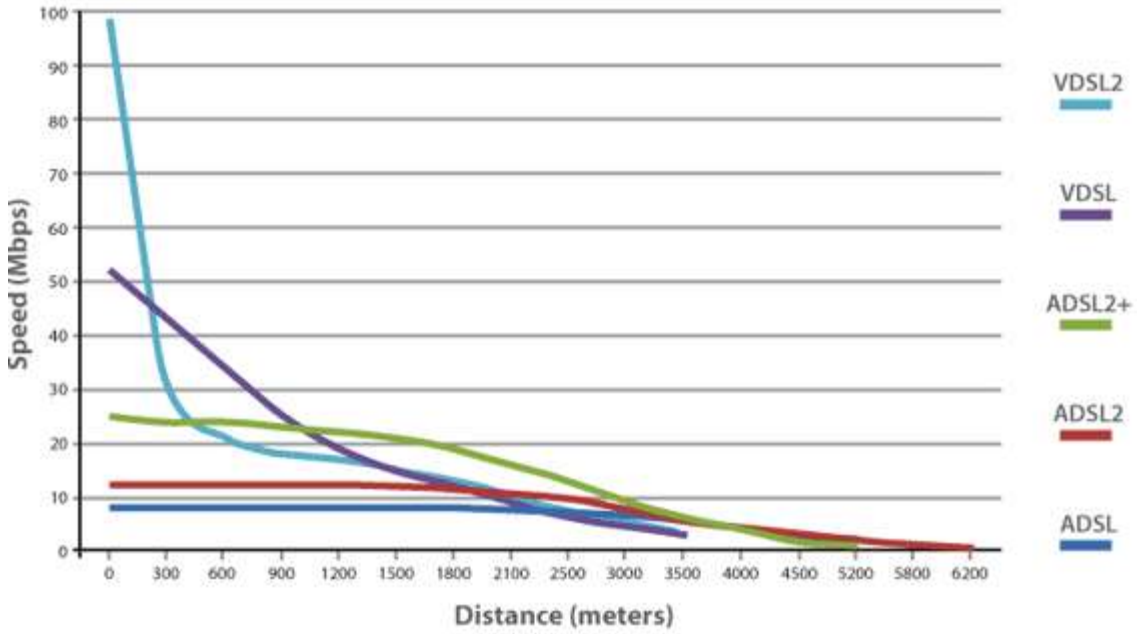
Access Network Architectures

KIS FRI ZU
PrS II

Roman Kaloč

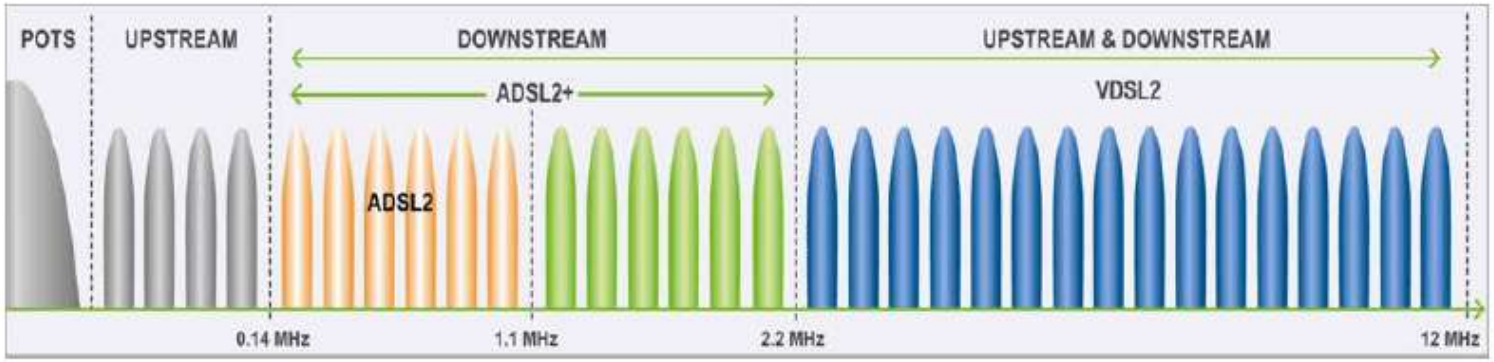
xDSL Digital Subscriber Line technology

- ADSL Asymetric Digital Subscriber Line
- VDSL Very High Speed Digital Subscriber Line
- Copper based High speed network access technology
- Rapidly growing broadband access solution for home networking and small business systems
- Uses multi-carrier modulation over unused frequency bands in phone lines
- Supports data rates up to 6144 Kbps downstream and 640 Kbps upstream
- ADSL typically up to 4 km

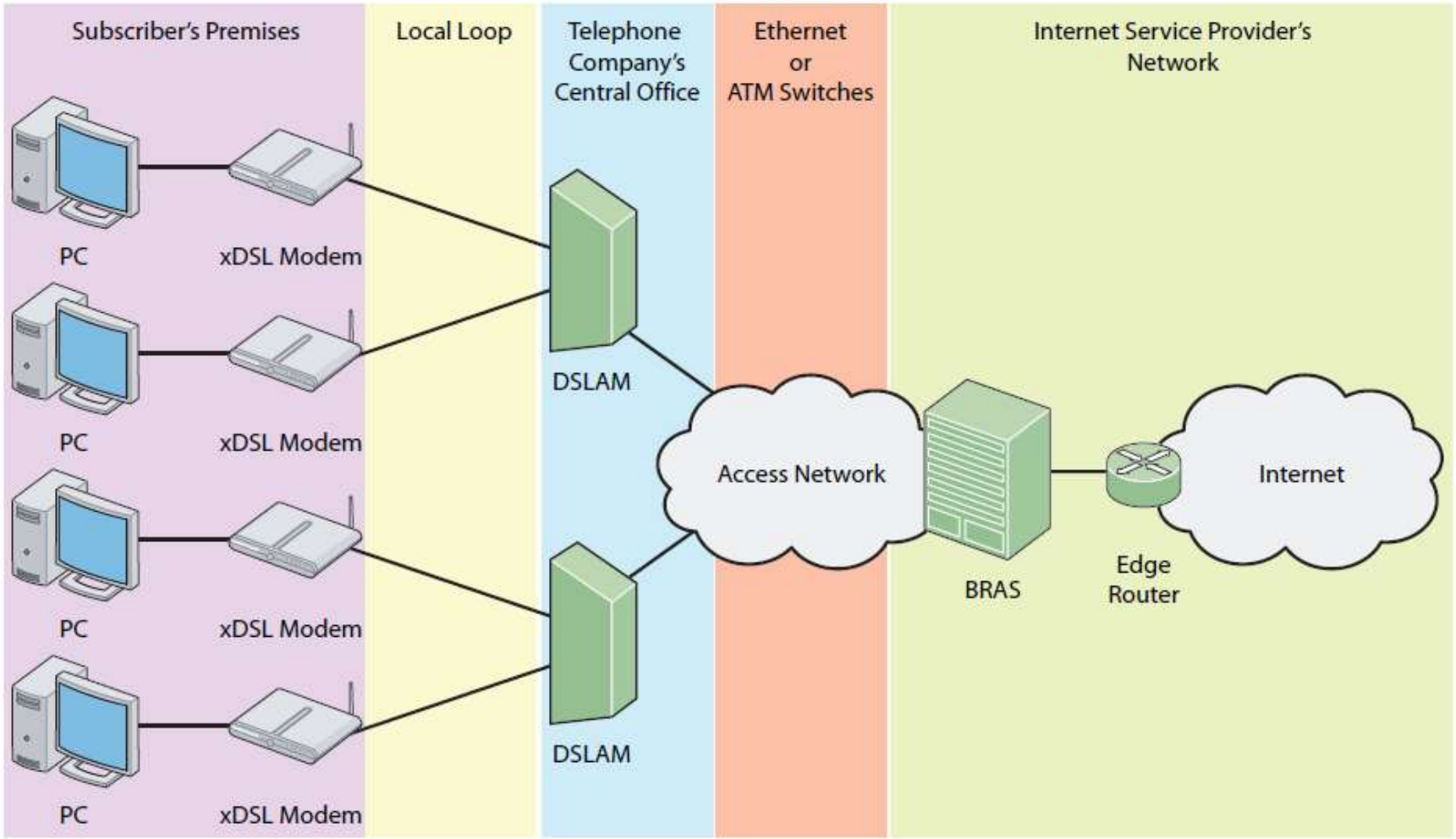


xDSL Digital Subscriber Line technology

Version	Standard name	Common name	Downstream rate	Upstream rate	Approved in
ADSL	ANSI T1.413-1998 Issue 2	ADSL	8.0 Mbit/s	1.0 Mbit/s	1998
ADSL	ITU G.992.2	ADSL Lite (G.lite)	1.5 Mbit/s	0.5 Mbit/s	1999-07
ADSL	ITU G.992.1	ADSL (G.dmt)	8.0 Mbit/s	1.3 Mbit/s	1999-07
ADSL	ITU G.992.1 Annex A	ADSL over POTS	12.0 Mbit/s	1.3 Mbit/s	2001
ADSL	ITU G.992.1 Annex B	ADSL over ISDN	12.0 Mbit/s	1.8 Mbit/s	2005
ADSL2	ITU G.992.3 Annex L	RE-ADSL2	5.0 Mbit/s	0.8 Mbit/s	2002-07
ADSL2	ITU G.992.3	ADSL2	12.0 Mbit/s	1.3 Mbit/s	2002-07
ADSL2	ITU G.992.3 Annex J	ADSL2	12.0 Mbit/s	3.5 Mbit/s	2002-07
ADSL2	ITU G.992.4	splitterless ADSL2	1.5 Mbit/s	0.5 Mbit/s	2002-07
ADSL2+	ITU G.992.5	ADSL2+	24.0 Mbit/s	1.4 Mbit/s	2003-05
ADSL2+	ITU G.992.5 Annex M	ADSL2+M	24.0 Mbit/s	3.3 Mbit/s	2008

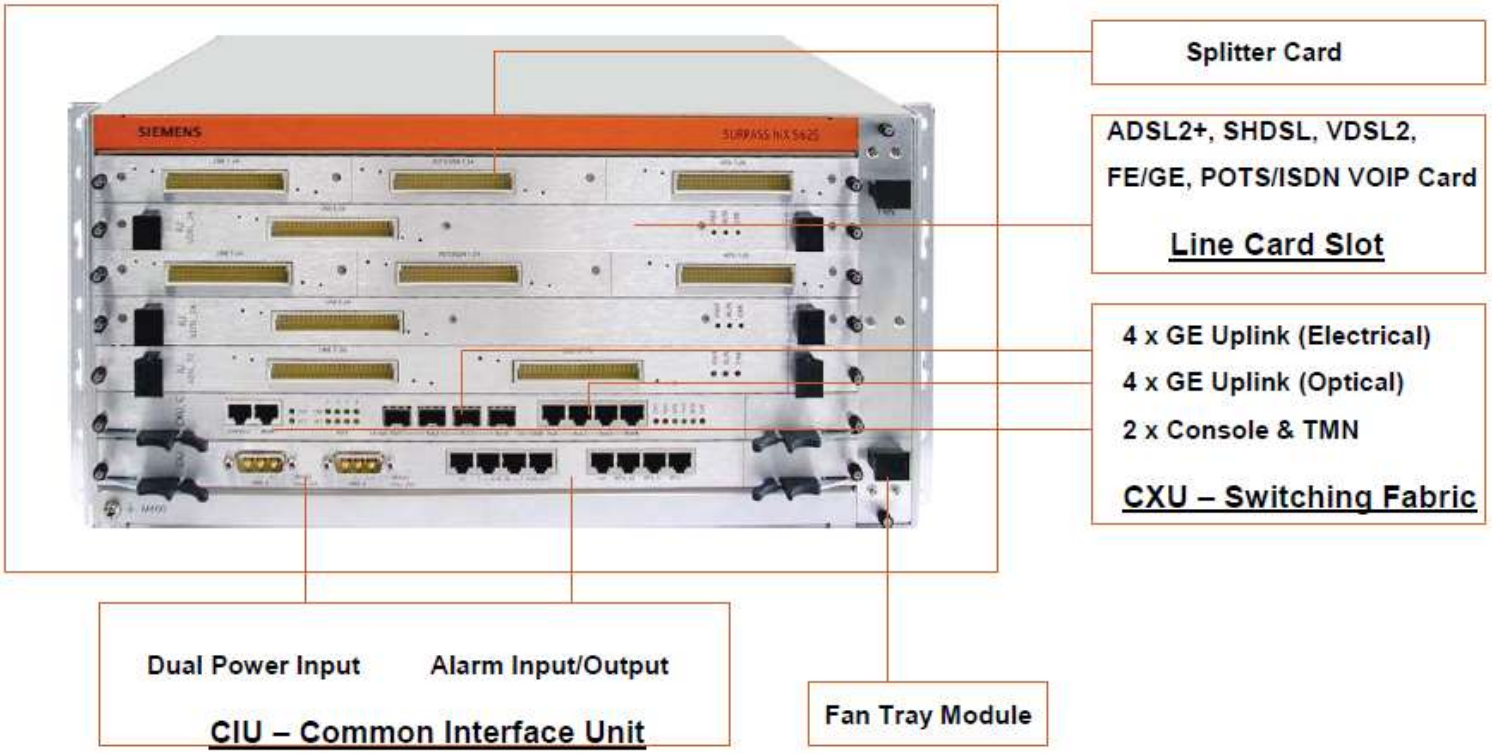


DSL network infrastructure

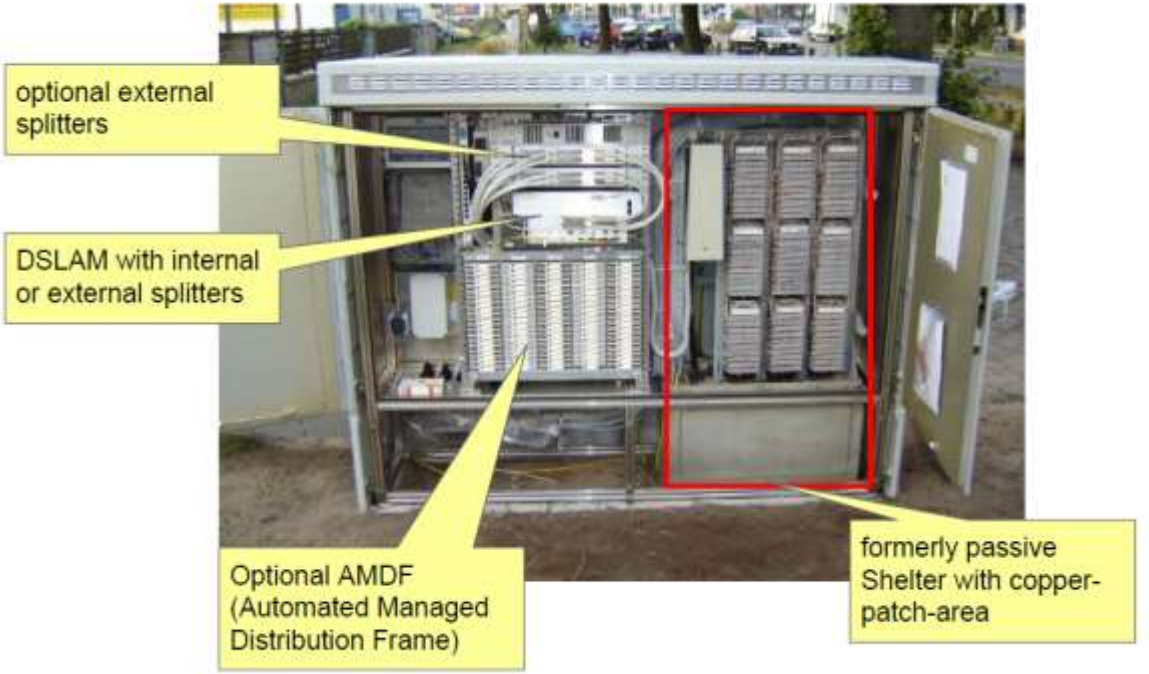


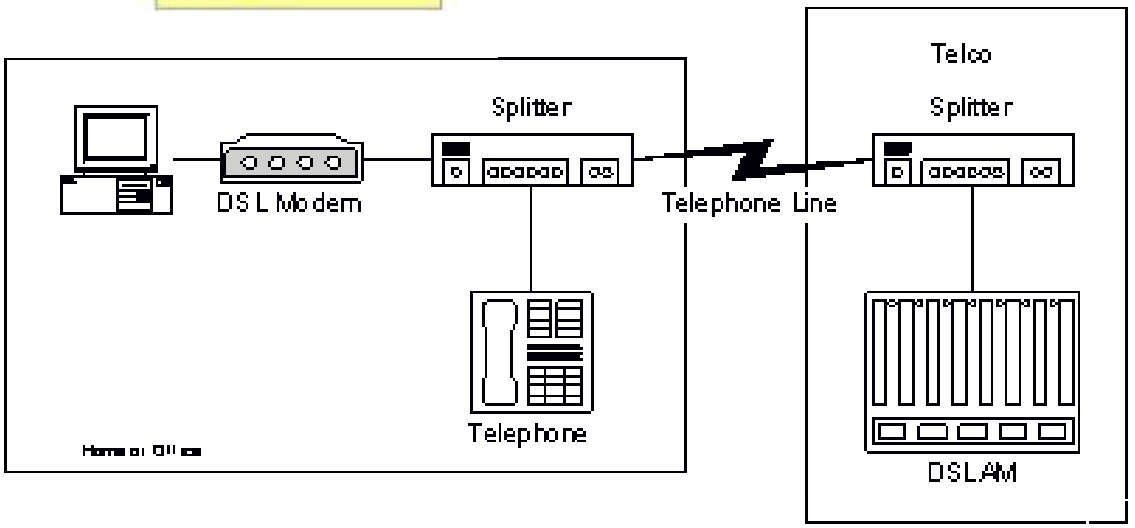
DSLAM - Digital Subscriber Line Access Multiplexer

- Also called MSAN – MultiService Access Node
- The DSLAM equipment collects the data from its many modem ports and aggregates their voice and data traffic
- The DSLAM traffic is switched to a Broadband Remote Access Server where the end-user traffic is then routed across the ISP network to the Internet
- ATM DSLAMs and IP DSLAMs

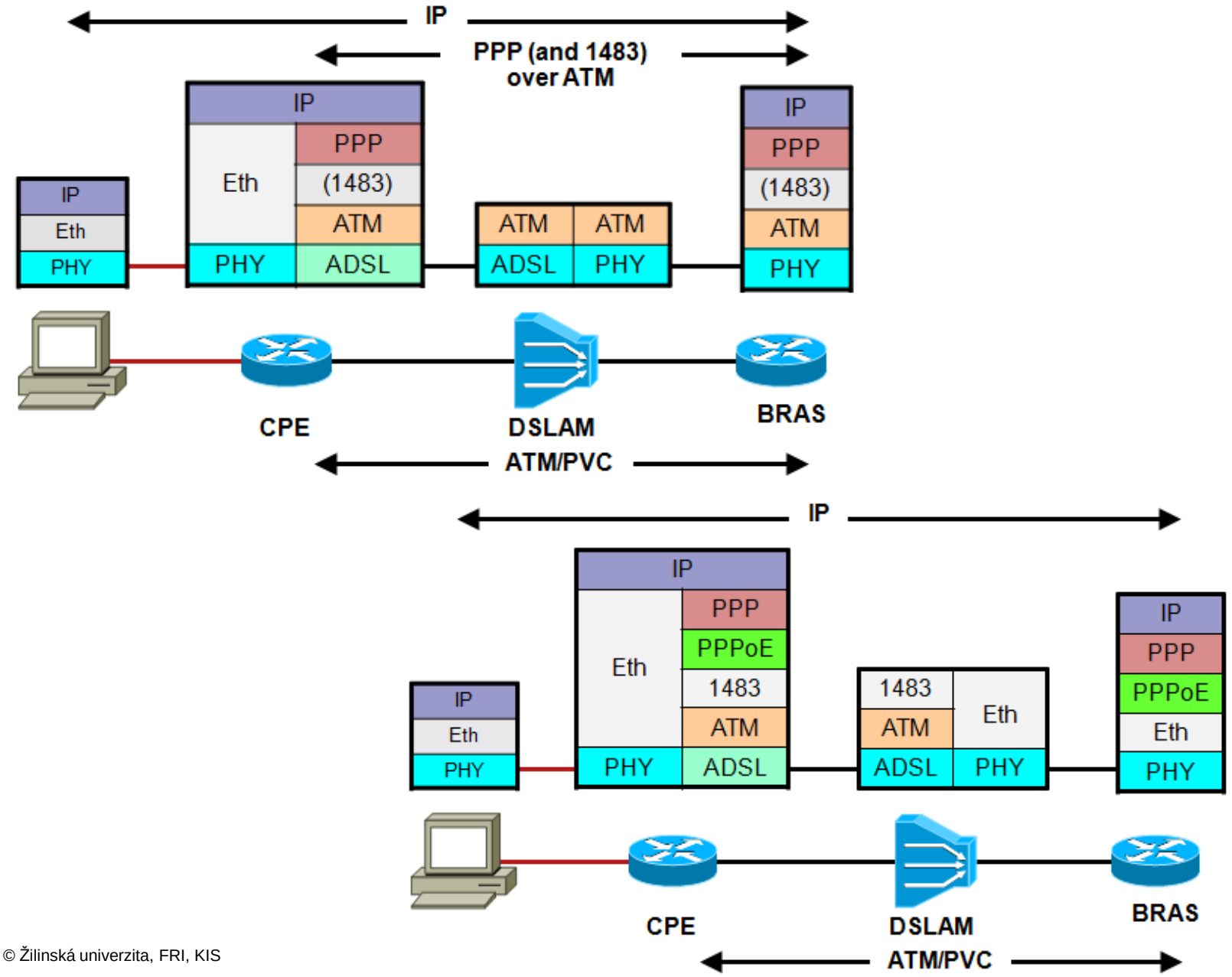


DSLAM - Digital Subscriber Line Access Multiplexer





ATM and IP DSLAMs



Optical Access Network

From the architecture diagram, the optical access network comprises the following scenarios:

1. FTTB scenario

As an access scenario for business users, Fiber to The Business (FTTB) scenario falls into single business unit (SBU) and Business Multi-tenant unit (MTU) in terms of capacity. Of them, SBU provides a comparatively small number of ports, including following types: POTS, 10/100/1000BASE-T, RF(33dBmV), and DS1/T1/E1 ports; MTU provides a comparatively larger number of ports, including following types: POTS, 10/100/1000BASE-T, RF and DS1/T1/E1 ports.

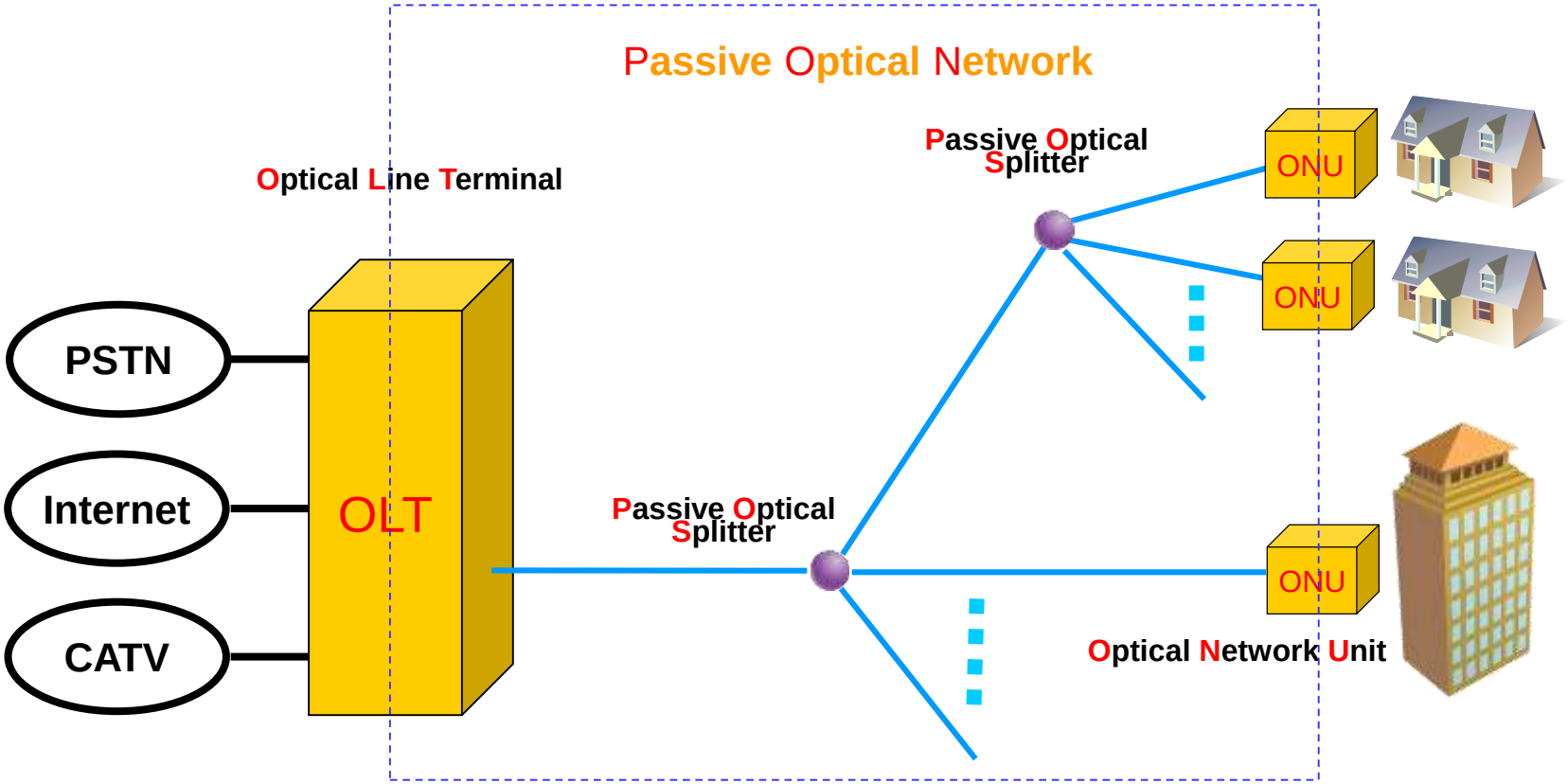
2. FTTC & FTTCab scenario

As an access to the curb or the cabinet over fibre, Fiber to The Curb& Fiber to The Cabinet (FTTC & FTTCab) scenario is for the Multi-dwelling unit (MDU), providing a comparatively larger number of ports, including following types: 10/100/1000BASE-T, RF(33dBmV), VDSL2, and so on.

3. FTTH scenario

As an access to the home over fibre, Fiber to The Home (FTTH) scenario is mainly for the single family unit (SFU), providing a comparatively small number of ports, including following types: POTS, 10/100/1000BASE-T, and RF(18dBmV).

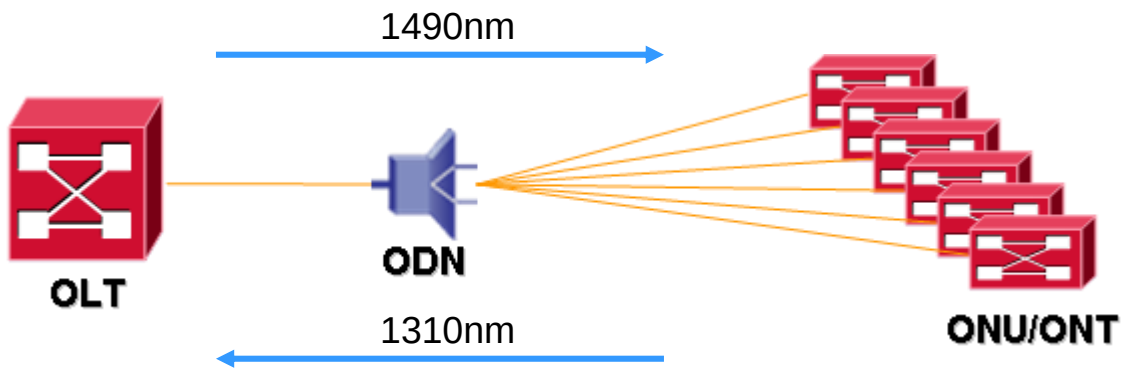
PON - assive Optical Networks



- **PON is a kind of passive optical network featuring one-to-multiple-point architecture;**
- **PON is short for Passive Optical Network ;**
- **PON consists of Optical Line Terminal (OLT), Optical Network Unit (ONU) and Passive Optical Splitter.**
- GPON supports the long-reach (up to 20 km) service coverage to overcome the obstacle of the access technology over twisted pair cables and reduce the network nodes.

GPON Principle

GPON adopts Wavelength Division Multiplexing (WDM) technology, facilitating bi-direction communication over a single fiber.

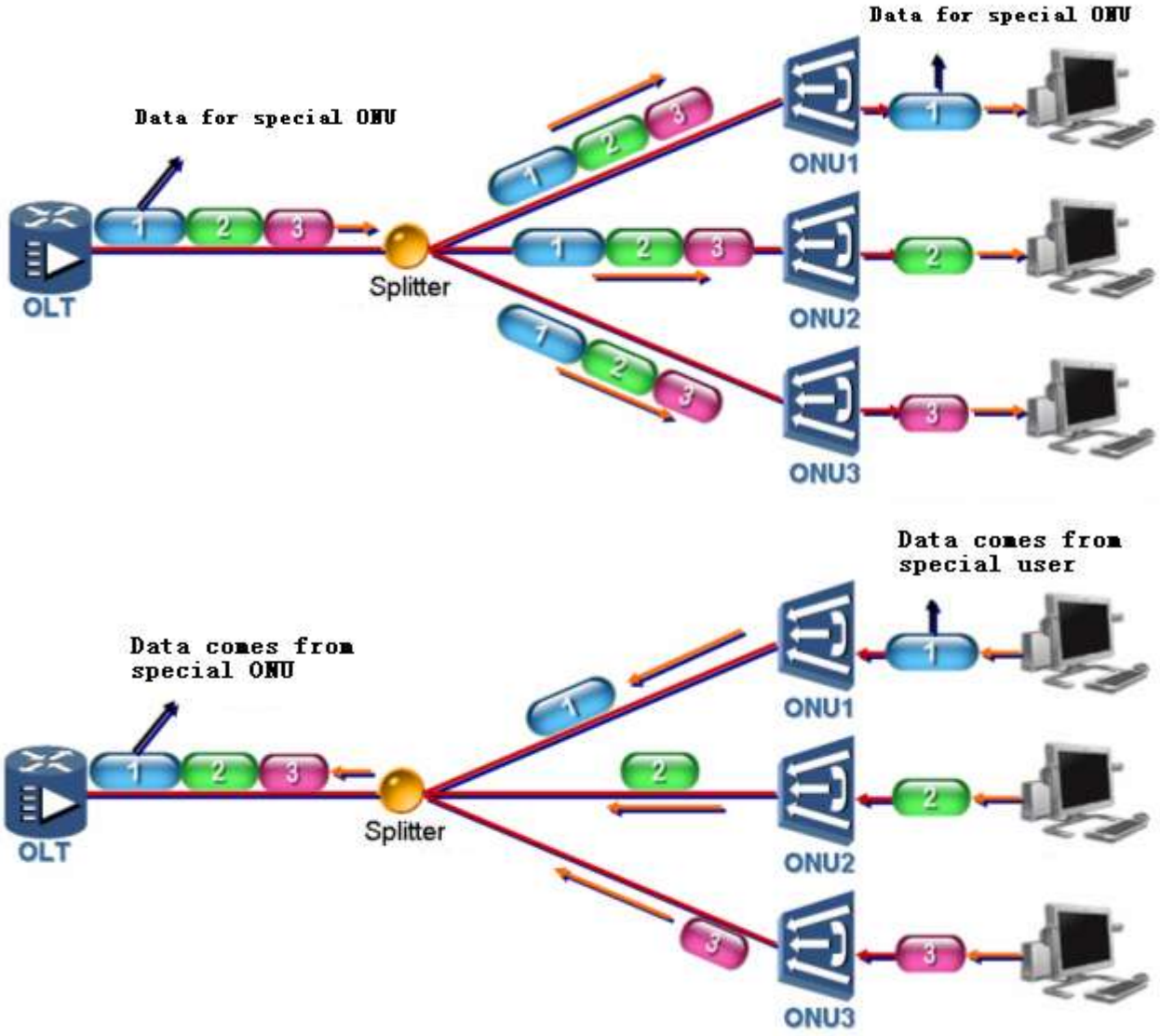


To separate upstream/downstream signals of multiple users over a single fibre, GPON adopts two multiplexing mechanism:

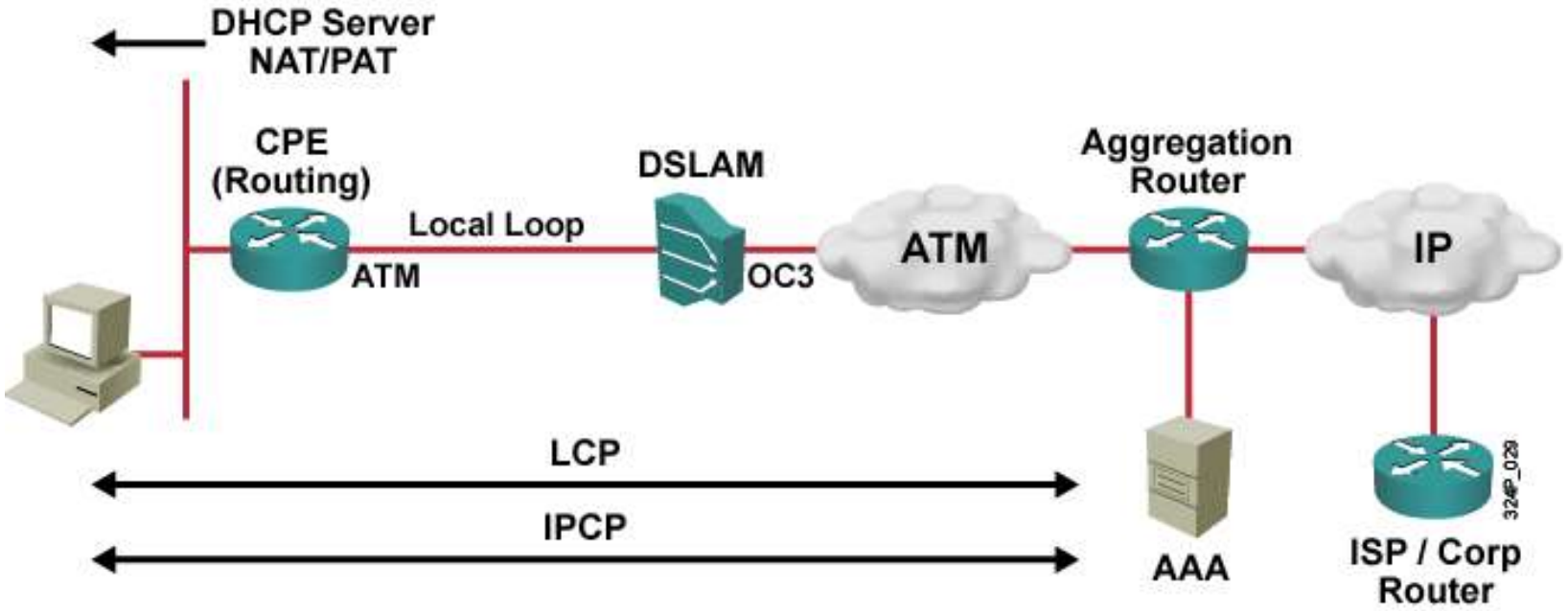
- In downstream direction, data packets are transmitted in a broadcast manner;
- In upstream direction, data packets are transmitted in a TDMA manner.

- ODN Optical Distributed Network

GPON Downstream (broadcast) and Upstream (TDMA)

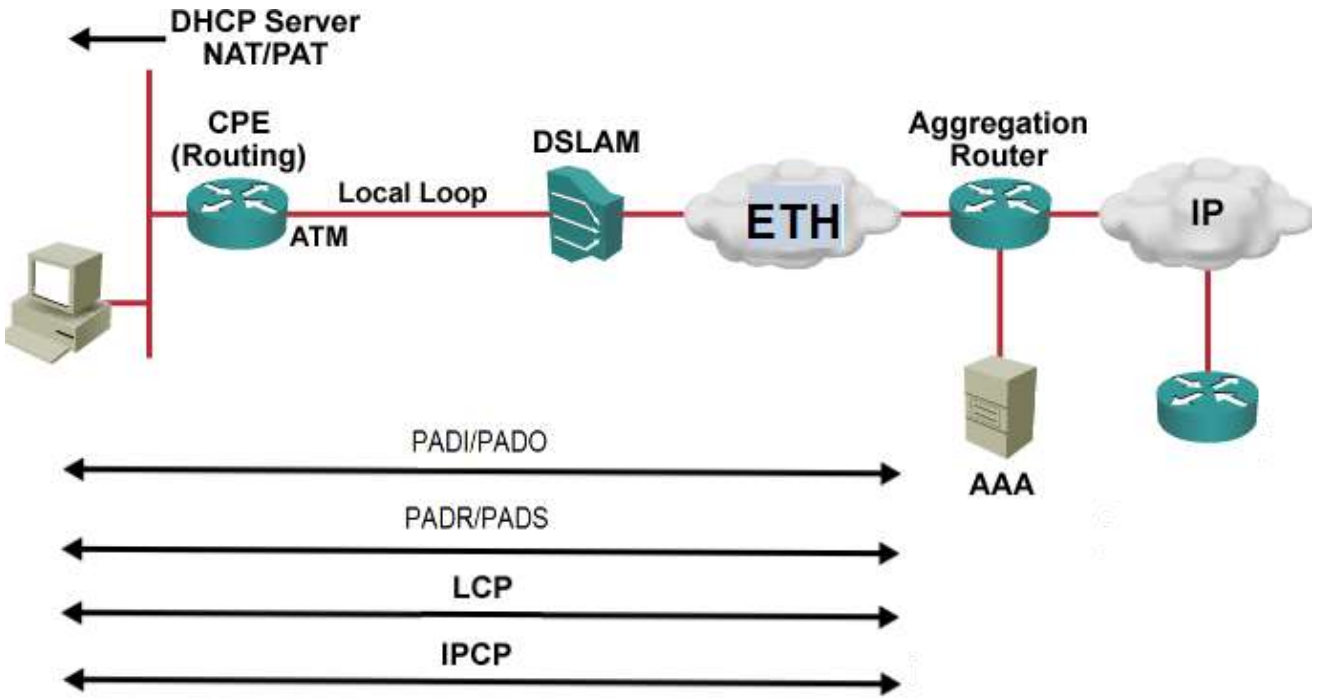


Establishing a PPP Session with PPPoA



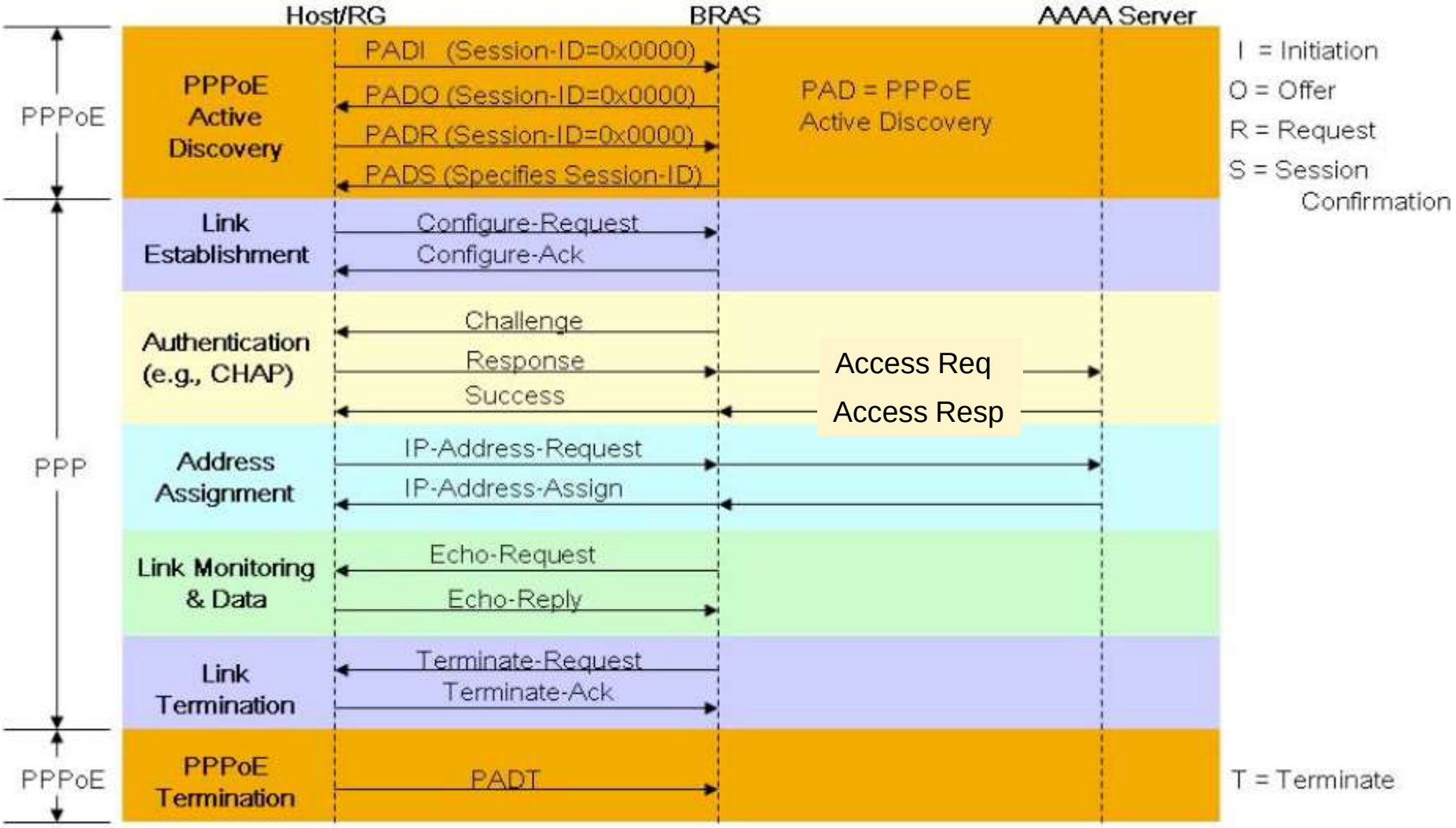
CPE receives an IP address via IPCP like in the dial model.

Establishing a PPP Session with PPPoE



- Point-to-point communications channel over an Ethernet network
- PPPoE includes a straightforward mechanism for the host to find a PPPoE server/BRAS to communicate with. The host broadcasts a request to establish a connection (PADI); all potential BRAS devices respond (PADO) with an “offer” to be the termination point; the host selects one (PADR); and the BRAS responds by assigning a session identifier

PPPoE and PPP Session Flow

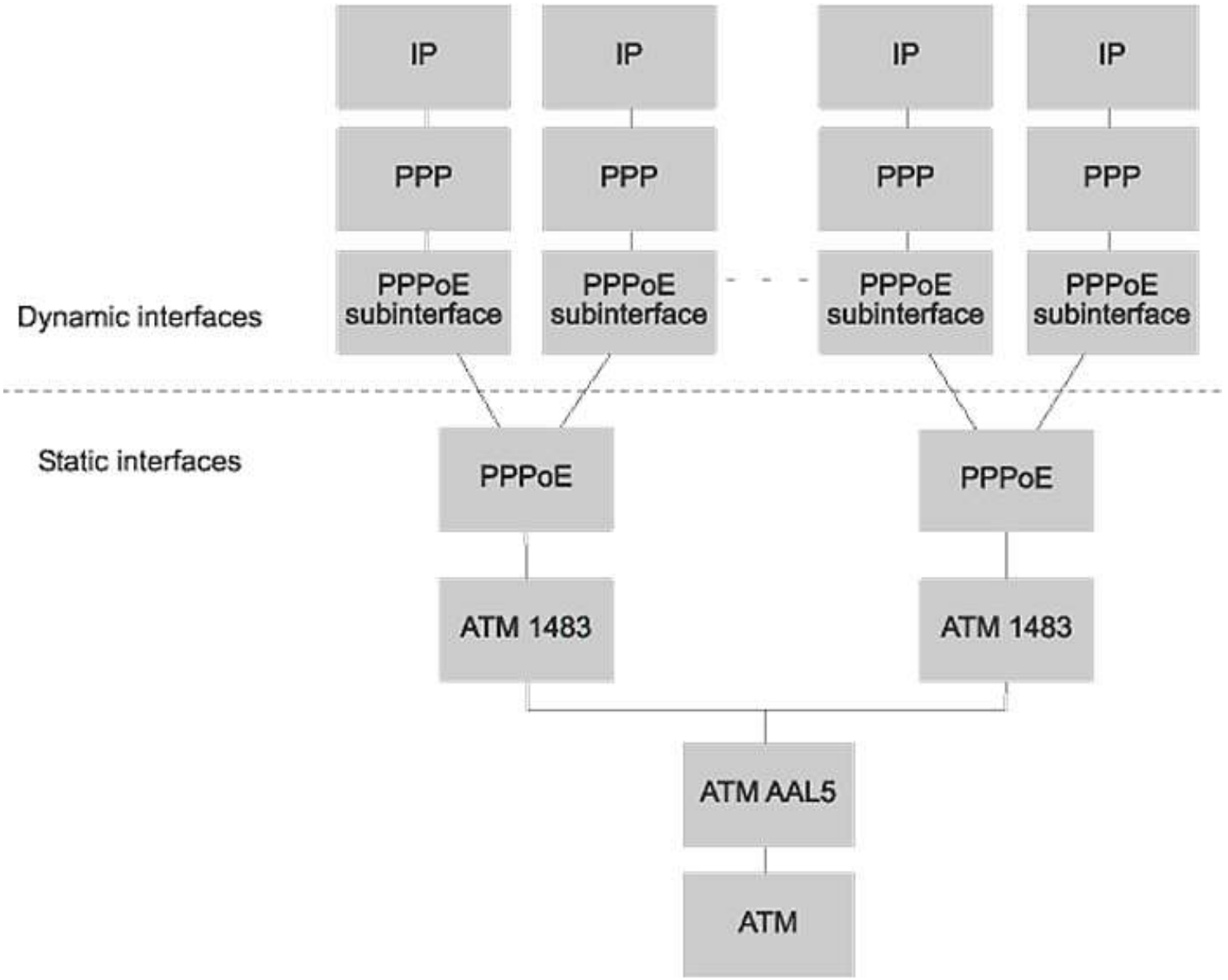


Radius User Profile Examples

johndoe Password = “abcde"
Service-Type = Frame-User,
Framed-Protocol = PPP,
cisco-avpair = "atm:peak-cell-rate=155000",
cisco-avpair = "atm:sustainable-cell-rate=155000"

user1@abc.com Password = “abcde", Service-Type = Outbound
cisco-avpair = "vpdn:tunnel-id=shiva",
cisco-avpair = "vpdn:tunnel-type=l2tp",
cisco-avpair = "vpdn:l2tp-tunnel-password=password2",
cisco-avpair = "vpdn:ip-addresses=172.16.1.1",

BRAS – static and dynamic subinterfaces



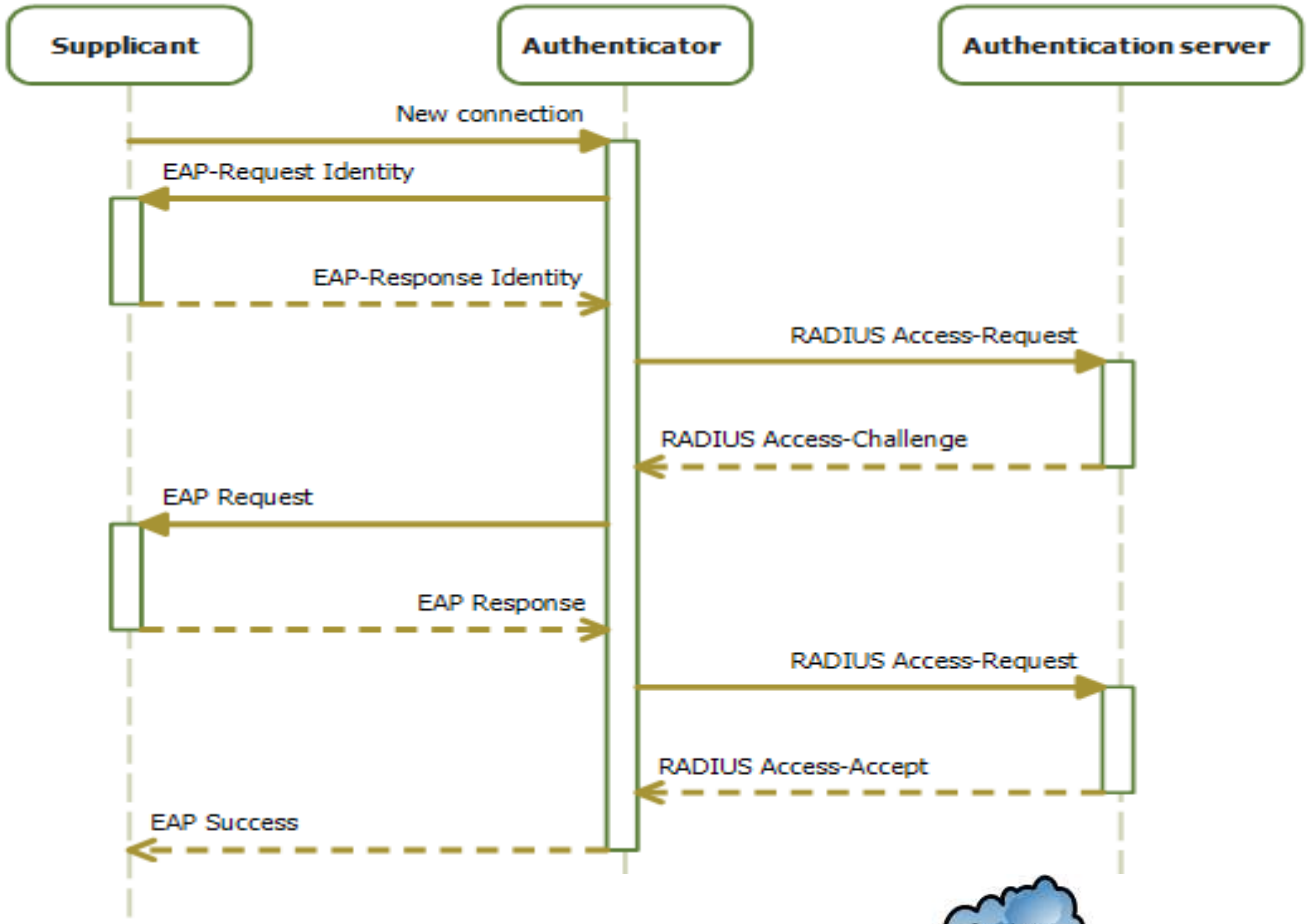
PPPoE Challenges

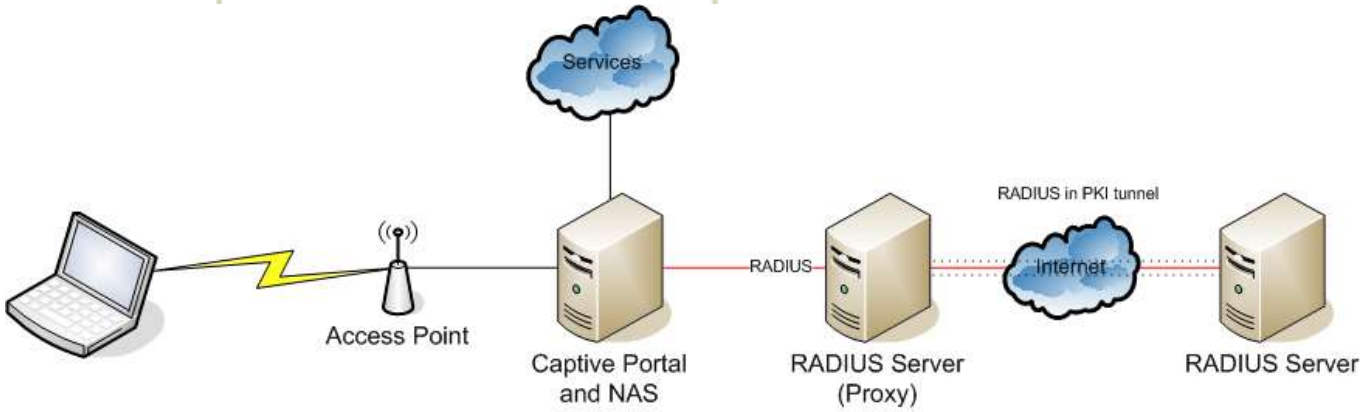
PPP has few drawbacks

- First, PPP essentially uses two levels of L2 encapsulation. This adds 10 bytes to every packet.
- Requires more processing to create, inspect and terminate each PPP packet than is required by the simpler IP over Ethernet (IPoE) method.
- The other challenge is that PPP is designed to support unicast (point-to-point) connections
- No multicasting

IP over Ethernet (IPoE)

- IP over Ethernet (IPoE) is a more recent alternative to the PPP-based models.
- IPoE relies on DHCP to provide the IP address.
- DHCP (Dynamic Host Configuration Protocol)
  - Application-layer protocol
  - Designed for broadcast networks
  - UDP broadcast from port 68 to port 67
  - Assign IP addresses, DNS servers, etc.
  - DHCP Discover, Offer, Request, Ack
- DHCP client renews its lease when it has reached half-way with its lease
- Extensions needed
  - No authentication - IEEE 802.1x EAP (Extensible Authentication Protocol) possibility, needs to be supported by client
  - IPoE does not incorporate link monitoring – BFD
  - Access before Authorization
  - Wholesale Support – requires unique subscr VLANs

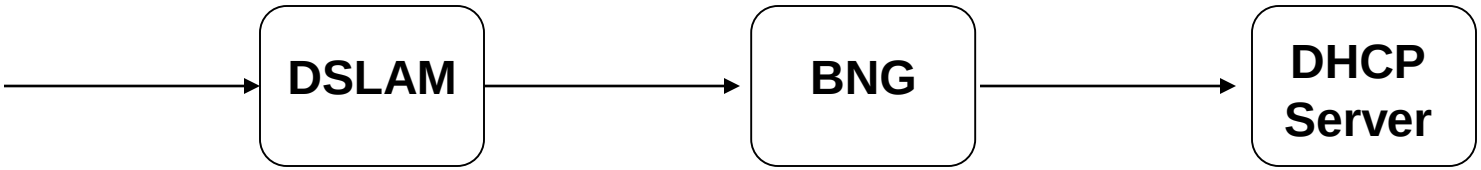




DHCP Option 82

Have DSLAM insert option identifying customer port

- DSLAM is configured as a DHCP relay agent with option 82.
- Transparent to customer, modifies the DHCP Discover packet
- circuit ID and remote ID



DISCOVER
DA: 255.255.255.255
SA: 0.0.0.0

DISCOVER
DA: 255.255.255.255
SA: 10.20.1.1
Option 82: DSLAM123/Port 20

DHCP models

BNG-hosted DHCP

- Local address pools
- Limited control over address allocation policy

DHCP relay

- BNG relays DHCP to central server
- BNG has no lease state

DHCP relay proxy

- BNG masquerades as DHCP server
- More complex functionality required on BNG to add new DHCP option types

DSLAM Security

- PPPoE Intermediate Agent
  - It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets
- Customer Traffic Isolation
  - No traffic possible from one DSL port to another DSL port – PVLAN, proxy/local-proxy ARP
- Access Control Lists – MACs, VLANs, etc
- BPDUs are blocked received from DSL port
- Limit Number of MAC addresses per DSL port
- MAC anti-spoofing, IP anti-spoofing (DHCP based)
  - blocks user traffic in case same MAC addresses is already in use by other user
  - snoops the DHCP messages and registers the assigned IP addresses
- Multicasting blocking upstream
  - Exceptions are ARP, PPPoE, DHCP and IGMP frames
- No multicast/unknown unicast/broadcast flooding downstream
- IGMP proxy / snooping – simple tree topology, no PIM needed, edge DSLAM as a IGMP router/switch which duplicates mcast

Layer 2 / Layer 3 Wholesale Services

Layer 2 wholesale

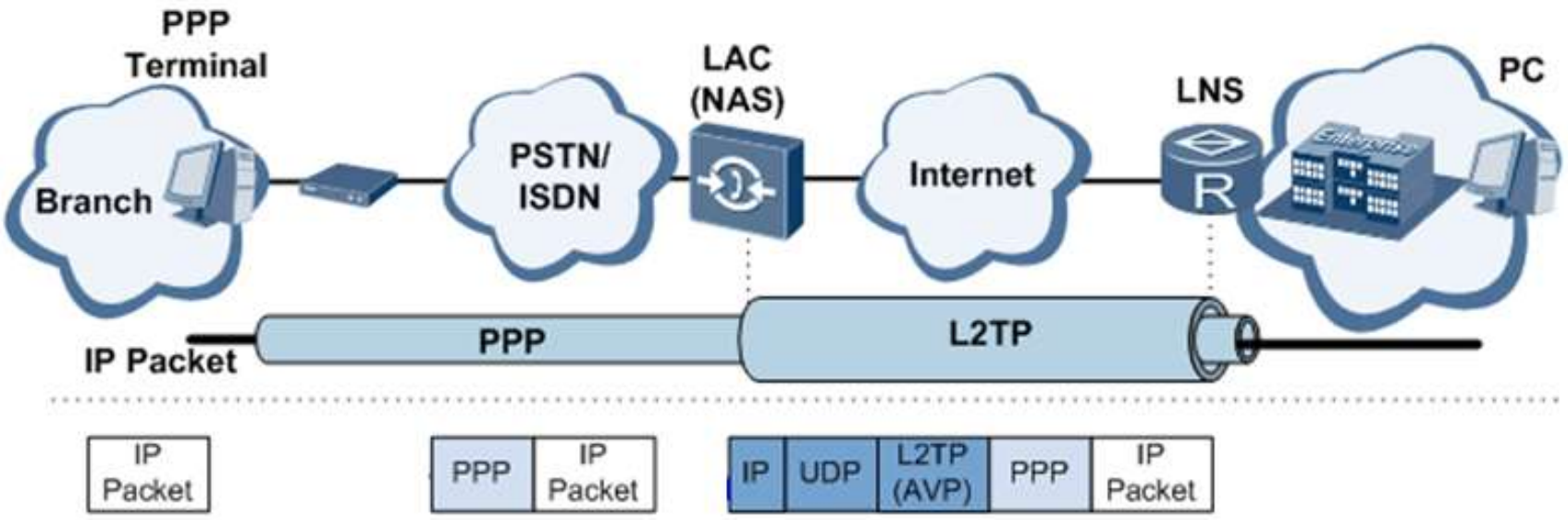
- Cross connect of layer 2 circuit into a VPN over to retail ISP
- Two ways
  - **L2TP tunneling**
  - **VLAN cross connect -** layer 2 circuit into a remote BRAS over to retail ISP network

Layer 3 wholesale

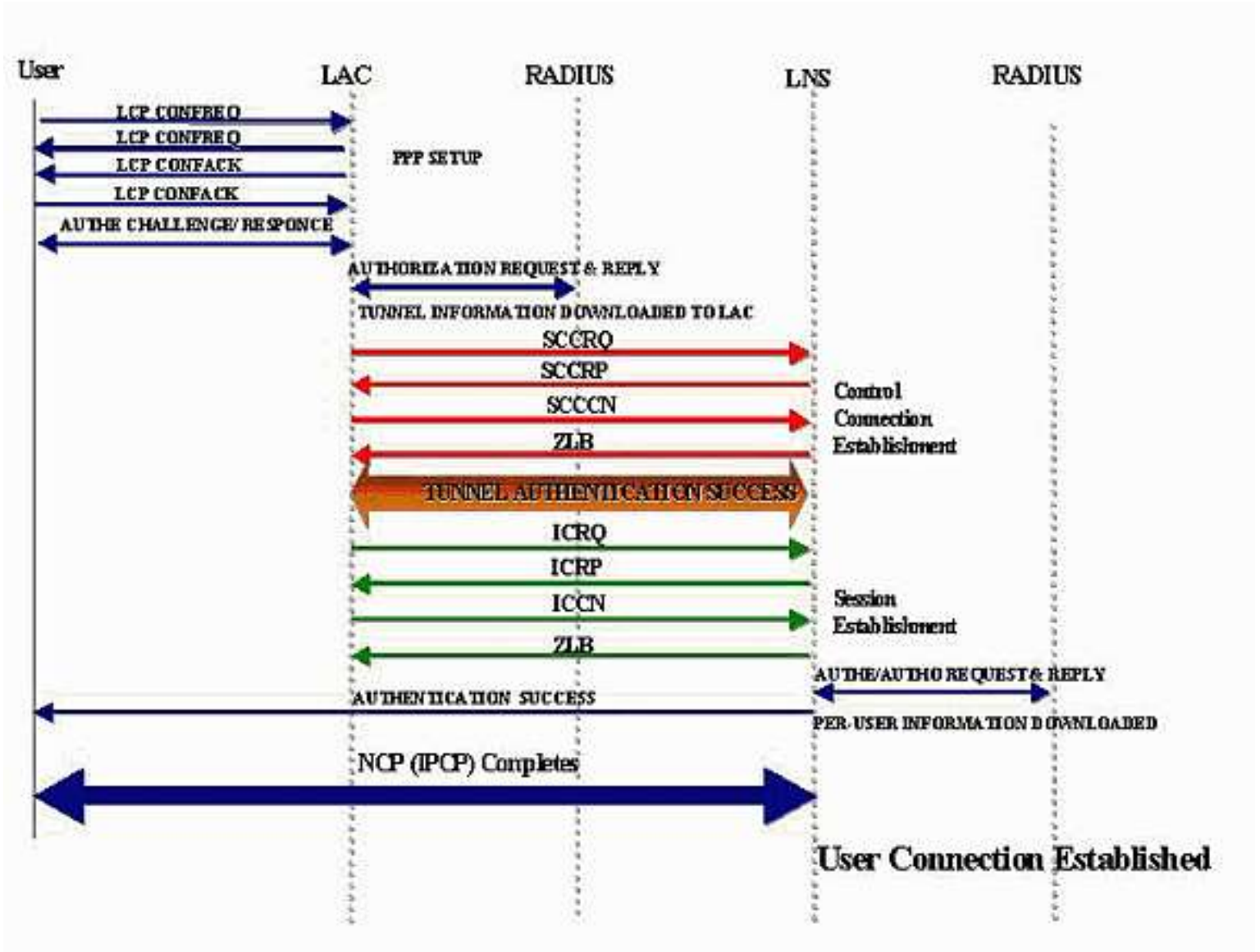
- **Termination of layer 3 (IPv4/IPv6) in a VRF corresponding to retail ISP**
  - Can be done for both DHCP and PPP

L2TP tunneling

- The Layer 2 Tunneling Protocol (L2TP) is a standard protocol for tunneling L2 traffic over an IP network. Its ability to carry almost any L2 data format over IP



L2TP connection establishment



BRAS functionalities and performance to be considered

- Call setup rate
- Number of concurrent sessions
- PPP termination in different routing instances
- Ingress & Egress policing
- QoS profile attachment
- Subscriber authentication (PAP, CHAP) & authorization using miscellaneous radius attributes, circuit-id
- Radius & different local pool IP address management
- Accounting (Radius)
- LI support ?
- Redundancy & High availability scenarios
- DHCP local-server/relay/relay-proxy/rebind subscriber management/option82
- Interopability with PE functionality (L3VPN, VPLS, multihoming, etc.)

Distributed versus Centralized Models

- Standard centralized option based on L2TP to allow hand-off to other ISP
  - Clear functional split between access provider and service provider. Reuses of existing infrastructure at ISP
    - RADIUS authentication / accounting, easy inter-provider accounting
    - PPP session monitoring
    - Each party needs to handle just its own resources
  - Each party needs to handle just its own resources:
    - Devices
    - IP addresses
- But
  - Dedicated powerful HW needed
  - Not optimal traffic flows
  - Inefficient for multicast applications due to tunneling
  - QoS handling is more difficult
  - Potential MTU size problems

Distributed versus Centralized Models

- Terminate subscriber session at distribued POP location and use other hand-off technologies:
  - MPLS VPN per ISP
  - Virtual Router and/or L2 traffic separation
- Obviously solves some/most of the disadvantages, but:
  - ISPs usually are very reluctant to give away control over subscriber (often, not even allow for RADIUS proxy)
  - ISPs typically do not see the individual subscriber interface anymore only aggregate of all user traffic
  - Does not allow the ISP to offer VPN services
  - Needs ISP to change his back-end office to improve the situation of access provider, who is a competitor typically
  - May result in very inefficient IP address pool splitting
  - May result in massive routing activities

Integrated Edge and Universal/Unified Edge

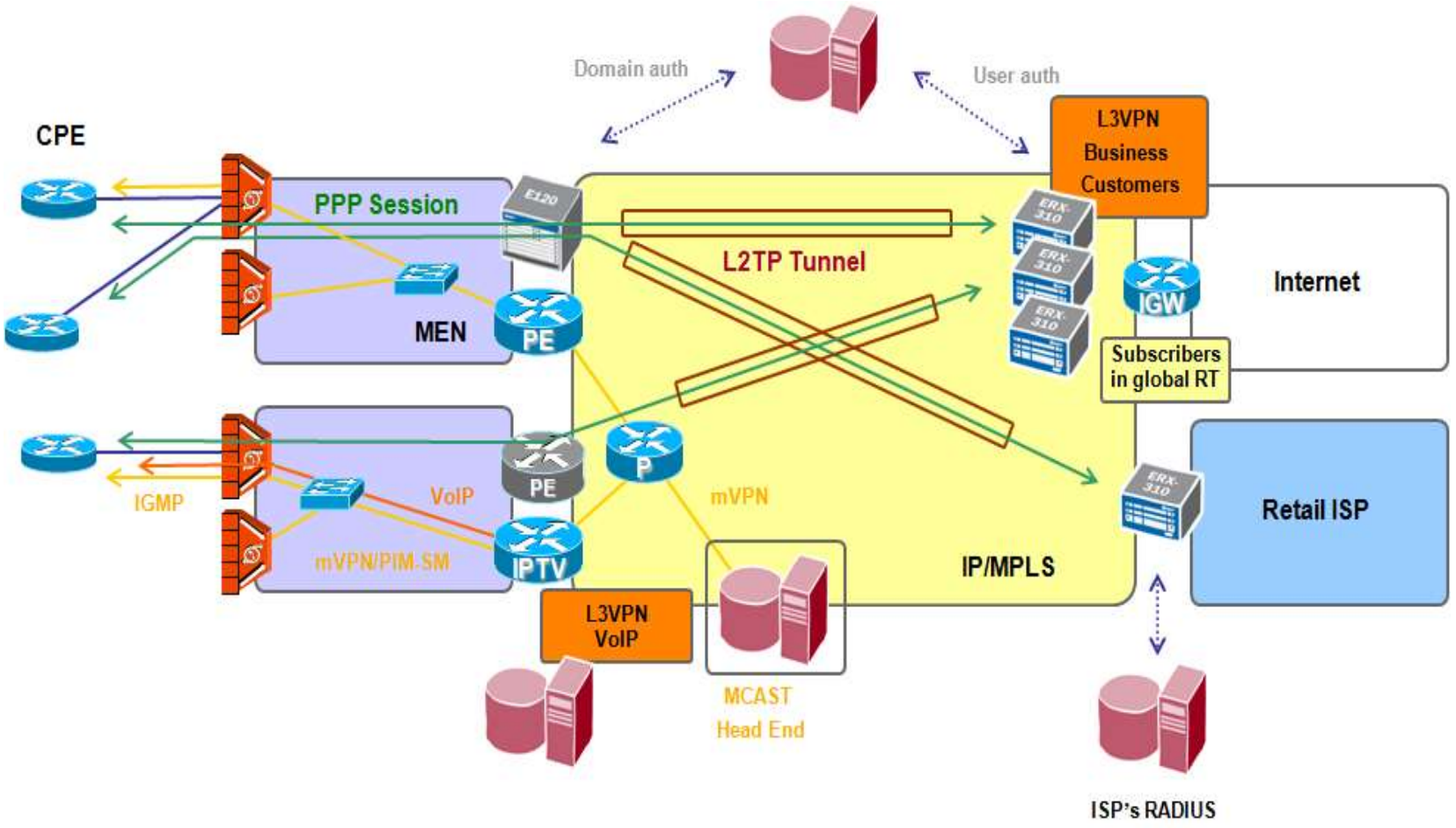
Integrated Edge

- Access agnostic to support all types of access technologies into a single access network
  - Multi-play service integration for VVD
  - DHCP and PPPoE
  - ATM and Ethernet access services

Universal/Unified Edge

- Enable true convergence of wireline and mobile edge without compromising on services or performance
  - Residential BRAS & business MSE
  - Aggregation, Transport, Backbone, Peering
  - Possible mobile gateway – 3G/LTE

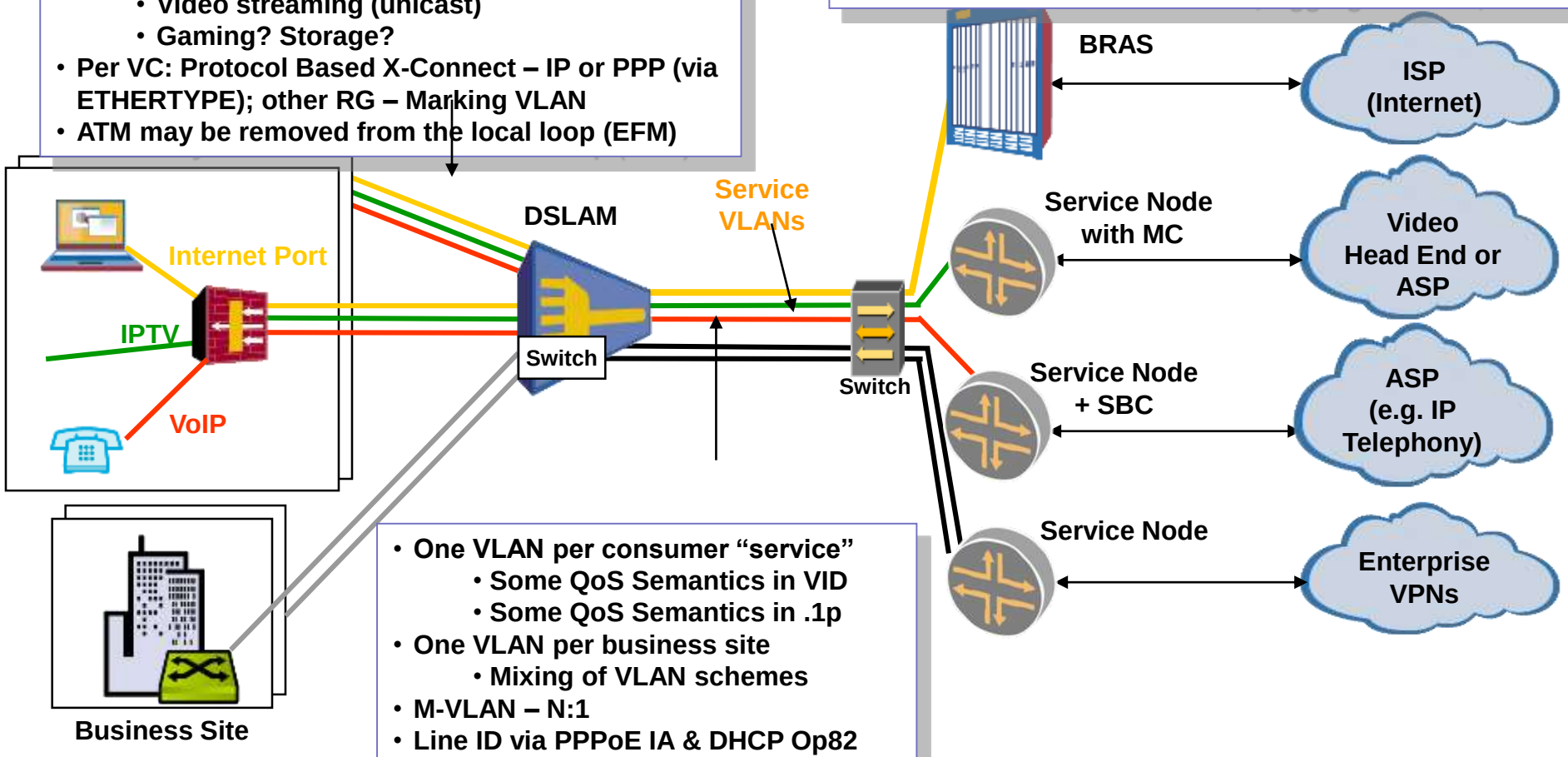
Wholesale model example



Triple Play - N:1 VLAN Solution

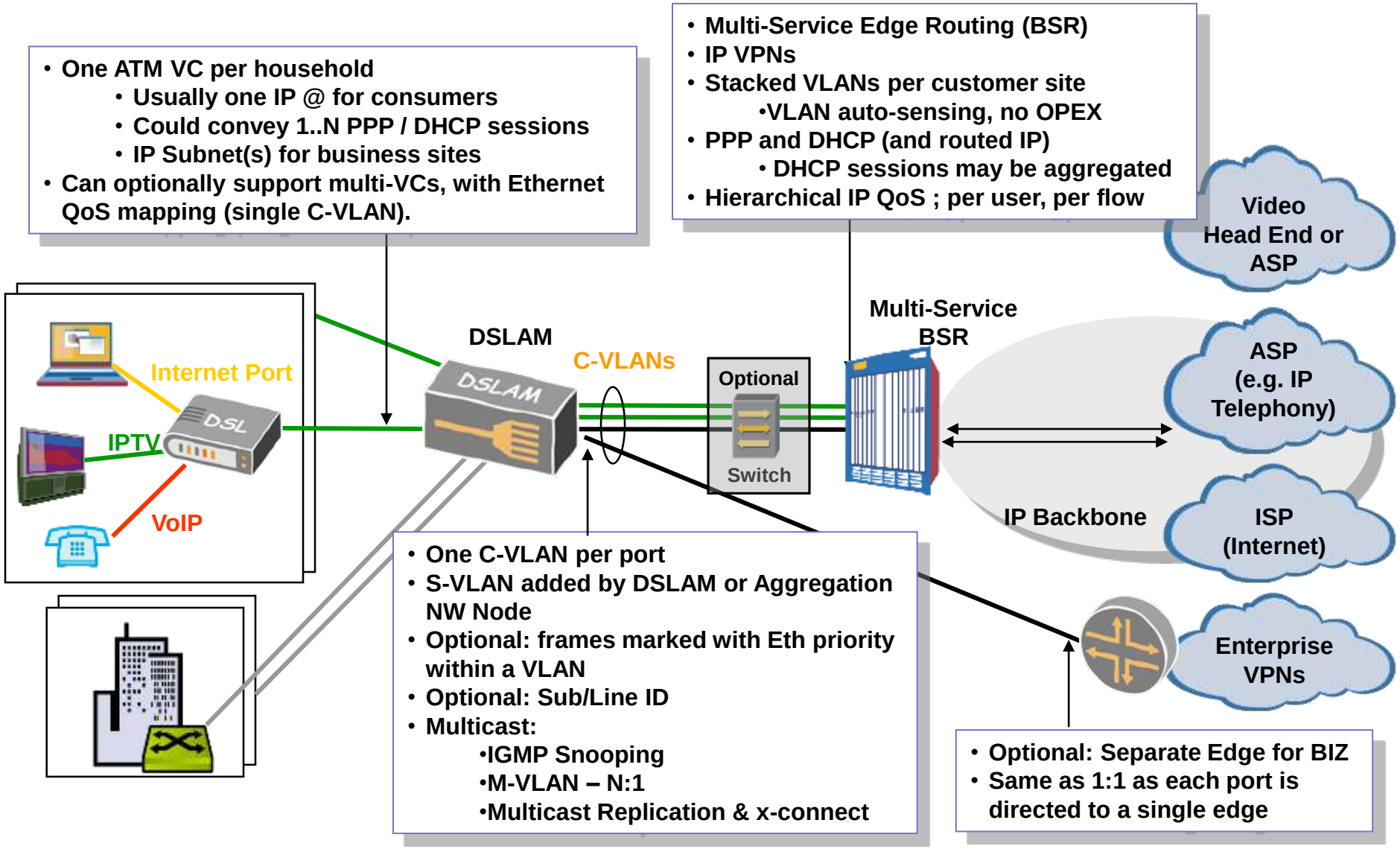
- One or more ATM VC (and IP@) per service
  - Internet or VPN Access
  - IP/Video Telephony
  - Broadcast TV
  - Video streaming (unicast)
  - Gaming? Storage?
- Per VC: Protocol Based X-Connect – IP or PPP (via ETHERTYPE); other RG – Marking VLAN
- ATM may be removed from the local loop (EFM)

- Multiple Service Nodes or “Broadband Gateways”
- QoS architecture: non standard H-QoS, DiffServ++
- SLAs
- Lawful intercept per BNG
- Security & OAM challenges (see other slides)
- Provisioning Overhead on AN, Aggregation NW, BNG



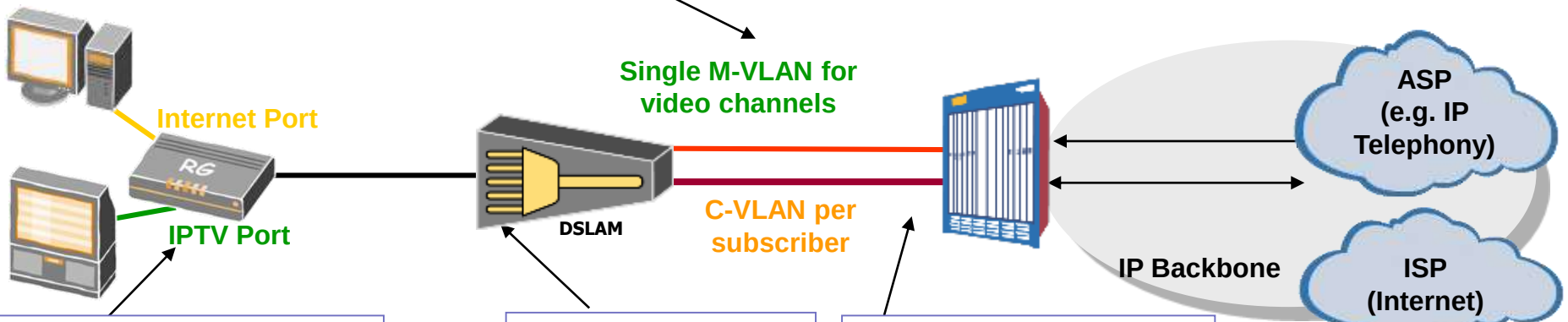
- One VLAN per consumer “service”
  - Some QoS Semantics in VID
  - Some QoS Semantics in .1p
- One VLAN per business site
  - Mixing of VLAN schemes
- M-VLAN – N:1
- Line ID via PPPoE IA & DHCP Op82

Triple Play - 1:1 VLAN Solution



Multicast overview for 1:1 model

- Single M- VLAN for all requested channels, i.e.: M-VLAN carries the channels actually requested or static broadcast subscription of all mcast groups.



- CPE may provide a single VC connection between home and DSLAM
- IPoE (video/IGMP-Proxy)

- Performs Transparent IGMP Snooping. MAC filters and multicast replication

- IGMP joins received on subscriber interface
- Adjusts (unicast) VLAN shaper in QoS h-scheduler to reflect MC traffic

Thank you