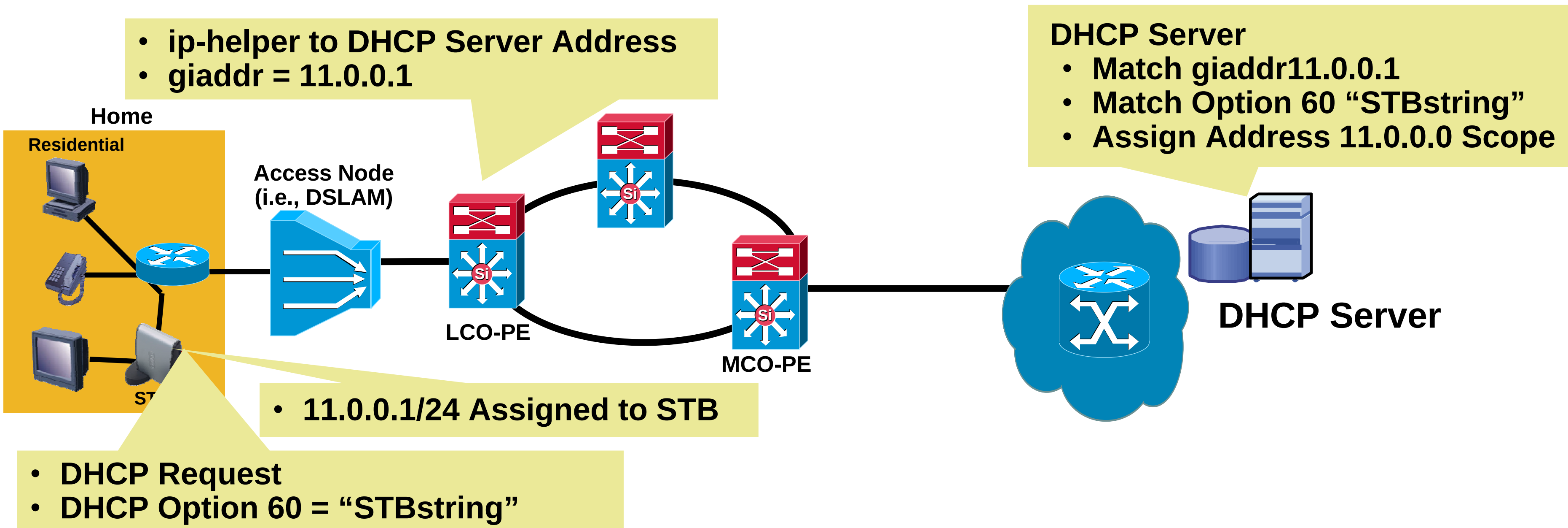
Home Networking Models

Home Networking Models
CPE GW as Bridged Mode



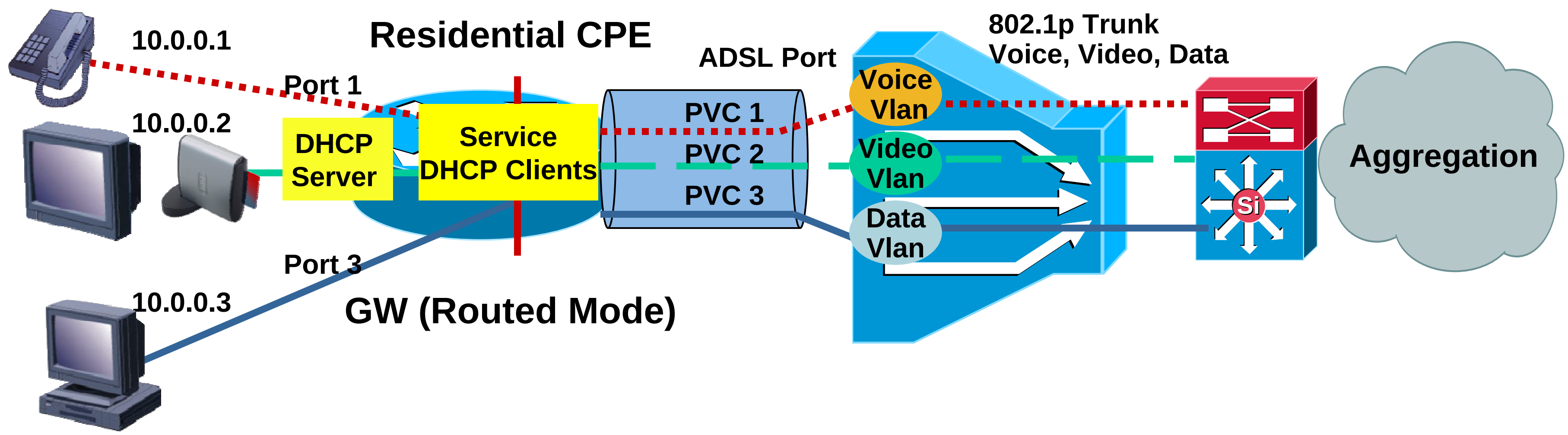
- CPE GW configured for bridge mode
- PVC per service from access device (i.e., DSLAM)
- DSLAM maps each service PVC to a service VLAN
- DHCP addresses allocated to each device (IP Phone, STB, PC) by DHCP server at head end
- CPE GW may support port-mapping (port to PVC) function

Bridged Mode—DHCP Address Allocation



- Each device (PC, IP Phone, STB) has internal string used in DHCP Option 60
- DHCP request forwarded to DHCP server via IP helper address
- DHCP server allocated addresses based on giaddr and DHCP Option 60

Home Networking Models
CPE GW as Routed Mode



- CPE GW configured for routed mode (RFC 1483)
- CPE GW must support L3/NAT functionality using external transport client, and service mapping functions
- DHCP addresses allocated to service client on CPE GW (voice, video, data)
- Local DHCP server on CPE GW to allocated local addresses to devices (IP phone, STB, PC)
- Private addresses (i.e., 10.0.0.x) NAT mapped to proper service client
- CPE GW must support NAT application layer gateway and IGMP snooping

Security

Common Security Recommendations
How to Secure the Network Against Attacks

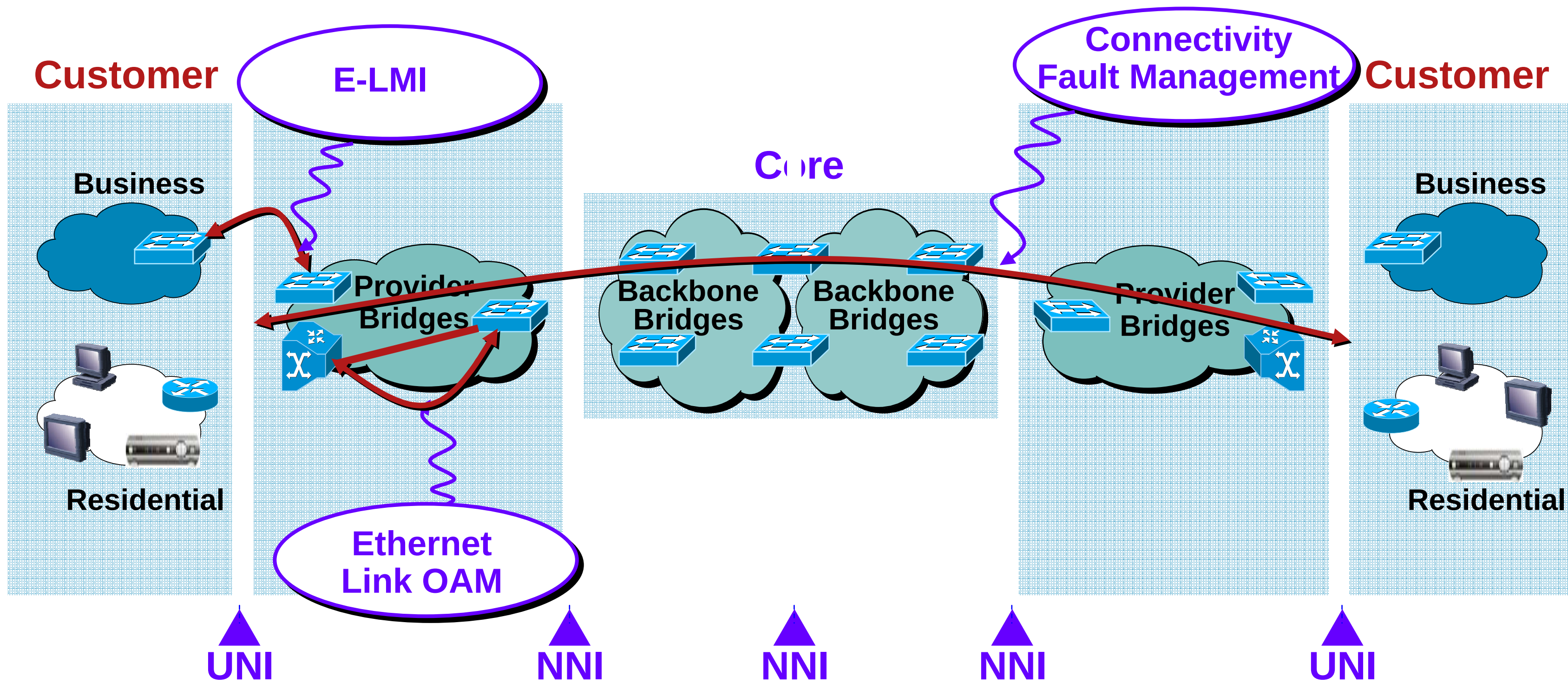
Leading Practice Category	Examples	Protects Against Threats
Disable Unnecessary Services	ICMP redirects, CDP, IP Source Routing	Reconnaissance, Denial-of-Service
Control Device Access	TACACS+, Radius, Password Encryption	Unauthorized Access
Secure Ports and Interfaces	Disable unused interfaces, VLAN Pruning	Reconnaissance, Denial-of-Service
Secure Routing Infrastructure	MD5 Authentication, Route Filters	Denial-of-Service
Secure Switching Infrastructure	Port Security, Storm Control	Denial-of-Service
Control Resource Exhaustion	Control Plane Policing (CoPP), Hardware-based Rate Limiters	Denial-of-Service
Policy Enforcement	uRPF, iACLs	IP Spoofing, Denial-of-Service
DSLAM	MAC Forced Forwarding, Virtual MACs, DHCP Option 82, IGMP Whitelist	Reconnaissance, MAC Spoofing, Theft-of-Service

Residential Access Leading Practices
How to Secure Users and Services

Goal	Features
Subscriber Identification	DHCP Option 60, DHCP Option 82
Subscriber Authentication	PPPoE or Web Portal (Using Radius)
Subscriber Isolation	MAC Forced Forwarding on DSLAM
Prevent MAC Address Spoofing	Virtual MAC Addresses on DSLAM
Prevent Theft of BTV Service	IGMP Whitelist on DSLAM

Network Management and OAM

Operation and Maintenance



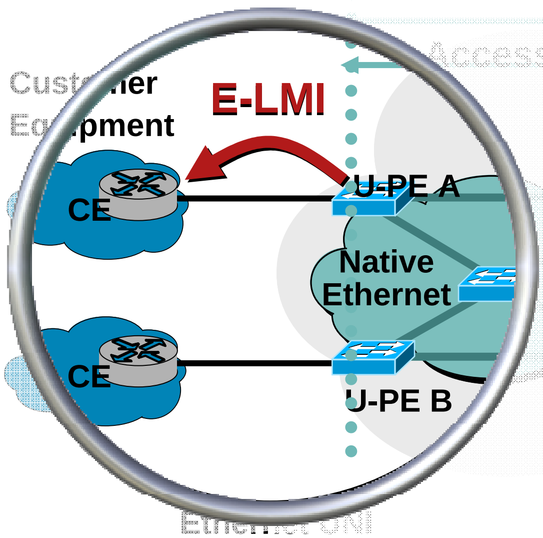
METRO Ethernet Forum — E-LMI: CE configuration, L2 connectivity management

IEEE — Link-Layer OAM: Per Link OAM

ITU, IEEE — Connectivity Fault Management: Per Service/VLAN OAM

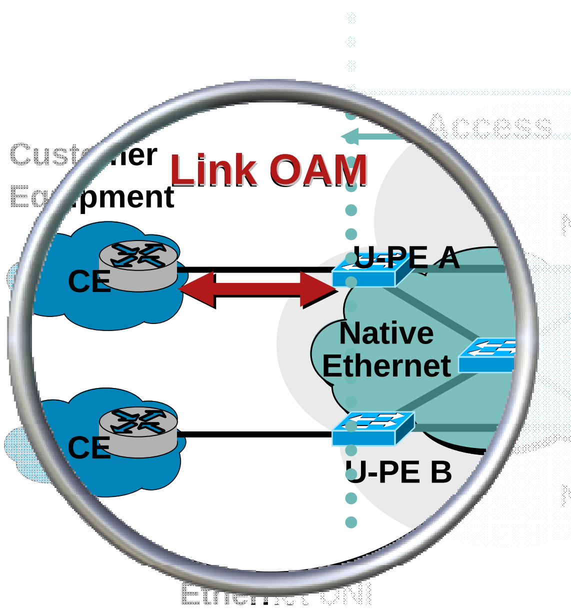
ITU, METRO Ethernet Forum — Performance Management

Ethernet LMI



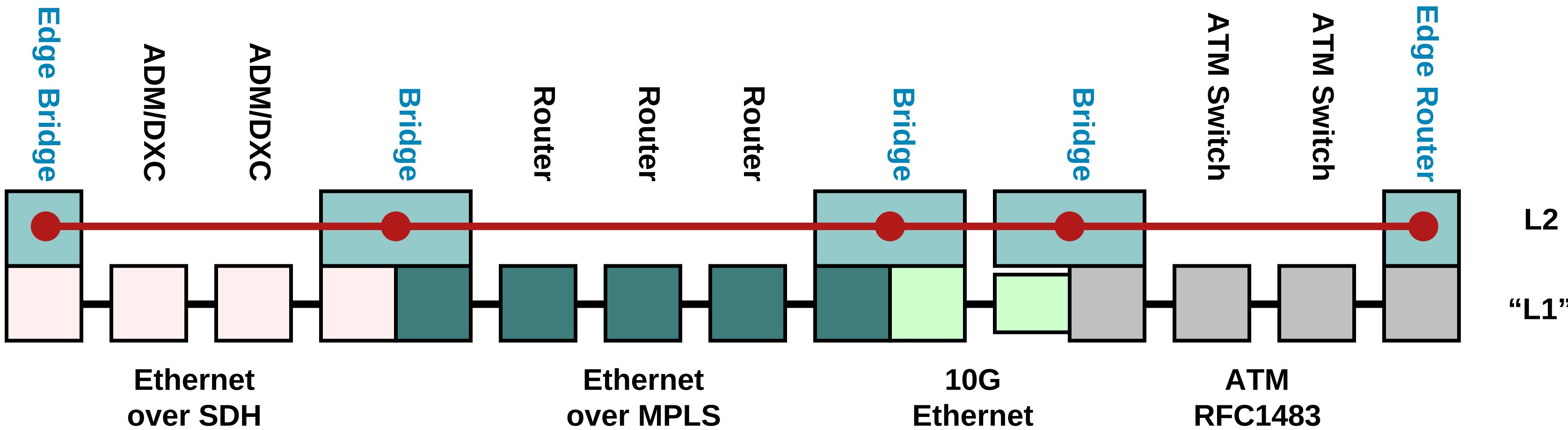
- Enables service providers to reduce customer configuration errors, as well as improve Ethernet Virtual Circuit (EVC) performance by shaping on CE egress
- Three Types of Information
  - EVC Status
  - Configuration Data
  - Provisioning Data
- Technical approach based on Frame Relay LMI
- LMI is complementary to OAM

Link OAM (IEEE 802.3, clause 57)



- Maintain consistency of an Ethernet transport connection (per link, or "physical" OAM)
- Address three key operational issues:
  - Link Monitoring
  - Fault Signaling
  - Remote loopback
- Operates on a single point-to-point link between 2 devices
- Slow protocol using packets called OAMPDUs which are never forwarded
- Standardized: IEEE 802.3, clause 57

Connectivity Fault Management (CFM) IEEE 802.1ag



- CFM is Ethernet standard frames, not MPLS, ATM, or SONET frames, cells, or sub-Ethernet control information
- May be per-service or per-wire. Passes end-to-end through bridges
- Only bridges see CFM because bridges are the only active relay functions that exist
- Three types of Messages:

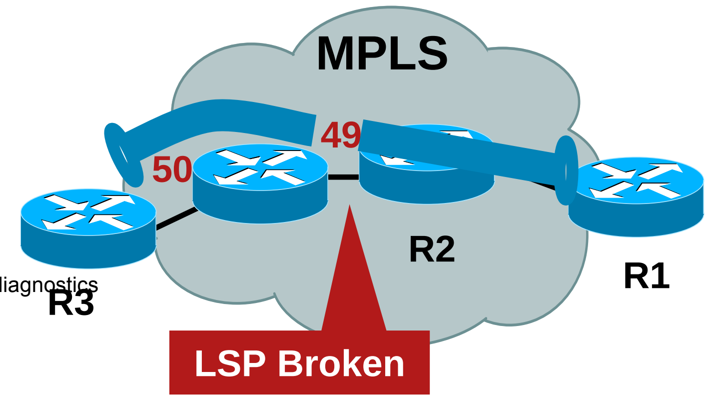
  Continuity Check Message (CCM)

  Loopback Message (LBM), Loopback Reply (LBR)

  Link Trace Message (LTM), Link Trace Reply (LTR)

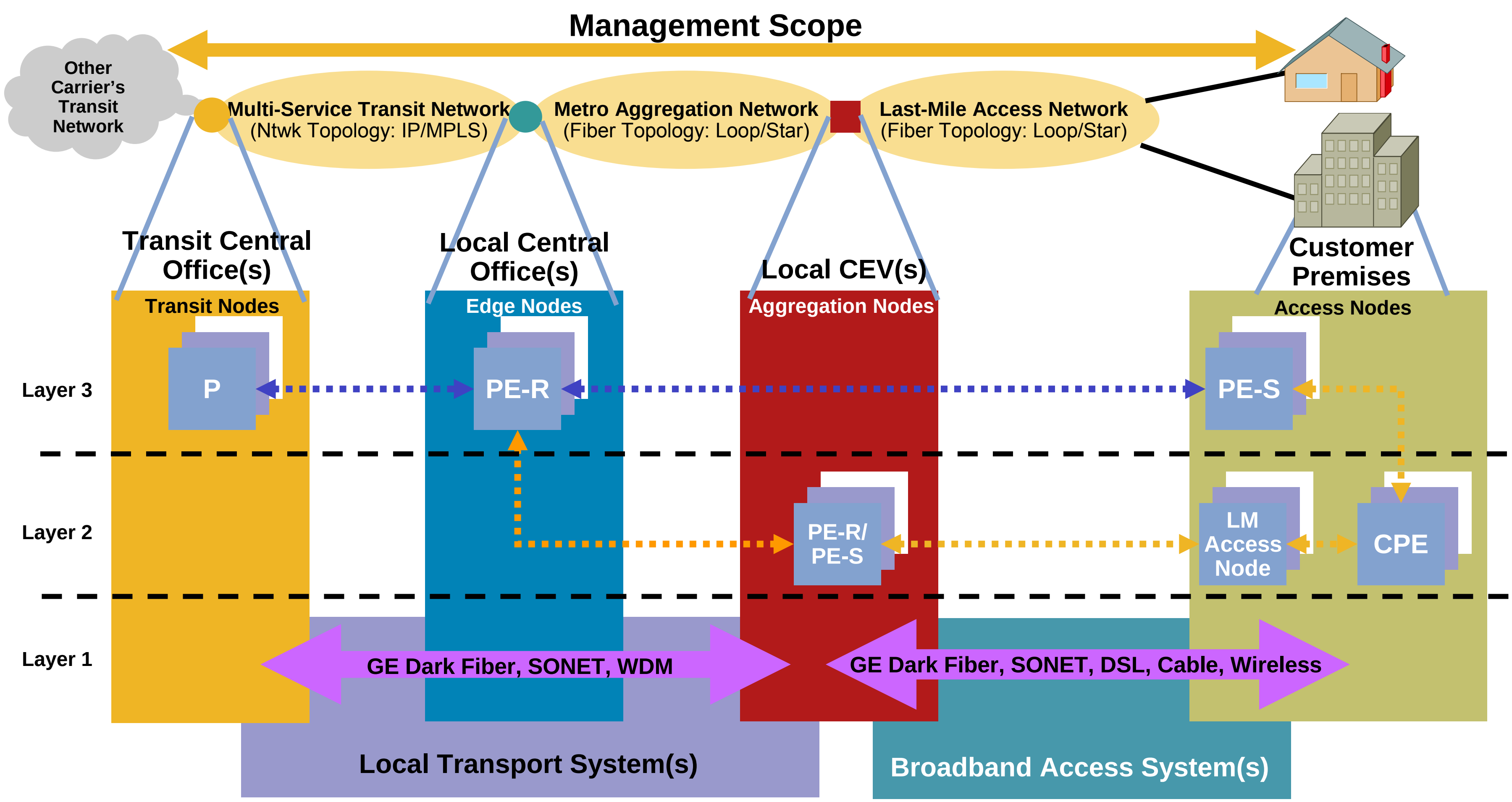
MPLS OAM

- A broken LSP will affect end to end connectivity and services, it is difficult to troubleshoot an MPLS failure:
  - Requires the operator to do manual/hop-by-hop work
- Various reasons for an LSP to break:
  - Broken LDP adjacency
  - MPLS not enabled (globally or per interface)
  - Mismatched labels
  - Software/hardware corruption—
- MPLS OAM facilitates and speeds Up troubleshooting of MPLS failures
- Principle…similar to traditional (ICMP based) tools:
  - LSP Ping: based on echo request and echo reply
  - LSP Trace: packets with incremental TTL
  - Virtual Circuit Connection Verification (VCCV): end-to-end fault detection and diagnostics for an emulated PW service
- LSP ping/trace do NOT use ICMP packets:
  - New packet format specifically designed for MPLS OAM
  - IPv4 (IPv6) UDP packets with port 3503
  - UDP packets : MPLS echo-req. or MPLS echo-reply



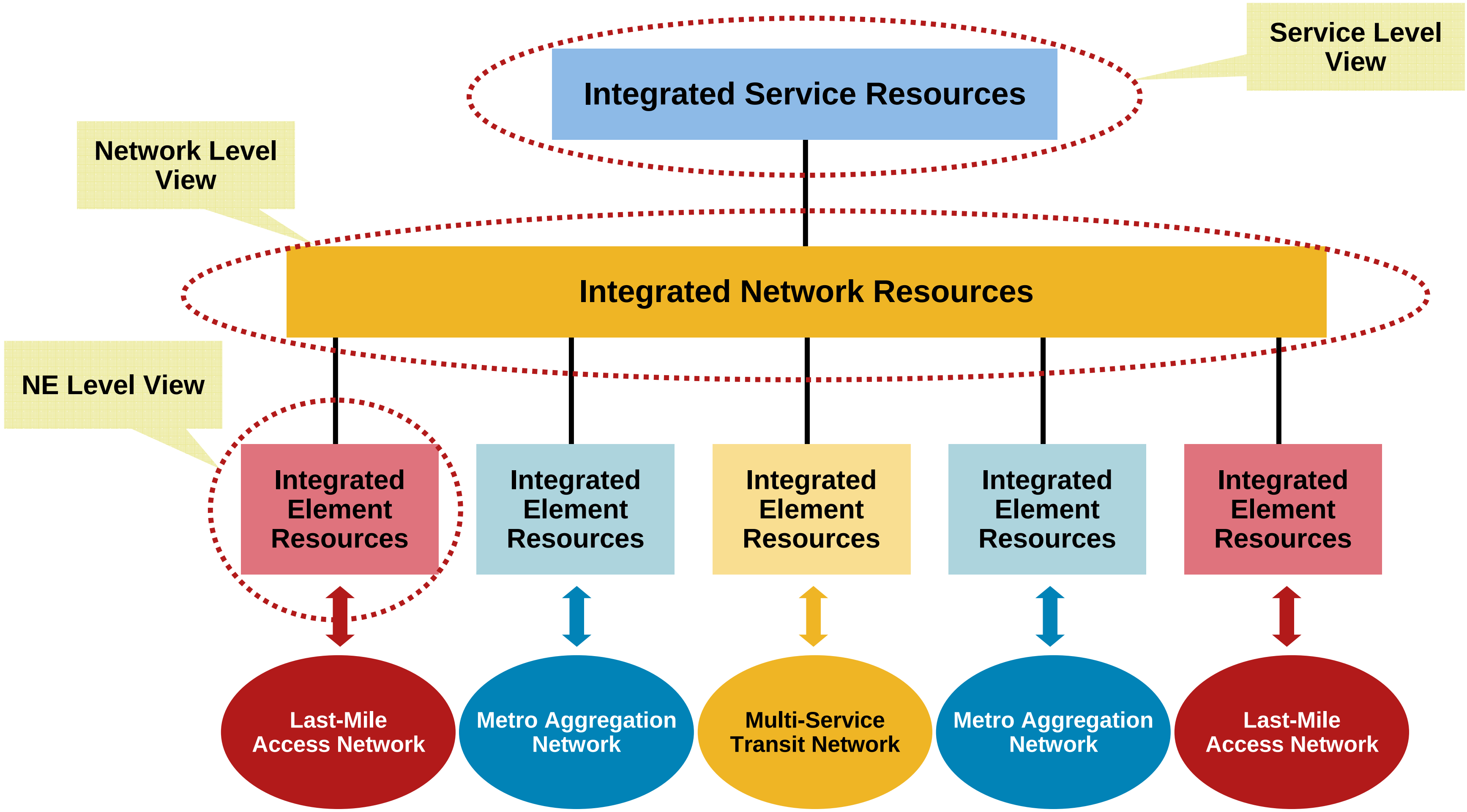
Converged Ethernet-Based Services

Requires End-to-End Resource Management Scope



Converged Ethernet-Based Services

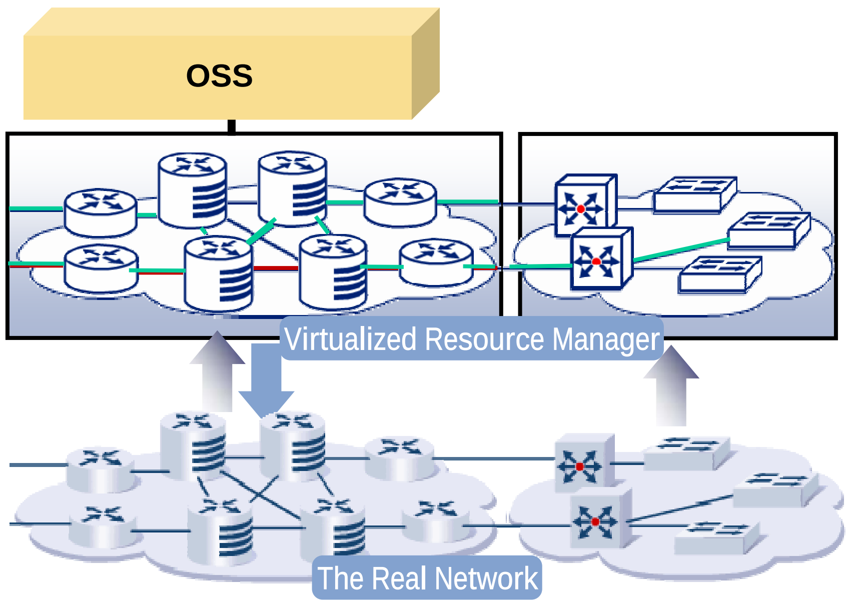
Drives Integration of Element, Network, and Service Management



Implementation Strategies for the Management of Converged Ethernet-Based Services

Real-Time Network Virtualization

- Requirements
  - Dynamic network abstraction's for OSS interaction
  - Auto-discovery of device and network inventory, network topology and service trails
- Benefits
  - Topology-based root cause and fault analysis
  - Highly flexible end-to-end service activation
  - Reduction of opex for service fulfillment and assurance



Converged Services Drives a Paradigm Shift from Hierarchical Static EMS/NMS to Reactive Virtualized Pro-Active Resource Management

Summary

Summary

- Converged network delivering residential and business service offerings
- Flexible transport architecture (Ethernet/IP and MPLS/IP)
- Flexible service insertion points
- 10GE aggregation to address massive scale requirements
- Sub-second convergence for real-time application
- Integrated network management and OAM functional tools

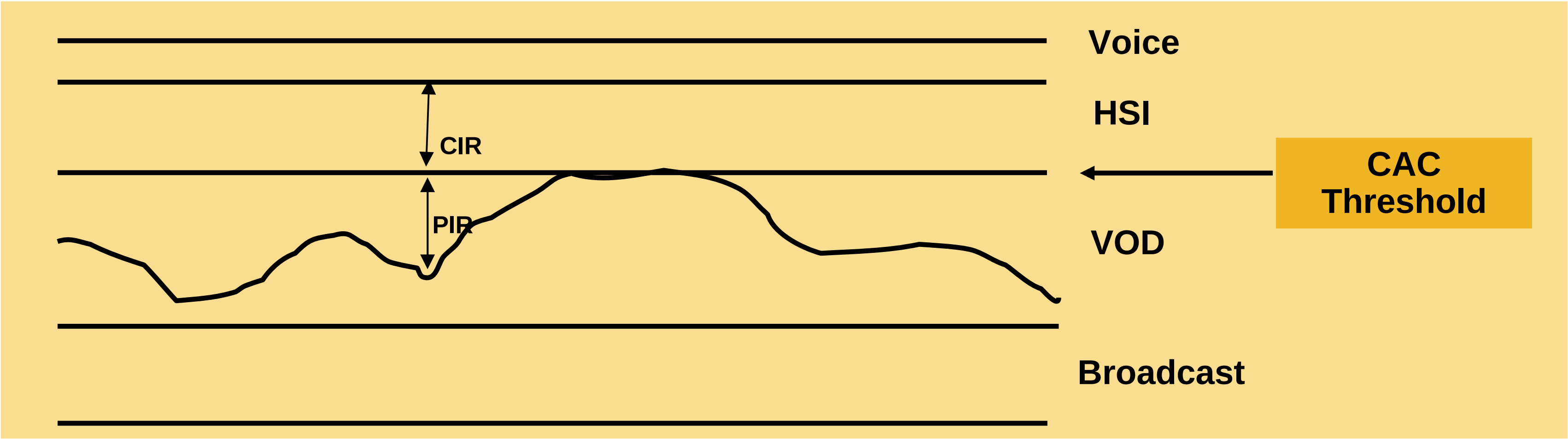
Q and A

Backup Reference Slides

Admission Control

Why Is Admission Control Essential for Video?

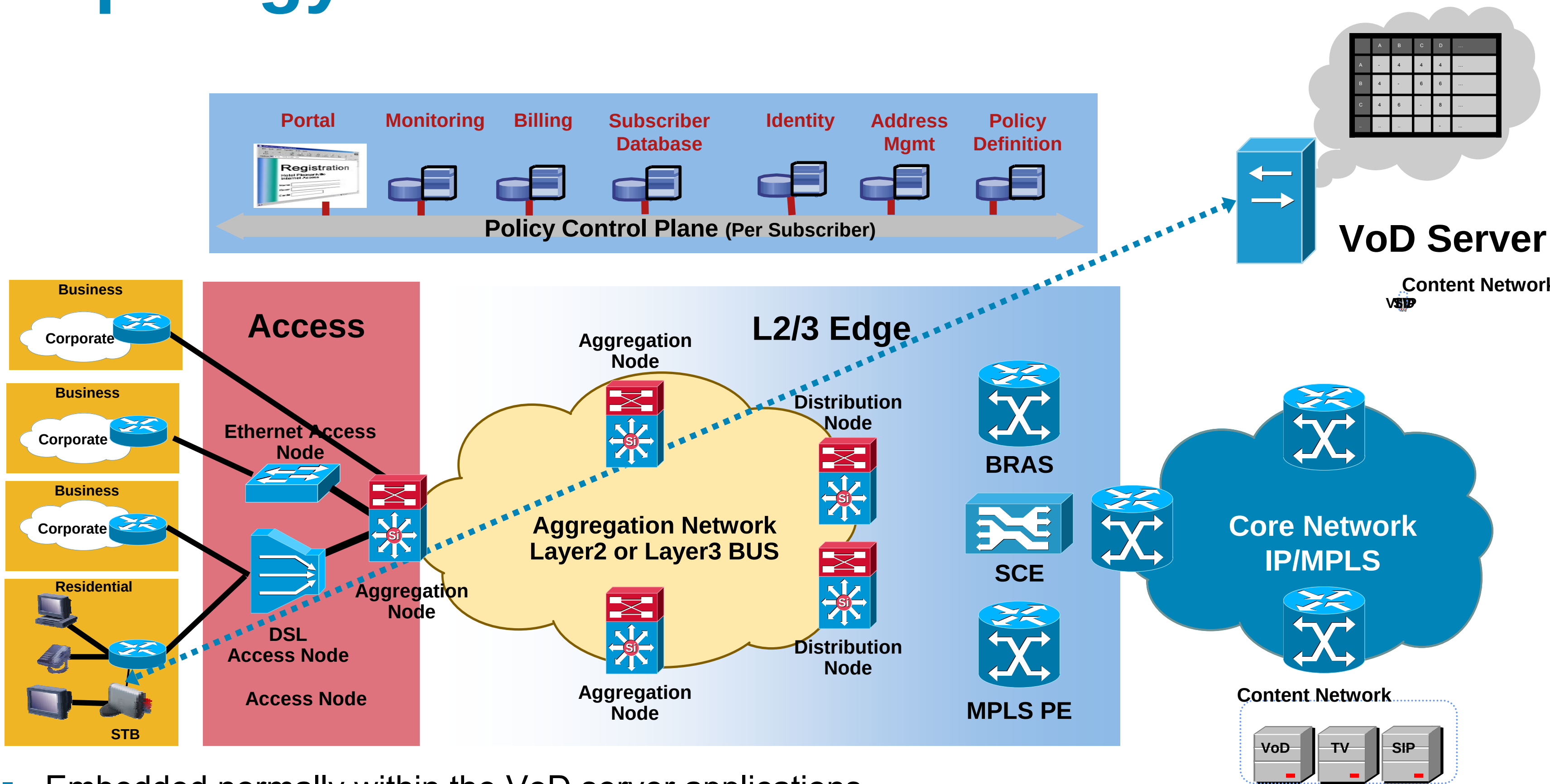
- Per-service QoS for broadcast video and VOD
  - Network must deliver 10-6 loss requirement to support video QoE
  - Per-sub QoS for video through BRAS function not optimal—can't shape/drop video packets
  - Per service QoS optimizes quality and operational efficiency
- VOD connection admission control
  - CAC VOD into network otherwise 1001st stream could degrade service of all users
  - Don't admit if results in dropped packets for new stream or any existing streams
  - If sub consuming near DSL line rate due to multiple active set tops in the home, DSLAM will drop HSI packets and invoke TCP backoff



Triple Play Services CAC Requirements

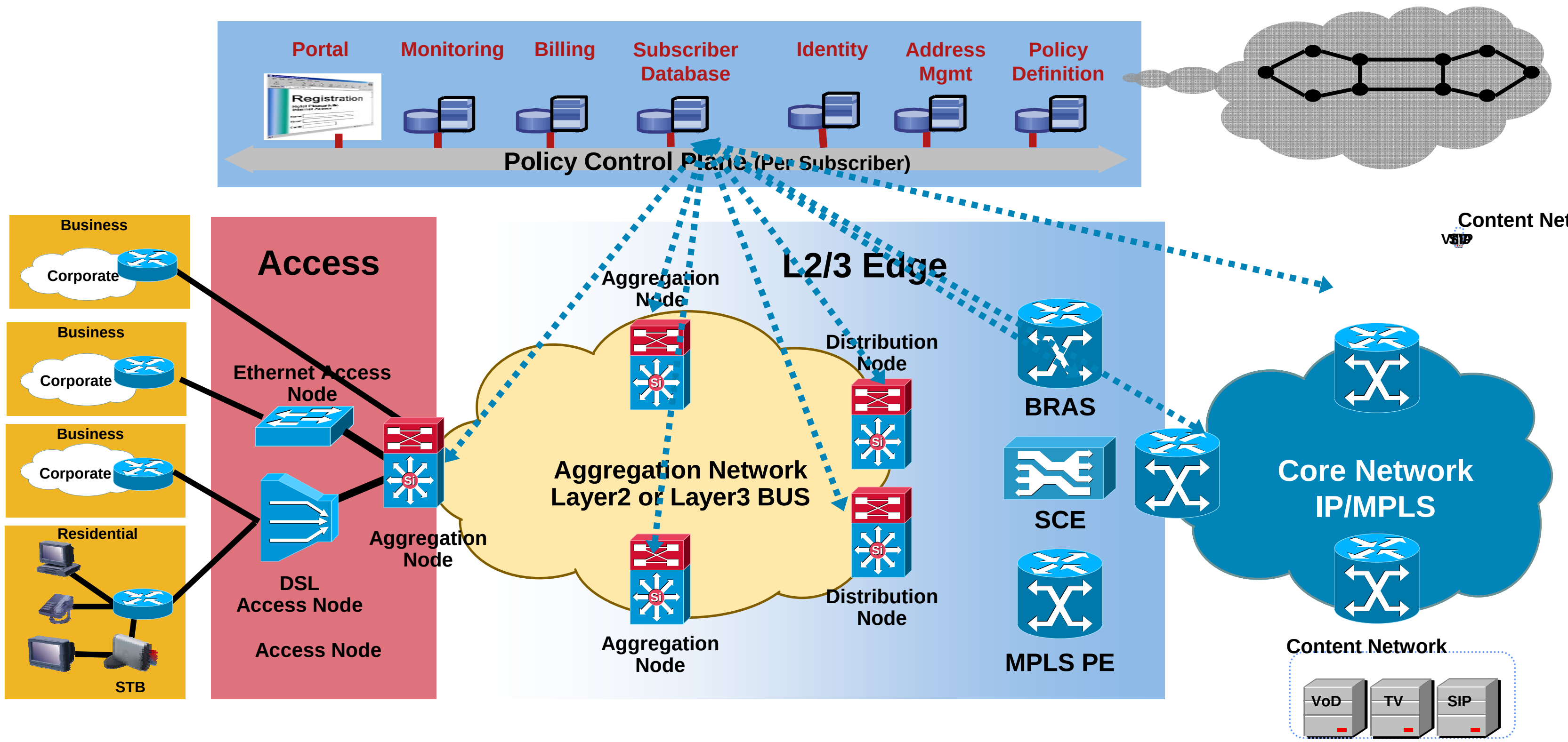
- VoIP telephony service
  - Subscriber line: no CAC required
    - The number of calls generally limited at the application level
  - Aggregation network: no CAC required
    - Generally provisioned with sufficient class bw to cope with peak during working and failure case
- TV broadcast service
  - Subscriber line: CAC required
  - Aggregation network: no CAC required
    - Generally provisioned with sufficient class bw to cope with peak during working and failure case
- Video on demand service
  - Subscriber line
    - For fixed number of channels per subscriber line: no CAC required
    - For variable number of channels per subscriber line/variable bandwidth cases: CAC required
  - Aggregation network: CAC required
    - Potential for congestion both in working and network failure cases

Topology-Unaware Off-Path CAC



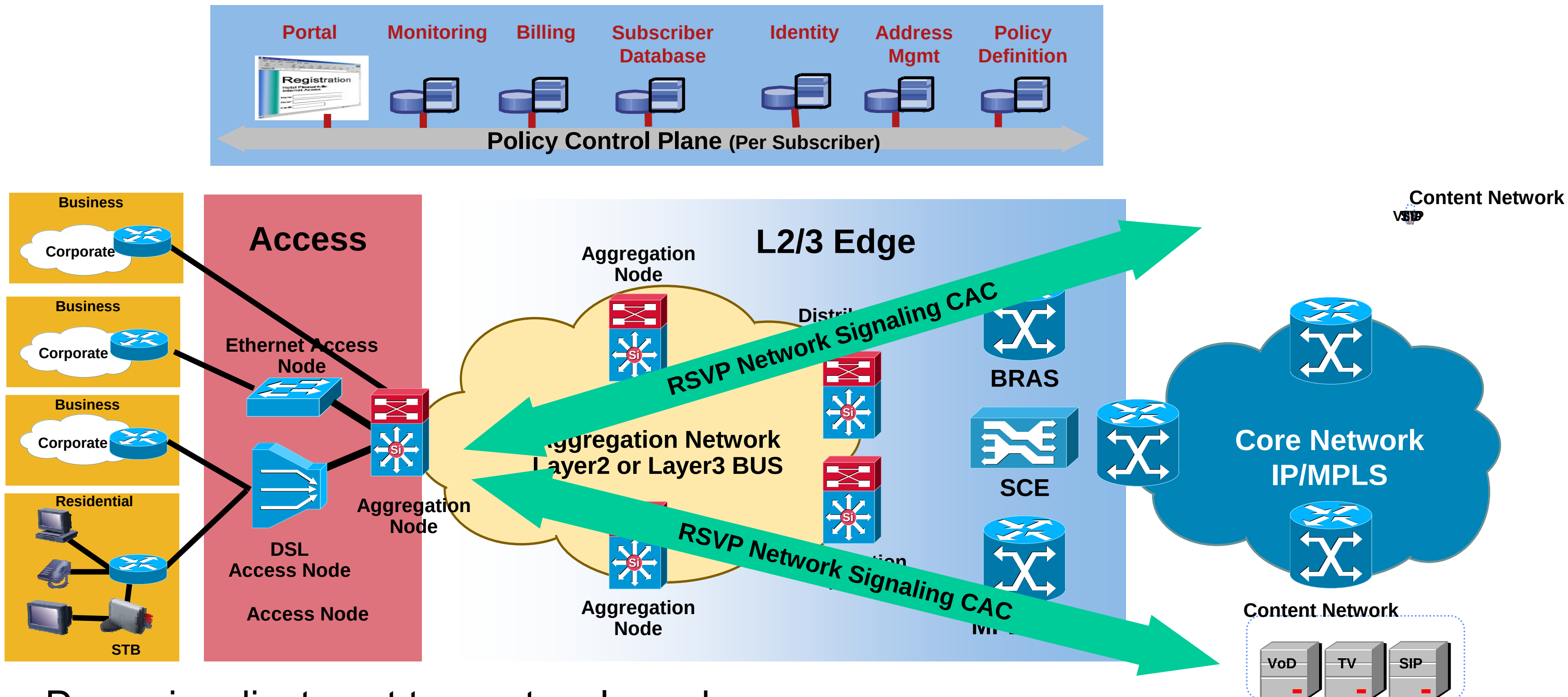
- Embedded normally within the VoD server applications
- CAC decisions not synchronized with the network topologies
- VoD server maintains static table of available bandwidth per site, region
- CAC mechanisms applicable to very simple network topologies or solely on the subscriber DSL line

Topology-Aware Off-Path CAC



- CAC decision outsourced to policy server/bandwidth manager
- Similar to the "RACS/RACF" function of ETSI TISPAN QoS architecture
- Policy server interaction with the network for topology synchronization
- Requires systems integration with VoD applications, network elements, NMS

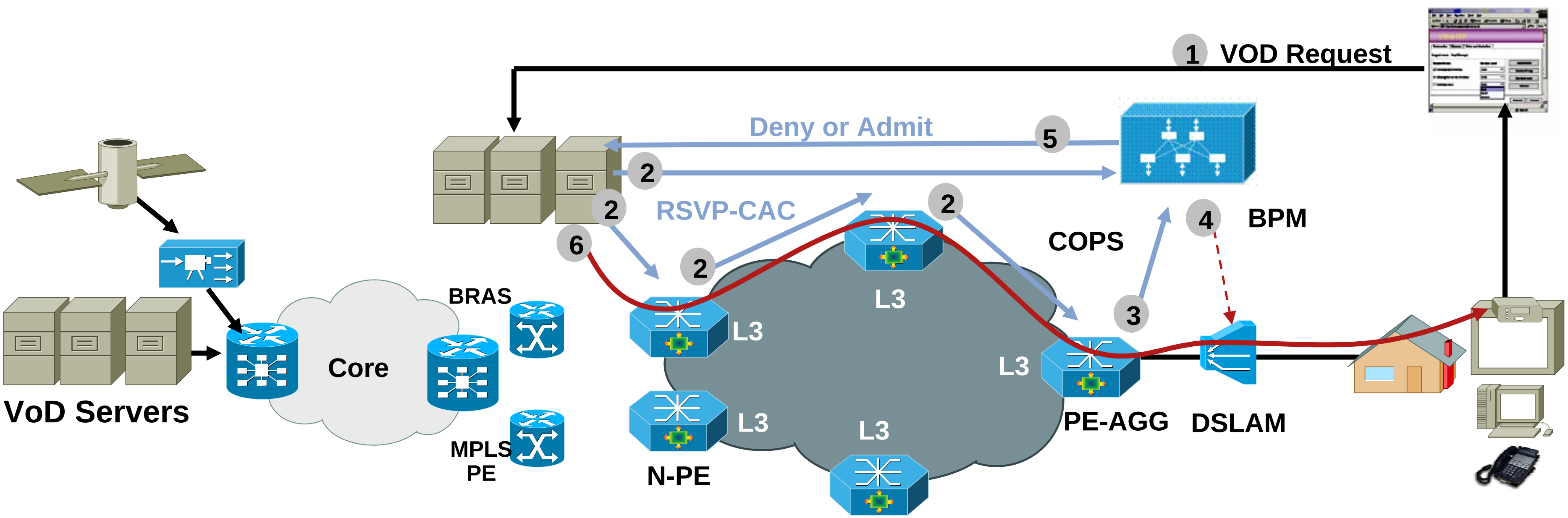
Topology-Aware On-Path CAC



- Dynamic adjustment to any topology change
- Requires network level connection admission control signalling:
  - RSVPoDiffserv in the network
  - RSVP support on video of demand pump
  - RSVP aggregation over MPLS TE where MPLS is used

Integrated Video CAC

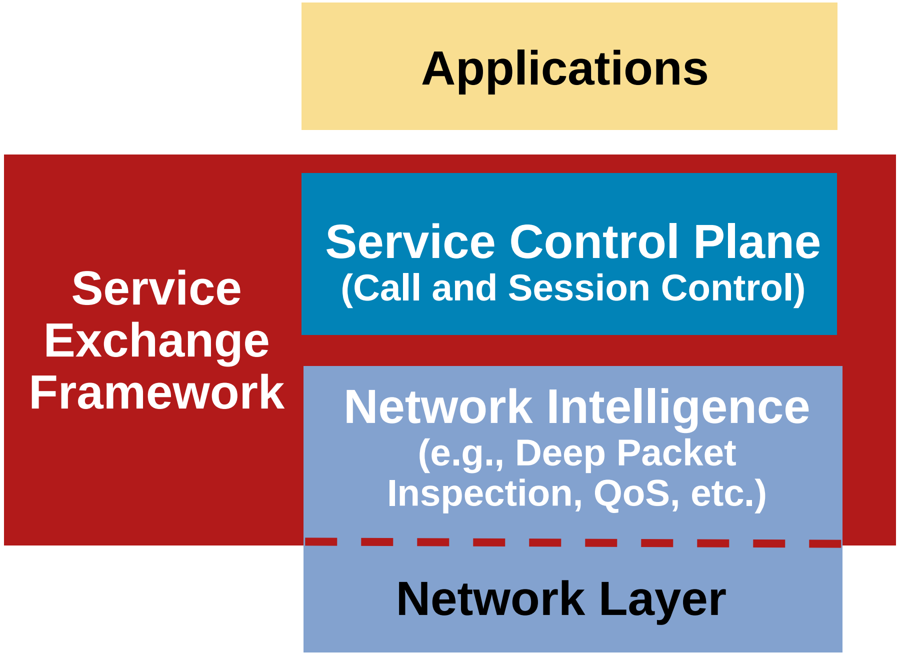
- Integrated video CAC approach combines two methods
- VOD stream will be denied if business rules of either fail
- Prioritize blocking of free VOD vs. pay VOD in network failure scenarios



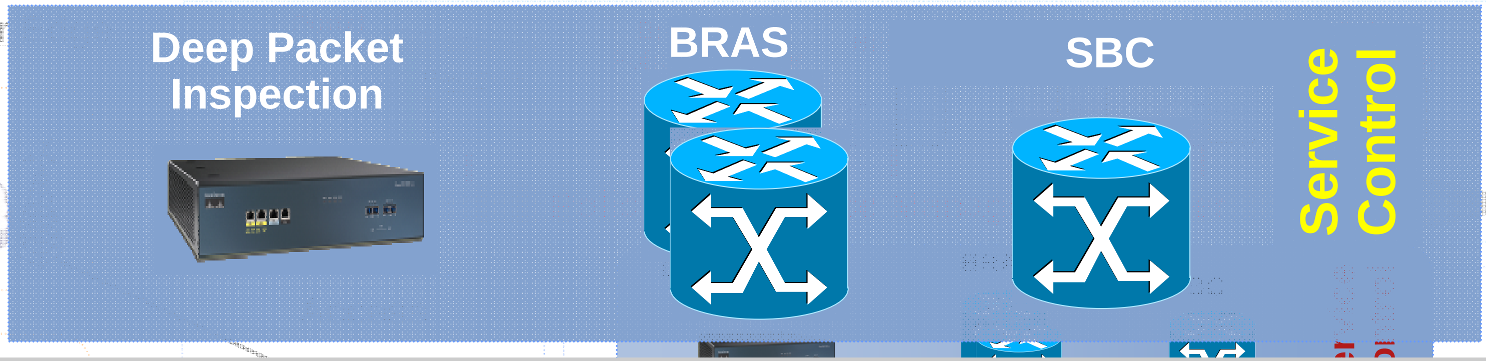
Policy Control

Service Exchange Framework

- Define and evolve the service control plane to deliver the service control attributes to enable SP application delivery
- Add instrumentation to the service control plane to control existing network intelligence capabilities
- Enhance and extend network intelligence to enable the service control plane (application-enabling infrastructure)
- Pull functions from the service control plane into network intelligence (where applicable and possible)



Next Generation Broadband Architecture
Service/Application Control Layer



Events occurring in the network trigger

Execution of rules in real time resulting in

Decisions that are enforced by

Dynamically configuring the network for service delivery

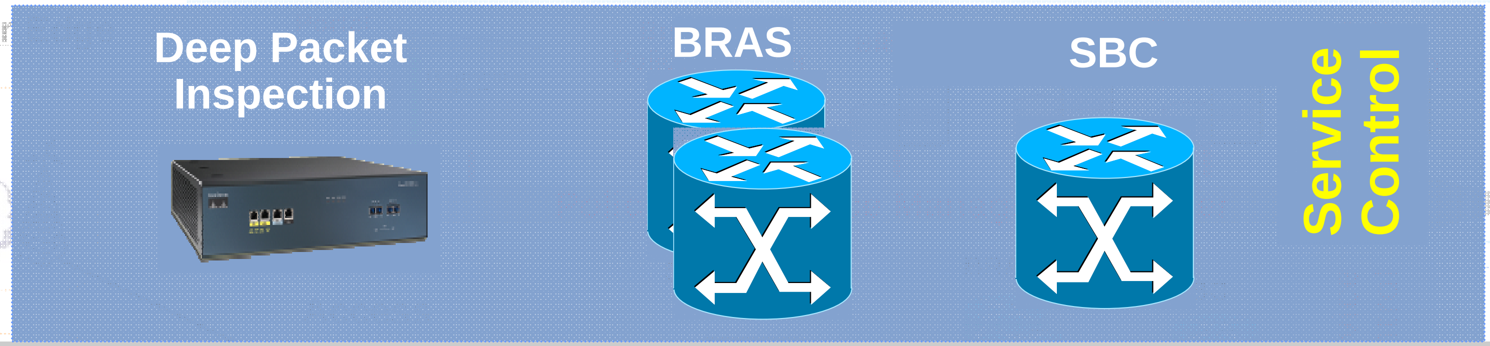
- Events include:

  User actions (Interaction with portals, network logon/logoff)

  Application services (IP telephony, Video services, P2P data)

  Network conditions (network outage, time-of-day, congestion

Next Generation Broadband Architecture
Service/Application Control Layer-Functions



- Service control—dynamic network provisioning

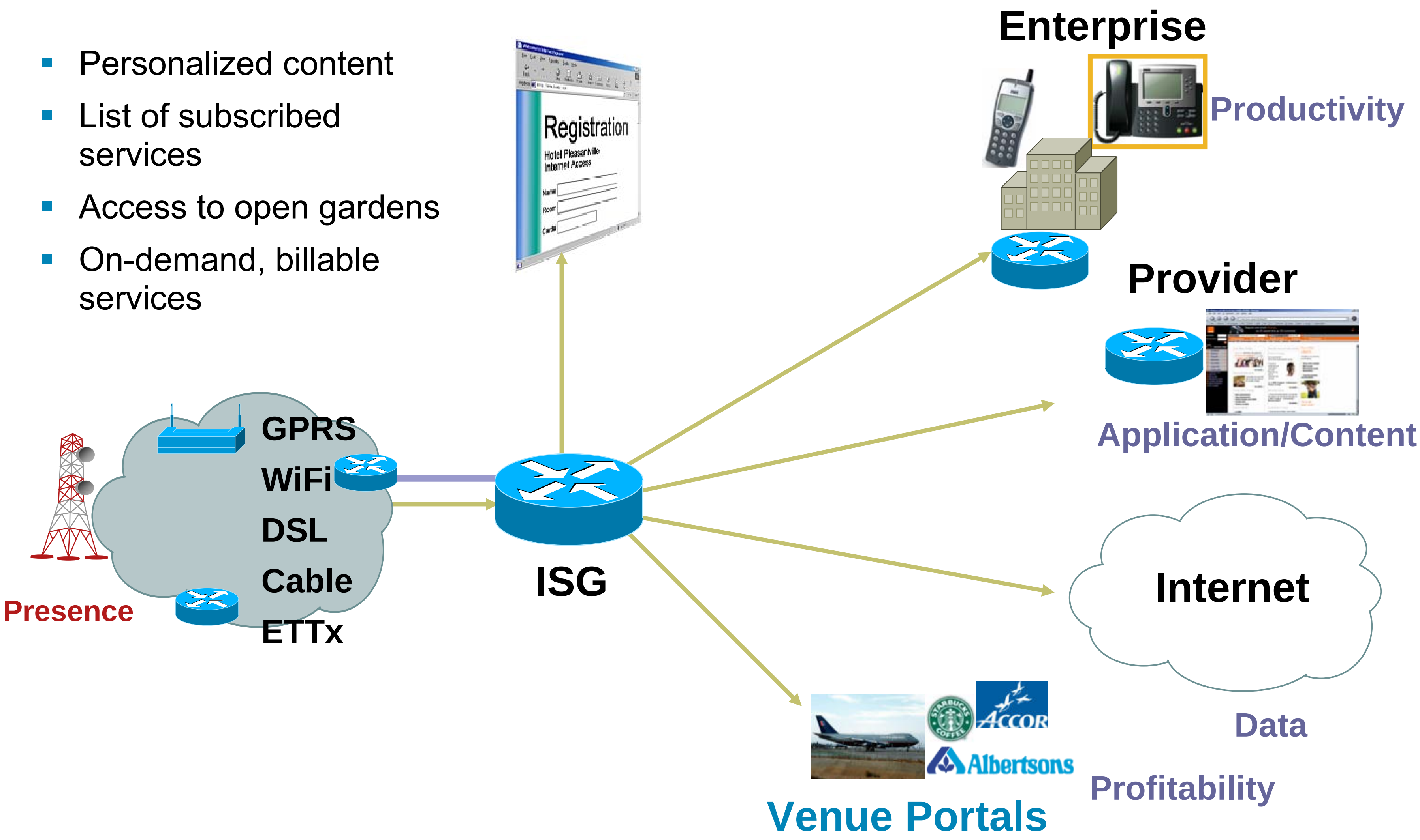
  Real-time management of QoS, peer-to-peer traffic, subscribers, services

- Admission control

  Manage network resources intelligently and efficiently

Dynamic Broadband Services with Intelligent Services Gateway

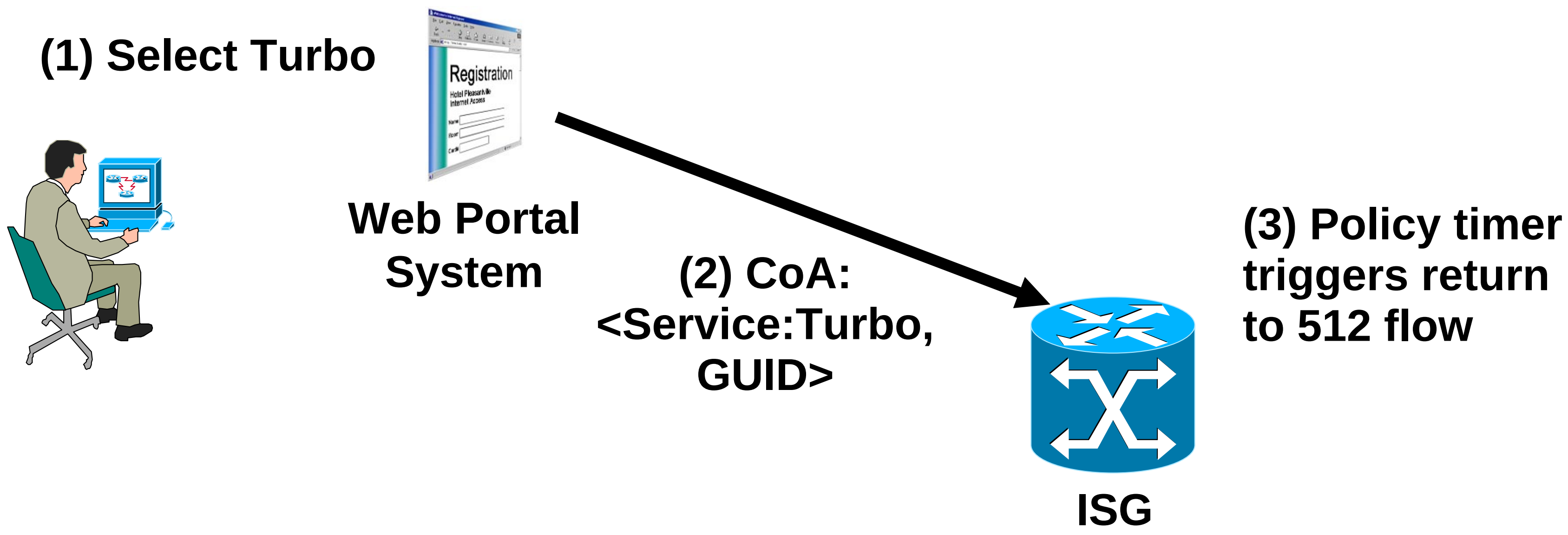
- Personalized content
- List of subscribed services
- Access to open gardens
- On-demand, billable services



Broadband Services Example: Turbo Boost

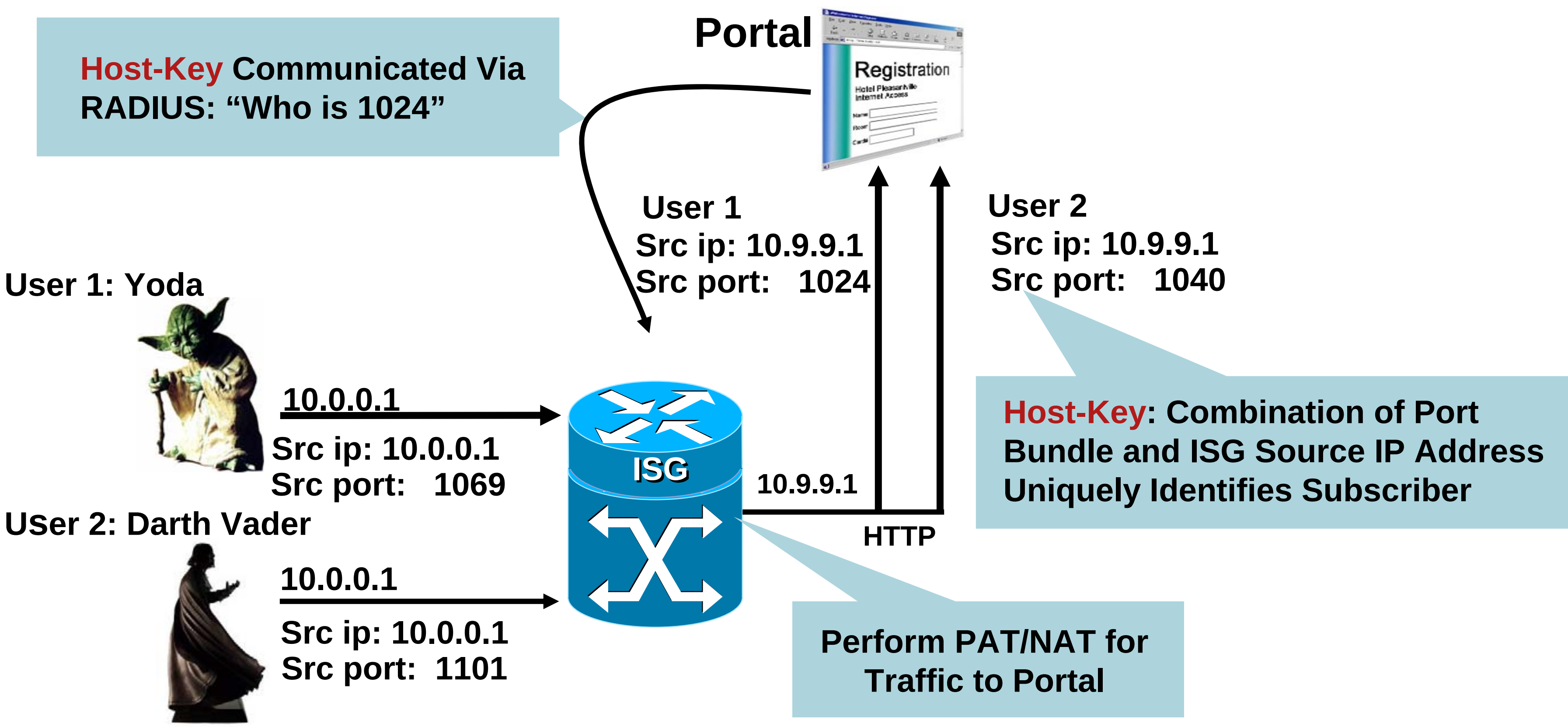
ISA Turbo Boost with a Timer

- User is connected by 512Kbps session
- He logs into service portal and selects turbo button
- His session gets upgraded to predefined 2048Kbps speed for fifteen minutes
- After timer expires, session returned to 512Kbps



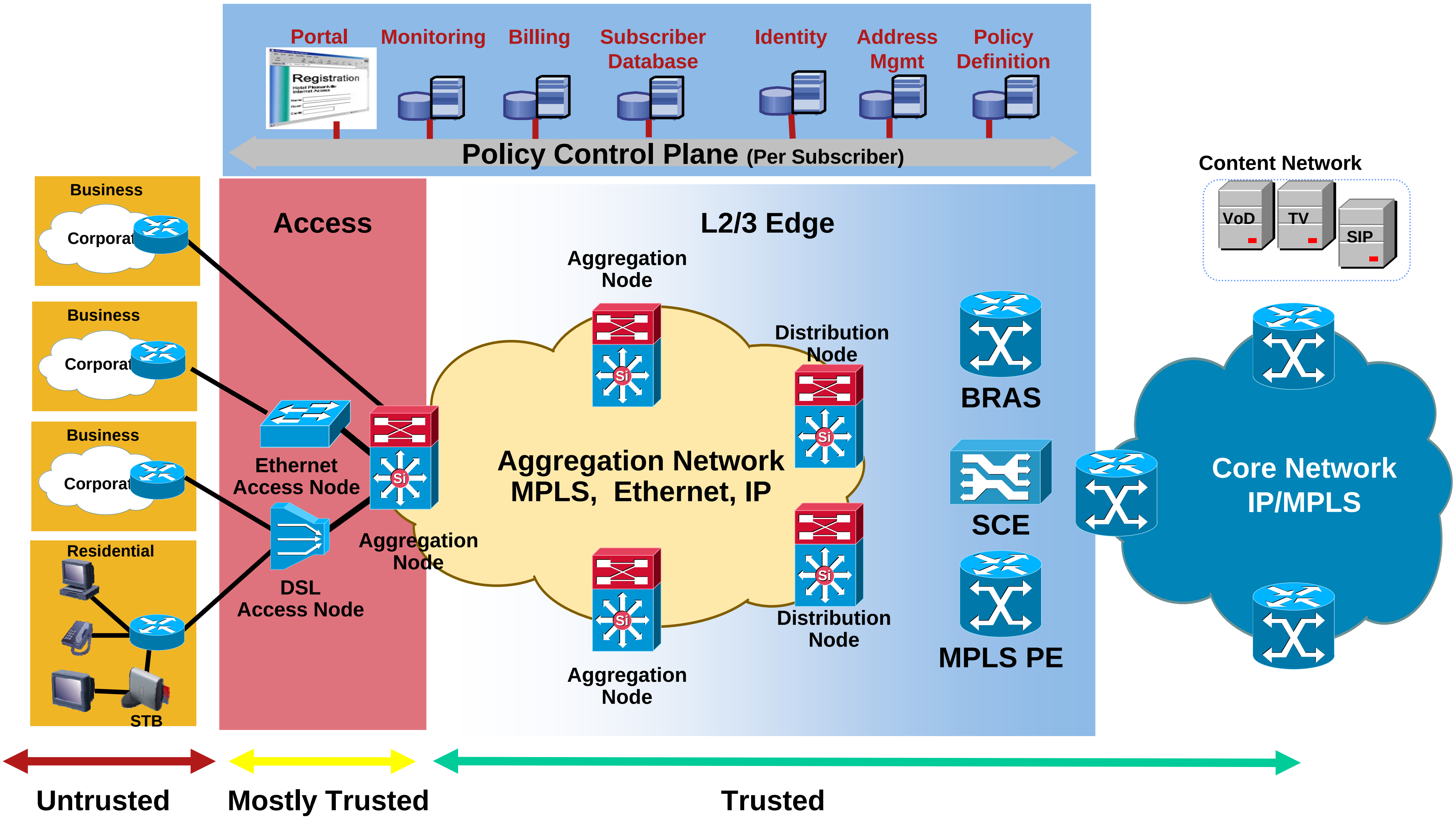
Identity Resolution Overlapping Host-IP Addresses?

ISA Single Sign on for Port Bundle Host Key



Security Reference Slides

Broadband Security Trust Model



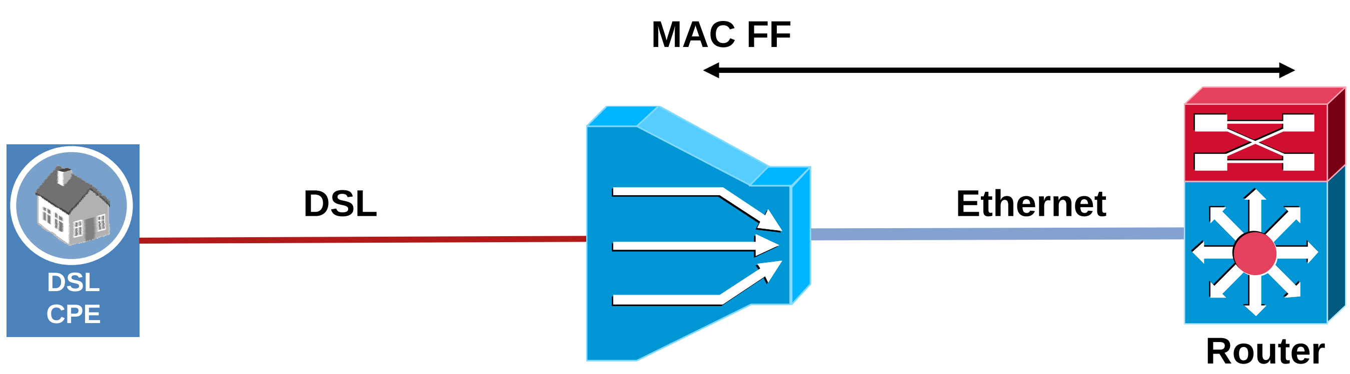
Layer 2 Leading Practices

How to Secure the Network Against Layer 2 Attacks

Attack	Defensive Features/Actions
MAC Attacks (CAM Table Overflow)	Port Security, Per VLAN MAC Limiting
Broadcast/Multicast Storm Attacks	Storm Control Thresholds
L2PDU DoS Attacks	Hardware Rate Limiters, Control Plane Policing, Storm Control Thresholds
VLAN Hopping, DTP Attacks	Disable Auto-trunking, Use Dedicated VLAN-ID for Trunk Ports, Set User Ports to Non-trunking, VLAN 1 Minimization/Pruning, Disable Unused Ports
DHCP Starvation Attack DHCP Rogue Server Attack	Port Security, DHCP Snooping, VLAN ACLs to block UDP port 68
Spanning Tree Attacks	BPDU Guard, Root Guard
ARP Man-in-the-Middle	Dynamic ARP Inspection

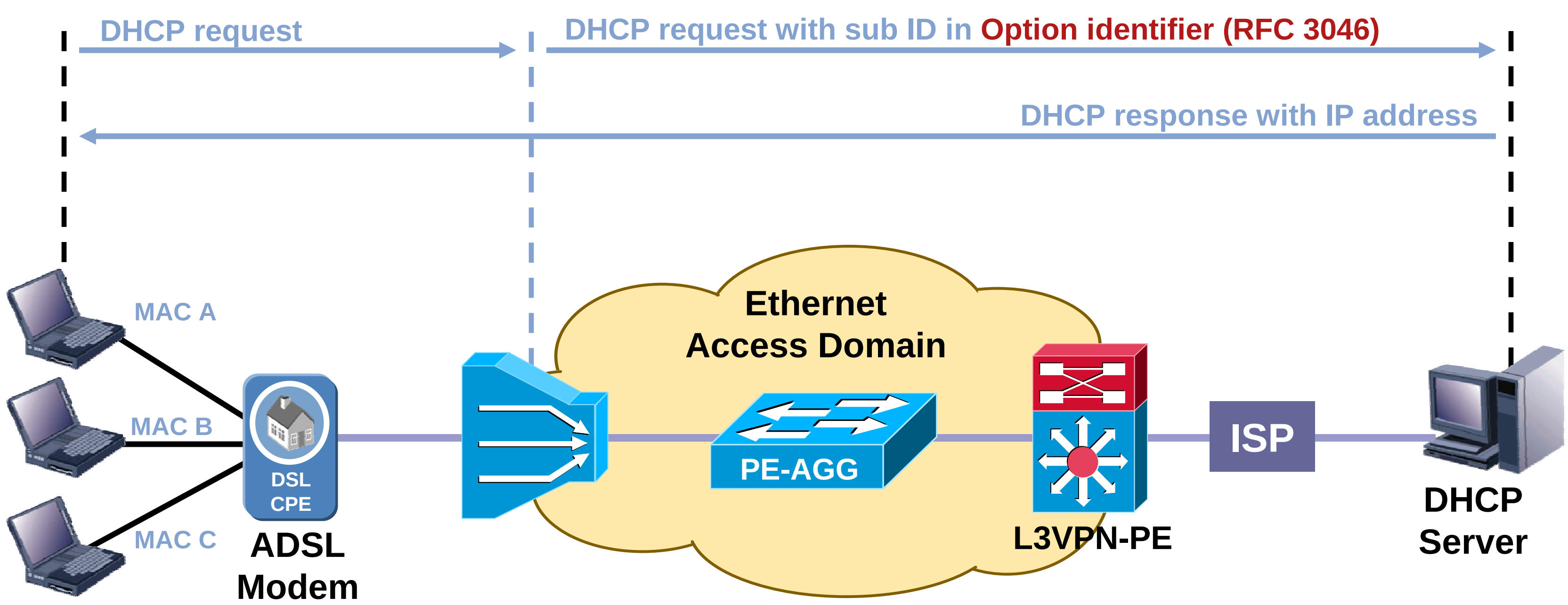
MAC Forced Forwarding

- Use MAC Forced Forwarding in the Ethernet DSLAM for user separation if using shared VLAN across DSLAM(s)
- DSLAM always responds to subscriber ARPs with BRAS (gateway) MAC
- DSLAM blocks all other traffic destined to MACs other than the BRAS



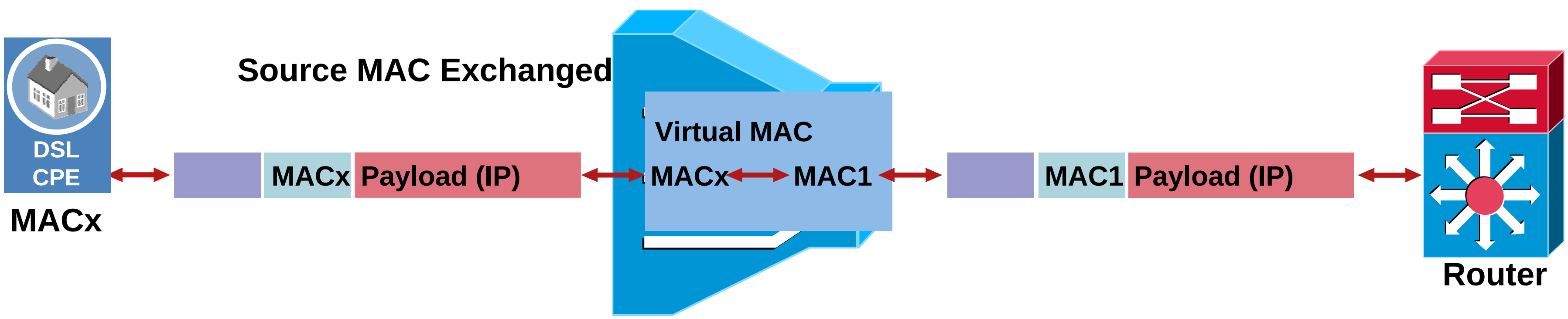
DHCP Option 82

- Use DHCP Option 82 in the IP DSLAM for end user traceability based on physical port
- DSLAM inserts option 82 with unique identifier of the location of the end user: DSLAM, DSLAM port, PVC or even a phone number



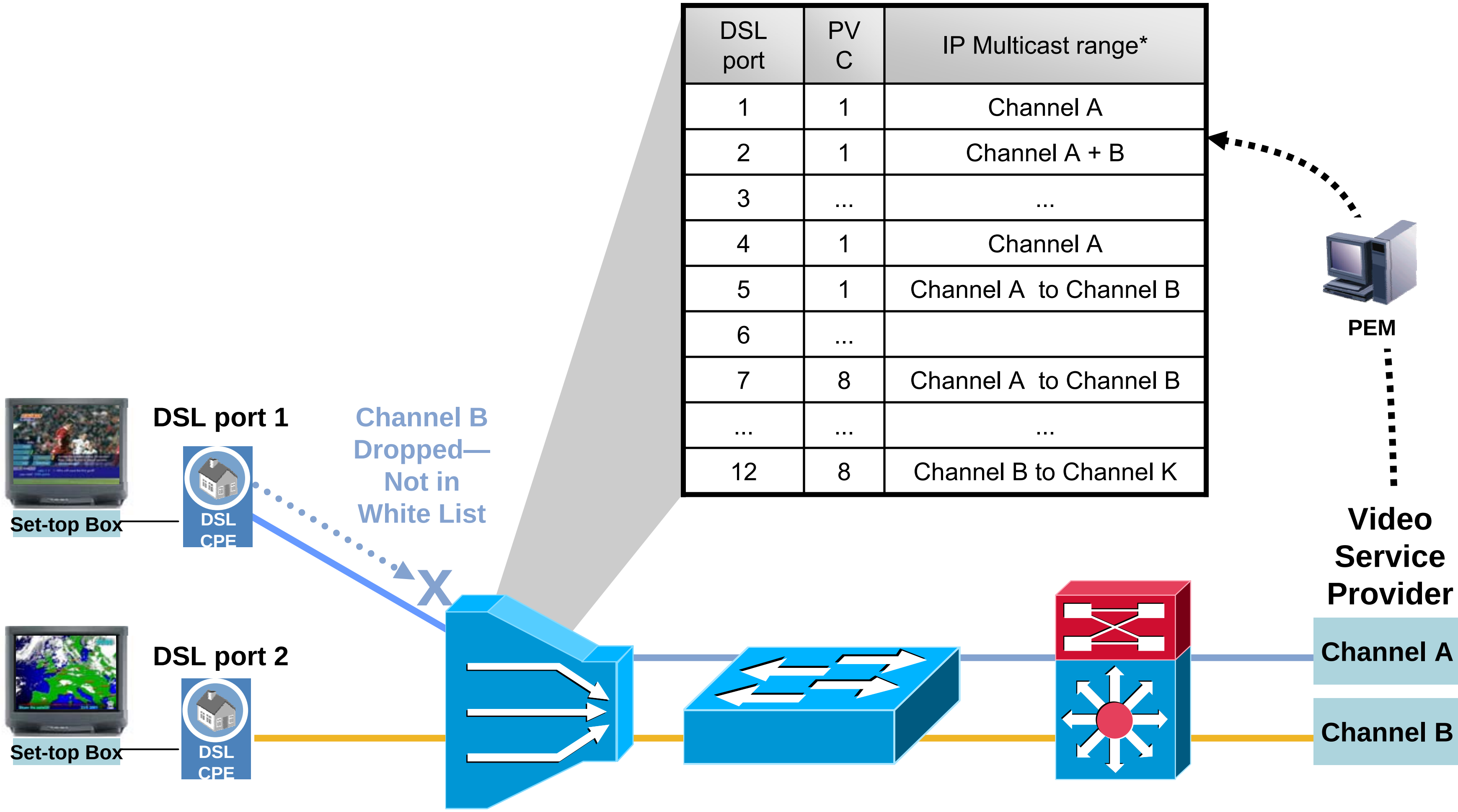
Virtual MAC (vMAC)

- Use Virtual MAC in the IP DSLAM for end user traceability based on physical port and PVC
- Prevents end users overloading the MAC address table in Ethernet switches, as well as MAC spoofing



IGMP Whitelist in Ethernet DSLAM

DSL port	PVC	IP Multicast range*
1	1	Channel A
2	1	Channel A + B
3	...	...
4	1	Channel A
5	1	Channel A to Channel B
6	...	
7	8	Channel A to Channel B
...	...	...
12	8	Channel B to Channel K



IGMP White list

***) IP Multicast Range is an IP Address Range**

Acronyms

Acronym	Description	Acronym	Description
ACL	Access Control List	NNI	Network-to-Network Interface
ARP	Address Resolution Protocol	N-PE	Network Provider Edge
CAM	Content Addressable Memory	OPEX	Operational Expenditure
CAPEX	Capital Expenditure	OTP	One-Time Password
CDP	Cisco Discovery Protocol	P	Provider (core router)
CoS	Class of Service	PAgP	Port Aggregation Protocol
DES	Data Encryption Standard	PDU	Protocol Data Unit
DHCP	Dynamic Host Configuration Protocol	PE-AGG	Provider Edge - Aggregation
DSCP	Differentiated Services Code Point	PON	Passive Optical Network
DTP	Dynamic Trunking Protocol	PVST+	Per VLAN Spanning Tree Plus
EAP	Extensible Authentication Protocol	SLA	Service Level Agreement
EAPOL	EAP Encapsulation Over LANs	STP	Spanning Tree Protocol
E-LAN	Ethernet LAN (service)	UDLD	Unidirectional Link Detection
EPL	Ethernet Private Line (service)	UNI	User Network Interface
EVPL	Ethernet Virtual Private Line (service)	U-PE	User Provider Edge
IPP	IP Precedence	VPLS	Virtual Private LAN Service
L2PT	Layer 2 Protocol Tunneling	VPN	Virtual Private Network
LACP	Link Aggregation Control Protocol	VPWS	Virtual Private Wire Service
MEF	Metro Ethernet Forum	VTP	VLAN Trunking Protocol

Acronyms

Acronym	Description	Acronym	Description
PW	Pseudowire	H-VPLS	Hierarchical Virtual Private LAN service
E-Line	Ethernet -Line	PIM	Protocol Independent Multicast
E-LAN	Ethernet – Local Area Network	SSM	Source Specific Multicast
EPL	Ethernet Private Line	RSTP	Rapid Spanning Tree Protocol
EVPL	Ethernet Virtual Private Line	STP	Spanning Tree Protocol
LCO	Local Central Office (Aggregation Node)	IGP	Interior Gateway Protocol
MCO	Metro Central Office (Distribution Node)	IGMP	Internet Group Management Protocol
MEN	Metro Ethernet Network	QoS	Quality Of Service
EWS	Ethernet Wire Service	EoMPLS	Ethernet Over MPLS
ERS	Ethernet Relay Service	BFD	Bi-directional Forwarding Detection
CAC	Call Admission Control		
VFI	Virtual Forwarding Instance		
STB	Set Top Box		
TE	Traffic Engineering		
FRR	Fast Re-Route		
MPLS	Multi Protocol Label Switching		
BRAS	Broadband Remote Access Server		
SCE	Service Control Engine		
SBC	Session Border Control		