Next Steps in Broadband

Services and Network Designs

Robert Healey
Product Manager, Edge
Juniper Networks APAC

Juniper™ NETWORKS

Agenda Overview

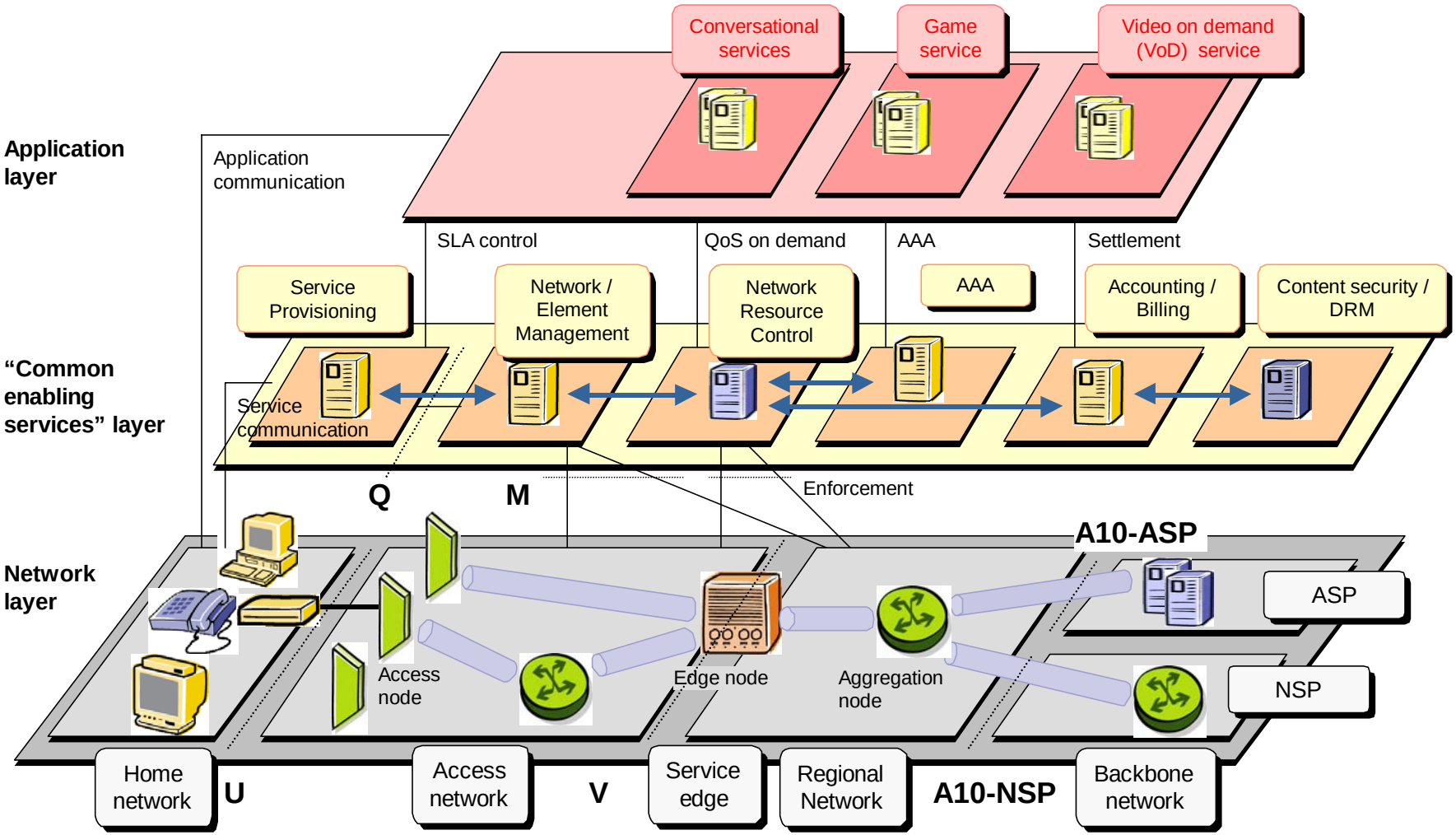
- Subscriber Broadband Access Technologies
- Protocols in use in the networks
- IP DSLAMs – where they fit
- Works in progress to address issues with emerging technology
- QoS for Broadband Access Networks
- IPv6 for Broadband Access Networks

Refresher

xDSL Access Refresher

- xDSL variants
  - ADSL2 (8Mbps downstream, 800kbps upstream)
  - ADSL+ (downstream - 16Mbps@1.3km, 10Mbps@2km, 7Mbps@3km)
  - SHDSL (192kbps-2.3Mbps/single pair, 384kbps-4.6Mbps/two pairs, 3-6km)
  - VDSL (13-52Mbps, 1.5-2.3Mbps, 300m-1.5km)
- DSL Access network
  - ATM – NA and tier 1 SP (OAM)
  - Trend towards ETH
- DSLAMs
  - ETH interface and frame processing
  - Any FX requirements for Edge Router???
  - Subscriber density
- DSL-Forum TR-59

DSL Forum TR-59 Model



TR-59 - BRAS Requirements

Category	TR-59 BRAS Requirements
QoS	Hierarchical Schedulers, strict priority queuing
	DiffServ, RED, WRED, traffic shaping
Sub Mgmt	PPP, L2TP (LAC, LTS, LNS)
	Radius, DHCP, IP address pools
Routing	BGP, OSPF, IS-IS, RIP
	Virtual Routers
	Multicast
IP VPN	VR, RFC2547
L2	MPLS
	ATM cross connect
	ATM VC, VLAN, VLAN stacking
Policy Mgmt	Packet classification
	Policing and Filtering
IPv6	IPv6 BRAS
LI	Interface mirroring

Typical BRAS Network (DSL)

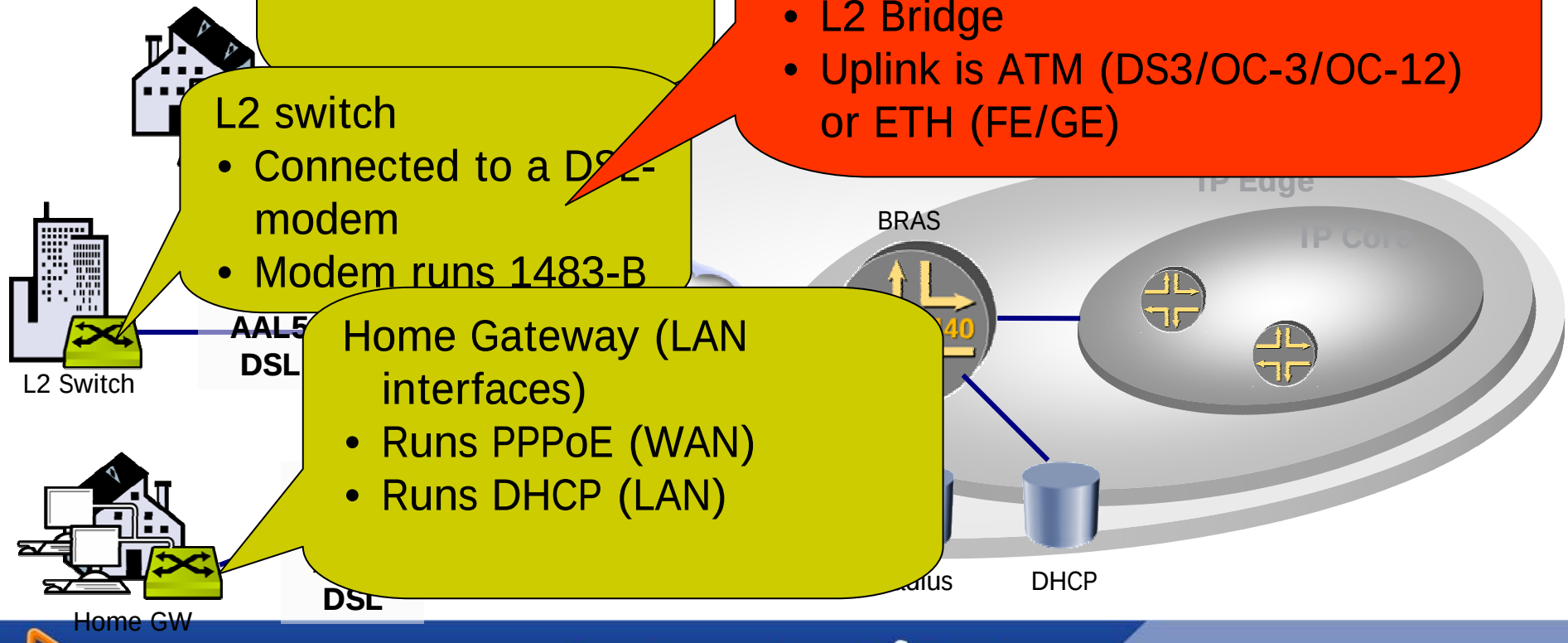
- DSL to ving to ETH
- Popu
  - s
  -)

PC client with
- PCI-based DSL-modem
- Runs PPPoA

DSLAM (Digital Subscriber Line Access MUX)
- DSL lines aggregation and termination
- L2 Bridge
- Uplink is ATM (DS3/OC-3/OC-12) or ETH (FE/GE)

L2 switch
- Connected to a DSL-modem
- Modem runs 1483-B

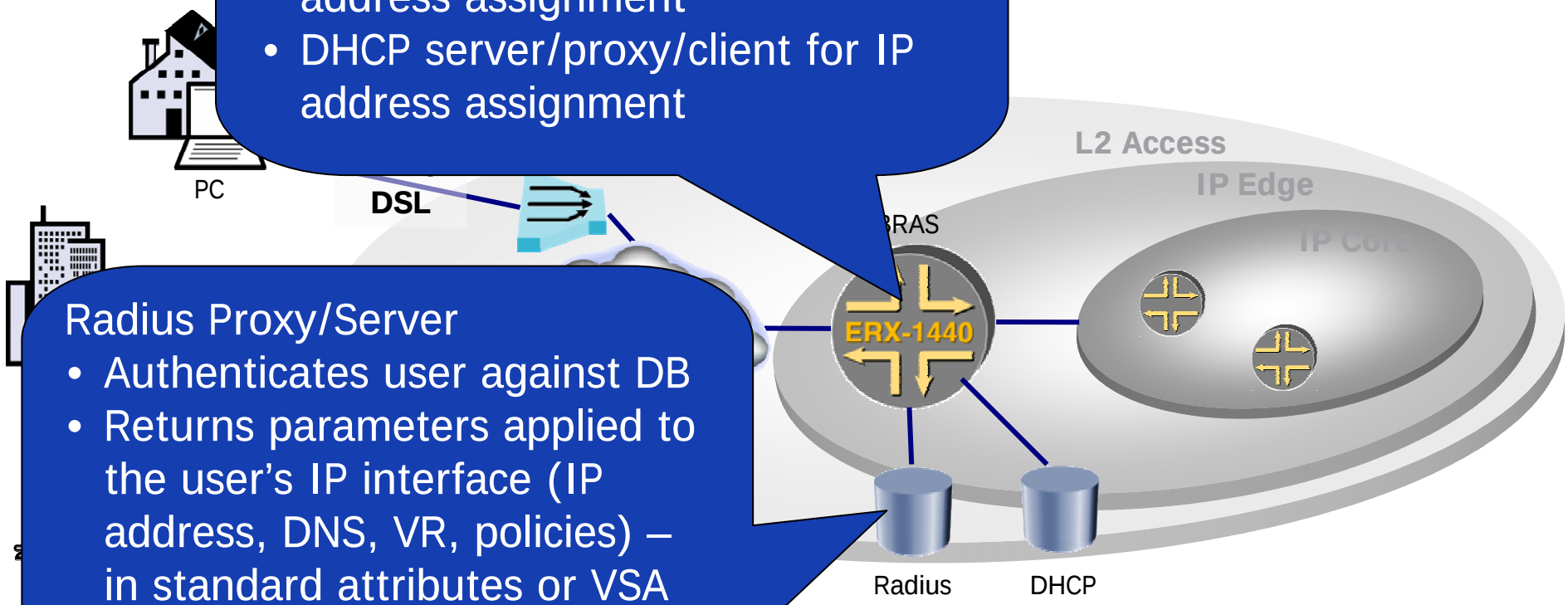
Home Gateway (LAN interfaces)
- Runs PPPoE (WAN)
- Runs DHCP (LAN)



Typical BRAS Network (DSL)

- DSL
- Pop
  -
  -

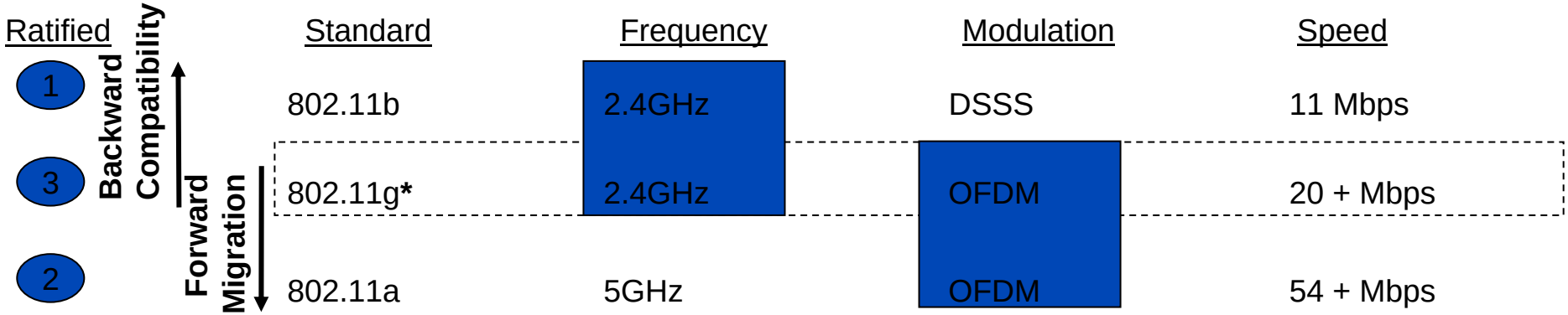
BRAS
- L2 termination and L3 forwarding
- Radius client for user authentication, accounting, IP address assignment
- DHCP server/proxy/client for IP address assignment



Radius Proxy/Server
- Authenticates user against DB
- Returns parameters applied to the user's IP interface (IP address, DNS, VR, policies) – in standard attributes or VSA
- Collects accounting data

802.11 (WLAN) Access Refresher

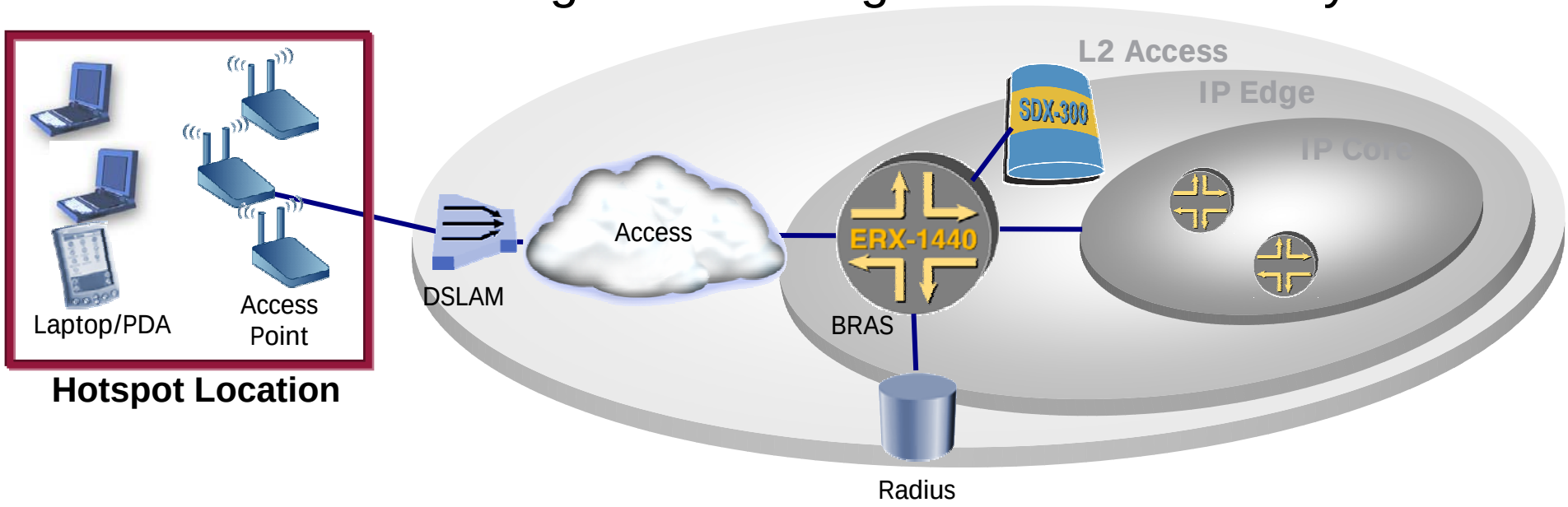
- WLAN scenarios
  - Web-based authentication
  - PPPoE
  - Remote Secure Access using IPSec/L2TP
  - 802.1X/EAP



802.11f* … Mobility
802.11e* … QoS (WME spec is a subset)
802.11i* … Enhanced Security (WPA spec is a subset)

Typical PWLAN Network

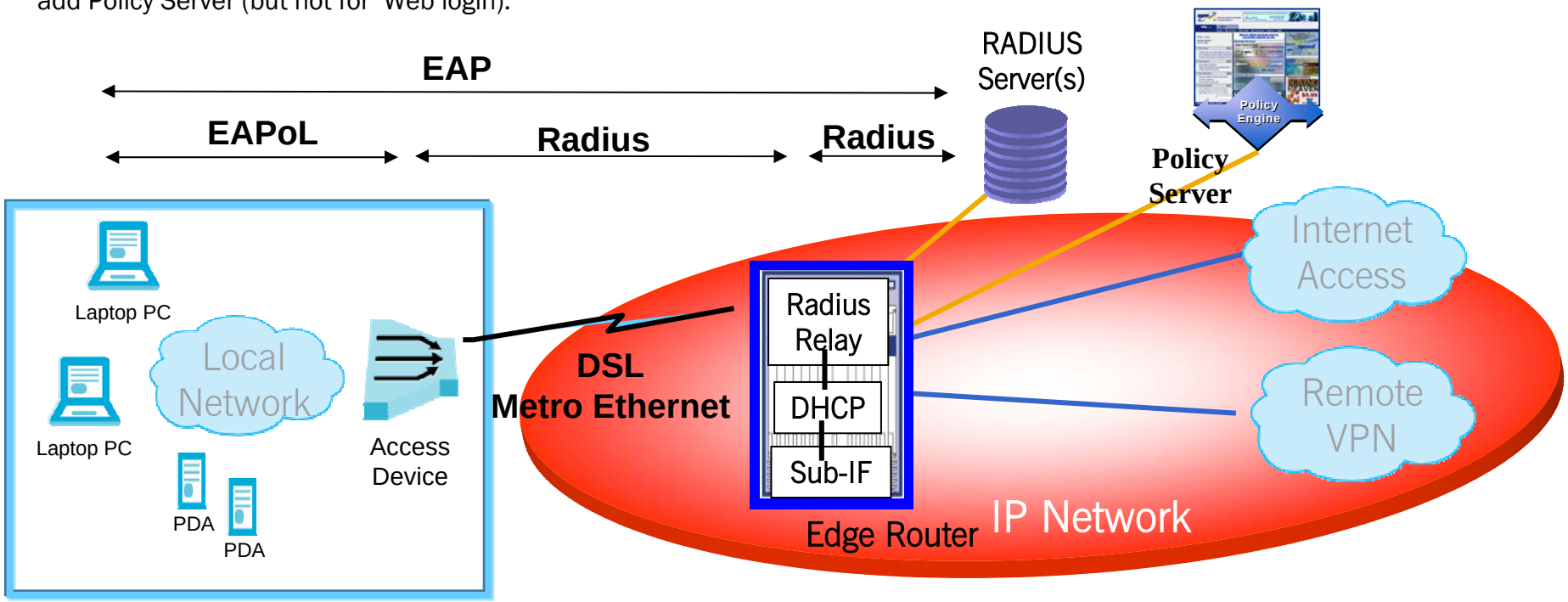
- Hotspot…1-N Access Points (AP)
- Backhaul AP traffic over DSL, M-ETH, leased line (n x T1), or… IP tunnel (think cable; think routed access network).
- Subscriber management in Edge Router and Policy Server



Transparent Radius Relay Concept for 802.1x/EAP

Multi-stage process, with a pretty good PPP-like behavior:

- Access point conveys EAP messages via Radius messages. It includes the host MAC@ in the calling-station-attribute and username@domain comes from the EAP "identity" request/response. Radius authentication and accounting (stop).
- Edge Router Radius Relay queries the real Radius server(s), and gets authorization data (VR to use, IP pool/address to use, filters, etc). To memorize with host MAC @.
- At DHCP/DCM time, create subscriber interface in proper context/VR, pick IP address, assign default "filter" policies, etc. Optional: add Policy Server (but not for Web login).

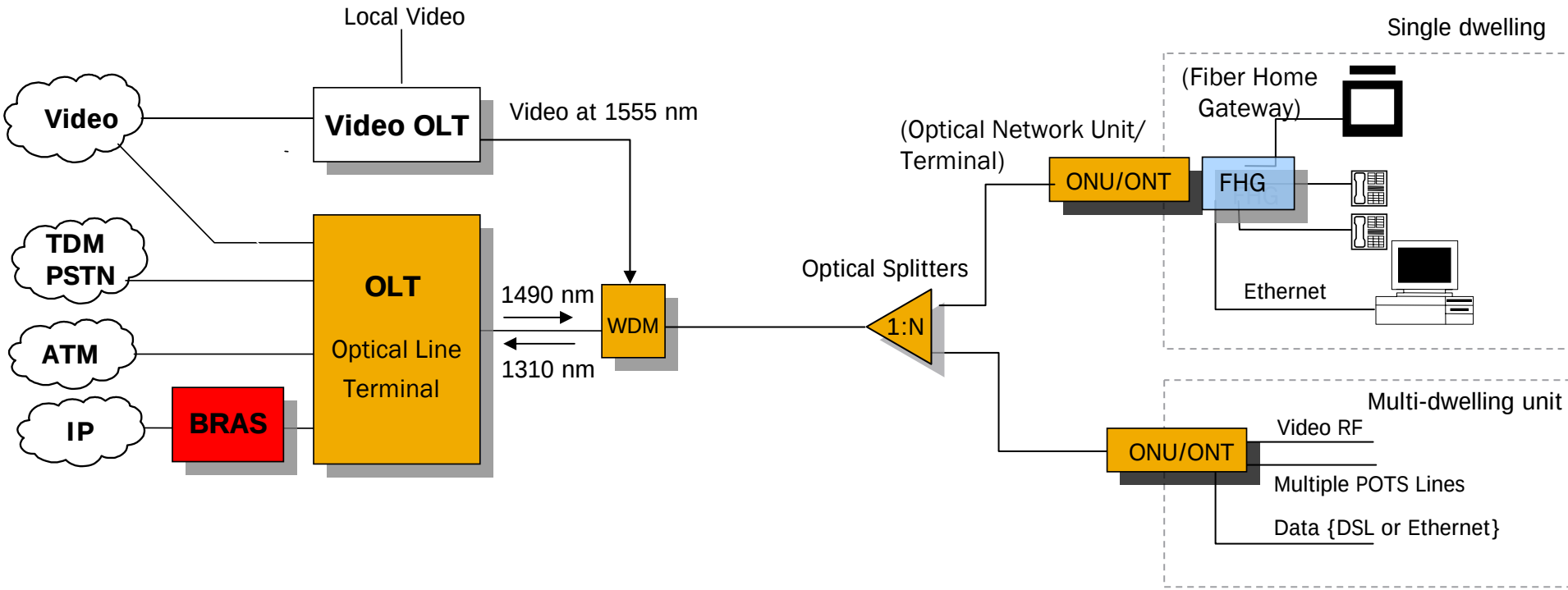


FTTP/PON

FTTP – PON Access

- FTTP…Fiber to the Premise
- PON…Passive Optical Networks
- Driver: NA JPC (BLS, VZ, SBC)
- Various flavors – APON moving to GPON
- PON already deployed in APAC (eg Japan)

PON Network Architecture



APON = ATM-based BPON	622 Mbps downstream and 155 Mbps upstream (shared)
BPON = Broadband PON	622 Mbps downstream and 155 Mbps upstream (shared)
EPON = Ethernet PON	1Gbps downstream
GPON = Gigabit PON	Various Gbps speed combinations e.g. 1.2 Gbps down, 622 Mbps upstream

PON Technologies

- BPON = Broadband PON
  - Same as APON. ATM PON was being interpreted as limited to ATM services
  - Sponsors FSAN (Full Service Access Networks Organization) and ITU-T
  - ITU G.983 series 622 Mbps downstream and 155 Mbps upstream and video option
- EPON = Ethernet PON
  - Sponsors EFMA (Ethernet in the First Mile Alliance) and IEEE 802.3ah
  - EFMA and IEE also defining Ethernet over Copper VDSL
  - Mainly data vendor membership, Cisco an EPON advocate
- GPON = Gigabit PON
  - Evolution of BPON by FSAN and ITU-T
  - Improved IP data and TDM handling in new frame encapsulation
  - ITU G.984 series in final stages of ratification
  - 1.2 Gbps downstream and 622Mbps shared upstream
- Metro WDM, SDH, are active P-to-P FITL suitable for metropolitan/business
- Broadcast video / HDTV service usually on separate wavelength = not driver for IP bandwidth

http://www.ponforum.org/technology

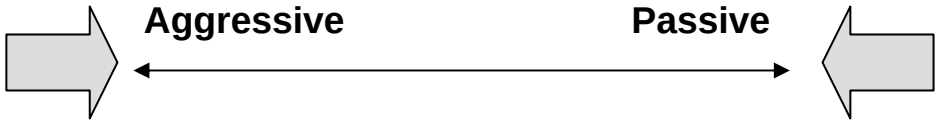
FTTP Market Dynamics

Drivers - Offensive

- Copper Loop Deterioration
- Future-proofed for high bandwidth services
- Technology cheaper

Blockers - External

- Regulatory climate
- Technology maturity
- Emerging alternatives



Drivers - Defensive

- Voice revenue declining to wireless, IXC, MSOs (but still cash generating)
- Cable triple threat

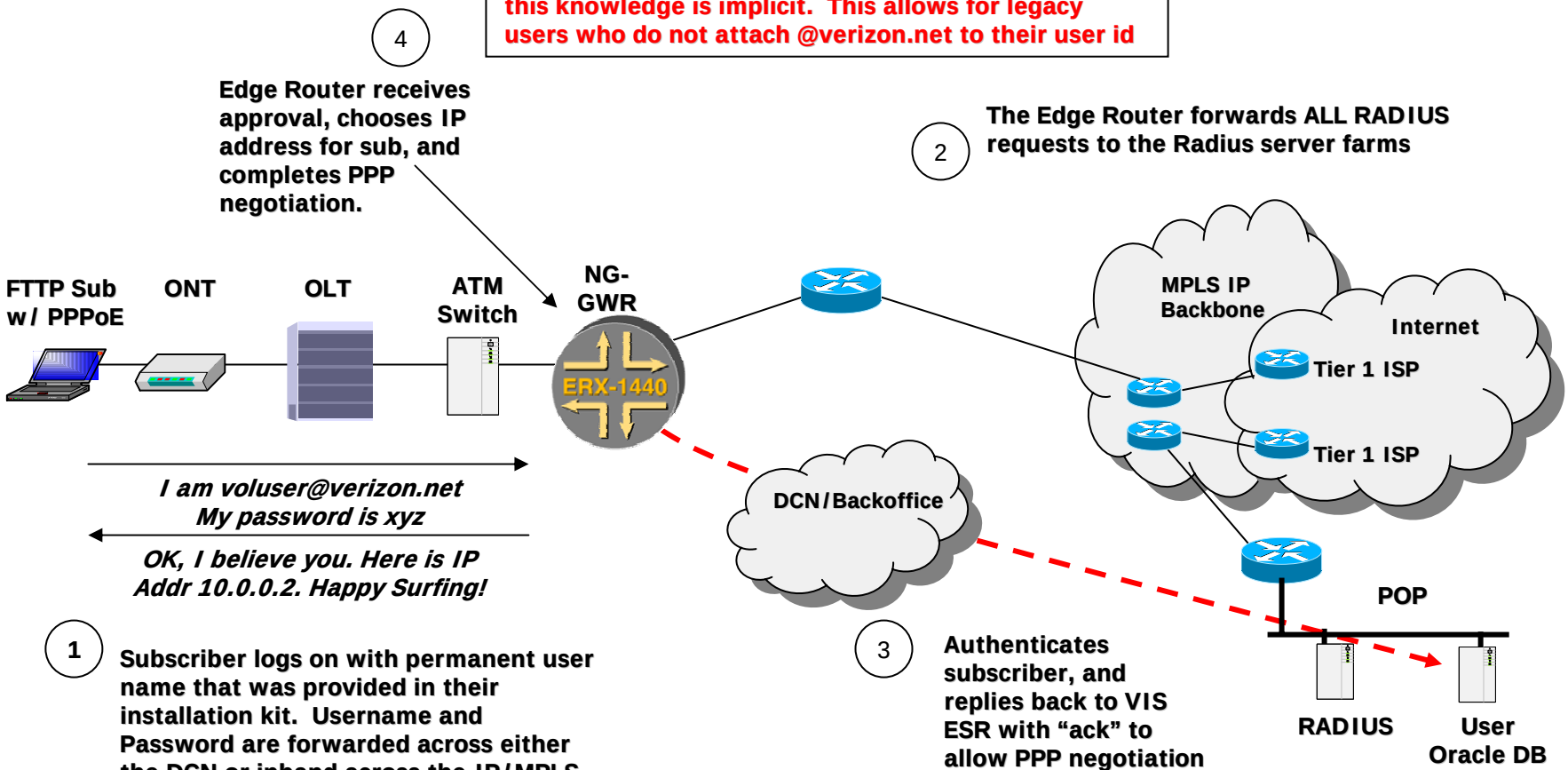
APAC
Verizon
BellSouth
SBC
EMEA
Qwest

Blockers - Internal

- No rev/"killer-app" today
- Capital structure
- Capex intensive
- Operational hurdles

US PON Network Concept

Users mapped to a single Edge Router VR. The Edge Router does not need to determine the realm of a user (ie, which service provider they belong to), since this knowledge is implicit. This allows for legacy users who do not attach @verizon.net to their user id



PON Summary

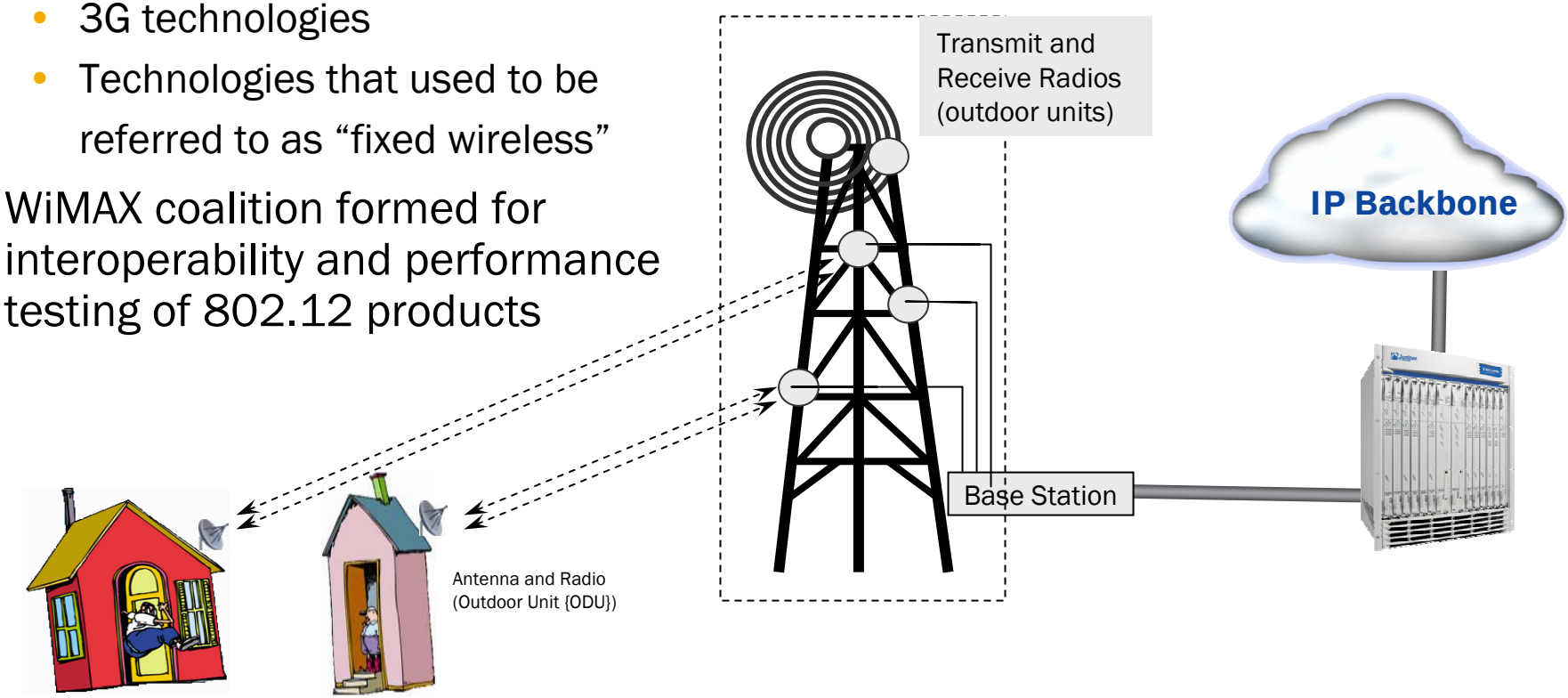
- FTTP PON technology maturing and deployment ready
  - DSL and Cable will continue to dominate broadband access
  - Metro-E alternatives growing in APAC
- Blockers outweigh market drivers for FTTP near-term
  - Key blockers: regulatory instability, massive capital expenditures, no significant revenue return
  - Deployment rate dependent on changes in blockers

Emerging Broadband Networks

- Broadband Wireless
- Free-Space Optics
- Satellite
- Powerline Communications

Broadband Wireless

- Broadband Wireless can refer to
  - 802.11 wireless
  - 3G technologies
  - Technologies that used to be referred to as “fixed wireless”
- WiMAX coalition formed for interoperability and performance testing of 802.12 products

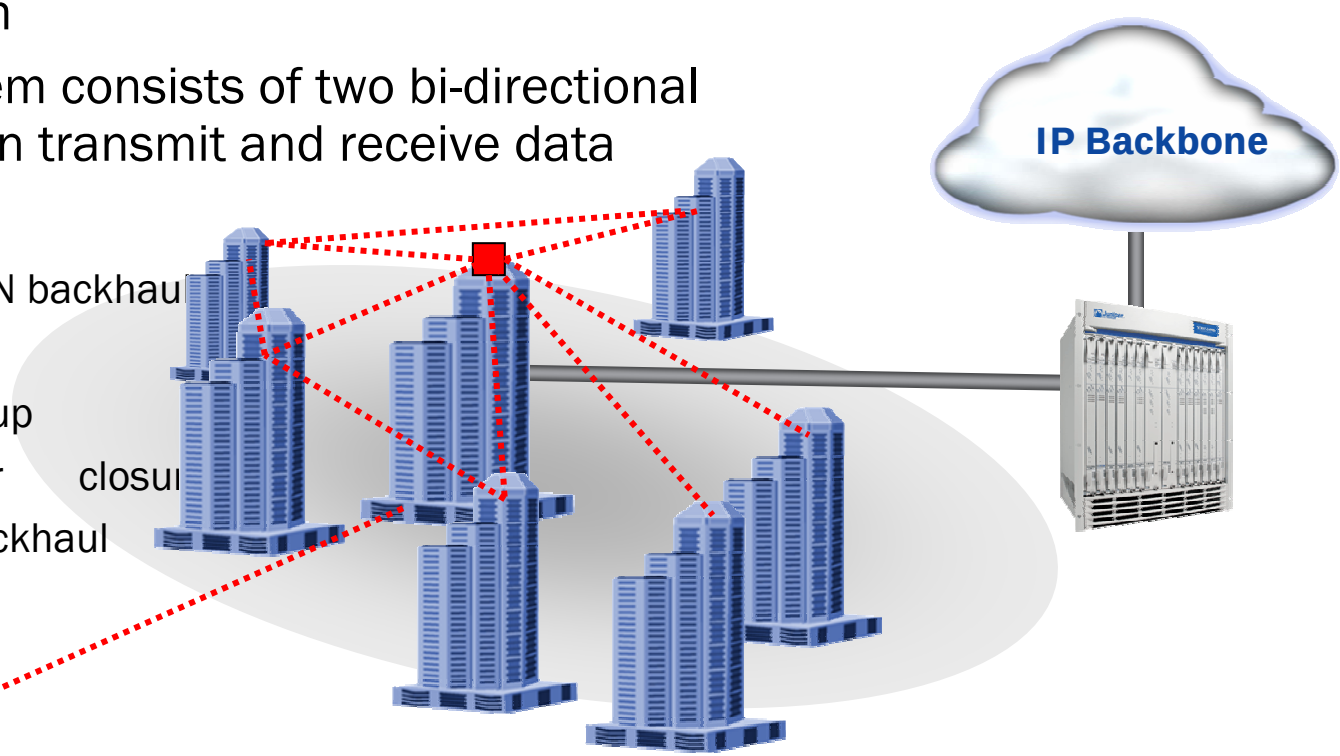


Free Space Optics

- Transmits data via an infrared laser in the unlicensed terahertz spectrum
- A typical FSO system consists of two bi-directional telescopes that can transmit and receive data

Applications

- Gigabit Ethernet or PON backhau
- Large building access
- Redundant fiber back up
- Metro ring extension or closu
- 2.5 and 3G cellular backhaul

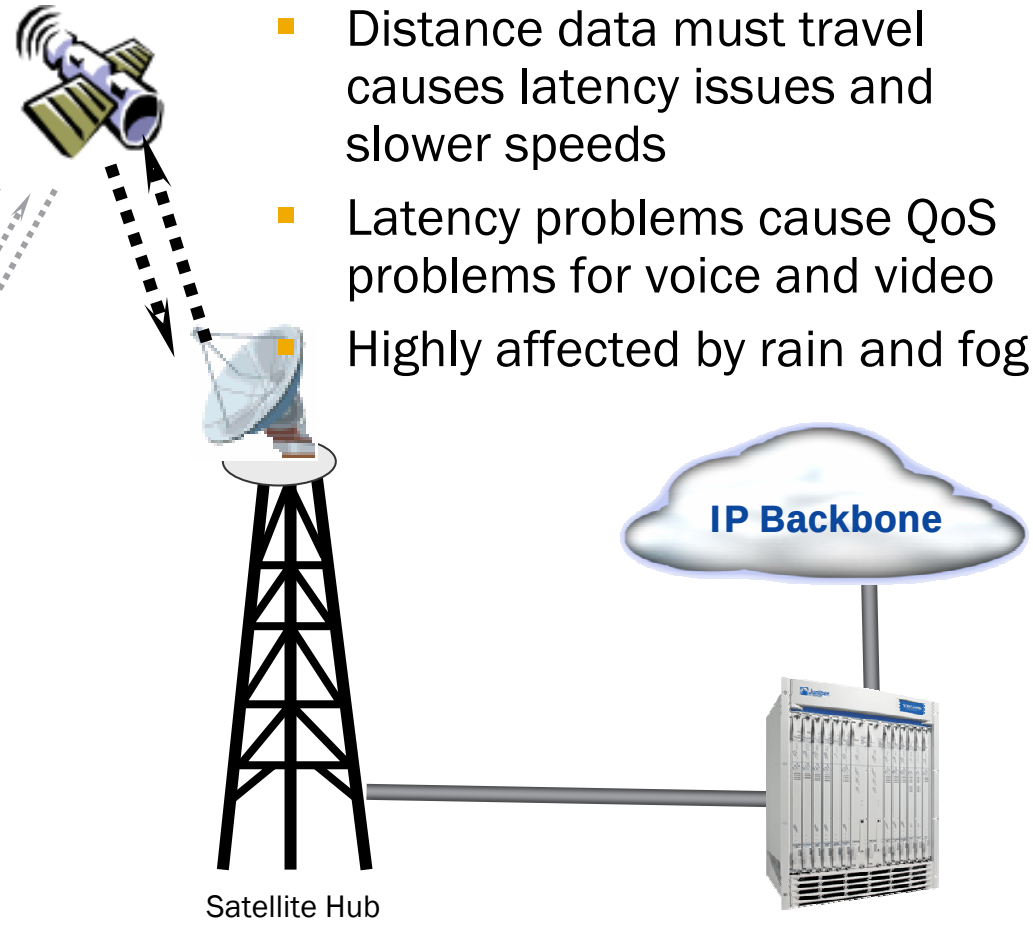


Lightpointe, Terabeam and fSONA still making sales. AirFiber shut down

Satellite Networks

- Growing segment for mobile communications in government sector
- Good for multicasting to many locations
- Good for connection dispersed and underserved locations

Good for best-effort, rural consumer high-speed internet service and Rural remote office access. Not a strong business focus due to QoS issues

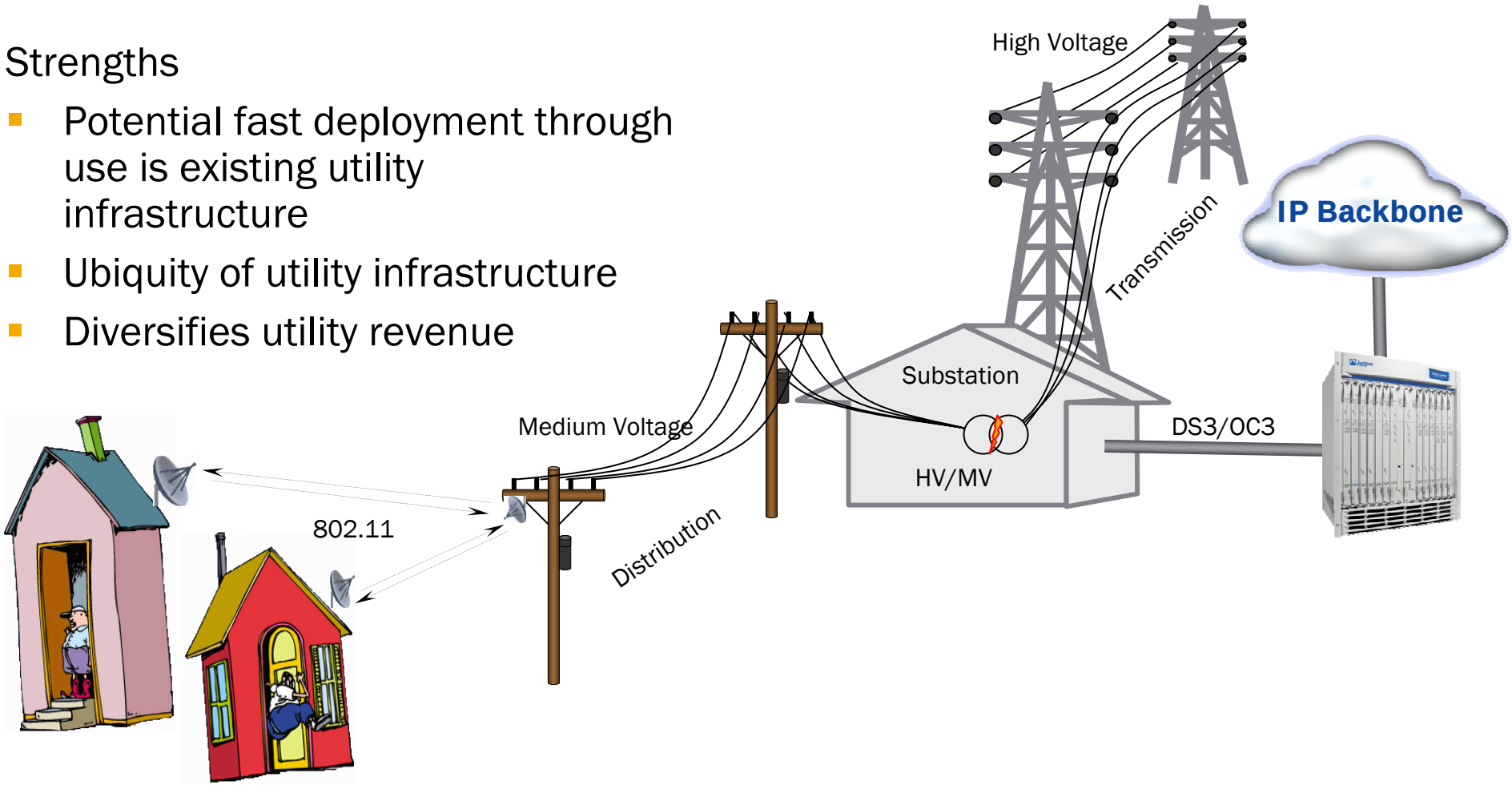


- Distance data must travel causes latency issues and slower speeds
- Latency problems cause QoS problems for voice and video
- Highly affected by rain and fog

Powerline Networks

Strengths

- Potential fast deployment through use is existing utility infrastructure
- Ubiquity of utility infrastructure
- Diversifies utility revenue



PPP and Non-PPP Broadband Access Models

Current State and Future Directions

Juniper™ NETWORKS

Background - IPv4 BRAS Service Models

- PPP-based model
- Requires PPPoE or PPPoA client software or CPE device
- Session based service model
- User authentication & accounting information present
- Radius based AAA
- Leverages LCP and IPCP protocols

- Non PPP-based model
- Business services
  - Bridged / Routed 1483 services (Business broadband)
- Subscriber Services
  - DHCP based broadband remote access
  - Good for lightweight clients
  - Requires many add-ins to DHCP to allow AAA, session monitoring, accounting, etc etc etc etc....

Typical BRAS Network (DSL)

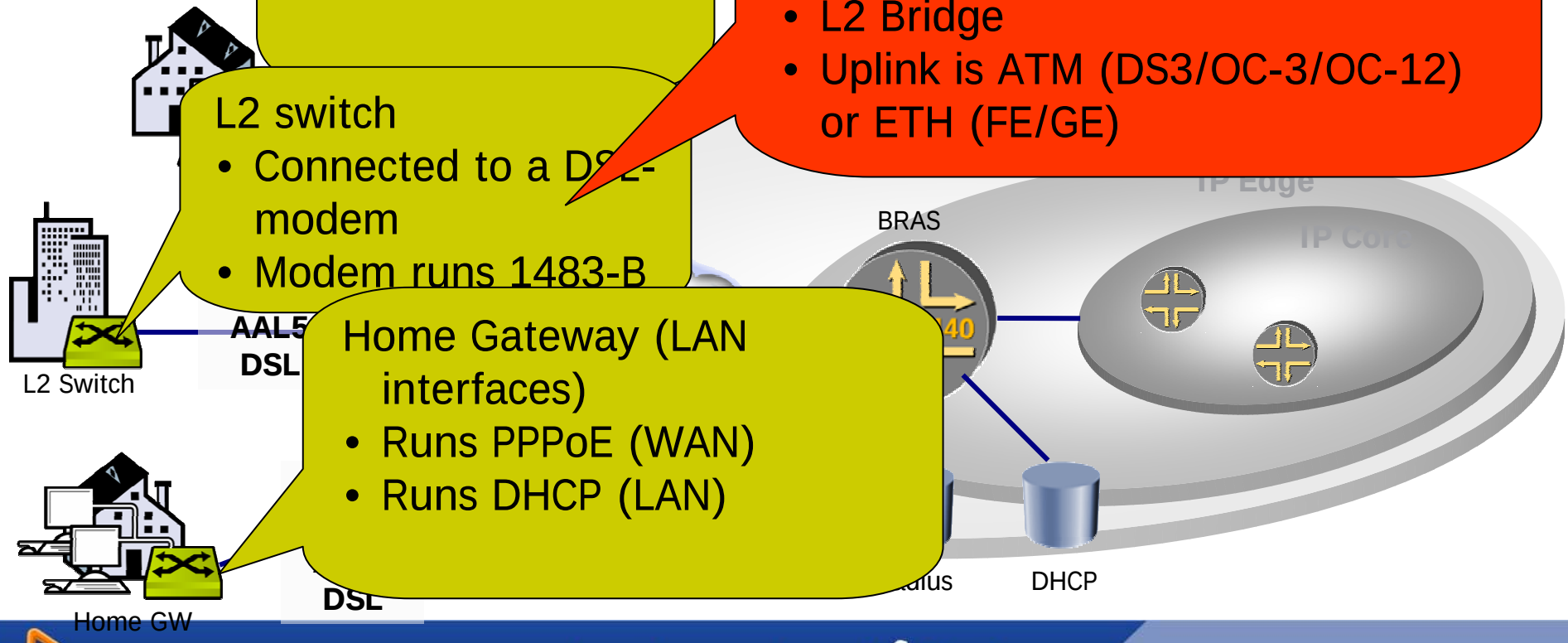
- DSL to ving to ETH
- Popu
  - s
  -)

PC client with
- PCI-based DSL-modem
- Runs PPPoA

DSLAM (Digital Subscriber Line Access MUX)
- DSL lines aggregation and termination
- L2 Bridge
- Uplink is ATM (DS3/OC-3/OC-12) or ETH (FE/GE)

L2 switch
- Connected to a DSL-modem
- Modem runs 1483-B

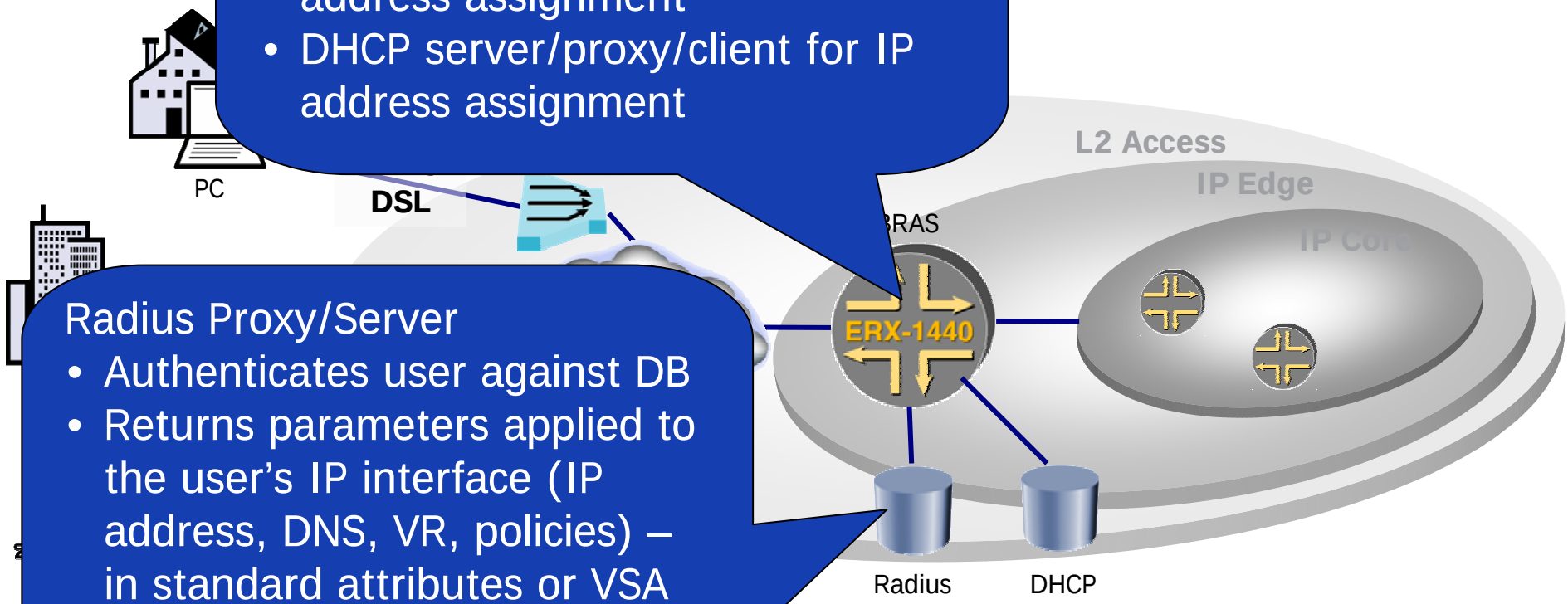
Home Gateway (LAN interfaces)
- Runs PPPoE (WAN)
- Runs DHCP (LAN)



Typical BRAS Network (DSL)

- DSL
- Pop
  -
  -

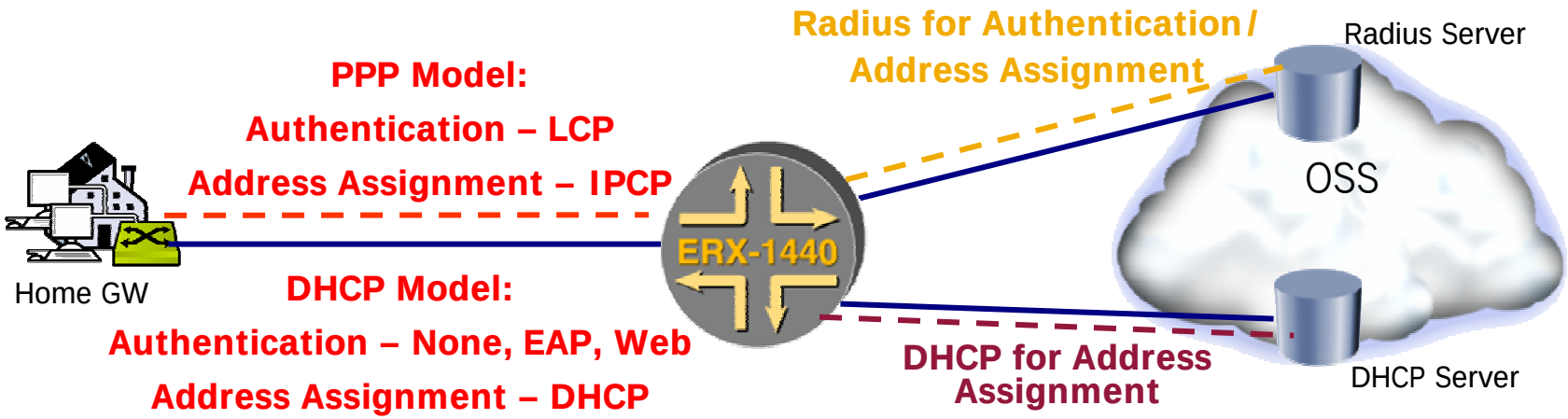
BRAS
- L2 termination and L3 forwarding
- Radius client for user authentication, accounting, IP address assignment
- DHCP server/proxy/client for IP address assignment



Radius Proxy/Server
- Authenticates user against DB
- Returns parameters applied to the user's IP interface (IP address, DNS, VR, policies) – in standard attributes or VSA
- Collects accounting data

DHCP-Access Model

- What is it?
  - IP address assignment through DHCP (instead of IPCP like in PPP)
  - Mixed models
    - Public WLAN: Web Login or 802.1.x/EAP for user authentication, DHCP for address assignment
  - Link is authenticated, but IP address assignment can change
  - Subscriber management is preserved



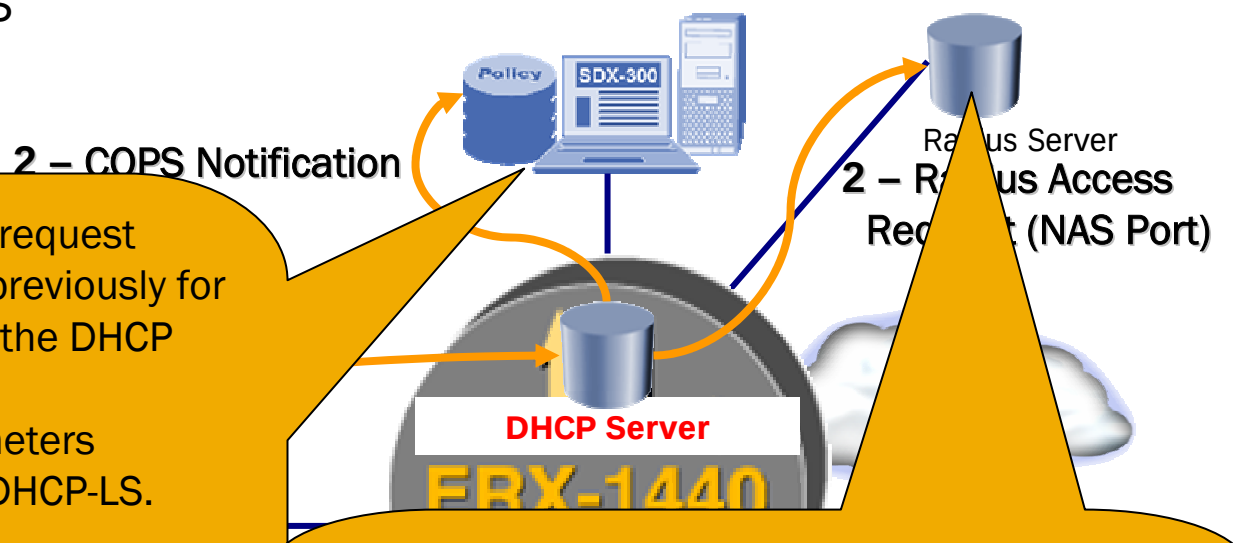
DHCP-Access Drivers and Issues

- Drivers
  - Metro Edge, Public WLAN, IPv6
  - Some DSL access providers prefer DHCP over PPP
  - Non-PPP based appliances/applications
  - Indirectly through FTTP/PON (FHG auto-configuration management)
- Creates some other issues to be addressed
  - PPP"-equivalent to create IP interface per user ➔ "Subscriber Interface" concepts
  - No inherent user authentication ➔ EAP, Web, "implicit login"
  - Wholesale models ➔ service subscription-based
- Objective - leverage subscriber management smarts in Edge Router

Edge Router DHCP Communication with OSS (Radius/Policy Server)

- OSS == Radius, Policy Server and DHCP server

- Upon the DHCP discover message, the Edge Router (server) can query the Policy Server (COPS) and/or the Radius server (Radius) for additional information, e.g. accept/deny, IP address/pool, VR, policies, QoS



- Edge Router client sends a request similar to the message sent previously for the Token Request including the DHCP options
- Policy Server returns parameters intended to be used only by DHCP-LS. Currently supported:
  - Framed-IP-address, Framed-Pool, Virtual-Router-name, domain-name, User-name, Service-bundle, Radius-class
- User-name, Service-Bundle and Radius-class are only sent back to Policy Server when the address was accepted by the client

- Session with Radius server (access and accounting) based on user name and/or NAS Port
- Radius server can return parameter to be applied to the IP interface

Edge Router DHCP Communication with OSS – Policy Server

- Policy Server can also disconnect a user (i.e. revoke a lease for a given user) in DHCP mode (makes switch of IP address space/VR possible)

- Policy Server allows for setting additional fields which are currently ignored by DHCP Server:
  - Accept/deny DHCP address, lease time, serverName/bootFile (bootP options), DHCP Options

Edge Router DHCP Communication with OSS – Policy Server (cont'd)

- Policy Server distinguishes between "authenticated" and "unauthenticated" modes based on whether the User-Name was included in the address request
  - "Unauthenticated" mode can be viewed as "Token" IP addresses that refer to pools with a very short lease time only
  - "Authenticated" mode can be viewed as "Public" IP addresses
  - Switching from unauthenticated to authenticated mode is handled by Policy Server (i.e. revoking the lease for a given user)

New Paradigm – Policy Enabled BRAS

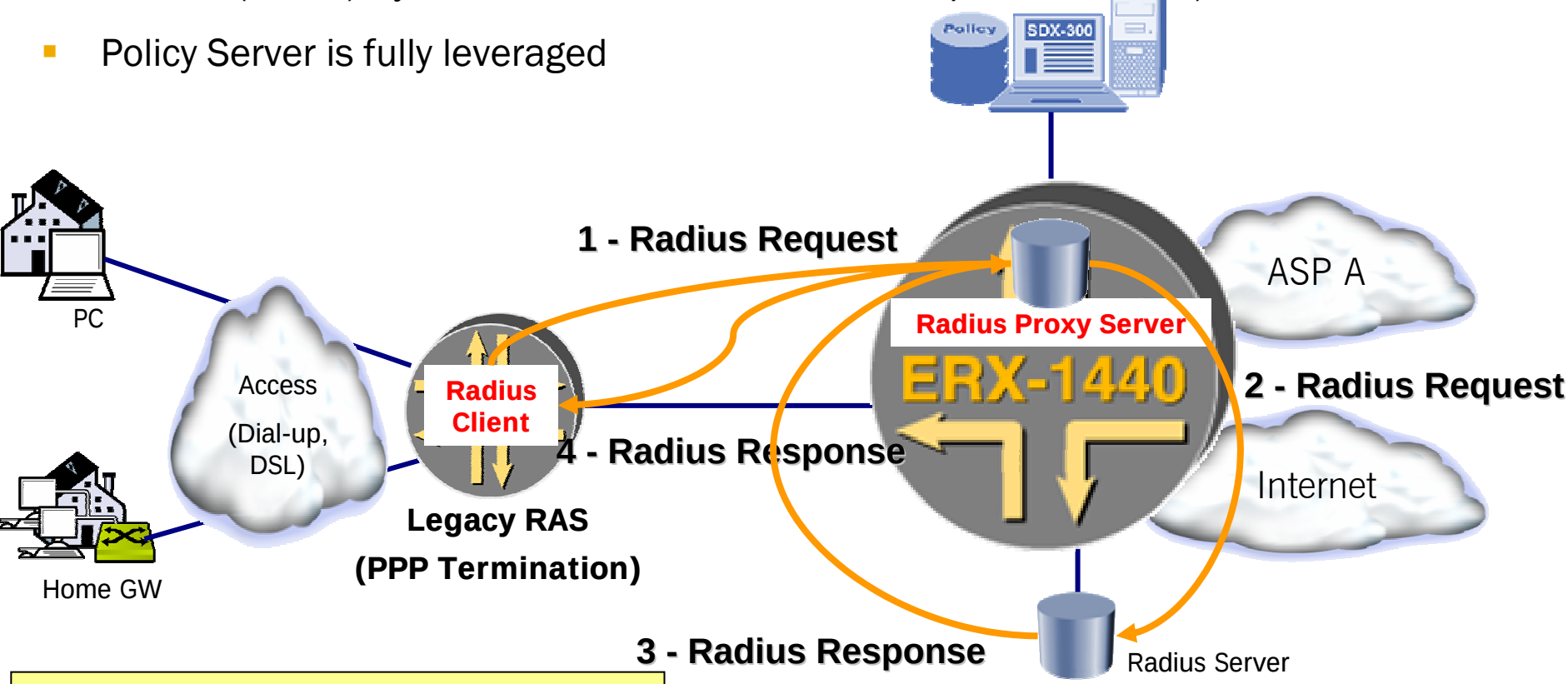
(over both PPP and non-PPP Models)

Policy Enabled BRAS

- Concept : Increase service intelligence of existing BRAS networks, without replacing everything
- Utilise legacy equipment as much as possible
- Add in new, improved BRAS devices, perhaps as a back-end system, to allow new service creation & delivery
- Ideally, should work for both PPP and DHCP based access

NEW Edge Router behind Legacy BRAS (PPP Model)

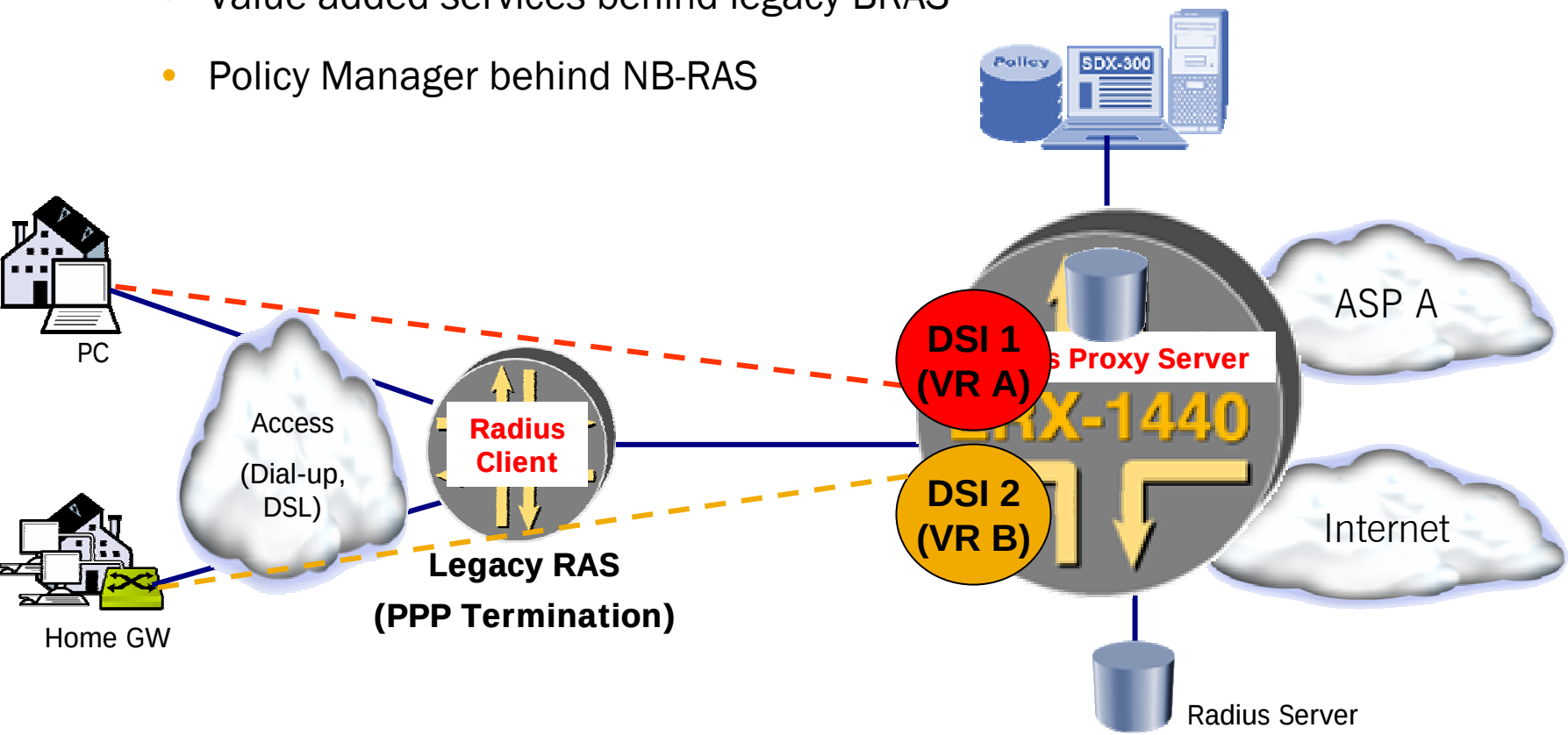
- NEW Edge Router sits behind legacy BRAS (no L2TP) for value-added services
- Radius Proxy Server in Edge Router is in the Radius control plane loop and creates (or not) Dynamic Subscriber Interfaces for particular user)
- Policy Server is fully leveraged



Note: This behavior will not be included in the first release of the Radius-Proxy, which is solely geared at EAP scenarios.

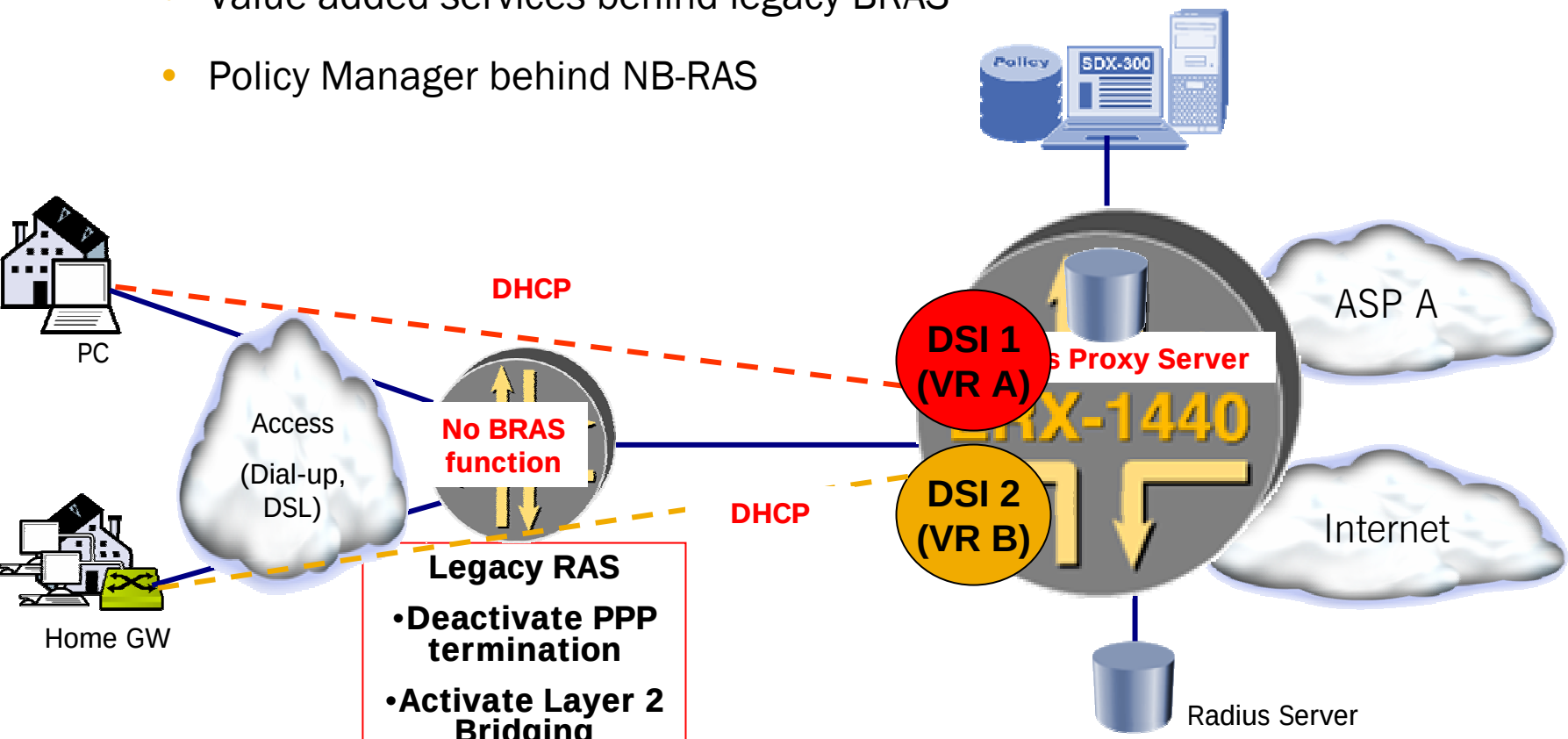
Edge Router behind Legacy BRAS (PPP Model)

- Applications
  - Value-added services behind legacy BRAS
  - Policy Manager behind NB-RAS



Edge Router behind Legacy BRAS (DHCP Model)

- Applications
  - Value-added services behind legacy BRAS
  - Policy Manager behind NB-RAS



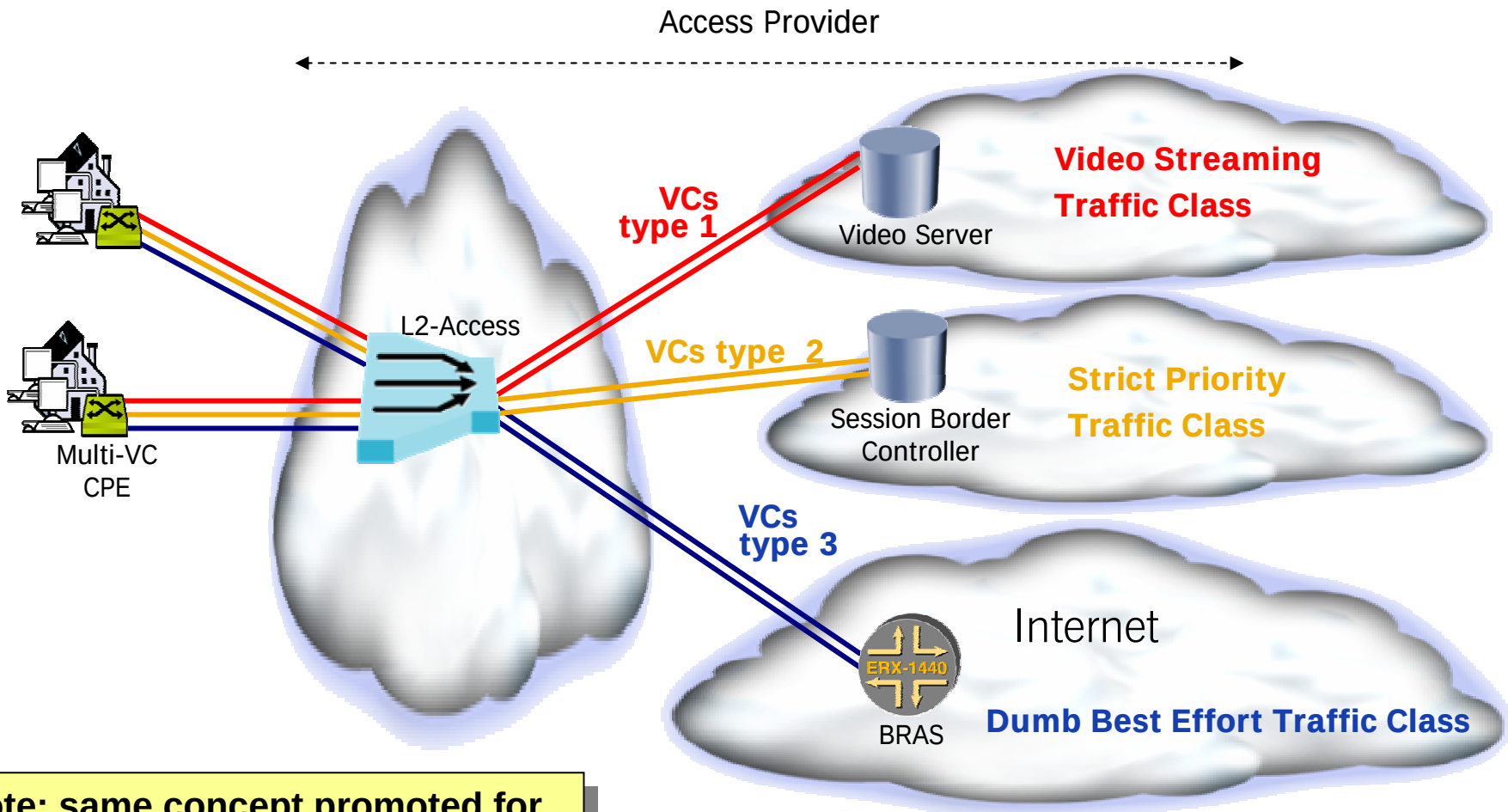
“Intelligent DSLAM”

Service Models

The IP DSLAM Vendors' View

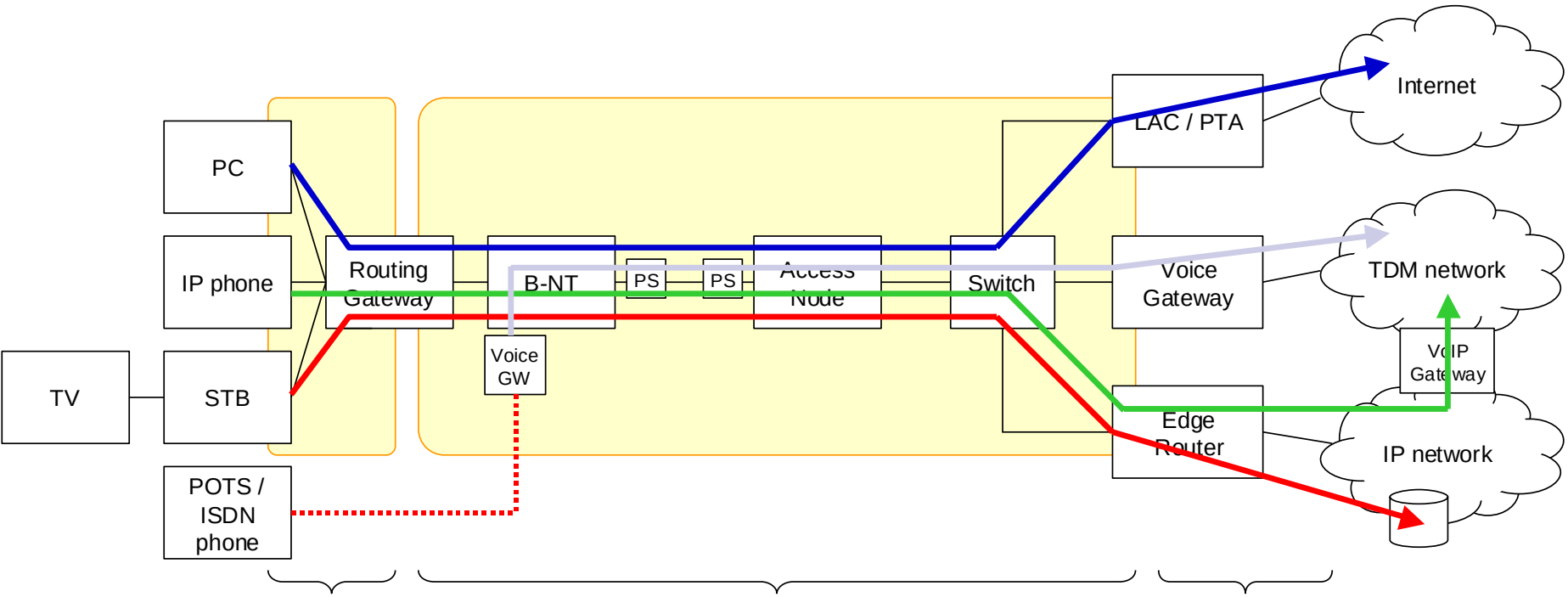
- IP DSLAM Vendors's DSL-F dsl2003.427.doc presented at DSL-Forum in Paris disclosed their access network strategy (co-authored by FT and Telefonica; BT issued a separate supporting contribution)
- Concept calls for a "VC/VLAN per Service" model including a dedicated edge device per service (e.g. session border controller for IP Telephony service; video server for broadcast-TV or VoD)
  - Issue : BRAS is completely bypassed for all value-added services

DSLAM Vendors' views on Broadband



Note: same concept promoted for Ethernet access, using VLANs instead of ATM VCs.

IP DSLAM Vendors's Network Reference Model



Flow segregation at layer 2/3/4
- src/dest MAC address
- VLAN ID
- Ethernet priority field
- src/dest IP address
- TCP/UDP
- src/dest port number

Service & customer segregation at layer 2
- ATM VPI/VCI
- src/dest MAC address
- VLAN ID (stack)
- Ethernet priority field
- MPLS label (stack)

Service segregation at layer 2
- multi-edge

Flow segregation at layer 3/4
- src/dest IP address
- TCP/UDP
- src/dest port number

- Multi-VC/VLAN approach
- 1 VC/VLAN per application/service

Terminology for this Network Model

- Switching and Routing of traffic based on multiple logical layer 2 connections
- Applicable to multiple Regional/Access Network transmission technologies (e.g. Ethernet, MPLS, IP)
- Support for the appropriate QoS for the various services using Layer 2 QoS features
- Support for Network Resource Control if contention of bandwidth occurs
- Multicasting of traffic at optimal network location(s)
- ATM, IP and Service auto-configuration

Note: Network Resource Control means Admission Control here.

Issues with this Service Model

- In the Service Provider's eyes:
  - Architecture relies on ATM, local loop and access (QoS) => not suitable for low-cost ATM-free access technologies. Not future-proof
  - More application-oriented devices in Central Offices, or very distributed Data Centers => high capex, high opex
  - Overall subscriber management logic very distributed (OSS integr. nightmare)
  - To allow deterministic routing via the multiple paths to the customer premises, multiple IP addresses need to be allocated by the carrier to a given subscriber (on the WAN interface)
    - This implies in turn a waste of IP addresses
    - Plus NAT (with many ALGs) in the res'l gateway since a multi-service host (e.g. PC, STB) typically has a single host address. This will stay true for IPv6 (!!).
  - Much less opportunity for cost reduction by cleverly over-subscribing access network across multiple applications & traffic classes.

The Edge Router and Security

	Infrastructure Protection	Customer Protection
Prevention	1. Hardware based router protection 2. Encryption of Control Traffic	3. Secure Remote Access (L2TP/IPSec) 4. Secure VPN trunking 5. Policies 6. Source address validation
Detection	7. Real time traffic analysis (port mirroring) for Lawful Intercept, IDS 8. Flow Monitoring (Netflow) 9. Event Manager Thresholds 10. Policy Server Services w/ VTA	11. Stateful Firewall 12. Event Manager Thresholds 13. Policy Server Services w/ VTA
Suppression/ Isolation	15. I/O filters to block attack flows 16. SRP Rate limiting	17. Hitless filter implementation 18. Rate Limiting 19. Policy Server Services
Correction	20. Policy Server Services	21. Policy Server Services

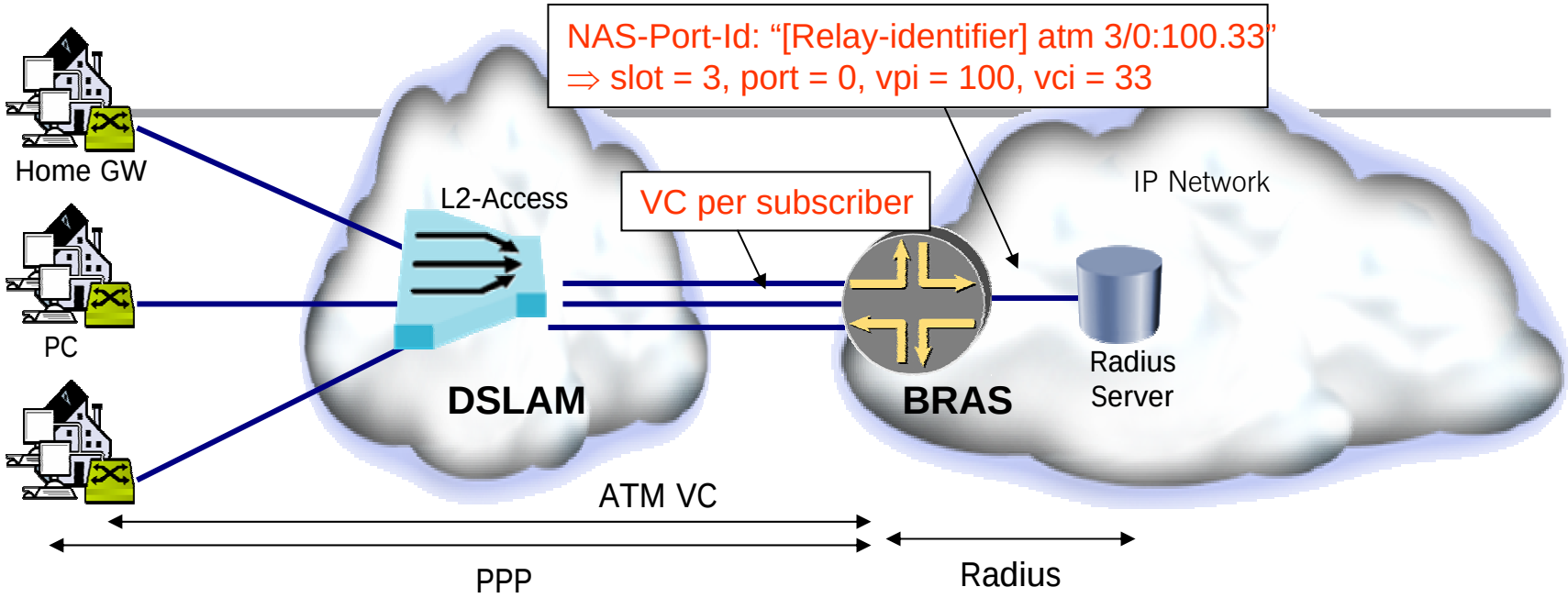
Use of DHCP Relay Agents and PPPoE Intermediate Agents for DSL line identification

Motivation & Concept

Problem statement

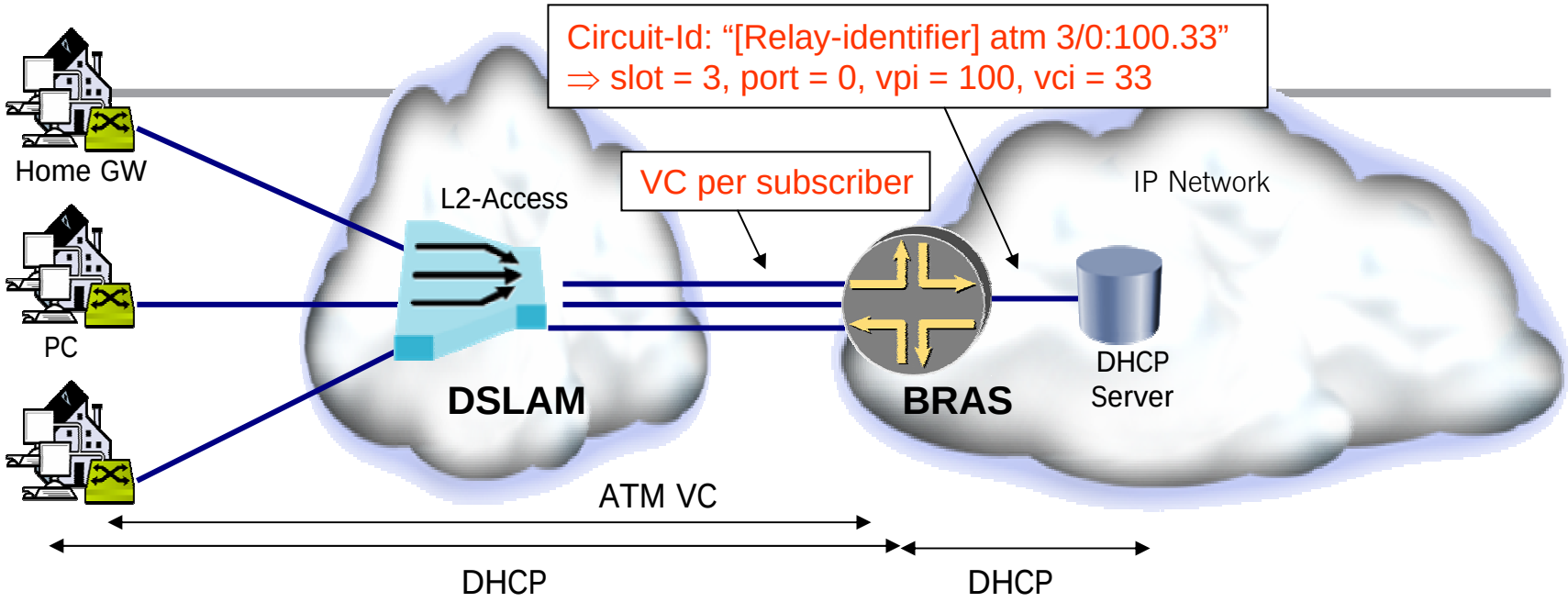
& Motivation

ATM/PPP: DSL Line identification



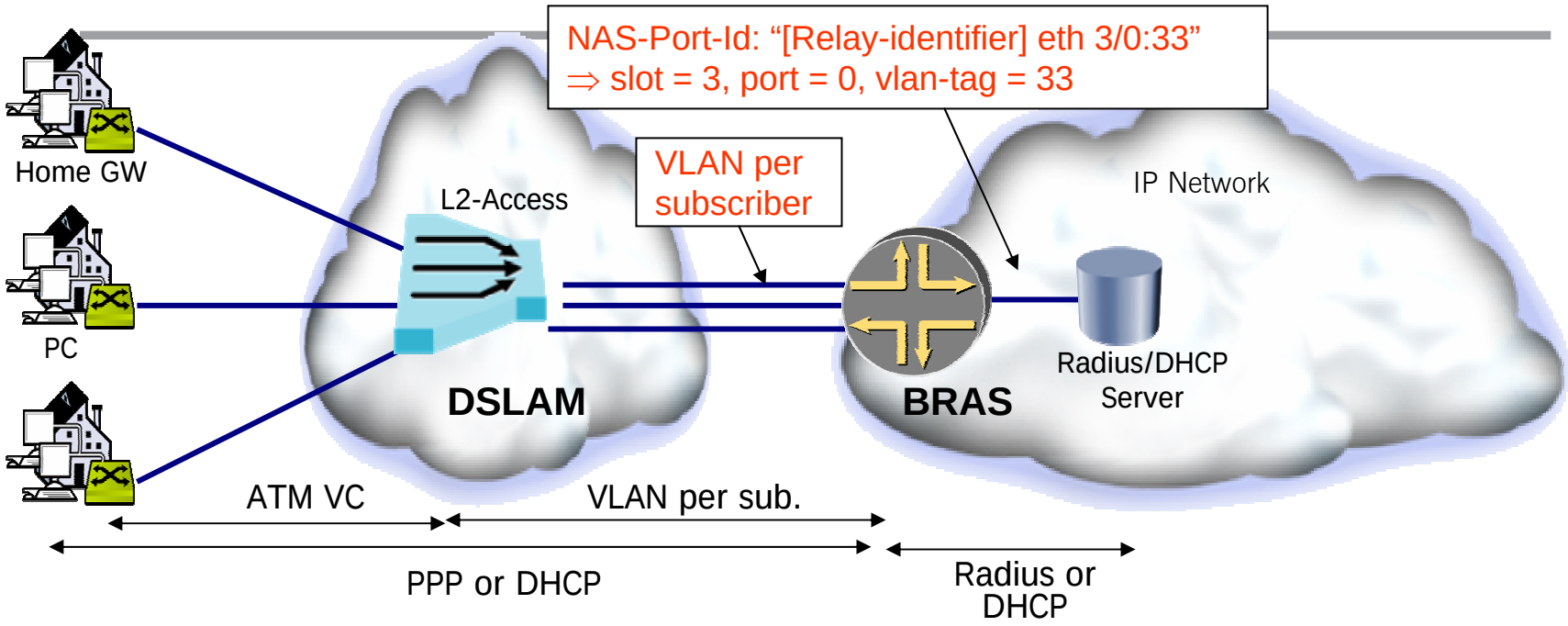
- The identification of the ATM VC is enough to figure out the DSL line.
- ATM VC and PPP are terminated on the BRAS, which acts as a Radius client
- BRAS inserts a Nas-Port-Id (or Nas-Port) in the Radius requests
- This enables DSL line identification for critical processes like port-based authentication as well as troubleshooting (via Radius logs).
- BRAS creates host route for client IP address

ATM/DHCP: DSL Line identification



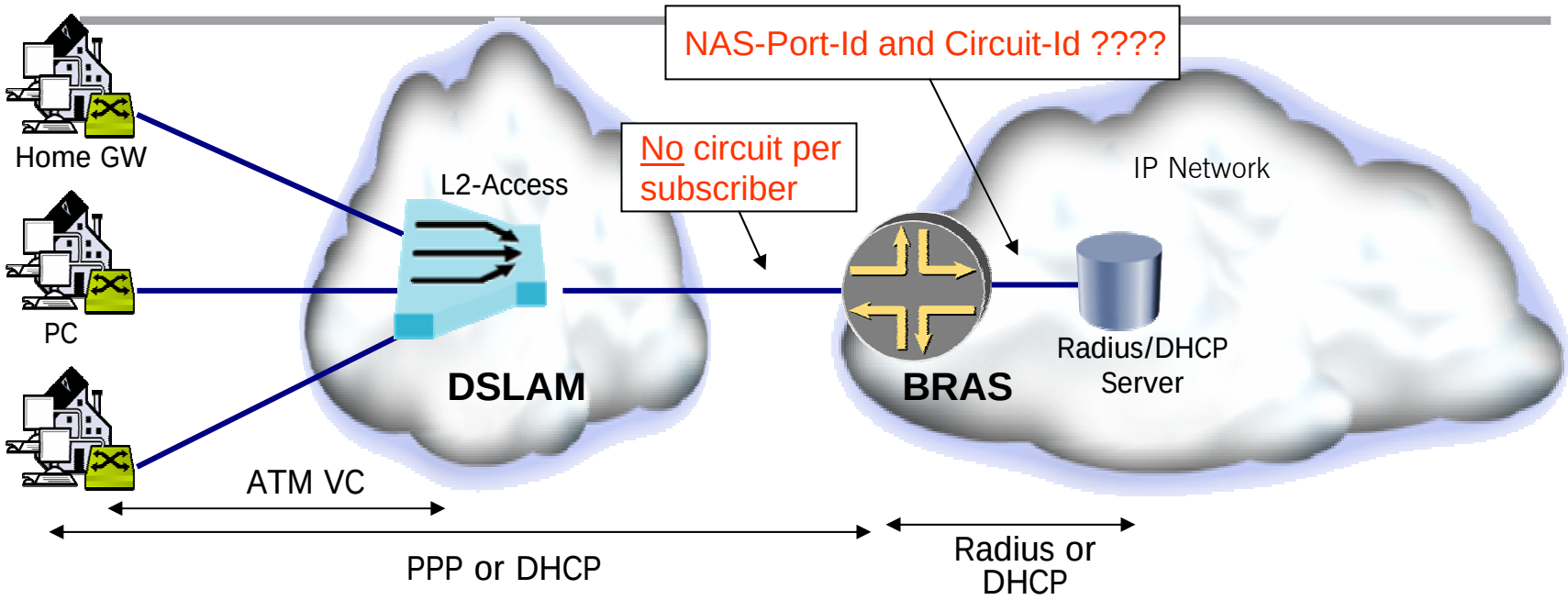
- The identification of the ATM VC is enough to figure out the DSL line.
- ATM VC is terminated on the BRAS, which acts as a DHCP Relay Agent
- BRAS inserts a Circuit-Id (option 82) in the DHCP Discover packet
- This enables DSL line identification for critical processes like port-based IP address assignment as well as troubleshooting (via DHCP logs).
- BRAS creates host route for client IP address

Eth/VLAN: DSL Line identification



- **Ethernet-based Access Network with one VLAN per subscriber**
- **VLAN stacking may be used to reflect two levels (~ VP/VC pair)**
- **VLANs terminated on the BRAS**
- **Then similar schemes apply (NAS-Port-Id / Circuit-Id will reflect the VLAN, hence the DSL-Line)**

Ethernet: DSL Line identification

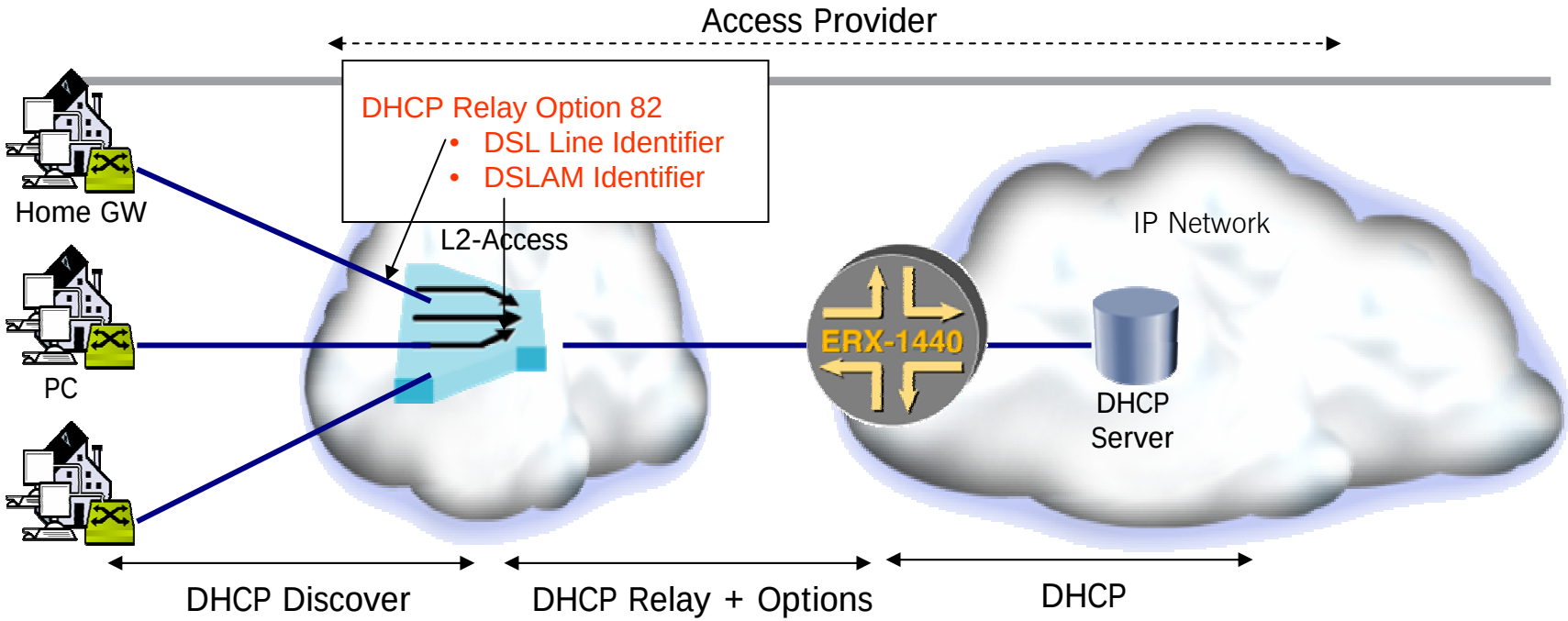


- Ethernet-based Access Network with no VLAN/Circuit per subscriber
- E.g. desire from access provider to simplify provisioning processes
- BRAS has no information about the DSL Line Identification…
- Radius and/or DHCP server will not get the information either
- **PROBLEM !**

Proposed solution

for DHCP scenario

DSL Line Parameter in DHCP



- **DSLAM knows the subscriber's DSL line**
- **DSLAM acts as a simplified DHCP Relay**
- **Simplified DHCP Relay inserts DSL line identifier and DSLAM identifier in DHCP Option 82 (Sub-option Agent Circuit ID). DHCP giaddr field is left unchanged.**
- **BRAS acts as regular DHCP-Relay, forwards DHCP packet to DHCP Server, processes DHCP responses, creates host route for client IP address**

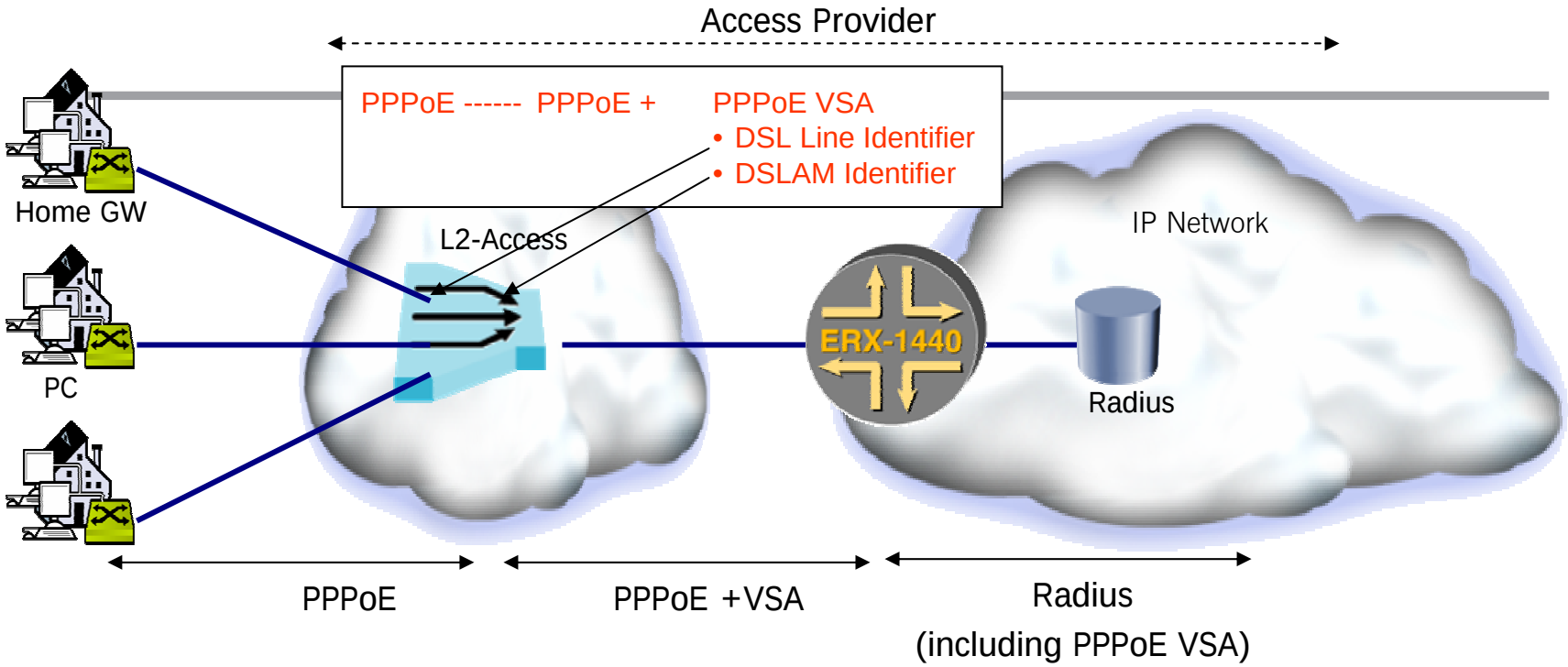
DSL Line Parameter in DHCP (cont'd)

- DHCP option 82 (RFC 3046) includes sub-options
  - Circuit-Id: [Relay-identifier] atm slot/port:vpi.vci
  - Remote-Id: logical identifier of the remote (e.g. configurable string)
- Acting as a simplified DHCP-Relay (no giaddr processing) allows to:
  - Simplify DSLAM processing
  - Avoid to create routes to send back DHCP messages to DSLAM
  - Keep the BRAS as a regular DHCP-Relay (cf. host routes)

Proposed solution

for PPPoE scenario

DSL Line Parameter in PPPoE



- **DSLAM knows the subscriber's DSL line**
- **DSLAM acts as a PPPoE Intermediate Agent**
- **PPPoE Intermediate Agent inserts DSL line identifier and DSLAM identifier in PPPoE VSA**
- **BRAS forwards PPPoE VSA information to Radius Server in NAS Port ID**

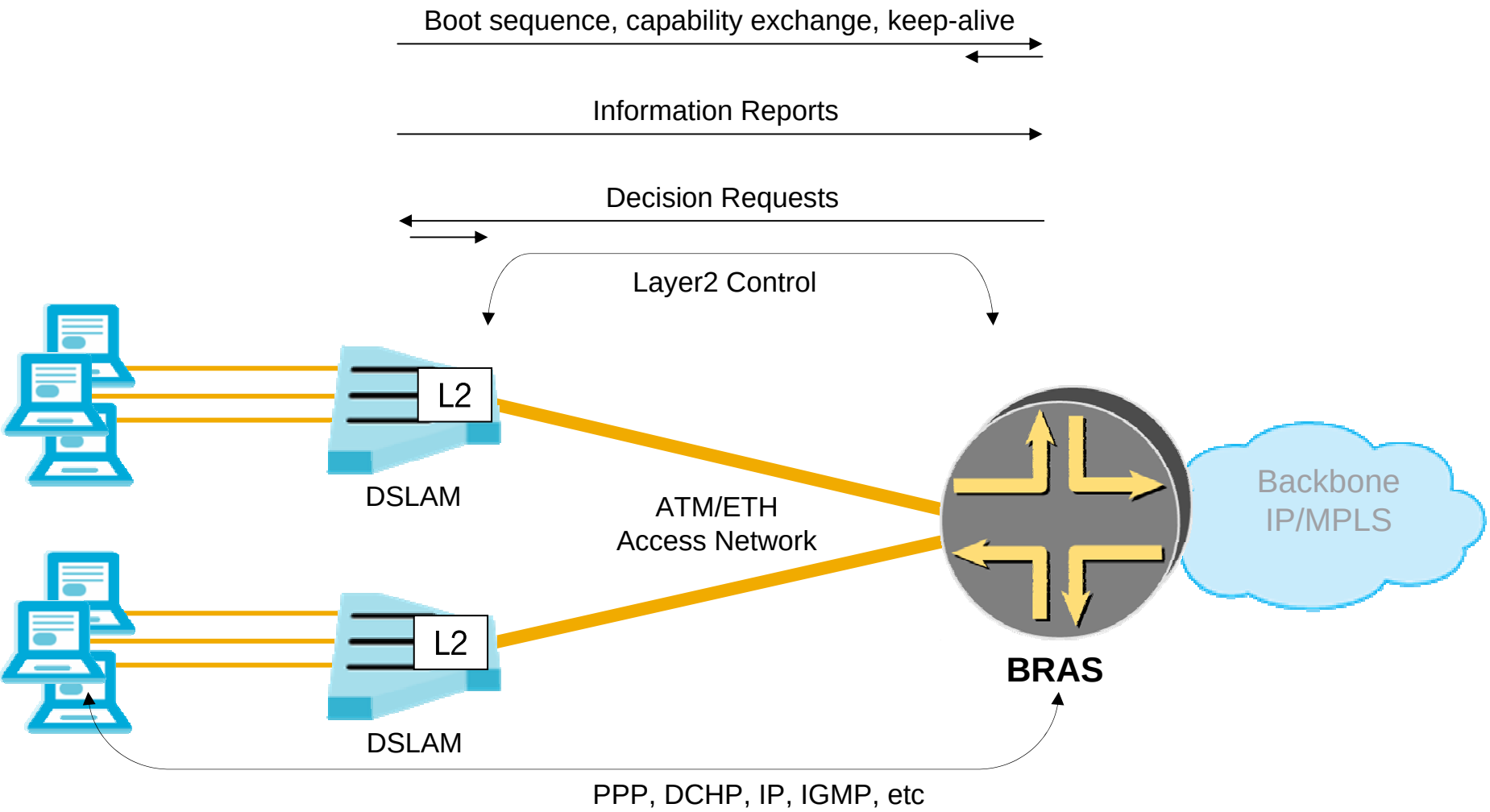
DSL Line Parameter in PPPoE (cont'd)

- PPPoE (RFC2516) is described by two stages and therefore by a specific ETH-Type
  - Discovery/negotiation (ETH-Type: 0x8863)
  - PPP Payload (ETH-type: 0x8864)
- PPPoE Intermediate Agent is interested in the Discovery (more specific in PADR) stage to append DSL line information in PPPoE VSA
- PPPoE PADR
  - ETH-Type == 0x8863
  - Destination Address == BRAS MAC address
  - Code Field == 0x19
- Vendor-specific Attributes/Information == 0x0105
  - Same encoding as DHCP option 82 (sub-options as TLVs, circuit-id)

Layer 2 Control Mechanism

Motivation & Concept

Concept of L2 Control Channel



Optimization of multicast traffic between BRAS and DSLAM

DSL Forum 2003 - 367

Multicast: business incentive

- DSL needs to be competitive with cable (triple-play)
- Many DSL Service Providers want to deliver multimedia services implying the use of multicast technology:
  - IP-TV
  - Near Video-On-Demand
  - IP Radio
  - Broadcast of special events (e.g. sports – world cup, …)
- If so, it must be performed in an economical way (capex and opex), respecting domain boundaries

➔ **Business Case remains CHALLENGING**

Issues with Video (Multicast)

- **ADSL speeds may be limited to only 1 or 2 concurrent video (multicast) channels, but VDSL is definitely not**
- **Multicast packet replication at BRAS with 2.5Mbps stream**

	1 MC Stream/ Household	2 MC Streams/ Household	3 MC Streams/ Household
Households* per OC-3 (ADSL)	50	25	N/a
Households* per OC-3 (VDSL)	50	25	12

*** ...US average: 2.5 TV's per household**

- **Also, distributing the content to the majority of remote locations (CO's) and the "injection" of IP traffic at those locations suffer from significant CAPEX and OPEX issues**

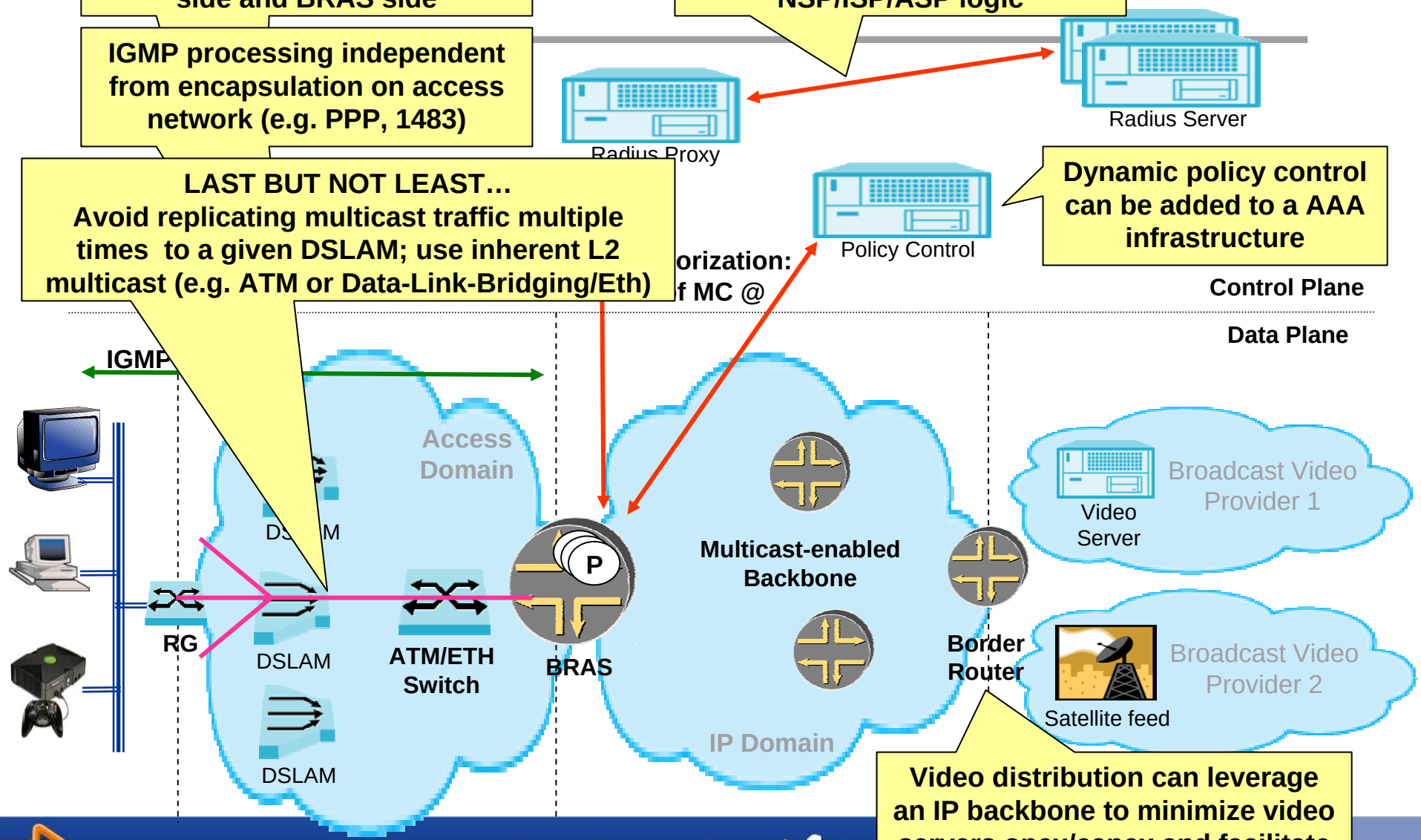
s fo

No complex OSS integration for subscriber & service management between DSLAM side and BRAS side

Authentication & Authorization leverages on existing Radius infrastructure, facilitating an NSP/ISP/ASP logic

IGMP processing independent from encapsulation on access network (e.g. PPP, 1483)

LAST BUT NOT LEAST…
Avoid replicating multicast traffic multiple times to a given DSLAM; use inherent L2 multicast (e.g. ATM or Data-Link-Bridging/Eth)

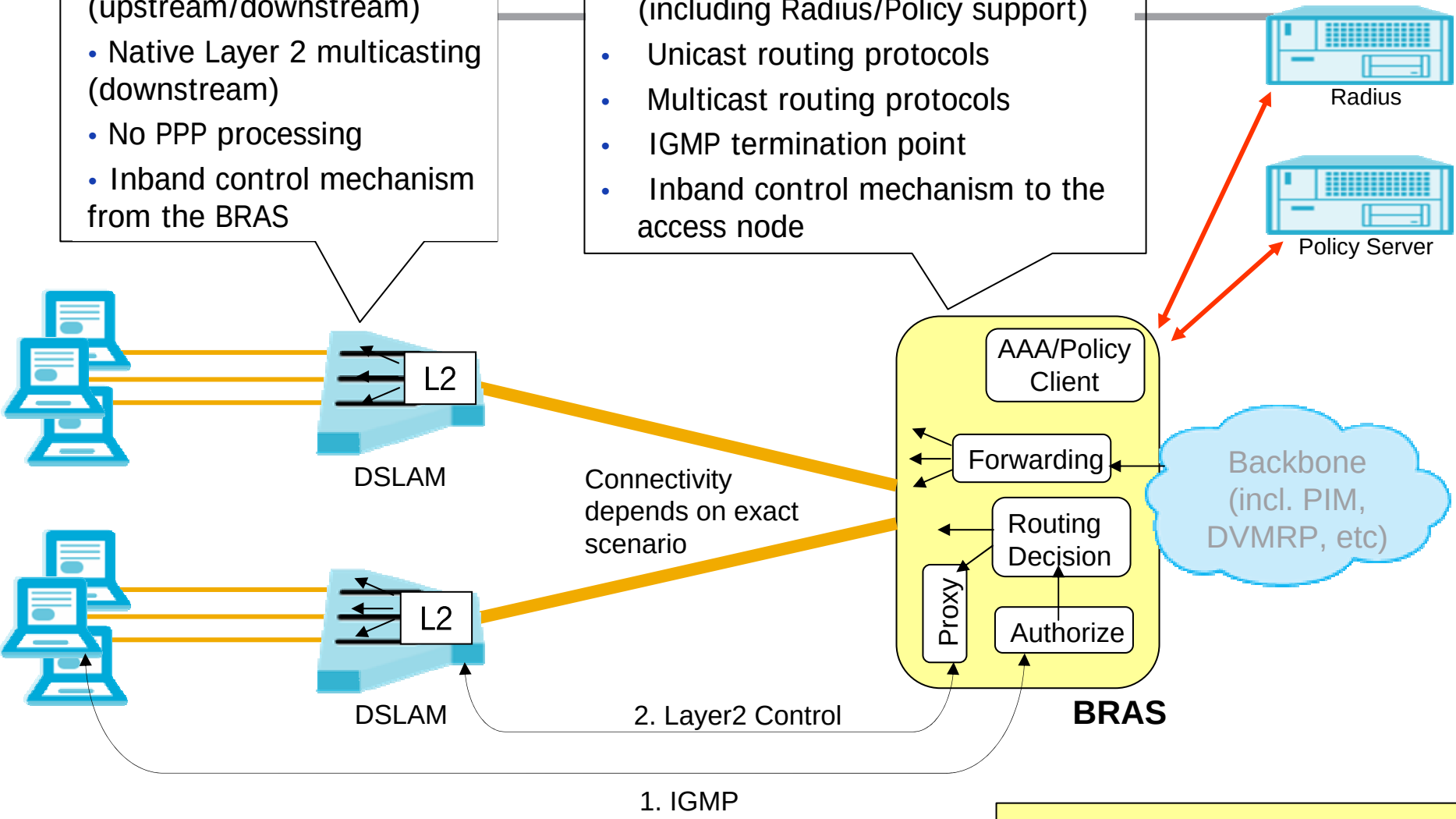


Video distribution can leverage an IP backbone to minimize video servers opex/capex and facilitate an NSP/ASP logic

Applicability to Multicast (1)

- Native Layer 2 forwarding (upstream/downstream)
- Native Layer 2 multicasting (downstream)
- No PPP processing
- Inband control mechanism from the BRAS

- BRAS/Subscriber management (including Radius/Policy support)
- Unicast routing protocols
- Multicast routing protocols
- IGMP termination point
- Inband control mechanism to the access node

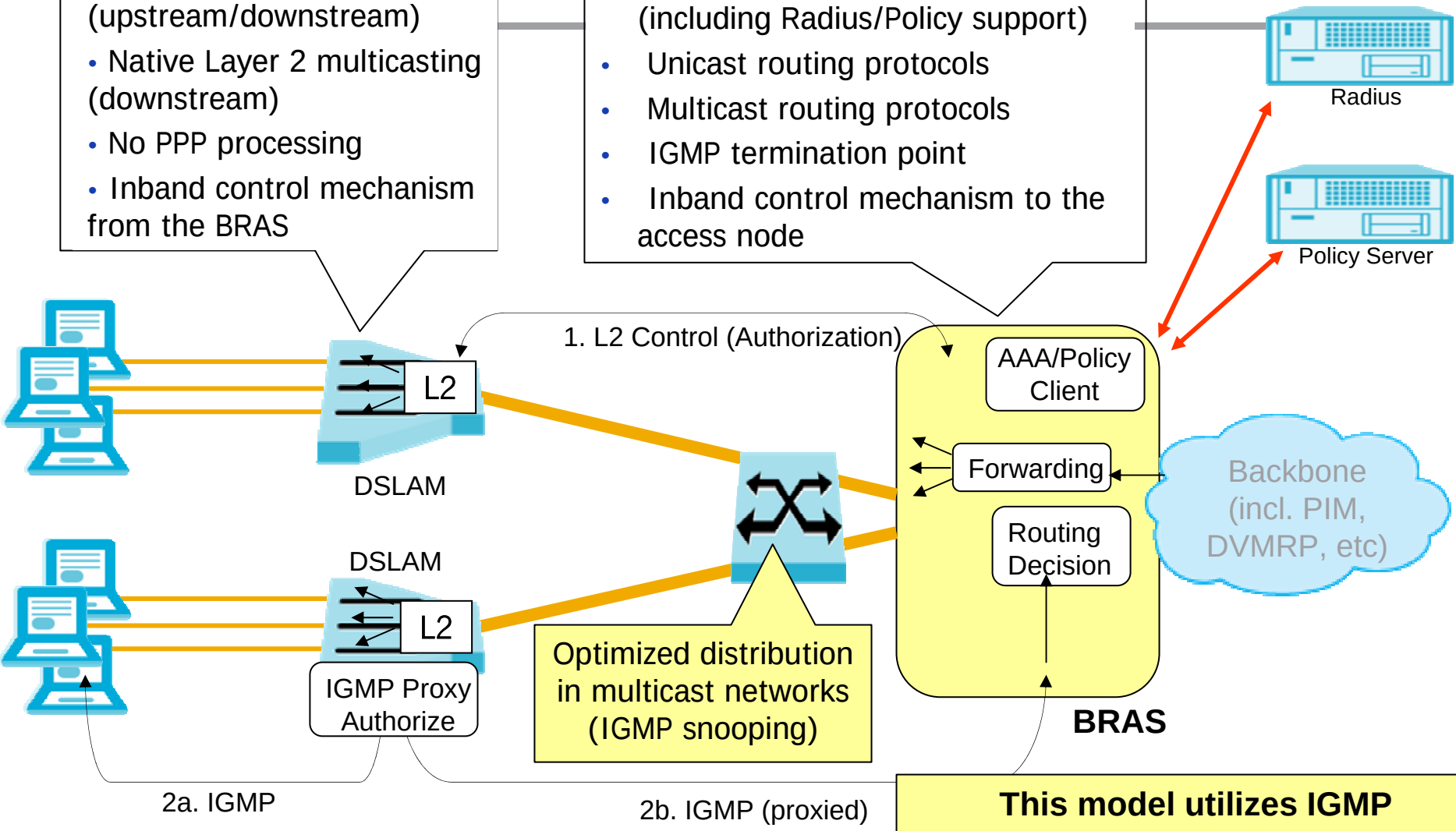


This model doesn't require any IGMP processing in the access node (e.g. DSLAM).

Applicability to Multicast (2)

- Native Layer 2 forwarding (upstream/downstream)
- Native Layer 2 multicasting (downstream)
- No PPP processing
- Inband control mechanism from the BRAS

- BRAS/Subscriber management (including Radius/Policy support)
- Unicast routing protocols
- Multicast routing protocols
- IGMP termination point
- Inband control mechanism to the access node



This model utilizes IGMP awareness in DSLAM and access network; this is an extension of the FS-VDSL model (TR-056, chapter 8)

Access Network topology discovery and line configuration

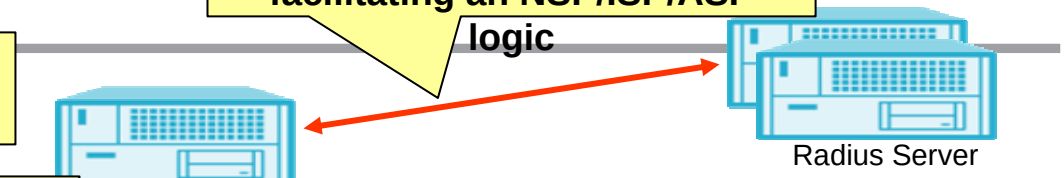
DSL Forum 2003 - 368

s fo

1b. No complex OSS integration for discovering/updating access network topology & capacity

2b. Authentication & Authorization leverages on existing Radius infrastructure, facilitating an NSP/ISP/ASP logic

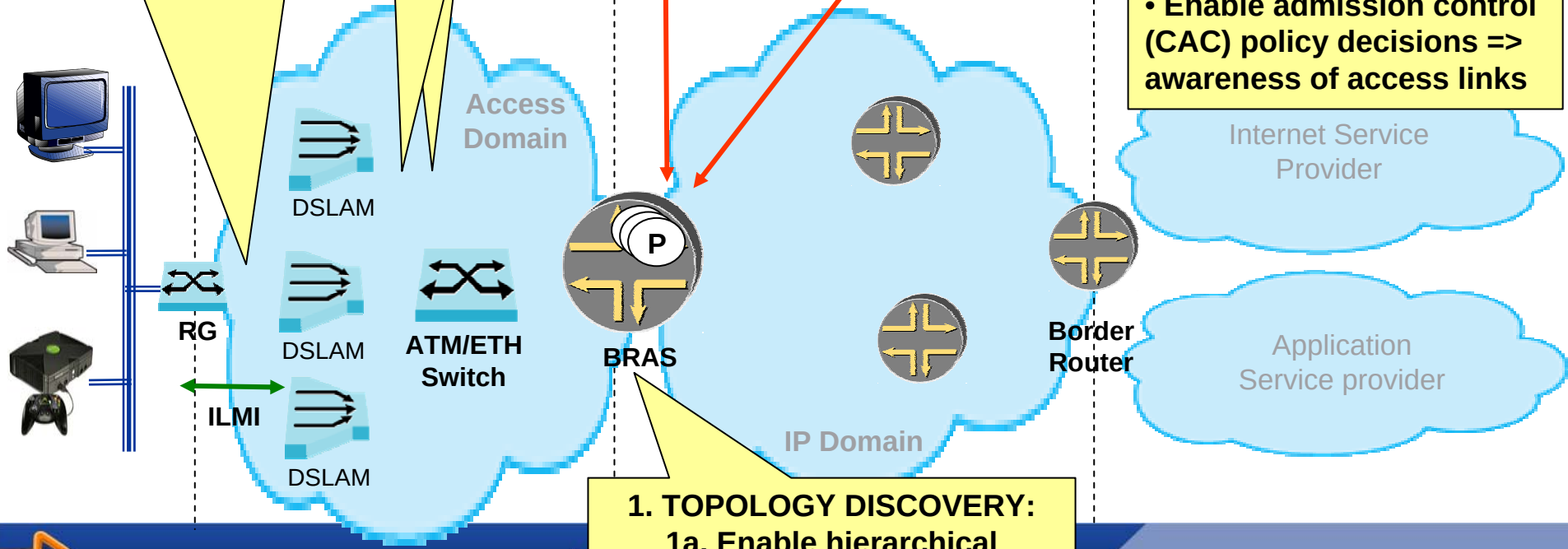
1c. Account for dynamic changes (e.g. DSL sync rate)



2. LINE CONFIGURATION:
2a. Allow DSL line service parameters to automatically come from service/subscriber management logic (e.g. DSL checksum, max-speed).

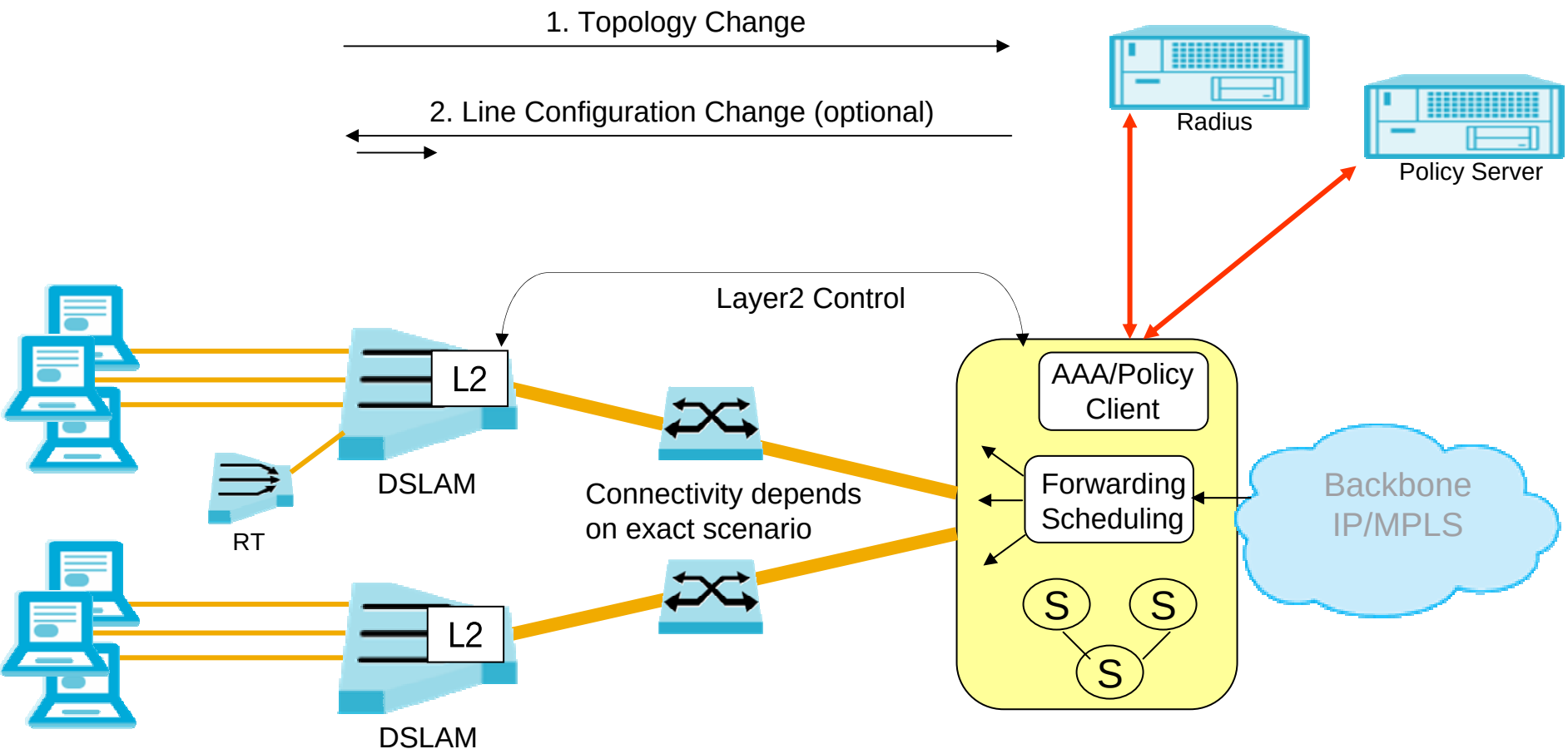
Authorization Data

BOTH TOPICS:
3. Optional policy control
• Enable dynamic policy reconfiguration (e.g. on-demand service model)
• Enable admission control (CAC) policy decisions => awareness of access links



1. TOPOLOGY DISCOVERY:
1a. Enable hierarchical weighted queuing and network constraints enforcement

Applicability to Topology Discovery and Line Configuration



QoS for Broadband Services

Juniper NETWORKS™

Why Hierarchical Scheduling

Hierarchical scheduling eliminates congestion/queuing downstream of the BRAS.

No congestion means access can be pre-provisioned, the BRAS is final and exclusive arbiter of access QoS.

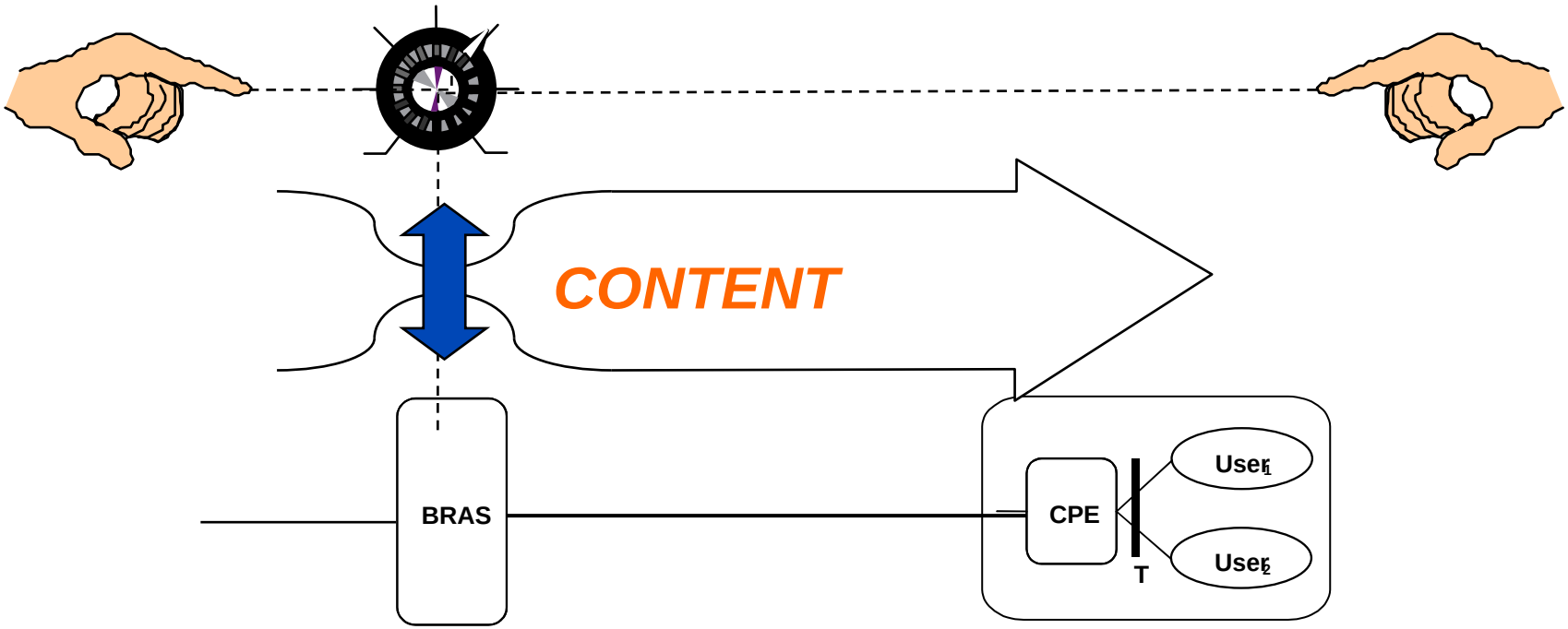
- *no further coordination of downstream NEs required*

Three steps:

- Arbitrate between flows within a session …*enabling*
- Arbitrate between sessions on a common loop…*enabling*
- Arbitrate between loops across the access build…*retrofitting*

Phase 1 QoS

The “Turbo” button *(bandwidth on demand)*

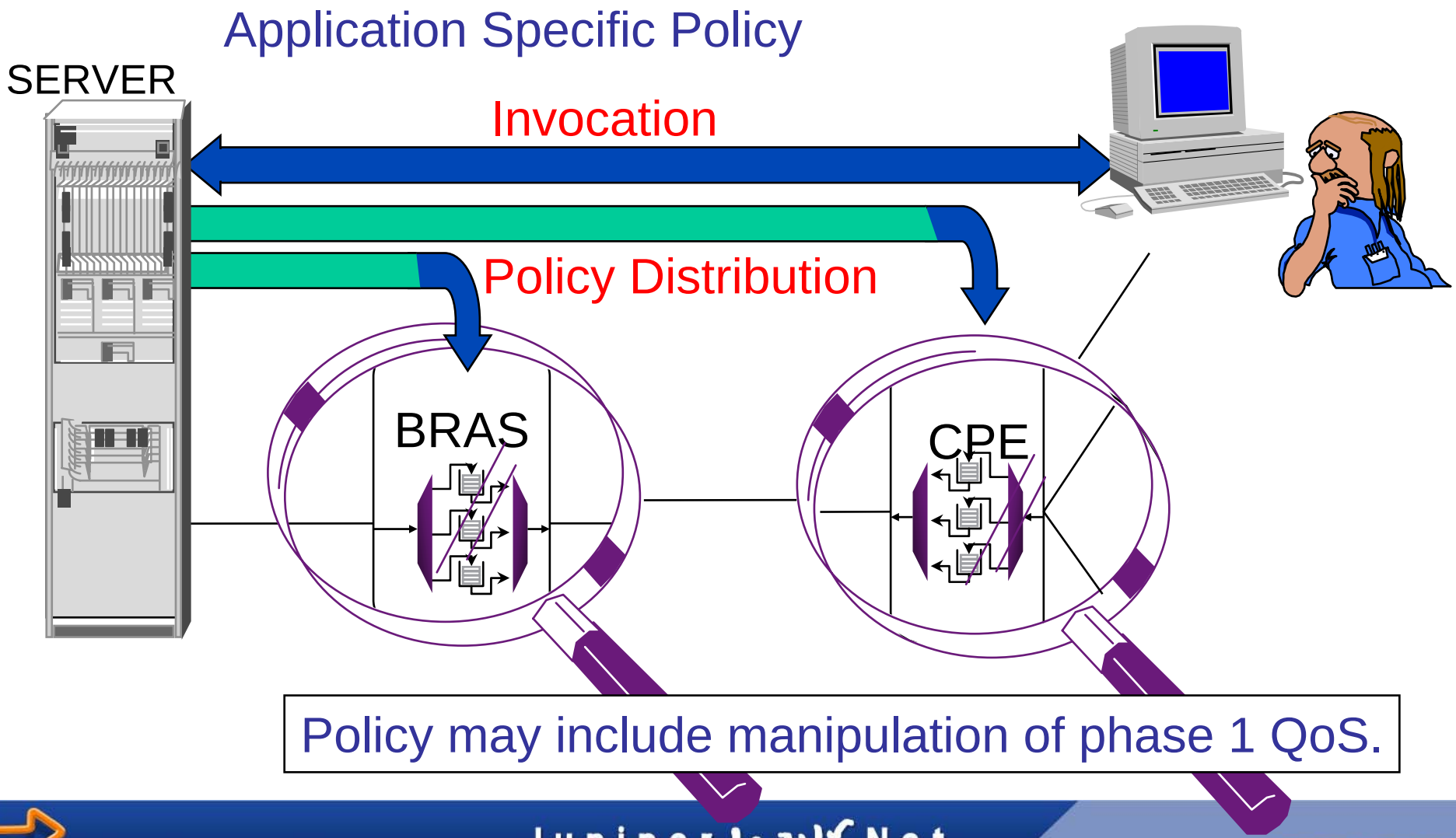


User *or* ASP can modify available bandwidth.

BRAS modifies per session shaping/scheduling

manages service assurance, generates billing records

Phase 2 QoS



TR-059 Content

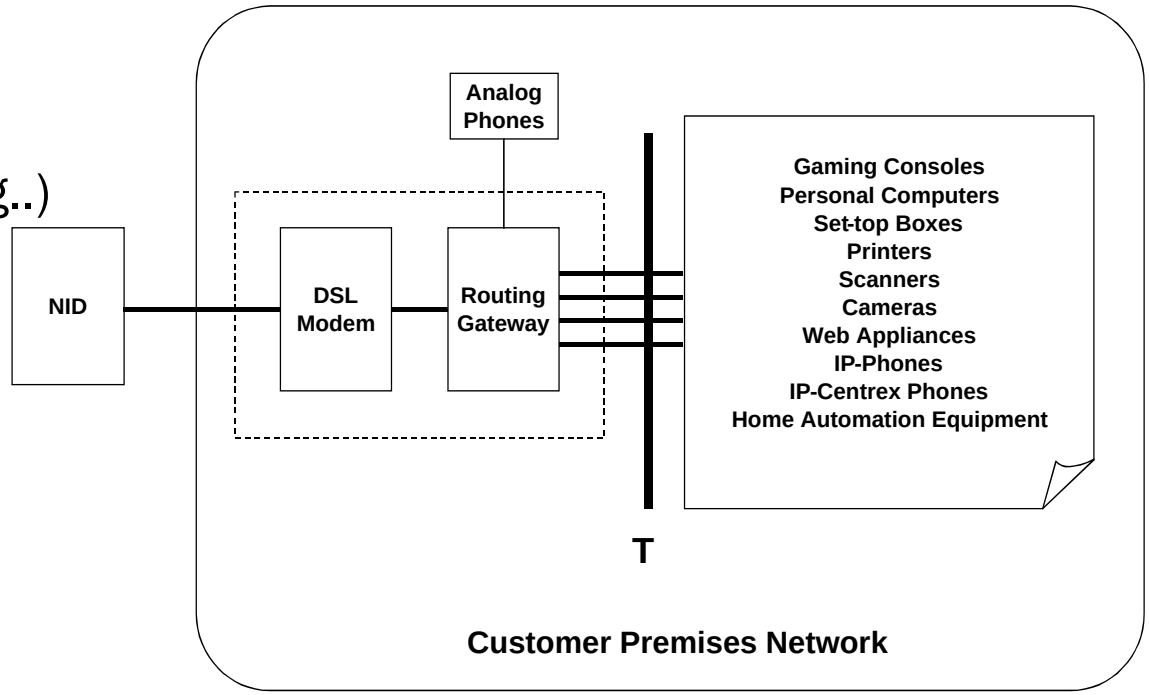
Some Requirements for the BRAS

- MUST
  - PPP, Bridged Ethernet, RADIUS, L2TP, DHCP, Multi-VC
  - Bandwidth management (ATM, PPP, Ethernet, IP), IP QoS Marking, Per Subscriber Policing, Queuing and Prioritization per Flow
  - Traffic Engineering for ATM, MPLS and Ethernet
  - DiffServ aware Hierarchical Scheduler “that allows to manage the network so that any potential congestion in the Access Network between the BRAS and the RGs is avoided”
  - Shaping of Subscriber Aggregated Traffic (to a lower value than DSL Sync Rate)
  - RED/WRED
- SHOULD
  - Multiple ATM Categories, VP/VC Cross Connection
- MAY
  - Multicast
  - Ethernet interface for Local Content

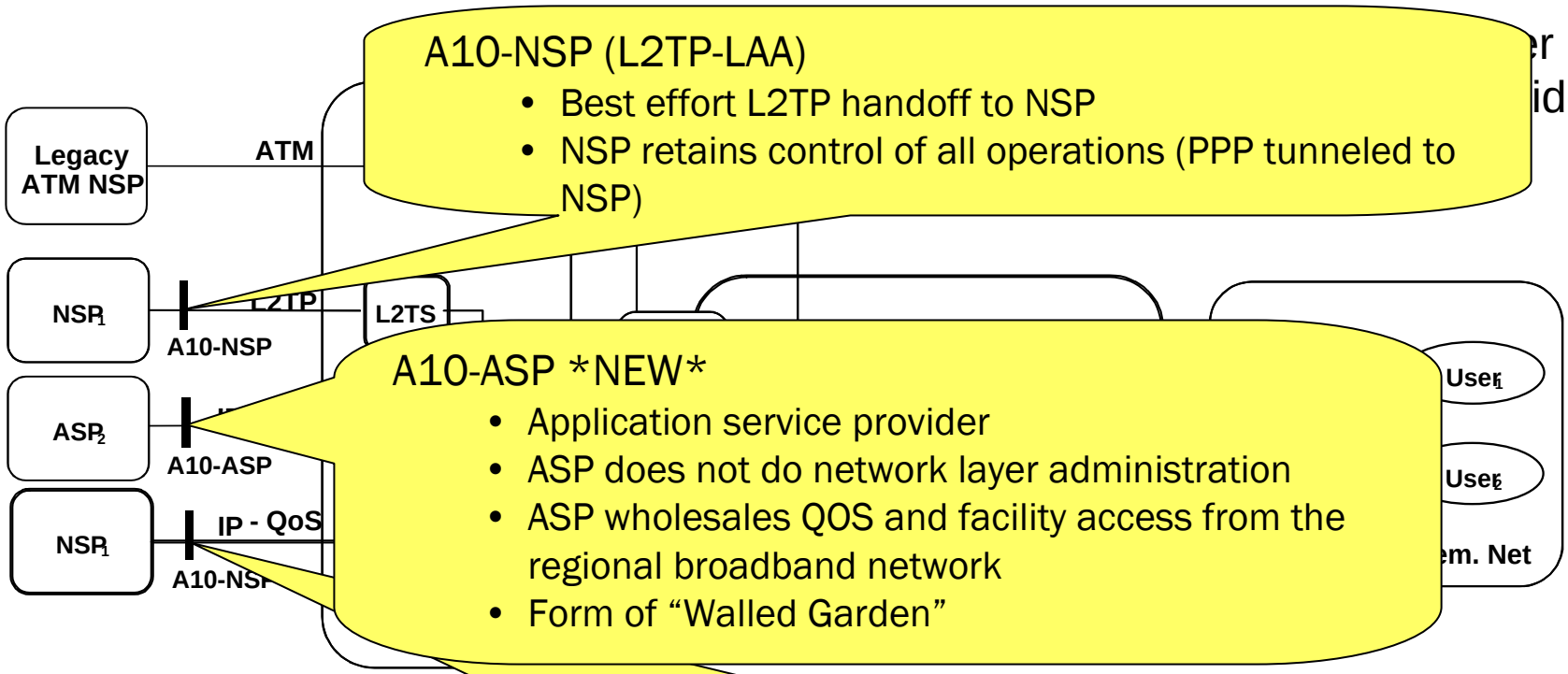
TR-059 Content (cont'd)

RG = Routing Gateway (beyond DSL Modem)

- NAPT, Firewall (H.323, SIP, IPSec)
- Local DHCP
- MTU Negotiation
- QoS (remarking, queuing..)
- Fragmentation (MLPPP)
- IPv6 (optional)



Working Model



Edge Router QOS

Overview

Edge Router Forwarding: Policy

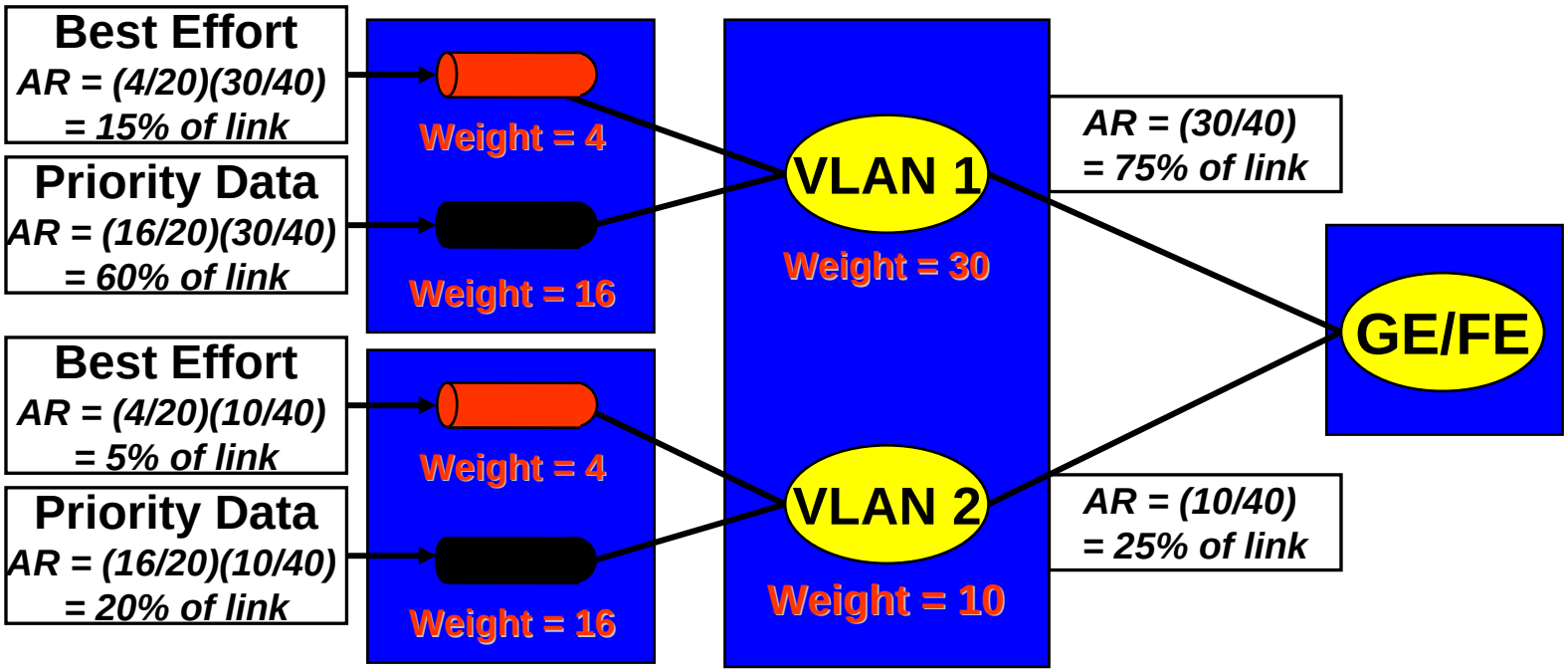
- IP Policy
  - ToS or MF Classification into *Flows*
  - Per flow actions: policing, ToS stamping
  - Setting drop precedence(color) and Traffic Class
- Non-IP policy
  - Classification & stamping based on (802.1p, MPLS EXP)
  - Policing
- Done both ingress and again on egress interfaces

Edge Router Forwarding: QoS

- HRR: Hierarchical Round Robin scheduler
- 64,000 queues per LC, 8 queues per subscriber
- SCBQ: Subscriber Class Based Queuing
- Features
  - Strict Priority
  - Rate Shaping
  - Weighted scheduling(WRR)
- Integrated with ATM SAR

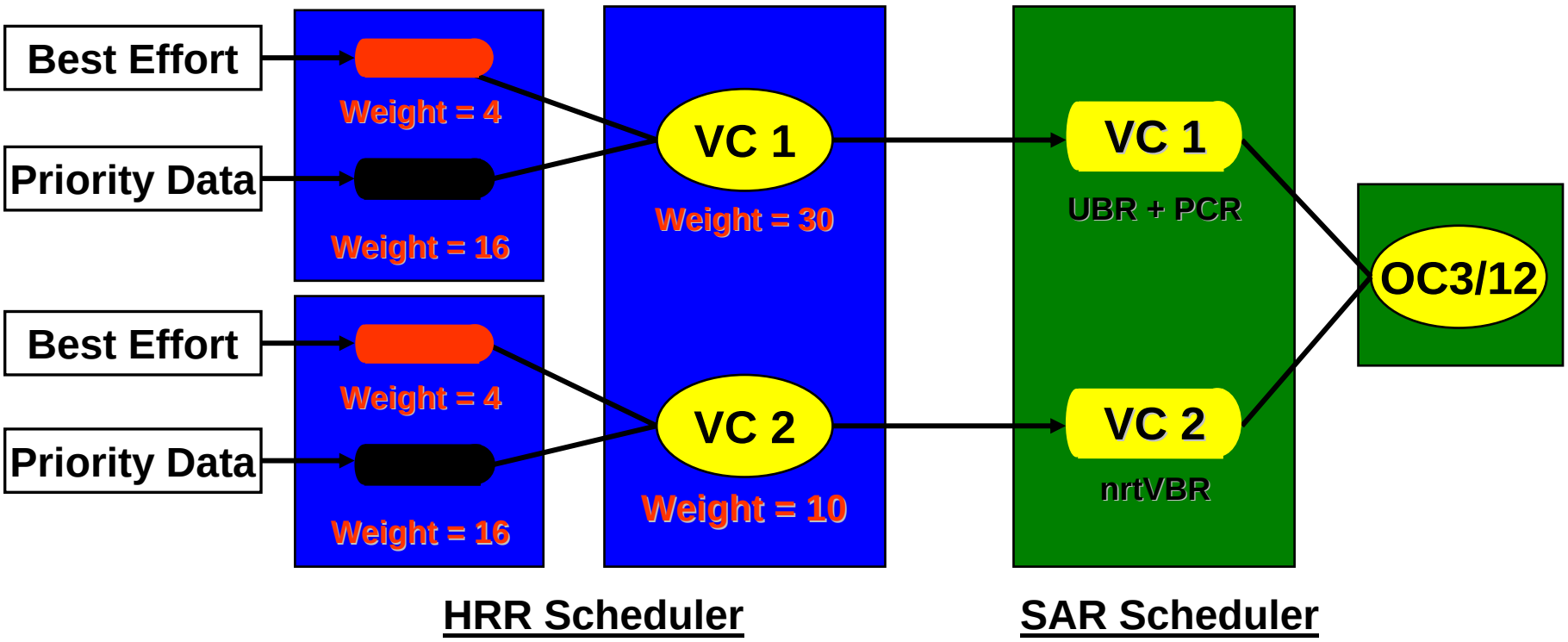
VLAN Scheduling

- Per VLAN bandwidth allocation (based on weights)
- Within VLAN, per Traffic Class bandwidth



VC Scheduling

- Same HRR scheduler as on Ethernet
- Integrated with SAR

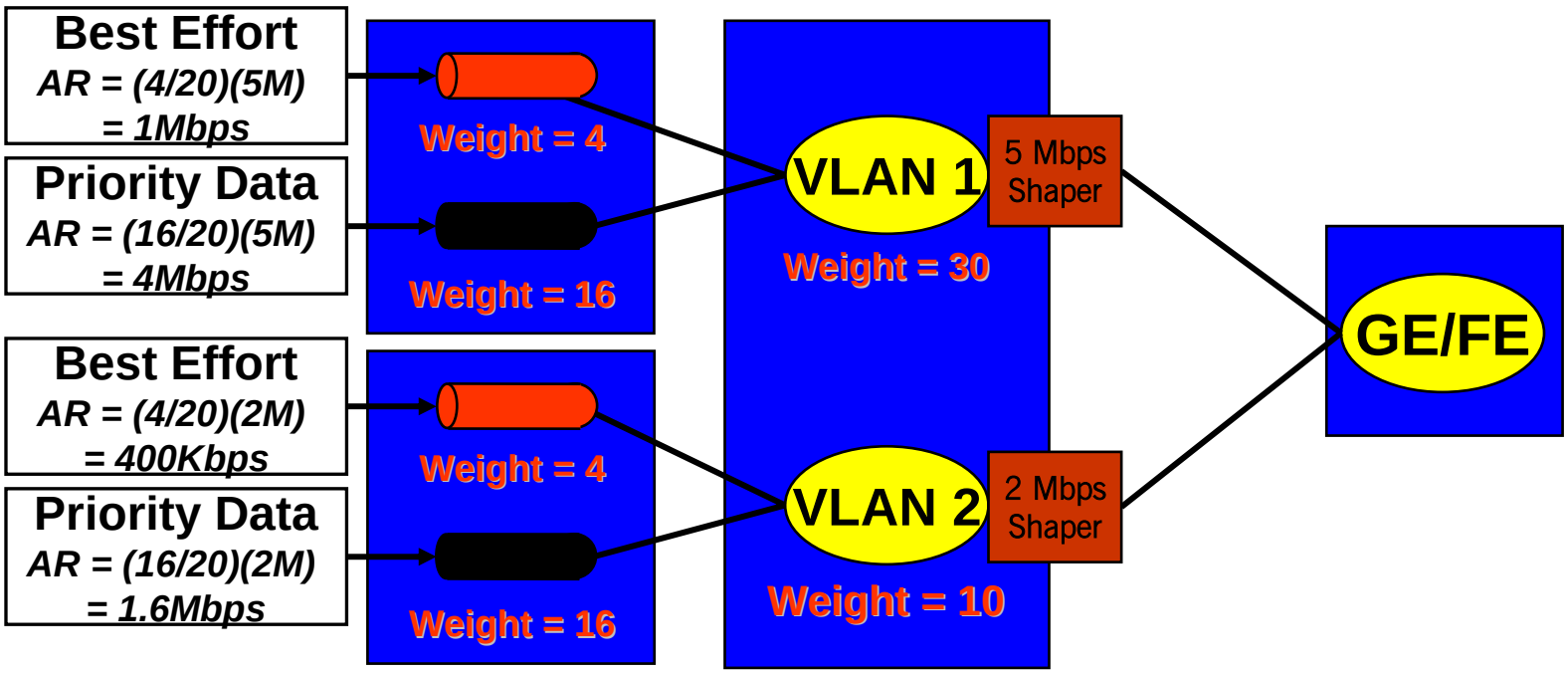


HRR / ATM Integration

- HRR has 32MB packet buffer, SAR has another 32MB
- VC Backpressure : per VC XON/XOFF from SAR to HRR
- Without it, HRR would drain into SAR at 1Gbps
- SAR backpressure controls how HRR & SAR work in tandem
  - Backpressure pushes bytes into one or the other scheduler
  - Scheduler that owns the buffered bytes *tends* to dominate
  - Backpressure is user configurable

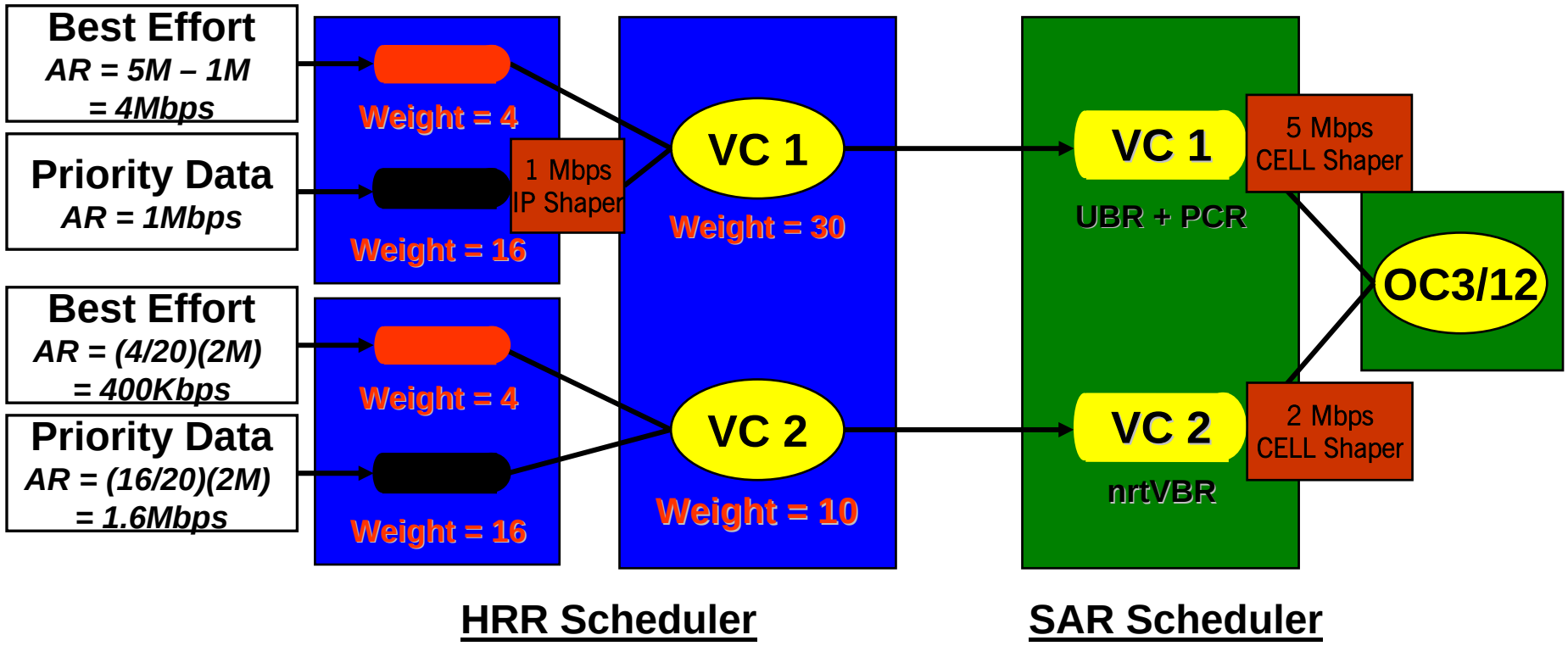
VLAN Shaping

- Weights allocate *minimum* rate (under congestion)
- Shaping rate caps the node/queue at a *maximum* rate



VC Shaping

- Same HRR scheduler as on Ethernet
- Integrated with SAR



HRR / ATM Integration Modes

1. Default Integrated Mode
   - VC backpressure enabled for data, NOT for Voice and Video
   - Least radical approach
2. Low-latency Mode
   - VC backpressure and SAR disabled
   - Per-packet cell bursting – not for policed ATM networks
3. Low-CDV Mode
   - VC backpressure disabled, but HRR and SAR shaping at same rate
   - Good for VP-based scheduling

IPv6 over Broadband Networks

PPP and Non-PPP Service Models

IPv6 over Broadband Services – Target Market and Service Requirements

- Carriers in APAC – Japan in particular - want to run IPv6 across their broadband networks
- NTT Com, ACCA, KDDI etc in Japan are running or trialling PPP based IPv4 and IPv6 “Dual Stack” BRAS
- NTT East / West / SI Labs is building a whole new nationwide network and they want Non-PPP based services.

Background - IPv4 BRAS Service Models

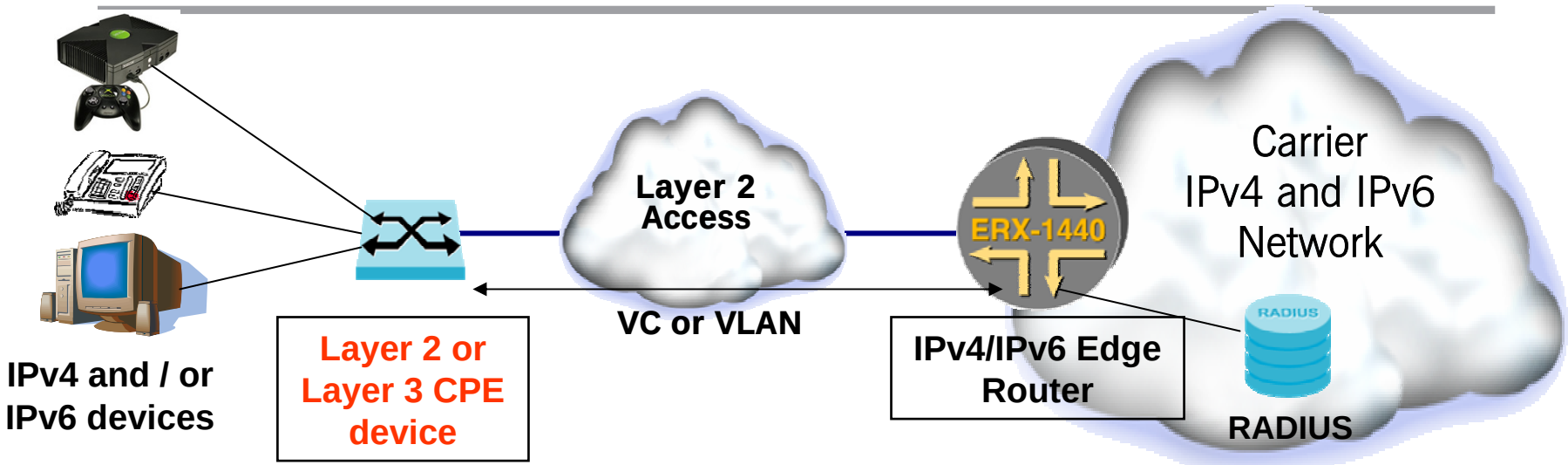
- PPP-based model
- Requires PPPoE client software or CPE device
- Session based service model
- User authentication & accounting information present
- Radius based AAA
- Leverages LCP and IPCP protocols

- Non PPP-based model
- Business services
  - Bridged / Routed 1483 services (Business broadband)
- Subscriber Services
  - DHCP based broadband remote access
  - Good for lightweight clients
  - Requires many add-ins to DHCP to allow AAA, session monitoring, accounting, etc etc etc etc....

Technical Service Details

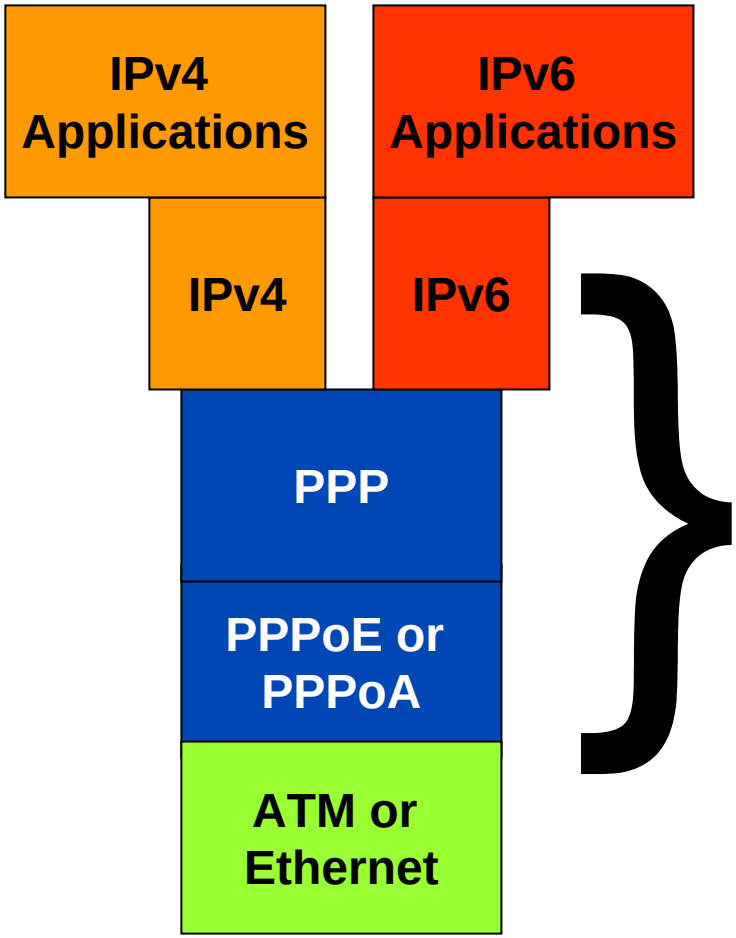
- PPP-Based Services
- Non PPP-Based Services

The PPP-Based IPv4/IPv6 Service Model



Simultaneous Support for IPv4 and IPv6 traffic over a single PPP connection

Dual Stack BRAS - protocols



- Based on PPP(oX)
- One PPP Session
- Two Layer 3 Protocols

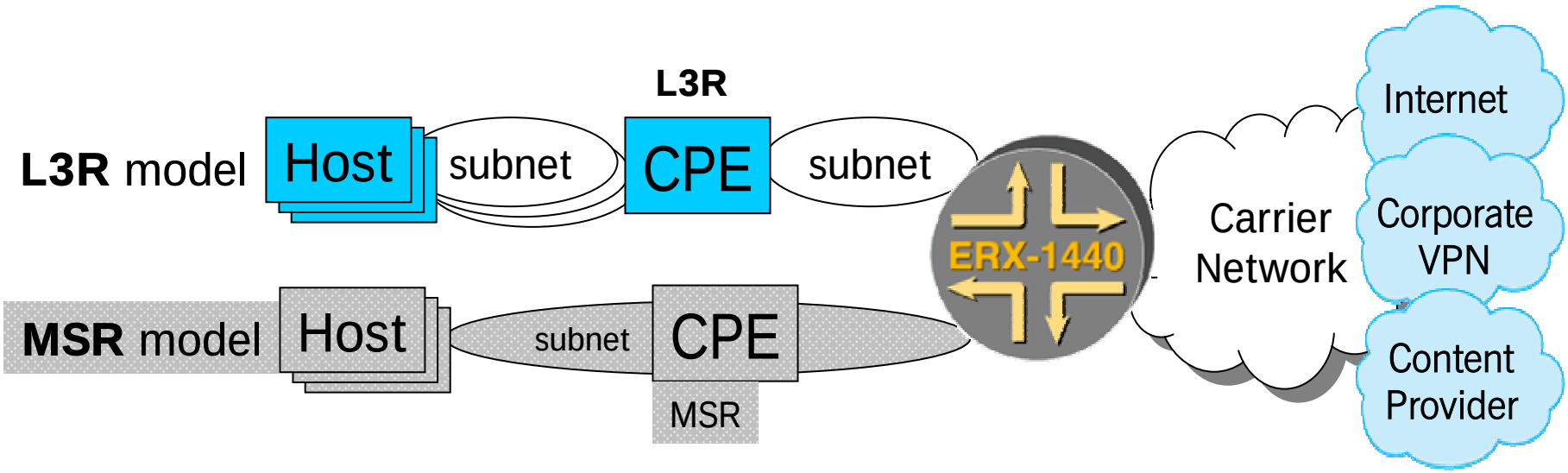
IPv4 Connection Setup

- Based on PPP & IP Protocols
  - LCP used for :
    - user authentication
    - connection establishment
    - connection maintenance / monitoring
    - etc
  - NCP - IPCP used for
    - IP address assignment – Local pools or Radius
    - DNS Server addresses, etc
    - etc

The PPP Based "Dual Stack" Models

- Defined in : draft-shirasaki-dualstack-service-01.txt
- Two models defined but only 1 implemented so far :

Model	CPE type	Subnet	Site Prefix	Notes
L3R Model	L3 Router	leaf subnets	/48, /64	Today's solution
MSR Model	Multi-link subnet Router	one subnet	/64	*Not currently implemented*



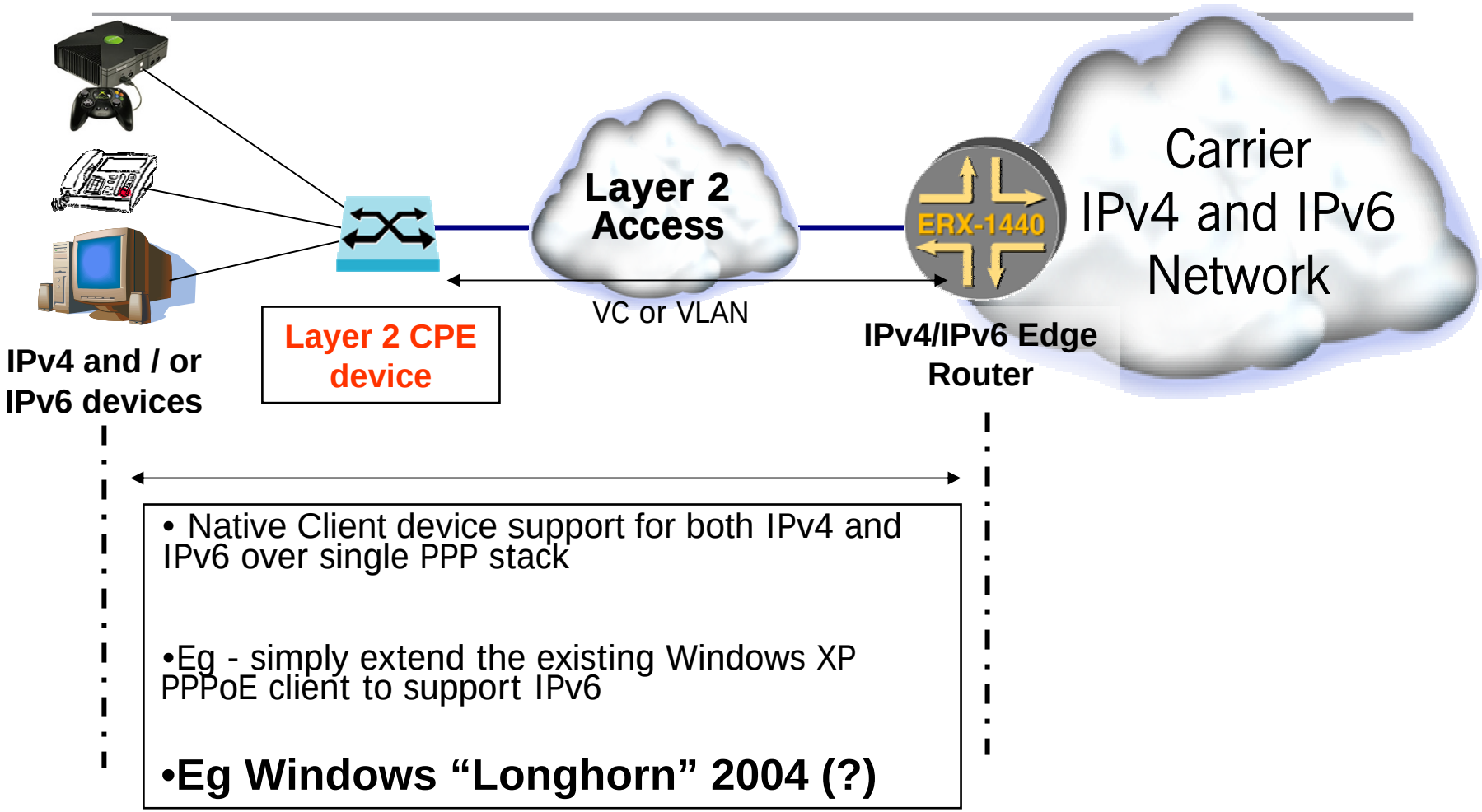
IPv6 Connection Setup

- Based on :
  - draft-shirasaki-dualstack-service-01.txt which references :
  - draft-ietf-dhc-dhcp6-26.txt
    - Use is made of DHCPv6 messages
  - draft-troan-dhcpv6-opt-prefix-delegation-01.txt
    - Assigns IPv6 Prefixes (eg /48) from Edge Router to CPE
  - draft-ietf-dhc-dhcpv6-opt-dnsconfig-03
    - Assigns IPv6 DNS server addresses to CPE

Notes about IPv6 Connection setup:

- LCP stuff (eg User Authentication) done once during connection setup
- NCP – IPv6CP used only for exchange of Link-Local addresses - not very useful
- Specifications are Internet Drafts but becoming RFCs shortly
- Specifications and Edge Router functionality will be updated as needed when these Internet Drafts become RFCs

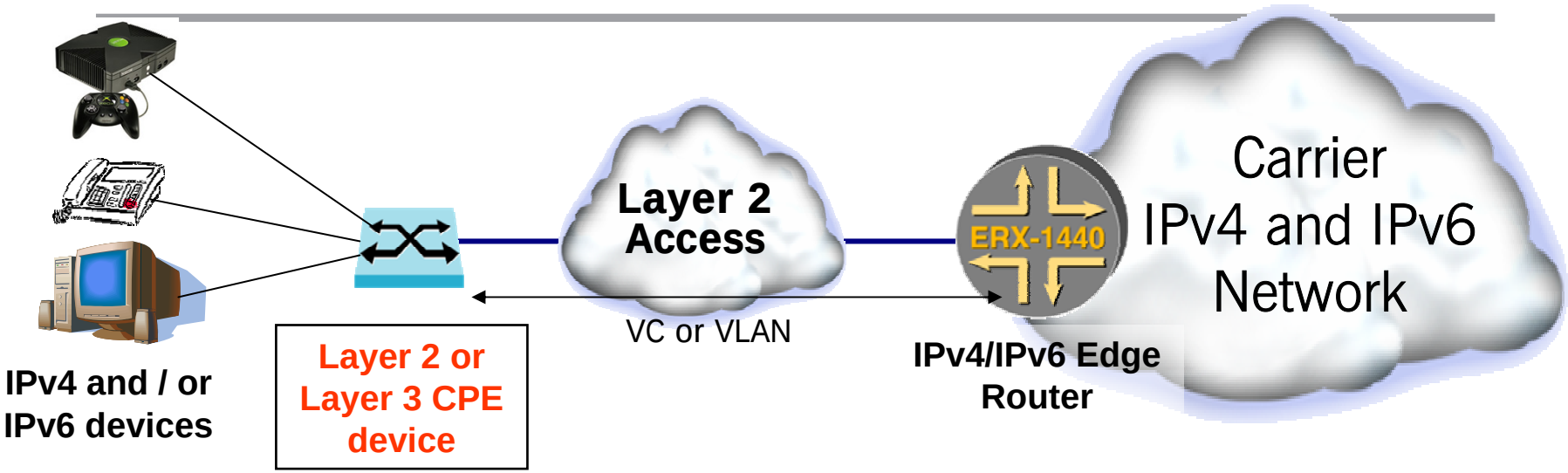
Futures of the PPP model



Technical Service Details

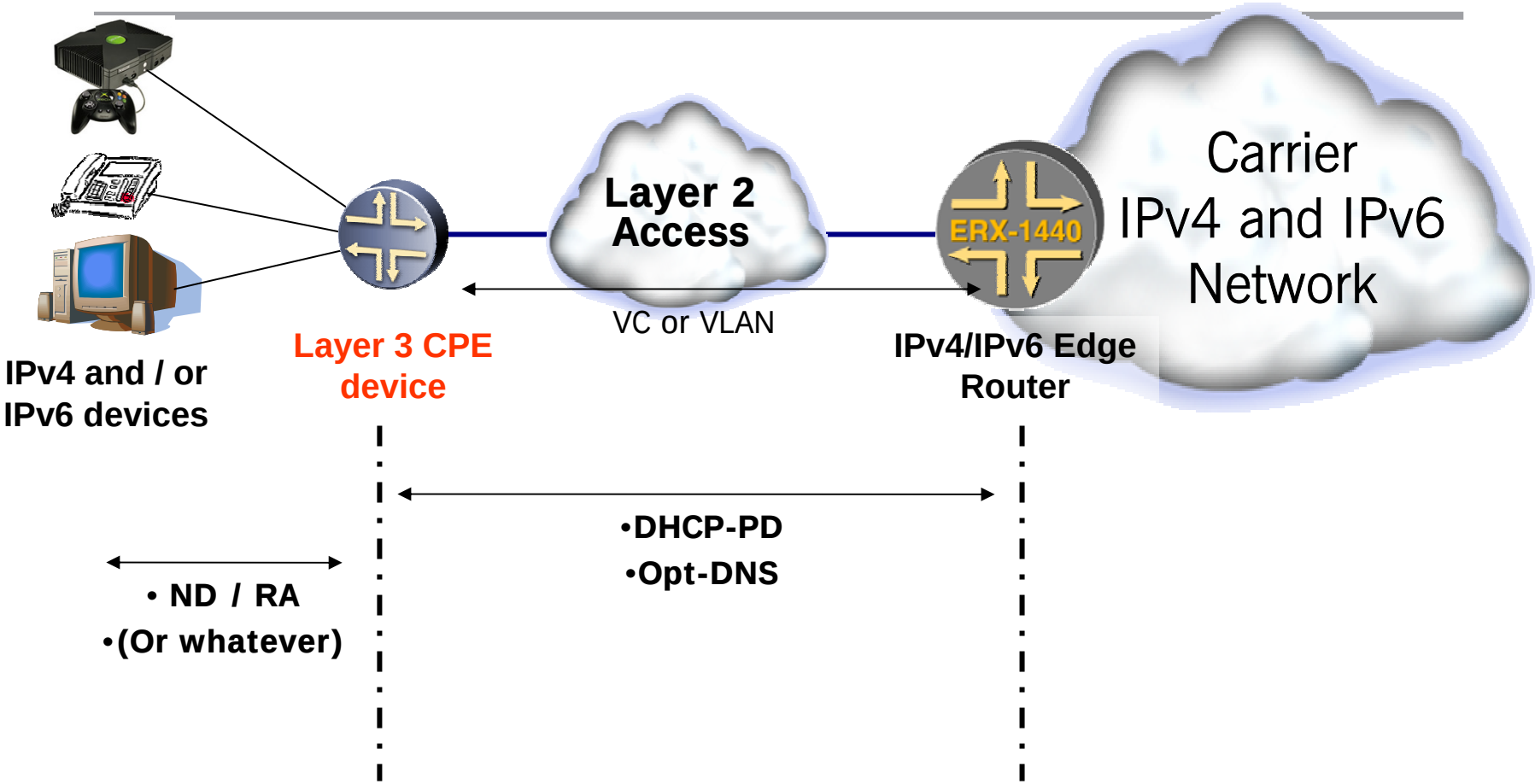
- PPP-Based Services
- Non PPP-Based Services

The Non-PPP model



- Prefixes statically provisioned on user facing interface (VC / VLAN)
- DHCP-PD and opt-DNS could also be used without PPP
- ND / RA could also be used to advertise prefixes over Ethernet access
  - How to do DNS in this case ?
- Less protocol overhead due to no PPP – BUT – bit of a drag due to lost functionality (user auth, accounting, session monitoring, etc)

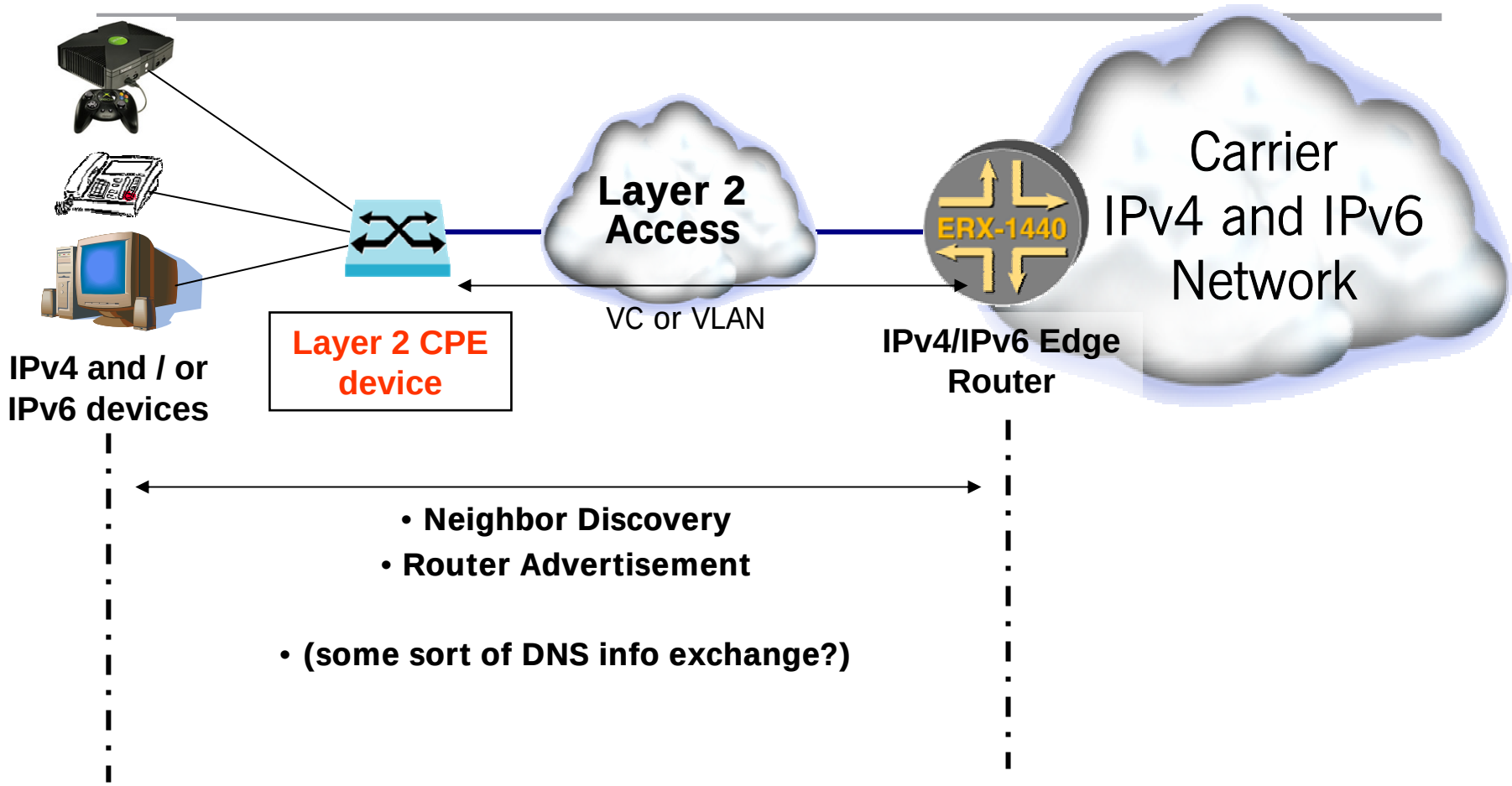
Prefix Assignment in the Non-PPP model - Layer 3 CPE Case



Layer 3 CPE - Details

- Prefixes statically provisioned on the Edge Router
  - One Prefix per access subinterface (VC / VLAN)
- DHCP-PD and opt-DNS used between Edge Router and CPE router
- CPE initiates DHCPv6 exchange to Edge Router
  - Requests IPv6 Prefix via DHCP-PD
  - Requests DNSv6 info via Opt-DNS
- Edge Router responds with configured values
- ND / RA used to assign IPv6 addresses to IPv6 devices behind CPE Router.

Prefix Assignment in the Non-PPP model - Layer 2 CPE Case



Layer 2 CPE - Details

- Prefixes statically provisioned on the Edge Router
  - One Prefix per access subinterface (VC / VLAN)
- Neighbor Discovery & Router Advertisement used between Edge Router and IPv6 hosts
- IPv6 host devices initiate Neighbor Discovery to Edge Router
  - Host Retrieves IPv6 Prefix info and default gateway data via ND / RA
  - **DNSv6 info retrieved via IPv6 DNS client software**
- Edge Router responds with configured IPv6 Prefix & DNS information
- Stateless Autoconfiguration used to generate IPv6 addresses for IPv6 devices

DHCP-PD model details

- client authentication based entirely on interface
- one prefix per interface, statically configured
  - Large provisioning workload !
- default prefix lifetime may be overridden by per-interface manual configuration
- DNS information per VR only, not per client or per interface
- DNS information may be retrieved during prefix delegation, or with an Information request

Non-PPP Model Summary

Function	Layer 2 CPE	Layer 3 CPE
IPv6 Prefix configuration	Static per interface (via ND config)	Static per interface (via DHCP-PD config)
Prefix assignment method	Neighbor Discovery / Router Advertisement on PC	DHCP-PD on CPE router
DNS Server assignment method	NTT "Opt-DNS" Client software, DHCPv6 on Edge Router	Opt-DNS on CPE router, DHCPv6 on Edge Router
User authentication	None	None
Access media supported	ATM Bridged Ethernet, Ethernet	ATM Bridged Ethernet, Ethernet
Accounting data	Per subinterface	Per subinterface
# hosts supported per VC / VLAN	1 only (?)	Many (behind CPE)

PPP Model Summary

Function	Layer 2 CPE (future)	Layer 3 CPE
IPv6 Prefix configuration	Radius	Radius
Prefix assignment method	DHCP-PD on host	DHCP-PD on CPE router
DNS Server assignment method	Opt-DNS on host	Opt-DNS on CPE router
User authentication	Username / Password	Username / Password
Access media supported	All	All
Accounting data	Radius	Radius
# hosts supported per VC / VLAN	Many (via multiple PPPoE sessions)	Many (behind CPE)

IPv6 BRAS Service Model Summary

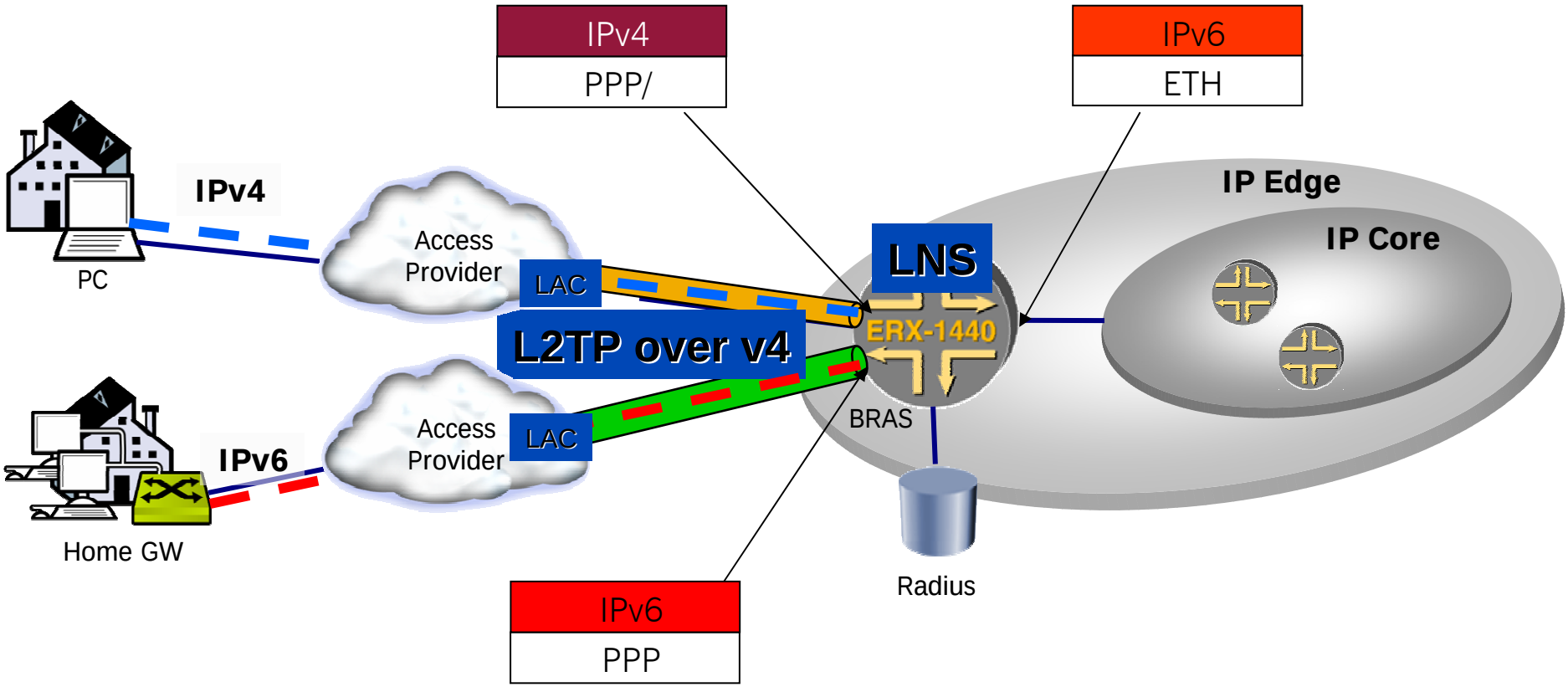
- PPP based
- Requires Dual Stack (IPv4/v6) PPPoE client or device
- Session based service model
- User authentication & accounting information present
- Radius based AAA
- Leverages DHCP-PD and opt-DNS

- Non PPP-based
- DHCP-PD or ND/RA can be used in the access network
- No native authentication or accounting
- More suitable to “always-on” service

IPv6 Broadband Service Models

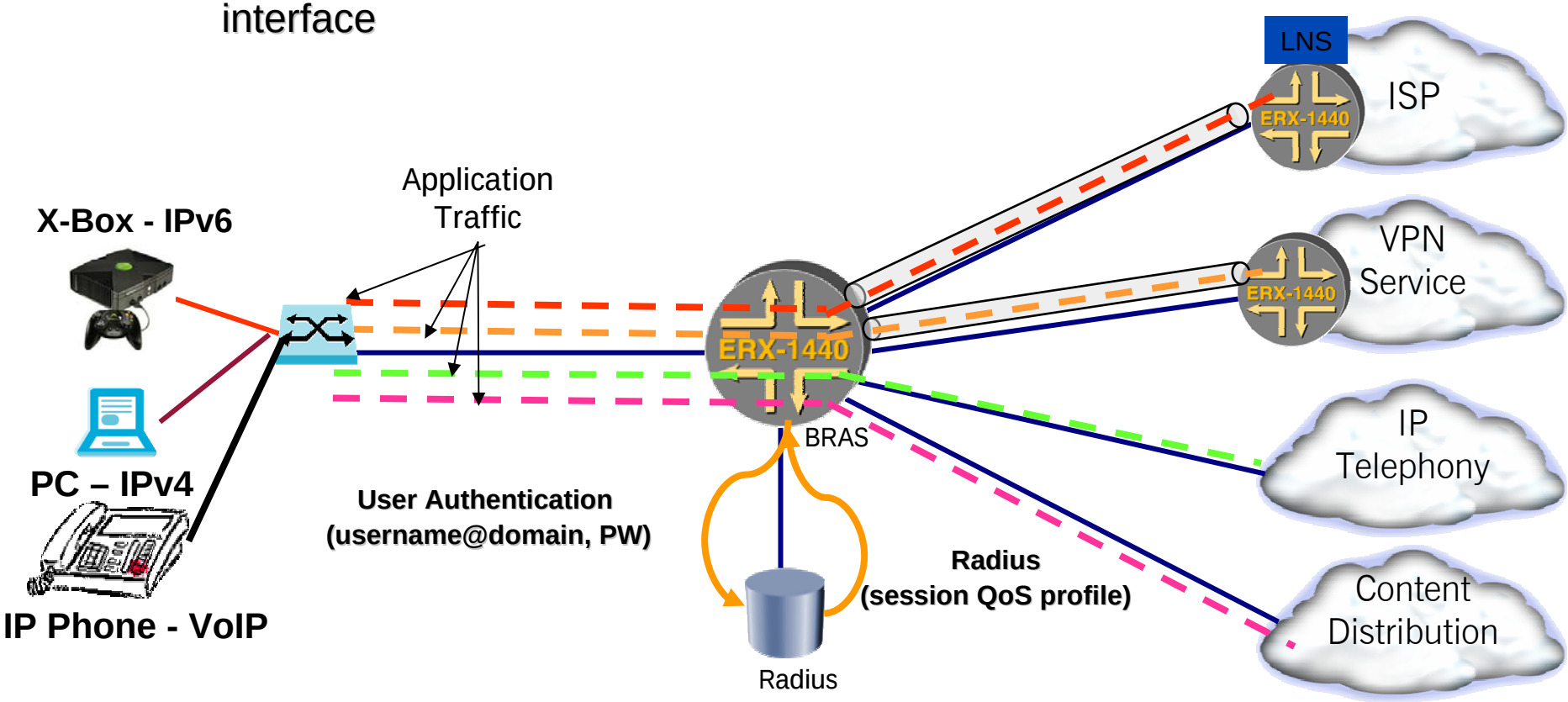
- Retail
- Wholesale
  - L2TP LAC and LNS
  - VR-based wholesale
- VPNs (VR, 6PE)
- QoS-Enabled Value Added Services
  - Voice
  - Video
  - Gaming, etc

The IPv6 LNS

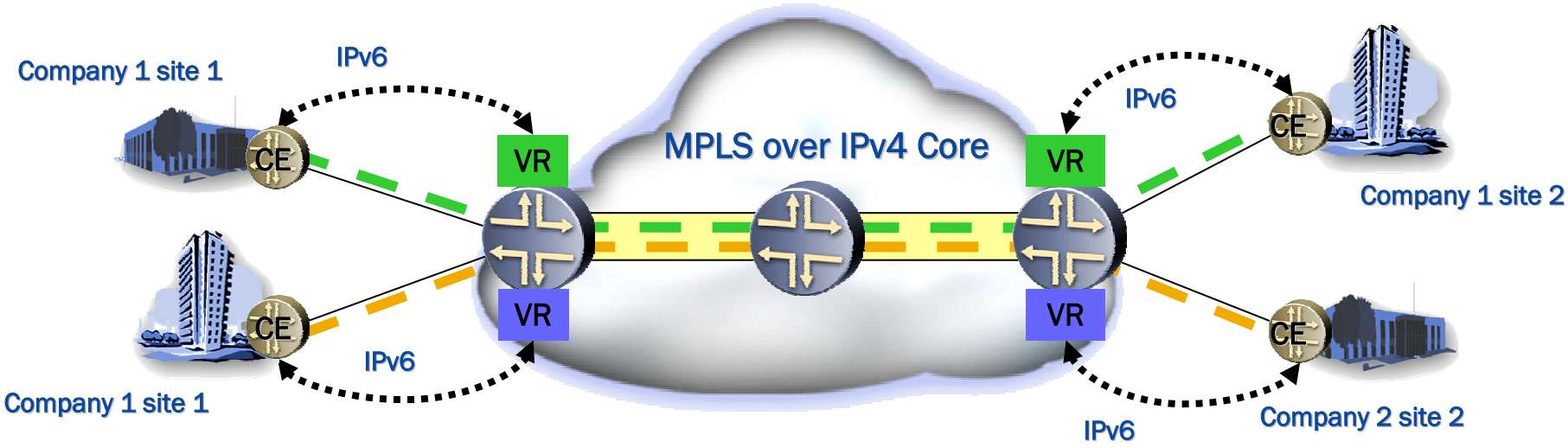


QoS for IPv4 and IPv6 Traffic on the BRAS

- V4 & V6 sessions can be terminated or tunneled (L2TP)
  - Decision made by Radius (terminate or tunnel ppp session)
  - QoS profile (returned via Radius) is attached to L2TP session or PPP/IP interface



“6PE” - IPv6 over MPLS / IPv4



- Tunnel IPv6 traffic across your existing MPLS / IPv4 network
- Easily and cheaply introduce IPv6 VPN services

Edge Router Multicast Implementation Overview

Juniper NETWORKS™

Multicast Control Knobs

- Controlled User Access
  - IGMP/MLD Join Policy
    - Reject requests to join disallowed channels
    - Join requests compared to contents of access-list (possibly provided via user authentication)
  - IGMP/MLD dynamic capabilities from RADIUS/Policy Server
  - IGMP/MLD Group Join Limits
    - Per port and/or IP interface
    - Provides a CAC to prevent degradation from congestion (e.g., allow 200 5Mb sessions on a GE link but reject the 201st)
- Rapid Response
  - IGMP/MLD Immediate Leave
    - Avoid (Robustness * Last Member Query Interval) delay when leaving a channel
  - IGMP/MLD Last Member Query Interval may be 100ms if “Immediate Leave” not used

Multicast Statistics

- Separate Multicast packet stats per IIF/OIF
- CLACL match stats and QoS queue stats as with unicast IP

Multicast Join/Leave Accounting

- Bulkstat join/leave tracking
  - Identify when a users on an interface joined/left each group
  - Valuable for identifying highly viewed content (e.g., for advertising revenue)
  - FTP'd off-chassis at regular intervals
- Sample output (IPv6/MLD in this case)

Igmp Schema: {ifDescr, ifType, usdIfType} : {ifIndex; ifLowerInterface; usdRouterIndex; dstIpAddr; srcIpAddr; multicastGroup; IGMP/MLD cmd (Report1/2/3); ifTimeStamp}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff0e::4:1; fe80::90:1a00:210:10dd; ff0e::4:1; Report2; MON DEC 29 2003 13:11:14.110 UTC}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff0e::4:1; fe80::90:1a00:210:10dd; ff0e::4:1; Report2; MON DEC 29 2003 13:11:15.510 UTC}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff02::2; fe80::90:1a00:210:10dd; ff0e::4:1; Leave; MON DEC 29 2003 13:11:19.440 UTC}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff02::1; ff02::1; ff0e::4:1; GroupDelete; MON DEC 29 2003 13:11:45.60 UTC}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff0e::4:1; fe80::90:1a00:210:10dd; ff0e::4:1; Report2; MON DEC 29 2003 13:11:49.990 UTC}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff0e::4:1; fe80::90:1a00:210:10dd; ff0e::4:1; Report2; MON DEC 29 2003 13:11:55.190 UTC}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff02::2; fe80::90:1a00:210:10dd; ff0e::4:1; Leave; MON DEC 29 2003 13:11:55.310 UTC}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff02::1; ff02::1; ff0e::4:1; GroupDelete; MON DEC 29 2003 13:12:46.60 UTC}

{IPv6If, 1, 50} : {838860810; 184549379; 2147483651; ff0e::4:1; fe80::90:1a00:210:10dd; ff0e::4:1; Report2; MON DEC 29 2003 13:12:50.870 UTC}

Edge Router Multicast Functionality

- Summary
  - IGMP & IGMP Proxy (v1 & v2)
  - MLDv1 and v2
  - PIM for IPv6, PIM SSM
  - PIM-SM, PIM-DM, PIM-SM/DM (v2)
  - DVMRP (v3)
  - MBGP
  - MTRACE (traceroute for multicast)
  - Multicast translation table for MLDv1
  - Block mcast traffic from user into the network

Security and Protection for IPv6 over Broadband

- Security Features needed in the Edge Router
  - Radius based User Authentication (PPP Dual Stack only)
  - IPv6 Policy Routing – CoS classification & marking
  - IPv6 Source-Address validation
  - IPV6 Policy - Rate Limit profile
  - IPV6 Policy – full SA/DA based classification
  - Blocking multicast traffic from subscribers into the network

Juniper™
NETWORKS

Juniper your Net™