Cisco live!

What You Make Possible

TOMORROW
starts here.

cisco

Residential Broadband Subscriber Aggregation and BNG Deployment Models

BRKSPG-2303

TOMORROW starts here.

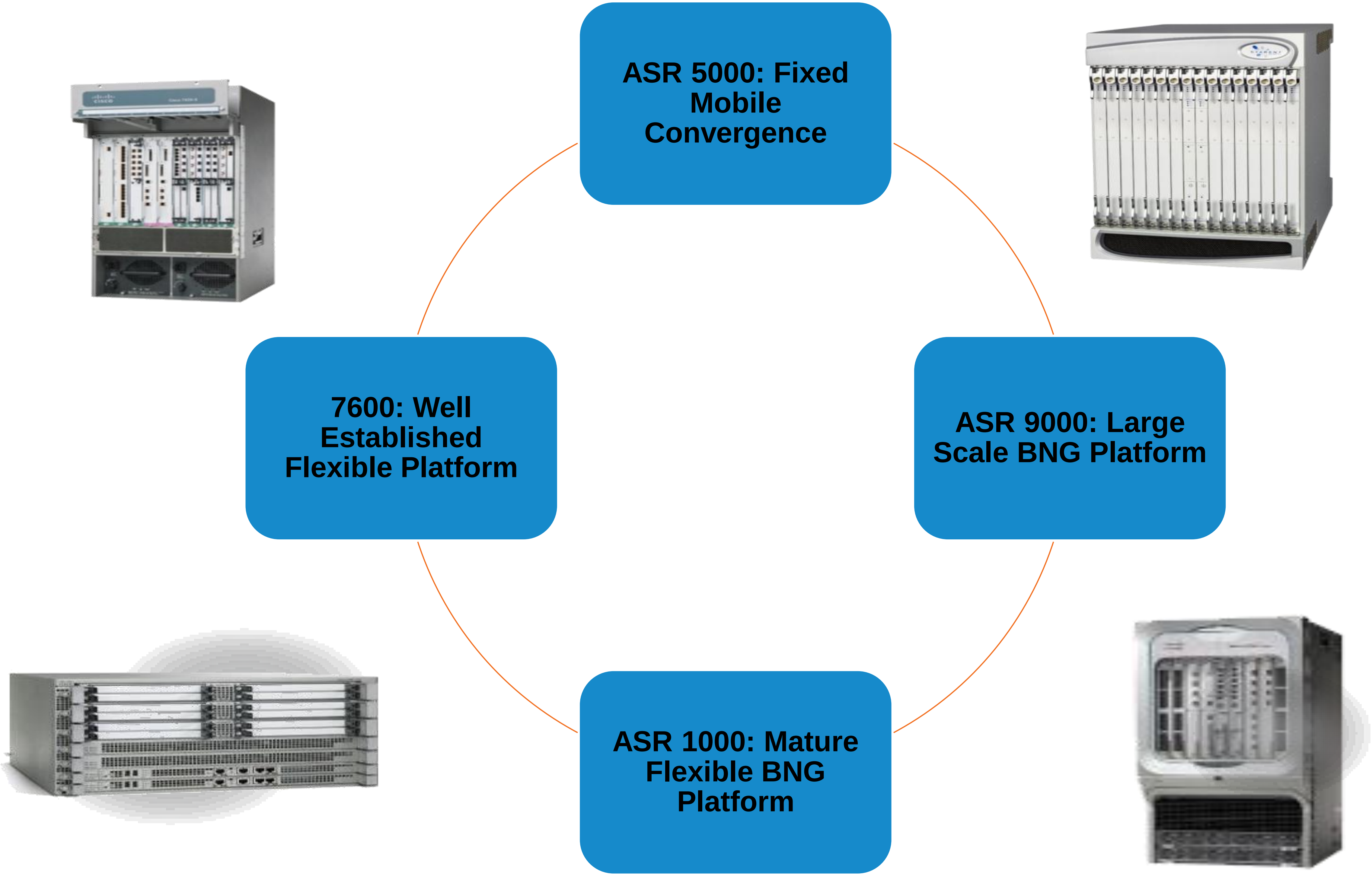
Agenda

- Service Provider Networks Overview
- Access Network Evolution
- Aggregation Network Evolution
- Subscriber Access Protocol Evolution
- Aggregation Service Delivery Models
- Edge Network Architectures
- IPv6 Solutions
- ASR9K BNG Configuration

Service Provider Networks Overview

Platforms

Different Products for Different Solution Segments



ASR 5000: Fixed Mobile Convergence

ASR 9000: Large Scale BNG Platform

ASR 1000: Mature Flexible BNG Platform

7600: Well Established Flexible Platform

SP Architectures – Last 15 Years

Mid 90s

Internet Access

Leased Lines – ATM/FR/Serial

PPP sessions /Broadband

Dedicated core networks

IPSec VPNs

Early 2000

IP/MPLS Offerings – Layer 3 VPNs

Initial rollouts of core network consolidation

Core network redundancy – Fast Reroute

Push to drive Layer 2 VPNs (Martini drafts)

Mid 2000

Layer 2 – Multi-Service Edge

ISG / IP Sessions

IPv6 arrives – IPv4 address exhaustion surfaces

Initial Public Wireless offerings

Managed Services – DHCP, Content Hosting

Current

Aggregation Network Consolidation

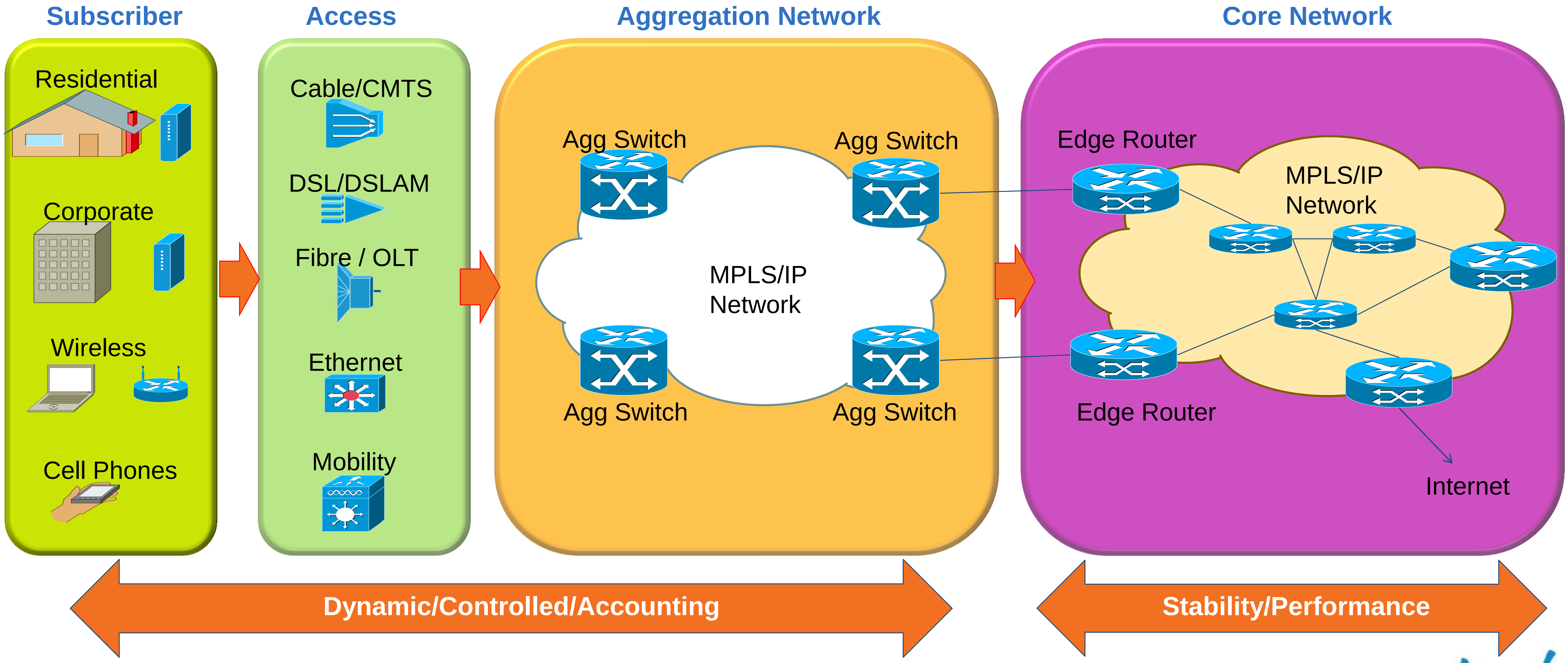
Edge Redundancy – Intra/Inter-Chassis

IPv6 goes mainstream – IPv4 address exhaustion imminent (Feb 2011)

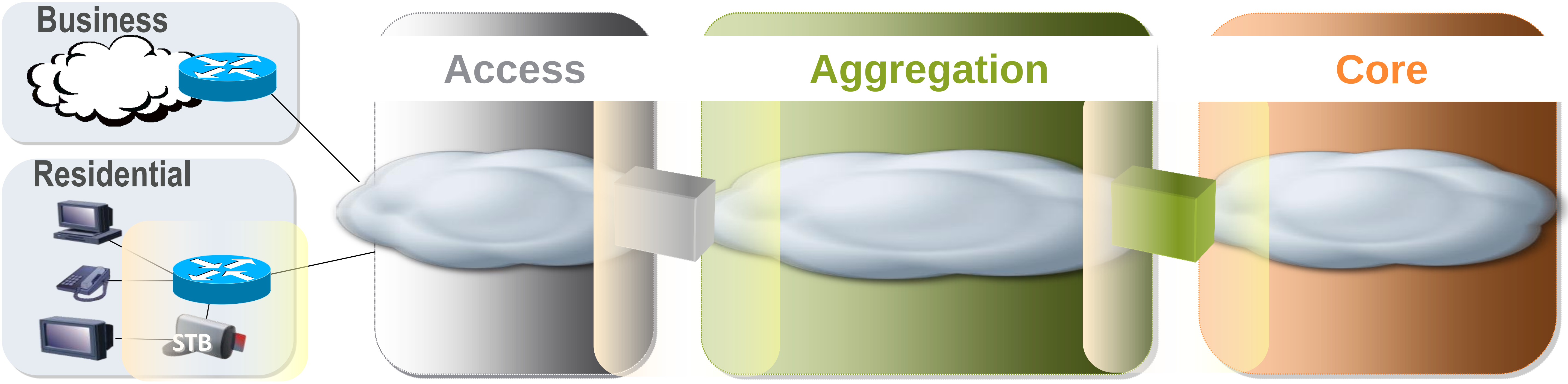
PWLAN/ Community WiFi rollouts

Reduction of OPEX – Transport Profile

Service Provider Networks Architecture



A More Classic View...



CPE

- Customer Premises Equipment—typically a modem
- Modem type varies with Access Technology
- Can operate in routed or bridged mode

Access Node (AN)

- Terminates local loop
- Located at access provider Central Office (CO)
- AN varies based on Access technology

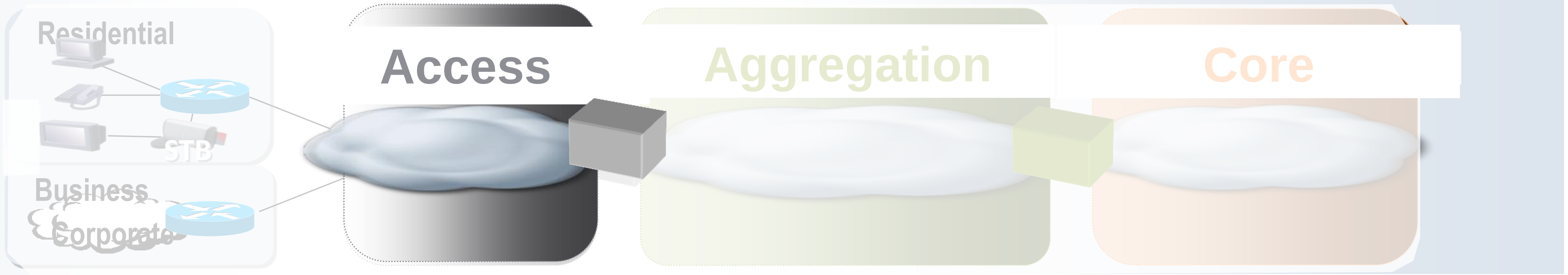
IP Edge

- Gateway towards an MPLS/IP service enabled network
- May terminate subscriber L2 connection (retail services)
- Can be EoMPLS PW termination

Multiple Aspects of Subscriber Aggregation Evolution

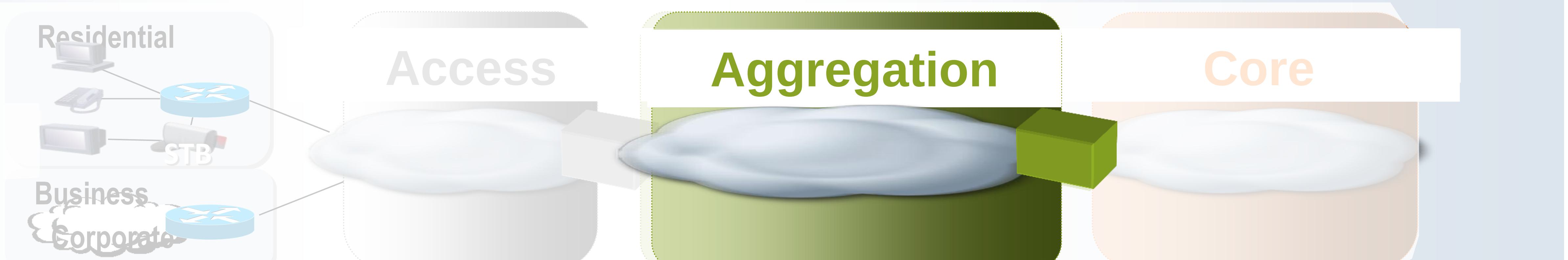
Access Network Technology

Dial, ISDN, DSL, DOCSIS, PON, PTP, ...



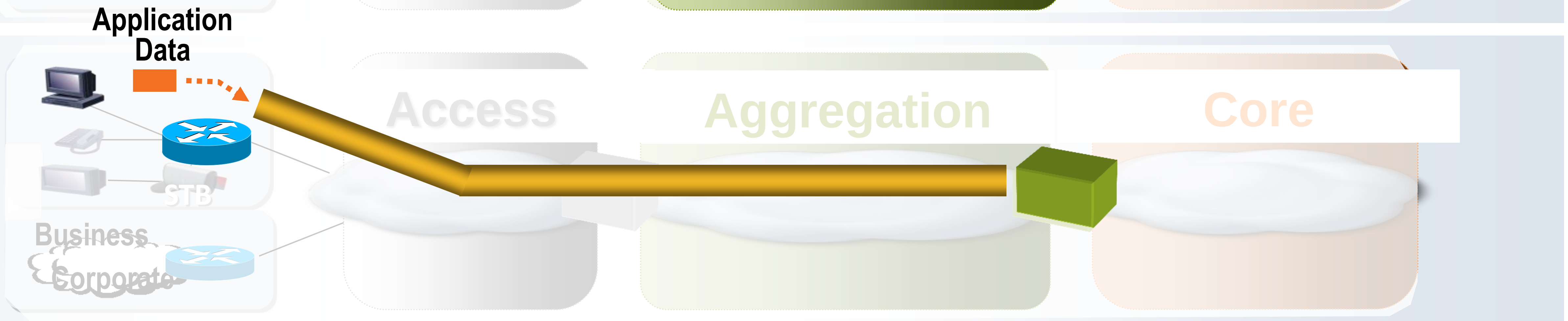
Aggregation Network Technology

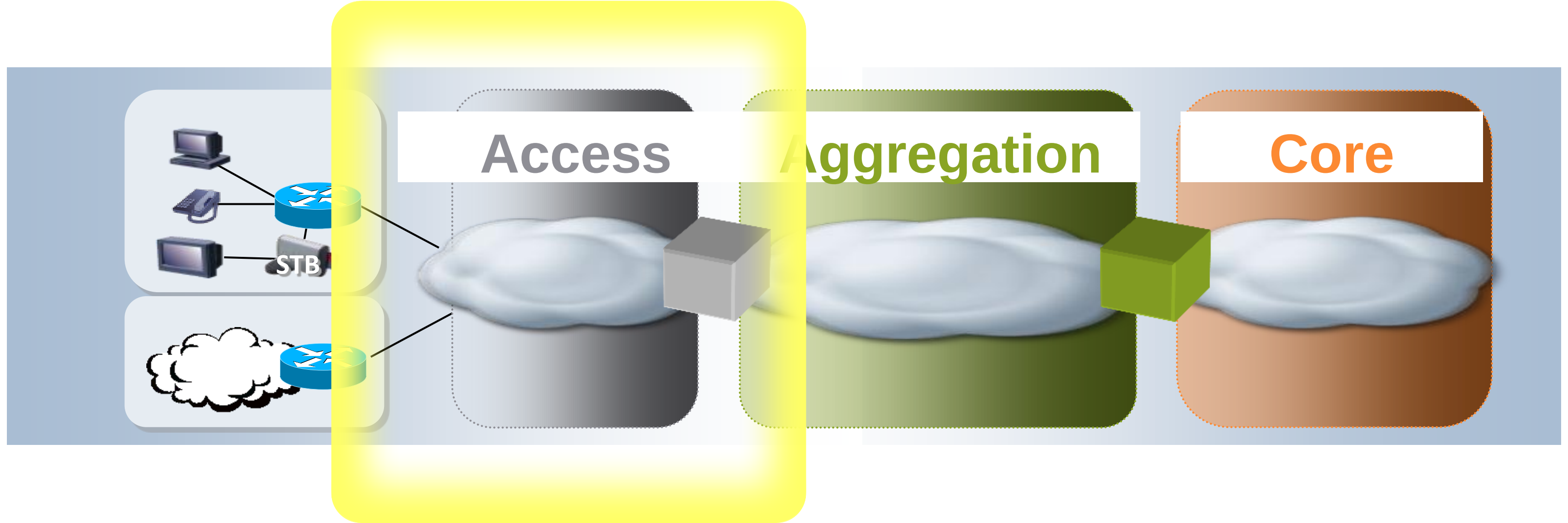
From ATM to Ethernet



Access Protocol

From PPP to IP

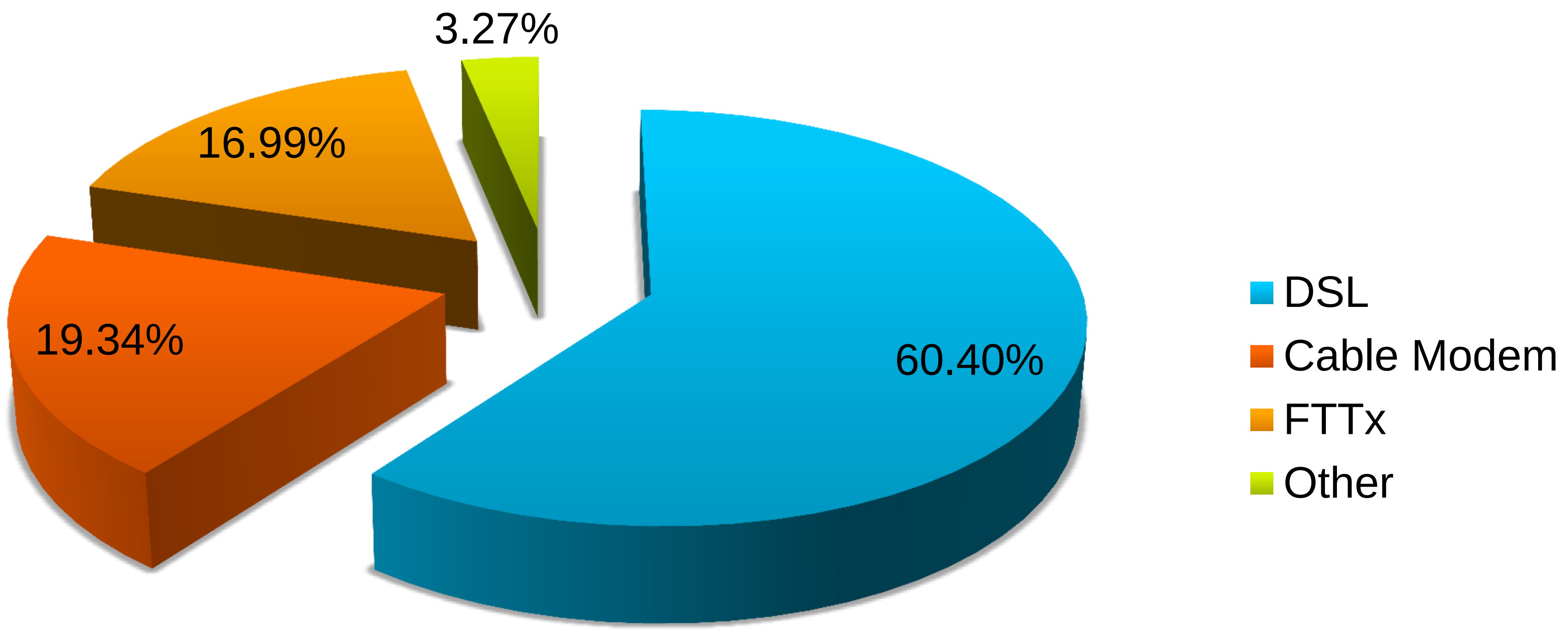




Access Network Evolution

Current Global Market Segmentation Between Access Technologies

Over 600 Million Subscriber Access Lines Globally with Yearly Growth of ~11.5%



DSL: most dominant; ~60.40% share of global broadband market

Major DSL Players by Regions:

- Asia (~36.12%)
- Western Europe (~28.81%)

Cable: 2nd most popular choice with ~19.34% share

Major Cable Players by Regions:

- North America (~51% share)
- Western Europe (~18.4%)

FTTx: 3rd with ~16.99% share

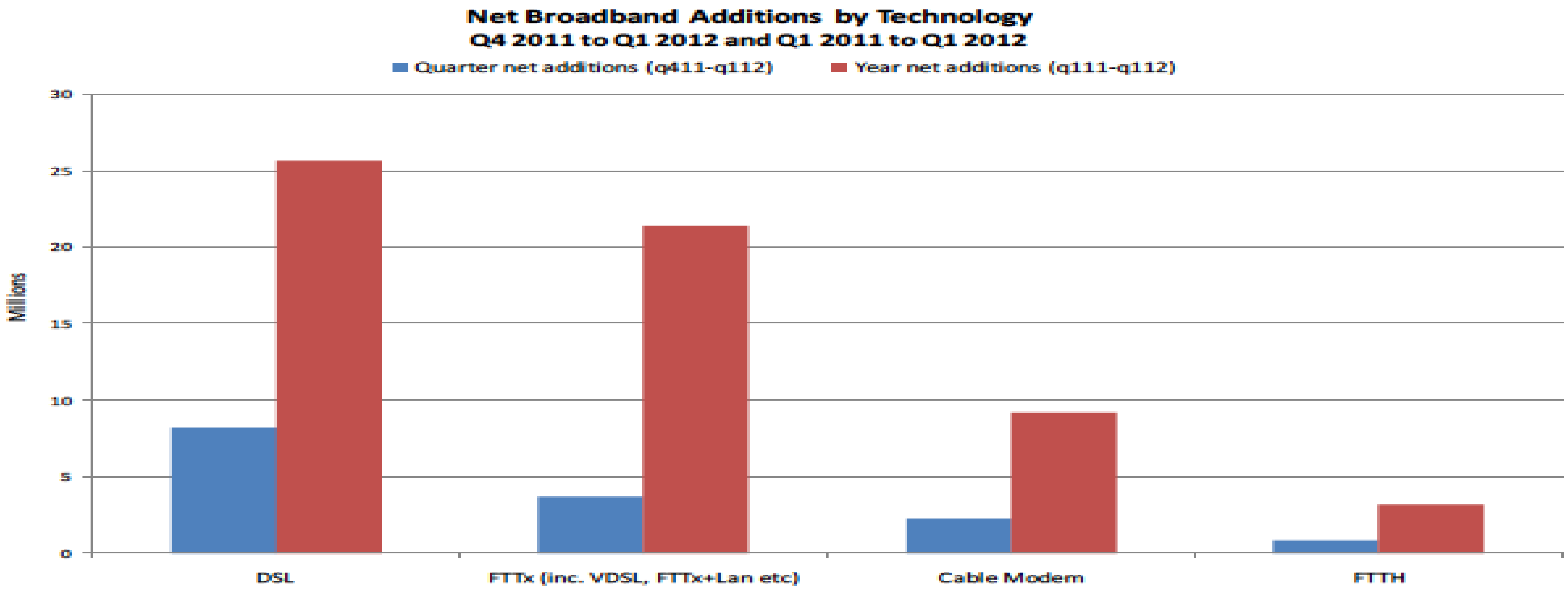
Major Players by Regions:

- Asia (~81%)
- North America (~8.8%)

Source: http://www.point-topic.com

Global Growth Trends Between Broadband Access Technologies

Total Broadband by Technology



DSL: lost ~2.27% market share

Cable: lost ~0.53% market share

FTTx: gained ~2.25% market share

Source: http://www.point-topic.com

POINT topic

Cisco live!

For Your Reference

DSL Access Technologies

- Most commonly deployed Broadband access technology worldwide
- Two hierarchies:

Asymmetric: different speeds upstream/downstream

Symmetric: same speed in each direction

Residential Data Services

Business Data Services

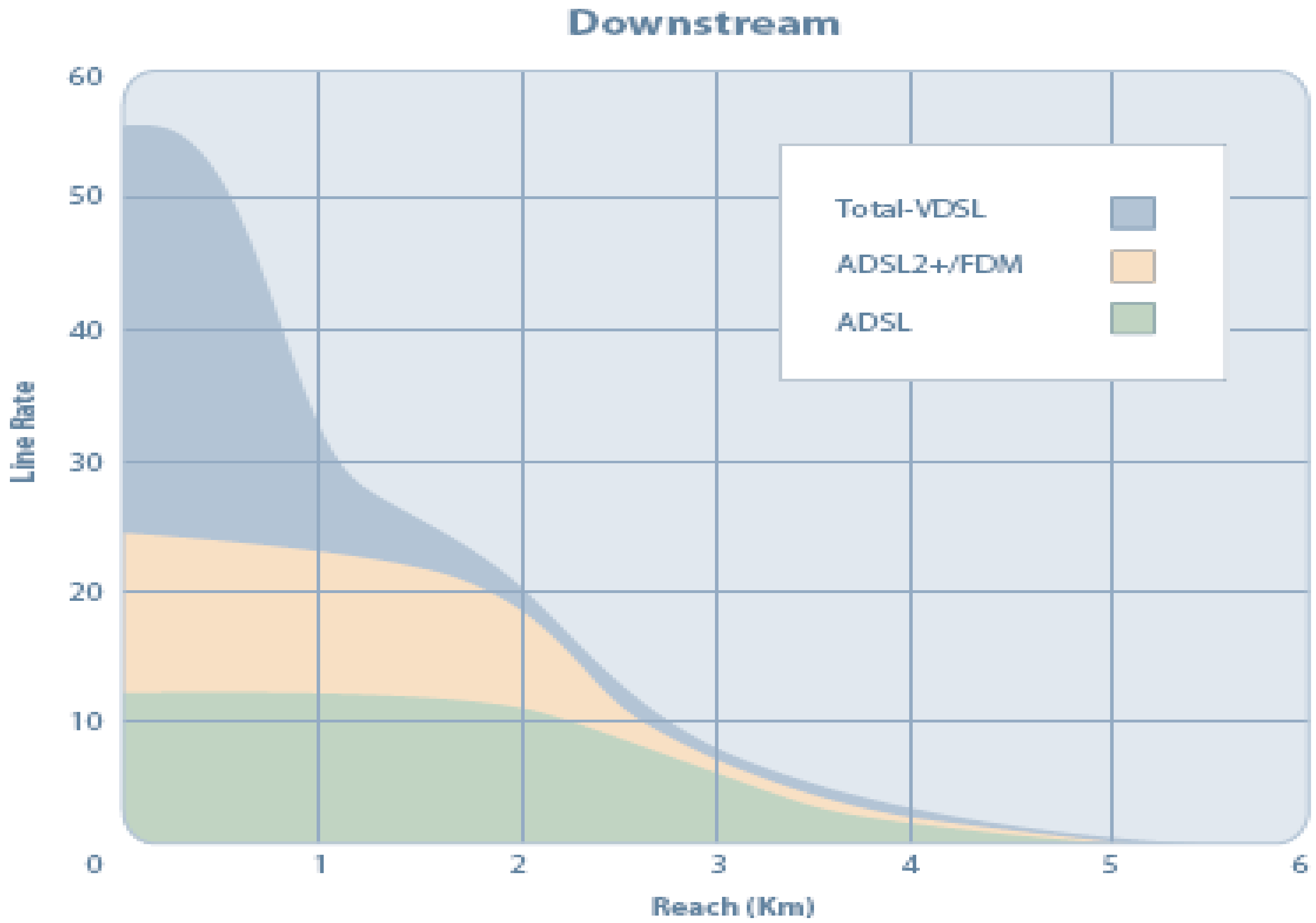
Evolution of Asymmetric DSL

	ADSL (Asymmetric DSL)	ADSL2	ADSL2+	VDSL (Very High Speed DSL)	VDSL2
Standard	ITU-T G.992.1	ITU-T G.992.3	ITU-T G.992.5	ITU-T G.993.1	ITU-T G.993.2
L2 Protocol	ATM	ATM	ATM	ATM. Ethernet	ATM, Ethernet
Speed (up to)	8 Mbps DS 1 Mbps US	12 Mbps DS 1 Mbps US	24 Mbps DS 1 Mbps US	22 Mbps DS 13 Mbps US	100 Mbps DS 100 Mbps US
Reach (up to) (*)	3-5km	4.5 – 5.5 km	3-5km	< 1.5 km	< 3-5 km (LR-VDSL2)

*Maximum reach before synch loss – speed rate (max reach) << maximum speed

The DSL Enemy

The Local Loop Reach

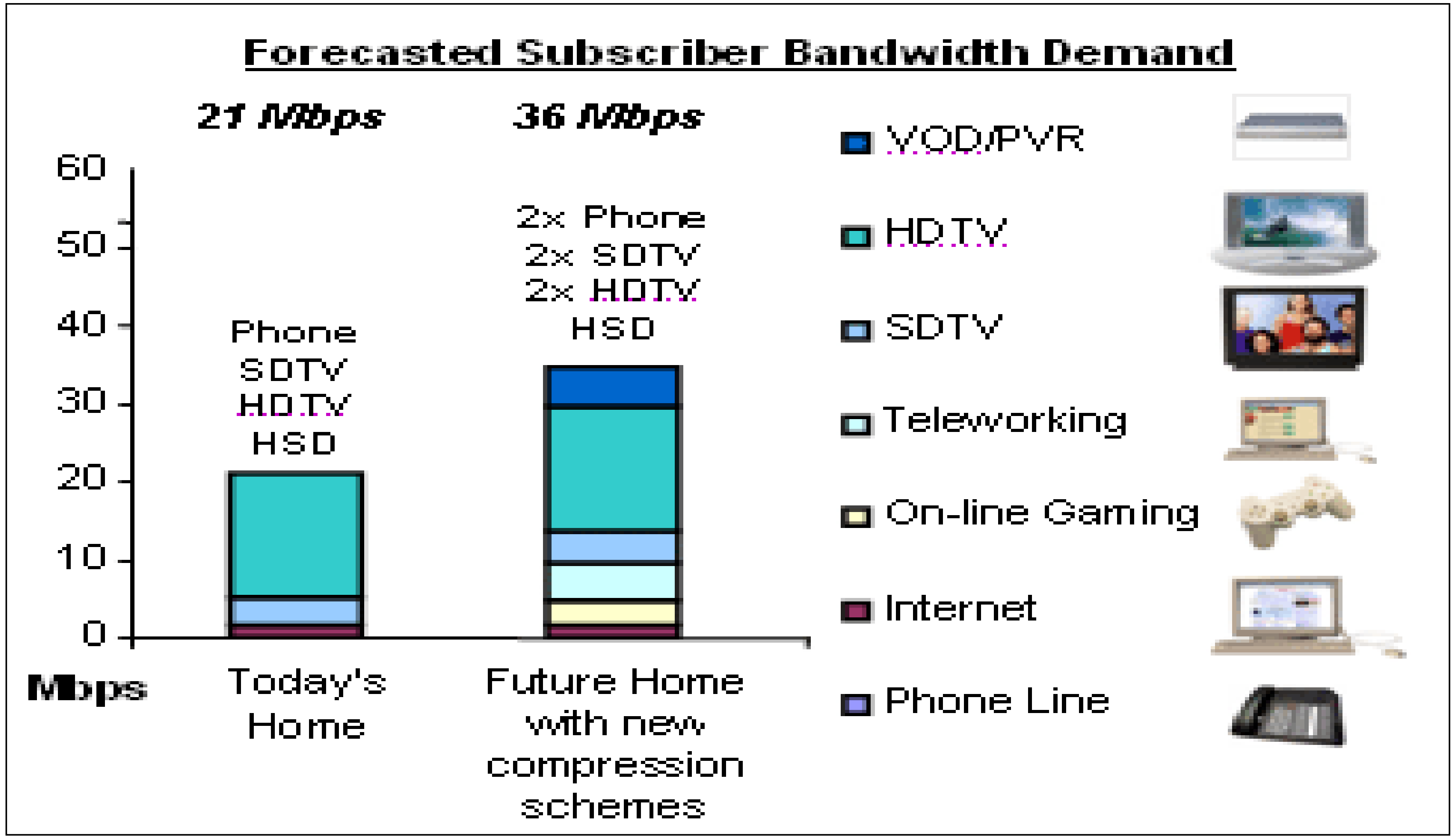


ADSL Technologies available bandwidth dramatically decreases after first mile

VDSL has some gain over ADSL2+ for local loop lengths of less than half a mile

Fibre to the Home, Curb, Building (FTTx)

Moving Away from Copper Twisted Pair Lines



More Bandwidth, More Reach to Residential Users

Applications are converging over a single transport

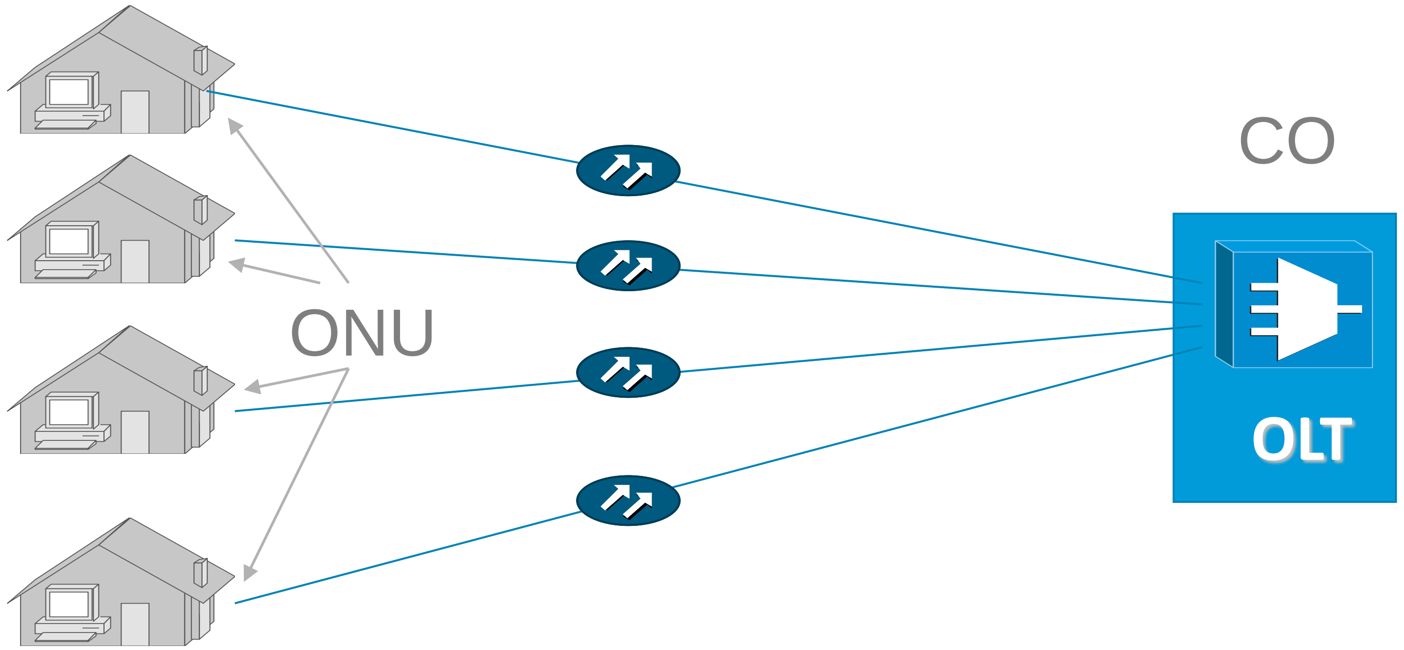
Forecasted subscriber bandwidth demand will double in next 3 to 5 years

Source: http://www.iec.org

FTTH Configurations

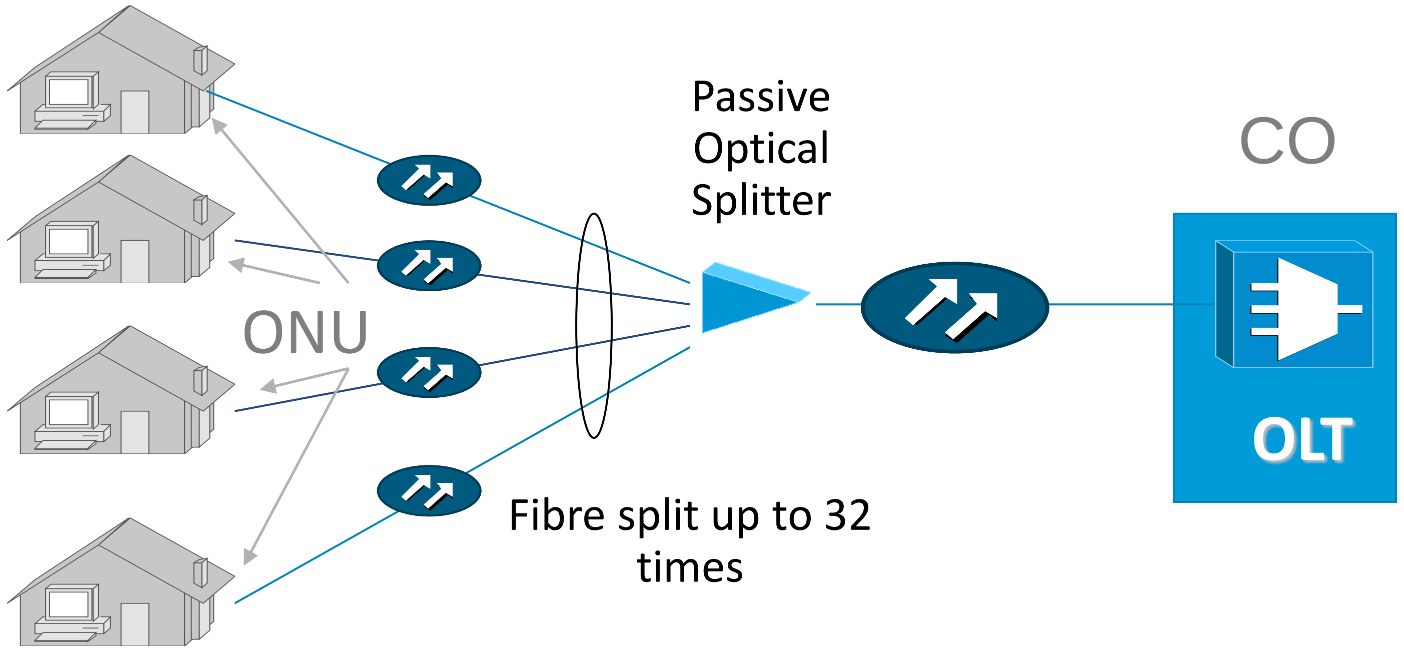
Point To Point Optical Networks (PTP)

- Single fibre strand and laser dedicated to each user (household)



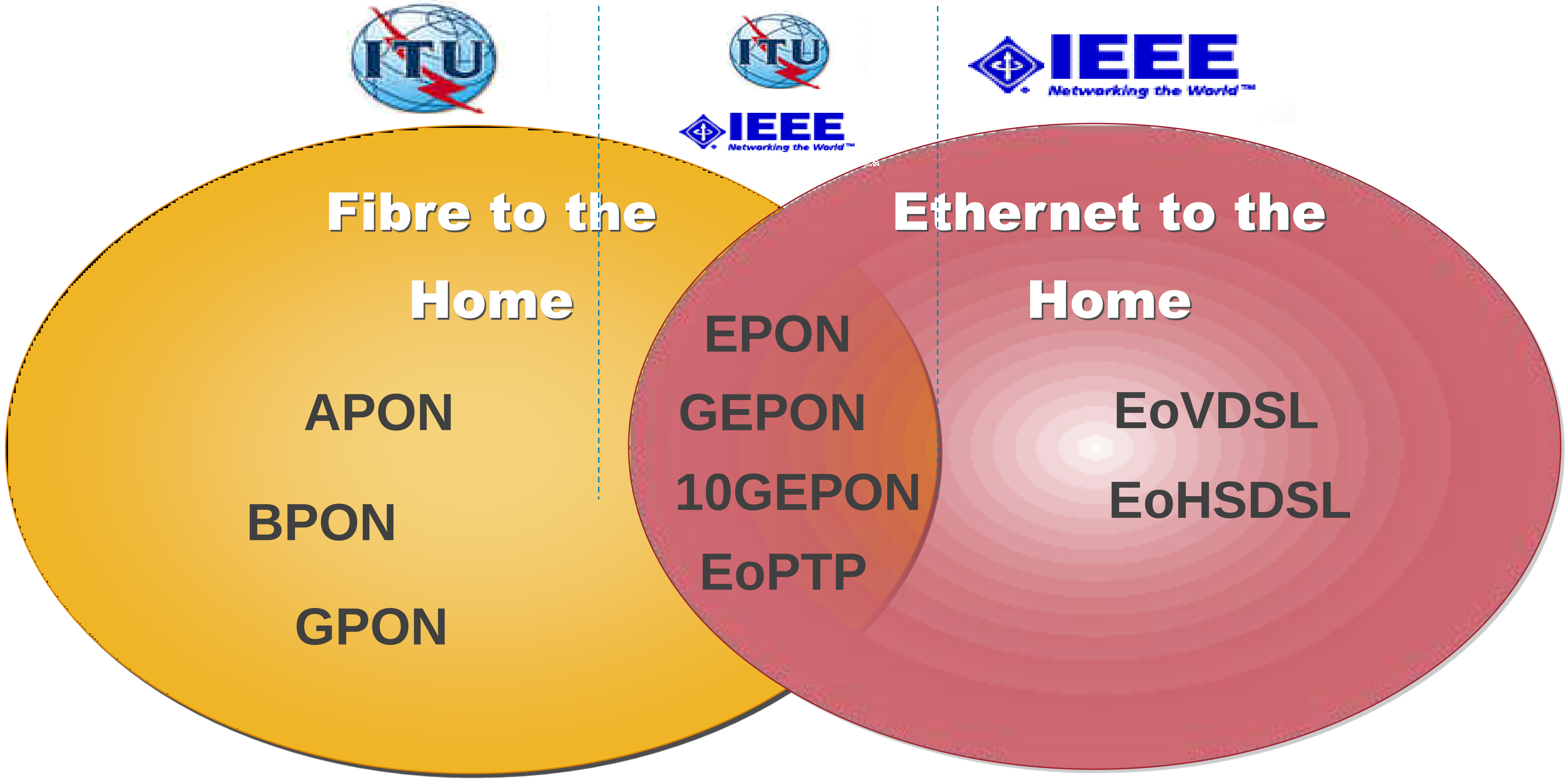
Passive Optical Networks (PON)

- Fibre strand is split one or multiple times
- Fibre and laser shared across multiple users (households)
- Shared CO bandwidth



Free of copper from CO to subscriber household

Fibre to the Home vs. Ethernet to the Home



- Not all Ethernet To The Home (ETTH) Technologies run over Fibre links
- Not all FibreTo The Home (FTTH) Technologies support Ethernet
- ETTH ratification work mostly done by IEEE in 802.3ah
- IEEE 802.3ah aka Ethernet in the First Mile (EFM)

EFM - Physical Layer Specifications

For Your Reference

EFM Extends Ethernet Supported Physical Medias to Include:

Voice-Grade Copper (Category 1 - unshielded twisted pair) – over DSL

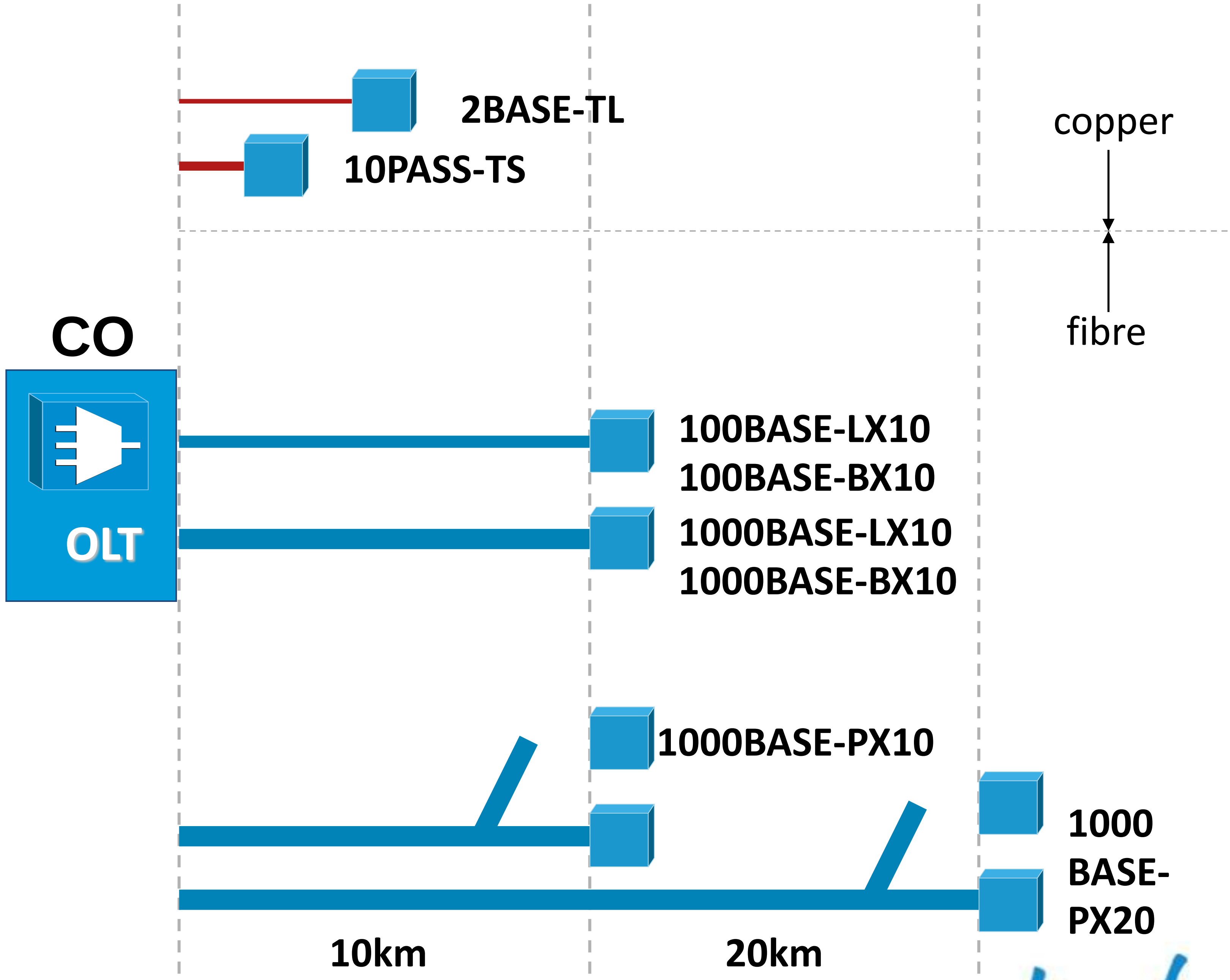
	DSL	Speed (Mbps)	Reach
2BASE-TL	SHDSL	2 – 5.69	2.7 km
10PASS-TS	VDSL	10	750 m

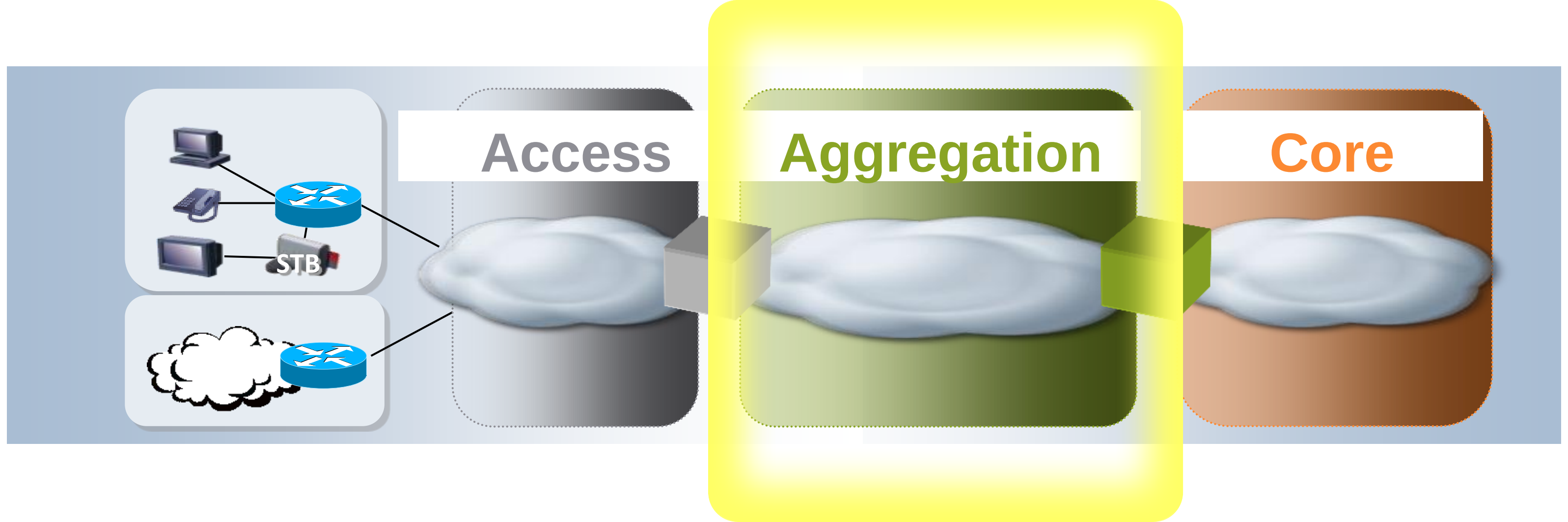
PTP: Long wavelength single and dual strand fibre

	Fibre Type	Speed (Mbps)	Reach
100BASE-LX10 100BASE-BX10	Single Mode	100	10 km
1000BASE-LX10 1000BASE-BX10	Single Mode	1000	10 km

PON: Point-To-Multipoint fibre

	Speed (Mbps)	Reach
1000BASE-PX10	1000	10 km
1000BASE-PX20	1000	20 km

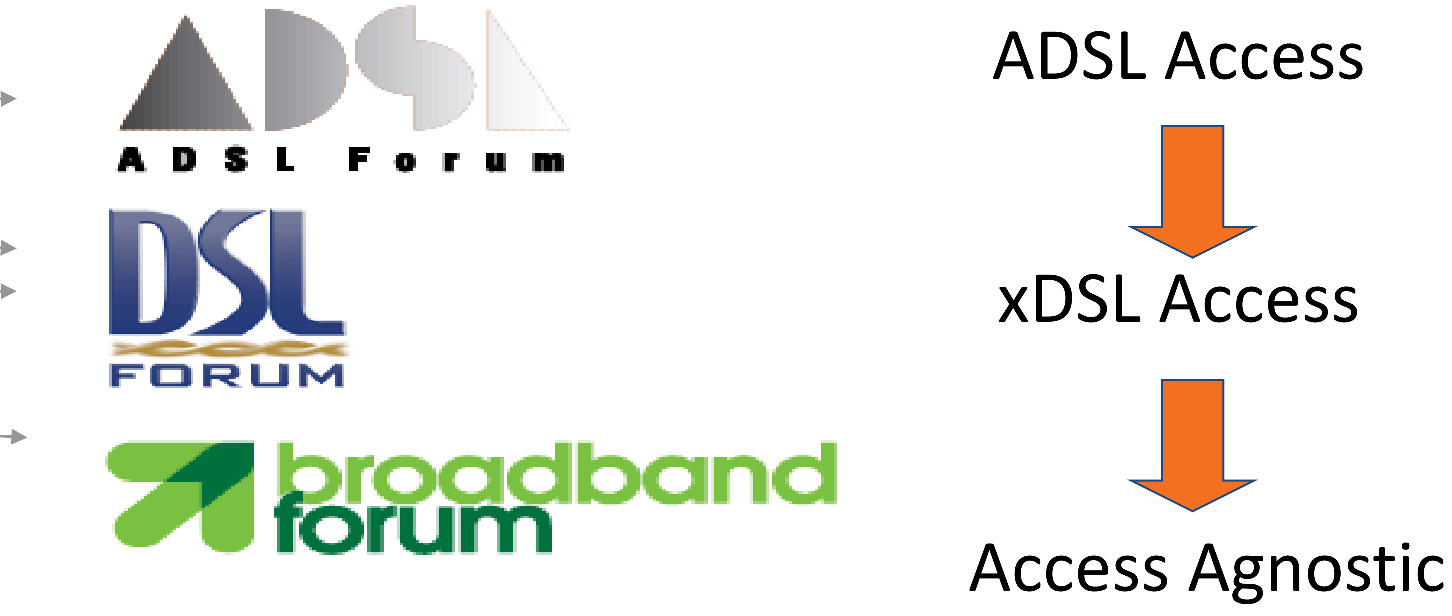




Aggregation Network Evolution

Agenda for this Section

- Aggregation Network Evolution – Broadband-Forum Case Study*
  - –TR-25
  - –TR-59
  - –TR-101
  - –TR-156



ADSL Access

xDSL Access

Access Agnostic

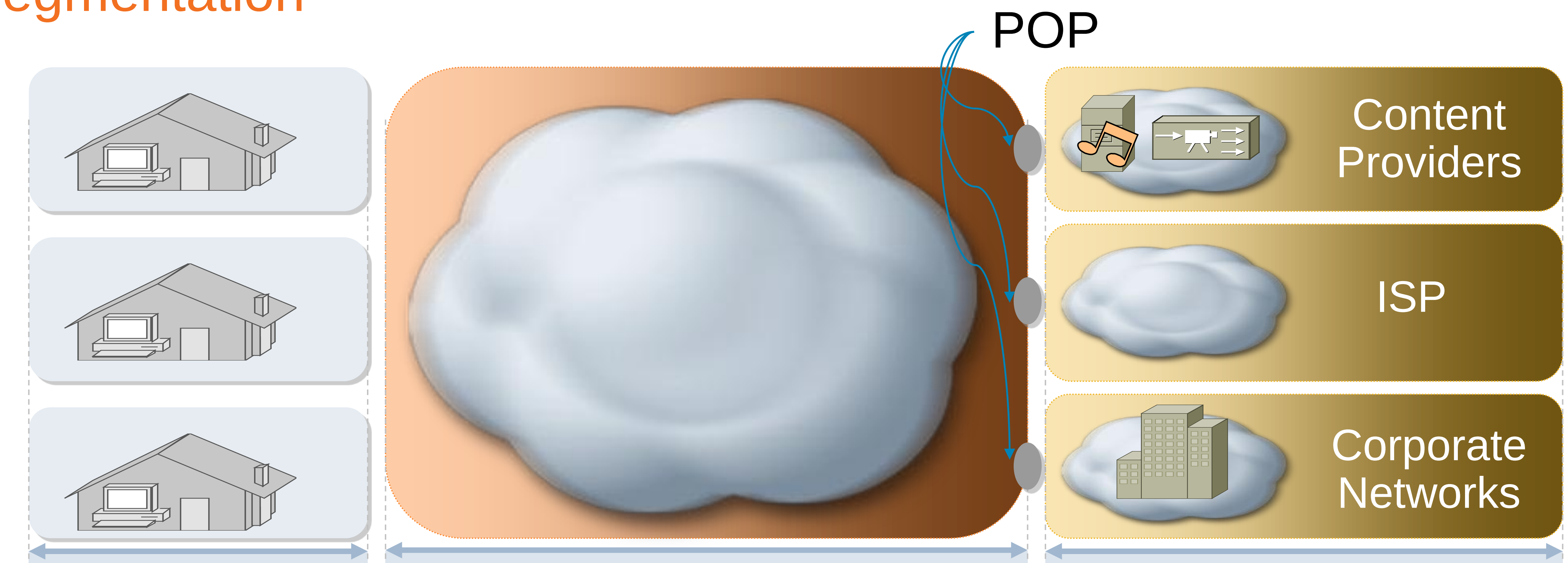
- Ethernet in Aggregation Network
  - –Native IP over Ethernet
  - –EoMPLS/IP => Ethernet Virtual Circuits (EVCs)
  - –Cisco EVC implementation
- Architecting the IP Edge
  - –Centralised vs. Distributed Architectures
  - –Single Edge vs. Multi Edge

* Most real-life deployments deviate or expand over Broadband Forum Technical Reports recommendations and guidelines

Broadband Forum

Provider Networks Segmentation

Broadband Forum Divides Networks Entities in Three Groups



Customer Premises

NAP

Provides connectivity to Service Providers

Encompasses:

- Access network (DSL or else)
- Aggregation and core networks

NSP

Implements services:

- Internet Connectivity
- Business Access
- Application specific content hosting

Handles authentication and address assignment

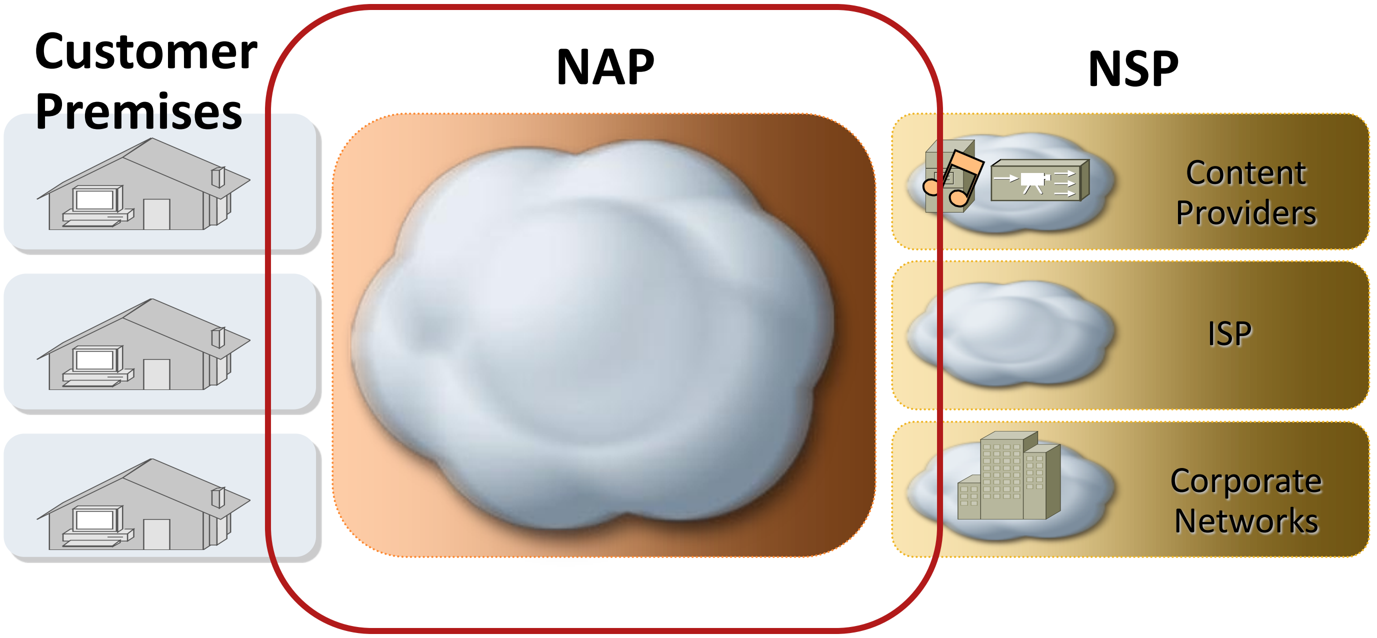
Can Be Same Operator

Broadband Forum Case Study

Evolution of the NAP Network

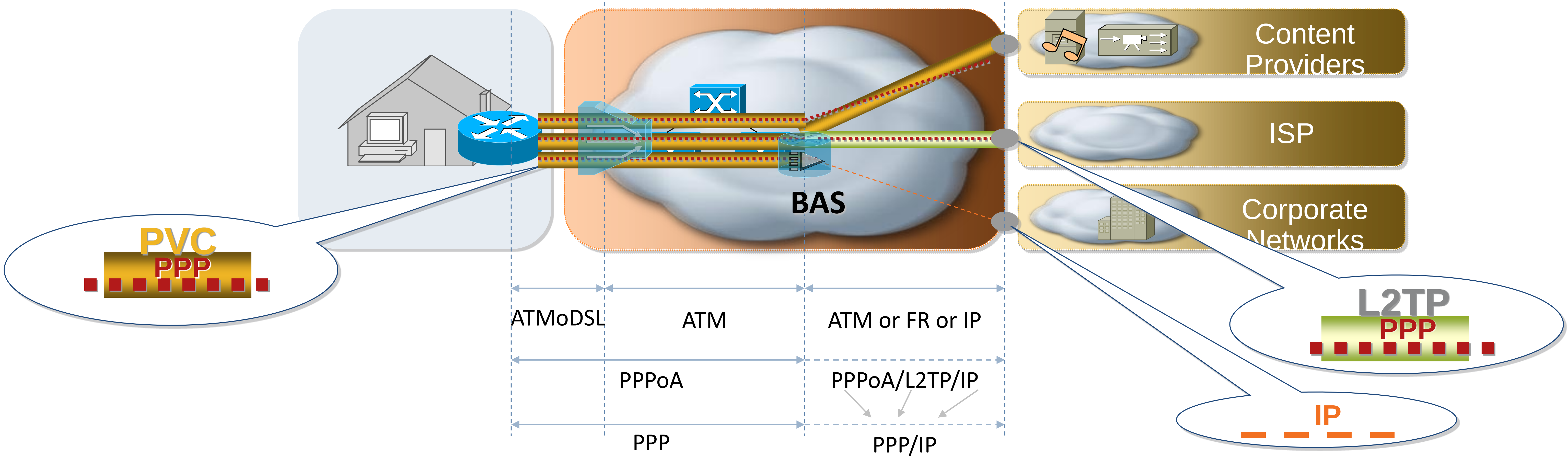
- Three Technical Reports from Broadband Forum describe dynamic of how NAP network has evolved over years:
  - – TR-25 (1999)
  - – TR-59 (2004)
  - – TR-101 (2006)

  (TR-156 (2008))
- Evolution aspects addressed:
  - – From Best Effort to Service Aware
  - – From PPPoA to PPPoE to IPoE
  - – From ATM to Ethernet



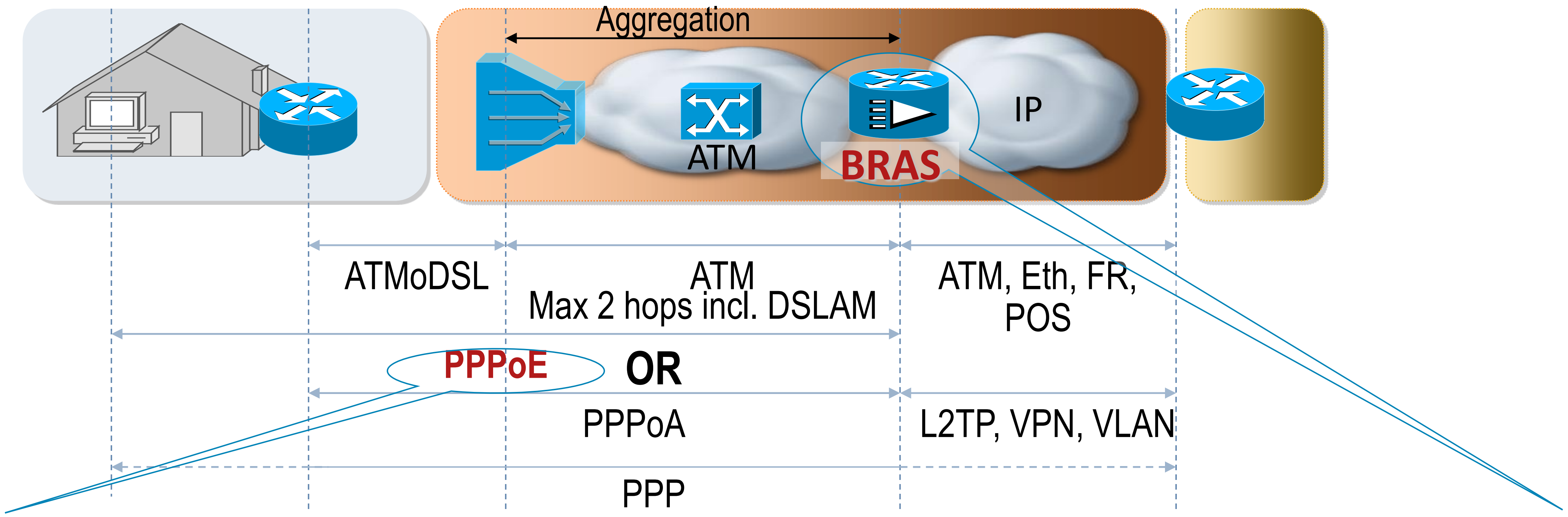
Access Loop Technology: From DSL Specific to Access Agnostic

From this...TR-25



- NAP core network can be ATM end to end or a combination of ATM and IP based interfaces toward NSPs (ATM VC terminated on a Broadband Access Server (BAS) in NAP)
- PPP is subscriber access protocol with PPPoA stack
  - ATM VC (typically PVC) required for each subscriber PPP session toward a NSP service
- PPP can be terminated at NSP or inside NAP network depending on architecture

To this - TR-59 Service Enablers



Adoption of **PPPoE**, as replacement of PPPoA, as subscriber access protocol

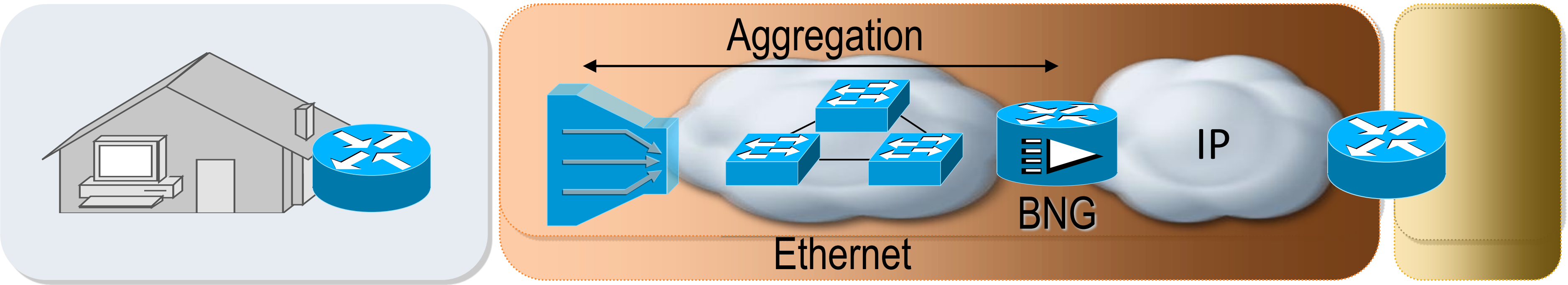
- PPPoE can multiplex several PPP sessions over any point to point or multipoint transport
  - – Each End Client Station can start PPP session (CPE in bridged mode)
  - – => Simultaneous Multi Provider access supported
  - – PPPoE session can also be started by CPE (CPE in routed mode)
- PPPoA still supported

Mandatory presence of a **subscriber aggregation** device with routing and QoS capabilities

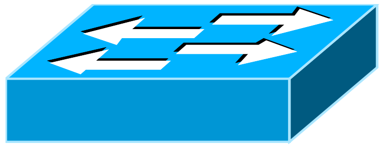
- Formalised presence of BAS in all supported architectures
- BAS becomes **BRAS**: Broadband Remote Access Server
- BRAS can aggregate at IP level (PPP session terminated) or at PPP level (PPP session forwarded)
- BRAS is injection point for per subscriber policy management and IP QoS => ATM Depth limited

To this - TR-101

From ATM to Ethernet



DSLAM becomes Ethernet DSLAM



TR-101 Outlines How an ATM Network Can Be Migrated to an Ethernet-Based Aggregation Network

Highlights

- Supports same set of services as TR-59 architectures
- Optimised multicast distribution and QoS in aggregation network
- From BRAS to Broadband Network Gateway (BNG) at IP Edge
- From Single IP Edge to Dual IP Edge (service segregation: HSI vs. Video)
- From ATM OAM to Ethernet OAM (CFM: 802.1ag)

For Your Reference

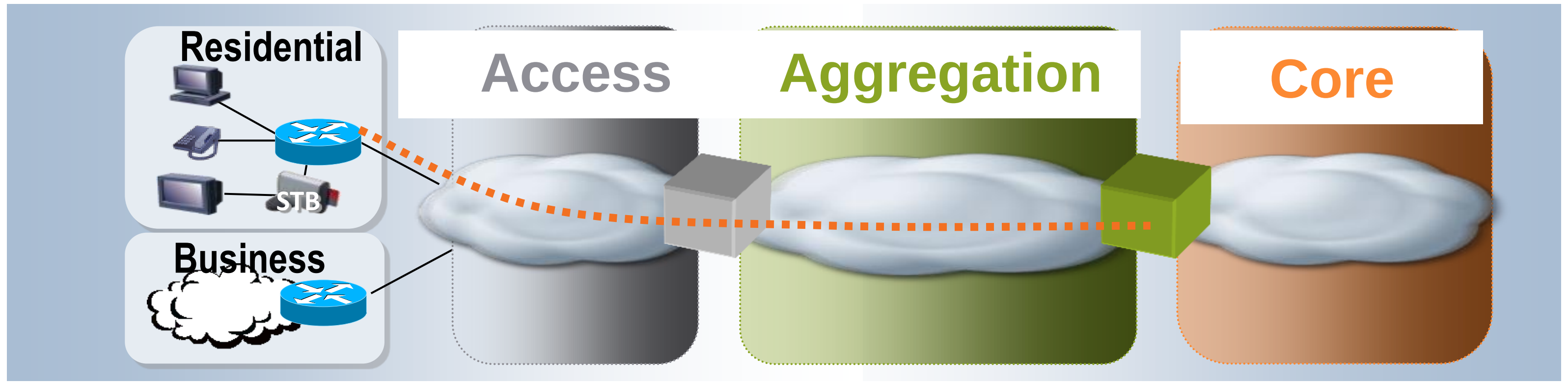
ATM to Ethernet Migration Drivers

ATM

- Point to Point: High Provisioning Costs; Linear with number of users
- Centralised Service Insertion: Optimised for Internet Access; Inefficient Routing and Multicast distribution
- Data-Plane Scalability limits: Low-speed ATM uplinks from CO (typically STM-1), STM-4 handoff to Core

Ethernet

- Point to Cloud Service Access: Reduced Provisioning Cost
- Supports distributed Service Insertion (“Multi Edge”)
- Virtualised Layer-2 Services (with VLANs)
- Flexible Transport for many Services (well suited for 3Play—Efficient Multicast distribution with IGMP Snooping)
- Highly Scalable Data-Plane (10GE and beyond)



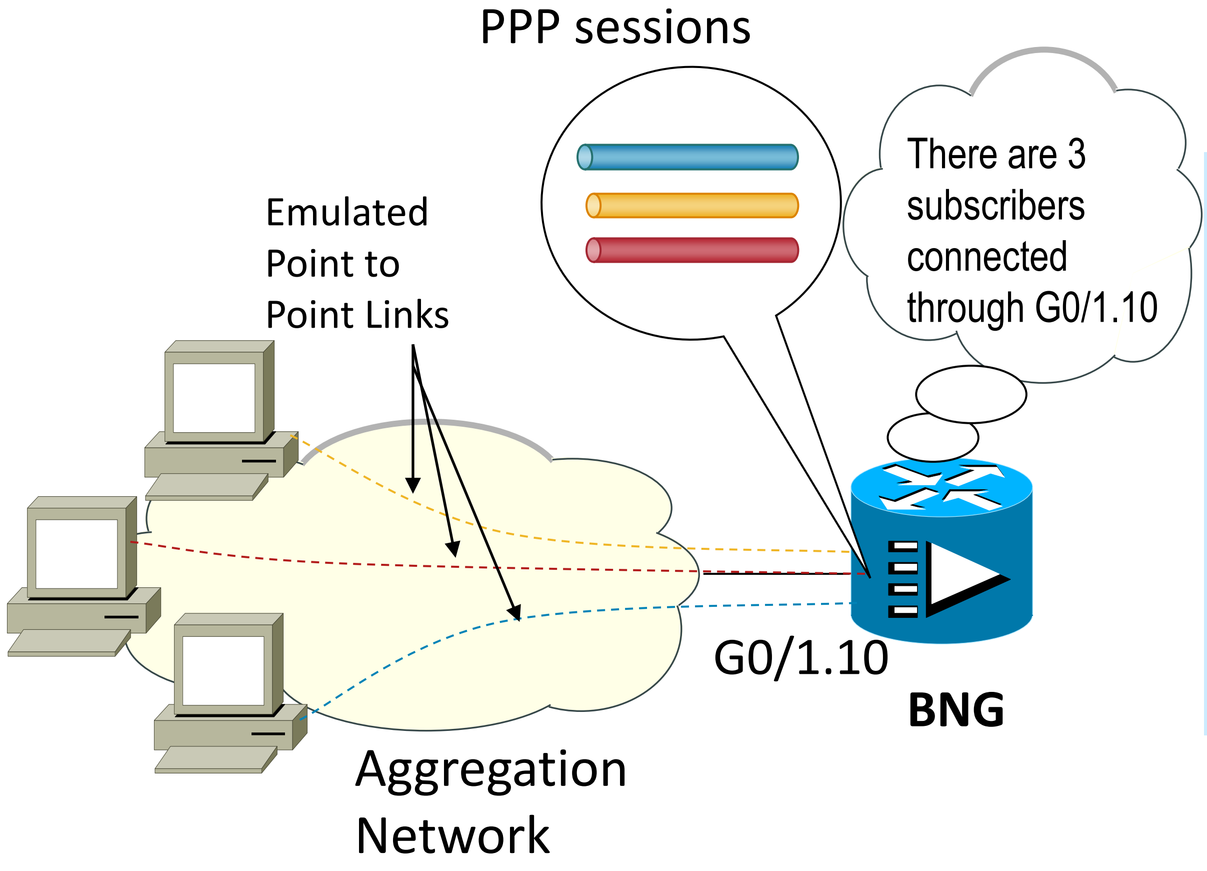
Subscriber Access Protocol Evolution

Agenda for this Section

- Review of PPP in Broadband Environments
- Why PPP Is Getting Old
- PPP vs. IP as Subscriber Access Protocol
- Intelligent Services Gateway

PPP as Subscriber Access-Protocol

- PPP no longer tied to Point to Point Serial links
- First adopted in dial up applications, then extended to operate in broadband environments with introduction of PPPoA and PPPoE
- PPPoA and PPPoE purpose is to emulate a point to point environment over broadband architectures
- **PPPoX enables per subscriber awareness on edge device(s) in a broadband network**



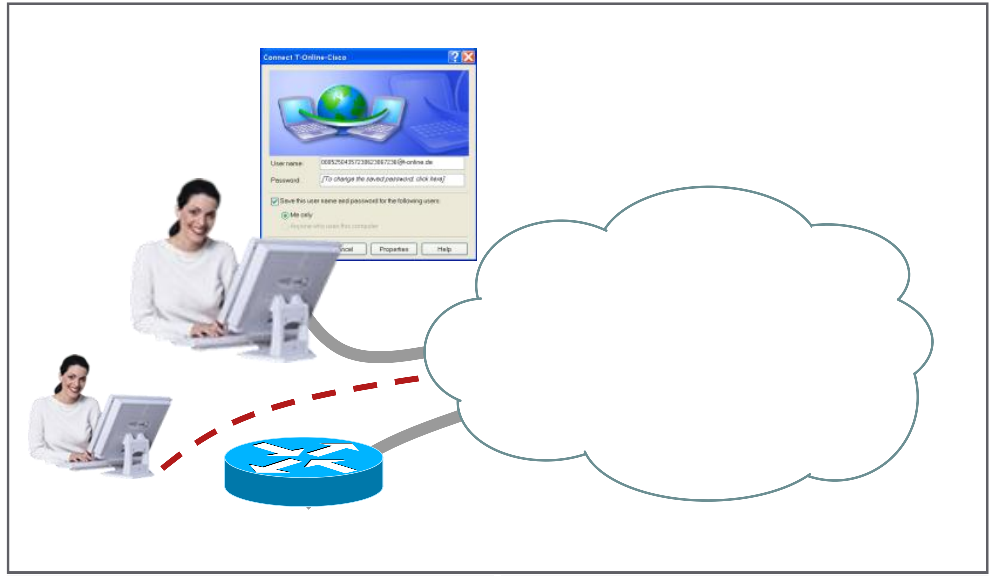
```
BNG#sh pppoe session
   3 sessions in LOCALLY_TERMINATED (PTA) State
   3 sessions total

Uniq ID  PPPoE     RemMAC          Port          VT  VA        State
         SID       LocMAC                            VA-st     Type
     1         1   aabb.cc01.f420  Et0/3.21      21  Vi2.1     PTA
                   aabb.cc01.f630  VLAN:  21         UP
     3         2   aabb.cc01.f520  Et0/3.21      21  Vi2.2     PTA
                   aabb.cc01.f630  VLAN:  21         UP
     5         3   aabb.cc01.f620  Et0/3.21      21  Vi2.3     PTA
                   aabb.cc01.f630  VLAN:  21         UP
```

Multiple "independent" sessions over same shared interface

Why PPP is Aging …

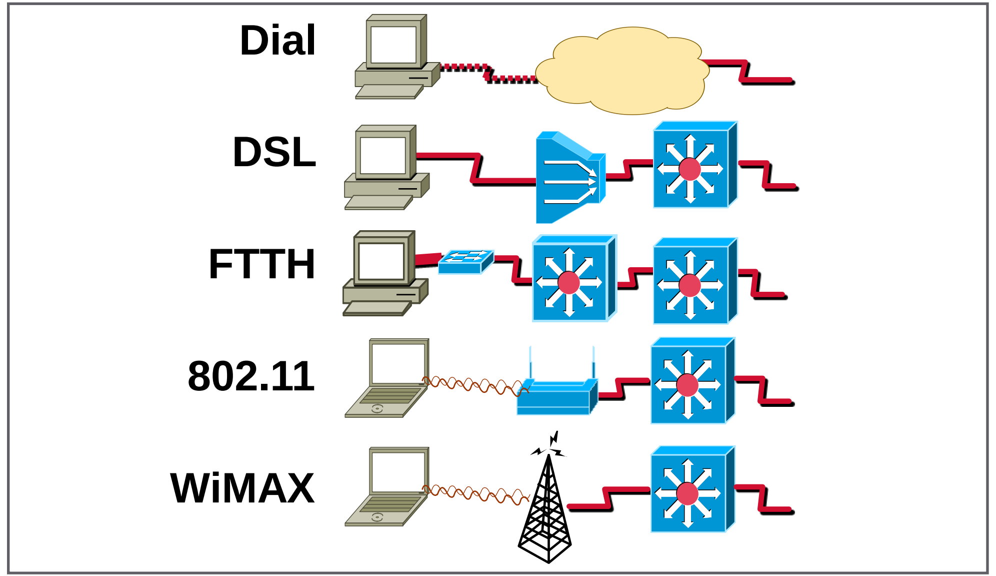
- Client PC must be provisioned with PPPoE stack OR additional intelligence required at CPE
  - per subscriber configuration (e.g. authentication param)
  - extra cost factor
- Access Media partiality
- Multi-Edge Support challenging

Client/Endpoint Requirements



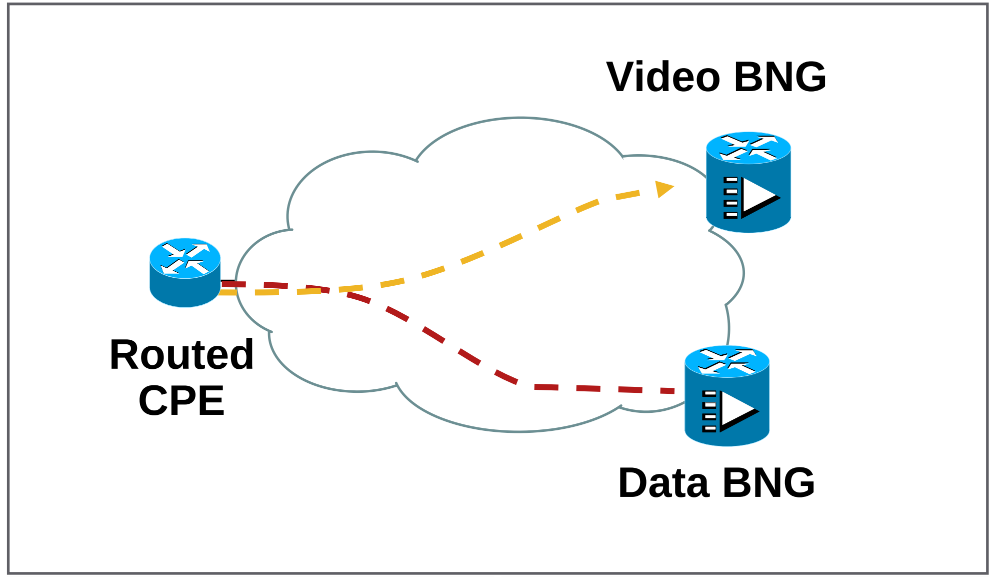
PPP-Sessions	👍 IP-Sessions

Access Media Independence



PPP-Sessions	👍 IP-Sessions

Multi-Edge Support

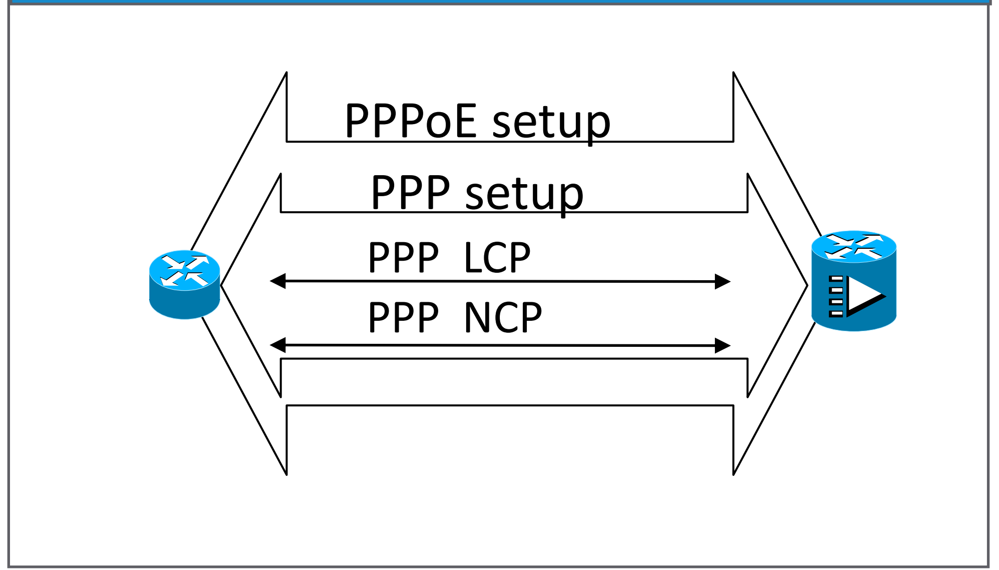


👎 PPP-Sessions	👍 IP-Sessions

Why PPP is Aging …

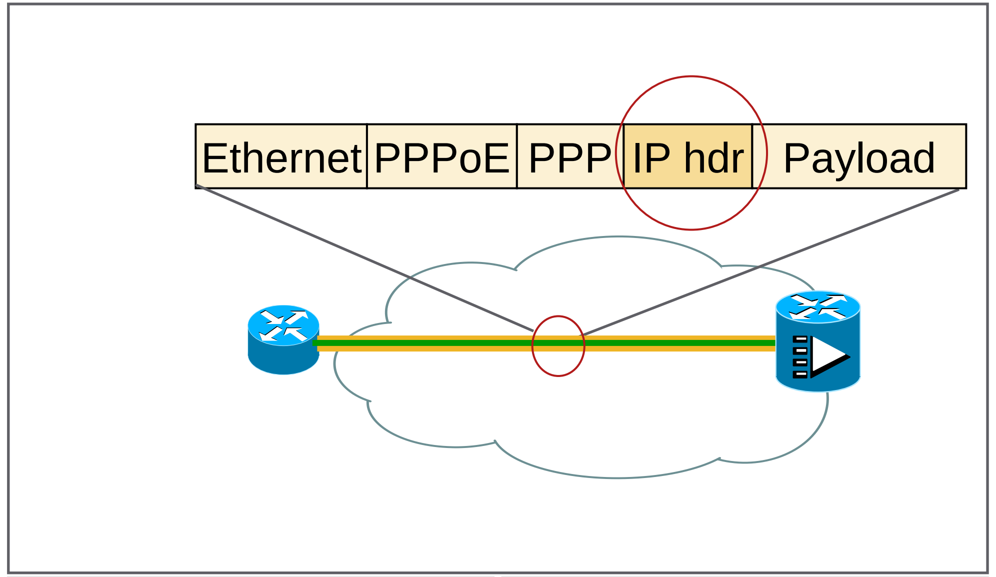
- Mandates specialised functionalities for PPP session set up and tear down
- Residential Access converged to all IP PPP adds unnecessary overhead
- Support for Multicast Multimedia applications (e.g. IPTV)

Operational Simplicity



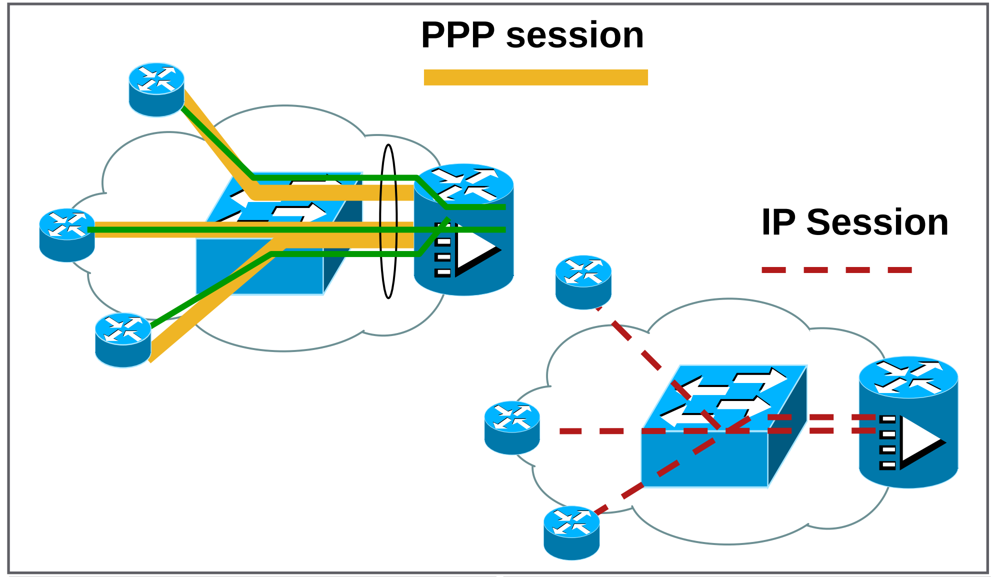
👎 PPP-Sessions | 👍 IP-Sessions

IP Services (QoS, etc.)



👎 PPP-Sessions | 👍 IP-Sessions

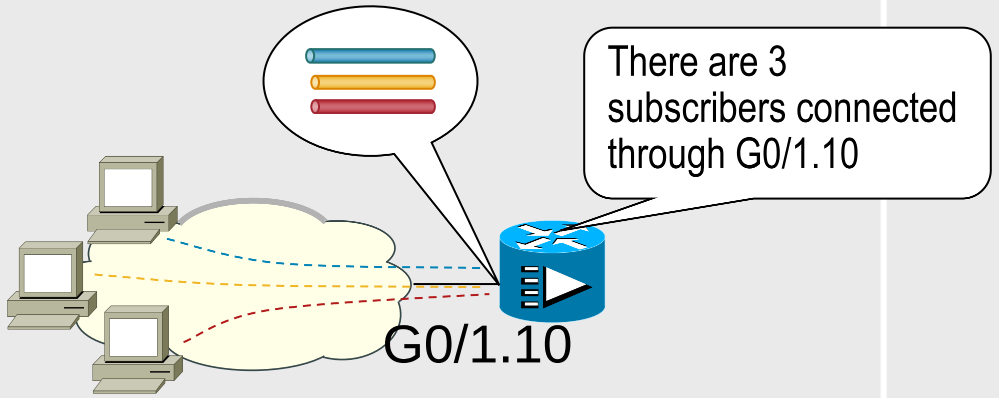
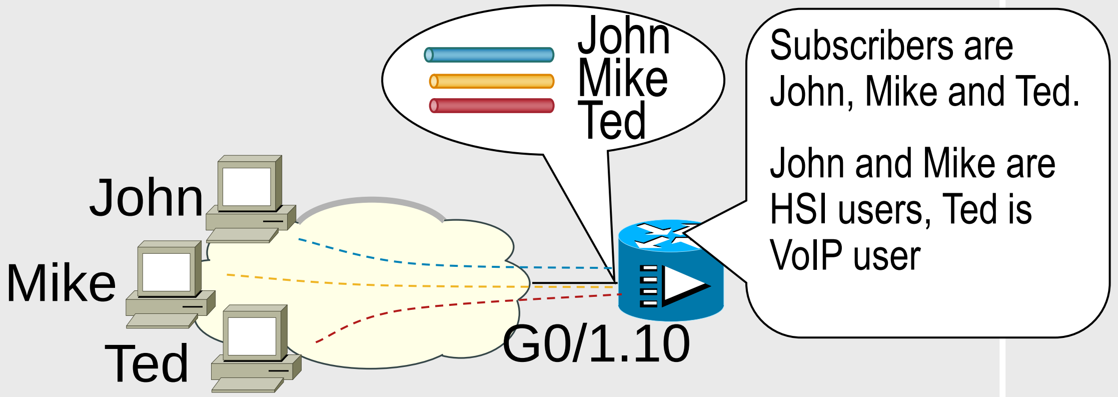
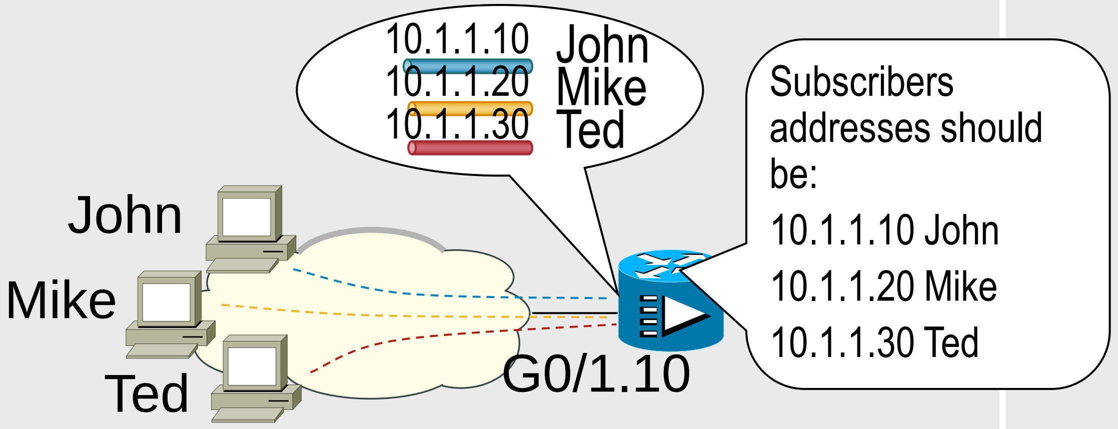
Efficient Multicast Replication



👎 PPP-Sessions | 👍 IP-Sessions

Migrating from PPP to IP

What Do We Need?

		Goal
Subscriber Identification	 There are 3 subscribers connected through G0/1.10	Create a per subscriber construct over a shared interface (“subscriber session”)
Subscriber Authentication and Authorisation	 Subscribers are John, Mike and Ted. John and Mike are HSI users, Ted is VoIP user	Uniquely establish subscriber identity and determine services and service levels per subscriber
Subscriber Address Management	 10.1.1.10 John 10.1.1.20 Mike 10.1.1.30 Ted John Mike Ted G0/1.10 Subscribers addresses should be: 10.1.1.10 John 10.1.1.20 Mike 10.1.1.30 Ted	Assign a unique IP address to each subscriber based on provider domain

Migrating from PPP to IP

What Do We Have?

	PPP	IP	
Subscriber Identification	Per Subscriber PPP sessions thanks to PPPoX point to point emulation	?	**How do we create an IP session?**
Subscriber Authentication and Authorisation	PPP embedded authentication protocols	?	**How do we authenticate an IP session?**
Subscriber Address Management	Address allocation during PPP IPCP phase	?	**How can we assign address to IP subscribers?**

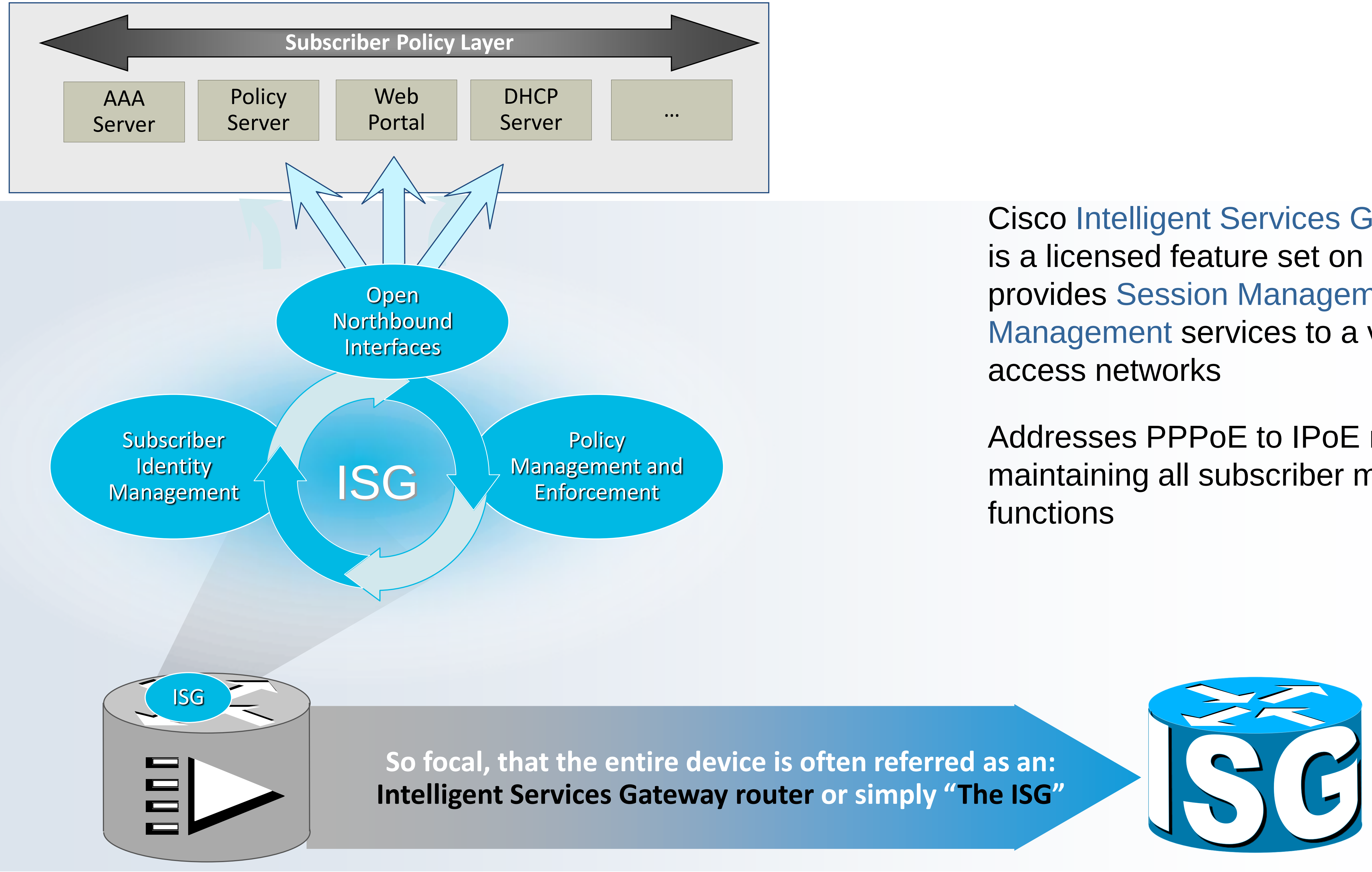
Migrating from PPP to IP

What Do We Have?

	PPP	IP
Subscriber Identification	Per Subscriber PPP sessions thanks to PPPoX point to point emulation	? **How do we create an IP session?**
Sub Aut and Authorization		e
Subscriber Address Management	Address allocation during PPP IPCP phase	? **How can we assign address to IP subscribers?**

Cisco Offers Intelligent Services Gateway (IOS) & Control Policy Language (XR) to Address PPPoE to IPoE Migration while Maintaining All Subscriber Management Functions

What is ISG?

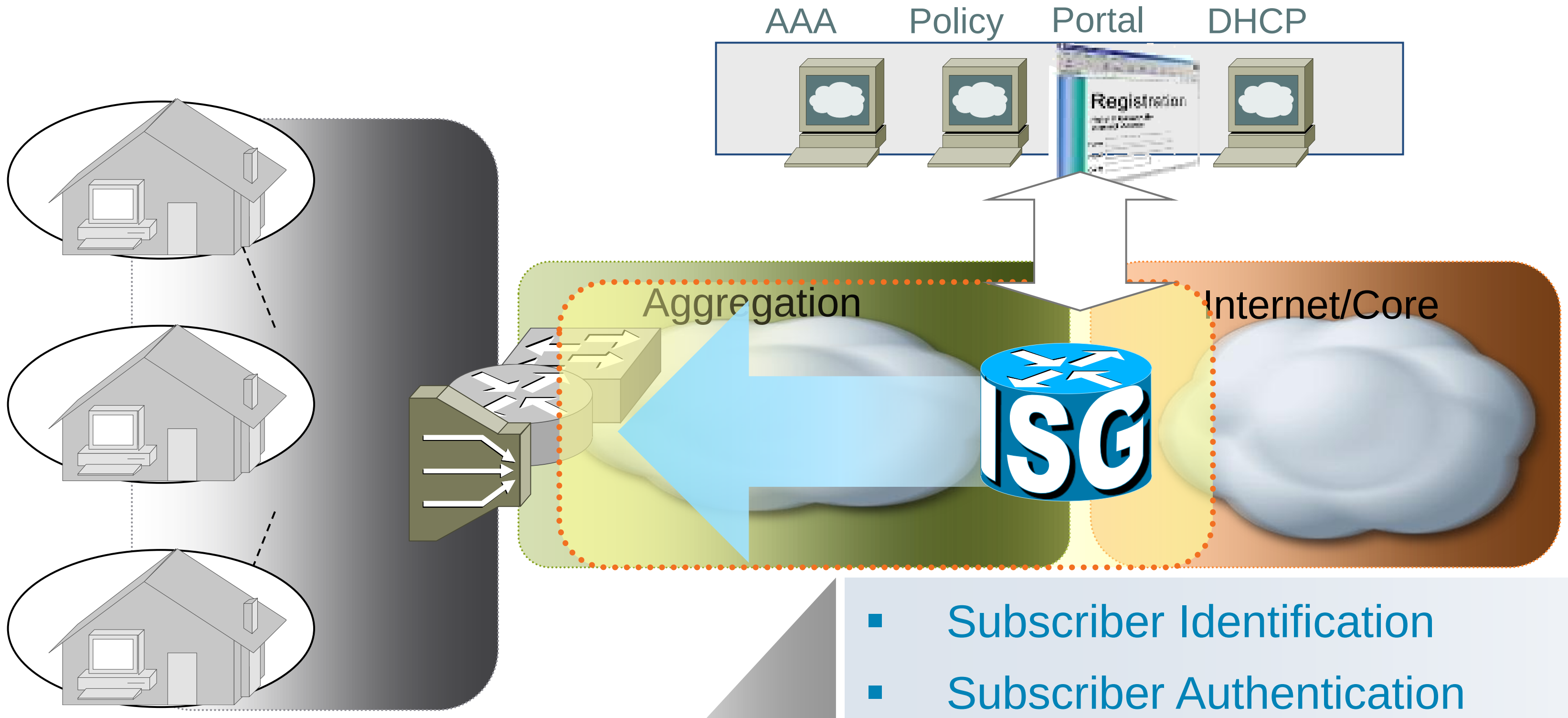

Subscriber Policy Layer
AAA Server
Policy Server
Web Portal
DHCP Server
…
Open Northbound Interfaces
Subscriber Identity Management
ISG
Policy Management and Enforcement
ISG
ISG

So focal, that the entire device is often referred as an:
Intelligent Services Gateway router or simply “**The ISG**”

Cisco Intelligent Services Gateway (ISG) is a licensed feature set on Cisco IOS that provides Session Management and Policy Management services to a variety of access networks

Addresses PPPoE to IPoE migration while maintaining all subscriber management functions

ISG’s Place in the Network

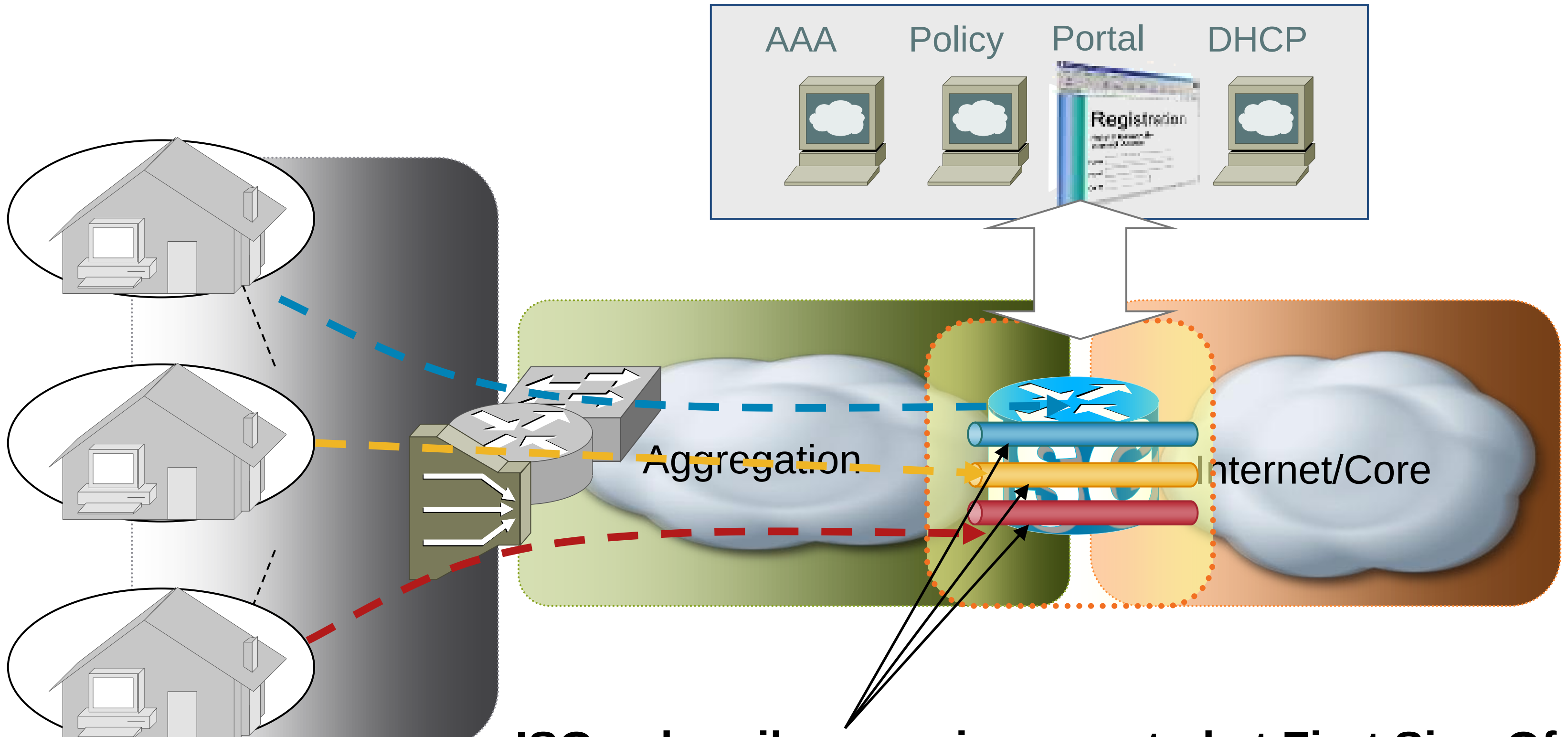


- Deployed at access or service edge
- Communicates with other devices to control all aspects of subscriber access in network
- Single point of contact

- Subscriber Identification
- Subscriber Authentication
  - PPP CHAP/PAP
  - Transparent Auto Logon (TAL)
  - Web Logon
  - RADIUS
- Subscriber Services Determination and Enforcement
- Dynamic Service update
- Session Lifecycle Management
  - Establishment
  - Configuration
  - Tear Down

Based on:
- Who he is
- Where he is
- How he behaves
- What he requires

ISG’s Subscriber Identification



A construct in Cisco IOS that represents subscriber

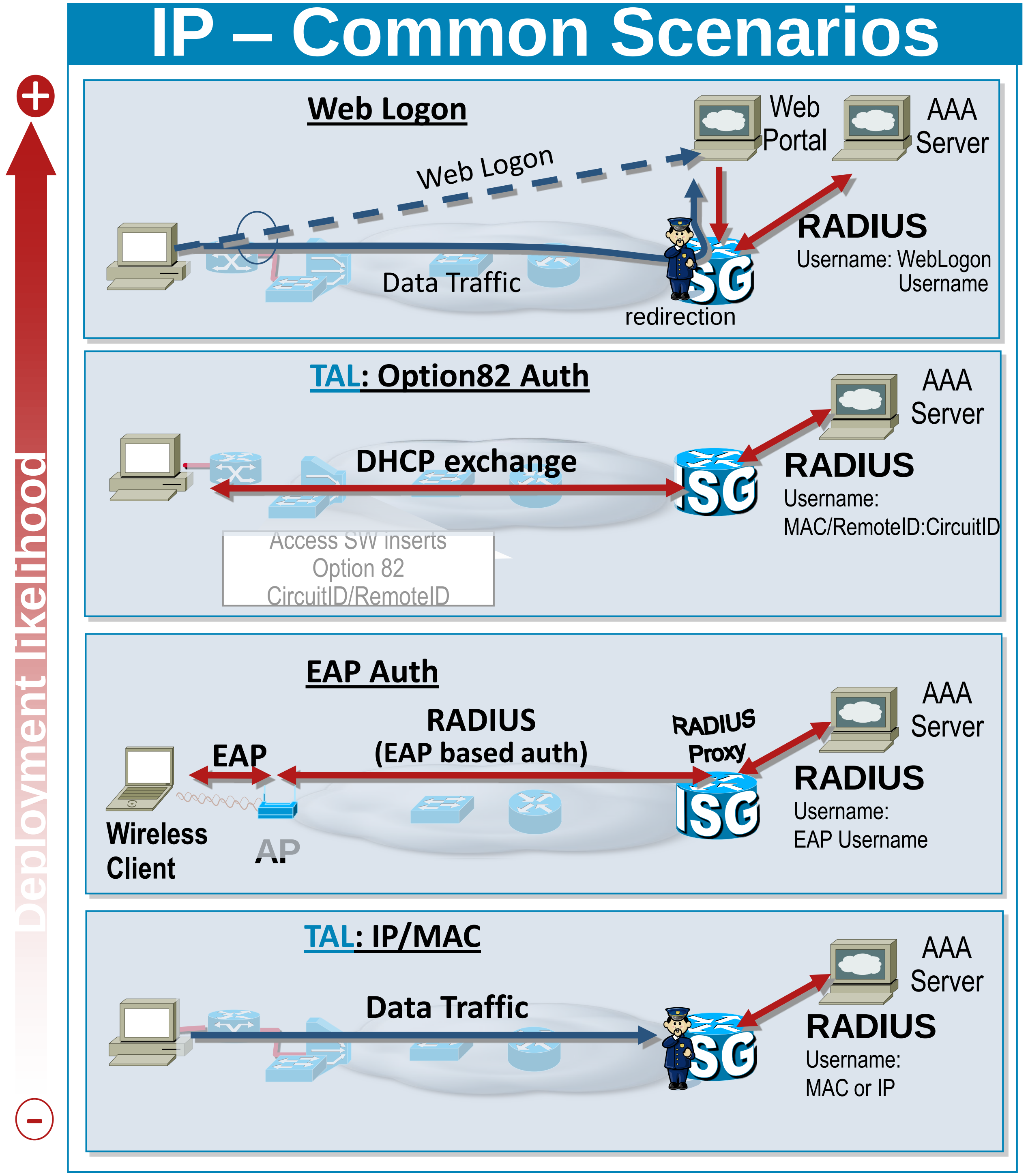
ISG subscriber session: created at First Sign Of Life (FSOL)

N:1 relationship between session and interface

	FSOL	
PPP Sessions	PPP call request	
IP Session	Received Packet w/ unknown IP or MAC source address	IP or MAC initiated IP session
	DHCP Discover	DHCP initiated IP session
	RADIUS Request	RADIUS initiated IP session

ISG's Subscriber Authentication

(IP Sessions)



IP – Common Scenarios

Deployment likelihood

+

-

Web Logon

Web Logon

Data Traffic

redirection

Web Portal

AAA Server

RADIUS

Username: WebLogon Username

TAL: Option82 Auth

DHCP exchange

Access SW inserts Option 82 CircuitID/RemoteID

AAA Server

RADIUS

Username: MAC/RemoteID:CircuitID

EAP Auth

EAP

RADIUS (EAP based auth)

RADIUS Proxy

Wireless Client

AP

AAA Server

RADIUS

Username: EAP Username

TAL: IP/MAC

Data Traffic

AAA Server

RADIUS

Username: MAC or IP

- User traffic redirected to Web Portal to enter credentials
- User Credentials propagated to ISG
- ISG uses credentials to authenticate user with AAA server
- Applicable to all session types

- Access Switch inserts Option82 Circuit and Remote ID in DHCP Requests
- ISG performs authentication using a combination of Circuit and RemoteID
- ISG session must be DHCP initiated

- User starts EAP authentication with Access Point (AP)
- ISG impersonates RADIUS server toward AP, and RADIUS client toward real server
- ISG learns session authentication status by proxying RADIUS messages between real RADIUS client and Server
- ISG session must be RADIUS initiated

- ISG performs authentication using identifiers from subscriber traffic (source IP/MAC)
- Typically used in topologies w/ L2 connected subscribers to support clients w/ static IP address or in IP-routed topologies

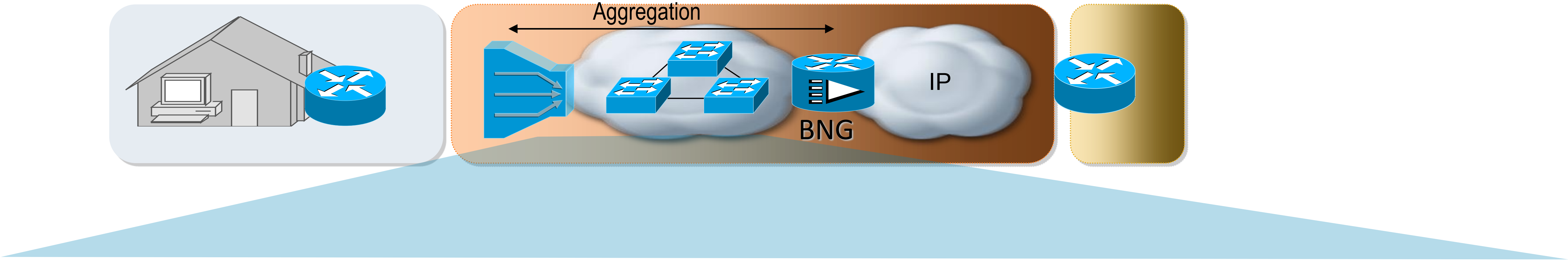
PPP to IP Session Comparison ….

For Your Reference

Session Requirement	PPP / PPPoE - Session	IP-Session
Subscriber Session Endpoint	PPPoE/PPP client	Multiple Options – Common: Device (see also “Identification”)
Subscriber Authentication (Authentication Protocol Selection)	PPP LCP Auth.Phase (PAP, CHAP,..)	MAC/Line-Authentication, Portal solutions, DHCP-Auth
Subscriber Isolation	Per-Session PPP encap	L3: Session Controller, ACLs, VRFs L2: VLAN, private VLAN
Subscriber/Session Identification	Session ID	Multiple Options (Interface, MAC, IP-address,…)
IP-Addressing	PPP NCP	DHCP, static, …
Session Health - Keepalive	PPP LCP	Multiple Options (ARP ping, ICMP ping, …)
Start/Stop Session	PPP LCP	Multiple Options (Packet arrivals, DHCP,…)
Traffic Encapsulation	PPPoE, PPP encap	none
Traffic Forwarding	Point to Point	Point to Point & Multipoint
Wholesale	PPP/L2TP	L3: VRF L2: VLAN, EoMPLS PW
Subscriber Mobility/Nomadism	Reestablish PPP-Session	Transparent Autologon, Portal solutions

Aggregation Service Delivery Models

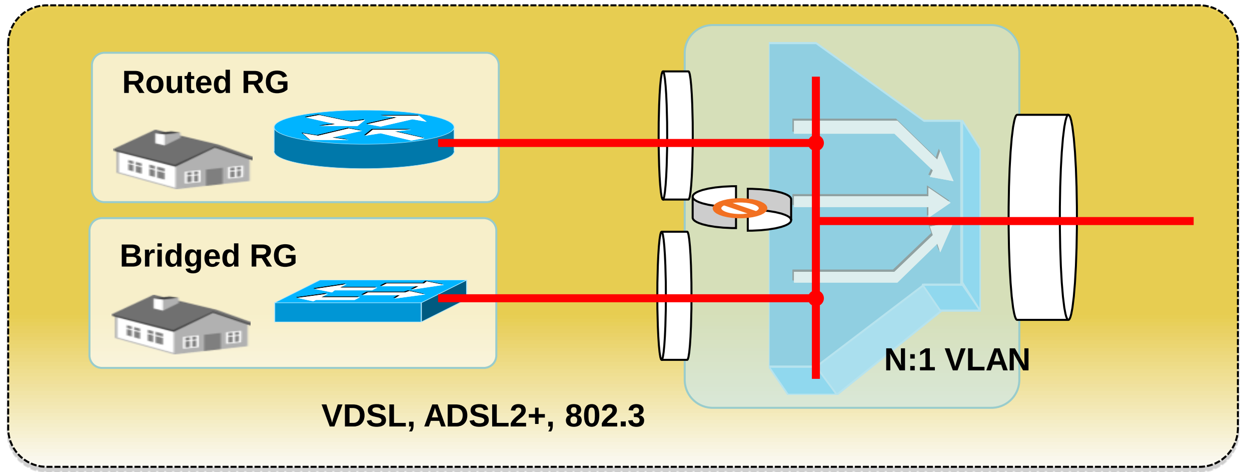
Aggregation Network Architectures



- Subscriber isolation is accomplished by:
  - Using VLANs (single and double tagging)
  - DSLAM filtering capabilities
  - Aggregation network filtering capabilities (split horizon forwarding)
- Several VLAN architectures are available for aggregation network
  - Based on broadband forum TR-101 recommendations
  - Choice of UNI model is access agnostic
    - 1:1 VLAN Model
    - N:1 Service VLAN
    - N:1 Shared VLAN
- Access Node as an 802.1ad Provider Edge Bridge

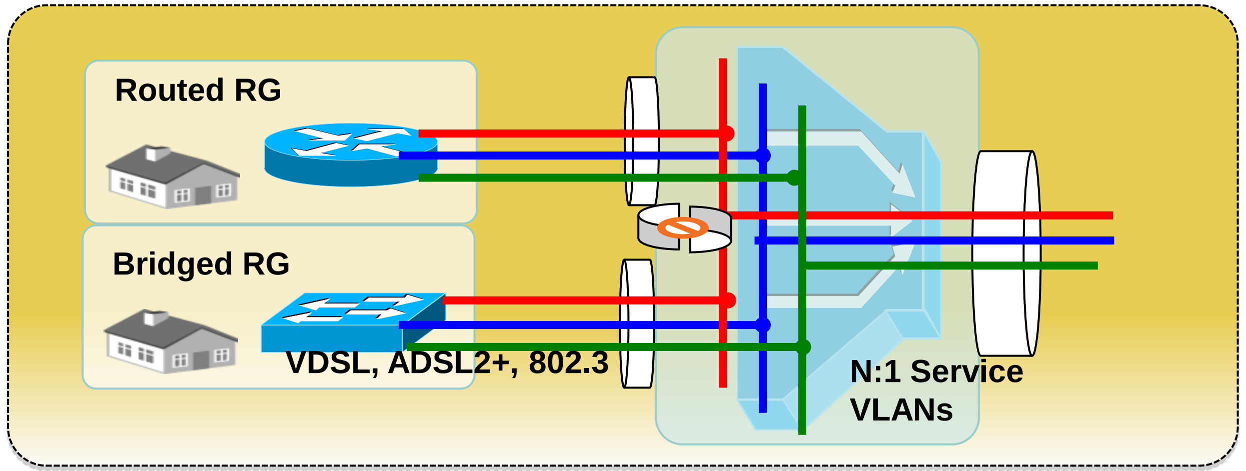
broadband forum

Service Delivery Models



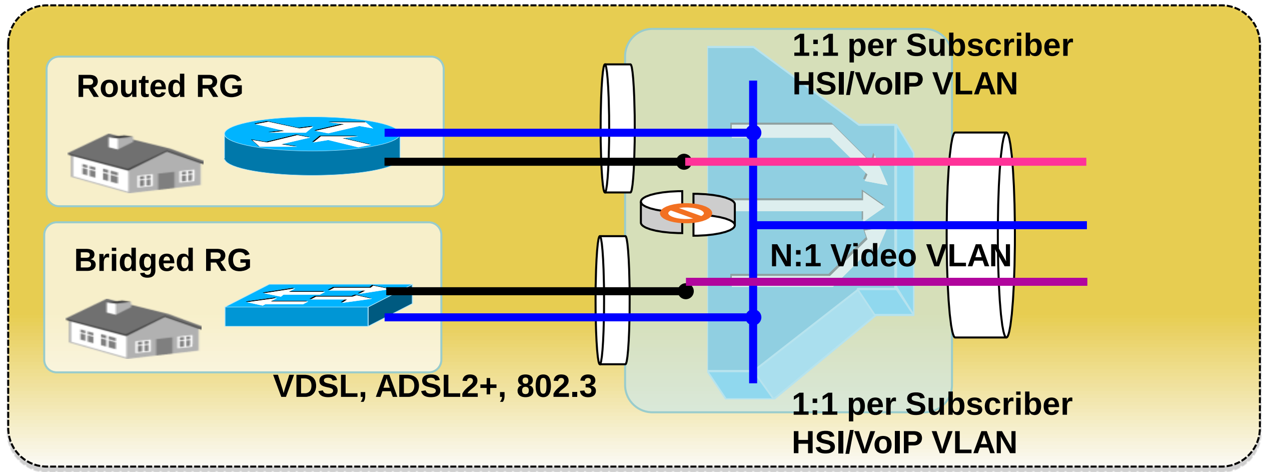
N:1 Shared VLAN Model

- CPE: Single VC or Ethernet priority tagged
- Access: Common 802.1q VLAN



N:1 Service VLAN Model

- CPE: Multi VC or Ethernet 802.1q tagged
- Access: Common 802.1q VLAN per service



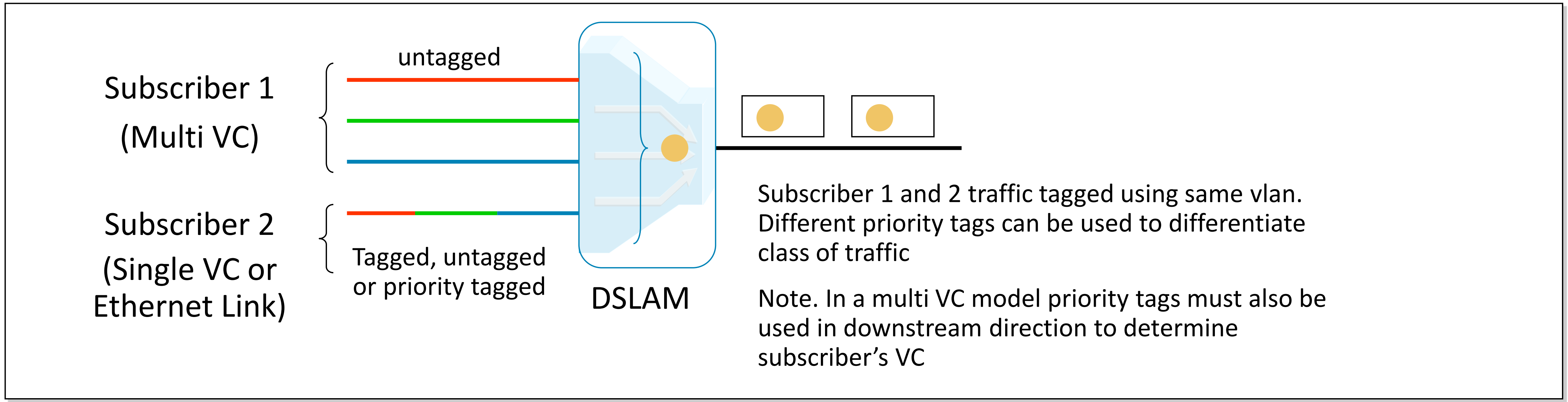
1:1 Access VLAN Model

- CPE: Multi VC or Ethernet 802.1q tagged
- Access: 1:1 per subscriber 802.1q VLANs for HSI/VoIP, Common 802.1q VLAN for Video

Aggregation Service Delivery Models

N:1 VLAN Model - Shared VLAN

- All service and subscribers carried over same VLAN
- Single tagging is used for subscriber traffic


Subscriber 1
(Multi VC)
untagged
Subscriber 2
(Single VC or Ethernet Link)
Tagged, untagged or priority tagged
DSLAM

Subscriber 1 and 2 traffic tagged using same vlan. Different priority tags can be used to differentiate class of traffic

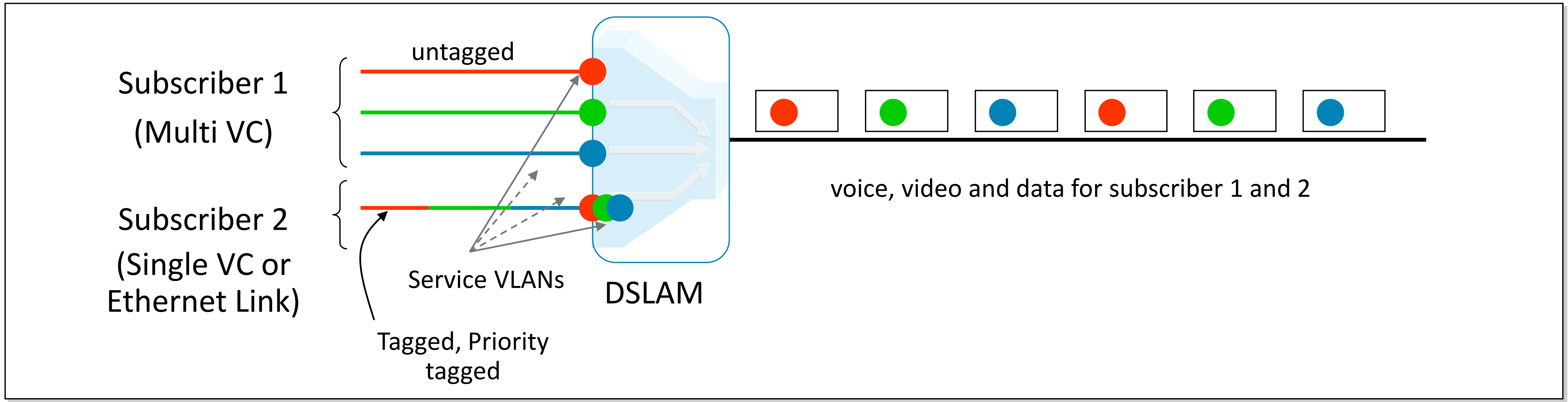
Note. In a multi VC model priority tags must also be used in downstream direction to determine subscriber's VC

- Simplest provisioning

Aggregation Service Delivery Models

N:1 VLAN Model - Service VLAN

- Requires that Services (one or more) can be uniquely identifiable by stack of vlan tags
- Typically single tagging is used for subscriber traffic:
  - – VLAN tag represents customer service

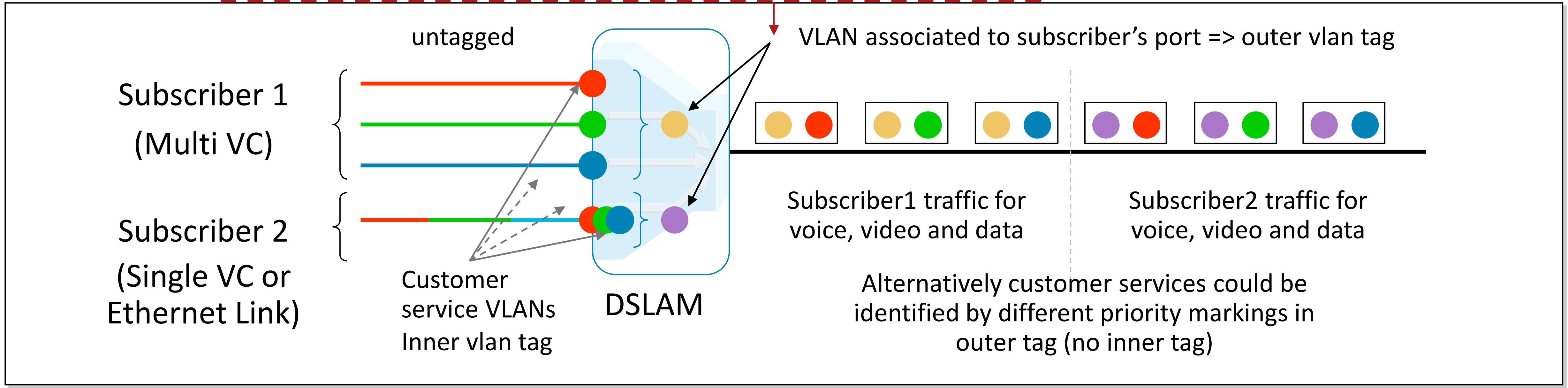


- Simpler provisioning (per service vs. per subscriber(/service))
- Multiple injection points per VLAN possible
- Multicast replication within access/aggregation
- Network Elements take care of subscriber L2 isolation through ‘split horizon forwarding’

Aggregation Service Delivery Models

1:1 VLAN Model

- Subscriber and Services (if any) must be uniquely identifiable by stack of vlan tags
- Typically uses dual tagging:
  - Outer vlan tag represents subscriber (or DSLAM); cannot be reused in aggregation network
  - Inner vlan tag represents customer service (or Port)



- VLAN use similar to ATM, i.e. Point To Point VC, i.e. configuration intensive
- Multicast replication inside Single BNG, not inside Ethernet Aggregation Network
- Multi-homing to two or more BNGs complex, additional configuration across aggregation network
- Good for p2p business services; less ideal for Triple-Play Services

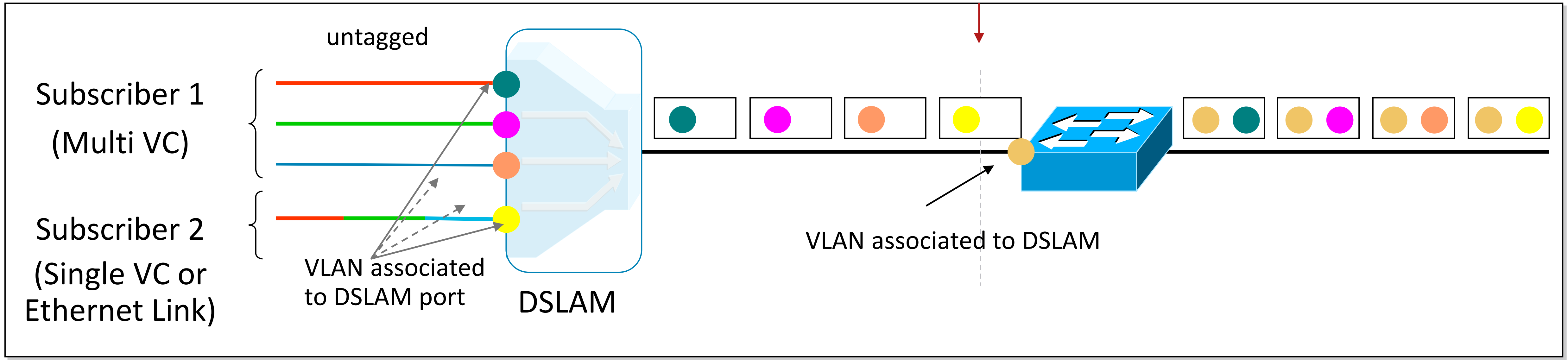
Aggregation Service Delivery Models

1:1 VLAN Model

- Subscriber and Services (if any) must be uniquely identifiable by stack of vlan tags
- Typically uses dual tagging:

  Outer vlan tag represents subscriber (or DSLAM); cannot be reused in aggregation network

  Inner vlan tag represents customer service (or Port)



- Outer VLAN tagging at first aggregation switch—DSLAM port vlan becomes inner vlan
- All DSLAMs configured alike—unique vlan per each port, vlan reused across DSLAM
- Limited functions at DSLAM -> reduces equipment costs and resources management
- Most common deployment of 1:1 VLAN model

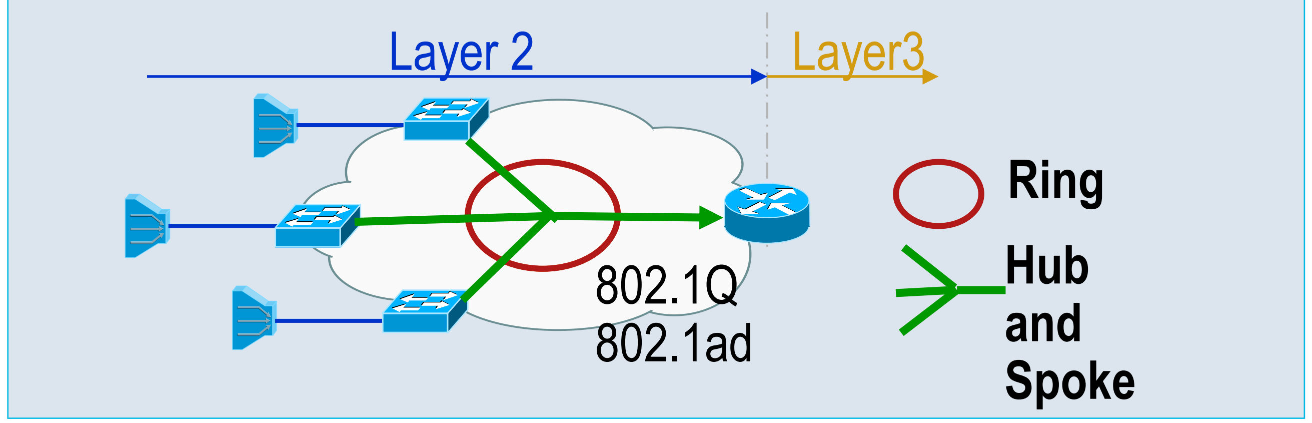
Residential Services and VLAN Models

For Your Reference

	Traffic Type	VLAN Model	Access Protocol
High Speed Internet (HSI)	Unicast	1:1, N:1	IPoE, PPPoE
Voice over IP (VoIP)	Unicast, Multicast	N:1	IPoE, PPPoE
Video on Demand (VoD)	Unicast	N:1	IPoE, PPPoE
Broadcast IPTV	Multicast	N:1	IPoE

Architecting Aggregation Network Subscriber Ethernet Transport Technologies

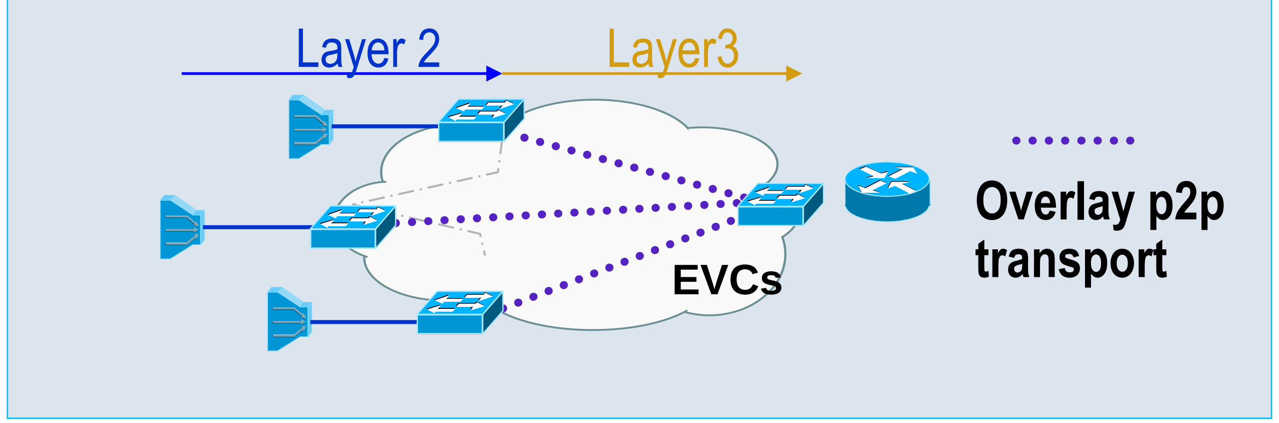
Layer 2 – Bridged Ethernet
IEEE 802.1q / 802.1ad



- Point to Cloud Service Access (*)
- Supports distributed Service Insertion ("Multi-Edge")*
- Flexible Transport for many Services (well suited for 3Play—Efficient Multicast distribution with IGMP Snooping)
- Virtualised Layer-2 Services (with VLANs)
- Control Plane Resiliency: Requires STP or special solutions with constrained topologies
- Additional Support of: Mobile RAN, Legacy ATM/FR/TDM with L2TPv3

* With IPoE

Layer 3 – MPLS
EoMPLS/ H-VPLS (EVCs)



- Point to Cloud and Point to Point Service Access
- Allows different or common Administrative Domains
- Supports virtualised Layer 2 and 3 services thru MPLS VPNs (EoMPLS and H-VPLS -> EVC)
- Pseudo Wire (PW) used to transport Layer 2 domain across MPLS/IP network
- Supports Traffic Engineering; Fast Restoration
- Efficient Multicast, natively (PIM) or with multicast MPLS
- Additional Support of: Mobile RAN, Legacy ATM/FR/TDM with MPLS AToM

Bridged Ethernet, N:1 Service VLAN

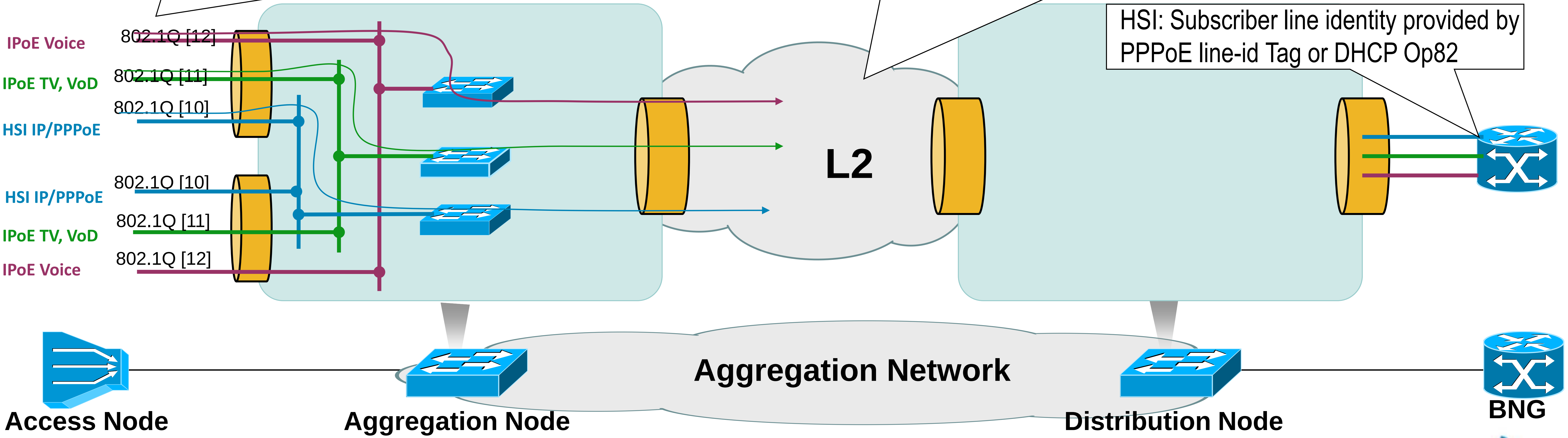
Residential Service Connectivity Overview

- Shared Service VLANs, end to end significance
- HSI: Isolation for IPoE subscribers requires Private Vlan deployment
- IPTV: IGMP Snooping implemented in aggregation Node for optimised multicast replication

- HSI: Isolation for IPoE subscribers requires

  Private VLAN deployment in aggregation network, or

  Dedicated Service VLAN per Aggregation Node (1:1)
- IPTV: IGMP Snooping implemented in aggregation network for optimised multicast replication



HSI: Subscriber line identity provided by PPPoE line-id Tag or DHCP Op82

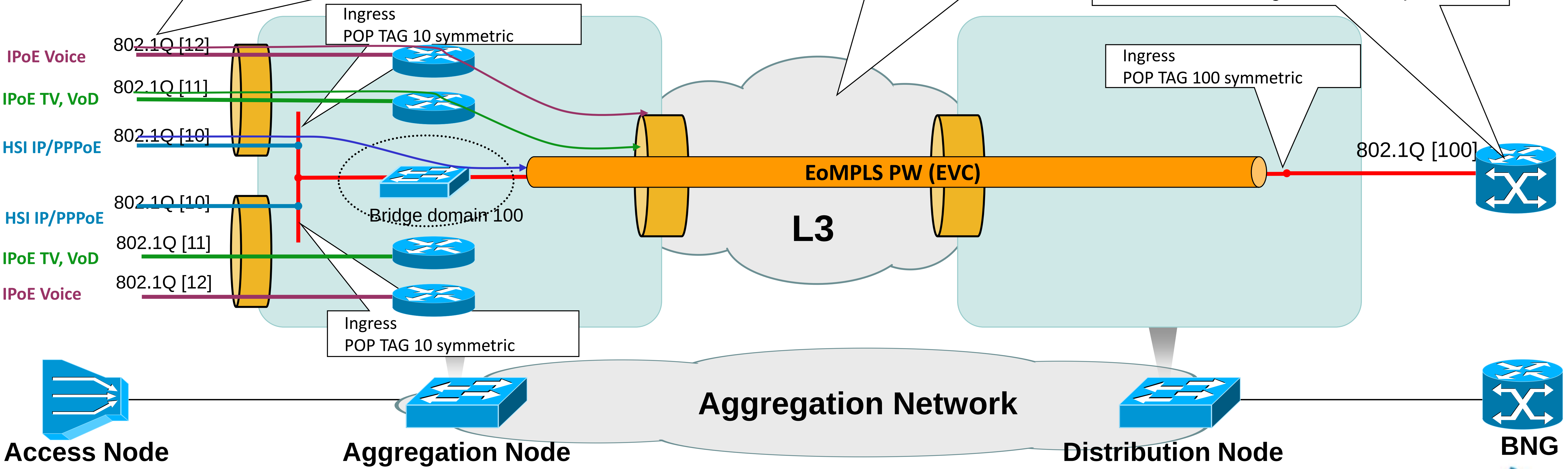
MPLS, N:1 Service VLAN

Residential Service Connectivity Overview

- Service VLAN, local significance
- HSI: Bridge Domain with split horizon for all connected Access Nodes
- IPTV/VoD: mapped to SVI running IP unicast
- IPTV: IGMP/PIM implemented in aggregation Node for optimised multicast replication

- HSI: EoMPLS (EVC), one pseudowire per Aggregation Node
- IPTV: PIM implemented in aggregation network for optimised multicast replication

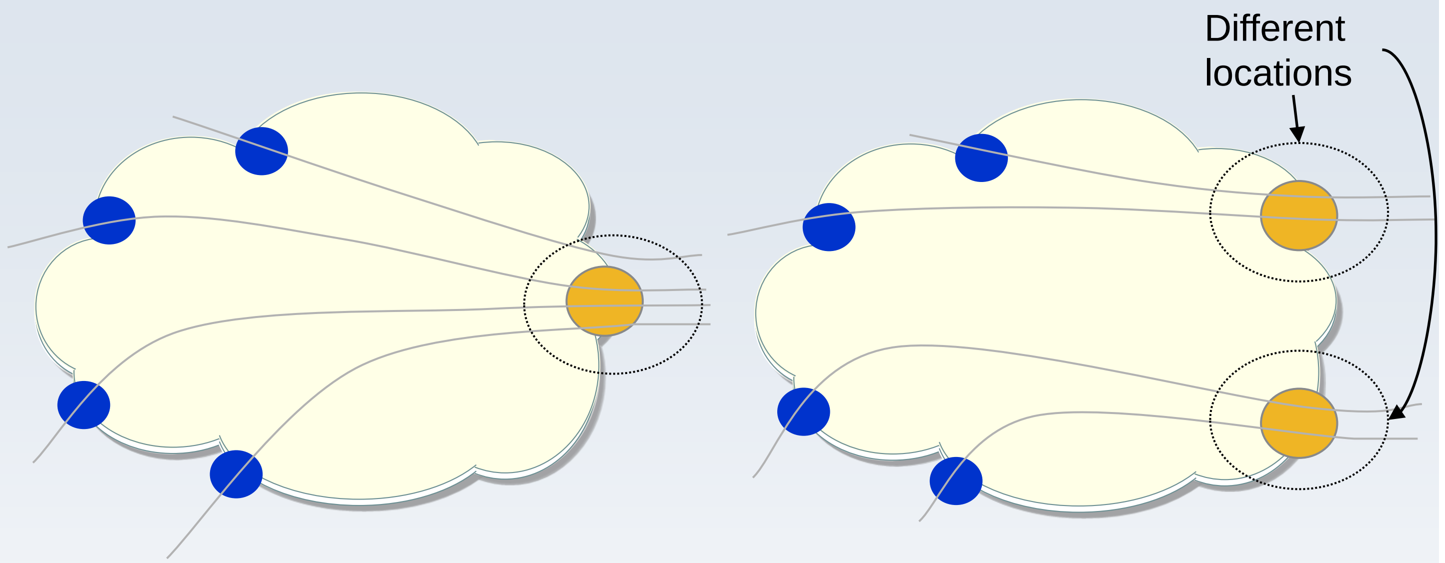
HSI: Subscriber line identity provided by PPPoE line-id Tag or DHCP Op82



Edge Network Architectures

Architecting the IP Edge

Centralised versus Distributed



Edge systems are concentrated in 1 or few IP PoPs and are connected to aggregation nodes via an aggregation network

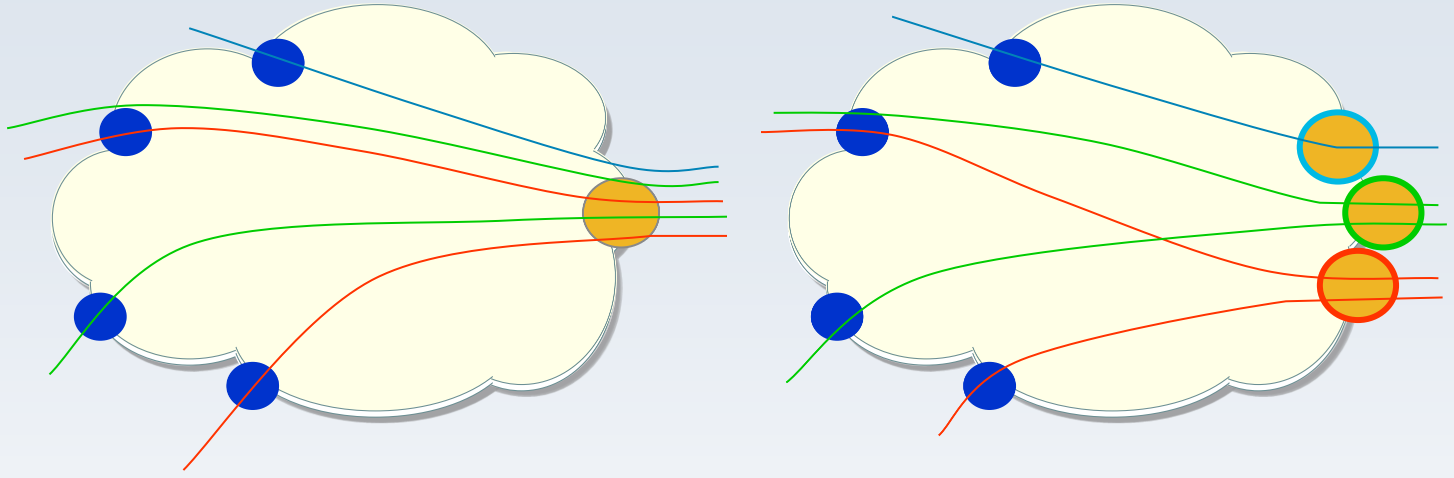
(Existing HSI architecture)

Edge systems are dispersed in many IP PoPs closer to subscribers and may even be co-located with aggregation nodes

● Aggregation Node (AgN)

● Multi-Service Edge Node

Single Edge versus Multi Edge



All services destined to same subscriber flow through one edge system, forming an integrated policy enforcement point

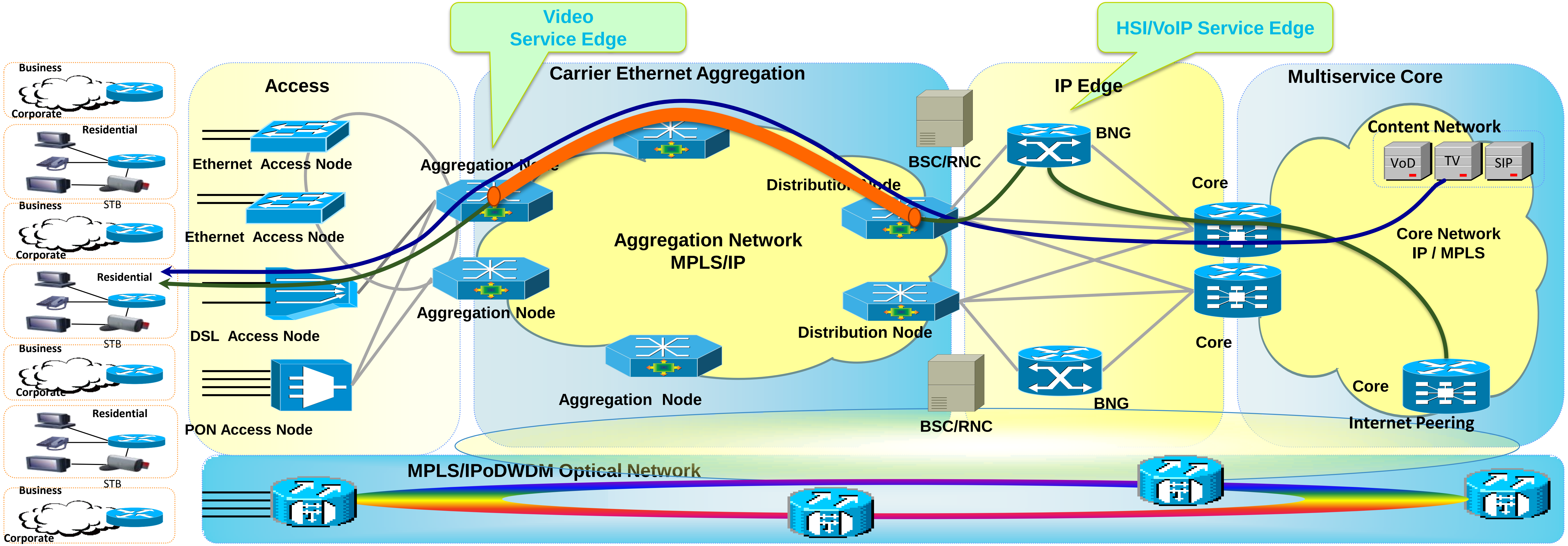
Services destined to same subscriber may be handled by different “service specific” edge systems

● Application Specific Edge Nodes

─	Voice Traffic
─	Video Traffic
─	Data Traffic

Hybrid Service Edge

MPLS/IP Packet Aggregation for 3play Service Delivery



Video Service Edge

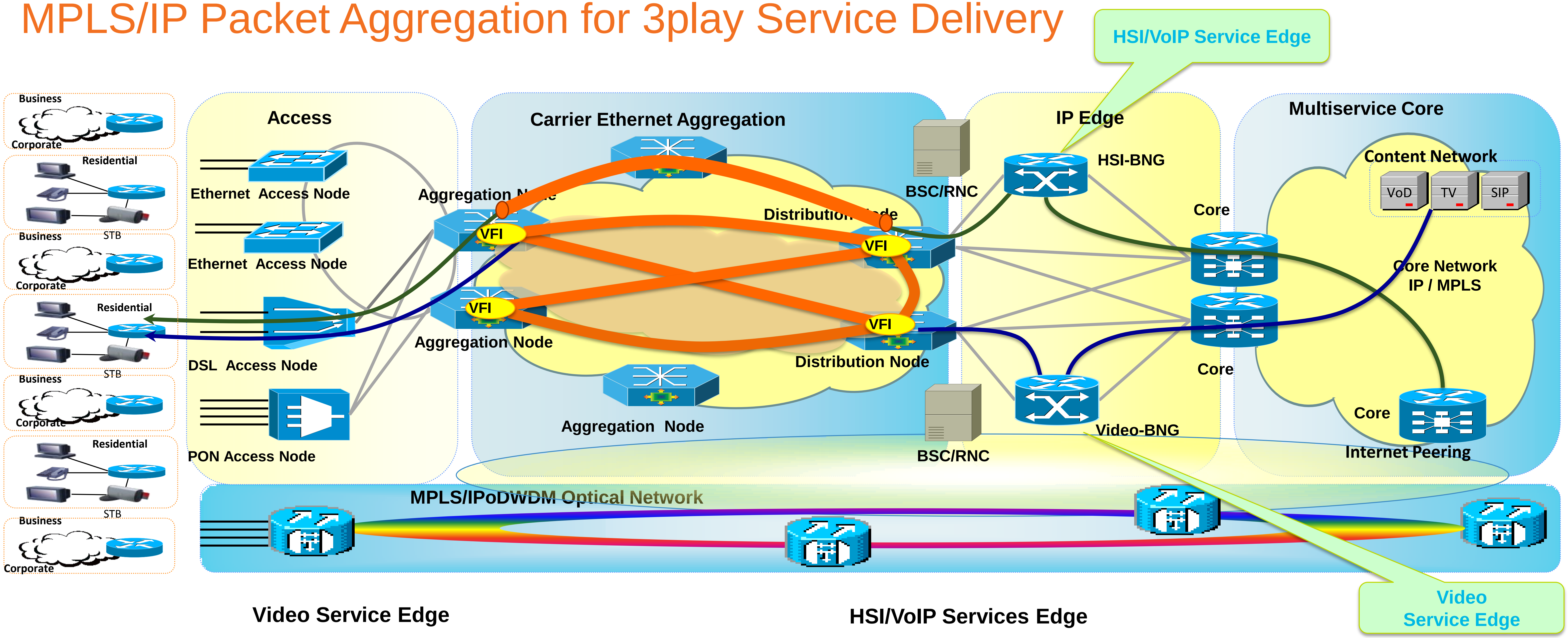
- Implemented on Aggregation Node
- Layer-3 MPLS/IP unicast VoD and multicast IPTV transport for video service distribution

HSI/VoIP Services Edge

- Implemented on Centralised BNG
- IPoE and PPPoE service transport over 802.1Q and QinQ interfaces enabled by per subscriber ISG sessions

Centralised Service Edge

MPLS/IP Packet Aggregation for 3play Service Delivery



Video Service Edge

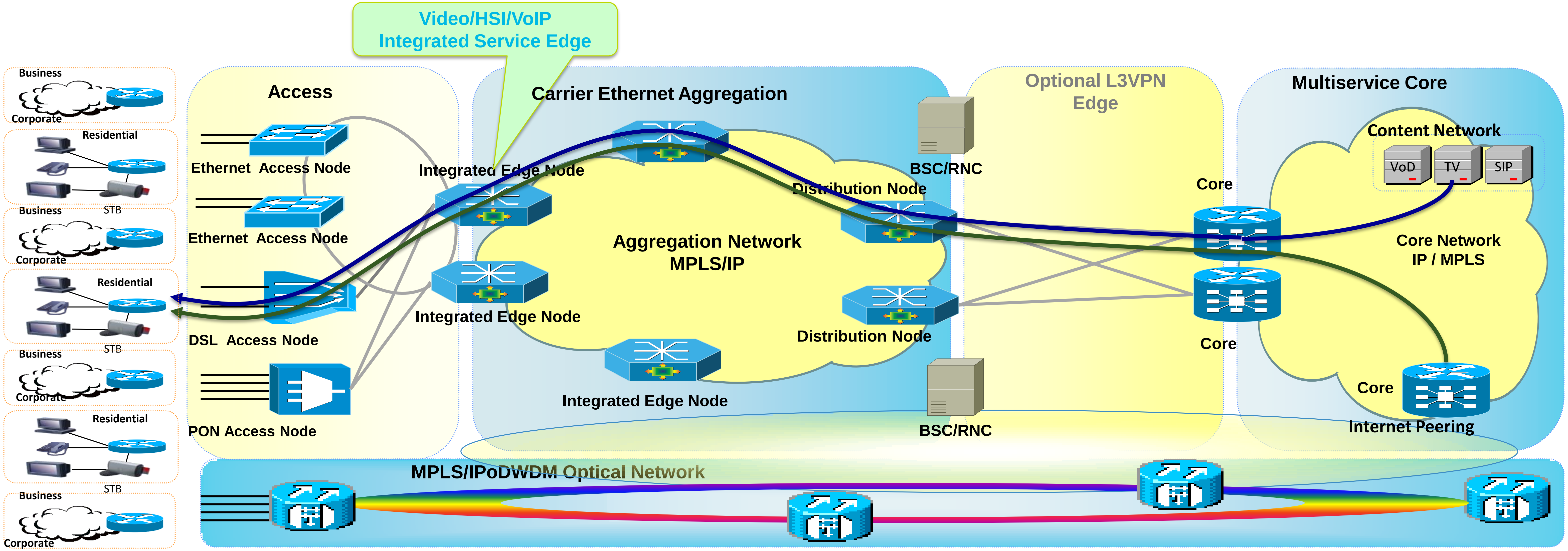
- Implemented on Centralised Video-BNG
- Layer-2 VPLS transport of unicast VoD and multicast IPTV for video service distribution

HSI/VoIP Services Edge

- Implemented on Centralised HSI-BNG
- IPoE and PPPoE service transport over 802.1Q and QinQ interfaces enabled by per subscriber ISG sessions

Distributed Service Edge

MPLS/IP Packet Aggregation for 3play Service Delivery

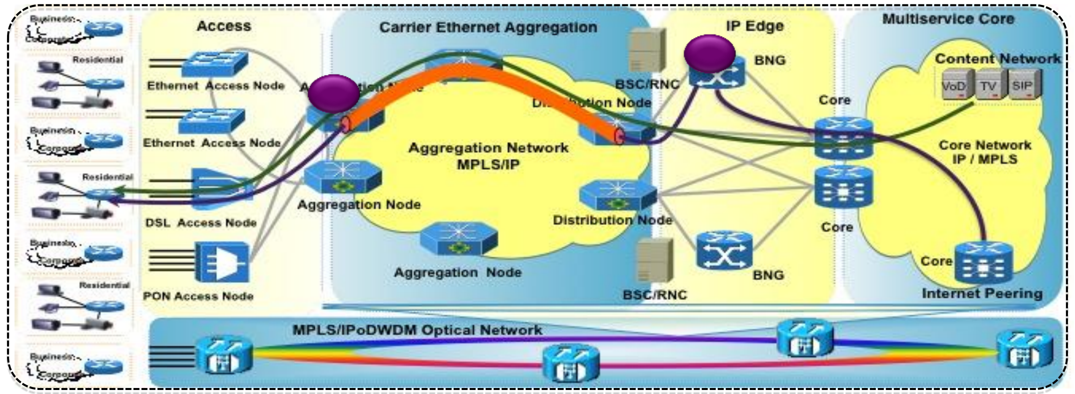


3Play Service Edge

- Implemented on Integrated Edge Node
- Unicast services (HSI/VoIP/VoD) enabled by IPoE or PPPoE per subscriber ISG sessions
- Multicast services (IPTV) coexist with ISG sessions
- Aggregation network implements MPLS/IP for unicast and IP multicast for service transport

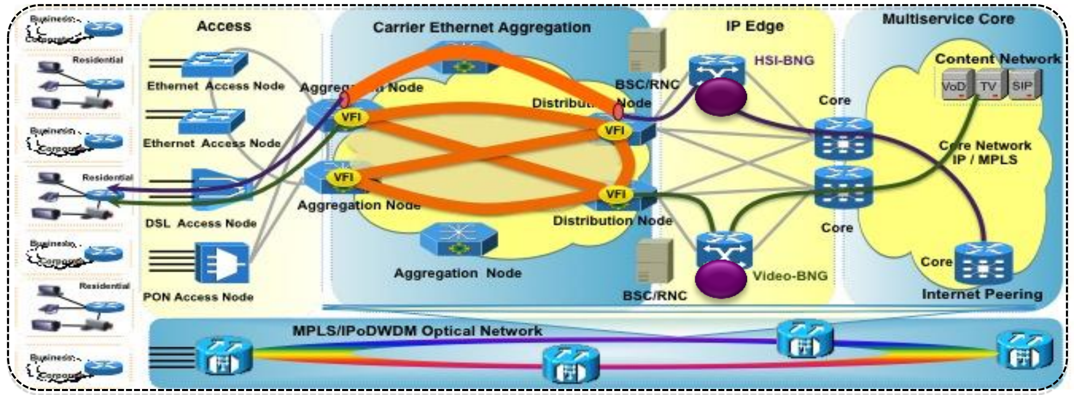
Architecture Comparisons

Typical Deployments



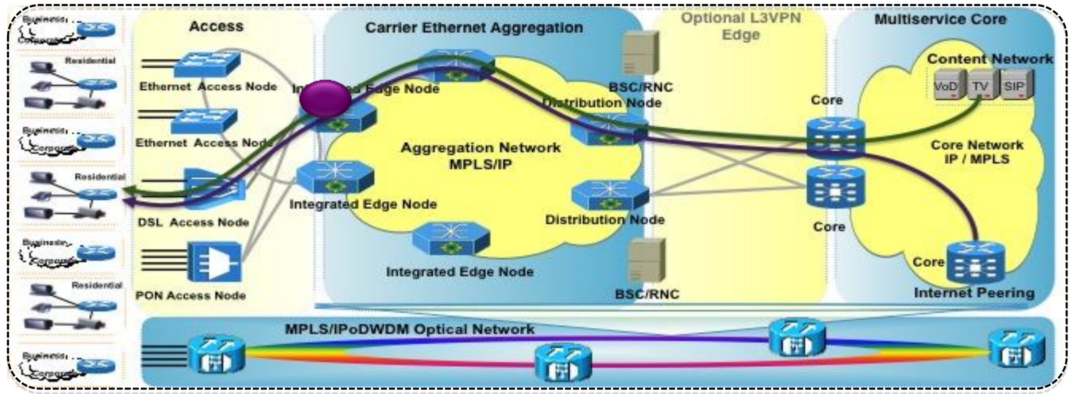
Hybrid-Edge Deployment

- Derived from TR-101
- SP first deployed Internet service and then added Video service
- Legacy HSI-BNG untouched – Collocated/Integrated Video-BNG introduced
- Smaller 3Play subscriber base



Centralised-Edge Deployment

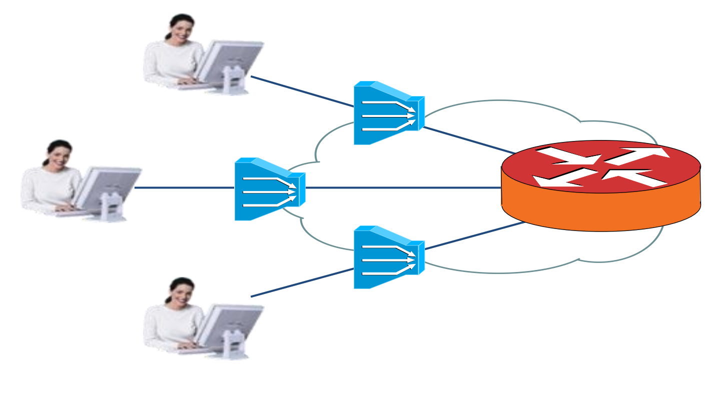
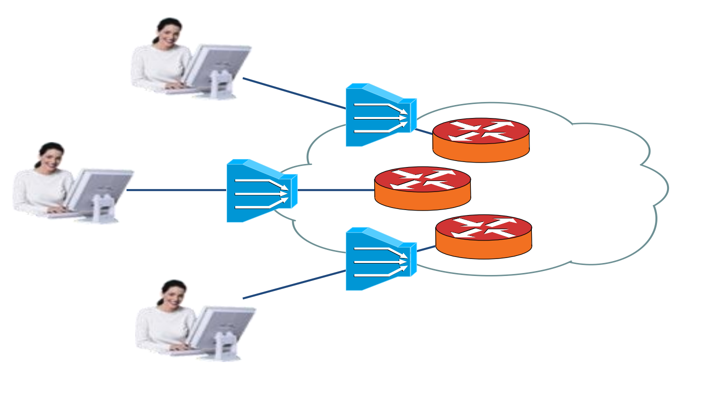
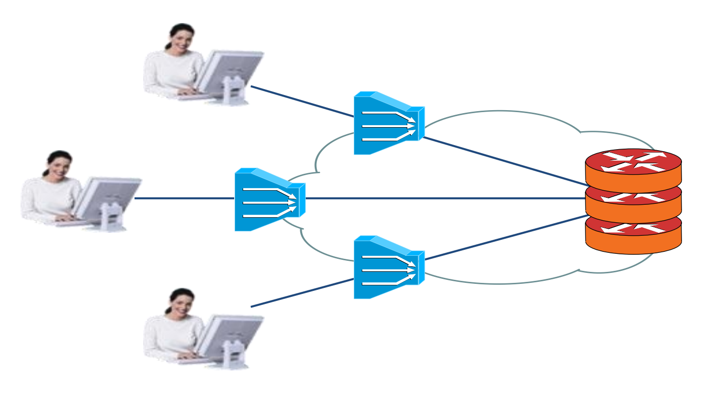
- Aggregation & Edge networks typically operated by different departments
- Edge concentrated in few Centralised PoPs - Benefits from incumbency, evolution of existing architecture
- Operational simplicity – Centralised subscriber provisioning & maintenance
- Requires Service Edge Nodes capable of handling large scale



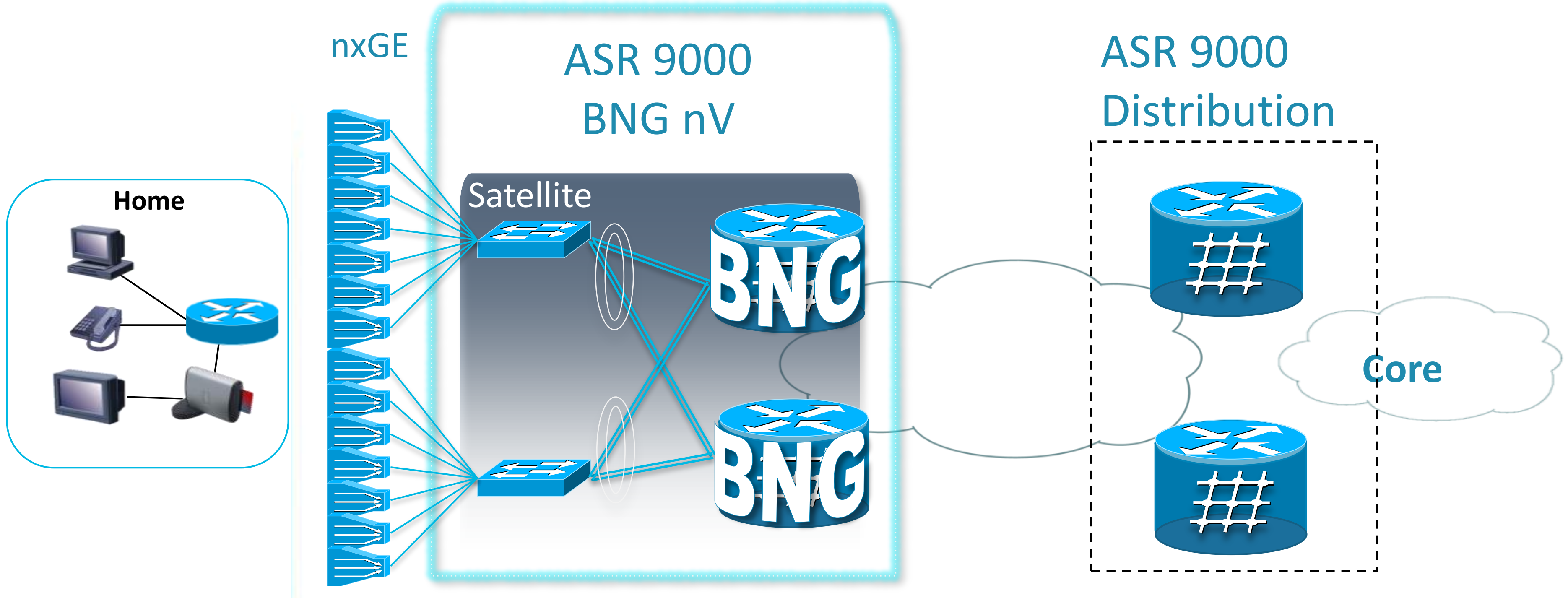
Distributed-Edge Deployment

- Edge fully-distributed in Aggregation Network - Requires Integrated Multi Service Edge Nodes
- Distributed subscriber provisioning & maintenance
- Edge placement close to subscriber - efficient bandwidth utilisation and best scaling properties

IP Edge Architectures Comparison

		Scalability	Availability	Operations
Centralised		▪ Limited (number of users, call-setup-time bandwidth per user) ▪ Example: 2.7Mbps/User; 60k Users: Already requires 160 Gbps engine	▪ Large failure domain ▪ Long time to re-establish sessions after failure ▪ Example: 100cps; 200k Users: 33min to create all sessions	▪ Central Address Pool Management ▪ Centralised Management ▪ Requires per-user access network provisioning for 1:1 VLAN or ATM
Distributed		▪ Scales with the number of devices	▪ Small failure domain ▪ Fast boot/recovery time	▪ Distributed Address Pool Management (Fragmentation) ▪ Distributed Management ▪ No/Limited L2-access ▪ Efficient Multicast & Peer-to-Peer traffic
Clustered		▪ Scales with the number of devices	▪ Small failure domain ▪ Fast boot/recovery time	▪ Central Address Pool Management (Pool per cluster) ▪ Centralised Management ▪ Requires per-user access network provisioning for 1:1 VLAN or ATM

Satellite + Cluster (4.3.0)



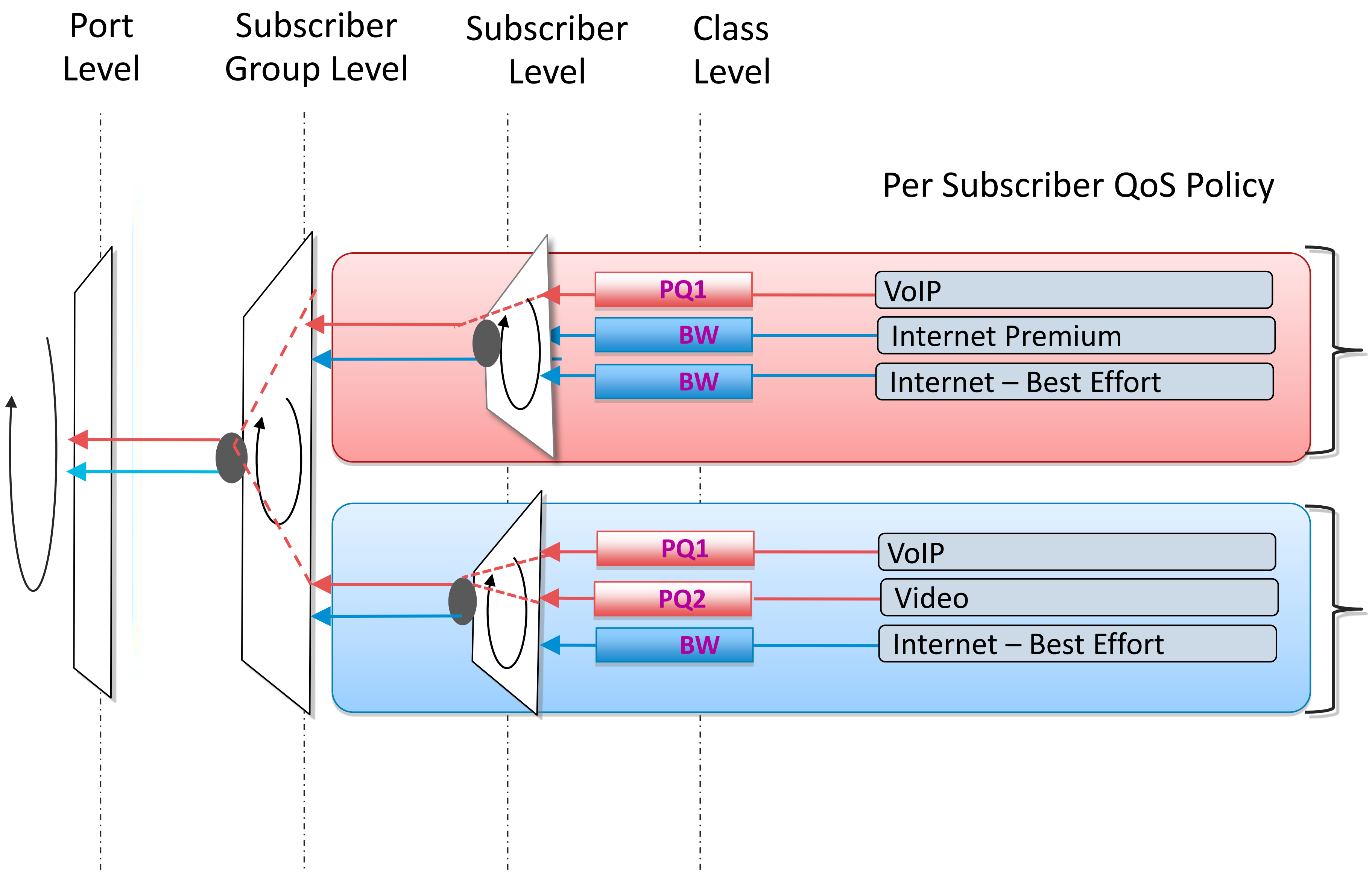
- Geo-redundant Dual Homing
- High Availability
- Huge 1GE Fan-out toward DSLAM
- Single-Chassis-like look & feel and Management of Cluster Members and Satellite
- Satellites appear like ASR 9000 Linecards
- Simplified topology, No Spanning tree/MC-LAG or other L2 redundancy protocols needed

Quality of Service (QoS)

- QoS Residential Model Overview
- Residential QoS for N:1
- Residential QoS for 1:1

Residential H-QoS Model

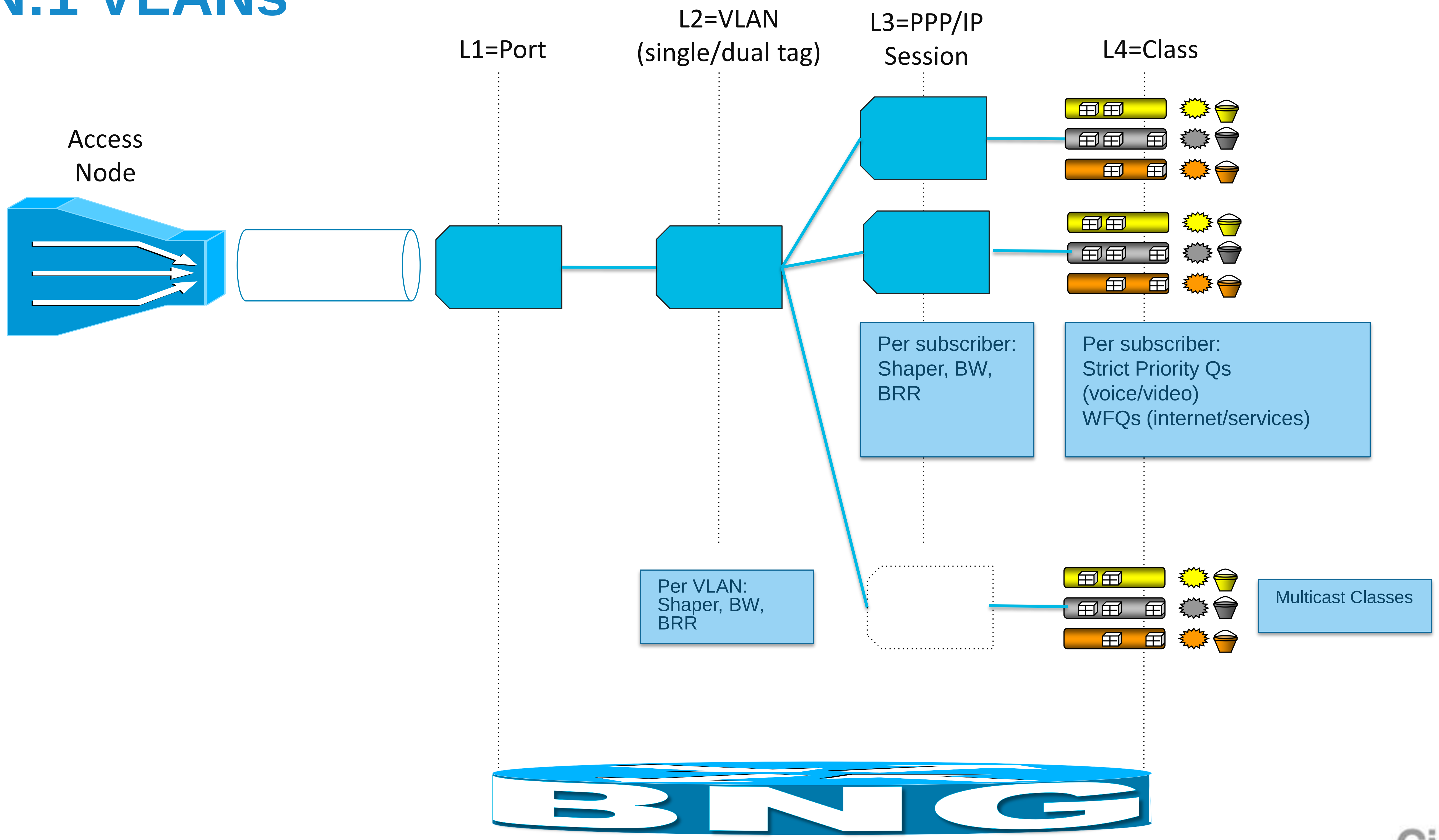
4-Level Hierarchy



Key Features

- Hierarchical SLA for all subscribers in the system
- 3 Strict Priority queues (ASR9K) / 2 Strict Priority queues (ASR1K)
- Aggregate Traffic Policers for capacity planning and disaster insurance
- Scalable WRED
- 2R3C policers, hierarchical policing
- 4 layers H-QOS
- Voice and Video grade Priority scheduling with priority propagation for minimum latency & jitter

4-Layer - Hierarchical QoS and Scheduler Node Hierarchy for N:1 VLANs



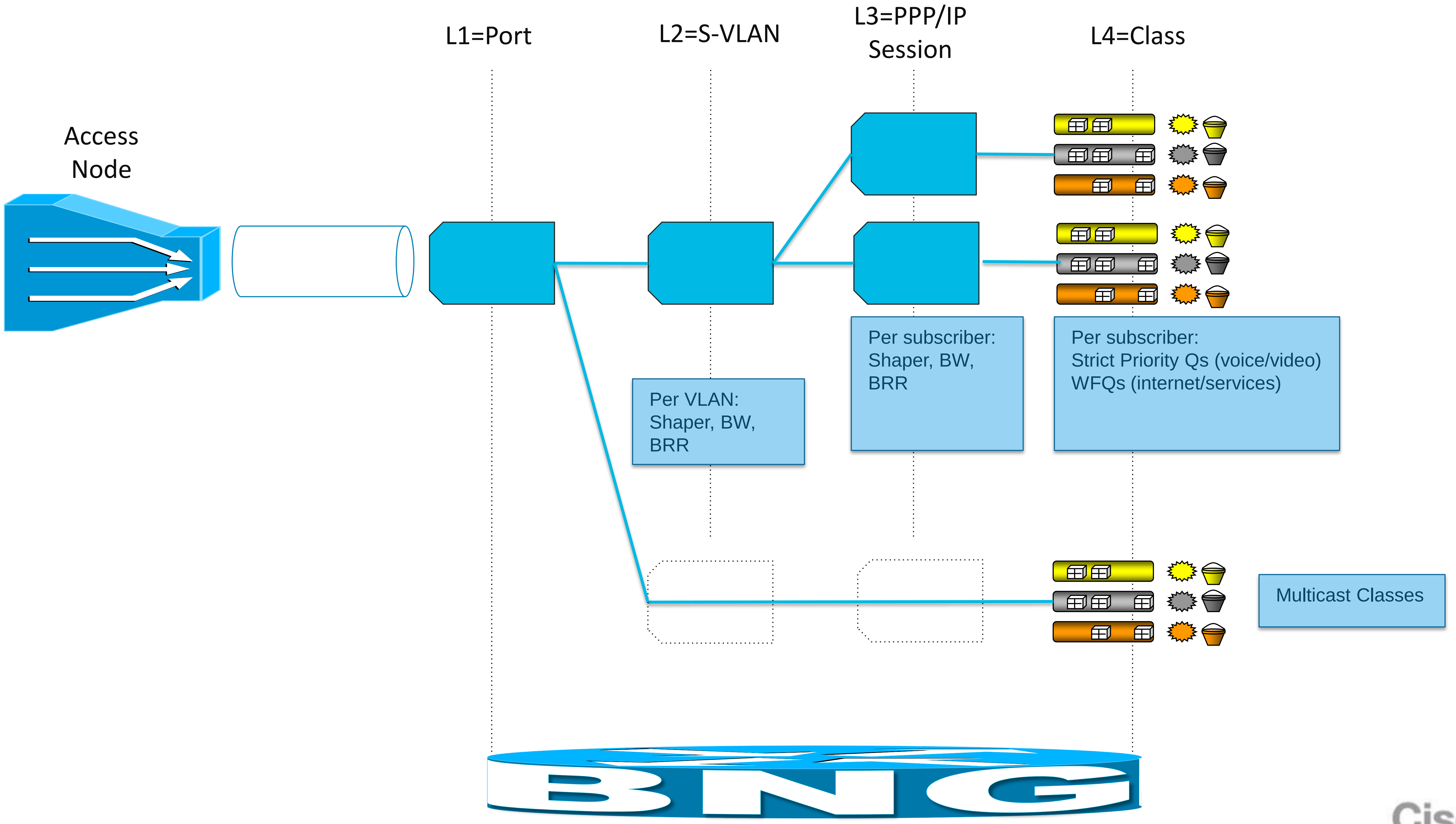
Per subscriber: Shaper, BW, BRR

Per subscriber: Strict Priority Qs (voice/video) WFQs (internet/services)

Per VLAN: Shaper, BW, BRR

Multicast Classes

4-Layer - Hierarchical QoS and scheduler node hierarchy for 1:1 VLANs



Per VLAN:
Shaper, BW,
BRR

Per subscriber:
Shaper, BW,
BRR

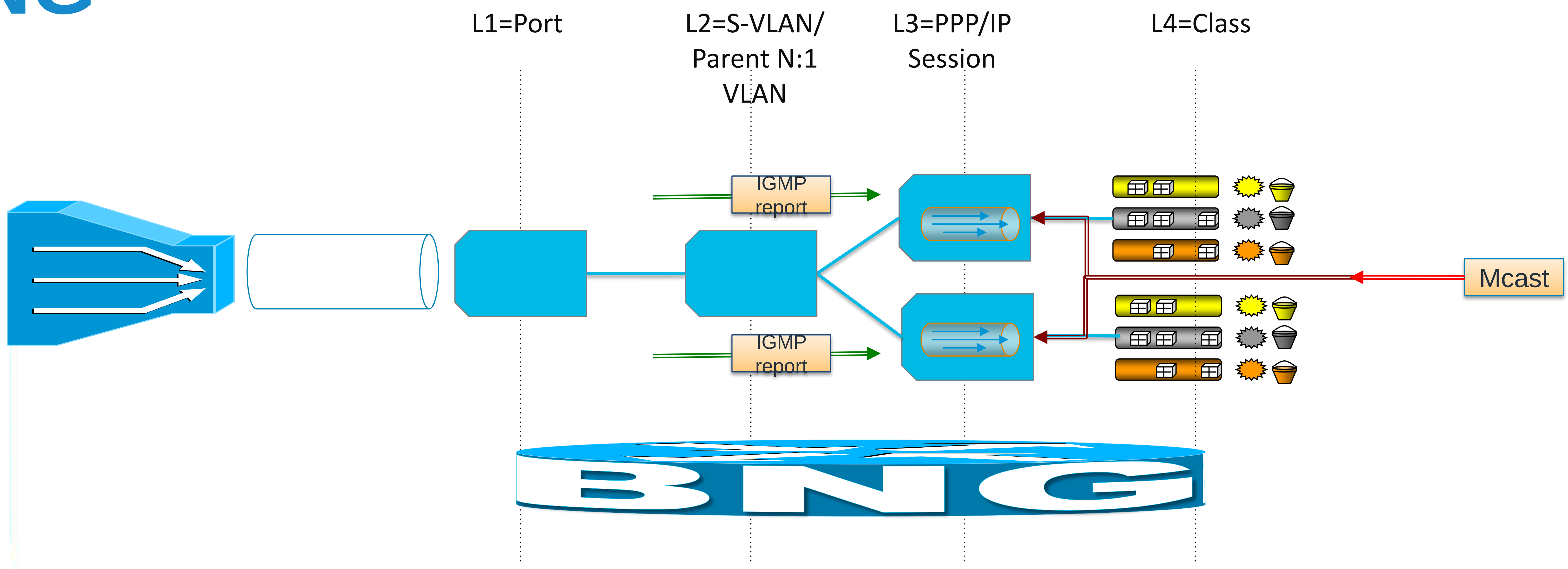
Per subscriber:
Strict Priority Qs (voice/video)
WFQs (internet/services)

Multicast Classes

Multicast

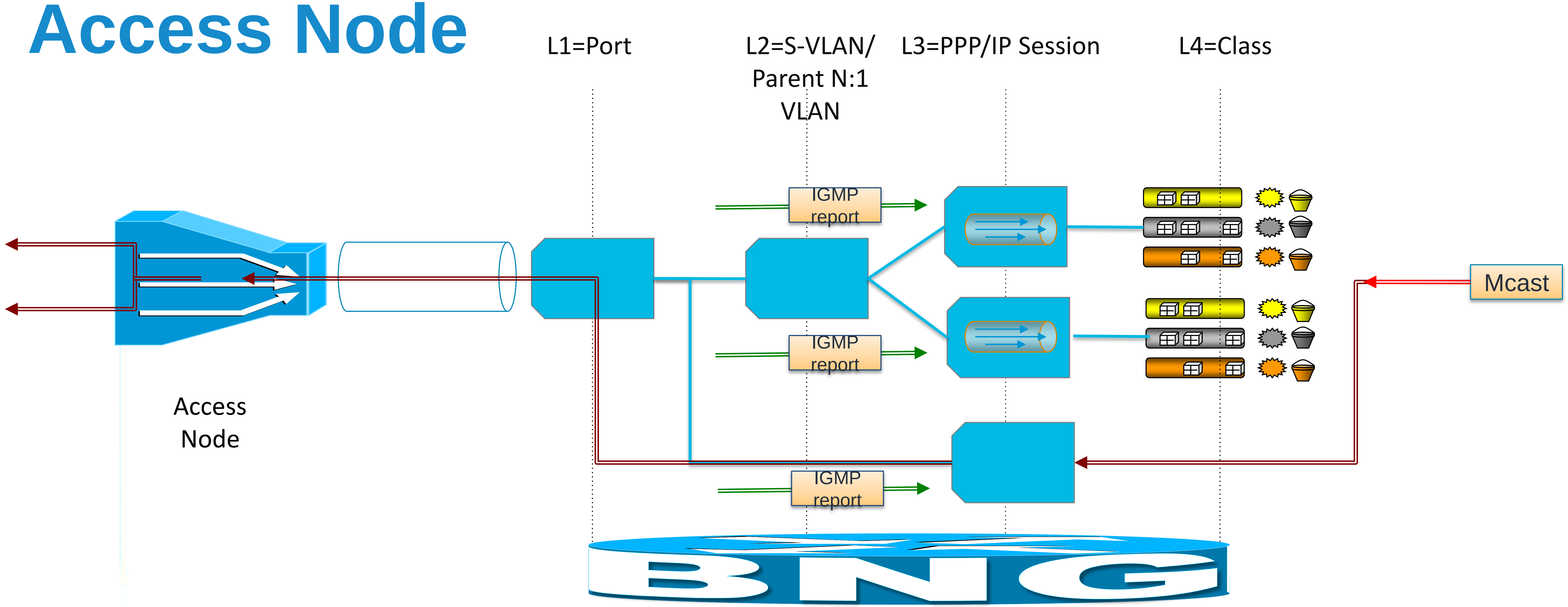
- Multicast and Per Subscriber Replication on BNG
- Multicast and Per Subscriber Replication on Access Node

Multicast and Per Subscriber Replication on BNG



- Multicast goes through subscriber session
- Subscriber Shaper enforces all subscriber traffic
- Access node is NOT involved in multicast, can remain simple

Multicast and Per Subscriber Replication on Access Node

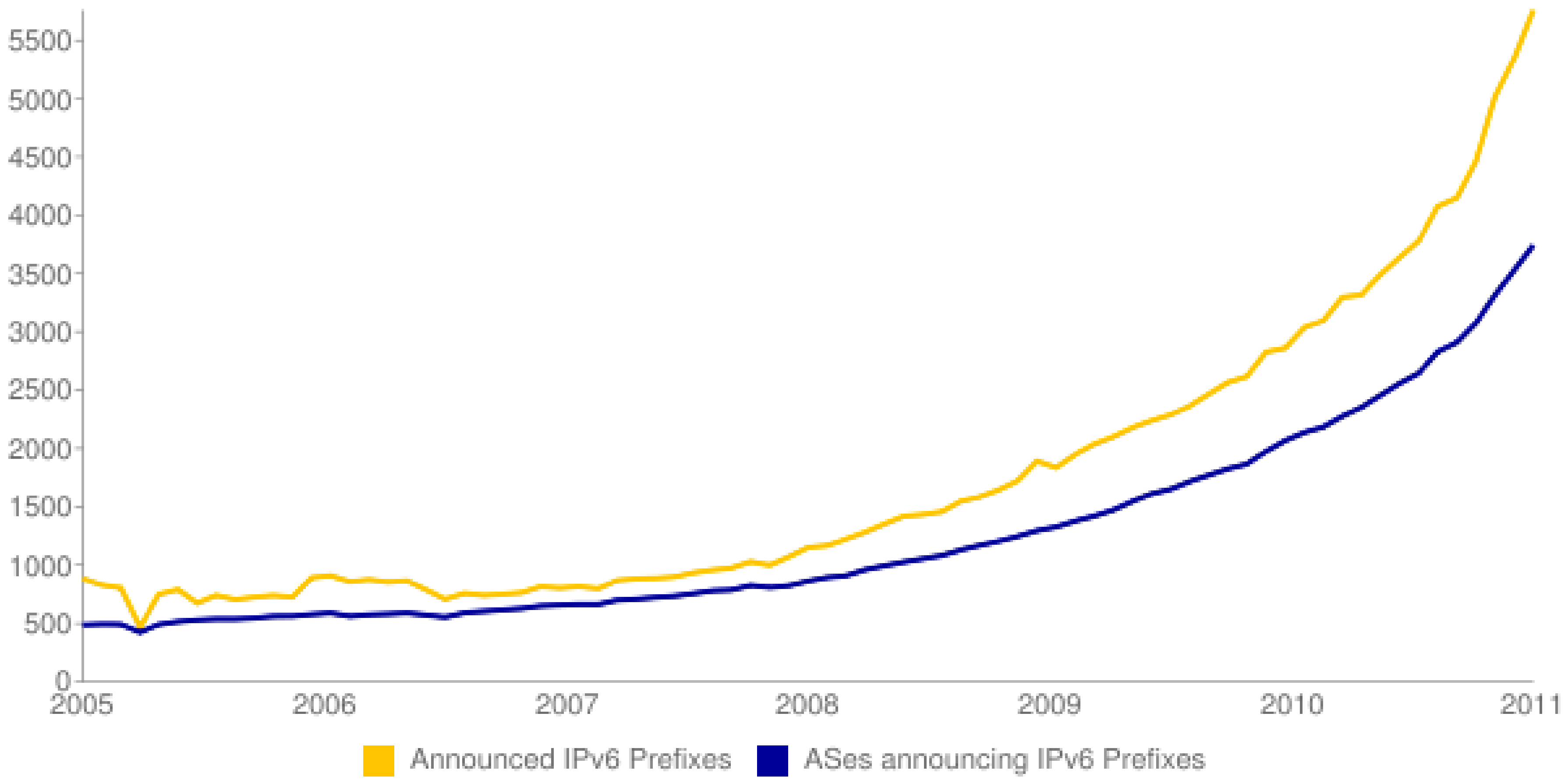


- Multicast does not go through subscriber session
- A separate VLAN interface provides N:1 Multicast forwarding towards DSLAM
- Access node is involved in multicast, needs to support IGMP snooping, security

IPv6 Solutions

State of IPv4 Address Space

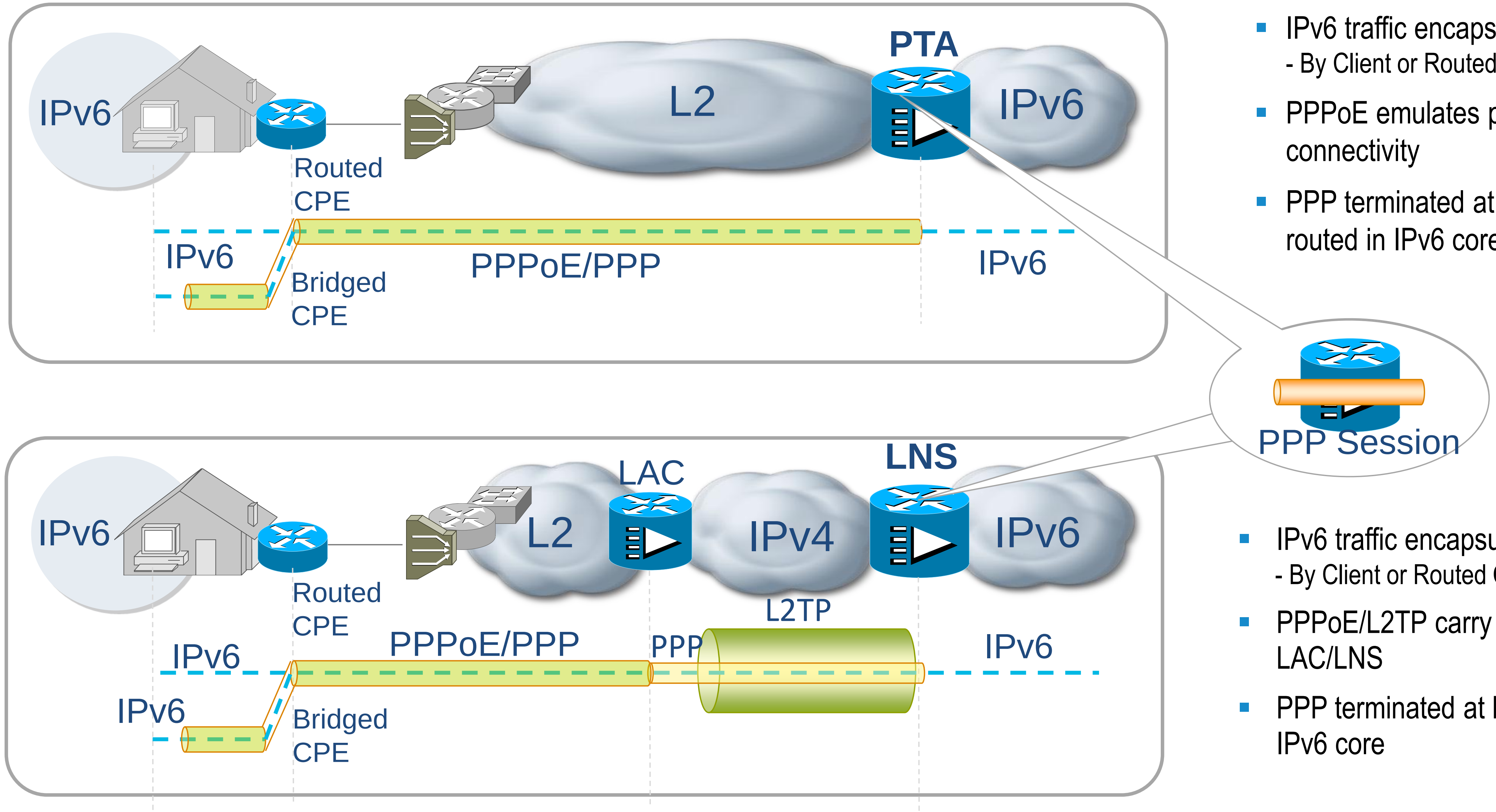
- IANA's central pool of available IPv4 addresses was exhausted on February 1st, 2011.
- February 3rd , 2011, the five RIRs each received one of the IANA's five reserved /8 blocks. One /8 is equal to 16.8 million IPv4 addresses.



Cisco IPv6 Solutions for Subscriber Aggregation

- IPv6 for PPP Subscribers
- IPv6 for IP and PPP Subscribers
- Dual Stack for IP and PPP Subscribers
- 6RD for IP and PPP Subscribers

IPv6 for PPP Subscribers

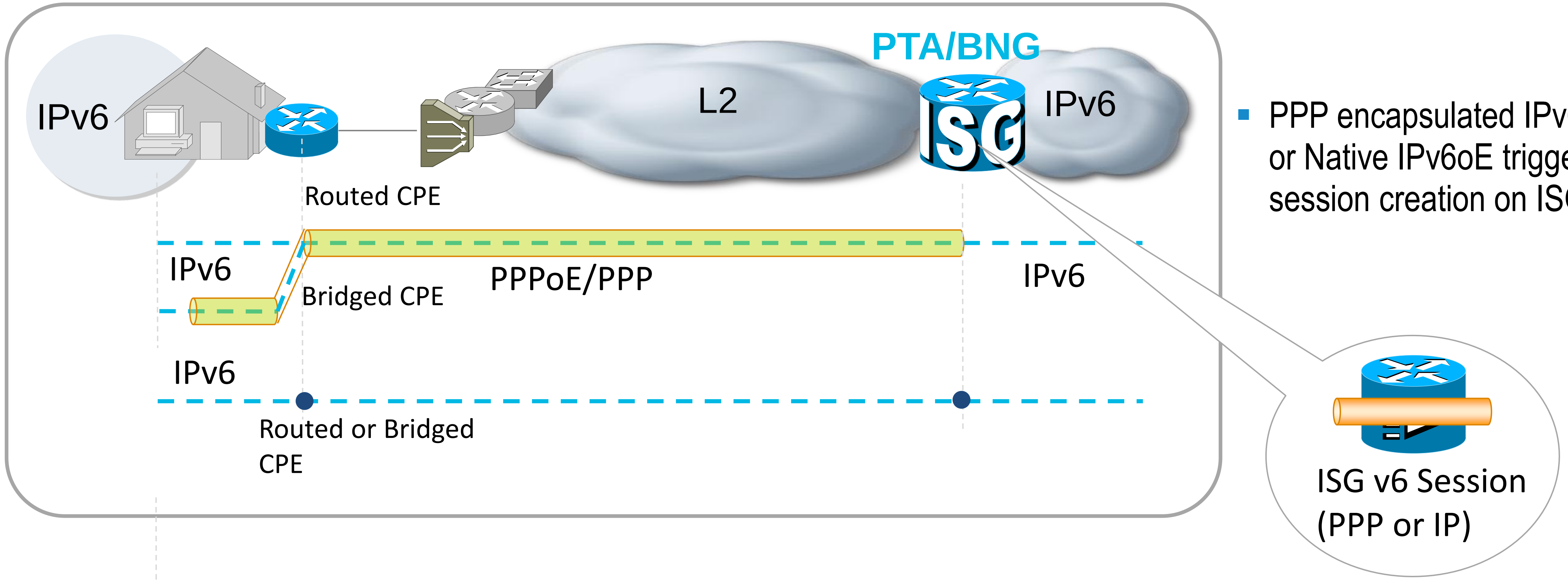


- IPv6 traffic encapsulated in PPP
  - By Client or Routed CPE
- PPPoE emulates point to point connectivity
- PPP terminated at PTA - traffic routed in IPv6 core

- IPv6 traffic encapsulated in PPP
  - By Client or Routed CPE
- PPPoE/L2TP carry PPP frames to LAC/LNS
- PPP terminated at LNS - traffic routed in IPv6 core

- Allow for IPv6 deployment at residential premises
- Address IPv4 address exhaustion

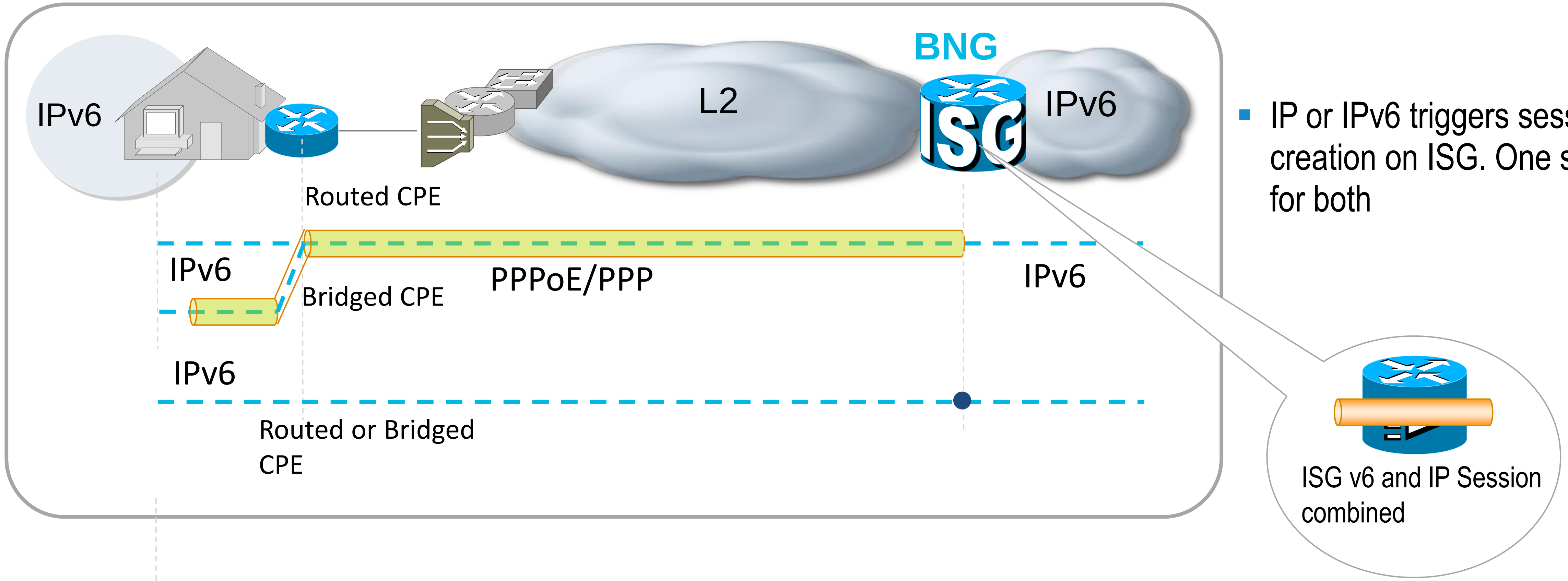
IPv6 for IP and PPP Subscribers



- PPP encapsulated IPv6 traffic or Native IPv6oE triggers session creation on ISG

- Allow for IPv6 deployment at residential premises
- Address IPv4 address exhaustion

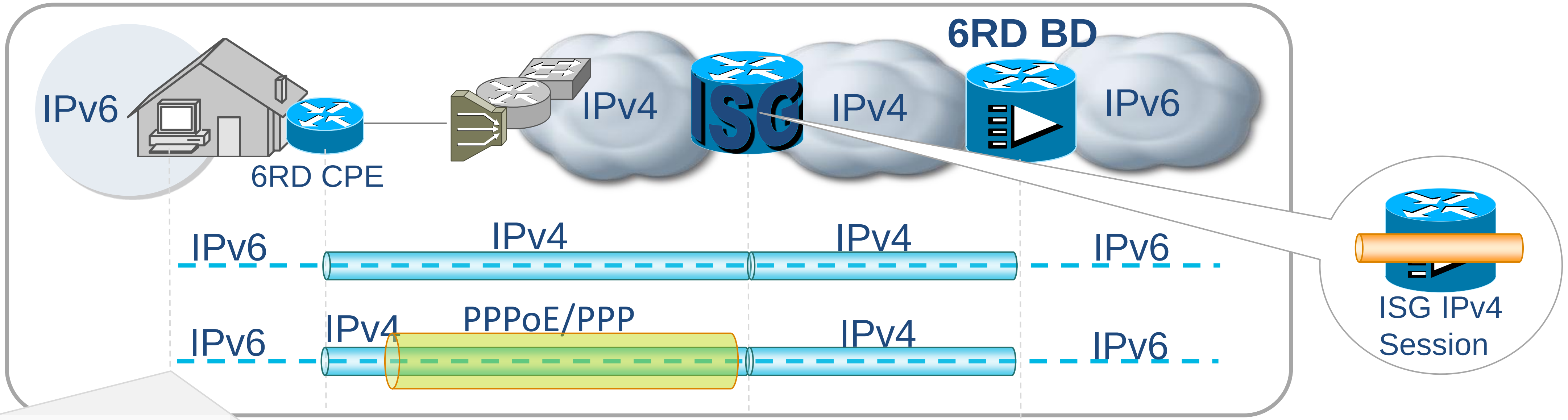
Dual Stack for IP and PPP Subscribers



- IP or IPv6 triggers session creation on ISG. One session for both

- Allow for IPv6 deployment at residential premises, while keeping IPv4 support
- Address IPv4 Migration

6RD for IP and PPP IPv6 Subscribers



Client IPv6 address format

ISP's IPv6 Prefix	RG IPv4 Addr Subnet ID	Interface ID

Includes Residential Gateway IPv4 address

- 6RD CPE encapsulates IPv6 client traffic in IPv4 tunnel
  - One IPv4 tunnel per CPE
- IPv4 tunnel header addresses built of IPv4 portion of IPv6 address
  - IPv4 Destination address set to 6RD Border Router IPv4 address

6RD Border Router (BD) terminates IPv4 tunnel – IPV6 traffic forwarded in IPv6 core

- Dynamic subscriber management function supported
  - One ISG session (PPP or IPv4) per IPv6 household (6RD CPE)
- Allow for IPv6 deployment at residential premises
- IPv4 address exhaustion addressed in conjunction with other techniques

BNG Service Manager for Cisco Prime (BroadHop)

Technology Partner Overview: BroadHop

BroadHop empowers service providers to control, monetise, and personalise the broadband experience, while introducing consumer choice.

Leadership and Experience

BroadHop's Policy Management solution has been deployed by over 80 customers in over 40 countries

Founded in 2003. Focused on Policy and Subscriber Data Management for fixed, mobile, and Wi-Fi service providers

Proven as industry's most scalable, highest-performance solution; 20 times more scalable than nearest competitor (Source: European Advanced Networking Test Center 2010)

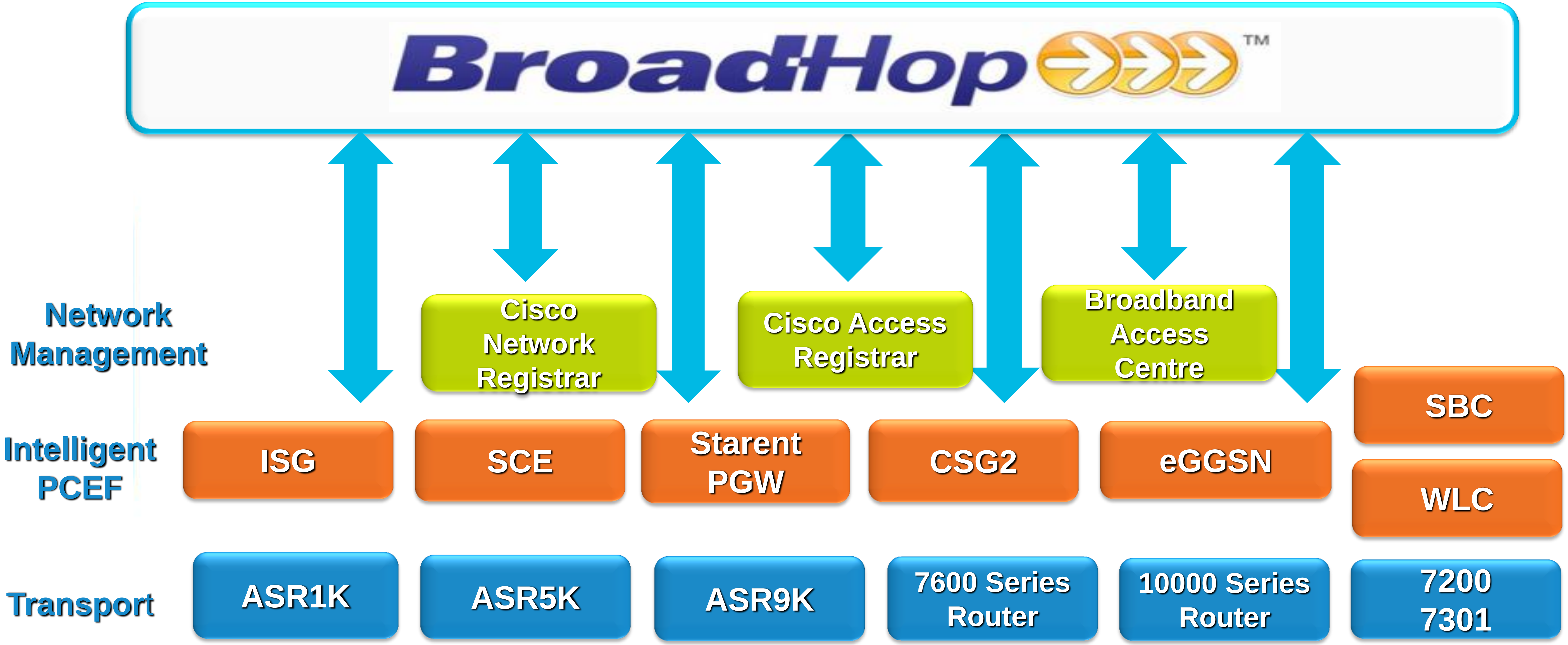
Certified for use with Cisco Intelligent Services Gateway (ISG) and Service Control Engine (SCE) platforms, with multiple global deployments at some of the most demanding SPs

BroadHop

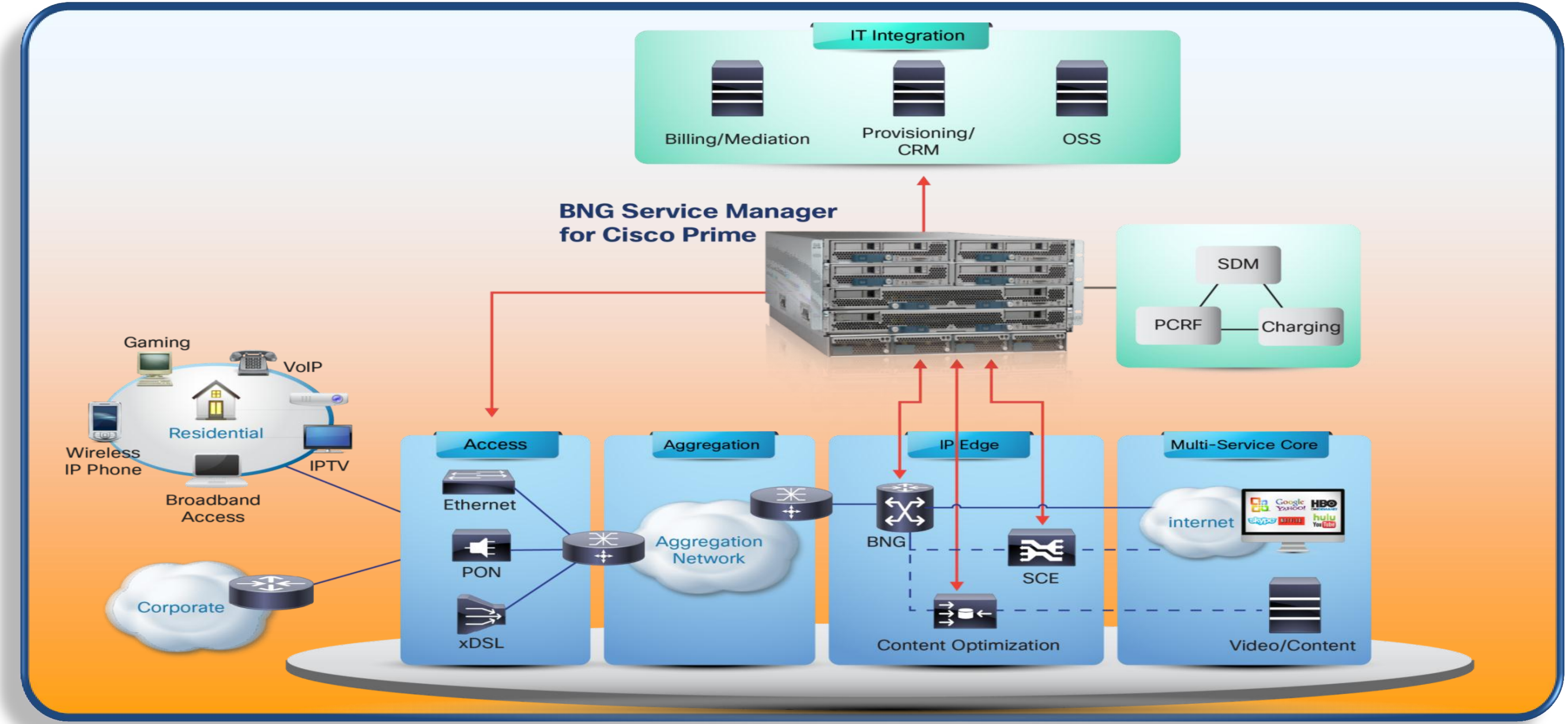
Solutions Plus Partner

- **Mobile World Congress 2011 Fierce Wireless: Infrastructure Policy Control and Optimisation**
- **2010 Product of the Year: TMC Communications**
- **2010 Light Reading: Leading Lights Finalist**

BroadHop and Cisco: Extensive Integration

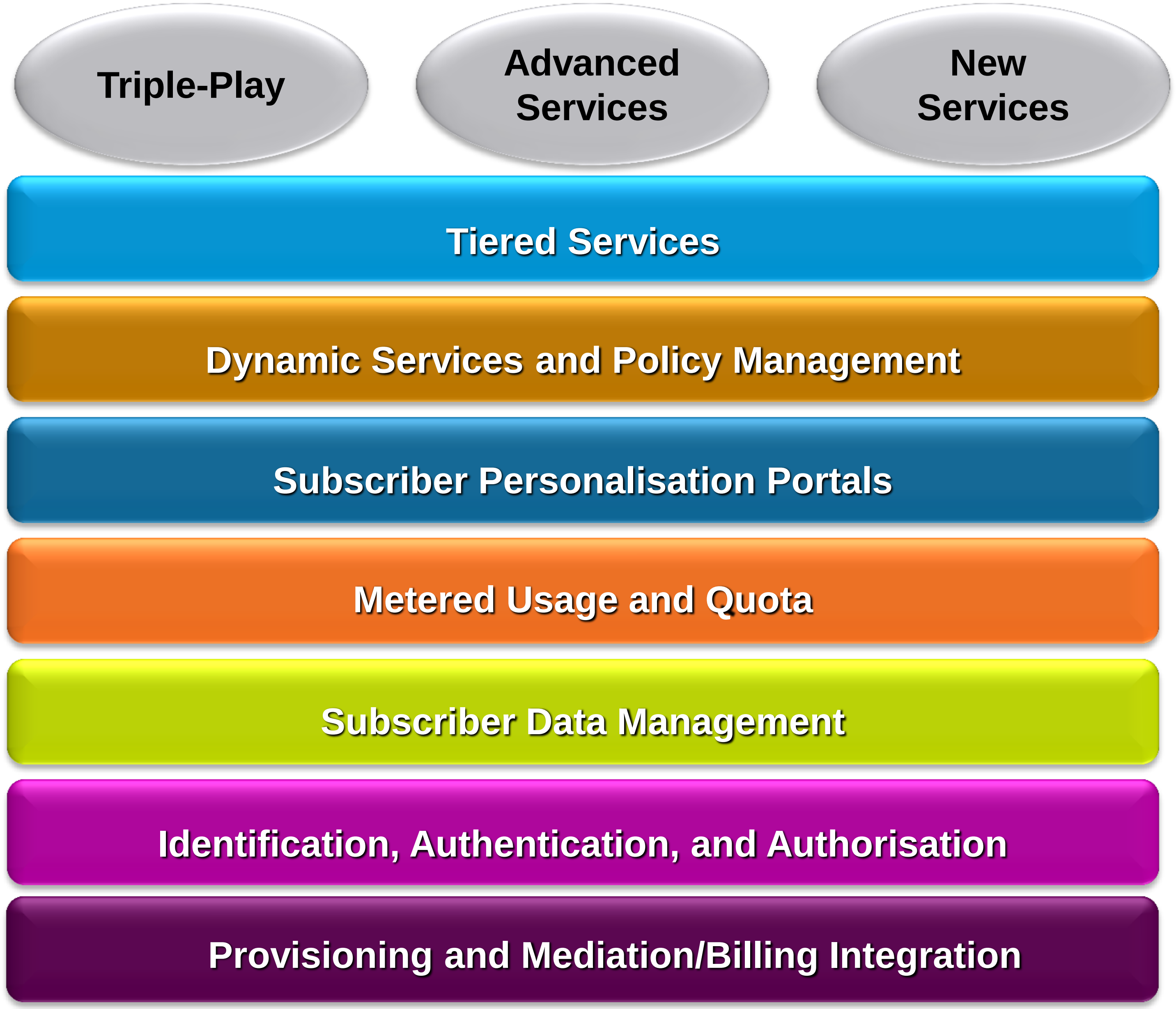


BNG Service Manager for Cisco Prime Architecture



BNG Service Manager for Cisco Prime

- The BNG Service Manager for Cisco Prime™ controls and coordinates the subscriber's session across multiple enforcement points in the network, including:
  - Broadband network gateways, such as the Cisco® ISG
  - Deep packet inspection devices, such as the Cisco SCE
  - Content optimisation servers (video, web, and more)
- Policy decisions and enforcement actions include:
  - Subscriber session authorisation
  - Service selection and personalisation
  - QoS and bandwidth control
  - Session and application-specific quota authorisation
  - Application-based admission control



Triple-Play

Advanced Services

New Services

Tiered Services

Dynamic Services and Policy Management

Subscriber Personalisation Portals

Metered Usage and Quota

Subscriber Data Management

Identification, Authentication, and Authorisation

Provisioning and Mediation/Billing Integration

BNG Service Manager

Key Features and Use Cases

- **Subscriber Data Management**
  - Subscriber Account/User Group management, Identity Management
  - Balance Management
  - OSS/BSS Provisioning API
  - Portal Provisioning API
  - Federation with existing Subscriber DBs
- **Policy Control**
  - Subscriber Auth and Login Methods
  - Subscriber Redirection
  - Service Plan Definition
  - Tiered Services & QoS
  - Time-based Service Passes
  - Volume-limited Services
  - Concurrent Login Limits
  - Quota Control and Usage Metering
  - DPI Integration
    - Application Based QoS and Metering
- **Reporting**
  - Subscriber usage CDRs
- **Authentication & Authorisation**
  - RADIUS PAP/CHAP
  - Diameter Gx
  - Transparent Auto Login: Subscriber MAC, IP Address, Option 82
  - Location-based Authorisation
  - Subscriber Provisioning Portal APIs
- **Online/Offline Charging**
  - Online Charging and Balance Mgmt (RADIUS Prepaid)
  - Real-time Rating
  - CDR accumulation, validation, and formatting
  - CDR data insertion
  - CDRs accumulation per session, hour, and day
- **Subscriber Service Portal API**
  - Self Provisioning & Service Selection
  - On-demand Service Upgrades
  - Quota/Usage Metering
  - Identity and Profile Management
  - Sub-account Management and Parental Controls

ASR9K BNG Configuration Example

Structured Configuration Model

I. Configure Northbound interfaces

AAA

Portal/Policy Server

CoA

II. Configure Templates, User and Service Profiles

III. Configure Subscriber Access

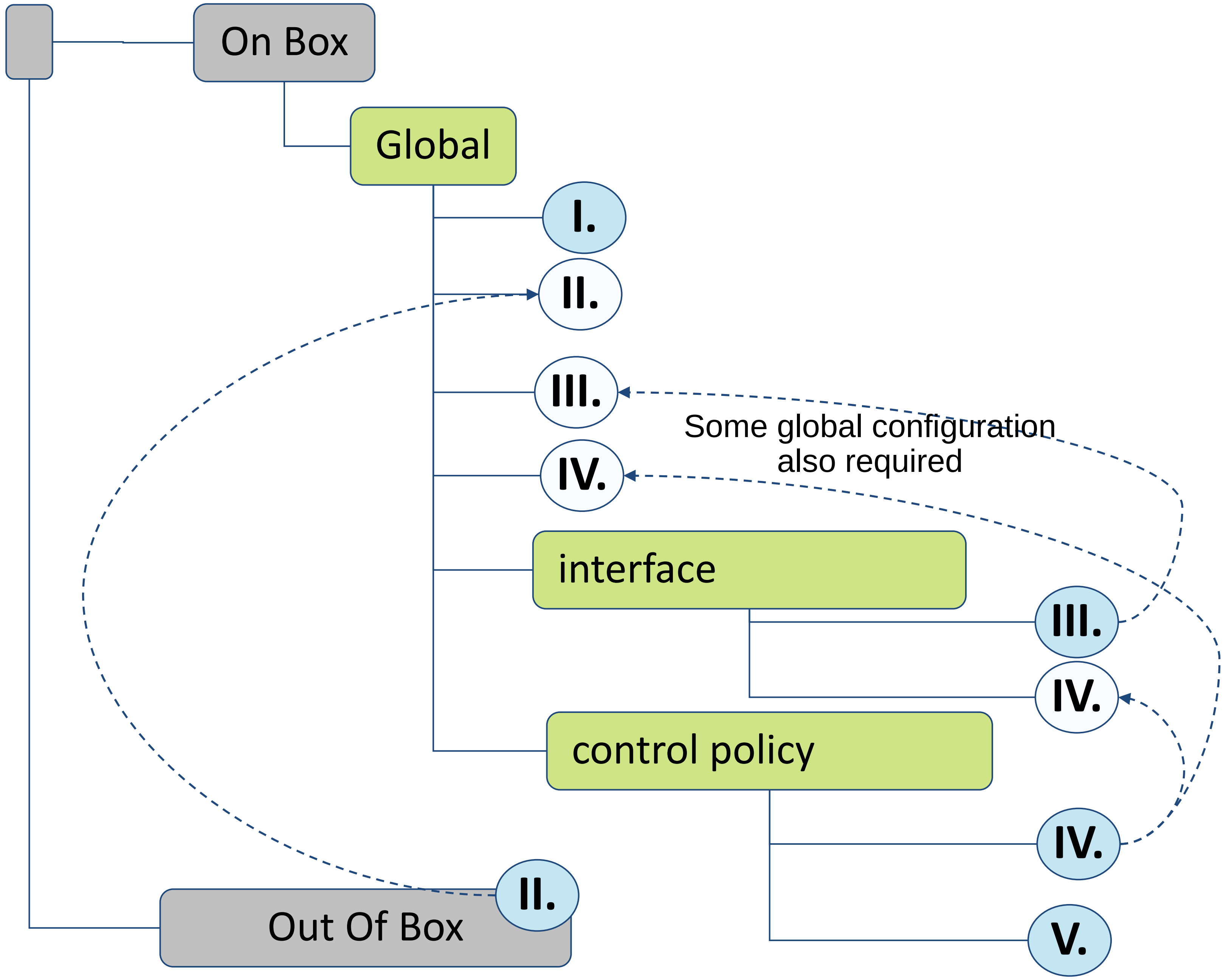
Configure session type and initiator

Create and apply the control policy

Other deployment specific cfgs

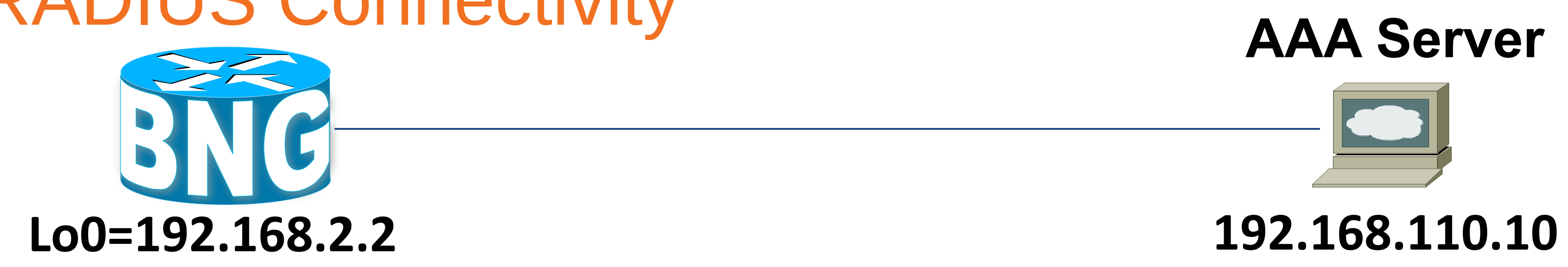
IV. Configure Subscriber Authentication

V. Dynamic Management of Dynamic Templates



I. Configure Northbound Interfaces

a. AAA–Basic RADIUS Connectivity

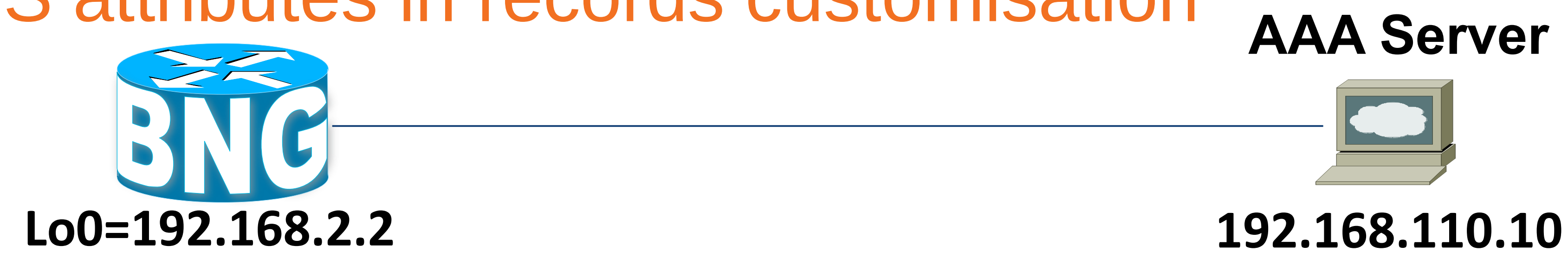


```
aaa group server radius SERVER_GRP
 server 192.168.110.10 auth-port 1812 acct-port 1813
!
interface Loopback0
 ipv4 address 192.168.2.2 255.255.255.255
!
radius source-interface Loopback0
radius-server host 192.168.110.10 auth-port 1812 acct-port
1813 key aaacisco
```

Define the RADIUS server and server group

I. Configure Northbound Interfaces

b. AAA–RADIUS attributes in records customisation



```
radius-server attribute list ATTR_LIST
  attribute <attr-list>
  attribute vendor-specific <…>
!
```

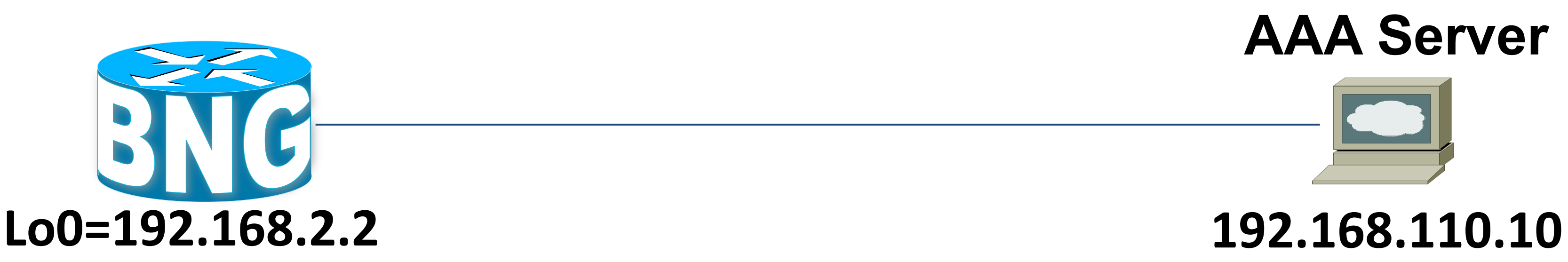
Defines a list of attributes

```
aaa group server
 { authentication | authorization | accounting }
                 { reply | request } { accept | reject }
ATTR_LIST
!
```

Associates attribute list filters to RADIUS records sent/received a specific server group

I. Configure Northbound Interfaces

b. AAA–RADIUS attributes customisation (NAS Port ID)



AAA Server

Lo0=192.168.2.2

192.168.110.10

```
aaa attribute format NAS-PORT-ID
 circuit-id plus remote-id
!
```

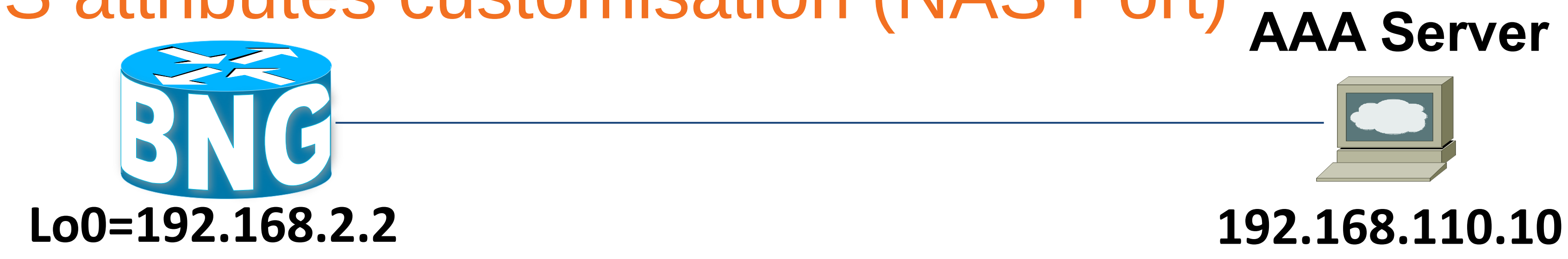
Defines NAS-PORT-ID format

```
aaa radius attribute nas-port-id format NAS-PORT-ID
```

Associates NAS-PORT-ID format to RADIUS attribute (Attr 87)

I. Configure Northbound Interfaces

c. AAA–RADIUS attributes customisation (NAS Port)



```
aaa radius attribute nas-port format e <format> [type <0-44>]
```

Defines NAS-PORT format (Attr 5)

“Type” keyword allows for different formats for different access intf

Format (32bits): entered as a string of letters:

- Zero : 0
- One : 1
- Slot : S
- Adapter : A
- Port : P
- (Outer) VLAN Id : V
- Session-Id : U
- Inner VLAN ID: Q

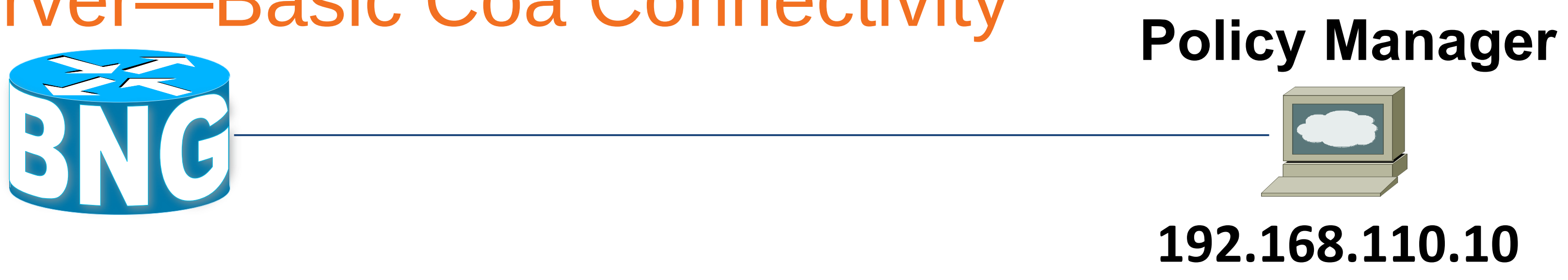
Ex “SSSSAAPPPPPVVVVVVVVVVVVVVVVVVVVV”

Type

ETHERNET	15	IPOEOE	39
PPPOEOE	32	IPOEOVLAN	40
PPPOEOVLAN	33	IPOEOQINQ	41
PPPOEOQINQ	34	VIRTUAL_IPOEOE	42
VIRTUAL_PPPOEOE	35	VIRTUAL_IPOEOVLAN	43
VIRTUAL_PPPOEOVLAN	36	VIRTUAL_IPOEOQINQ	44
VIRTUAL_PPPOEOQINQ	37		

I. Configure Northbound Interfaces

d. Portal/Policy Server—Basic Coa Connectivity



```
aaa server radius dynamic-author
 client 192.168.110.10 vrf default server-key cisco
 auth-type [ any | all ]
 port (1700)
```

client device sending CoA requests and shared password with BNG

Match all or any of session lookup keys in CoA request

UDP Port for RADIUS CoA messages (default: 1700)

Structured Configuration Model

I. Configure Northbound interfaces

AAA

Portal/Policy Server

CoA

II. Configure Templates, User and Service Profiles

III. Configure Subscriber Access

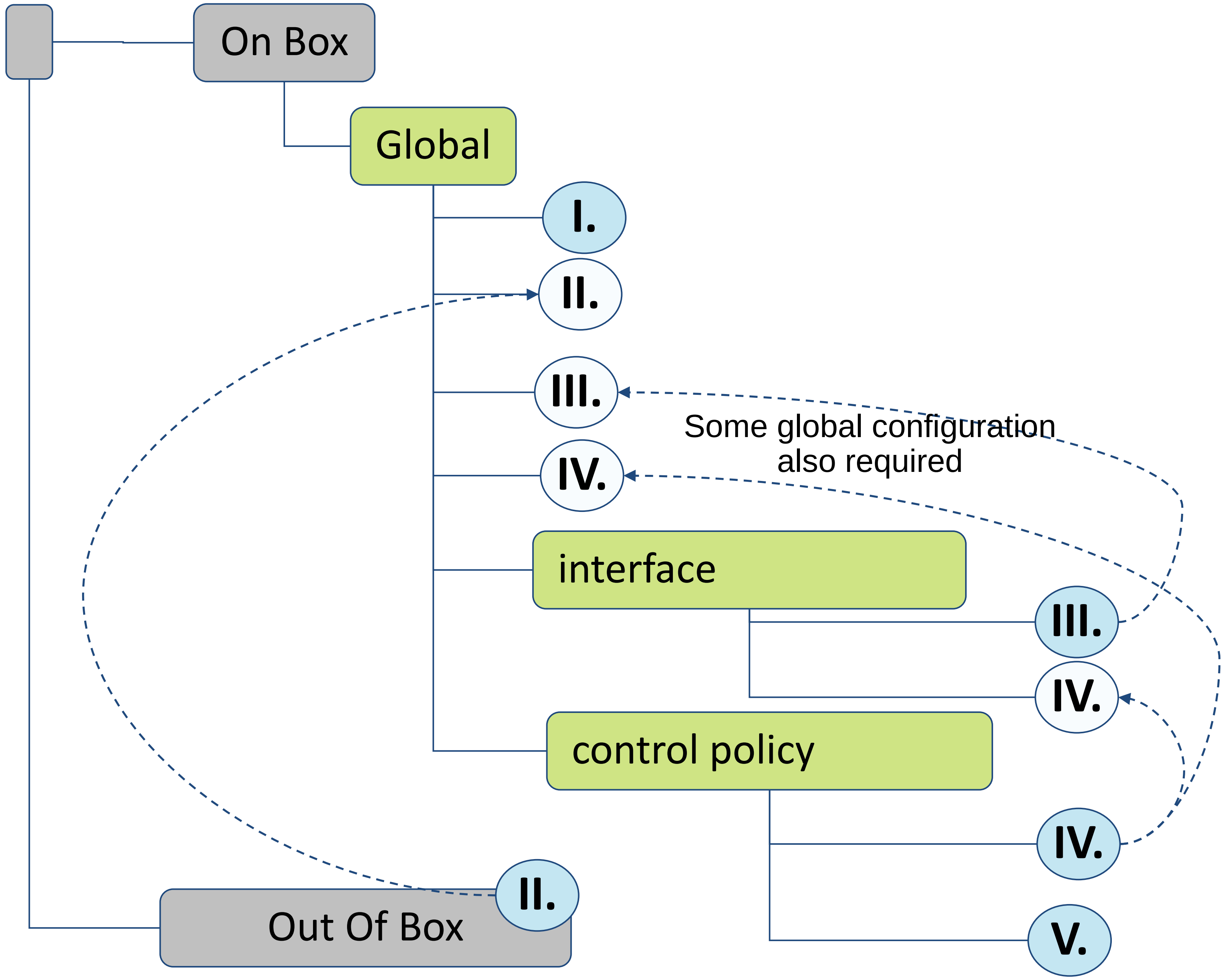
Configure session type and initiator

Create and apply the control policy

Other deployment specific cfgs

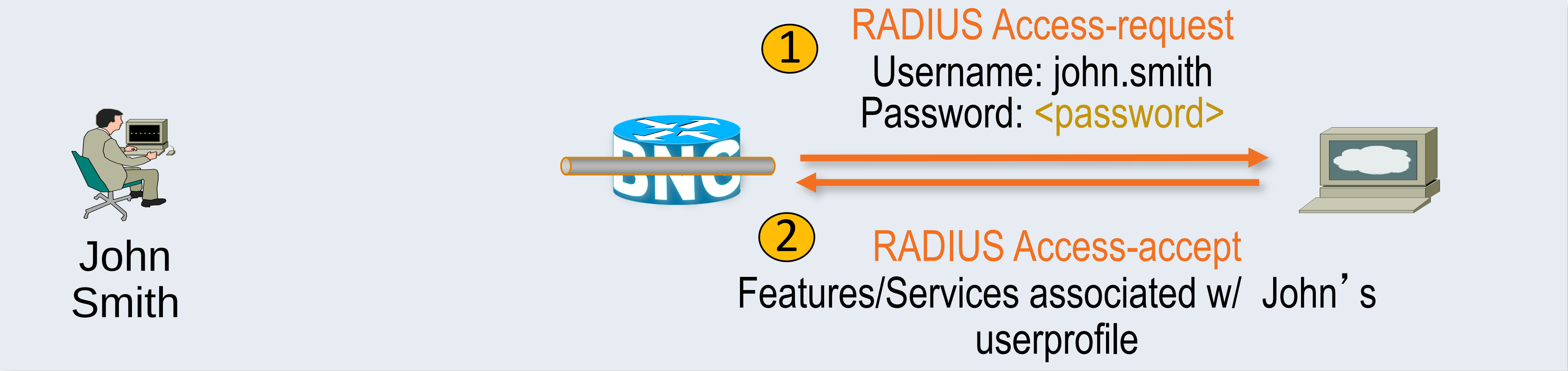
IV. Configure Subscriber Authentication

V. Dynamic Management of Dynamic Templates



II. Configure Templates, User and Service Profiles

a. User Profiles



John Smith

1 RADIUS Access-request
Username: john.smith
Password: <password>

2 RADIUS Access-accept
Features/Services associated w/ John’s userprofile

- User Profiles include subscriber specific attributes that should be activated on the session

```
User-Name:          “john.smith”
User-Password:      “******”
Attr 28: idle-timeout=600
AVPair:  “subscriber:accounting-list=
                    SESS_ACCNT_LIST”
```

- Attributes can be modified, but not unapplied from session

II. Configure Templates, User and Service Profiles

Specify Template Definition Location

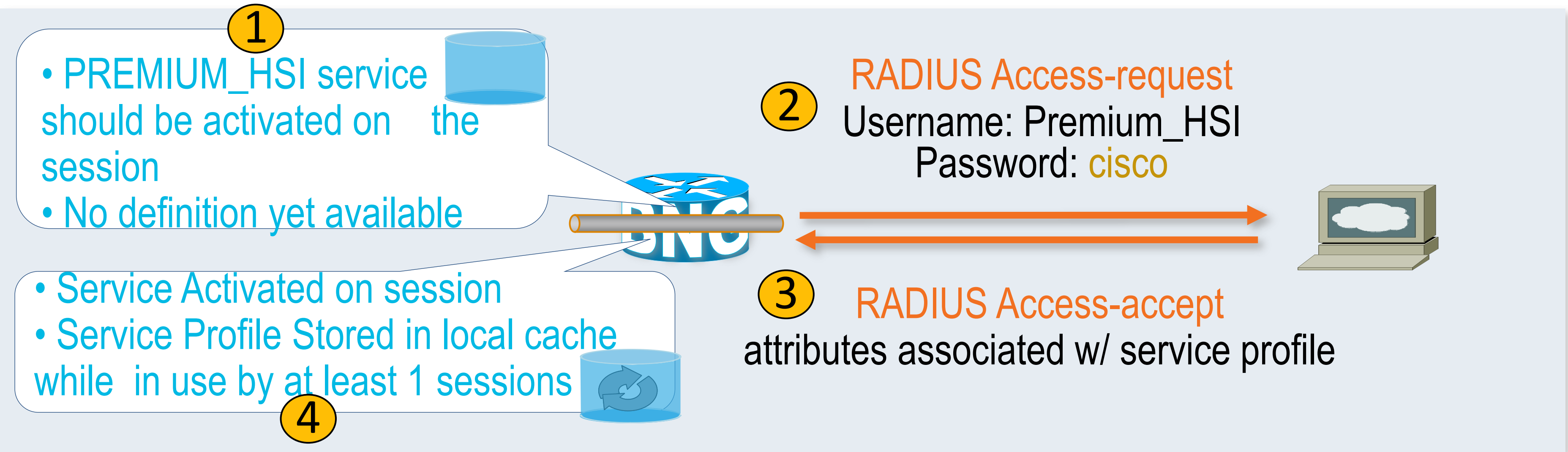
```
aaa authorization subscriber TPL_ML group <srv group>
```

Dynamic-template location specified at activation in control policy

```
10 activate dynamic-template <template name> [ aaa list TPL_ML ]
```

If a method-list is not specified, local configuration is used

Password for template download from external AAA server defaults to “cisco”



1

- PREMIUM_HSI service should be activated on the session
- No definition yet available

2

RADIUS Access-request
Username: Premium_HSI
Password: cisco

3

RADIUS Access-accept
attributes associated w/ service profile

4

- Service Activated on session
- Service Profile Stored in local cache while in use by at least 1 sessions

II. Configure Templates, User and Service Profiles

a. Subscriber Templates—Examples

AAA Server
BNG

Dynamic Template

AAA Profiles

Subscriber attributes can be equally defined in “Dynamic Templates” or on the AAA in “Service Profiles”

```
dynamic-template
  type { ppp | ipsub | service } TPL
    ipv4 access-group BNG_ACL_IN ingress
    ipv4 access-group BNG_ACL_OUT egress
    timeout idle 3600
    accounting aaa list SESS_ACCNT_LIST
```

```
Service-Name:      “TPL”
Service-Password: “cisco”
AVPair: “ip:in_acl=BNG_ACL_IN”
AVPair: “ip:out_acl=BNG_ACL_OUT”
Attr 28: idle-timeout = 60
AVPair: “subscriber:accounting-list=SESS_ACCNT_LIST”
```

ACL/Accounting method list definition on BNG

```
aaa accounting network SESS_ACCNT_LIST group SERVER_GRP
!
ipv4 access-list BNG_ACL_IN
   <acl definition>
!
ipv4 access-list BNG_ACL_OUT
   <acl definition>
```

Structured Configuration Model

I. Configure Northbound interfaces

AAA

Portal/Policy Server

CoA

II. Configure Templates, User and Service Profiles

III. Configure Subscriber Access

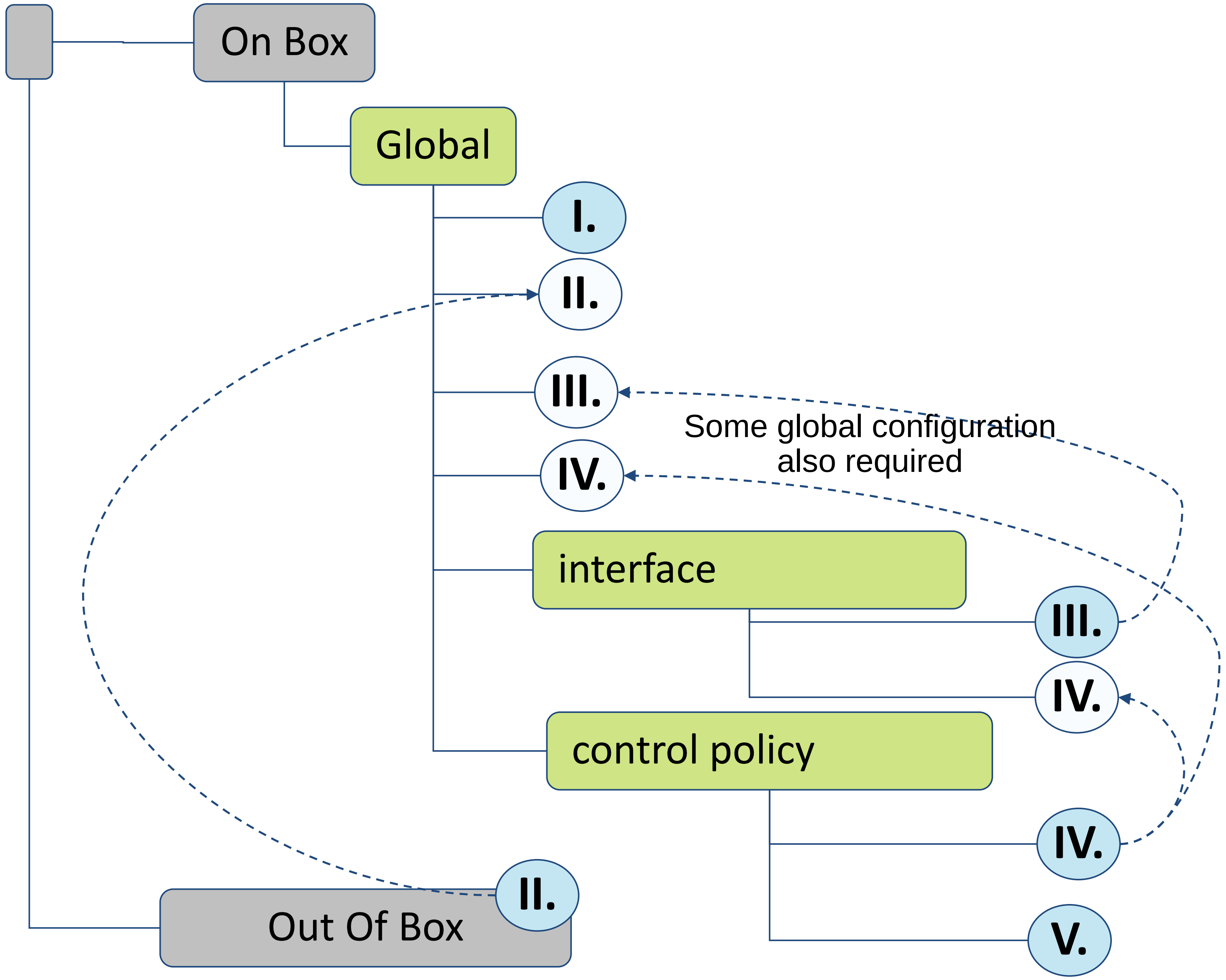
Configure session type and initiator

Create and apply the control policy

Other deployment specific cfgs

IV. Configure Subscriber Authentication

V. Dynamic Management of Dynamic Templates



III. Configure Subscriber Access

- IP Sessions–L2 Connected Subscribers
- PPP Sessions

III. Configure Subscriber Access

IP Sessions–L2 Connected Subscribers –Part 1

```
class-map type control subscriber match-any IP
 match protocol dhcpv4
 end-class-map
!
policy-map type control subscriber IP_PM
 event session-start match-first
  class type control subscriber IP do-until-failure
   10 activate dynamic-template IP_BASE_TPL
!
```

Create control policy

Configure control policy to activate common session attributes when a new session is initiated

```
dynamic-template
 type ipsub IP_BASE_TPL
   ipv4 unnumbered Loopback50
 !
```

III. Configure Subscriber Access

IP Sessions–L2 Connected Subscribers – Part 2

```
interface Bundle-Ethert10.60
  ipv4 point-to-point
  ipv4 unnumbered Loopback1060
  encapsulation dot1q 60
                 OR
  encapsulation dot1q 60 second-dot1q 10
  service-policy type control IP_PM
  ipsubscriber ipv4 l2-connected
    initiator dhcp
```

Explicit encap

Single/Double tagged (.1q and .1ad)

apply the control policy

define the type of session

specify the session initiator

DHCP Proxy functionalities required for supporting DHCP initiated sessions

```
dhcp ipv4
 profile DHCP_B10_60_PF proxy
  helper-address vrf default 192.168.110.10 giaddr 10.60.1.1
 !
 interface Bundle-Ether10.60 proxy profile DHCP_10_60
```

DHCP Server reachable via global or VRF routing

III. Configure Subscriber Access

PPP Sessions – Part 1

```
class-map type control subscriber match-any PPP
 match protocol ppp
 end-class-map
!
policy-map type control subscriber PPP_PM
 event session-start match-first
  class type control subscriber PPP do-until-failure
   10 activate dynamic-template PPP_BASE_TPL
!
```

Create control policy

Configure control policy to activate common session attributes when a new session is initiated

```
dynamic-template
 type ppp PPP_BASE_TPL
  ppp authentication pap
  ppp ipcp peer-address pool PPP_BUNDLE_10_50_POOL
  ipv4 unnumbered Loopback50
 !
```

III. Configure Subscriber Access

PPP Sessions – Part 2

```
interface Bundle-Ether10.50
 service-policy type control subscriber PPP_PM
 pppoe enable bba-group default
 encapsulation ambiguous dot1q 50 second-dot1q any
                    OR
 encapsulation dot1q 50 second-dot1q 10
                    OR
 encapsulation dot1q 50
!
```

apply the control policy

Enables PPPoE processing and specify optional BBA group

Explicit and ambiguous encap

Single/Double tagged (.1q and .1ad)

BBA group definition

```
ppoe bba-group default
  service name <name>
       OR
  service selection disable
!
```

Service selection enabled by default.

MUST be disabled if not supported by client

Structured Configuration Model

I. Configure Northbound interfaces

AAA

Portal/Policy Server

CoA

II. Configure Templates, User and Service Profiles

III. Configure Subscriber Access

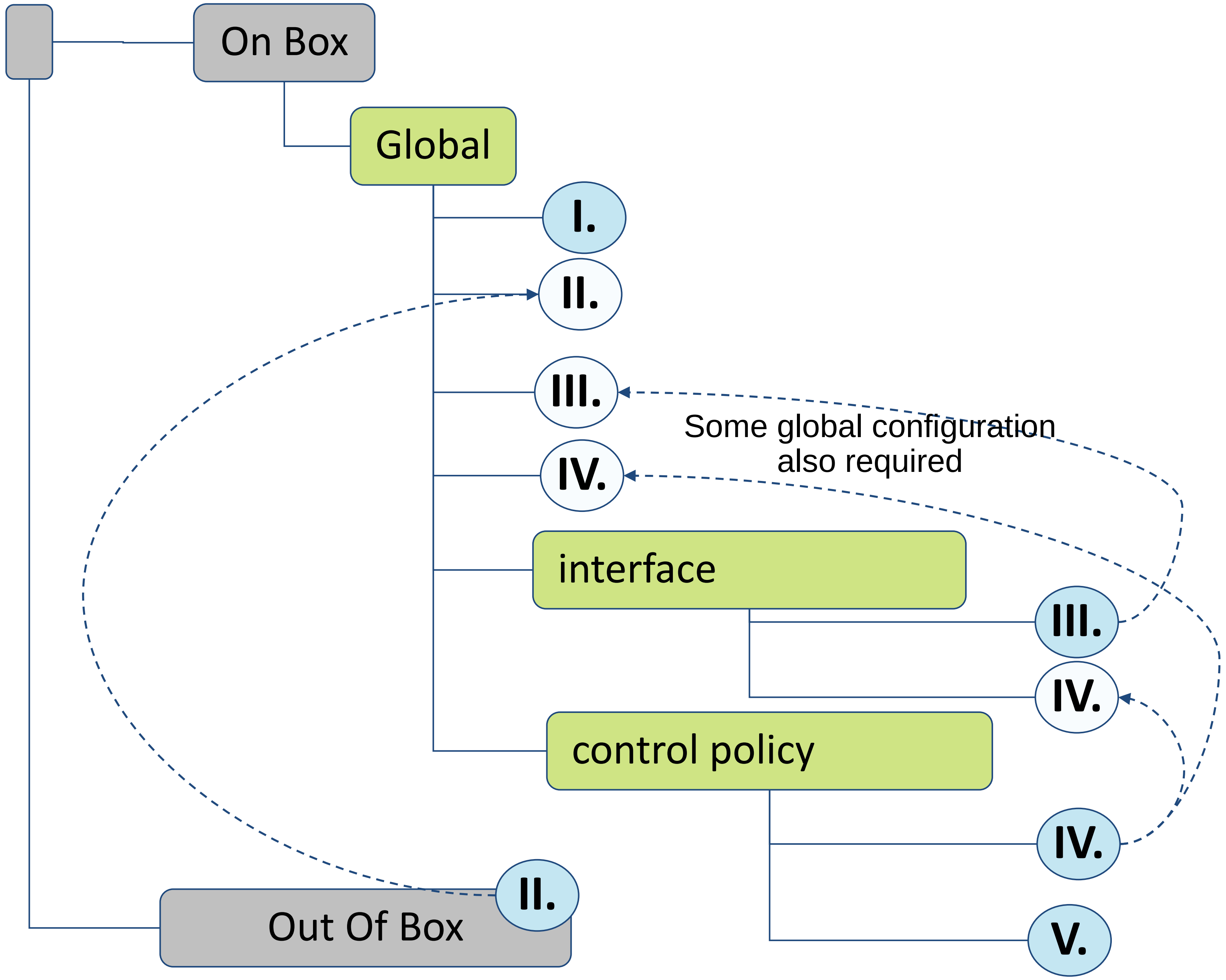
Configure session type and initiator

Create and apply the control policy

Other deployment specific cfgs

IV. Configure Subscriber Authentication

V. Dynamic Management of Dynamic Templates



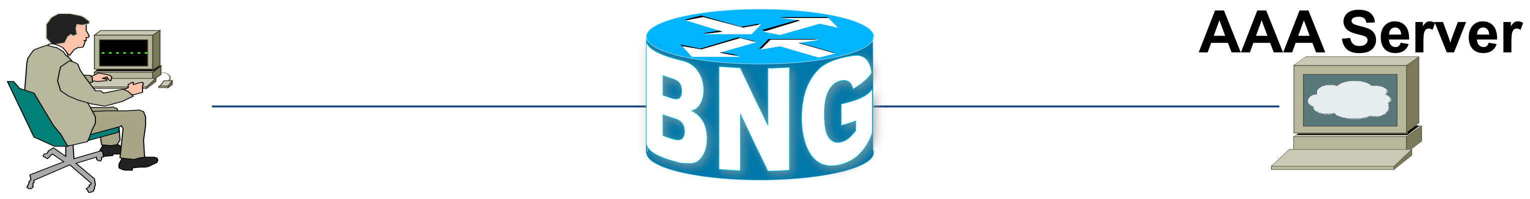
IV. Configure Subscriber Authentication

AAA Server
BNG

- IP Sessions–TAL by MAC SA
- IP Sessions–TAL by DHCP Opt82
- IP Sessions–influencing subscriber address assignment based on class-name
- IP Sessions–influencing subscriber address assignment based on DHCP attributes
- Web Logon
- PPP Sessions–CHAP
- PPP Sessions–TAL by PPPoE IA tags

IV. Configure Subscriber Authentication

IP Sessions L2 connected–TAL by MAC SrcAddr



Specifies the RADIUS server group used to authenticate subscriber

Specifies username format

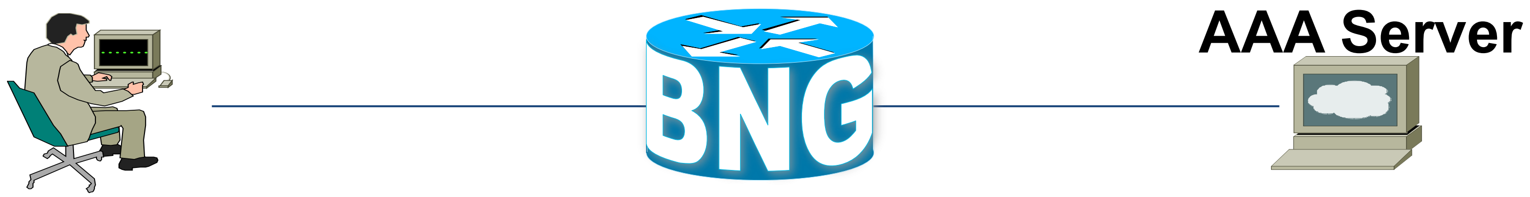
```
aaa authorization subscriber AUTHOR_LIST group SERVER_GRP
!
aaa attribute format USERNAME_FORMAT
 mac-address
!
policy-map type control subscriber IP_PM
 event session-start match-first
  class type control subscriber IP do-until-failure
   <snip>
   20 authorize aaa list AUTHOR_LIST format USERNAME_FORMAT password cisco
```

Upon Session initiation (session-start) TAL based authentication is attempted:

- username: <subscriber’s MAC>
- password: cisco123

IV. Configure Subscriber Authentication

IP Sessions L2 connected–TAL by DHCP Opt82



```
dhcp ipv4
 profile DHCP_B10_60_PF proxy
  relay information option
  relay information policy keep
  relay information option allow-untrusted
 !
!
aaa authorization network AUTHOR_LIST group SERVER_GRP
!
aaa attribute format USERNAME_FORMAT
 remote-id plus circuit-id
!
policy-map type control subscriber IP_PM
 event session-start match-first
  class type control subscriber IP do-until-failure
   <snip>
   20 authorize aaa list AUTHOR_LIST format USERNAME_FORMAT password cisco
```

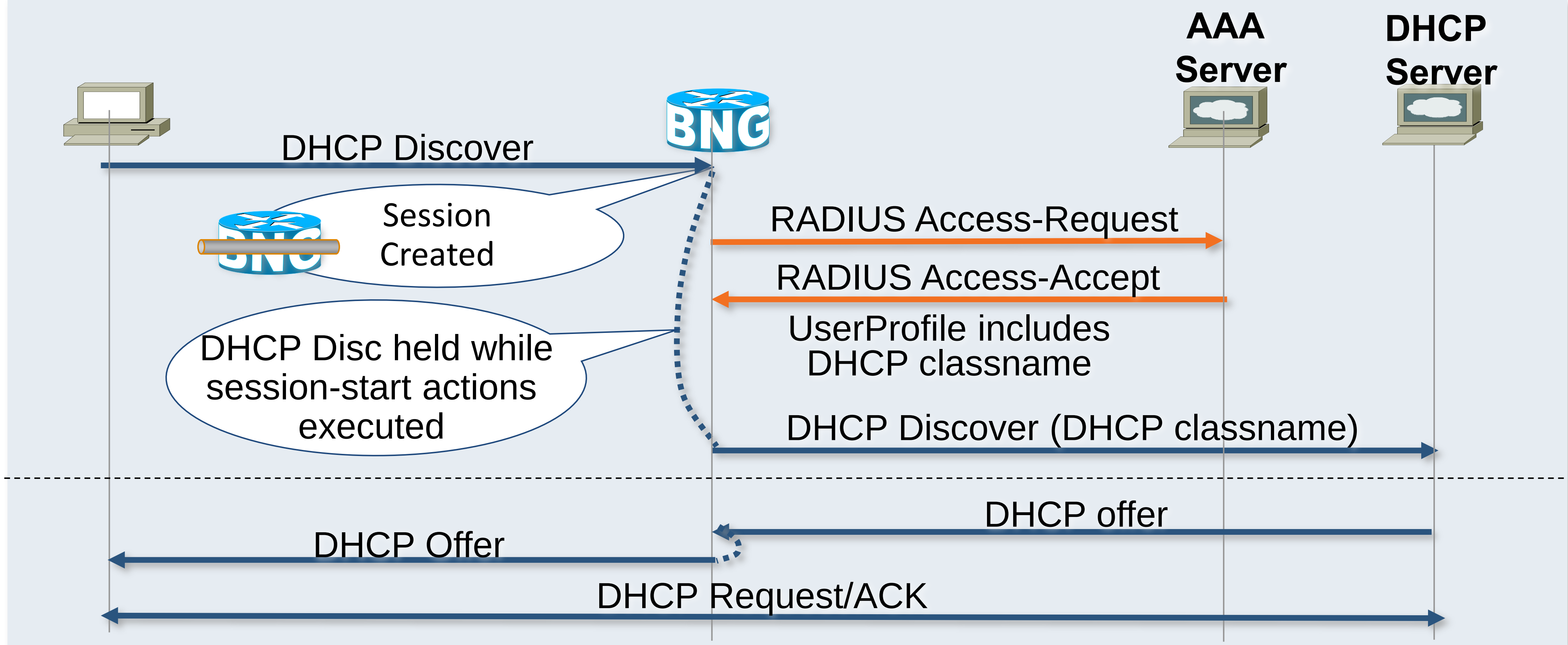
DHCP Proxy instructed to accept and keep access node Opt82 and forward it to server

Upon Session initiation (session-start) TAL based authentication is attempted:

username:	**<Opt82 RID>:<Opt82 CID>**
password:	**cisco**

IV. Configure Subscriber Authentication

DHCP Initiated Sessions–Influencing Subscriber Address Assignment based on class-name



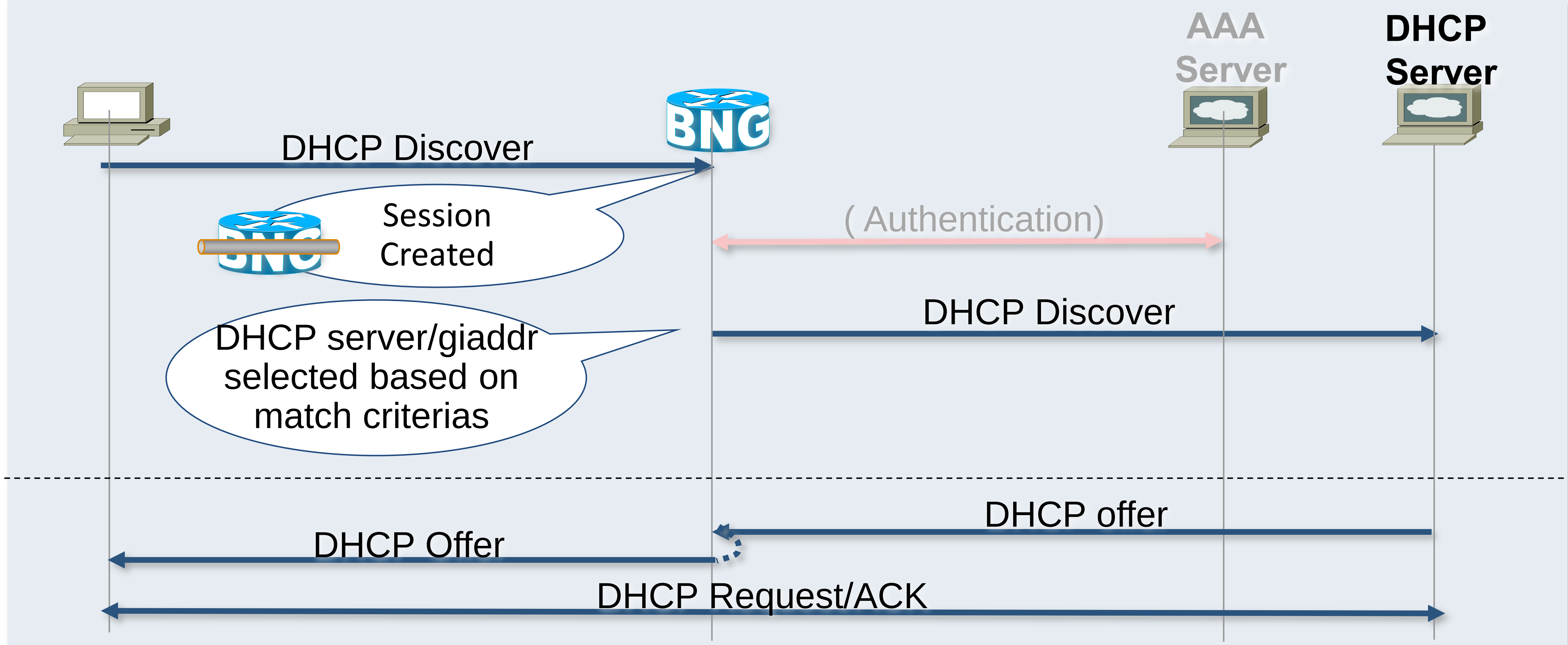
```
dhcp ipv4
 profile DHCP_B10_60_PF proxy
  class default-class
    helper-address vrf default 192.168.110.10 giaddr 10.60.1.1
  !
  class SUBNET1_CLASS_POOL
    helper-address vrf default 192.168.110.12 giaddr 10.60.1.1
  !
 interface Bundle-Ether10.60 proxy profile DHCP_10_60
```

- Subscriber attempts to discover its IP address
- BNG holds the Discover message while session-start actions are executed
- TAL is performed for the subscriber
- Authentication successful. Subscriber user-profile may includes a DHCP class-name
- DHCP discover is forwarded to the DHCP server including the DHCP class-name returned by RADIUS

- DHCP Server performs address allocation based on DHCP class-name

IV. Configure Subscriber Authentication

DHCP Initiated Sessions–Influencing Subscriber Address Assignment based on DHCP attributes



```
dhcp ipv4
 profile DHCP_B10_60_PF proxy
  class CLASS1
    match option 124 hex <value1>
    helper-address vrf default 192.168.110.10 giaddr 10.60.1.1
  !
  class CLASS2
    match option 124 hex <value2>
    helper-address vrf default 192.168.110.12 giaddr 10.60.1.1
  !
 interface Bundle-Ether10.60 proxy profile DHCP_10_60
```

Options in DHCP Discovery used for DHCP serer selection:

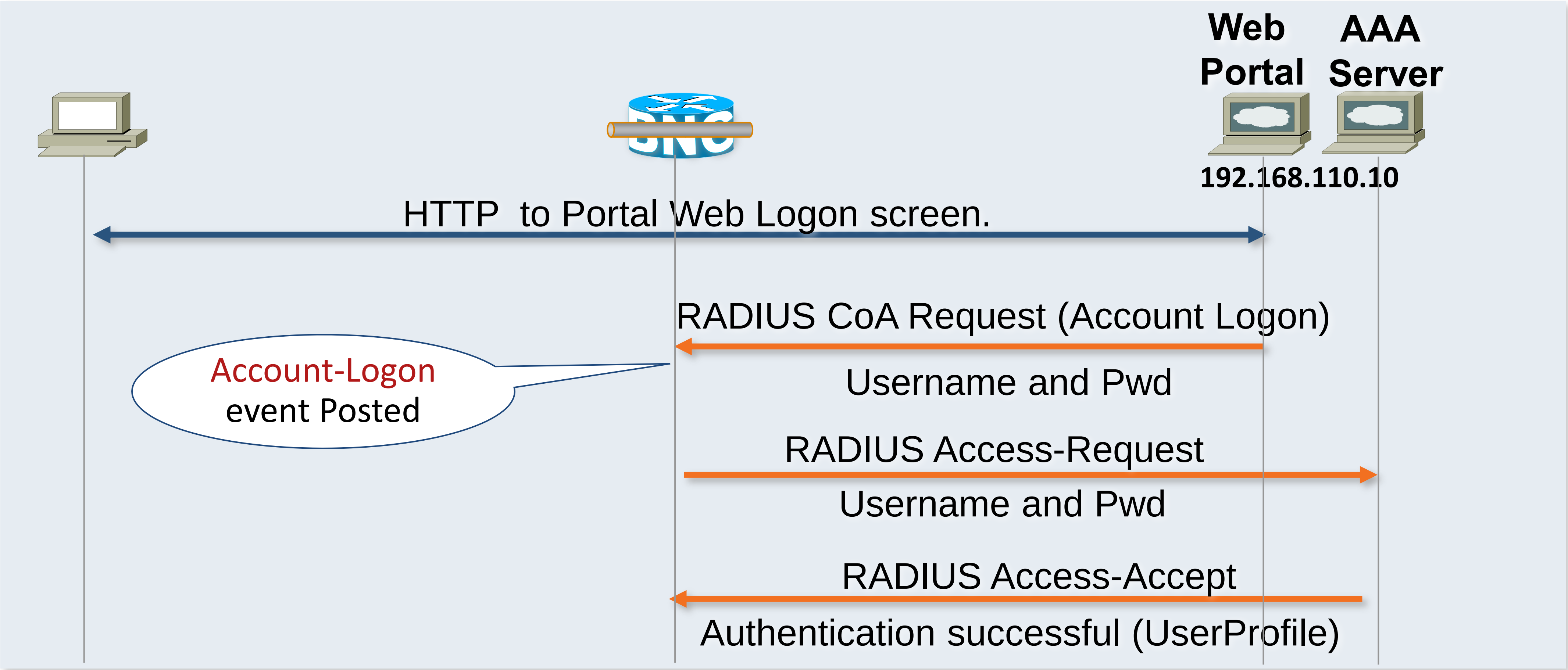
- Option 124 vendor-identifying vendor class
- Option 125 vendor-identifying vendor-specific info
- Option 60 vendor class-id
- Option 77 user class

Single match

Different match criteria in different classes

IV. Configure Subscriber Authentication

Web Logon



Web Portal

AAA Server

192.168.110.10

HTTP to Portal Web Logon screen.

RADIUS CoA Request (Account Logon)

Username and Pwd

Account-Logon event Posted

RADIUS Access-Request

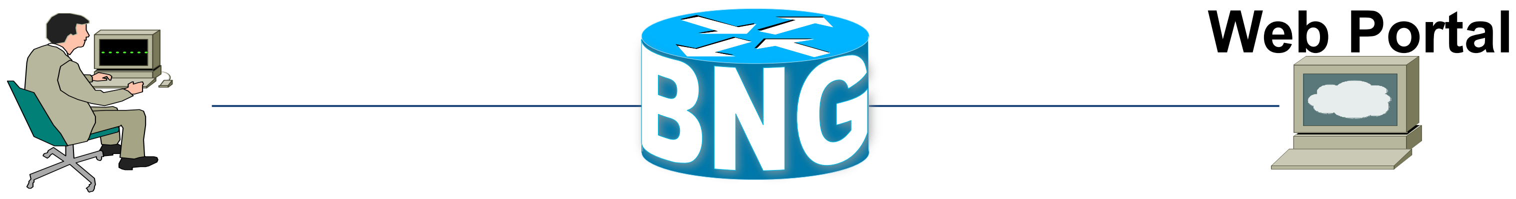
Username and Pwd

RADIUS Access-Accept

Authentication successful (UserProfile)

IV. Configure Subscriber Authentication

Web Logon



```
aaa authentication subscriber default group SERVER_GRP
!
policy-map type control subscriber IP_PM
 event account-logon match-first
  class type control subscriber IP do-until-failure
    10 authenticate aaa list default
  !
 event authentication-failure match-first
  class type control subscriber IP do-until-failure
   10 activate dynamic-template AUTH_FAILURE_TPL
                          OR
   10 disconnect
```

Credentials returned by the portal are used for AAA authentication

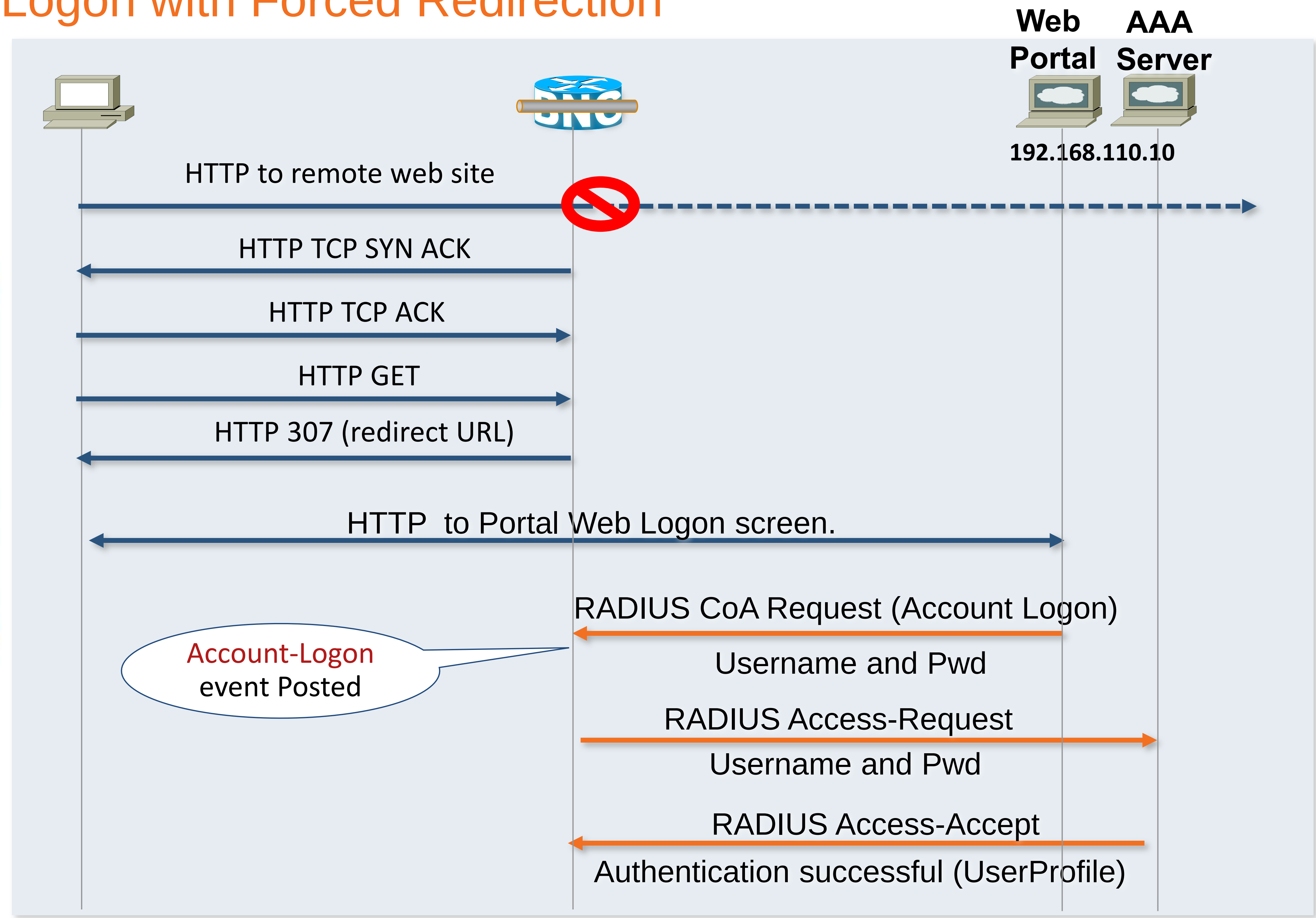
If authentication fails an additional event allows you to perform further actions

e.g. start a fall back service, disconnect the session, …

Note: **Example shows default behaviour**

IV. Configure Subscriber Authentication

Web Logon with Forced Redirection



IV. Configure Subscriber Authentication

Web Logon with Forced Redirection

BNG
Web Portal

```
aaa authentication subscriber default group SERVER_GRP
!
policy-map type control subscriber IP_PM
 event session-start match-first
  class type control subscriber IP do-until-failure
   10 activate dynamic-template IP_BASE_TPL
   20 activate dynamic-template HTTPR_TPL
  !
  <snip: + Web Logon regular control policy config>
```

Enables HTTP redirect service

```
dynamic-template
 type service HTTPRDRT_TPL
  service-policy type pbr HTTPRDRT_PM
 !
```

```
policy-map type pbr HTTPRDRT_PM
 class type traffic OpG_CM
  transmit
 !
 class type traffic HTTPRDRT_CM
  http-redirect www.portal.com/192.168.2.2
 !
 class type traffic class-default
  drop
 !
 end-policy-map
```

IV. Configure Subscriber Authentication

Web Logon with Forced Redirection – HTTPR Service

HTTP-R PBR Policy

```
policy-map type pbr HTTPRDRT_PM
 class type traffic OpG_CM
  transmit
 !
 class type traffic HTTPRDRT_CM
  http-redirect portal.com/nas_ip=192.168.2.2
 !
 class type traffic class-default
  drop
 !
 end-policy-map
```

HTTP-R Traffic Classes

```
class-map type traffic match-any OpG_CM
 match access-group ipv4 OpG_ACL
 end-class-map
!
class-map type traffic match-any HTTPRDRT_CM
 match access-group ipv4 HTTPRDRT_ACL
 end-class-map
!
```

HTTP-R ACLs

```
ipv4 access-list OpG_ACL
 10 permit tcp any host 192.168.110.10 eq www
!
ipv4 access-list HTTPRDRT_ACL
 10 permit tcp any any eq www
!
```

IV. Configure Subscriber Authentication

Web Logon with Forced Redirection on TAL Failure

Web Portal
BNG

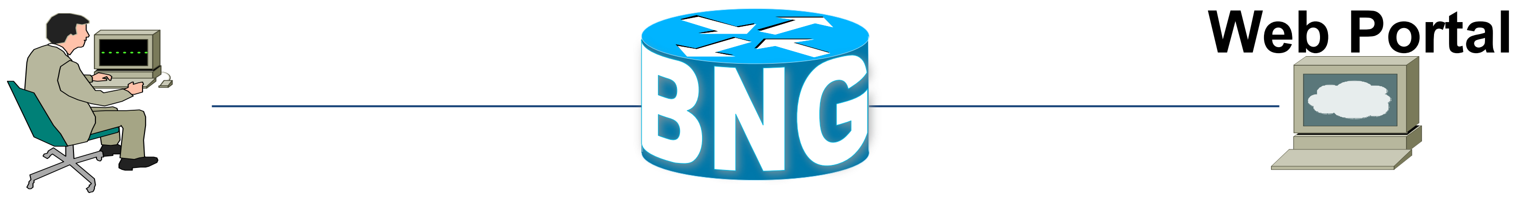
```
aaa authorization subscriber AUTHOR_LIST group SERVER_GRP
aaa authentication subscriber default group SERVER_GRP
!
policy-map type control subscriber IP_PM
event session-start match-first
  class type control subscriber IP do-until-failure
   <snip>
   20 authorize aaa list AUTHOR_LIST format USERNAME_FORMAT password cisco
  !
 !
 event authorization-failure match-first
  class type control subscriber DHCP do-until-failure
   10 activate dynamic-template HTTPRDRT_TPL
  !
 !
 event account-logon match-first
  class type control subscriber DHCP do-until-failure
   10 authenticate aaa list default
   20 deactivate dynamic-template HTTPRDRT_TPL
```

Enables HTTP redirect service if TAL fails

Disables HTTP redirect service if Web Logon is successful

IV. Configure Subscriber Authentication

Terminating a session that does not authenticate in time



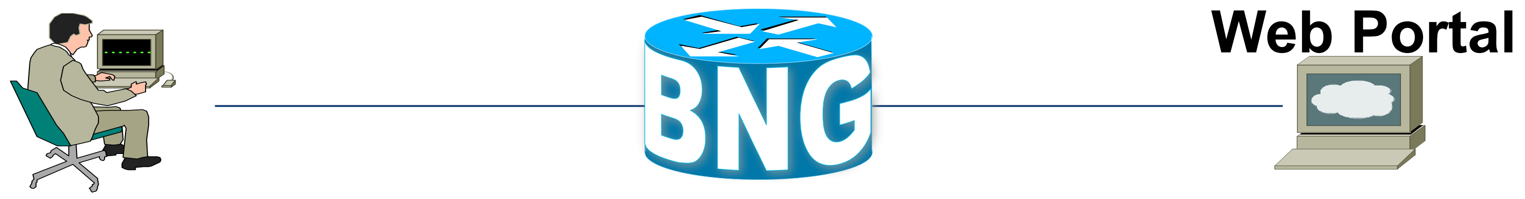
```
class-map type control subscriber match-all AUTH_TMR_CM
  match timer AUTH_TMR
  match authen-status unauthenticated
!
policy-map type control subscriber IP_PM
 <snip>
 event authorization-failure match-first
  class type control subscriber DHCP do-until-failure
   10 activate dynamic-template HTTPRDRT_TPL
   20 set-timer AUTH_TMR 10
  !
 !
 event timed-policy-expiry match-first
  class type control subscriber AUTH_TMR_CM do-until-failure
   10 disconnect
```

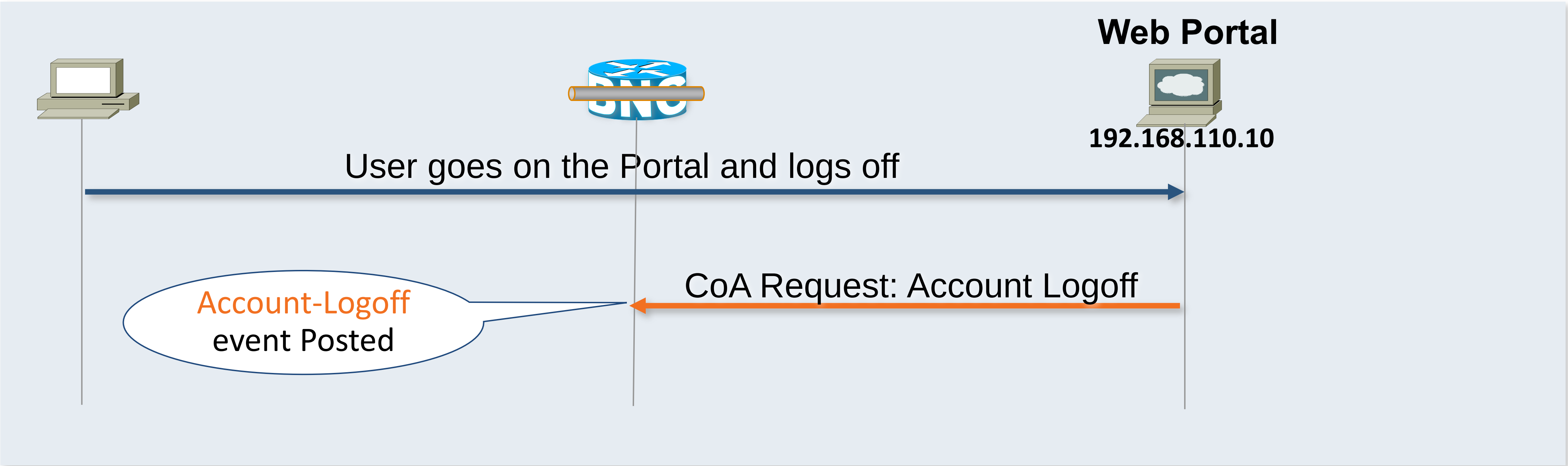
Start timer when redirection is enabled

Disconnect session if session is unauthenticated when timer expires

IV. Configure Subscriber Authentication

Web Logoff




Web Portal
192.168.110.10
User goes on the Portal and logs off
CoA Request: Account Logoff
Account-Logoff
event Posted

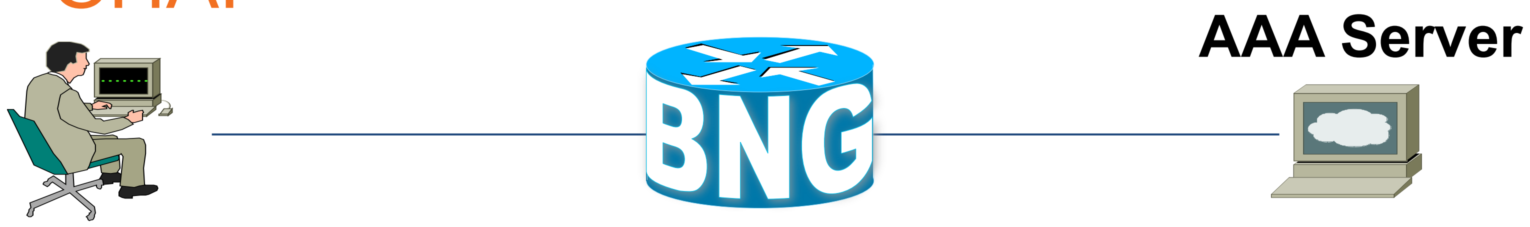
```
policy-map type control subscriber IP_PM
 event account-logoff match-first
  class type control subscriber IP do-until-failure
    10 disconnect
   !
```

session torn down after subscriber logs off

Note: Example shows default behaviour

IV. Configure Subscriber Authentication

PPP Sessions–PPP CHAP



```
aaa authentication subscriber AUTHEN_LIST
                              group SERVER_GRP
!
policy-map type control subscriber PPP_PM
 event session-activate match-first
  class type control subscriber PPP do-until-failure
   10 authenticate aaa list AUTHEN_LIST
  !
 !
```

Session will be automatically destroyed if PPP native authentication fails

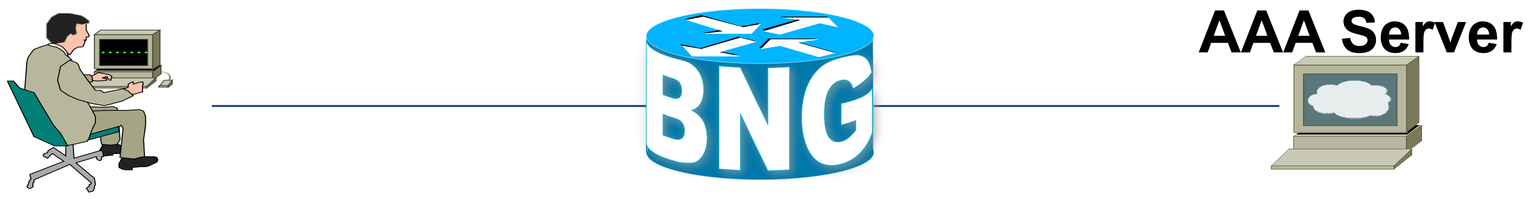
Session-activate event triggered when LCP opens

Enables authentication and specify authentication method list

CHAP Authentication was selected on dynamic template

IV. Configure Subscriber Authentication

PPP Sessions–TAL by PPPoE Tags



Requires DSLAM capable of inserting PPPoE IA tags

```
aaa authorization network AUTHOR_LIST group SERVER_GRP
!
aaa attribute format USERNAME_FORMAT
 remote-id plus circuit-id
!
policy-map type control subscriber IP_PM
 event session-start match-first
  class type control subscriber PPP do-until-failure
   <snip>
   20 authorize aaa list AUTHOR_LIST format USERNAME_FORMAT password cisco
  !
```

Upon Session initiation (session-start) or at session-activate TAL based authentication is attempted:

- **username:** **<PPPoE RID>:<PPPoE CID>**
- **password:** **cisco**

Structured Configuration Model

I. Configure Northbound interfaces

AAA

Portal/Policy Server

CoA

II. Configure Templates, User and Service Profiles

III. Configure Subscriber Access

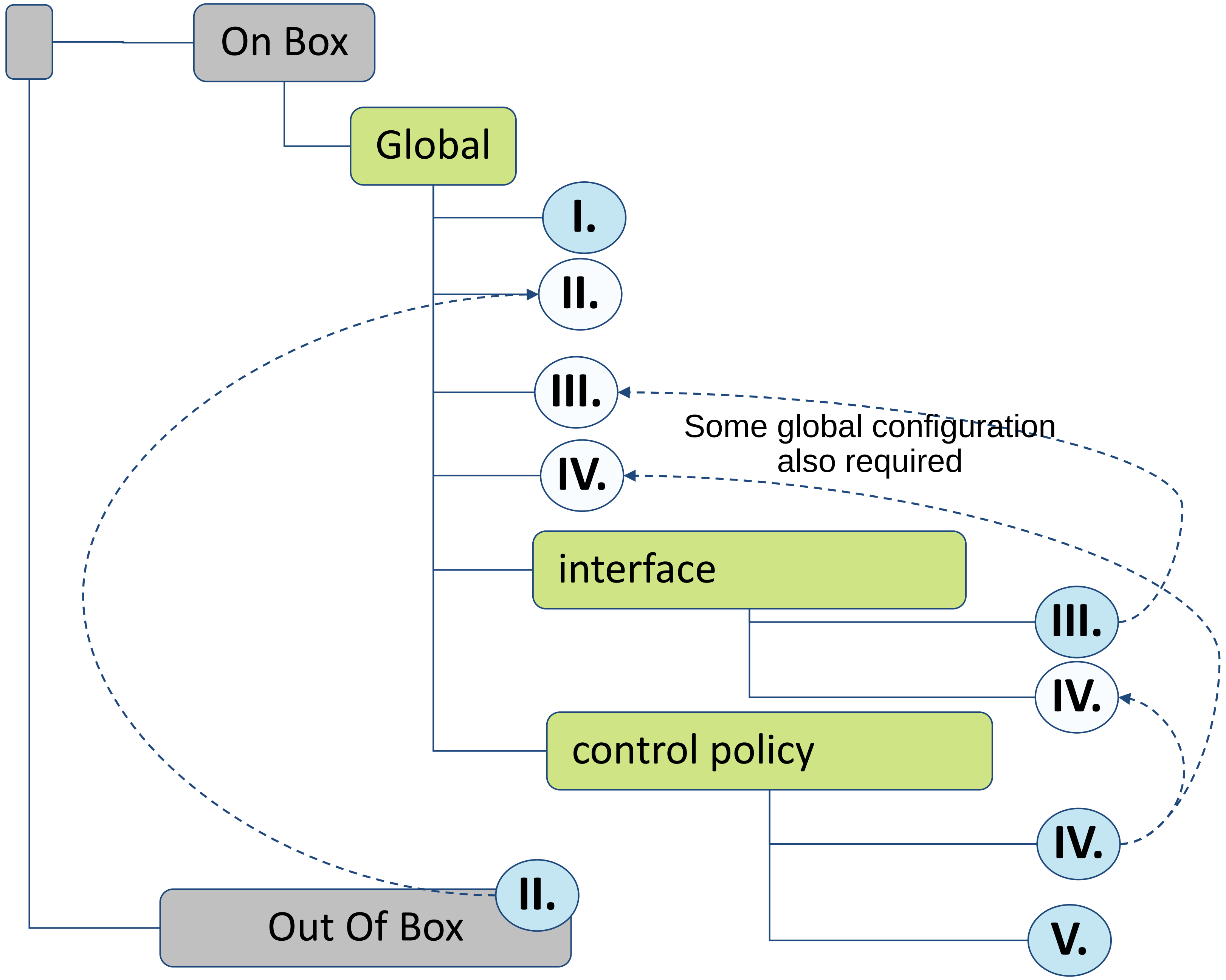
Configure session type and initiator

Create and apply the control policy

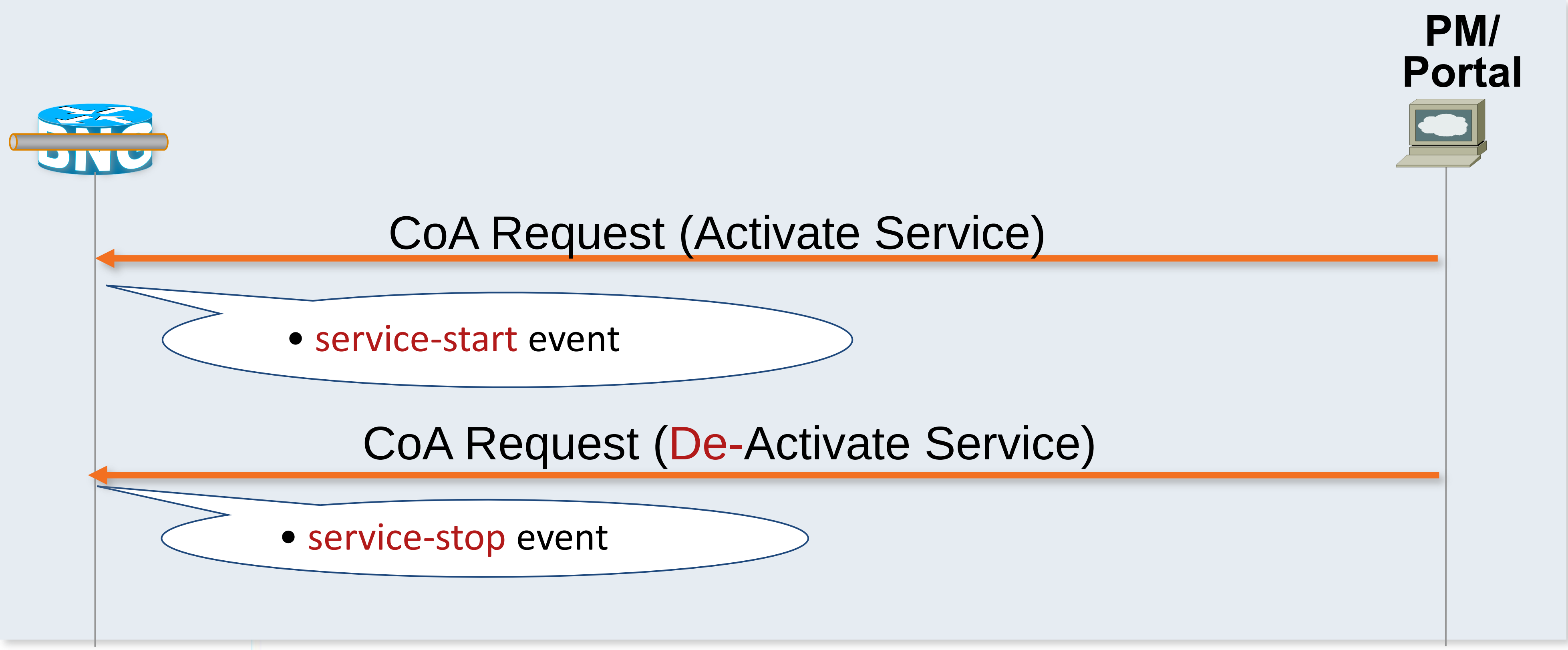
Other deployment specific cfgs

IV. Configure Subscriber Authentication

V. Dynamic Management of Dynamic Templates



V. Dynamic Managing of Dynamic Template



PM/ Portal
CoA Request (Activate Service)
• service-start event
CoA Request (De-Activate Service)
• service-stop event

- External requests to activate/deactivate a dynamic-template cause a “service-start” /“service-stop” event to be triggered
- Valid external messages

  CoA Service Activation or Deactivation request

```
policy-map type control subscriber IP_PM
 event service-stop match-first
  class type control subscriber IP do-until-failure
   10 activate dynamic-template SRV_TPL_2
  !
```

Un-applies the requested template and enable another in its place

Useful Verification Commands

- -- show subscriber session all
- -- show subscriber session all detail
- -- show subscriber database association
- -- show subscriber database summary
- -- show pppoe statistics access-interface …
- -- show pppoe summary { per-access-interface | total } location …
- -- show ppp interfaces
- -- show ppp statistics …
- -- show ipsub interface
- -- show ipsub summary
- -- show dhcp ipv4 proxy binding [detail]
- -- show radius {dynamic-author | authentication | accounting }

BNG References

- ASR9K Configuration Guides:
  - http://www.cisco.com/en/US/products/ps9853/products_installation_and_configuration_guides_list.html
- ASR1K Configuration Guides:
  - http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html
- ASR9K BNG Deployment Guide:
  - https://supportforums.cisco.com/docs/DOC-23170
- ASR9K BNG Configuration Walkthrough:
  - https://supportforums.cisco.com/docs/DOC-19726
- ASR9K BNG Training Guide (PPPoE & IPoE Sessions):
  - https://supportforums.cisco.com/docs/DOC-19702
- ASR9K BNG Debugging PPPoE Sessions:
  - https://supportforums.cisco.com/docs/DOC-19705
- Using Change of Authorization (CoA) for Access and BNG Platforms:
  - https://supportforums.cisco.com/docs/DOC-16677

Summary

- Service Provider Networks Overview
- Access Network Evolution
- Aggregation Network Evolution
- Subscriber Access Protocol Evolution
- Aggregation Service Delivery Models
- Edge Network Architectures
- IPv6 Solutions
- ASR9K BNG Configuration

Broadband Challenges…

Scalability	**Reaching millions of subscribers over high speed connections**	Next Gen Access Technologies
Cost Effectiveness	**Providing high-capacity services at low cost**	Ethernet
Flexibility	**Adding new services seamlessly**	IP
Address Space scalability	**Any appliance access to the Internet**	IPv6
Subscriber and service awareness	**Subscriber Identification and personalisation of services**	L2 and L3 access control (ISG)

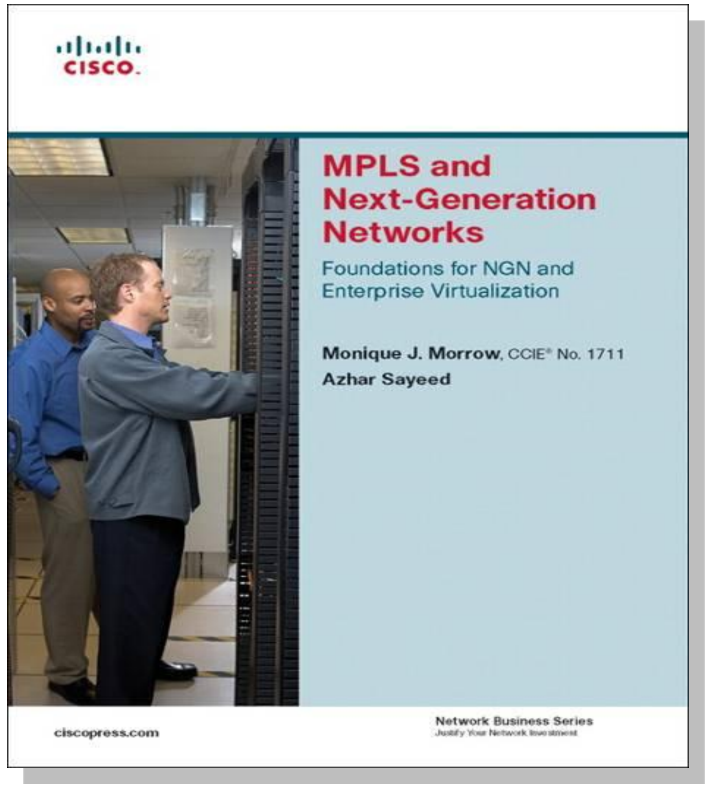
Glossary

Acronyms	
AAA	Accounting Authentication Authorization
AgN	Aggregation Node
AN	Access Node
ANCP	Access Node Control Protocol
ADSL	Asymmetric DSL
ATM	Asynchronous Transfer Mode
BNG	Broadband Network Gateway
BoD	Bandwidth on Demand
BPON	Broadband PON
BRAS	Broadband Remote Access Server
CO	Central Office
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data Over Cable Service Interface Specification
DS	Down Stream
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EAP	Extensible Authentication Protocol
EoMPLS	Ethernet over MPLS
ETTH	Ethernet To The Home
EVC	Ethernet Virtual Circuit
FRR	Fast Restoration
FSOL	First Sign Of Life
FTTC	Fiber To The Curb

Acronyms	
FTTH	Fiber To The Home
FTTN	Fiber To The Node
FTTP	Fiber To The Premises
FTTx	Fiber To The x
GPON	Gigabit PON
(G)EPON	(Gigabit) Ethernet PON
IPoE	IP over Ethernet
IPTV	IP Television
HA	High Availability
HSI	High Speed Internet
H-VPLS	Hierarchical VPLS
IGMP	Internet Group Management Protocol
ISDN	Integrated Services Digital Network
ISG	Intelligent Services Gateway
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
LR-VDSL2	Long Reach VDSL2
MPLS	Multi Protocol Label Switching
NAP	Network Access Provider
NAS	Network Access Server
NSP	Network Service Provider
OLT	Optical Line Termination
ONU	Optical Network Unit
PIM	Protocol Independent Multicast

Acronyms	
PON	Passive Optical Network
PoP	Point of Presence
PPP	Point to Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PTA	PPP Aggregation and Termination
PTP	Point To Point
PW	Pseudo Wire
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RT	Remote Terminal
SP	Service Provide
TAL	Transparent Auto Logon
TDM	Time Division Multiplexing
TE	Traffic Engineering
TR	Technical Report
UBR	Universal Broadband Router
US	Upstream
VDSL	Very High Speed DSL
VoIP	Voice over IP
VoD	Video on Demand
VPLS	Virtual Private LAN Services
VPN	Virtual Private Network
VRF	Virtual Routing Forwarding

Recommended Reading – BRKSPG-1303



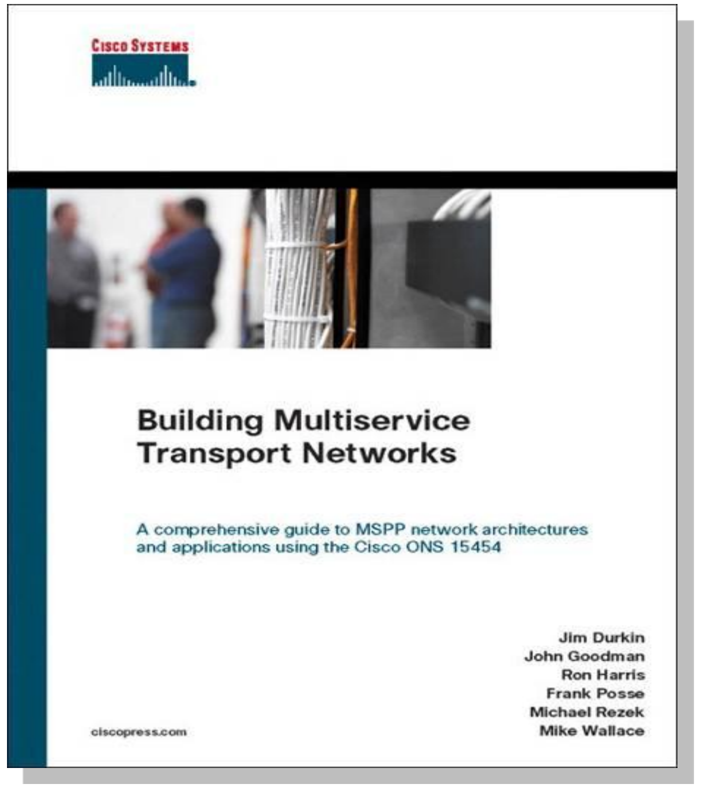
MPLS and Next-Generation Networks

Foundations for NGN and Enterprise Virtualization

Monique J. Morrow, CCIE® No. 1711
Azhar Sayeed

ciscopress.com

Network Business Series
Justify Your Network Investment

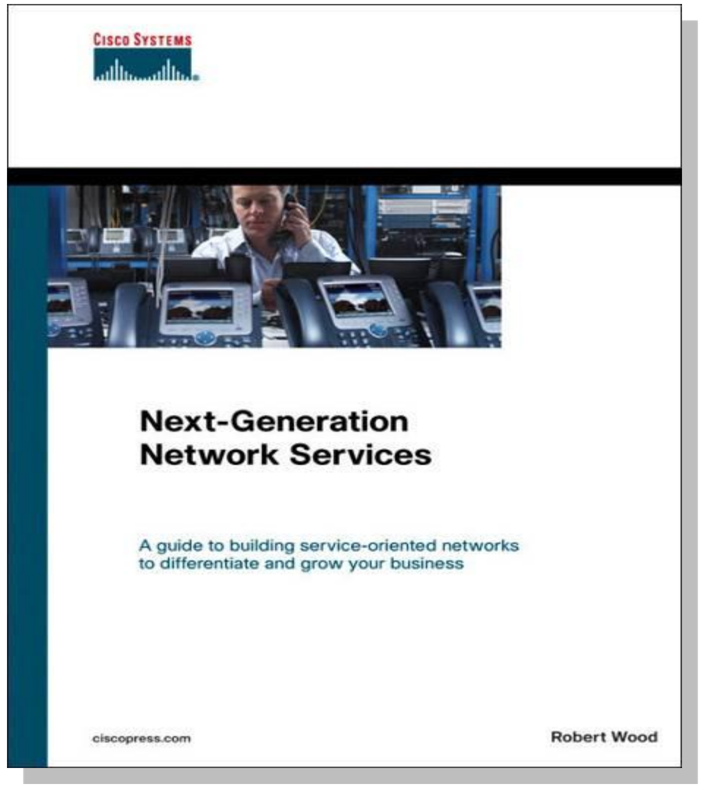


Building Multiservice Transport Networks

A comprehensive guide to MSPP network architectures and applications using the Cisco ONS 15454

Jim Durkin
John Goodman
Ron Harris
Frank Posse
Michael Rezek
Mike Wallace

ciscopress.com

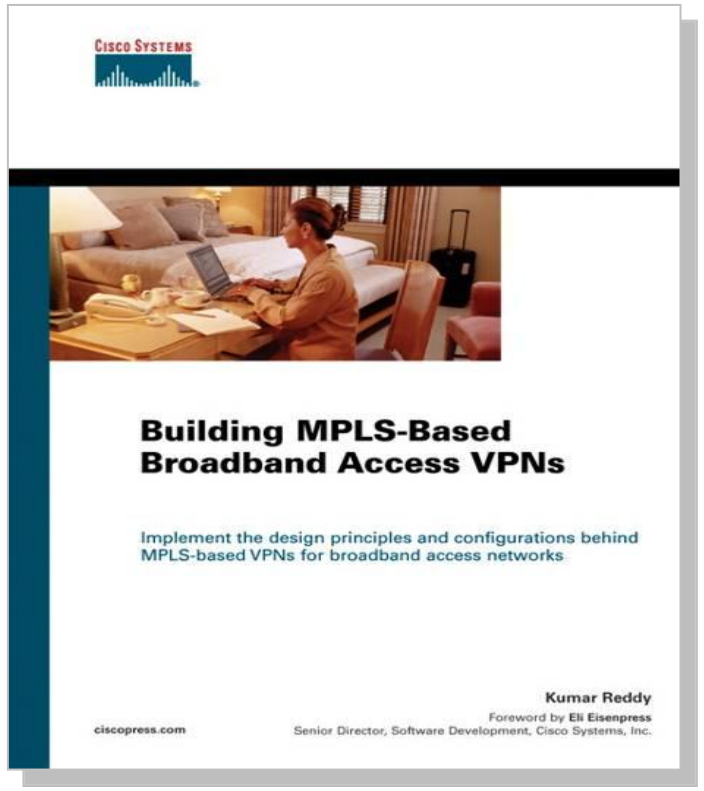


Next-Generation Network Services

A guide to building service-oriented networks to differentiate and grow your business

Robert Wood

ciscopress.com



Building MPLS-Based Broadband Access VPNs

Implement the design principles and configurations behind MPLS-based VPNs for broadband access networks

Kumar Reddy
Foreword by Eli Eisenpress
Senior Director, Software Development, Cisco Systems, Inc.

ciscopress.com

Source: Cisco Press®

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button. www.ciscoliveaustralia.com/portal/login.ww