DSL Forum

Technical Report

TR-056

(Formerly WT-075v5)

Network Migration

February 2003

ABSTRACT:

This document describes possible network evolution scenarios for service provider access networks incorporating DSL. Different service providers will have different legacy systems, regulatory and competitive environments, broadband strategies and deployment timescales. Hence it is not feasible to make all encompassing recommendations for all possible network evolution scenarios. This document seeks to capture the drivers that may lead a service provider to consider a particular evolution path. It then presents various technical options together with the salient features, advantages and disadvantages to assist service providers in forming evolution plans for an access network that will incorporate DSL. It is hoped that this working text will serve as a useful reference text for both the technical and marketing professionals in the DSL Forum. The Architecture & Transport WG may later choose to explore one, two or several of the key scenarios in further detail, possibly by development of specific TRs.

TABLE OF CONTENTS

1. STATEMENT OF PROJECT

The objective of this project is to capture a range of possible DSL network evolution scenarios for a set of defined initial and proposed target network scenarios, identifying the key issues associated with each option. It will also describe related technical issues that may impact the deployment of a next generation DSL access network. This working text leverages off TR-04 and should be considered an update which considers possible market / industry future trends.

The scope of the project is any access network migration scenarios that would involve use of ADSL, DSL-lite, SHDSL or VDSL on a customer's line in either the initial or proposed target network scenarios.

The primary focus is ADSL, SHDSL and VDSL technologies and the networks that support them. However, to complete the picture of evolution scenarios, other xDSL technologies are not specifically excluded.

The approach taken is that for each evolution situation, there exist several attributes:

- Starting network scenario
- Proposed target network scenario
- Drivers (factors that will initiate and influence the evolution)
- Options (including advantages and disadvantages)

Each evolution situation forms an individual sub-section within this Network Evolution Text. In addition generic factors influencing evolution are also described.

2. Factors Influencing the Evolution of the DSL Network

The context of this working text is to describe possible evolution scenarios for DSL access networks. If the reader is attempting to evaluate migrating to DSL from a non-DSL based network, then TR-04 is considered a prerequisite to this working text. Evolution of DSL networks is driven by several factors: a) Business case to deploy/maintain b) Services support/creation. The rest of this section is dedicated to capturing some of the catalysts for DSL network evolutions.

a. Current generation systems may not have enough capacity to scale to the bandwidth demands of services being researched for the future.

b. Current generation networks/systems may not have the resiliency to offer 5 9s type services.

c. Services provided require several systems that each provide a function. The number of systems required for service is burdensome from a maintenance perspective, and a reduction in the number of elements should reduce management system burden.

d. Current systems / networks may not allow providers enough flexibility to address the services that are being demanded or created by their customers.

e. Current systems / networks may not adequately address providing DSL to all types of access lines that exist in a carriers network.

3. CLASSIFICATION OF MIGRATION OPTIONS

Through contributions the Architecture & Transport WG has produced the following list of possible evolution scenarios for study. These scenarios are not classified or prioritised in terms of their perceived relevance to shorter and longer term decisions of telcos. They are presented as a list of possible options for the consideration of the DSL Forum membership.

Starting Network Scenarios	**Proposed Target Network Scenarios**	**Contribution Reference**	**Details in Section**
ADSL from CO providing Internet Access.	DSL supporting Content Distribution Networks	DSLForum2001-266	4
ADSL from CO using ATM/BAS infrastructure	Access Node with Integrated Routing and Multicast Support	DSLForum2001-266	5
ADSL from CO / NGDLC	Access Node with integrated voice line circuits and loop voice gateway	DSLForum2002-216	6
ADSL from CO	DSL Bonding	DSLForum2001-496 + DSLForum2002-034	7
ADSL from CO using video server without multicast / multipoint	Broadcast TV using IGMP	DSLForum2002-061, DSLForum2002-211	8
ADSL from CO using ATM/BAS infrastructure	Multicast and PPP based Access Network Scenario	DSLForum2002-106	9
ADSL from CO using ATM/BAS infrastructure	QoS IP Services through RSVP over ATM SVC in DSL Network	DSLForum2002.141	10
ADSL from CO using ATM/BAS infrastructure	MPLS Generic Architecture	DSLForum2001-447	11
ADSL from CO using ATM/BAS infrastructure	MPLS/ATM Layer 2 Cross Connections	DSLForum2001-449	12
ADSL from CO using ATM/BAS infrastructure	MPLS VPNs	DSLForum2001-467	13
ADSL from CO using ATM/BAS infrastructure	Ethernet Transport in the Regional Broadband Network	DSLForum2002-196	14

Table 1 : Classification and Prioritisation of Identified Migration Paths

The following sections contain descriptions of a number of possible DSL network evolution scenarios. Each possible network evolution scenario section follows a standard document format which is outlined as follows: Each possible migration option is defined in terms of the starting network scenario and the proposed target network scenario. The drivers that will initiate and influence the migration towards the proposed target network scenario are discussed and the technical options to facilitate the network migration are then presented including their advantages and disadvantages.

4. DSL in the Context of Content Distribution Networks (CDNs)[1]

4.1 Starting Network Scenario

The assumed initial architecture is based around an ATM VC connection from the customer's DSL CPE through the Access Node, across the WAN backbone to an aggregation device (sometimes referred to as a Broadband Access Server – BAS or L2TP Access Concentrator – LAC or tunnel switch). The aggregation devices terminate the PVC and pass the IP packets onto the service provider over an L2TP tunnel via an IP aggregation link to the service provider's PoP. Note that some services will use PPPoE instead of PPPoA in the protocol stack shown below. Note also that many Access Nodes will include SHDSL line cards as well as ADSL. Content will often be located in a centralised service provider data centre which an end user may have to access across a national WAN backbone in order to retrieve the content.

The main benefits of this existing architecture and some of the reasons it has been widely adopted are as follows :

For the Network Infrastructure Provider or Telco :

- Enhanced scalability compared to end-to-end PVCs between users and service providers.
- Thousands of customers PPP sessions can be multiplexed to a single tunnel.
- More efficient use of the backbone network resources.
- Enables customers to switch between different service providers.
- PVCs from the Access Node to the BAS aggregator can be pre-provisioned to simplify service activation.The L2TP tunnel from the BAS to the NSP is not restricted to ATM.NSPs do not have to terminate anywhere near as many PVCs.
- Makes it easier for the NSP to effectively terminate connections from several different ADSL access providers.
- Similar processes as to those used by dial-up customers.
- Opportunity to provide usage based billing.
- Efficient use of an NSP's pool of IP addresses.
- Ability to switch between ISP's could also be extended to switch between service classes to the same ISP.

For the End-User

- Can switch between ISPs, without the need for SVCs and associated signalling stacks.
- PPP is already being use by customers for session, authentication and IP configuration management.

Disadvantages:

- The BAS/LAC aggregator device represents a single point of failure affecting many users
- Non-Internet service providers need to be integrated into the service selection process at the customer's premises which needs consideration.

[1] Portions of the material in this section is based upon a presentation at the DSL Forum summit in May 2000 by Nortel Networks

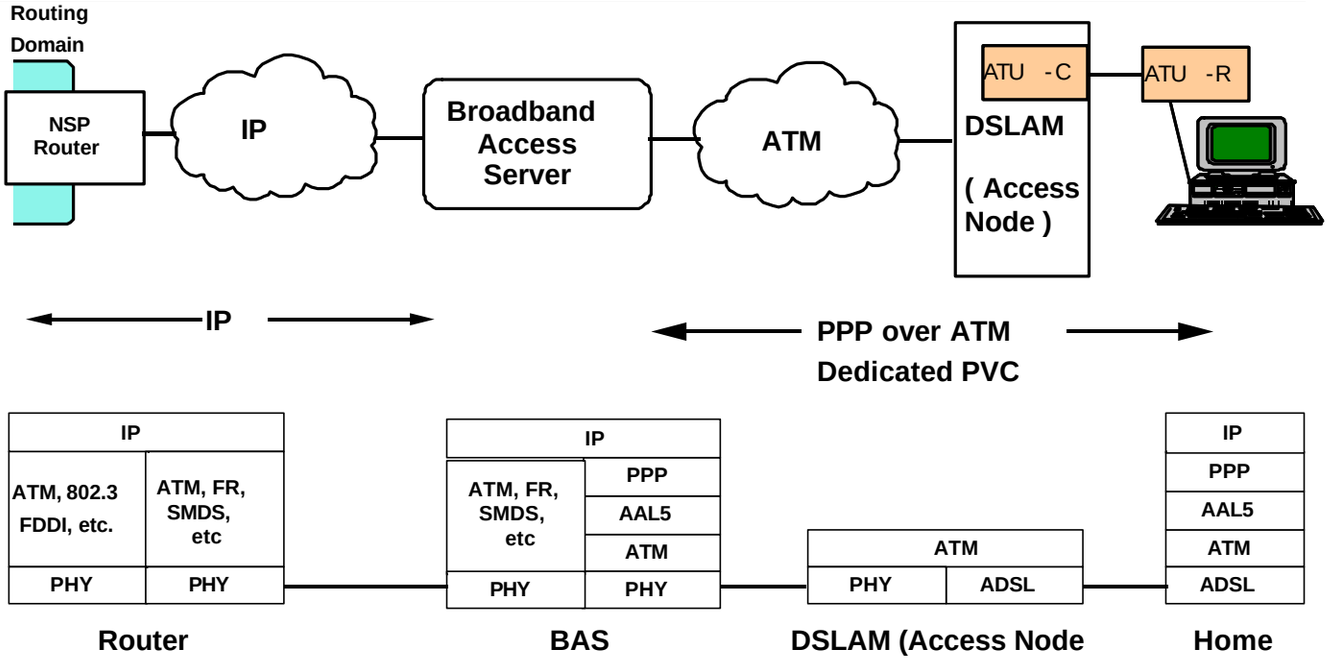


Figure 1 : Standard ADSL Architecture as Deployed 1999 - 2001

4.2 Proposed Target Network Scenario

The proposed target network scenario is as above but with content caches located (increasingly) close to the end user to hold large files and streaming content. The caches could be in the data centres of ISP regional or metro PoPs and ultimately (especially for corporate sites) the cache could be on the customer's network. With significant improvements in storage technology caches could ultimately reside in a DSL CPE gateway for a residential customer. The trend will be for such caches to move closer to the end user. For IP-centric content delivery this trend could necessitate moving of IP routing functionality out of the centralised aggregation device (BAS) and closer to (or included within) the Access Node to enable "peer to peer" communication among edge cache storage entities to update each other and allow users to access content from the closest storage device and avoiding "tromboning" of IP traffic.

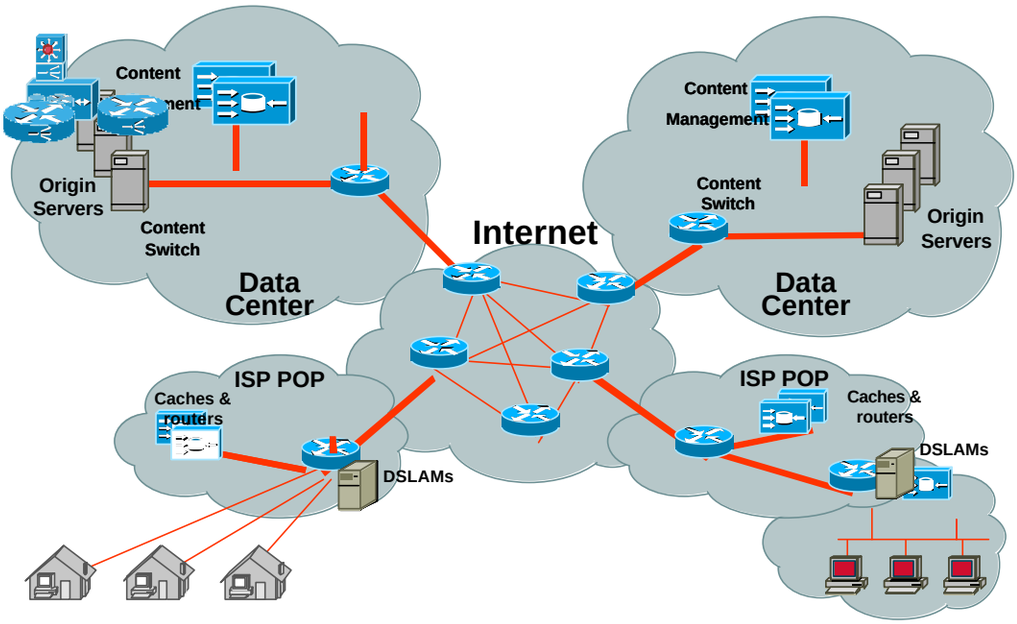


Figure 2 : DSL in a Content Distribution Network

4.3 Drivers

Some of the drivers towards CDNs are:

- Number, frequency, and impact of streaming events is growing
- Content delivery industry is growing and innovating
- Internet technologies will dominate application space, including streaming app
- Video compression technologies continue to improve
- New generation of video servers taking advantage of Moore's law
- The rising threat of cable companies and their ability to offer a video, data, and voice bundle is causing reaction amongst ILECs and DLECs
- Digital Broadcast Satellite has affected user's appetite (and expectations) for channel surfing in the digital video domain
- FTTx is not an easy business proposition (but service usage per household continues to grow)

The value proposition to the various stakeholders is:

- Service Providers: Increases demand and value of broadband access services while increasing bandwidth efficiency
- End-Users: Enhances end-user experience (50%+ decrease in download time)
  Enables new content services
- Content Providers: New delivery channel for content offers

4.4 Options

Key products required to build a content delivery service offering are:

- Content distribution intelligence software
- Content switches
- Large scale caches
- Media servers.

There will be impacts on the network design, specifically:

a) DSL networks are engineered today for ~25 kbps per subscriber; streaming apps drive average up an order of magnitude and higher.
b) Local caching will be required to guarantee a positive user experience and differentiate broadband content.
c) Streaming drives the need to guarantee end-to-end (from head end to home LAN or STB) bandwidth dynamically
d) Service quality will need to be derived from applications, and be compatible with content partners
e) The content network increasingly operates at layer three (IP) and higher, today's DSL networks operate at Layer 2 (ATM)

The delivery of content over a network with DSL access requires the following capabilities:

Content Aware Traffic Engineering

- It includes the ability to recognize when an end user client has requested streaming content. Reading the request and/or destination server address for streaming media and server ID for media type e.g. bandwidth required 300kb/s or 3.5Mb/s.
- To open a path end client to server with the attributes for optimum performance. Translation to ATM pre-provisioned PVC or SVC initiation, or use of MPLS LSP from Access Node or CPE.
- To protect the path from other applications which may contend for the same bandwidth
- To close the path when it is no longer required by the end client

Multicasting

- The ability to replicate non-timeshifted channels on demand for bandwidth savings in the Acess Node WAN. Creation of Multicast 'leaf' in the IP layer in response to IGMP 'join' or proxy into ATM point-to-multipoint, with / without VC merge (see section 8 for detail). This requires signalling protocol functionality.

Multi-Path Customer Premises Equipment / Home Gateway

- The ability to direct specific traffic to designated ports to prevent conflicts on the home LAN

5. Access Node with Integrated Router & Multicast

5.1 Starting Network Scenario

The Access Node connects directly to an ATM WAN which in turn may terminate the ATM PVC and pass the IP packets to the service provider via an "inner" routed IP WAN infrastructure (see Fig.1). An ATM PVC effectively connects from the end user's DSL CPE through to the broadband aggregation device which resides at the boundary of the ATM and IP core backbone WANs. The BAS tunnel switch is potentially a scalability/feature bottleneck and a conservative approach to ATM dimensioning in the backbone could limit QoS capabilities. Multicast routing would be required on a per ISP basis and can only operate at tunnel endpoints (BAS / Access Node).

5.2 Proposed Target Network Scenario

The proposed target network scenario has IP routing functionality co-located with the Access Node or integrated into it. This enables the Access Node to hand-off traffic directly into a fully routed IP WAN backbone using any layer 2 transport (or even without a layer 2 transport such as "IP over glass"). This avoids the need to extend ATM VCs across the WAN from the Access Node to the BAS aggregation device. It may also give options to reduce the issues associated with the need to bind together signalling and QoS mechanisms between the IP and ATM WAN layers.

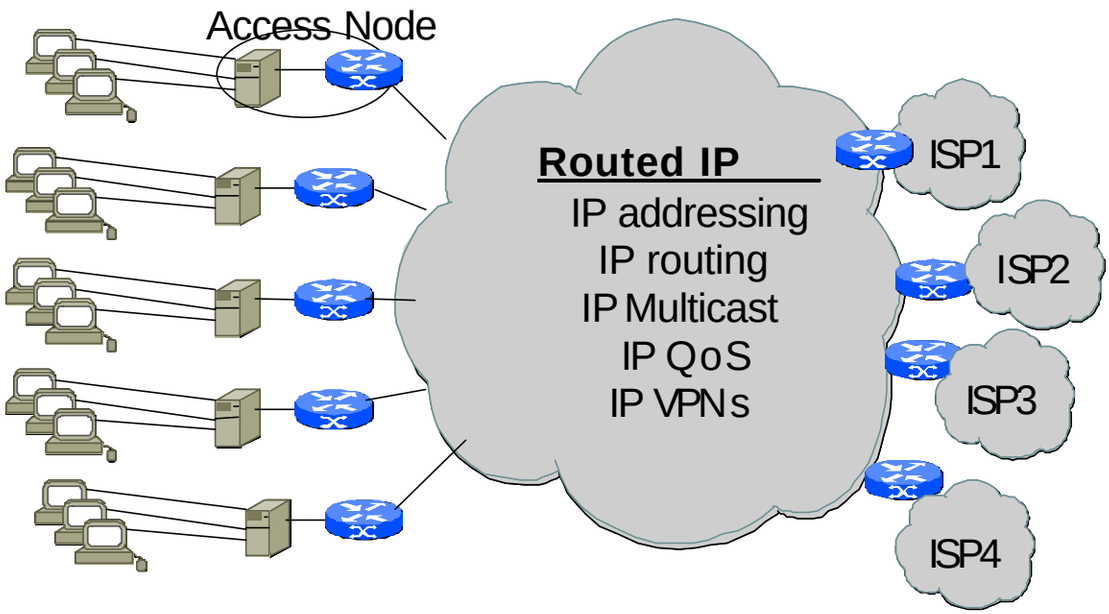


Figure 3 : Access Node with Colocated Router Connecting to IP WAN

The local Access Node router could provide; DHCP relay agent, NAT, dynamic firewall, local connectivity, IP QoS control capability, multicast benefits, admission and local policy control point

5.3 Drivers

With the existing internet access DSL architecture, a NAP (ILEC or DLEC) usually sells either an ATM VC or a VC/tunnel hybrid to service providers. In many cases, the service provider will be providing an IP address to the end user which means that multiple home hosts connecting to different service providers can be complicated because of the way in which PPP is used between service providers and their end user customers including handing out IP addresses in some cases. Areas of concern are complexity in the home network routing (potential tromboning of local traffic) as well as potentially introducing security holes. Using a point-to-point ATM circuit across the WAN to the aggregation device (BAS) in a classical client-server approach will restrict the full potential for scalable and efficient multicast routing, for example for conversational services or multi-player gaming. For some applications e.g. Broadcast TV Point-to-multipoint ATM and IP multicast can provide more scalable solutions. For other service types access node switching and routing makes sense. In addition classifiers for IP QoS and for policy routing features may be desirable for real-time IP applications and admission control.

With the PPP connection between an end user's host PC going across the WAN to the ISP, all traffic generated in the home has to go all the way across the WAN to the ISP (see Figure 4) even if it then has to be tromboned back to a local peer (e.g. in the same town connected to the same Access Node or even in the same building). Applications such as gaming, VoIP and Web Pages on home servers can generate local traffic. A router at the Access Node saves WAN capacity, increases multicast gain and decreases latency. Meshing of the local Access Node routers further increases availability and bandwidth gains. The implications of meshing the local Access Node routers in the presence of local traffic should be considered.

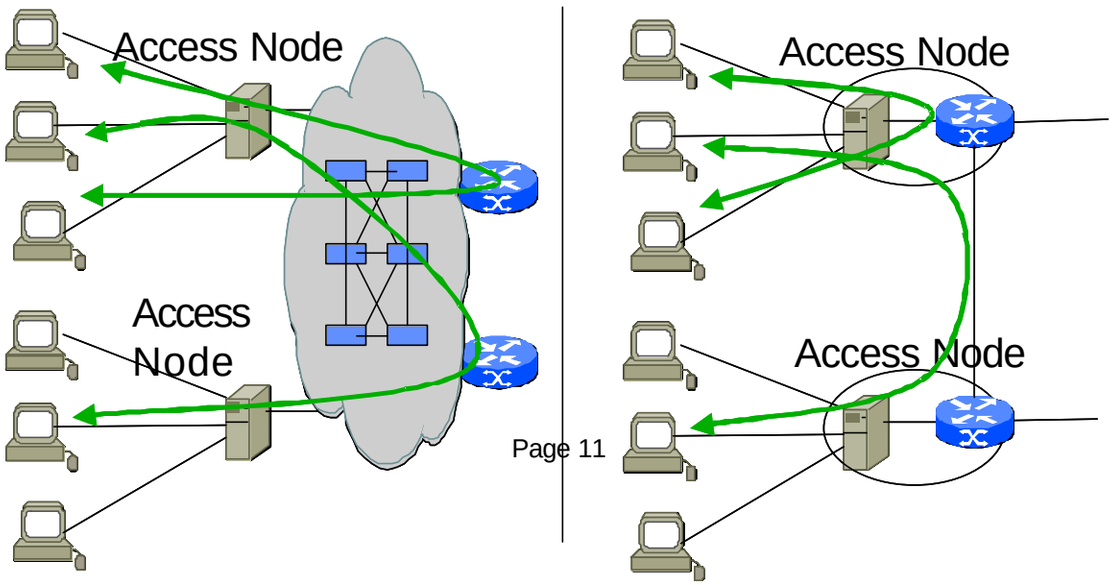


Figure 4 : Effect of Tromboning of Local Traffic Solved by Access Node Routers

Other benefits include:

Service Providers:

- Basic IP connectivity management offerings
- Scaleable network for real time services
- Efficient streaming of media

End-Users/ Content Providers:

- Ports of various types can be purchased depending on location and quality.

Potential impacts are:

- Complicates having multiple hosts connecting to different service providers.
- Adds complexity in home network routing (e.g requires additional multicast protocol(s) and policy).

- Introduces additional security requirements.
- Pre-planned, reserved, high priority routes may be required to satisfy guarantees.
- DiffServ and ToS marks may need to be added to provide for relative QoS guarantees.
- Absolute QoS guarantees may need dedicated signaling and path set-up.

5.4 Options

Physically the options are whether to co-locate the router with the Access Node, integrate it into the Access Node or have it logically associated with a Access Node but physically separate The appropriateness of collocating routing functionality at the same physical site as the Access Node may depend on the proportion of local traffic (which could be peer to peer) which is expected. In the early days when this may be low, it may be better to have a router on the outside edge of the core backbone network but associated with a few Access Nodes and connected to them by fast pipes such as large (non-blocking?) ATM VPs. This is a classic “transmission versus switching” architectural trade-off. Additional routers could then later be added at the Access Node end of the ATM VPs as local traffic grows. These

steps allow a smooth evolution from today's DSL architectures since ATM VPs are already connecting the Access Nodes to the WAN. The VPs may need to be re-dimensioned and the associated "per-user" VCs altered to turn the VP into a single "fast packet pipe" containing all Access Node users data as a packet stream. Internal VCs within this "Access Node to router PoP VP" could be use for traffic management such as having a VC/VP per service provider or VC/VP per traffic class. The router collocated with the Access Node could terminate the per-user VCs on its access interface and then route the packets into the per ISP or per CoS VC/VPs on the WAN interface. The router could provide downstream shaping into the per-user VCs. An additional step in the evolution could be to remove the aggregation BAS device and perform AAA functions at the Access Node router and ISP peering points. The local authentication and accounting enables users to only be charged for packets delivered to them over the access and not for those that may have been dropped within the backbone network on their way to the Access Node. In addition to this improved accuracy, the local approach to AAA may also have benefits for multicast, QOS, VoIP, and VPN policy evolution.

The second option is around the issue of controls and administration of the IP backbone WAN. Where does the infrastructure provider responsibilities end and the service providers begin? With a coherent addressing and routing plan, an infrastructure provider could create an IP network into which DSL end-users and service and content providers can buy ports of various types depending on location / quality. This infrastructure provider's IP network could be network layer only without providing 'services' to customers apart from basic connectivity management. The service providers benefit as the infrastructure provider then provides broadband IP interconnect and a single port to reach "all" of its DSL customers and potentially those on other connected networks via peering arrangements. With a coherent domain the infrastructure provider can provide value-add capability to service providers such as IP QoS, multicast, VPN and admission control which may be more cumbersome in the PPP/aggregator/tunnel model.

An issue with the fully routed approach to Access Node WAN hand-off is scaleability of the network for real time services. QoS constraints could potentially dictate that for any given session all packets must be routed over the same path. This could not be guaranteed in a fully routed network, therefore nailed up (pre-planned) routes may be required if excess capacity will not solve the problem with adequate guarantees. A second problem is that connectionless routed networks have no call admission control (CAC) function. If parts of the network are dimensioned for N users and N+1 users try to use it, then all of these N+1 users will suffer a degree of degradation. This could be a real problem since network hot spots will inevitably occur either at the edge or in the core. Relative QoS guarantees can be given for such a network via the use of DiffServ and ToS marking with actual performance within a traffic class being impacted by the mix of traffic on the network (i.e. doesn't work if everything is marked as high priority). However absolute QoS guarantees such as bounds on jitter may need dedicated signaling and path set-up (such as via RSVP) with associated scalability issues to consider (see section 10).

6. Access Node to IMAP Network Migration (integrated voice line circuits and loop voice gateway)

6.1 Introduction

This section describes the requirements for a possible DSL network migration from the NGDLC (Next-Generation Digital Loop Carrier) or DSLAM types of Access Node to a next-generation access network. Today's NGDLC support IP / ATM transport capabilities while providing traditional voice, analog/digital special services as well as business and consumer DSL terminations. Today's DSLAM is an Access Node similar to NGDLC with the major exception that it does NOT support traditional voice transport across the "U" and "V" reference points using TDM within the Access Node. The NGDLC / DSLAM can be located either at the CO or at the remote site. This section focuses on describing the migration of the capabilities of today's Access Node to an IMAP (Integrated Multi-Service Access Platform) or an Access Gateway in the NGAN (Next Generation Access Network).

6.2 Starting Network Scenario

The Access Node / NGDLC is currently deployed in the network as shown in the following network diagram. In some cases, the Access Node / NGDLC can be thought of as a "distributed Access Node" since it can aggregate DSL traffic at a remote location and provide transport to bring back the traffic to the CO or provide the ability to directly bring data traffic into an ATM switch. The following figure depicts the starting network scenario in which an Access Node / NGDLC provides "distributed Access Node" functionality by having some parts of the Access Node / NGDLC in the CO and other parts at the remotes closer to the subscribers.

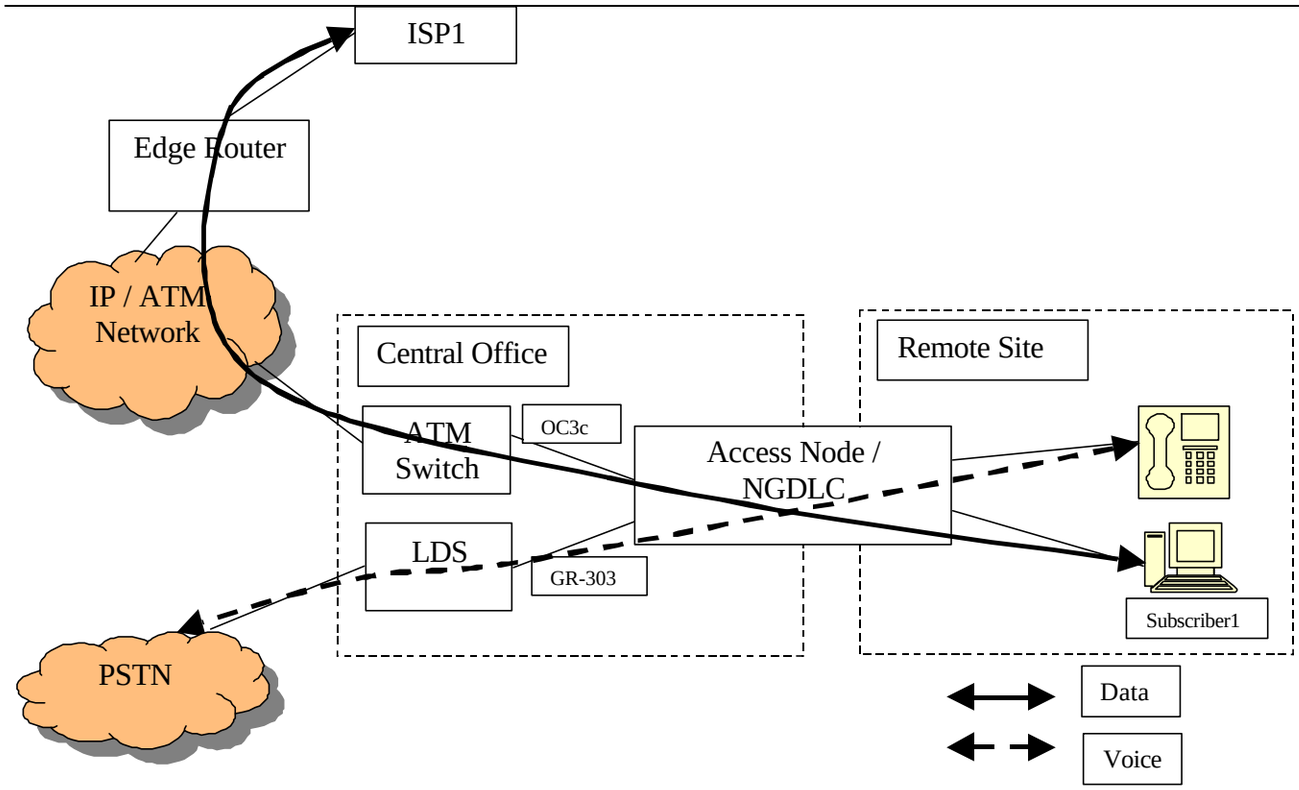


Figure 5 Starting Network Scenario

6.3 Proposed Target Network Scenario

In this proposal the intelligence is moving from the core network to the access/edge of the network. In this proposal the network evolves to packet-based technologies (i.e. IP and/or ATM), the traditional PSTN (Public Switched Telephony Network) is also evolving. This includes separation of call control and bearer. The Access network is also evolving.

The following figure depicts the proposed target network scenario, which shows an evolution of the Access Node to an Access/Media gateway that communicates with a SoftSwitch/MGC using separate control and bearer channels. The control channel can be inband using IP/ATM or out of band using IP/Ethernet. The bearer channel can be either IP or ATM. If the bearer is transported over an ATM network, the Access/Media gateway may support circuit emulation service over AAL1 or AAL2 (e.g.TR-043 Annex A or other standards that meet the proposed voice requirements of the service provider)

This proposed architecture can work with or without Combo line cards. Combo line cards meet both voice and ADSL line circuit requirements on the same line. This is accomplished though incorporation of splitter functionality onto the linecard which terminates POTS and converts it to AAL2 / packet for transport across the regional broadband network.

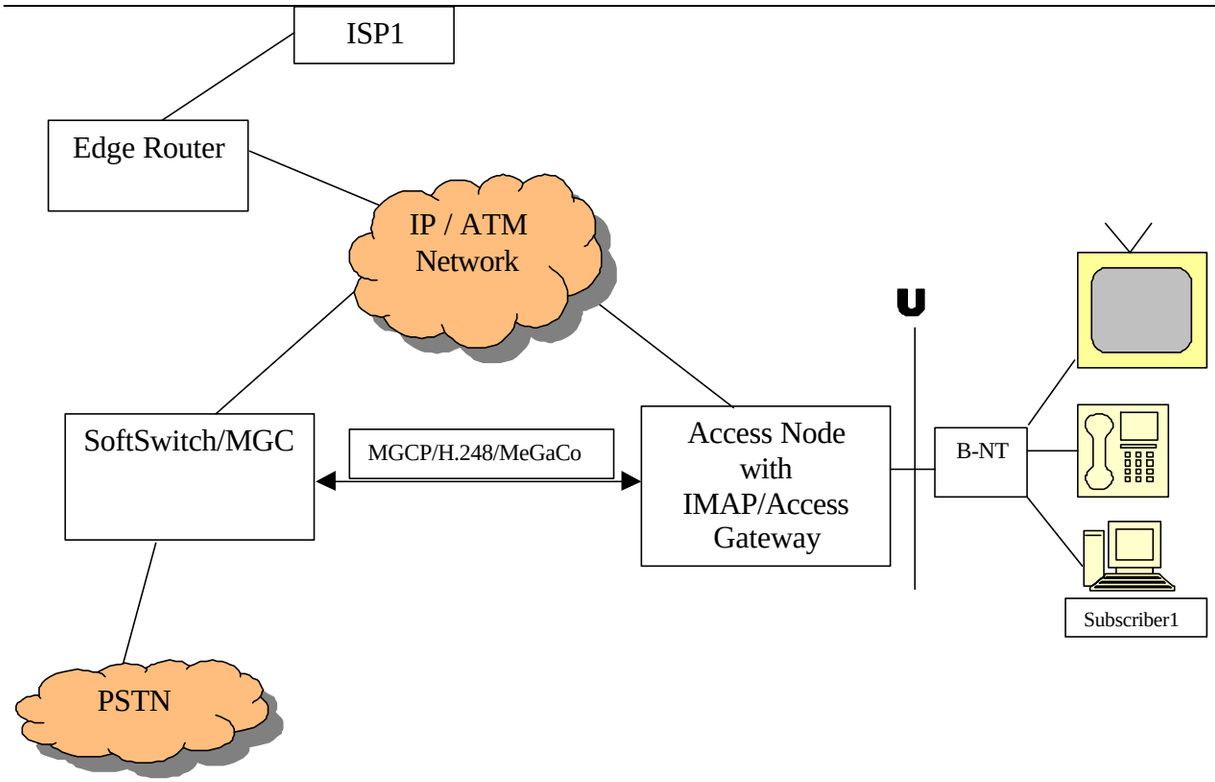


Figure 6: Target Network Scenario

6.4 Drivers

The key drivers for the migration of Access Node to the IMAP / Access Gateway type of network are as follows:

- Move to Packet (ATM/IP) based voice away from TDM based voice
- Can reduce (re)wiring efforts via use of Combo (voice+ADSL on same wire) cards – particularly useful in copper centers where high DSL penetrations and uptakes are expected
- The separation or decoupling of bearer and control channels
- Voice / Video intelligence moves from the core into the Access Node to improve, enhance or solve scalability issues for large ATM access networks
- Voice / Video intelligence is offered from the Access Node to enable new and enhanced service offerings and improved performance
- Potential Integration of multiple functionalities within a single network element as it fits into Service Providers' network and operations models.

6.5 Options

There are two physical options for evolving the Access Node to a Access Node with IMAP (Integrated Multi-Service Access Platform) capabilities such as an Access/Media Gateway to support the migration of the existing voice network

from circuit to packet. Note that these two physical options are not necessarily distinct enough in that one can choose to do either or a combination of the two depending on the migration strategy.

The IMAP option involves the integration of additional functionality into the Access Node. The evolution of today's Access Node to IMAP would require the new platform to support the bearer traffic to be transported over IP or ATM core networks. The IMAP optionally also integrates Edge router functionality in order to support IP services and routing functionality. The IMAP resulting from evolution of the Access Node supports all of TDM, xDSL, video or other IP services.

The Access/Media gateway evolution option requires the Access Node to support the separation of control and bearer by supporting control protocol such as MGCP or H.248/MeGaCo and ATM or IP bearer interface for transporting the bearer traffic over ATM or IP network, respectively. The Access/Media Gateway can provide termination for a variety of line circuits most notably POTS and DSL.

6.6 Conclusions

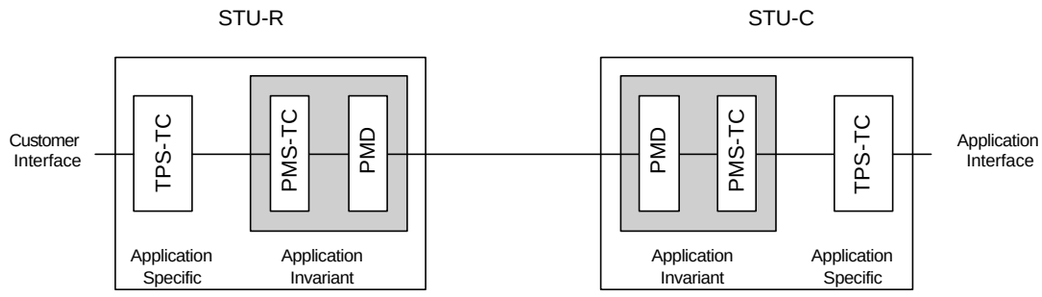
In conclusion, it is recognized that traditional DLCs, NGDLCs and DSLAMs are types of Access Nodes that exist in service providers' networks today. This proposed migration towards the NGAN (Next Generation Access Network) will allow DLCs and DSLAMs to evolve into an IMAP or an Access/Media gateway device that provides voice, video and data services over IP or ATM transport network. The IMAP or the Access/Media gateway device will need to support control/signaling protocols such as MGCP / H.248 for next generation voice support. This migration strategy will allow service providers the flexibility to evolve to support multiple services over different regional broadband network technologies and to offer additional value added services.

7. DSL Bonding

This section summarizes requirements and technology alternatives for bonding DSL lines on the "U" interface. The section focuses on the dataplane aspects - management plane issues are not discussed. The intent is to provide an overview of related standards and techniques and to provide a preliminary discussion of DSL-specific configurations.

7.1 Starting Network Scenario

Operators have typically provided business customers with data and voice services via DS1/E1 or DS3/E3 lines. SHDSL is being used from an ATM mode DSLAM or the transmission of TDM directly over the DSL PHY. In the case of an ATM based transport the starting network scenario pictured below the TPS-TC would be an ATM TPS-TC up to a DS1/E1 equivalent bandwidth size using one SHDSL line as the physical media dependent over copper Figure 7.



Acronyms
STU-R SHDSL Transceiver Unit at the Remote End
STU-C SHDSL Transceiver Unit at the Central Office
TPS-TC Transmission Protocol-specific Transmission Convergence (TC) Layer
PMS-TC Physical Medium Specific TC Layer
PMD Physical Media Dependent

Figure 7: Starting network scenario: No DSL Bonding

7.2 Proposed Target Network Scenario

Operators have typically provided business customers with data and voice services via DS1/E1 or DS3/E3 lines. Customers requiring intermediate service rates typically have had to choose between the limited options above. For service providers wishing to provide a flexible service offering within this "bandwidth gap", bonding of multiple DSL lines presents a viable proposal worth careful consideration.

In addition to the higher access rates, the DSL bonding proposal enables "standard" or increased bandwidth to customers located beyond the regular reach of DSL modems. This feature is based on rate-adaptiveness of DSL technologies, for example G.SHDSL or indeed any rate adaptive DSL when bonded.

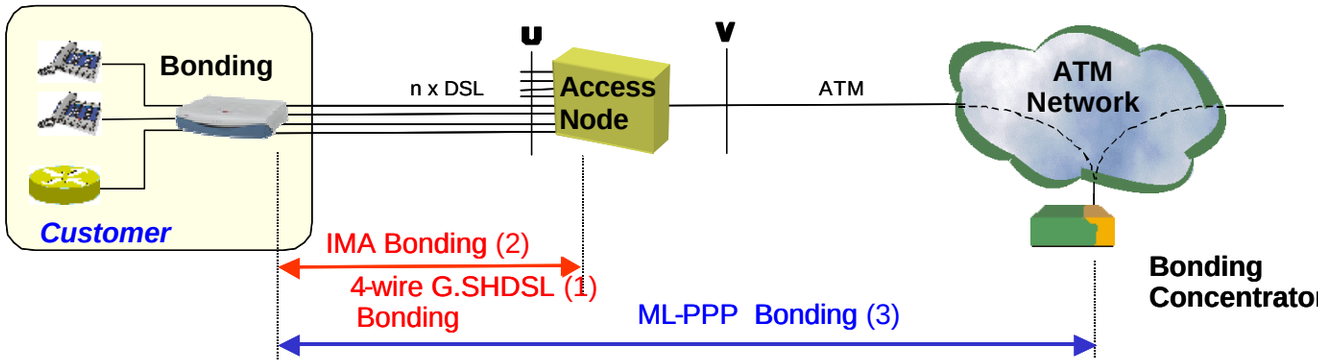


Figure 8: DSL Bonding options across an ATM RBN

In addition to the figure above bonding can also be between a hub access node and a remote MTU. The MTU bonding scenario is described and graphically depicted in section 7.3.

Alternatively, DSL bonding proposals could possibly be implemented over TDM (SDH/Sonet) infrastructure with DSL modem rack equipped with standard E1/T1 interfaces. However, this alternative approach involves many more changes from the starting network scenario based on ATM (i.e. TR-025) including architecture changes at the "U", "V" and "A10" reference points .

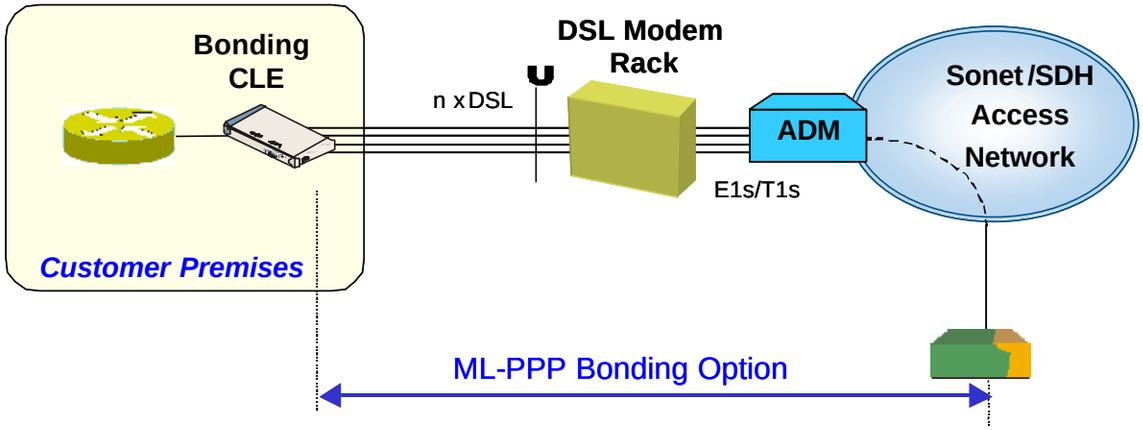


Figure 9: An example of DSL Bonding using ML-PPP across an all TDM network

DSL Bonding could be implemented with several standards-based techniques. The following three techniques for DSL bonding will be discussed in some detail:

- **[Technique 1] PHY-layer bonding** [1]. PHY-layer bonding, applicable to SHDSL, has advantages of simplicity and protocol transparency. However, it is relatively inflexible and it is currently limited to 2-pair bonding.

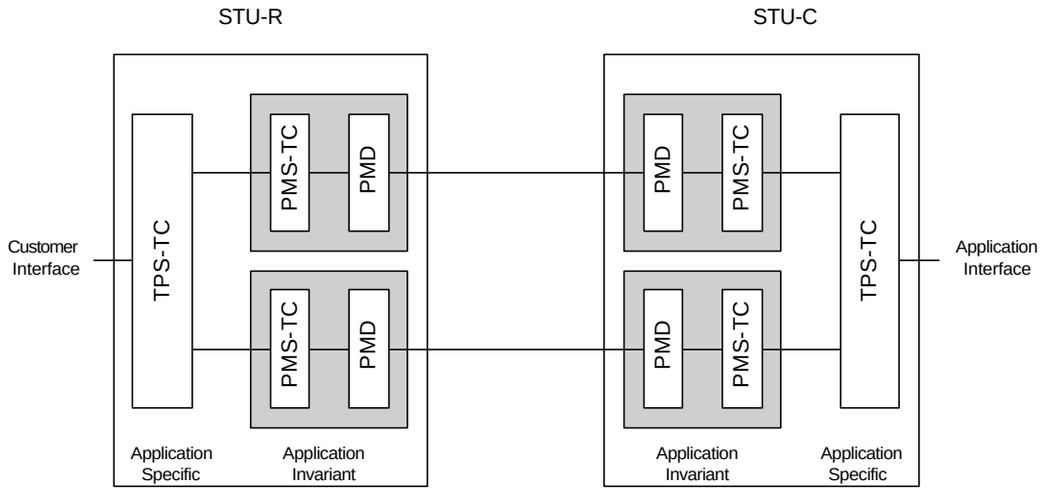


Figure 10: DSL Bonding using SHDSL PHY layer

- **[Technique 2] Inverse Multiplexing for ATM (IMA)** [3]. IMA may be provisioned to group up to 32 individual DSL lines together to form a single, aggregated ATM transport link. IMA requires an intermediate protocol layer between the PHY and ATM layers that must be implemented at the CLE and within the service provider's Access Node. Although IMA introduces some operational overhead, from a datapath point of view the IMA sublayer is relatively transparent to the ATM and upper layers.

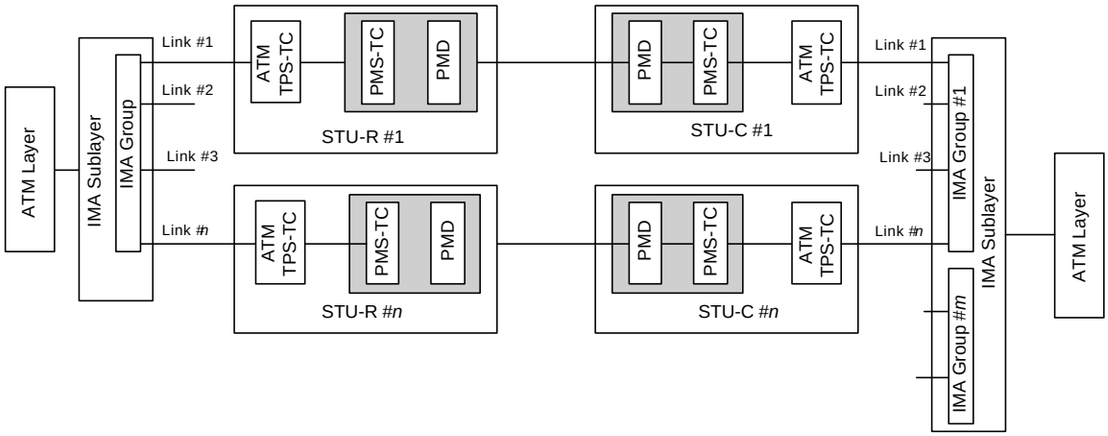


Figure 11: DSL bonding using IMA

- **[Technique 3] Multilink PPP** [5]. ML-PPP is another candidate technique for providing an aggregated transport link. In many cases, PPP already forms part of the IP-over-DSL stack. Like IMA, ML-PPP bonding must be implemented at the CLE. Within the operator's network there are a number of points where ML-PPP can be implemented - at the service aggregation point within the Access Node, or in an associated LAC (L2TP Access Concentrator), RAS (Remote Access Server), SMS (Subscriber Management System), or other platform. In cases where the ISP and DSL service provider are separate entities, ML-PPP could be implemented by either entity.

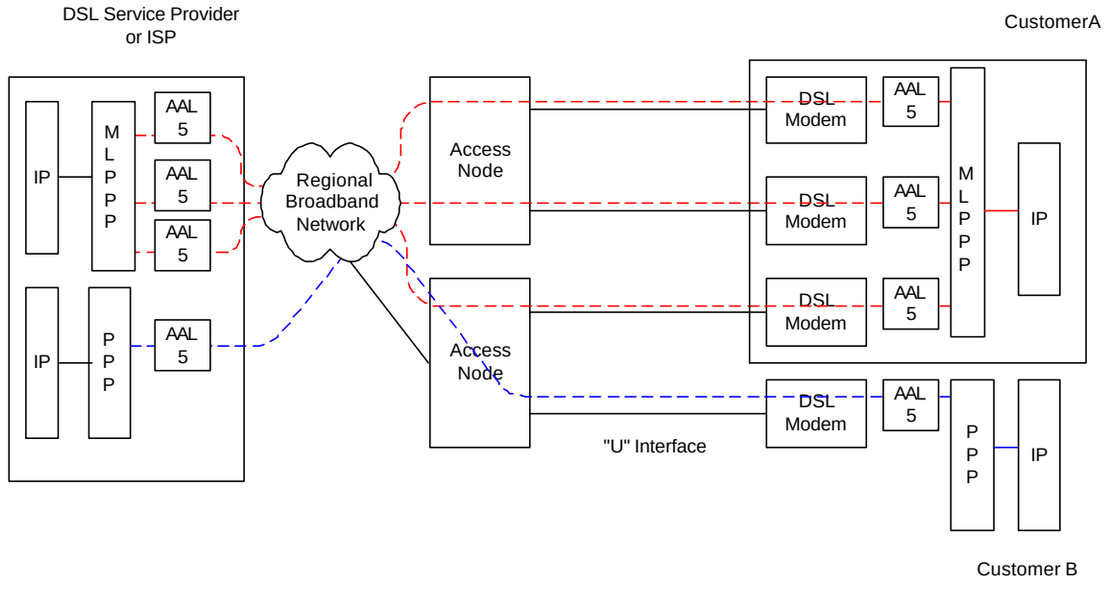


Figure 12: DSL Bonding using ML-PPP using AAL5

The table below summarizes the bonding options.

Bonding Protocols ========== Links	4-wire G.SHDSL	IMA	ML-PPP	
			Over ATM Infrastructure	Over TDM/SDH/Sonet Infrastructure
Multiple 2-wire xDSL	NA	B-NT ←→ Access Node	B-NT ←→ Access Node (transparently) ←→ bonding concentrator	B-NT ←→ DSL modem rack ←→ bonding concentrator
Single 4-wire (two pairs) G.SHDSL	CLE ←→ Access Node	NA?	NA	NA

7.3 Drivers for bonded DSL

A major driver for bonded DSL services is small-to-medium business customers seeking to upgrade from T1, E1 or single pair DSL service. Bonding allows these customers to incrementally increase their purchased bandwidth within a common “pipe” whose increased bandwidth is more efficiently shared than multiple independent links. Bonding may also allow a single IP address rather than multiple IP addresses to be provisioned. Alternatively bonding makes it possible to reach remotely located customers with regular or increased access rates.

Required business service rates can span the range from DS1 to DS3 (1.544 Mbps – 43.736 Mbps) or from E1 to E3 (2.048 Mbps - 34.368 Mbps). Typical applications of these business customers, such as telephony, Internet access, Web hosting, LAN/VPN extension, etc., often require symmetrical bandwidth.

Residential applications are a second driver for DSL bonding. Although residential customers using DSL for internet access typically do not require bandwidth greater than that available via single pair ADSL, DSL bonding can facilitate higher bandwidth residential services such as video delivery. Residential applications are primarily asymmetric.

Where fibre access to the customer premises or MTU is problematic then DSL bonding can be considered as a solution. In particular , where fibre access does not exist getting fibre access may be expensive or can have a long lead time particularly where underground work such as digging / excavating is involved. In addition in those situations where nearby access fibre resource has become scarce, fibres may be prioritised for very large buildings with larger customer communities first. In these scenarios either a permanent or transient solution using DSL bonding can be used. This also can be used to reduce risk until business drivers justify fiber access. Bonding can also be used to expand the reach or bandwidth to smaller MTU sites.

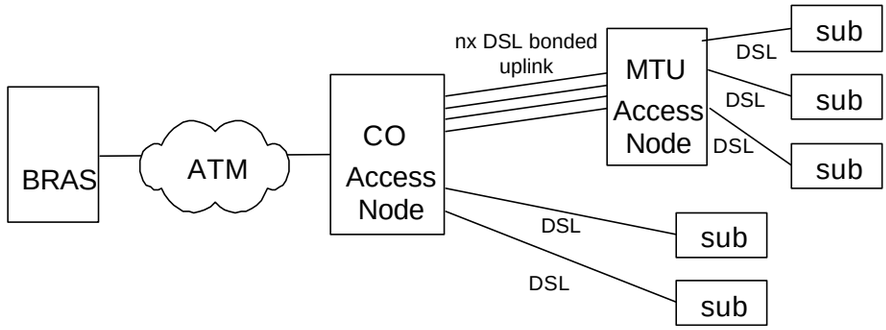


Figure 13: DSL Bonding to the MTU

From the service provider point of view, bonding provides new opportunities in both business and residential applications. It also provides operators with an alternative deployment scenario for providing high-bandwidth services to customers located at the extremes of DSL reach from the Central Office (CO). These customers may be serviced by deploying regenerators in the network to extend the reach and/or bandwidth of the DSL line. However, by bonding a number of lower-speed DSL lines the operator may meet the customer's service requirements without the need to deploy out-stationed equipment in the loop plant with its associated operational burden.

7.4 Applicable DSL Types

7.4.1 For Business Customers

Symmetrical DSLs (SHDSL and SDSL) and ADSL are among the DSL types available for business customers.

Because of its symmetry, flexible framing structures, and coverage of the common DS1/E1 access rates, SHDSL is particularly well suited to business access services. As SHDSL services and platforms roll out world-wide, bonded SHDSL will be a natural candidate for business access services requiring more than 2.3 Mbps. Methods for bonding SHDSL are a focus of this section.

Bonded ADSL may also be useful in the business context. Many "SOHOs" currently have internet connections served by ADSL. As usage of the internet connection increases, or where new services like VoDSL are added to a customer's service portfolio, increasing the ADSL bandwidth through bonding may have strong appeal.

7.4.2 For Residential Customers

As was mentioned in Section 7.3, DSL bonding for residential customers may be applicable for service reach extension or delivery of next generation services. Suitable DSLs would include both ADSL and VDSL.

7.5 Description of Techniques

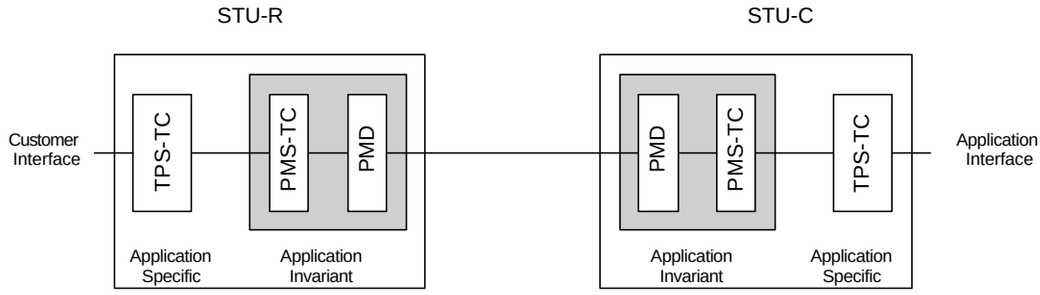
This section describes in more detail those techniques mentioned in Section 7.2.

7.5.1 PHY Layer Bonding

7.5.1.1 SHDSL

PHY Layer bonding, or 4-wire mode as defined for SHDSL in the G.991.2 standard [1] is briefly summarized here.

Figure 14 shows a simplified functional model of the SHDSL transceiver from [1]. The TPS-TC layer performs application dependent framing into the SHDSL payload structure.



Acronyms
STU-R SHDSL Transceiver Unit at the Remote End
STU-C SHDSL Transceiver Unit at the Central Office
TPS-TC Transmission Protocol-specific Transmission Convergence (TC) Layer
PMS-TC Physical Medium Specific TC Layer
PMD Physical Media Dependent

Figure 14 SHDSL STU functional transceiver (single pair SHDSL)

In the case of PHY bonding, a single TPS-TC frames data into two SHDSL lines and their associated payload structures. This is shown in **Figure 15.**

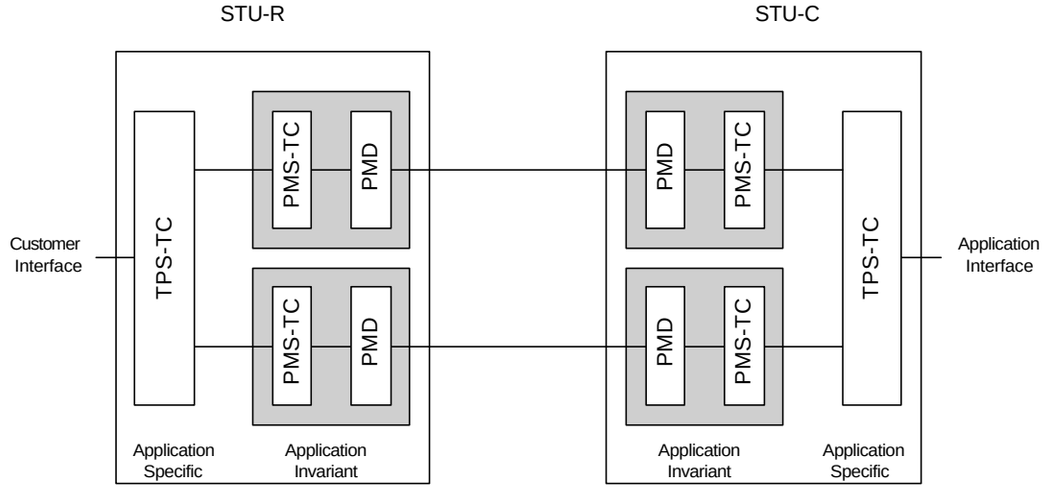


Figure 15 SHDSL STU functional transceiver (dual-pair SHDSL)

Available SHDSL application specific framing modes are summarized in Table 2. As the table shows, both TDM and ATM framing modes are supported in 4-wire mode.

7.5.1.1.1 G.SHDSL TPS-TC Mode	**Dual-Pair Bonding Applicable?**	**Single Pair Rates (n) x 64 Kbps + (i) x 8 Kbps**	**Dual Pair Rates**
1 Clear Channel Data	Yes	n = (3,..,36) i=(0,..,7) 192 ⇔ 2,312 Kbps	n = (6,8,..,72) i=(0,..,7) 384 ⇔ 4,608 Kbps
2 Clear Channel Byte-Oriented Data	Yes	n = (3,..,36) i=0 192 ⇔ 2,304 Kbps	n = (6,8,..,72) i=0 192 ⇔ 2,304 Kbps
3 Unaligned DS1	No	n = 24 i=1 1,544 Kbps	n/a
4 Aligned DS1 or Fractional DS1	Yes	n = (3,..,24) i=1 193 ⇔ 1,544 Kbps	n = (6,8,..,48) i=2 386 ⇔ 3,088 Kbps
5 European 2048 Kbps Unstructured Leased Line (D2048U)	Yes	n = 32 i=0 2,048 Kbps	n = 64 i=0 4,096 Kbps
6 Unaligned European 2048 Kbps Structured Leased Line (D2048S)	No	n = 32 i=0 2,048 Kbps	n/a
7 Aligned European 2048 Kbps Structured Leased Line and Fractional	Yes	n=(3,..,32) i=0 192 ⇔ 2,048 Kbps	n=(6,8,..,64) i=0 384 ⇔ 4,608 Kbps
8 Synchronous ISDN BRA	Yes	n=(3,..,36) i=(0,…,7) payload 1-16 BRA channels: 144 ⇔ 2,304Kbps	n=(6,8,..,72) i=(0,…,7) payload 1-16 BRA channels: 288 ⇔ 4,608 Kbps
9 ATM	Yes	n=(3,..,36) i=0 192 ⇔ 2,304 Kbps	n=(6,8,..,72) i=0 384 ⇔ 4,608 Kbps

Table 2 G.SHDSL PHY Layer Bonding Options

7.5.1.2 ADSL

No PHY layer bonding standard is available for ADSL.

7.5.1.3 VDSL

No PHY layer bonding standard is available for VDSL.

7.5.2 ATM Layer Bonding (IMA)

The ATM Forum document [3] describes Inverse Multiplexing for ATM (IMA). IMA is applicable to any ATM UNI/NNI, including the DSL loop in cases where ATM framing is used over DSL.

IMA works by introducing a common multiplexing sublayer between the ATM layer and the individual ATM transmission convergence sublayers of physical links being grouped. In the transmit direction, the IMA sublayer allocates ATM layer cells among the links of an IMA group in round-robin fashion. In the receive direction, the IMA sublayer recombines cells received on the links within an IMA group into a single cell stream, and delivers that stream to the ATM layer. To handle synchronization, a framing structure is introduced in which IMA Control Protocol cells are transmitted periodically on each link rather than payload cells. Thus the use of IMA introduces a very small bandwidth overhead.

Figure 16 shows one possible IMA over SHDSL configuration. A similar drawing could be made showing IMA over ADSL.

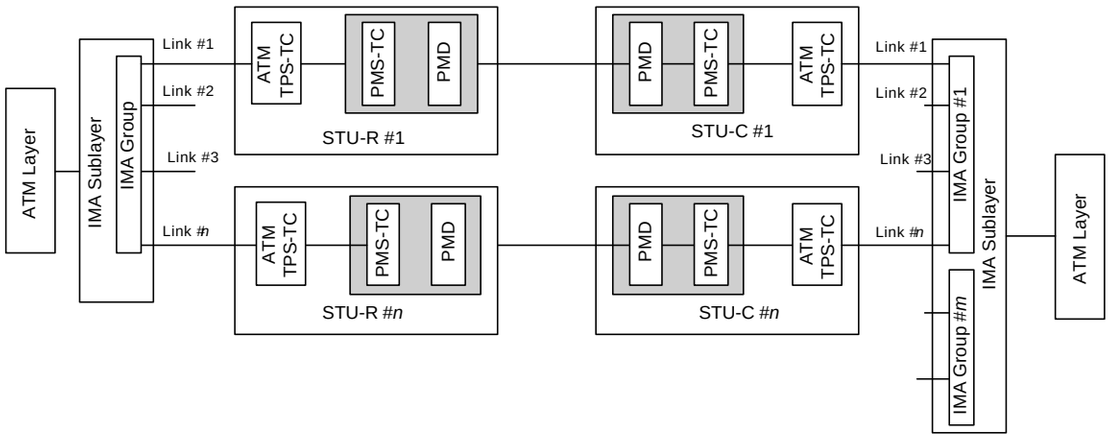


Figure 16 IMA over SHDSL (Configuration #1)

Figure 17 shows a second possible IMA over SHDSL configuration. Again, a similar diagram could be made showing IMA over ADSL. In both Configuration #1 and Configuration #2, an IMA sublayer implementation is shown which spans *n* SHDSL transceivers, where 1<= *n* <= 32. The difference between these configurations is explained in Section 7.5.2.6.

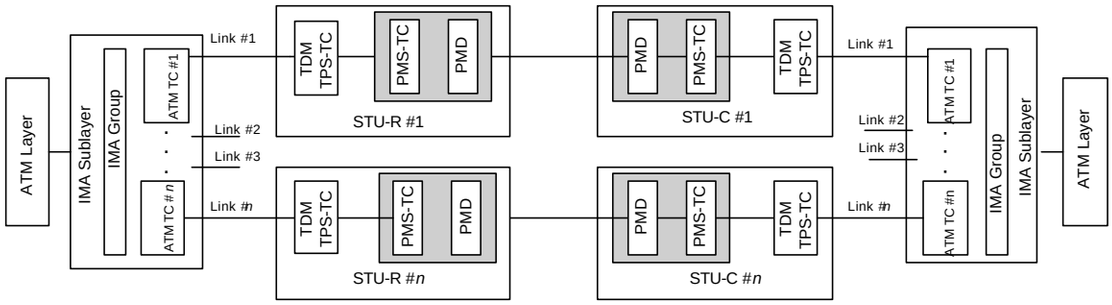


Figure 17 IMA over SHDSL (Configuration #2)

The following sections review some of the IMA technical parameters in the DSL context.

7.5.2.1 IMA Transmit clock mode

IMA supports both Common Transmit Clock (CTC) and Independent Transmit Clock (ITC) modes. While CTC requires that that the payload clocks of all links within the IMA group be clocked from the same clock source, ITC allows payload clocks across the links to be clocked from independent sources.

Clocking schemes within the Access Node typically distribute central office clocks to all DSL transceivers within the Access Node. Also, transceivers at the remote termination are typically loop timed. These arrangements suggest that CTC mode will be typically used for IMA over DSL applications.

7.5.2.2 Number of links per IMA group

IMA supports between 1 and 32 links per group. Although the typical application in DSL may be for smaller link groups, support for the full range of link group sizes will facilitate a wide range of services. Examples of aggregate and net rates for IMA link group sizes spanning this range are shown in Table 3.

Links per group	G.SHDSL (ATM TC mode)		ADSL	
	Gross aggregate bit rate (Mbps)	Net aggregate bit rate after IMA overhead assuming IMA frame size M = 128 (Mbps)	Gross aggregate bit rate for downlink / uplink (Mbps)	Net aggregate bit rate after IMA overhead assuming IMA frame size M = 128 for downlink / uplink (Mbps)
n = 1 (without IMA)	2.304	2.304	6.144 / 0.640	6.144 / 0.640
n = 1	2.304	2.285	6.144/ 0.640	6.093 / 0.635
n = 2	4.608	4.570	12.288 / 1.280	12.186 / 1.269
n = 8	18.432	18.279	49.152 / 5.120	48.744 / 5.078
n = 16	36.864	36.558	98.304 / 10.240	97.488 / 10.155
n = 32	73.728	73.116	196.608 / 20.480	194.977 / 20.310

Table 3 Examples of IMA/DSL Link Groupings

As an example, consider provision of DS3 service (44.736 Mbps). Such a service could be fully emulated with an IMA group formed of 20 SHDSL lines or 5 VDSL lines operating at 10 Mbps symmetric.

7.5.2.3 IMA Link Differential Delay Compensation

IMA requires the ability to equalize delay among the links within a group. A minimum capability of 25 ms of link delay compensation for IMA over DS1/E1 links is specified in [3]. For IMA over DSL, link delays differentials are likely to be much smaller than this value. Reducing link delay compensation requirement to a lower value for DSL may decrease the complexity of implementation. An appropriate value for IMA over DSL of 7 ms was recommended in [4]; however this value results in a requirement to buffer approximately 38 cells per link at maximum SHDSL link speeds- note that this recommendation may be excessive.

7.5.2.4 IMA Group Symmetry modes

IMA group symmetry options as defined in Section 5.2.2.7 of [3] are shown in Table 4. As shown, several asymmetric operation modes, in which fewer links are used in one direction than the other, are defined for IMA. The author knows of no requirement for such a DSL service.

Mode	Description	Requirement in IMA over DSL context
Symmetrical Configuration and Operation	IMA is configured in each direction for all physical links	This mode will typically be used.
Symmetrical Configuration and Asymmetrical Operation	IMA is configured in each direction for all physical links, but may be inactive on some links	For further study – applications unknown
Asymmetrical Configuration and Operation	IMA is configured independently in each direction for all physical links.	

Table 4 Group Symmetry Modes in IMA/DSL

7.5.2.5 Independent Uplink/Downlink Rates with IMA

The IMA specification [3] does not require nor preclude support for operation of IMA with data speeds independent in the uplink and downlink. For application of IMA over ADSL, independent uplink/downlink rate capability will be required. See Section 7.5.2.7 for further discussion of IMA over ADSL issues.

7.5.2.6 Interaction of SHDSL Framing Modes and IMA layer

This section looks at interactions between the IMA sublayer and the various framing modes of SHDSL. As show in Table 2, SHDSL supports both ATM and TDM framing modes. Both can be used in IMA over SHDSL applications.

In the following discussion, it will be helpful to refer to Figure 18, showing a protocol stack view of an IMA over DSL implementation. As can be seen, the IMA sublayer sits between the ATM layer and the ATM TC layer. This section discussed several alternatives for the location of the IMA and ATM TC sublayers, and the corresponding use of the SHDSL framing modes.

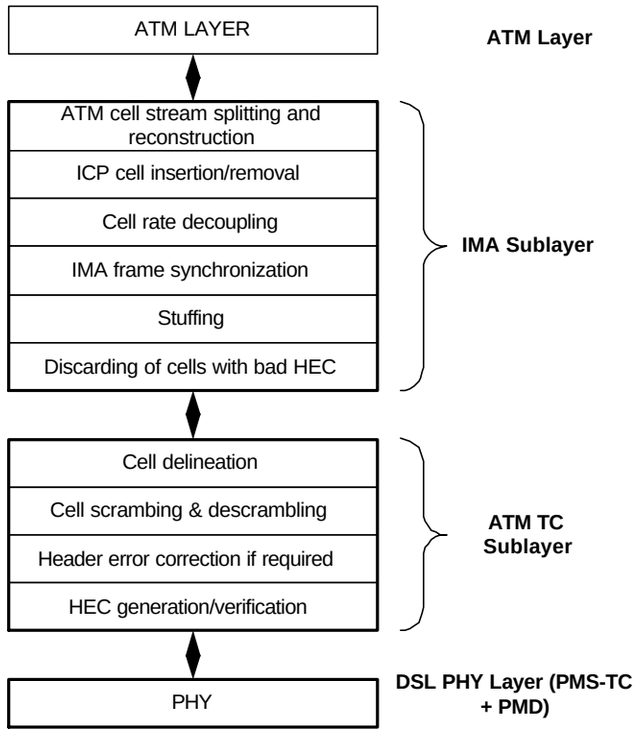


Figure 18 ATM/IMA/DSL protocol stack

7.5.2.6.1 SHDSL Internal ATM TC/ External IMA

Many DSL transceivers already include ATM TC functionality. For transceivers with internal ATM TC functions (SHDSL framing mode 9) the IMA sublayer can be implemented externally as shown in Configuration #1 (Figure 16). Communication between the transceiver ATM TC layer and the external IMA sublayer is typically via a shared ATM cell interface such as Utopia L2. Configuration #1 allows for flexible combinations of IMA groups across SHDSL links within the Access Node.

However, use of a shared cell interface in Configuration #1 introduces several complications in IMA over SHDSL system design:

- As explained in [3] and as noted in [8], when IMA is used, the ATM TC layer must not implement cell rate decoupling. As can be seen in Figure 18, cell rate decoupling (insertion of IDLE cells) in the downlink direction will be managed by the IMA sublayer rather than the ATM TC layer. In practice, the IMA implementation must prevent cell underflow down to the ATM TC layer so that the ATM TC layer will not be forced to insert IDLE cells; this requires a low delay jitter cell interface between these two layers, and may require additional cell buffering within the transceiver than would otherwise be necessary.

- Also as explained in [3] and as noted in [8], the ATM TC layer in the uplink direction must be configurable so as not to discard cells containing HEC checksum errors (or an indication that a cell with HEC checksum error was discarded must be made available to the IMA sublayer).

- For applications using IMA over SHDSL in ITC mode, delay jitter on the cell interface between the IMA and TC sublayers may increase the required cell buffering with the IMA implementation, and reduce the ability of the IMA protocol to track and correct for timing differences between the TRL (Timing Reference Links) and other links. These issue will not impact those applications using CTC mode for IMA over SHDSL.

7.5.2.6.2 SHDSL External ATM TC/ External IMA

Configuration #2 (Figure 17) of IMA over SHDSL also makes use of external IMA processing separate from the transceiver functions, but groups the ATM TC sublayer with the IMA processing. Configuration #2 also allows for flexible combinations of IMA groups across SHDSL links within the Access Node, while alleviating the system design complications associated with Configuration #1.

In addition, Configuration #2 has the advantage of directly supporting IMA in ATM over SHDSL using ATM modes which are now commonly deployed, such as ATM over DS1, ATM over E1, and ATM over fractional rate services.

In Configuration #2, the interface between the transceivers and the IMA function is typically a point-point interface configured according to the service mode in use, i.e. a mode chosen from those listed in Table 2.

7.5.2.6.3 SHDSL Internal ATM TC/ Internal IMA

Multi-port DSL transceivers could choose to integrate the IMA sublayer functionality within the DSL transceiver device itself. This integrated solution, "Configuration #3" aggregates the functions together to provide a compact implementation, particularly suited for the remote termination. However, an integrated implementation places rigid system constraints within the Access Node upon the granularity, size and link allocation of IMA groups that an external IMA implementation would not impose.

7.5.2.7 Operation of IMA over ADSL

IMA over ADSL is a candidate for increasing service bandwidth and/or service reach for residential and some business subscribers. The following technical issues require attention in this case:

- As noted in Section 7.5.2.5, uplink and downlink link rates will be different in ADSL. The IMA implementation must be capable of handling this difference.
- Allocation of ATM channels to fast path or interleaved path should be coordinated among the links so as not to cause excessive delay differential for the IMA sublayer.
- The IMA specification assumes that the different links operate at the same nominal link cell rate (Section 3 of [3]). However, ADSL transceivers negotiate a channel rate as a result of transceiver training, channel analysis, and capabilities exchange [2]. Final bit rates for both uplink and downlink channels are determined by the transceiver in the central office. In order to ensure proper operation of IMA, final bit rate settings must be coordinated among all the central office transceivers within an IMA group. Means to achieve this coordination require study by the DSL Forum.
- Dynamic link rate changes should be prevented for proper IMA operation. This issue is of particular concern to IMA used with G.lite.
- As in the case of SHDSL, several IMA/ATM TC sublayer configurations are possible.

7.5.3 Multilink PPP

Several DSL Forum protocol models for accessing data networks utilize the PPP protocol to carry packets over the "U" interface [7]. These protocol models are PPPoA, PPPoE, and L2TPoA. Because of the widespread use of PPP, it is interesting to consider how ML-PPP could be used for DSL Bonding.

ML-PPP as defined in RFC 1990 [5] can be used to group multiple PPP links into a single virtual bundle. In the transmit direction ML-PPP takes a PPP packet, optionally fragments it, and affixes a Multilink header. Each resulting fragment (or whole packet) is transmitted across a separate link. At the receiver, the per-fragment headers are used to reconstruct packets. This process is represented schematically in Figure 19.

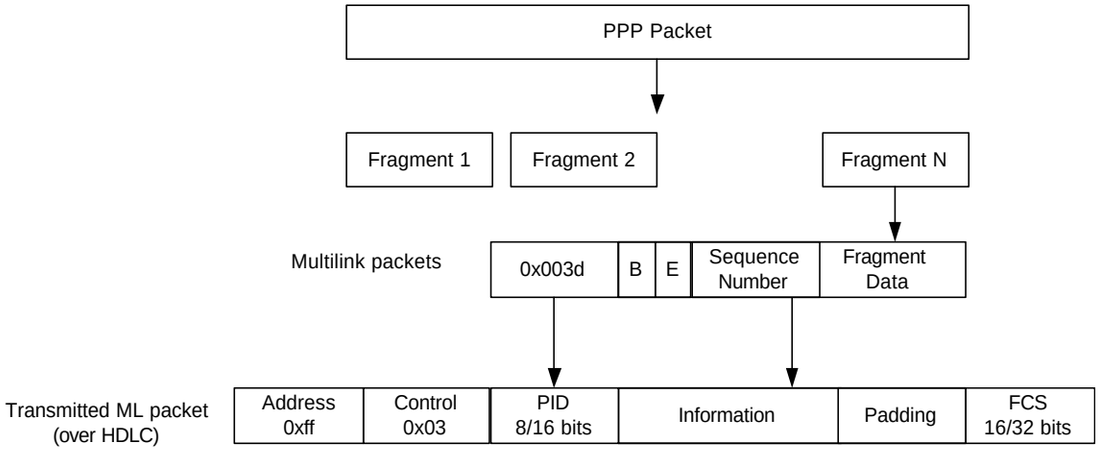


Figure 19 ML-PPP Operation

7.5.3.1 Differences between ML-PPP and IMA

Some of the differences in the way that data is multiplexed between IMA and ML-PPP are:

- Unlike IMA which uses a fixed round-robin method, ML-PPP distribution of fragments to links is not standardized. Therefore, the freedom to accommodate links of different bandwidth already exists in ML-PPP, and direct support of ML-PPP over ADSL may be easier than IMA over ADSL.
- Whereas IMA confines overhead information to a periodic framing structure, ML-PPP inserts additional header structures between Layer 3 and PPP on each packet fragment sent.
- Both IMA and ML-PPP include provisions for equalization of differential delay across the links. Estimation of delay differences is standardized in IMA but implementation specific in ML-PPP.
- ML-PPP fragmentation and reassembly operates on a single virtual bundle. Therefore, delays can occur to all traffic in that bundle when a single fragment is lost or delayed. IMA groups are maintained using a framing mechanism that is resilient to the loss or delay of individual cells.
- ML-PPP coexists with “normal” PPP on the same links, allowing the user to route delay sensitive traffic over a single like via PPP, bypassing the ML-PPP bundle and any associated delay in ML-PPP processing. This facility may be useful in support of interactive voice service over links with differential delay. By contrast, all ATM traffic passing through an IMA enabled set of links will be processed by the IMA sublayer.However, in typical DSL application the IMA implementation wi ll not add unduly to delay.
- ML-PPP when implemented with multi-class extensions [6] provides additional support for traffic of different priorities or classes.

7.5.3.2 Application of ML-PPP DSL context

Figure 20 shows a potential use of ML-PPP over DSL.

For reference, customer B with a single DSL link and “normal” PPP processing (in this case, PPPoA) is shown. The ATM and PPP connections are shown terminated in the same network box, but other configurations are possible.

Customer A is connected to the DSL service provider via an Integrated Access Device with three DSL links. Each DSL link carries ML-PPP fragments over AAL5. ML-PPP is used to bond the 3 links.

7.5.3.3 ML-PPP Protocol Issues

Typically, ML-PPP is used with PPP in HDLC framing. In the DSL context, PPP in HDLC framing, and ML-PPP could be used upstream from the Access Node. Alternately, the ML-PPP protocol could potentially be applied directly to PPP packets carried over AAL5. Similarly, the ML-PPP protocol could be applied to PPP packets carried over the PPPoE, but it is not clear that PPPoE would be used in applications requiring DSL bonding.

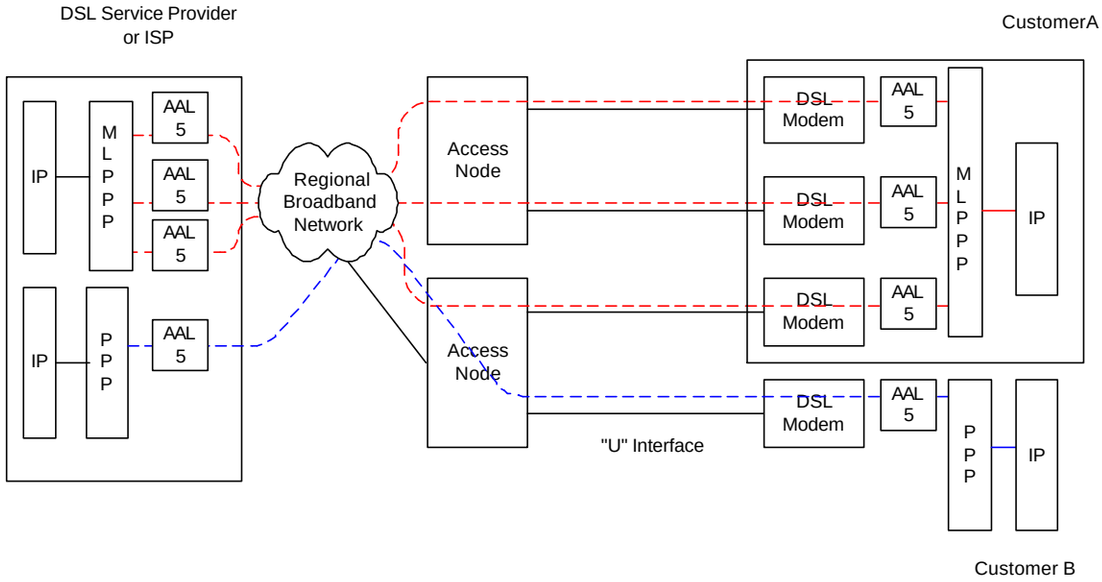


Figure 20 Potential Application of ML-PPP over DSL

7.6 Technical Comparison

7.6.1 Protocol Transparency

For services that are limited to 2-pair SHDSL, PHY-layer bonding is the most protocol-transparent option as it supports both TDM and ATM modes directly.

For multi-pair SHDSL most applications over DSL use ATM framing and IMA is well suited to these applications.

ML-PPP is suited only to those applications built over the PPP protocol.

7.6.2 Access Node Configuration Flexibility

Consider the deployment of these technologies within the Access Node.

PHY Layer bonding for SHDSL is of very limited flexibility. Only 2 pairs may be bonded. In order to bond any pair X with another pair Y, X and Y must be terminated by the same transceiver. Changes to configuration (for example bonding pair X with pair Z rather than Y) would require physical reconfiguration of the pair(s) through cross-connect facilities.

IMA bonding, if implemented in the Access Node external to the transceivers as in Configurations #1 and #2, is much more flexible than PHY layer bonding.

- For an Access Node line card implementation, IMA external to the transceiver provides flexible groupings and supports link additions and deletions from IMA groups as required.

- IMA may also be implemented in a "server card" approach in which cell traffic from Access Node line cards may be flexibly aggregated at a central location. The server card approach has the advantage of allowing IMA groupings across any set of links irrespective of their individual line card locations. In the server card approach, however, close attention must be paid to the delay jitter across the interface between server and line cards, particularly for Configuration #1.

ML-PPP bonding shares the advantage with IMA of flexibly grouping links irrespective of their physical configuration. ML-PPP may be implemented internal to the Access Node, and can also be implemented at upstream platforms such as LAC, RAS and SMS.

The bonding protocol should support the dynamic addition and removal of pairs for partial bandwidth use and possible redundancy, including accommodation of physical layer failures and recovery from failures. ML-PPP and IMA support dynamic addition and removal of pairs.

7.6.3 Added Delay

PHY layer bonding does not add significantly to fixed delay.

IMA implementations add fixed delay from the following sources

- transmission processing including buffering to maintain constant cell rate across IMA links;

- receive processing including buffering to smooth out differential delay.

The total added delay is not defined within [3] and is implementation specific.

ML-PPP implementations add fixed delay from the following sources

- transmission processing including fragmentation across the links;

- receive processing including buffering to smooth out differential delay across lines.

The total added delay is not defined within [5] and is implementation specific.

Regardless of bonding technique long data packets should traverse the bonded facility in a manner that minimizes transfer delay.

7.6.4 Different Link Bandwidths

PHY layer bonding and IMA both require that each link within a group be of the same bandwidth. (In the case of IMA small differences in clock rate can be accommodated through use of ITC mode, but common clocking arrangements in the Access Node suggest this capability will not typically be required.)

ML-PPP does not require that links have the same bandwidth. The ability of ML-PPP implementations to accommodate a wide range of bandwidth differences, such as may be encountered in ADSL where transceivers train to different rates, is implementation-specific.

7.6.5 Support of ADSL(Asymmetric Uplink/Downlink)

PHY layer bonding is not defined for ADSL.

Nothing in the IMA specification precludes implementation of IMA over asymmetric link bandwidths.

Similarly, ML-PPP does not preclude such operation.

7.6.6 Implementation Complexity

Comparing the implementation complexity of these techniques is likely a vendor-specific exercise. Only a few comments are made here to compare implementation options.

PHY layer bonding is typically implemented as an application-specific TPS-TC in a multi-PHY SHDSL transceiver. From a system point of view, the PHY-bonded SHDSL lines appear as a single transparent transmission link.

IMA is a data processing function which is available in off-the-shelf hardware chips. Such chips could interface directly with DSL transceivers on line cards, or could be deployed on server cards within the Access Node. Additionally IMA may be implemented within a multi-PHY transceiver, although the IMA group will be limited to just the lines terminated by the transceiver unless chaining of some sort among transceivers is implemented.

ML-PPP for PPP in HDLC framing is also available in off-the-shelf hardware chips. However, direct application of ML-PPP to the DSL Forum protocol stacks (PPPoA, PPPoE, L2TPoA) may require additional software or hardware support than is available in off-the-shelf chips.

Note that ML-PPP is less standardised in OAM than IMA and SHDSL 4 wire mode bonding.

The bonding protocol should have minimal overhead to carry data traffic at as close to 100% efficiency as possible.

7.6.7 Extension to other DSL types

While no PHY layer bonding is specified for ADSL or VDSL, both IMA and ML-PPP can be implemented over ADSL and VDSL.

7.7 Summary

In summary, DSL bonding applications are likely to be driven by both business and residential service requirements. Candidate technologies include PHY-layer bonding for SHDSL, IMA for SHDSL, ADSL and other ATM based DSLs and ML-PPP for any DSL using PPP as a protocol layer.

From the preliminary analysis presented in this section:

- PHY-layer bonding is protocol transparent, but is restricted in flexibility, and is currently restricted to SHDSL.
- IMA-over-SHDSL is flexible and well suited to meeting business service requirements, and may represent a natural upgrade path for SHDSL operators with an installed base of ATM services and equipment.
- IMA-over-ADSL may provide a good solution to delivery of higher rate business services, delivery of high bandwidth residential services such as video broadcast, and for service reach extension, particularly for those operators wishing to build upon their installed ATM base. For IMA over ADSL applications, further investigation of methods to coordinate data rates among ADSL lines could be considered as a work effort by the DSL Forum.
- Various configurations for deployment of IMA in the Access Node are feasible and it would be useful to undertake further study in this area to establish DSL Forum requirements.
- ML-PPP provides a packet-based alternative for those services already using PPP. ML-PPP has advantages including flexibility and tolerance of different link speeds within a bundle. Work should be undertaken by the DSL Forum to investigate the applications and preferred protocol stacks for ML-PPP

8. Broadcast television over DSL

Broadcast television (BTV) services are content that is traditionally delivered via RF or terrestrial cable networks. More recently broadcast television services are being delivered via Digital Broadcast Satellite to the residential consumer. Broadcast television content has regularly scheduled programming and includes local, national and international channels. Speciality channels make up a large portion of broadcast television channel selection.

Pay per view is a broadcast television service that is viewable if the consumer decides to pay for the event. Unlike Video on Demand (VoD), the video source is not under control by any of the users in terms of VCR-like controls.

Because the content of BTV and pay per view is typically scheduled ahead of time, a channel guide is generally available to display a list of scheduled programs.

DSL access is a comparatively new delivery mechanism for BTV. This section explores a possible architecture for the delivery of BTV over DSL.

8.1 Starting Network Scenario

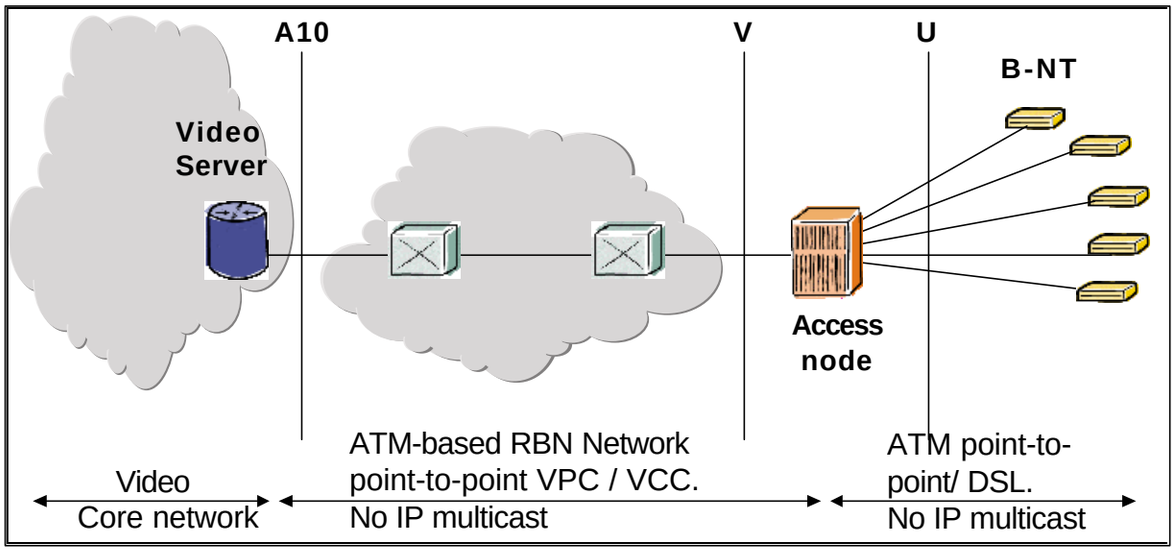


Figure 21: Starting scenario without multicast

The VCC / VPC point-to-point (PTP) connectivity approach used for basic internet access service today could perhaps be used across the ACCESS NODE to deliver broadcast services. Internet traffic has a bursty traffic characteristic which enables a high degree of statistical gain. This means the traffic of a large user community that only requires best effort internet access can be aggregated together over one network interface with reasonable service quality.

High quality video services require the reservation of significant quantities of guaranteed bandwidth. The reserved bandwidth required to meet the expected service quality means that the need for bandwidth between the ACCESS NODE and the core network increases in an almost linear manner per video channel per DSL subscriber when using PTP PVCs / PVPs. Therefore the PTP approach is not efficient to carry high quality (e.g. near studio quality) video services. This is because in the existing scenario bandwidth for every TV channel has to be carried separately and therefore duplicated across the network for every user when using ATM PTP connectivity.

8.2 Proposed target Network Scenario

A potential network architecture to deliver BTV service is shown in Figure 22. The head-end architecture to support delivery of BTV across multicast capable Access Nodes is shown in more detail in Figure 23.

The "head-end" is the part of the network where the video is encoded and passed to the Regional Broadband Network (RBN) for distribution. When multicast capable ACCESS NODEs are used, encoders stream each of the BTV channels across the broadband network on a separate PVC. BTV uses IP packets encapsulated into AAL5 and transported over ATM Point to multipoint (P2MP) connections to broadcast video content to subscribers. P2MP PVCs deliver content channels to a ACCESS NODE ATM interface, and P2MP VCs within the ACCESS NODE, to provide streams to individual subscribers. Within the ACCESS NODE the data is replicated and sent to the ADSL port of each subscriber who is requesting that channel.

Data for each BTV channel is assigned an IP multicast address defining the content. The ACCESS NODEs then switch ATM traffic to multiple ADSL lines for delivery to subscribers' homes. Each channel is sent to every ACCESS NODE, but the ACCESS NODE only forwards a channel to legitimate customers who request it. If multiple set top boxes on the same DSL port request the same channel, only one copy is sent to the port.

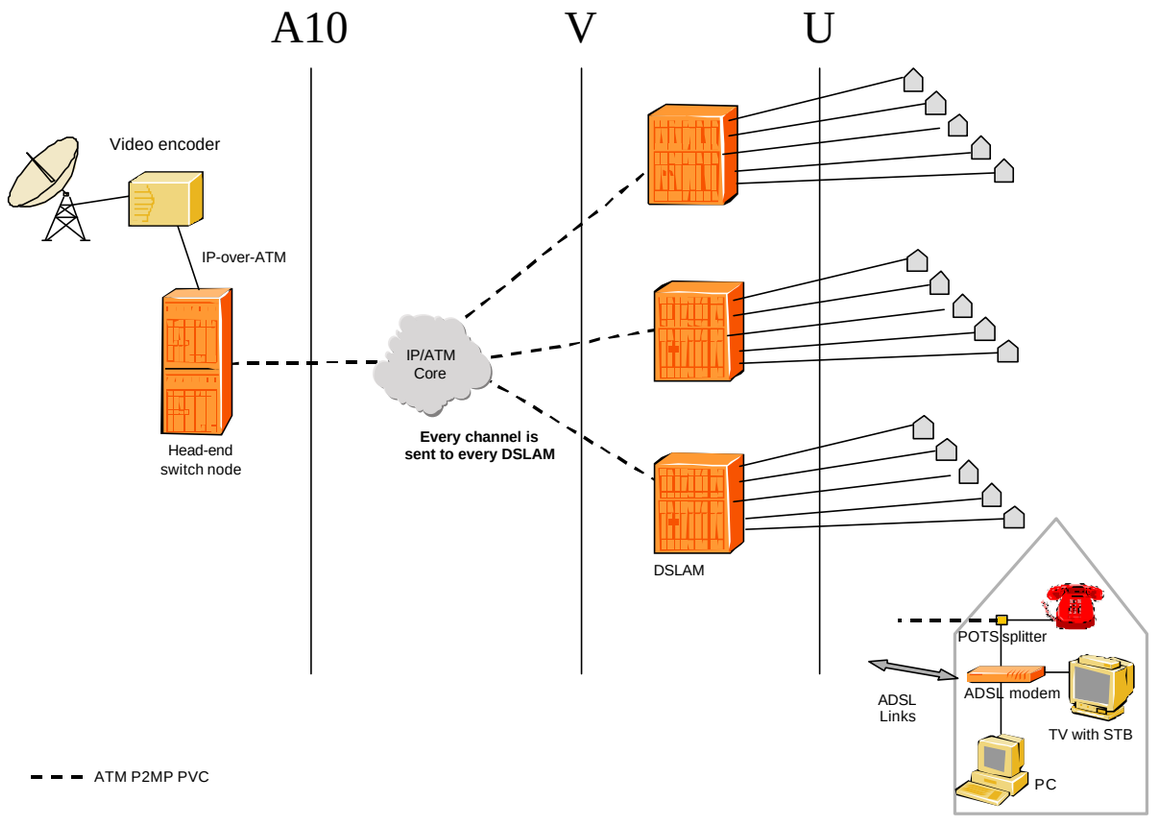


Figure 22: BTV Proposed Target Architecture – Multicast Network Topology

The head-end portion of the BTV network encodes and aggregates video channels. The IP/ATM infrastructure must be sized to accommodate head-end ATM traffic and transport it to the ADSL modem without loss. The backbone also must support IP unicast management traffic. The access end is sized per ACCESS NODE according to the number of subscribers.

Video encoders are used for audio, video/Web broadcasting, pay-per-view, or other unidirectional broadcasting. The egress port of the video encoder is either 100BASE-T Ethernet or an ATM interface and usually multiple encoders are required. OC-3c/STM1's or OC-12c/STM4's are usually used to connect the encoders to the Head-end switch if ATM is supported by the encoder as is shown in Figure 23. If an Ethernet interface is used, Ethernet-to-ATM adaptation is required, which maps the packets to VCs and perform the RFC 2684/1483 encapsulation. Each channel is mapped to an individual VC.

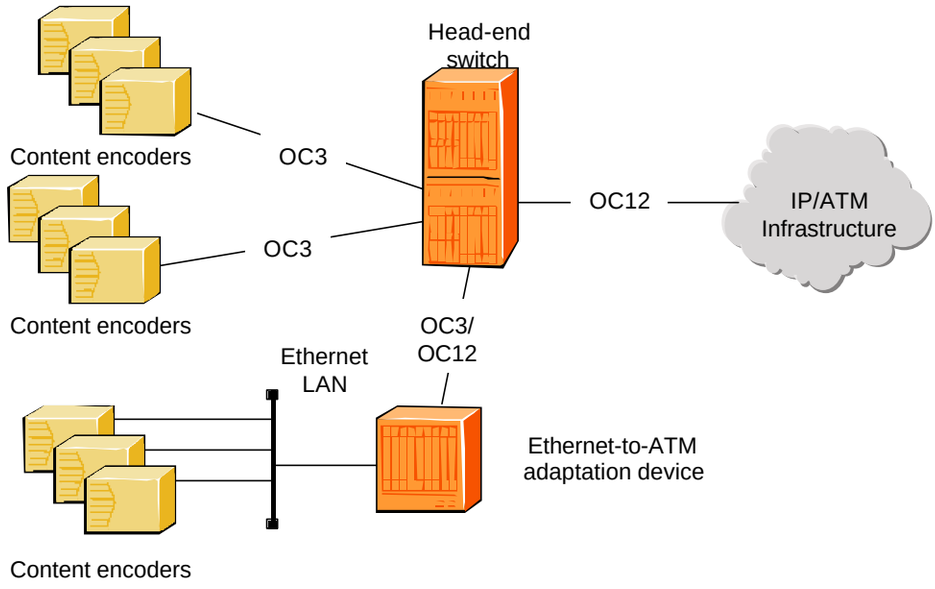


Figure 23: BTV Head-End equipment Example

Each content channel is associated with an IP multicast address. The ACCESS NODE uses this address to identify the channel and associate the P2MP endpoint with the ATM/ADSL distribution VC. Each ACCESS NODE has a table that maps the video channel IP multicast address to the unique, incoming interface port's VPI/VCI.

The STB also stores a table to map channel numbers to IP multicast addresses. Table 5 shows sample encoder, ACCESS NODE, and STB IP-mapping tables that are used to deliver the channel selected by the subscriber.

Encoder			**ACCESS NODE**		**STB**	
Encoder	IP multicast	VPI/VCI	IP multicast	Trunk interface port; VPI/VCI	Channel	IP multicast
Encoder 9	228.4.1.131	0/102	228.4.1.131	Port-id;0/102	CNN - 33	228.4.1.131
Encoder 11	224.0.0.101	0/150	224.0.0.101	Port-id;0/101	CityTV - 15	224.0.0.101

Table 5: IP multicast mapping

These tables are customized for each installation and must be correlated.

Note that the STB does not map the channel to a particular VPI/VCI. Typically the STB has an Ethernet interface and therefore is not aware of the VPI/VCI. From the point of view of the CPE modem, a small set of VPI/VCIs are use to receive the BTV channels and it is the responsibility of the ACCESS NODE to select the VPI/VCI. The CPE modem is

either preconfigured with the set of possible VPI/VCI channels, or ILMI[2] is used to inform the CPE modem of the VC connection. These connections are typically statically configured and the DSL modem's VPI/VCI values do not change as channels are changed.

8.3 Drivers for Broadcast TV using IGMP over DSL

To compete with Cable MSOs – BTV is a necessary part of the service mix.

Support BTV services using effective traffic management:

- Use bandwidth efficiently using IP multicast and point-to-multipoint ATM
- Support time sensitive video services MPEG 1, MPEG 2, MPEG 4
- Ensure channel change time is adequate
- Ensure delay variation is acceptable

Leverage off installed base of Access Nodes to have the widest possible service volume offering

Use standard protocols (e.g. IGMP) to ensure fast track to interoperability

8.4 Options

8.4.1 CPE (modem/STB) requirements

As known, the DSL CPE modem can range from quite complex boxes to simple bridges. The simple CPE Ethernet Bridge does not need to be IGMP aware, as the STB will cope with the IGMP protocol. Advanced DSL CPE Router could also play an active role in e.g. IGMPv2 proxy functions or even IGMPv2 routing between multiple local Ethernet ports.

The STB only needs to support standard IGMPv2 without any enhancements. Most / all enhancements to the performance can be achieved by introducing some changes to IGMPv2 on the Access Node side.

Some set top boxes have introduced a debounce time on the remote control to filter out unnecessary IGMP messages towards the ACCESS NODE. This reduces processing load on the ACCESS NODE and therefore improves performance and enables the ACCESS NODE to handle larger number of STBs simultaneously. However this is for a small acceptable debounce delay added to the channel change time. This debounce function could also be done by a more advanced CPE if multiple STB are connected.

Described below is the Bridged CPE model where the effort for the CPE modem is small to support IGMPv2.

8.4.2 CPE Connections

There are a number of connection configurations that can be used within a video application context. This section gives an overview of how multicast and unicast services can be combined. The number of VCs required to the CPE is a critical element and varies depending on the video middleware provider and network topology.

[2] DSLForum Technical Report – 037: Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM

8.4.3 IGMP External to Acess Node

Multicast control may also be external to the Access Node. When the multicast control (IGMP) is done external to the Access Node by a router or BRAS, it becomes important to minimize the VC count across the V interface.

It is possible in this architecture to carry all BTV related information on a single VC. When the multicast is done external to the Access Node, the solution becomes "user limited". This means that the number of STBs subtended from the Access Node is limited by the aggregate bandwidth. This is because the channel being received by each STB must be carried individually across the V interface even if the same channel is being received by multiple STBs. For example, if an OC-3c/STM1 is the aggregate and it is assumed that 140 Mbps are available for video traffic and each MPEG-2 video channel requires 2.5 Mbps, at most 56 STBs can be supported. Note that if lower encoding rates are used, more STBs can be supported.

Note that most STB don't get turned off, therefore even if the TV is turned off, the STB is constantly receiving a multicast group while on.

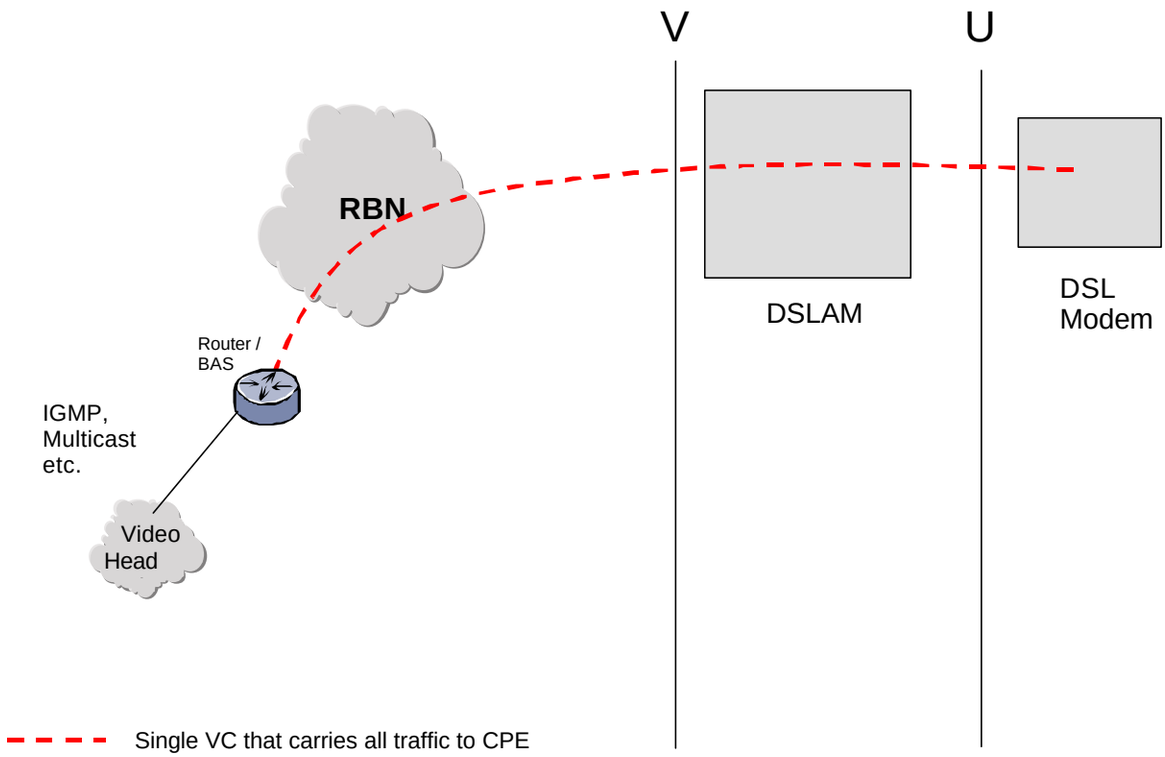


Figure 24 VC Requirement for IGMP Control External to Access Node

8.4.4 IGMP Integrated in Access Node

When the multicast control (IGMP) terminates on the Access Node, then several VCs are required on the CPE. However the multicast at the Access Node allows unlimited number of video users but puts a limit on the number of available video channels that is based on the aggregate interface at the Access Node. For example, if an OC-3c/STM1 is the aggregate and it is assumed that 140 Mbps are available for video traffic and each MPEG-2 video channel requires 2.5 Mbps, at most 56 video channels can be supported. Note that if lower encoding rates are used, more video channels can be supported.

In the IGMP integrated architecture two VC's minimum are required across the V interface.

When multicast is done in the Access Node, at least 2 other VCs are required:

- One static VC is required for IGMP signaling.

- One additional VC is required for each concurrent multicast streams (e.g. depending on the number of TV sets per user);

In case on-demand service is offered, another VC is added. This VC is usually connected to an Ethernet based Head-End system which integrates the application software platform and the video on-demand server. One VC is required to make the connection to both of these functions.

Additional VCs are required by the middleware that are outside the scope of this section. These VCs are needed to allow communication between the STB and the head end for various functions such as: Electronic Program Guide download, Channel Guide download, etc.

To summarize, the following VCs (all provided with RFC 2684 – bridged mode) are provisioned per subscriber:

- Video Multicast traffic forwarding VC('s)
- IGMP channel from STB to ACCESS NODE (distributed model across 'U' interface)
- Head-End (application platform + video on demand) traffic
- Any additional VCs required by the middleware

Figure 25 shows a typical VC distribution from the ACCESS NODE to the CPE.

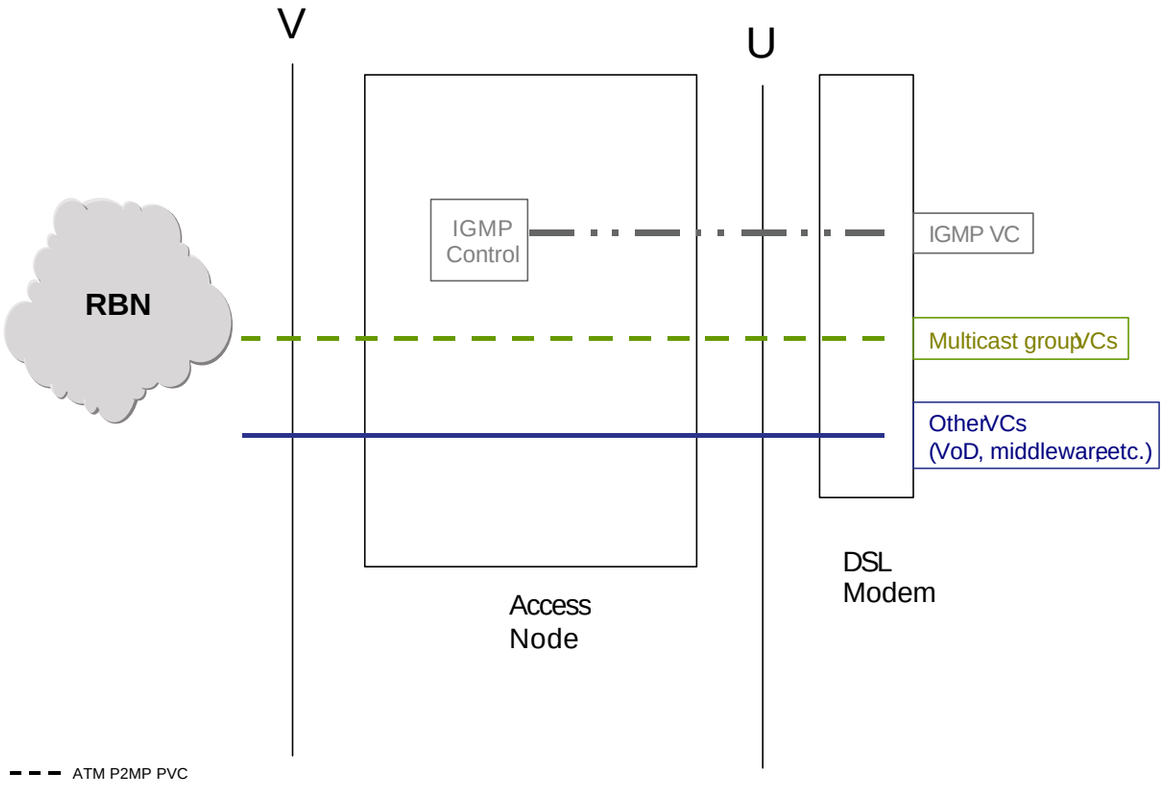


Figure 25 VC Requirement for IGMP Integrated in ACCESS NODE

8.4.5 Channel Changing

Channel changing is done using IGMPv2 (RFC2236) which is part of IP. IGMP is not a protocol that was designed specifically for video. Instead it was designed to allow devices to join IP multicast groups. In this architecture, each channel is directly mapped to an IP multicast group. This mapping is known by both the STB and the IGMP server as was shown in Table 5.

Most of the IGMP communication between the ACCESS NODE and the STB is a series of channel changes. In general, a channel change is also known as a zap which constitutes an IGMP Leave followed by an IGMP Report which specifies the desired group to join. In a typical zapping scenario, the user issues a channel change command to the STB, which sends an IGMP Leave Group message followed by an IGMP Group Membership Report message (which in effect is a join request for a particular multicast group). When the ACCESS NODE receives a Leave Group, it must ensure that the multicast group is not required by any other user on the same port. According to RFC 2236 it does this by entering a Checking Membership state in which it sends out 2 Group Specific queries to all STBs that are part of the IGMP signalling channel. If it does not receive a response it removes the port from the ATM multi-point connection.

In exploring IGMP, the potential for implementing an optimized version of the protocol while adhering to the standards-based protocol in external communications with the various video entities (e.g. STB's) is entirely feasible. For example there are ways to eliminate the 2 second delay before removing a "left" channel. This is a requirement for DSL because of the limited port bandwidth.

In summary, set top boxes contain IGMP client software which send channel change requests to the IGMP server. These requests are sent on a PVC from the CPE modem to the IGMP server. When the user requests a channel change, the STB sends an IGMP leave followed by a report (join). The Bridge CPE modem bridges this request on the PVC to the IGMP server. When the IGMP server receives the channel-change request, it instructs the connection control entity to break the connection between the ACCESS NODE ADSL port and the current channel stream and establish a new connection for the requested channel. Usually the VPI/VCI used on the ADSL port for the new connection is the same as the VPI/VCI used for the previous BTV connection. To the user, there is minimal delay between the STB request and the change of channel. See §8.4.7 for more information on the message flows.

8.4.6 Protocol Stacks

In a commonly supported BTV architecture with multicast on the ACCESS NODE, all data and control is transmitted as bridged Ethernet over ATM. Multiple Bridged PVCs terminate on the CPE modem. More complex CPE modem can also handle Routed PDU to be terminate and routed to the STB.

Figure 26 - Figure 28 show the protocol stacks involved for the actual broadcast video stream. As can be seen from the figures, the ACCESS NODE does not process the video stream, it simply does the multicast of the ATM cells, with appropriate VPI/VCI remapping. It is the video servers responsibility to put the video stream in MPEG format and transmit it on a preconfigured IP multicast address. The IP multicast address is mapped to an Ethernet MAC address using a standard formula and then the Ethernet frame is encapsulated using RFC 2684 (obsoletes RFC 1483) bridged PDUs with LLC-SNAP as is shown in Figure 26. Note that RFC2684 can also encapsulate IPv4 PDU, the more complex CPE can then route these packets to the local LAN or STB as is shown in Figure 27. The IP multicast address mapping to an Ethernet MAC address is then also done in the CPE. Note also that if the video encoder does not support ATM, then an Ethernet to ATM bridge or switch must be used as is shown in Figure 28.

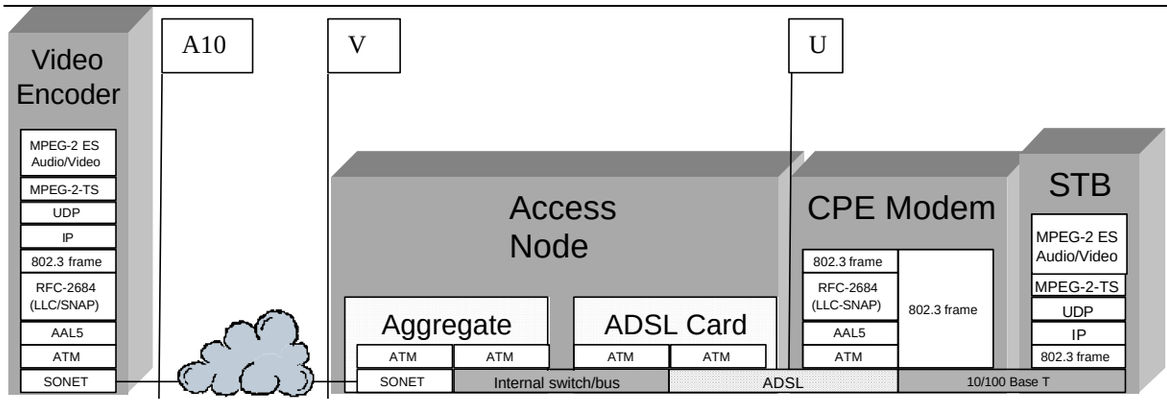


Figure 26: BTV CPE Bridged Video Stream Protocol Stack with ATM to Video Encoder

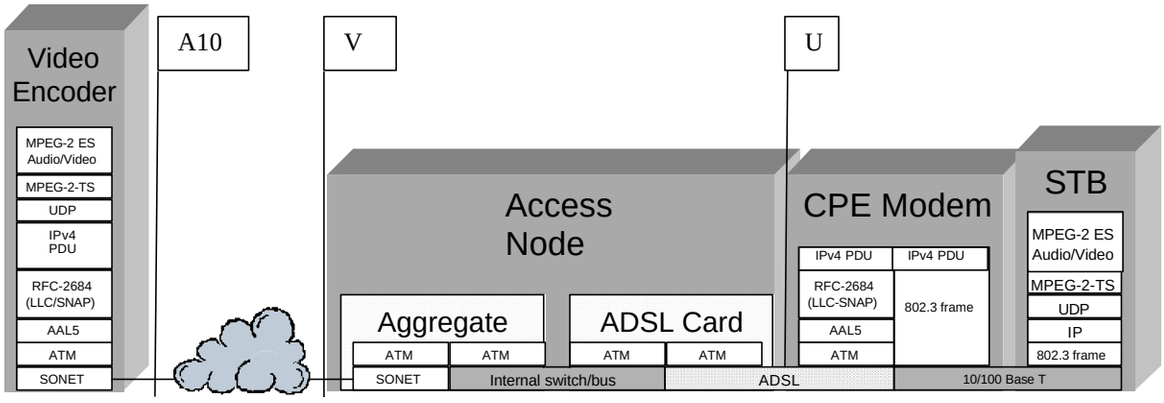


Figure 27: BTV CPE Routed Video Stream Protocol Stack with ATM to Video Encoder

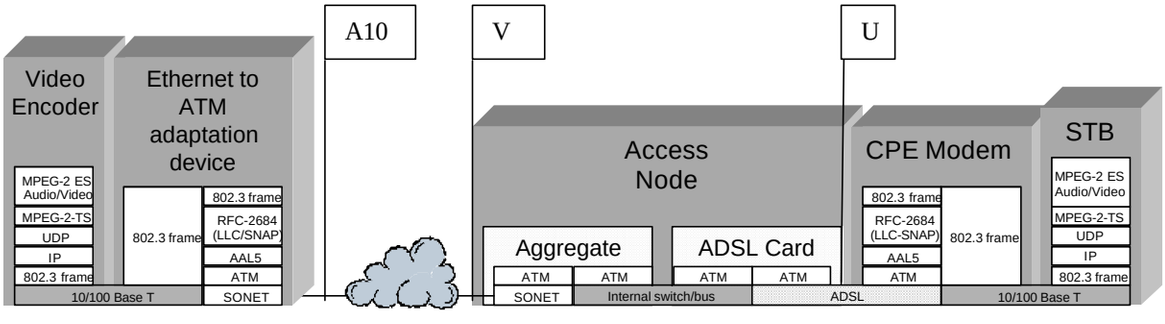


Figure 28: BTV CPE Bridged Video Stream Protocol Stack with Ethernet to Video Encoder

Figure 29 shows the protocol stacks involved in the IGMP messaging to control changing channels. The STB sends IGMP messages, which are a part of IP, to leave and join multicast groups (BTV channels).

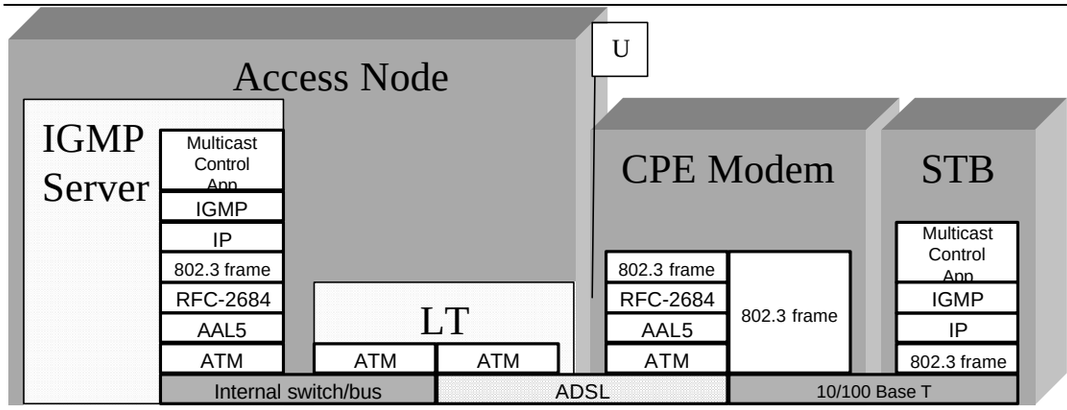


Figure 29: BTV IGMP Control Protocol Stack

8.4.7 Message Flows

Figure 30 shows the message flow that occurs when a user selects a new channel. When the user selects a new channel, the STB sends a message to the IGMP server. The message is actually addressed to the IP address of the multicast group (i.e. channel) that the user wishes to join. The IGMP Server arranges for the channel currently being transmitted to be disconnected and the new channel to be connected. Note that the protocol does not have a response message.

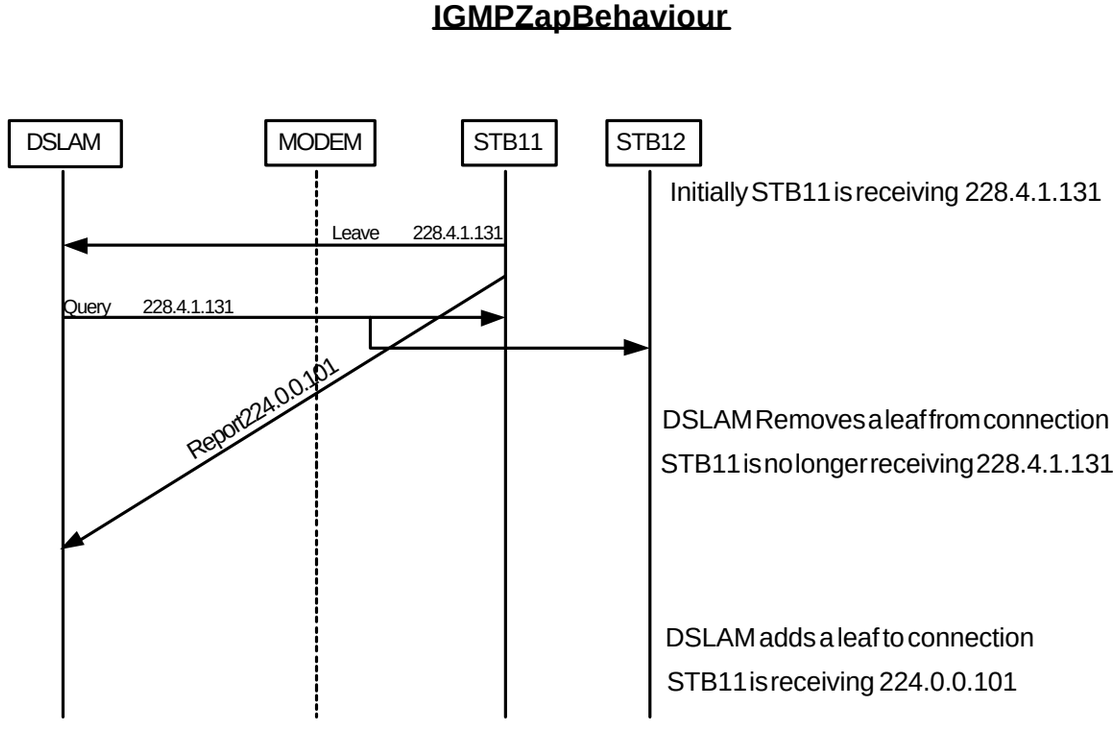
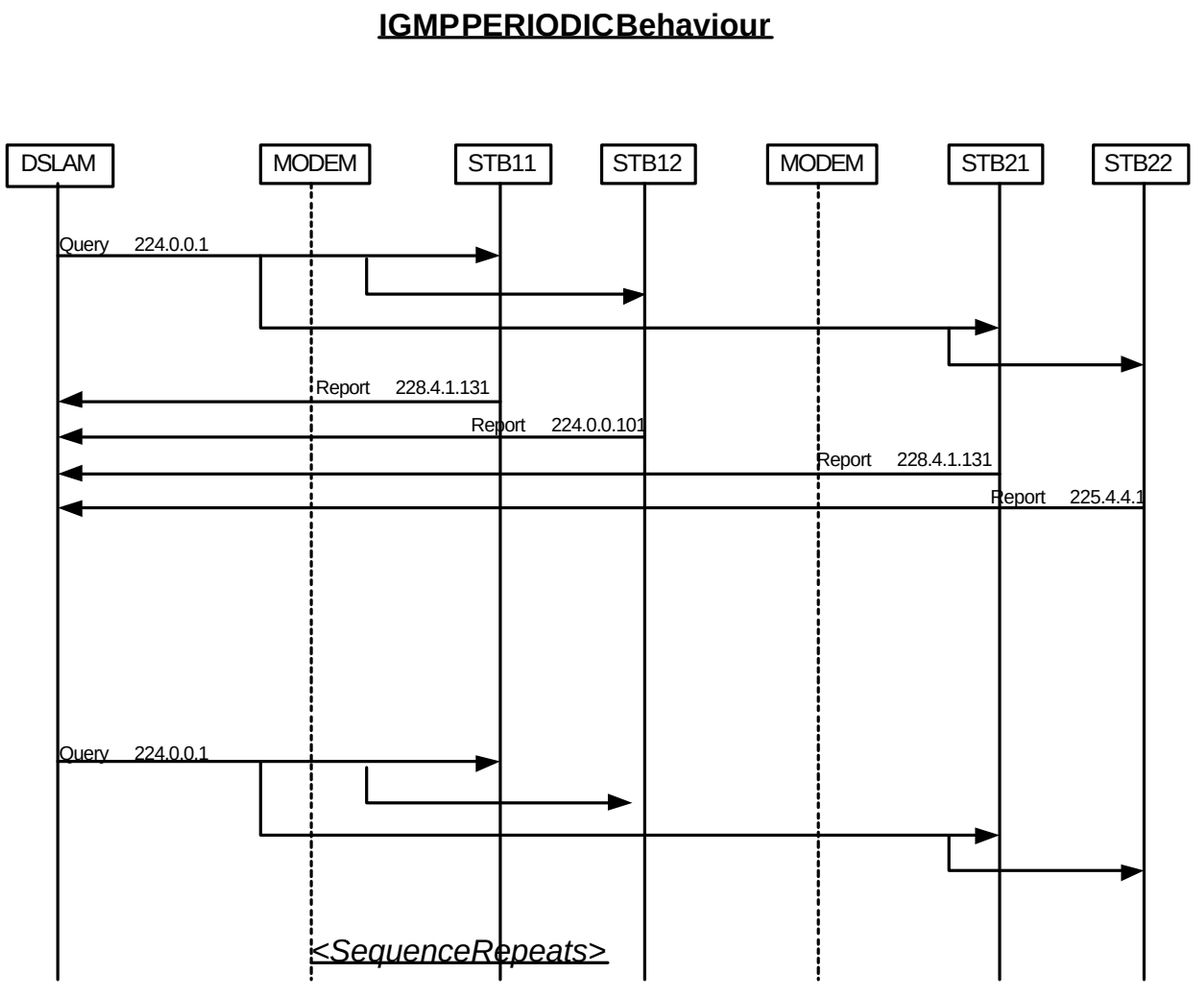


Figure 30: BTV Channel Selection Message Flow

In Figure 30 the ACCESS NODE sends a Query message in accordance with RFC 2236. Since the DSL port is



bandwidth limited, the ACCESS NODE may remove the connection immediately if it determines that the channel is not required by any other STB. Alternatively the ACCESS NODE may decide not to remove the connection and leave the response to the Query message decide the connection removal. However, if in the mean time prior to receiving the response to the Query a "Join" (Report message) is received by the ACCESS NODE, the ACCESS NODE may remove the connection immediately if it determines that the channel is not required by any other STB.

In conclusion the ACCESS NODE, due to bandwidth limitation on the DSL port, requires some intelligence by removing connections prior to the Query response message.

Figure 31 shows the periodic behaviour of IGMP as being the periodic audit from the ACCESS NODE to each set top box asking for current group memberships. This is a Query to 224.0.0.1 which is a special group address, meaning all hosts, that all set top boxes listen to. This keeps the ACCESS NODE synchronized to all set top boxes that are attached to it. As a result of the audit the ACCESS NODE removes unnecessary connections or create connections that should have been there that were not.

Figure 31: IGMP Periodic Behaviour (GMQ)

8.5 QoS Requirements are application specific

The traditional IP and Ethernet layers are not capable of supporting reliable delivery of MPEG-2 content without an underlying QoS capability.

Some parameters for the end-to-end service class to ensure a video service is offered with reasonable quality include[3]:

8.5.1 Bandwidth

- Committed Information Rate
- Allowable burst rate

8.5.2 Delay characteristics

- Maximum set-up time
- Maximum delay
- Maximum delay variance

In today's broadband services environment it seems that no single service provider manages all of the network resources that deliver data end-to-end[4]. However, it is clear that the Access Node plays a crucial bandwidth management & efficiency role in service delivery. The Access Node can be managed in the context of an end-to-end network to help deliver a consistent and predictable broadband service experience to users.

8.6 Summary

This section shows that IGMP is a simple and robust channel changing protocol to support broadcast TV over DSL.

The Standard Bridge CPE modems or CPE Routers provide easy connectivity with the STB.

STB needs only to support IGMPv2 standard without any changes.

Any added intelligence or enhancement to the IGMP protocol can be implemented in the Access Node.

9. Multicast and PPP based Access Network Scenario

IP - Broadcast and Dial In Access Network Scenario Starting from the existing scenario which is described in chapter 13 the following steps will guide to an enhanced architecture.

9.1 Starting Network Scenario

Basically the following diagram is used to refer to the existing DSL network deployment:

---

[3] Broadband Content Delivery Forum "Proposed Architecture for the end-to-end management of network quality of service." Version 1.3, 22 October 2001.

[4] Broadband Content Delivery Forum "Proposed Architecture for the end-to-end management of network quality of service." Version 1.3, 22 October 2001.

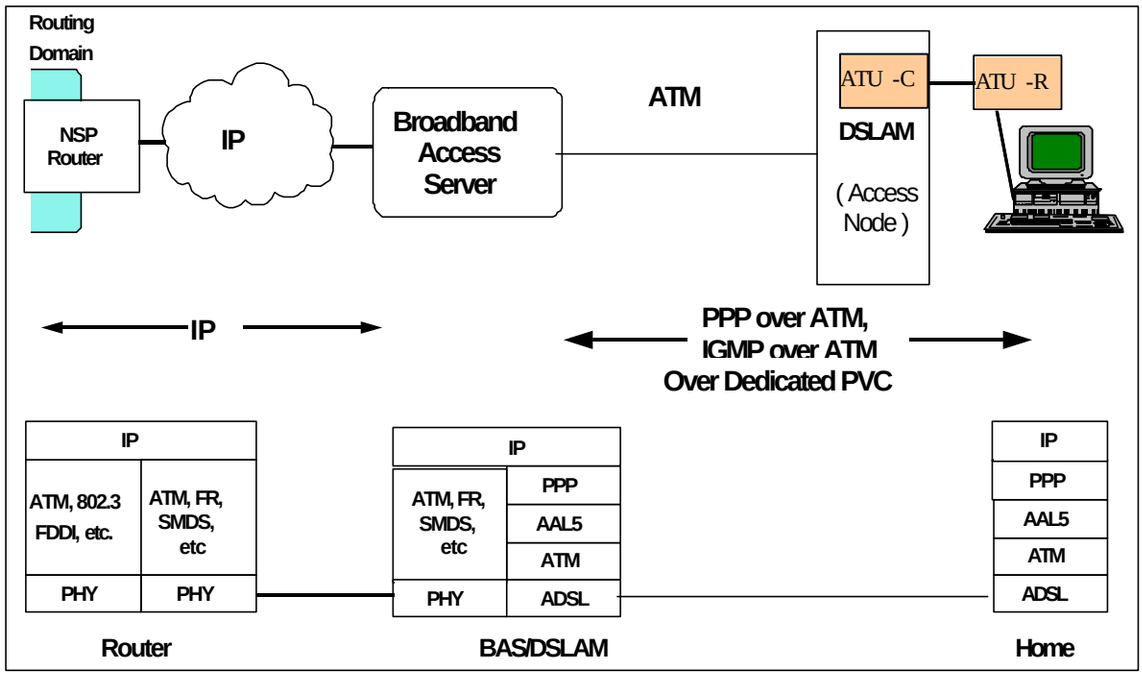


Figure 32 DSL Network Reference Diagram

As described in chapter 13 the network is used for providing DSL services being deployed to subscribers using ATM as the layer-2 technology from the subscriber (Home) and terminated at a broadband access server (BAS). The subscribers IP data is transported over PPP from the home end point and terminated at the BAS. The IP datagram then is routed over an IP infrastructure of the NAP carried by various layer-2 technologies that are NAP/NSP specific.

For broadcast services it is foreseen to use IGMP and a control function in the ACCESS NODE for control of access between different parallel streams which are delivered to the ACCESS NODE and carrying broadcast content like TV based on IP. From the perspective of traffic engineering it is necessary to save resources in the access network to locate the point for multicast as close as possible to the customer. Also aspects of guarantee of bandwidth and availability of service will lead to implement the access control functionality as close as possible to the subscriber. Therefore the most suitable element for this functionality is the ACCESS NODE.

9.2 Proposed target Network Scenario

The proposed target network scenario takes into account, that the design of an access network has to provide different services. But different services have different requirements regarding delay, availability and over subscription.

Service	**Authentication**	**Oversubscription**	**Multiplex Function in the ACCESS NODE**
VPN	No	No, dependent on QoS/SLA	ATM or PPP switching to MPLS; Segregation of traffic for groups of end users

PPP – dial in	Yes, e.g. Radius	Yes authentication support as close as possible to the customer reduces drastically network bandwidth / resources and gives QoS guarantees to customer that are in session	MPLS; Aggregation of residential customers and authentication Enabling of QoS to the customer without over subscription
Broadcast	Optional related to PPP – dial in	No Multicast support as close as possible to the customer reduces drastically network bandwidth / resources	IP multicast; Directs real-time traffic (e.g. video traffic) from one network server to a number of subscribers identified by a subscription list

9.2.1 Migration phase

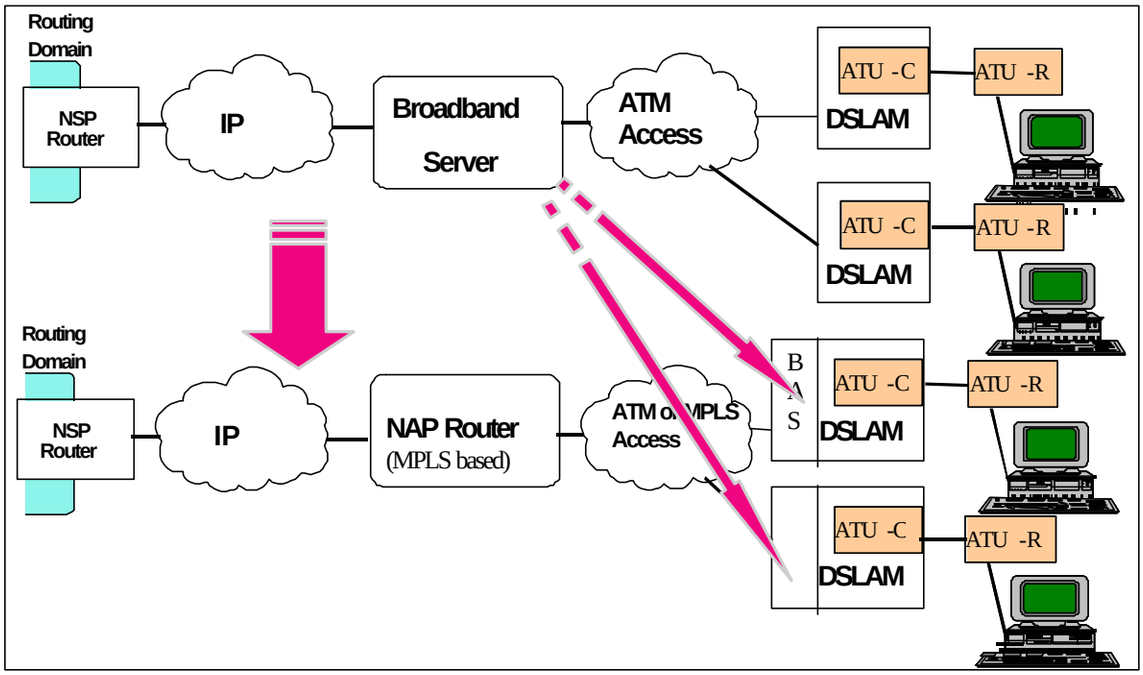


Figure 33: Integrated Multicast and PPP proposed scenario

Derived from the proposed target scenario of chapter 13 is shown a MPLS based access and core network that utilizes RFC 2547 to implement Virtual private networks within the core out to the edge of the network, PPP based dial in services and IP based broadcast services.

The ACCESS NODE takes the role of an integrated BAS and router with the additional capability of MPLS tagging based on RFC2547. From the starting scenario, PPP would be transported over L2TP inside an MPLS VPN toward the NSP.

In the case of authentication in the ACCESS NODE PPP will be terminated in the ACCESS NODE. A radius client will be necessary in the ACCESS NODE.

Additionally, the VPN could be used to transport RFC2684 (obsoletes RFC1483) based bridged or routed PDUs. This gives the NSP additional flexibility within a VPN, PPP - Dial In services and broadcast services. Additionally the new structure gives the flexibility of service generation. All control functions of authentication (PPP) traffic control and access control are implemented in the same element. Also from the point of management integration.

As an alternative an operator may use it's existing ATM-infrastructure for access BAS components at the ACCESS NODE side to connect to the NAP Router. This can be considered as an intermediate step of migration.

9.3 Drivers

Main drivers for this proposed target network beside the requirements of chapter 13 are depicted as follows. From service perspective and traffic engineering aspects it is expected that Network Access Provider and Network Service Provider will migrate if IP is the common network layer protocol. The functionality and the responsibility of the services will have an impact as well to NSP and NAP. But the differentiation between NAP and NSP will lose importance. Therefore NAP and NSP is included in one chapter.

Network Access Provider / Network Service Provider

Network Structure:

- Integrates with emerging core and access MPLS network.
- Integrates with existing routed and ATM switched infrastructure.
- Provides an aggregation capability for grouped subscribers (service level granularity).
- Provides an aggregation capability for individual subscribers
- Simplify the access because only one PVC must be established

QoS and SLA

- VPN creation signaled throughout the network versus manually provisioned per node.
- QoS guarantees from NAP/NSP based on VPN SLA(s).
- Provides SLA for broadcast and dedicated access control

Service delivery

- Provides termination of zapping control functions for broadcast
- Provides Management - integration for simplifying service delivery
- Standard benefits of a VPN (private addressing, etc), broadcast services and PPP based dial in services

End User

- Easy integration of new services – self provisioning possible
- Simplifying of service delivery – access control by NSP/NAP over PPP authentication centralized by RADIUS server
- Simplifying of CPE structure – one PVC between ACCESS NODE and CPE.

9.4 Options/Requirements

This section supports the basic requirement on the ACCESS NODE to support MPLS and VPNs as well as PPP and broadcast services. The migration of functionality of NSP and NAP gives an option for new structures in service delivery.

The ACCESS NODE terminates the ATM layer, and uses the physical port/VC coupled with the IP header to determine which VPN it belongs to. From a signaling perspective, the ACCESS NODE supports IP routing protocols like described in chapter 13. Additionally the ACCESS NODE terminates PPP to give the platform for authentication of the customer. Also the broadcast functionality (IGMP) makes the ACCESS NODE to an universal network element.

From the efficiency perspective this migration scenario is assumed that an oversubscribed access network already exists. One key success factor of this architecture is that it enables a smooth migration.

From the technical point of view Access Nodes should be used which that can be subtended and cascaded to aggregate more customers than the existing network link capacity can support.

From the traffic engineering perspective the conflict of the oversubscribed network versus QoS per subscriber can be resolved as described.

10. QoS IP Services through RSVP over ATM SVC in DSL network

This section describes the use of RSVP, including all the necessary extensions, to establish guaranteed QoS IP sessions over a signaled QoS network. The examples of signaled QoS network are ATM SVC network and MPLS network with proper UNI signaling.

10.1 Starting Network Scenario

The Access Node (i.e. the Access Node) connects to an ATM Regional Broadband Network (RBN), providing connectivity to an aggregation device, i.e. the broadband access server (BAS). The aggregation device terminates the ATM PVC and passes the IP packets onto the service provider in a routed infrastructure. If SVCs were to be used then in the starting network scenario there is no ability to map IP QoS into ATM QoS. In the starting network scenario SVC connection set-up and service activation is through proprietary means.

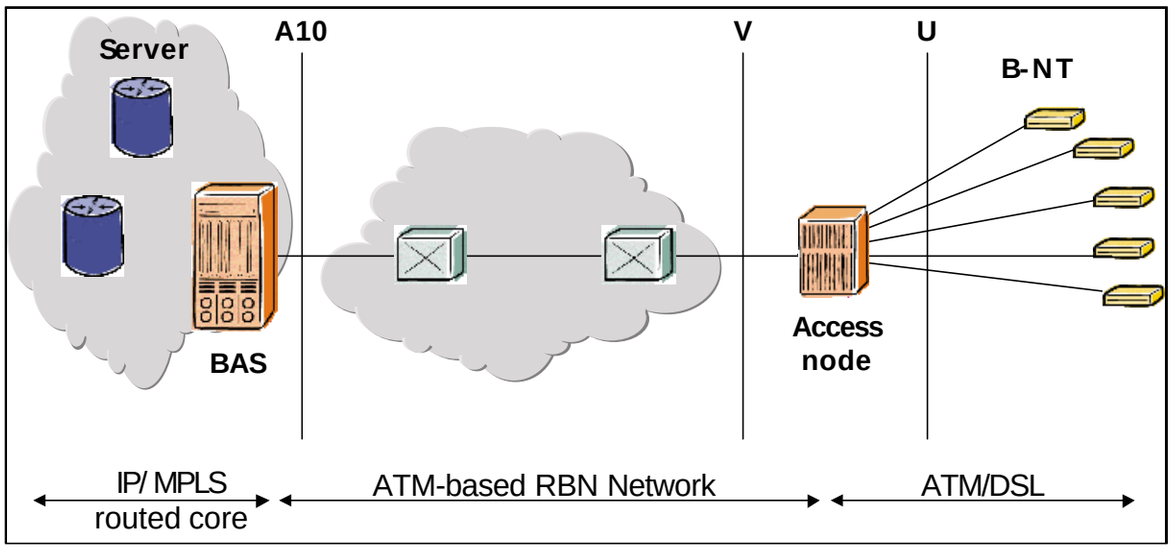


Figure 34: Starting scenario: Traditional ATM RBN

10.2 Target Network Scenario

This section discusses bridging native IP over native signaled QoS network (e.g. ATM SVC, MPLS) where UNI signaling of Signaled QoS Network (SQN) is used to support QoS tunnel, RSVP with extension is used to support QoS IP flow.

Bridging Device will take IP flow sent by IP Device and map them into proper QoS tunnel established in the signaled QoS network. QoS IP packet goes into QoS tunnel (e.g. CBR VC, VBR VC); best effort IP packet goes into best-effort tunnel (e.g. UBR VC). The entire tunnel establishment and IP flow to tunnel mapping happen dynamically through

RSVP and QoS network signaling without management system intervention. This approach provides a scalable solution to offer IP QoS service with today's IP network and signaled QoS network.

10.2.1 QoS IP Services

With development of audiovisual application on the current Internet, the demands for predictable bandwidth and delay support are increasing in the IP network, which currently supports best effort communications. On the other hand, there are signaled QoS networks such as ATM SVC, MPLS LSP which are switched multiplexing with QoS tunnel (VP/VC, LSP), and guaranteed QoS per tunnel through signaling. It is quite natural to use these distinctive functions of signaled QoS network to support QoS IP service.

Figure 1 shows an example scenario of network infrastructure for offering QoS IP service over SQN.

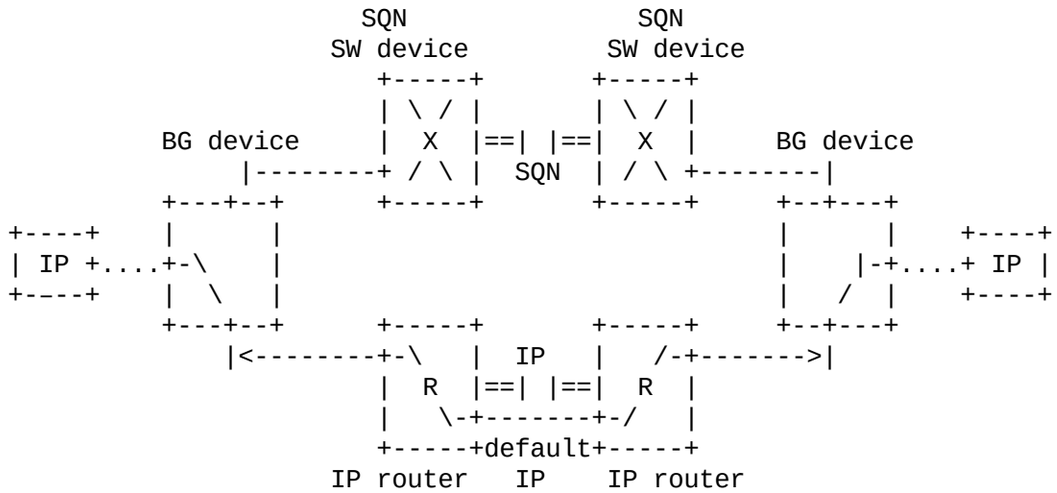


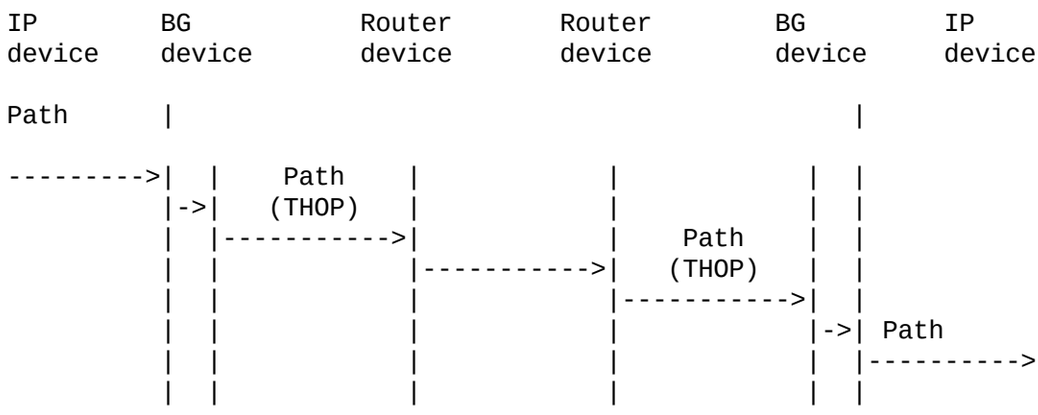
Figure 35: Example scenario of network for QoS IP

A default IP connection is established between IP devices through IP routers across IP networks. This default IP connection is used for normal best effort IP traffic between IP devices. However if an IP device requests a QoS IP session for a period of time, a QoS tunnel will be dynamic established between bridging devices across SQN networks. Hereafter, bridging device will route QoS IP flow through QoS tunnel instead of default IP connection during the period of QoS session.

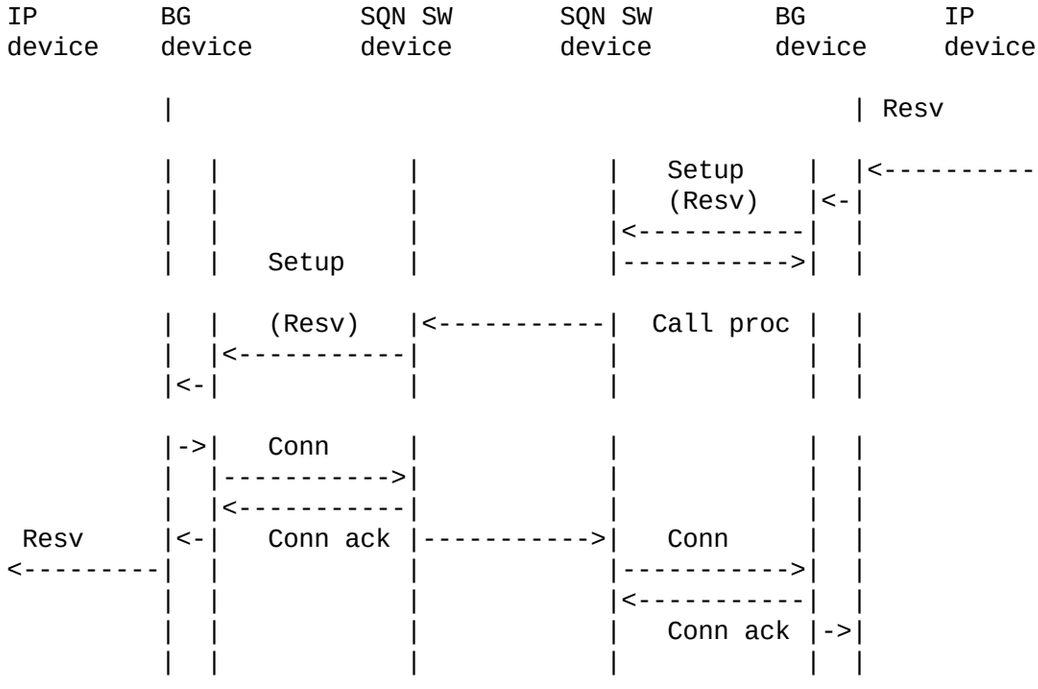
RSVP with minor extension is proposed for the QoS IP session setup protocol. The SQN UNI signaling MUST be the general connection setup protocol with confirmation procedure, for example ATM UNI 3.1 or ATM UNI 4.0.

10.2.2 QoS IP Session

Figure 2 depicts an example procedure for QoS IP session establishment.



A. Sender's Path procedure



B. Receiver's Resv procedure

Figure 36: Example procedure for QoS IP session

Sender IP device sends a RSVP Path message for each QoS IP flow it originates. It MAY contains a RSVP_CYSPEC object specifying bidirectional traffic characteristics of QoS IP flow instead of RSVP SENDER_TSPEC.

As in Figure 2.A, a Path message travels from a sender to receiver(s) along the default IP connection path used by the regular data packets. The sender Bridging device MUST insert its SQN address (e.g. ATM NSAP address) as

RSVP_THOP object. All RSVP-capable routers along the path(s) MUST NOT modify this object. However, they MAY insert additional RSVP_THOP object(s) according to the rule defined in Section 4.1.

The receiver Bridging device(s) capture the Path message and cache the mapping of the sender's IP address to the SQN address(s) in RSVP_THOP(s). It SHOULD remove the RSVP_THOP object(s) before passing Path message to the receiver IP device.

As in Figure 2.B, receiver IP device receives and validates the Path message. It then responds a RSVP Resv message. It MAY contains a RSVP_CYSPEC object confirming bidirectional traffic characteristics of QoS IP flow instead of RSVP FLOWSPEC.

Receiver Bridging device captures the Resv Message and launch a SQN call Setup message (e.g. ATM UNI SETUP) to the longest "short-cut" SQN address for a SQN QoS tunnel (e.g. ATM SVC). The SQN UNI signaling MUST support User-to-User signaling which enables the transfer of information between end-to-end users in the SQN (e.g. UU IE of ATM). The UU IE of the call Setup message MUST contain the Resv message. The assignment of Resv message in UU IE MUST follows RFC 3033 [16]. The traffic characteristics of SQN QoS tunnel MUST be constructed from RSVP traffic characteristics objects according to RFC 2210 [11], RFC 2211 [12], and RFC 2212 [13]. If SQN is ATM SVC network, the RFC 2381 [14] and RFC 2382 [15] MUST be followed in addition to above RFCs. If Resv message does not contain RSVP_CYSPEC, the upstream traffic characteristics of bidirectional SQN QoS tunnel are local matter. However, it is suggested that upstream QoS MAY be algorithmically calculated from RSVP FLOWSPEC.

Thereafter, the Resv message travels "short-cut" path from receiver to sender instead of typical hop-by-hop default IP connection path. Sender Bridging device validates Resv with cached Path and accepts corresponding SQN call Setup. The Resv message is forwarded to sender IP device.

Finally, both sender and receiver Bridging devices notify the IP layer entity that a new SQN QoS tunnel is established. Based on this information, the IP layer entity moves the QoS IP session to the new QoS tunnel as in Figure 3.

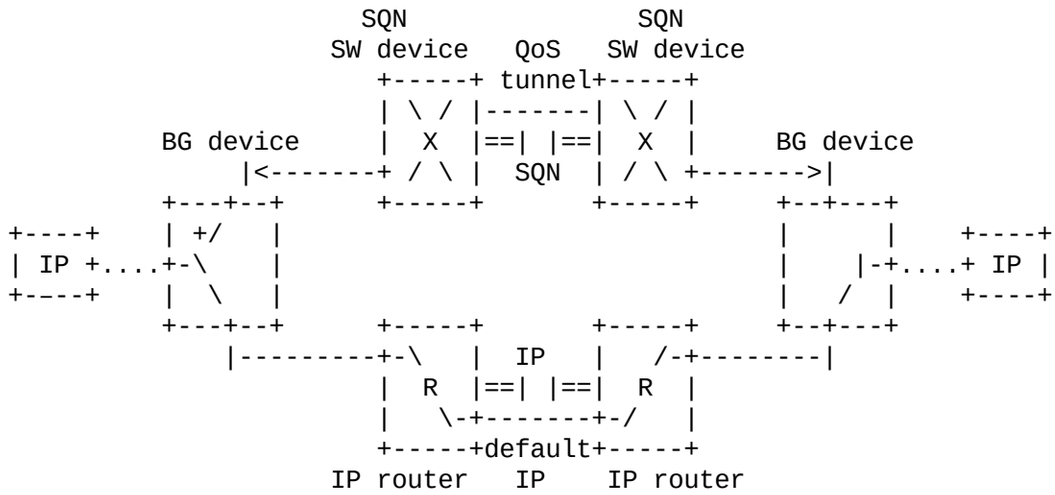


Figure 37: Example of new SQN QoS tunnel for QoS IP

The "soft state" natural of RSVP 2205 [10] SHALL be maintained to avoid orphan SQN QoS tunnel. Substantial losses of RSVP refreshment messages MUST cause a SQN QoS tunnel teardown.

10.2.3 Accounting Considerations

The usage accounting data is normally associated with calling party of SQN QoS tunnel. However, according to the previous section the SQN calling party is the receiver of RSVP Path message. Therefore a new RSVP_SVCSPEC reverse charging object is proposed to allow that accounting data can be associated with SQN called party. The called party of SQN QoS tunnel is the sender of RSVP Path message.

A Path and Resv message MAY contain RSVP_SVCSPEC reverse charging object to indicate that sender would like to accept the accounting charge instead of receiver bearing the charge. Bridging device MUST set the reverse charging indicator in SQN call Setup message when RSVP_SVCSPEC reverse charging indicator value is 1 (TRUE). If SQN UNI signaling does not support reverse charging, Bridging device MUST reject the RSVP message with corresponding error message.

10.3 Drivers

The specified approach is very scalable with large number of service subscribers and incurs minimum administrative and operation overhead of service providers.

10.4 Options

It is proposed that three additional objects that extend RSVP, allowing the establishment of guaranteed QoS IP sessions from an IP Device to a Bridging Device of QoS network using RSVP as a signaling protocol. UNI signaling protocol of signaled QoS network then allows establishment of guaranteed QoS tunnel among Bridging Devices, through which guaranteed QoS IP sessions are tunneled. Consequently, the guaranteed QoS IP sessions among IP Devices are established over the signaled QoS network.

10.4.1 Additional RSVP Object Definitions

All the additional objects are defined here. The object follows format described in RFC 2205 [10]. The Class-Num of objects SHOULD be 11bbbbbb (192+).

10.4.2 RSVP_THOP

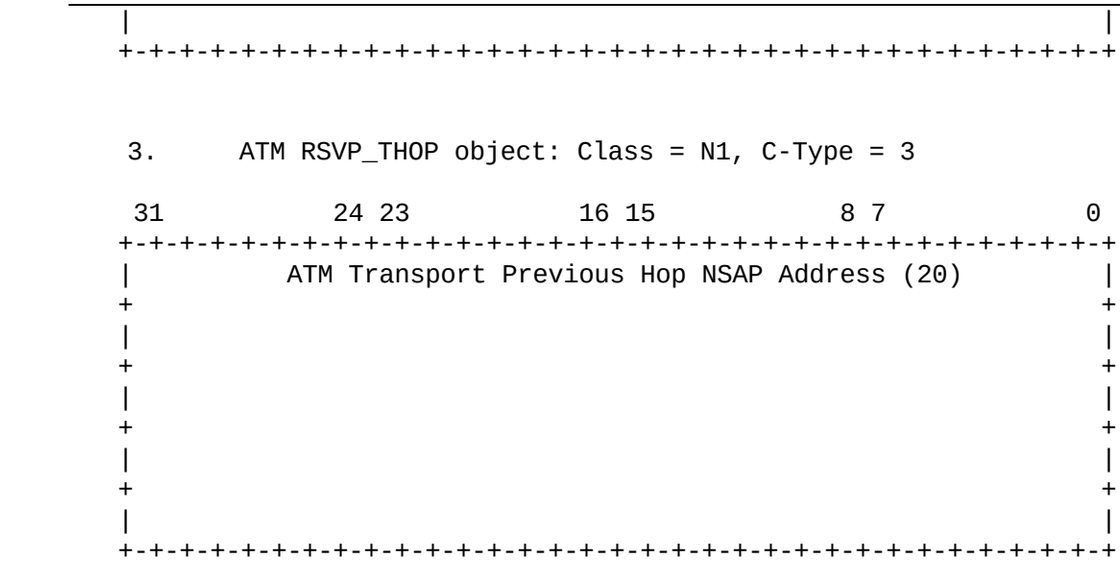
```
RSVP_THOP (transport hop) class = N1.

   1.     IPv4 RSVP_THOP object: Class = N1, C-Type = 1

    31           24 23           16 15            8 7             0
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             IPv4 Transport Previous Hop Address (4)           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


   2.     IPv6 RSVP_THOP object: Class = N1, C-Type = 2

    31           24 23           16 15            8 7             0
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             IPv6 Transport Previous Hop Address (16)          |
   +                                                               +
   |                                                               |
   +                                                               +
   |                                                               |
   +                                                               +
```



3. ATM RSVP_THOP object: Class = N1, C-Type = 3

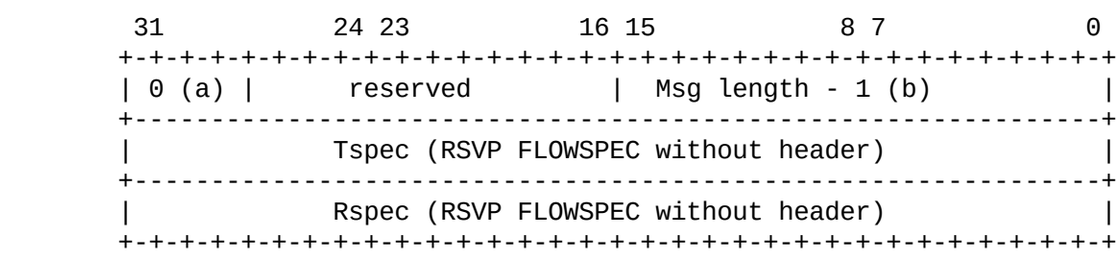
This object class MAY appear in RSVP Path message. It carries the transport network address of the interface through which the Path message was most recently sent. Only the IP Device that egress interface of RSVP Path message is connected to SQN (e.g. ATM SVC network) and ingress interface of RSVP Path is connected to a different transport network does send out this object. All other IP Devices must pass the object without modification. Multiple

RSVP_THOP objects MAY appear in a PATH message. The order of objects in the Path message MUST be LIFO (Last-In-First-Out).

10.4.3 RSVP_CYSPEC

RSVP_CYSPEC (bidirectional flow spec) class = N3.

1. RSVP_CYSPEC object: Class = N3, C-type = 2



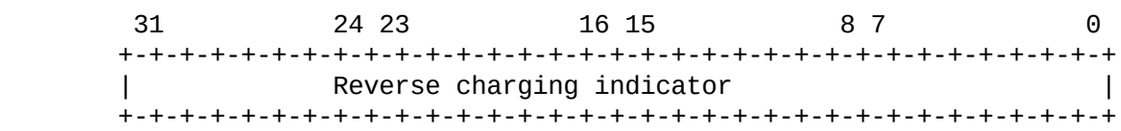
(a) - Message format version number (0)
(b) - Overall message length not including header word

This object contains bidirectional IP flow specification. It MAY appear in RSVP Path and Resv message. The Tspec field describers sending flow spec, Rspec field receiving flow spec. Rules for composing RSVP FLOWSPEC are defined in RFC 2210 [11].

10.4.4 RSVP_SVCSPEC

RSVP_SVCSPEC (SerViCe Specification) class = N4. This object class supports value-added RSVP service signaling from IP Device to IP Device.

1. RSVP_SVCSPEC reverse charging object: Class = N4, C-type = 2



This object contains a Boolean value to indicate whether RSVP Path message sender requests "Called Party Pay" feature of SQN. A value of 1 (TRUE) indicates "Called Party Pay". A value of 0 (FALSE) indicates no "Called Party Pay". Other values are not defined. It MAY appear in Path and Resv message.

10.4.5 Security Considerations

The same considerations stated in RFC 2205 [10] apply to this section. There are no additional security issues raised in this section regarding RSVP.

If the signaled QoS network is ATM SVC network, the same considerations stated in RFC 3033 [16] apply to this section. There are no additional security issues raised in this section regarding ATM UNI signaling.

If the signaled QoS network is other type network, the proposal in this section does not weaken the security of UNI signaling of that network.

11. Evolution to a Next Generation Network: MPLS Overview

11.1 Existing Network Scenario

DSL deployment has been mainly driven by the high demand for residential high-speed Internet access services. To meet this internet access demand DSL rollout has resulted in an increasingly widespread presence of ATM ACCESS NODEs in the central office and in remote locations. A number of possible evolution scenarios and some drivers for moving towards Next Generation Networks have been identified **[17]**. This inertia for ATM and the eventual need for change, translates to a number of networking scenarios that could potentially exist in the future.

Figure 38 depicts the reference architecture that this section refers to. The Access Node (i.e. the ACCESS NODE) connects to an ATM Regional Broadband Network (RBN), providing connectivity to an aggregation device, i.e. the broadband access server (BAS). The aggregation device terminates the ATM PVC and passes the IP packets onto the service provider in a routed infrastructure. Content will often be located in a centralized service provider datacenter. The names of the different interfaces are shown, as defined in **[18]**.

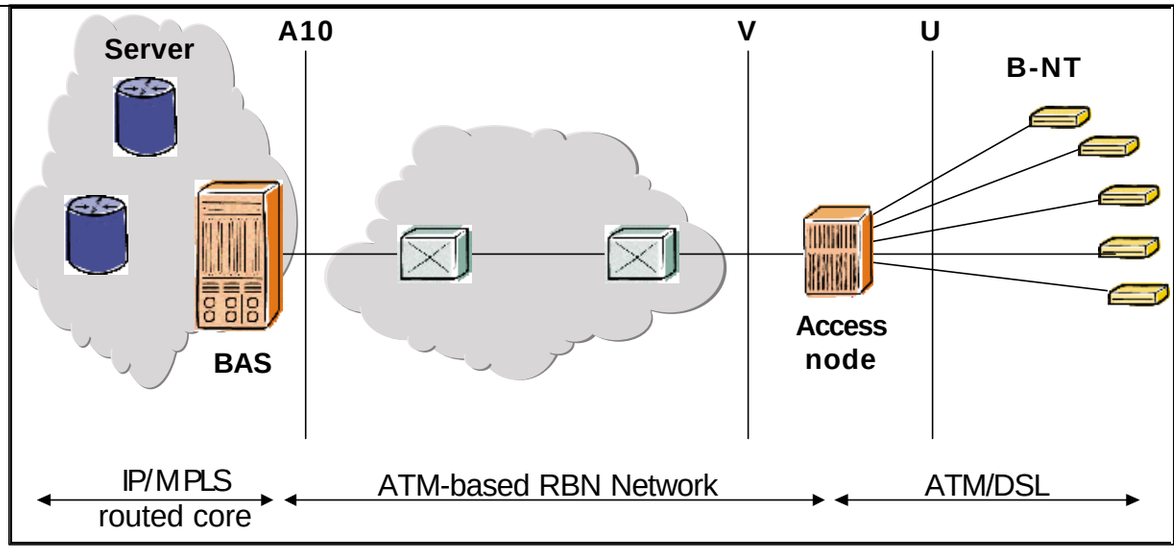


Figure 38 : Existing network scenario - Reference Architecture

11.2 Proposed target Network Scenarios

The prime focus of this section is to consider and compare several possible evolution scenarios for introducing MPLS into the aggregation network. Implementing MPLS in the BAS across the A10 interface to the V interface to the Access Node is a new concept that has not previously been fully addressed within the DSL Forum. It is this new architectural concept of MPLS between the BAS and Access Node (and the BAS and the Broadband Network Termination) which is the prime topic of study that follows in this section.

Examples of of high level scenarios that could utilize MPLS technology include:

- Co-existence of the installed base of ATM access networks with next generation access networks with some degree of MPLS capability;
- ATM access networks which include MPLS capabilities and functionality;
- End-to-end MPLS architectures;
- Some combination of the above.

First, the different drivers for the use of MPLS technology in the DSL aggregation network are given. Then the advantages and disadvantages of several next generation network scenarios are discussed. These scenarios are:

- 11.4.2 MPLS to the access node
  - 11.4.3 ATM-MPLS L2 Cross-Connect
  - 11.4.4 BGP/MPLS VPNs
- 11.4.5 MPLS to the B-NT
  - 11.4.6 Full MPLS using an MPLS PVC UNI
  - 11.4.7 Support of MPLS and MPLS PVC UNI over ATM access link
    - ATM is used for transporting MPLS packets

- MPLS is mapped on ATM

This section descibes architectures that use MPLS for setting up static connections, equivalent to ATM (S-)PVCs in the starting network scenario. Therefore the use of MPLS for dynamically setting up connections between the CPE and the BAS is not in the scope of this section. The conclusion to this section summarizes proposed migration steps. This should assist service providers in forming the appropriate evolution plans for their DSL equipment.

Given the likelihood of the scenarios above, consideration should be given to issues of total network ownership and operation. Operational processes which consolidate and improve the management of existing ATM access networks while effectively managing new MPLS functionality should be examined. In particular these next generation architectures should be cognizant of and take advantage of the recent work in the Auto-Configuration WG and Flow-Thru Service Fulfillment WG.

11.3 Drivers

Multi-Protocol label switching (MPLS) is a key technology for enabling service providers to respond to the challenges of next generation internetworking. To date the traffic engineering and also the VPN capabilities of MPLS have been used predominantly to cope with growth in the core of the internet.

- MPLS functionality is becoming increasingly available in BAS to inter-work with core MPLS routers.
- MPLS functional capability is available on many ATM switches that are installed in regional broadband networks[5]. This latent MPLS functionality could potentially be activated for use in end-to-end networks.
- A number of standards bodies are currently working on ATM-MPLS networking standards[6]. The relevance of this work should be considered in next generation DSL access architectures.
- MPLS features such as traffic engineering and QoS can also be used for non-ATM networks, for example Gigabit Ethernet. This versatile nature of MPLS makes it possible to provide a consistent traffic engineering methodology across heterogeneous RBN networks of ATM and non-ATM nodes. Another alternative is to use MPLS for future non-ATM networks, while keeping the reference ATM architecture unchanged for existing deployments.
- New work on MPLS OAM[7] is being developed which will result in useful capabilities for network operations such as:
    - Ensure that MPLS becomes a reliable network platform that can be operable, administered, and maintained through appropriate user-plane mechanisms.
    - Allow development of simple, consistent and measurable availability and QoS SLAs for services such as MPLS-based VPNs.
    - Drive down operational effort
    - Protect the security/integrity of the network.

---

[5] 2001 Multiservice WAN Switch Market Analysis: Yankee Group, Report Vol 2, No.12 – October 2001

[6] e.g. ATMF: AF-AIC-0178.000 “ATM-MPLS Network Interworking”,

IETF: a number of drafts are under discussion in the Pseudo Wire Emulation Edge to Edge (PWE3) working group,

ITU-T Y.atmpls draft Recommendation on ATM-MPLS network interworking

[7] IETF draft-harrison-mpls-oam-req-01.txt

- Reduce defect detection time and, thus, increase reliability.

11.3.1 Future Safeness and Ease of Migration

MPLS has the property that it can very easily be used over existing (connection-oriented) technologies that already perform the switching of data units on the basis of a fixed field in the datagram's header, such as ATM and Frame Relay.

11.3.2 Multi-protocol Capability

Using MPLS it is possible to provide 'virtual connections' from a user to a service provider in a scalable way over any technology, be it ATM, Frame Relay, Ethernet, plain IP or any other technology.

11.3.3 Multi-service Capability and VPNs

MPLS allows transport of any type of service, both IP based (e.g. IPv4, IPv6) or non-IP based (e.g. voice, TDM). Furthermore, MPLS is a tunneling technique allowing support for several types of VPNs. These can be categorized according to the type of data that is being transported, or according to the place where the MPLS tunnels are initiated. Both layer 2 and layer 3 VPNs are supported. Although it is becoming clear that MPLS can play a role in gracefully linking ATM-based and packet (e.g. Ethernet) based access networks together, the ATM footprint is widespread in DSL access networks and have well established operational methodologies. This is because Ethernet technology is still missing a large amount of basic functionality for use WAN technology in carriers' networks. This includes Quality of Service, end-to-end service provisioning, service management and OAM support.

11.4 Options

In the remainder of this section, the advantages and disadvantages of the next generation network scenarios are given. The description is divided in two sections. First, the next generation network scenarios using MPLS between the ACCESS NODE and the BAS are explained. Then, the use of MPLS up to the CPE is described as an extension to the first scenarios.

Table 6 summarizes the possible next generation network scenarios. Primary focus will be put on architectures using MPLS for setting up static connections, equivalent to ATM (S-)PVCs. For completeness, the last row indicates a combination of the second and third scenario. Therefore the conclusions will purely be a combination of both and need not be put in a separate section.

		BAS -> Access Node			AN ->B-NT		
	BAS / Voice Gateway Functionality	Data plane	Control plane	Access Node Functionality	Data plane	Control plane	B-NT Functionality
MPLS to the DSLAM	LER	LSP	MPLS (optional)	LER	ATM	ILMI	ATM
	LER	LSP	MPLS + BGP (RFC 2547)	Router + LER (PE)	ATM	ILMI	ATM + Routing protocols on IP (CE)
MPLS to the CPE	LER	LSP	MPLS (optional)	LSR	LSP	MPLS PVC UNI	LER
	LER	LSP	MPLS + BGP (RFC 2547)	LER + Router + LER (PE)	LSP	MPLS PVC UNI	LER + Routing protocols on IP (CE)

Table 6: Possible next generation network scenarios

Note that the (optional) control plane that is used in the architectures and scenarios described in this section is based on IP protocols, and thus uses IP addressing. The used IP addresses have only a local meaning within the access network, and will only be used for the establishment of MPLS tunnels. This places a requirement on the access network elements: they will need to participate in IP routing, but due to the specifics of an aggregation network (regarding the network topology and functions), some network elements will only need a limited IP routing/forwarding intelligence, e.g. default and/or static routes.

11.4.1 ATM Considerations

Beyond the MPLS specific drivers, the introduction of MPLS only makes sense if it brings similar or added advantages when compared with ATM technology. Topics which should be considered in a next generation DSL access architecture include the following.

11.4.1.1 Connection configuration

In many existing ATM access networks, changes in the network are dealt with by means of flow-through provisioning. This requires configuration of the network elements supporting the connection. For the CPE, the connection parameters are often pre-configured. Over the last months a lot of progress has been made in the standardization of both the auto-configuration of the CPE and Flow-Thru Service Fulfillment in existing network architectures **[19][20]**. The auto-configuration architecture now allows the CPE to retrieve the connection parameters itself, including all the necessary information to support the diversity of possible protocol stacks. The Flow-Thru Service Fulfillment process

has optimized the interaction process between several administrative domains, with a minimized configuration effort as a result.

In order to reduce the amount of configuration needed for establishing PVCs, S-PVCs can be used. This method requires only the endpoints to be configured. Additionally, hybrid S-PVCs are increasingly being used in ATM based broadband networks. Their role is to reduce the amount of management configuration tasks for PVC establishment, without impacting the operation of the Access Node and access server. This means that the endpoints use classical PVC operation, whereas S-PVC operation is used inside the Regional Broadband Network (RBN) network. These mechanisms have improved the ability to configure ATM based DSL access networks. Setting up MPLS connections in the access network can be done using (manual) configuration. Alternatively, MPLS can make use of a control plane that is based on IP-protocols. This means that IP addresses are used for identifying devices in the network, instead of ATM addresses. Deploying this dynamic signaled control plane could be used to efficiently cope with configuration tasks, comparable to the use of ATM (hybrid) S-PVCs

ATM and FR already have a control plane that allows traffic engineering type features, whereas traditional Ethernet and IP do not. Today PNNI is typically used as the control plane in RBN networks using ATM. Even in heterogeneous RBN networks (e.g. ATM-MPLS Network Interworking) ATM and MPLS control planes can exist within separate sub-domains (i.e. MPLS control for the MPLS network segment(s), ATM control for the ATM network segment(s). Only when the Access Node (ACCESS NODE) uses non-ATM network interfaces to the RBN does consideration for a full MPLS control plane implementation become necessary.

11.4.1.2 VP/VC scalability

ATM technology has established mechanisms that can be used to ease connection set-up and improve network scalability. Well know techniques to minimize the configuration effort and reduce the amount of connection identifiers are VC stacking using the concept of VP cross-connects, and VC merging. The concept of ATM VC merging has been introduced in an MPLS environment in the form of *label merging*. Another MPLS mechanism that can be used to improve scalability is *label stacking*. Each MPLS shim header consists of a 20-bit label value, theoretically allowing 1M connections on an interface. Adding multiple shim headers to the data can extend this. This MPLS nesting capability could be used to assist the when the NAP performs service unbundling for the NSP. The first label can be used to provide connectivity over the access network, whereas the second label further directs the data to the appropriate NSP.

11.4.1.3 Support of IP QoS

ATM QoS parameters and mechanisms are widespread and pervasive in DSL access networks today. Despite the success of ATM it is also true that almost all services offered on DSL networks are IP-based. MPLS uses IP-based signaling and negotiation of QoS on the basis of IP QoS parameters, and the mechanisms that have been defined for MPLS to support QoS are all IP QoS mechanisms (DiffServ E-LSPs and L-LSPs, or IntServ RSVP-TE).

11.4.2 MPLS To the Access Node

This section discusses the next generation network scenarios corresponding to the first two rows of

Table 6. In both scenarios there is no impact on the operation of the CPE. Specifically:

- There is no need to introduce MPLS functionality in the CPE
- It works with all existing ATM-based CPE. In fact, the CPE is not aware of this change deeper in the network
- If (auto-configuration) protocols are used by the CPE, the operation remains unchanged. This means that maximum use of Auto-Configuration procedures can be made.

This scenario represents an incremental approach, in the sense that MPLS awareness can still be added to the CPE in a later stage, by introducing the MPLS PVC UNI over the access link (see section 11.4.6). It is also incremental in the sense that MPLS could later on evolve to be the unifying signaling layer in the ATM and packet based networks. Note that in

Table 6, 'LSP' indicates that an LSP data plane is used on any layer 2 mechanism.

11.4.3 ATM-MPLS L2 Cross-Connect

The MPLS data plane is introduced between the ACCESS NODE and the BAS / Voice Gateway. This means that Label Switched Paths (LSPs) can be setup in the aggregation network. The impact on the access network is controllable, because the use of the MPLS control plane is not mandatory. The equivalent of ATM PVCs can also be used in the MPLS network. This means that each LSR is configured with the necessary label switching information. If the MPLS control plane is introduced, it can be used to offer the equivalent of ATM S-PVCs or hybrid S-PVCs. In the remainder of this section, this ATM-MPLS Interworking scenario is called the "ATM-MPLS L2 Cross-Connect". This refers to the fact that MPLS is used as a layer 2 technique analogous to ATM. This approach is described in more detail in **[21]**.

The ATM-MPLS L2 Cross-Connect network scenario is shown in

Figure 39. The CPE uses existing techniques to retrieve a list of available ATM connections. When sending ATM cells to the ACCESS NODE on a chosen VPI/VCI, the ACCESS NODE cross-connects the ATM connection to an MPLS LSP. The ACCESS NODE acts as a Label Edge Route (LER). This means that it is the device where the LSP is originated and where the MPLS label is added to the data. Once this is done, the MPLS packet is sent to the next hop in the aggregation network. The BAS terminates the LSP and removes the MPLS label(s) from the packet. Analogously, downstream MPLS packets arriving at the ACCESS NODE are placed on the appropriate ATM VP/VC towards the customer.

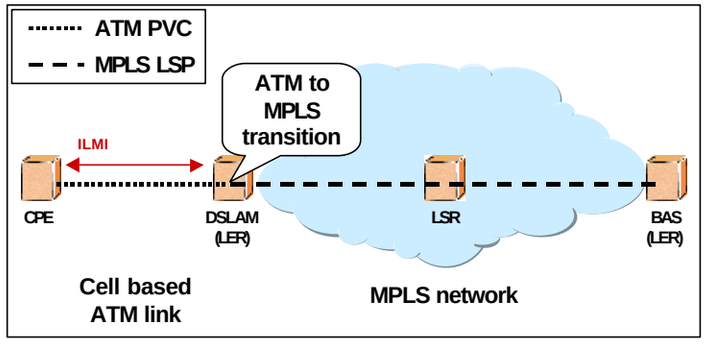


Figure 39: ATM-MPLS L2 Cross-Connect. Layer 2 forwarding is done in the ACCESS NODE

MPLS is used as a cross-connect layer 2 technology. Determining the label in the ACCESS NODE is not done based on IP address information, but purely on the ATM VPI/VCI. This first step enables scalable and flexible aggregation to take place in the network.

The newly introduced MPLS control plane can be used in two ways. The first option is to setup a single LSP per customer in the aggregation network. This can be interesting in case QoS guarantees need to be given to the connection. However, to improve scalability, the access provider can also establish large LSP pipes between the ACCESS NODEs and the BASs. These *pipe LSPs* (pre-configured LSPs) will be used to aggregate user connections that do not require dedicated resources and that can be served with aggregated resources. According to the provider's policy, more than one pipe can be established between a certain ACCESS NODE and a BAS, for example with different QoS/CoS guarantees. The equivalent in a pure ATM network is the manual/signaled establishment of VP pipes.

11.4.3.1 Required changes

For this scenario, the Access Node and access server have to interface with the MPLS network. This means that the network-side of the Access Node and the access-side of the BAS must be foreseen with an MPLS data plane. The same holds for the interfaces of the intermediate switches. The Access Node has to be frame aware and perform SAR on the access link. The Access Node uses MPLS to support either dedicated pipes per customer or pipe LSPs, carrying traffic from multiple customers. Optionally, the MPLS control plane is introduced to enable the equivalent of ATM S-PVCs.

11.4.4 BGP/MPLS VPNs

The next generation network scenario described in this section describes how the concepts of BGP/MPLS VPNs can be used in the aggregation network. The main difference with the previous section lies in the fact that MPLS is now used as a layer 3 tunneling technique instead of a layer 2 tunneling technique.

BGP/MPLS VPNs are traditionally used for supporting IP VPNs. This is defined in RFC 2547 **[22]**. The RFC describes how a VPN topology in an IP environment can be established between a number of Customer Edge devices (CEs) connected to Provider Edge devices (PEs). When used in an meshed network environment consisting of routers, this technique allows VPN topology discovery using BGP extensions and automated VPN establishment between the PEs using MPLS signaling.

The BGP/MPLS network scenario is shown in

Figure 40. When introducing BGP/MPLS VPNs in the aggregation network, the ACCESS NODE and BAS — being the endpoints of the MPLS tunnels — will both act as a PEs and are both IP routers and LERs. The customer's CPE connected to the ACCESS NODE will then act as CE. Also, both ACCESS NODE and BAS will handle BGP signaling and its extensions, in order to discover the VPN topology.

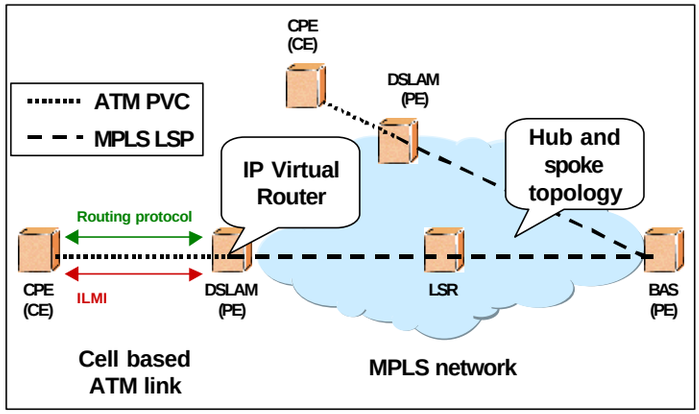


Figure 40: BGP/MPLS VPNs. Layer 3 forwarding is done in the ACCESS NODE

The connection between the CPE and the ACCESS NODE can be any point to point link, but the install-base of ACCESS NODEs will predominantly use ATM and ILMI. On top of the connection, the CPE will most likely use a routing protocol to communicate with the ACCESS NODE and discover the available routes.

11.4.4.1 Required changes

For this scenario, the Access Node and access server have to interface with the MPLS network. This means that the network-side of the Access Node and the access-side of the BAS must be foreseen with an MPLS data plane. The same holds for the interfaces of the intermediate switches. Additionally, BGP and its extensions defined in RFC 2547 need to be supported by on the network-side of the Access Node, the access-side of the BAS and possibly on the intermediate switches as well. Although the CPE is not MPLS aware, there is a need for routing protocols, in order to distribute the VPN routes to the CPE and vice versa.

11.4.5 MPLS to the B-NT

This section discusses the next generation network scenario corresponding to the third row of

Table 6. In this case, the B-NT will be impacted by the use of MPLS in the aggregation network, but the CPE will only be able to determine the available MPLS LSPs and not dynamically setup LSPs itself. Note that in

Table 6, 'LSP' indicates that an LSP data plane is used on any layer 2 mechanism. Because the MPLS data plane can be used on any layer 2 technology, this also holds for the access link. Although the access link can make use of packet based technologies, the installed-base is predominantly using ATM. Specific observations on the operation of MPLS over the ATM access link is described in section 11.4.7.

11.4.6 Full MPLS using an MPLS PVC UNI

This next generation network scenario is shown in Figure 41. It is basically an extension of the ATM-MPLS L2 Cross-Connect scenario. The MPLS data plane (and optionally the control plane) is once again introduced in the aggregation network, but in addition to this the CPE is also MPLS aware. As such the CPE can send and receive MPLS packets, but cannot establish LSPs itself. Instead it is able to find out about the LSPs that are available in the aggregation network and make use of these. This is achieved by defining a new UNI, the so-called MPLS PVC UNI. The MPLS PVC UNI allows the CPE to retrieve a list of available LSPs. As a minimum, the MPLS PVC UNI will indicate the label(s) to use to make use of the LSP in the aggregation network. Because the CPE adds the MPLS label, it will be a LER and the ACCESS NODE will be an LSR.

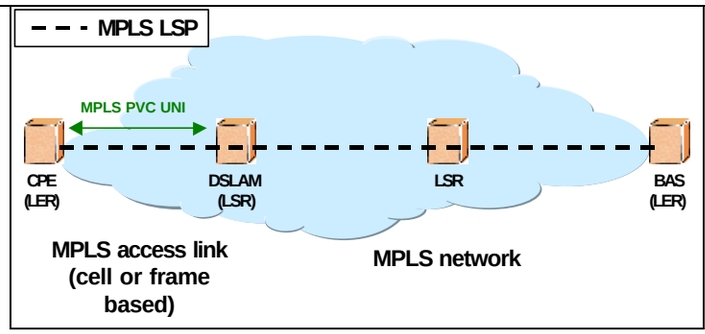


Figure 41: Full MPLS using an MPLS PVC UNI

The MPLS PVC UNI is currently under investigation at the MPLS forum. Three different protocols have been proposed, and can be categorized in two types. The first group of MPLS PVC UNI protocols is based on existing MPLS signaling protocols (LDP and RSVP-TE) that are being simplified for use as a PVC UNI. The third MPLS PVC UNI protocol is based on the experience of the need for auto-configuration in an ATM based access networks and using a similar approach in an MPLS access network. This means that the MPLS PVC UNI uses techniques that are comparable to ILMI and DSL Forum TR-37.

11.4.6.1 Required changes

The impact on the network is the same as in the intermediate approach, with the additional requirement that the MPLS PVC UNI needs to be defined on both the Access Node and the CPE. The CPE, now being MPLS capable, needs to handle MPLS labels and potentially encapsulate the labels in shim-headers and/or ATM VPI/VCI fields.

11.4.7 Support of MPLS and the MPLS PVC UNI over the ATM access link

When the CPE acts as a LER, but the access link is based on ATM, then there are two different operational models, depending on whether the MPLS label is mapped on the ATM VPI./VCI or not. This is shown in

Figure 42.

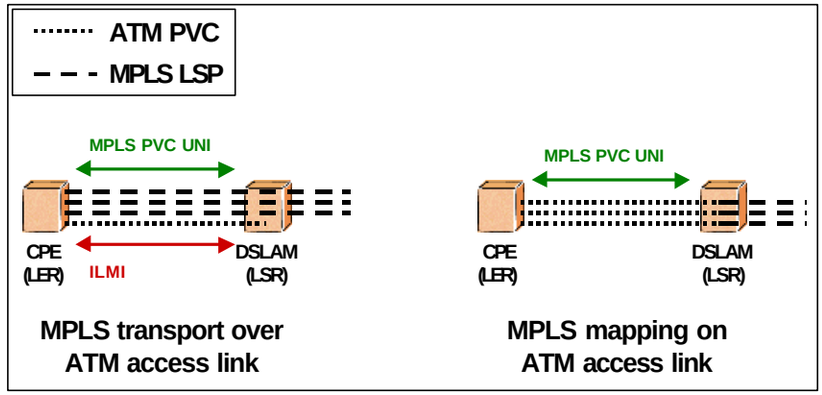


Figure 42: MPLS and the MPLS PVC UNI over the ATM access link

1. ATM is used for transporting MPLS packets: the ATM connection has local significance
   When MPLS packets need to be sent, the CPE places the entire MPLS packet on an ATM PVC. As such, multiple LSPs can use the same VPI/VCI, i.e. the same ATM PVC. The label is not mapped to an ATM VPI/VCI. This means that ILMI will be used as-is on the ATM access link in order to discover the VPI/VCI(s) that can be used to transport MPLS data. At the point where the ATM connection is terminated, the MPLS data will be re-examined. The MPLS PVC UNI messages are also transmitted using the same VPI/VCI. A mechanism on top of the ATM PVC must be used to make the distinction between MPLS data and control traffic, e.g. by introducing a reserved MPLS label;

2. MPLS is mapped on ATM: the MPLS label is mapped on a VPI/VCI
   When MPLS packets need to be sent, the CPE maps the top label to an ATM VPI/VCI before sending it. As such, each LSP will use a different VPI/VCI. Because there are no ATM PVCs anymore, ILMI will be replaced by the MPLS PVC UNI. The ACCESS NODE being an LSR can be an ATM-LSR or a frame-based LSR. In the first case the user traffic is switched as ATM cells, in the second case the ATM cells are reassembled to form a packet which is being switched. The MPLS PVC UNI messages are transmitted using a reserved MPLS label that is mapped to a reserved ATM VPI/VCI.

Both solutions have their merits and could be deployed. The first option is more in line with legacy MPLS networks and doesn't require standardizing an additional ATM VPI/VCI for the MPLS PVC UNI. The second option is more in line with legacy ATM networks and brings the values of controlled delay on low speed uplinks.

12. ATM/MPLS Layer 2 Cross Connection Support

12.1 Starting Network Scenario

Today the majority of DSL access deployments are based on ATM transport architectures. ATM has proven its value as an aggregation technology and is suitable for the delivery of a wide range of broadband services. Besides the traditional and well known ATM cell-based networks, packet-based aggregation techniques are starting to emerge. Inter-working with these packet based networks is becoming a new challenge for DSL access networks.

12.2 Proposed target Network Scenario

In the proposed target network scenario MPLS is a technology that may be used in cell and packet networks while supporting consistent QoS and traffic engineering capabilities. MPLS like ATM provides an architecture that enables effective multi-service delivery. In addition it can also support backwards compatibility with the installed base of Broadband Network Terminations (B-NTs) if the ATM-MPLS L2 cross-connect function as outlined in this section is provided. MPLS has without dispute enjoyed rapid adoption in selected core IP networks. One scenario for using MPLS in the access network is to extend MPLS from the BAS across the RBN up to the Access Node (AN), but not up to the B-NT, see 0. This can be reformulated with MPLS terminology by stating that the AN is the LER. The peer LER is the BAS or Voice Gateway. This means MPLS is required in the BAS, the Regional Broadband Network (RBN) and the AN. This results from the assumption that MPLS in the core network will not necessarily be identical with MPLS in the RBN and access network. Therefore it is assumed that core and access are two isolated MPLS networks and the BAS behaves twice as a LER.

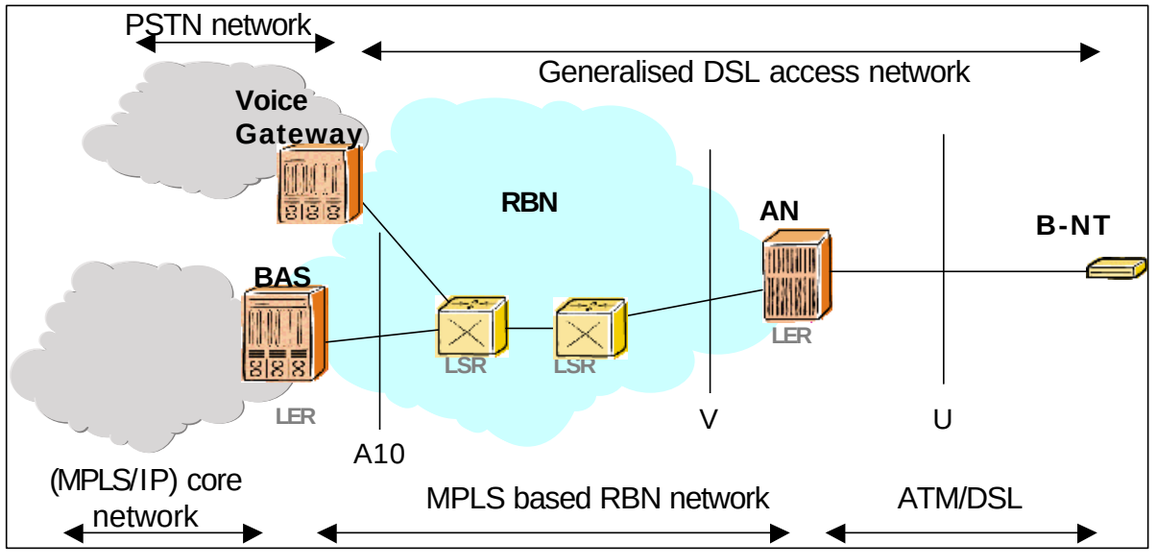


Figure 43: Reference architecture overview

12.3 Drivers

An ATM-MPLS L2 cross-connect function is proposed in preference to the layer 3 solution referred to in section

- It is consistent with and analogous to the current ATM (layer 2) methods which can be deployed on any size of AN.
- Forwarding decisions are taken at layer 2 rather than at layer 3. This L2 approach avoids the expected issues of scalability that arise when layer 3 forwarding occurs in the access network. Support for multiple service providers will even make the first problem worse.
- Besides IP based services also non-IP services like VoDSL, leased line with Frame Relay interconnect, Transparent LAN Services can also be supported in this layer 2 architecture.
- At some stage in the future it is possible to migrate an existing ATM access network into a heterogeneous MPLS access network. When an ATM-MPLS L2 cross-connect function is implemented in the AN then the benefits of MPLS can be enjoyed across the edge and into the Access Node. Gradual migration is possible by for example first migrating some combination of the installed edge ATM nodes with the ATM-MPLS L2 cross-connect function using the 'ships in the night' approach.
- Once MPLS is available in the edge / RBN network and BAS then the ATM-MPLS L2 cross-connect function can be introduced into the AN when appropriate.
- Today's installed 'ATM' B-NTs are not MPLS aware. This means MPLS to the B-NT is not possible with installed base and existing stock of B-NTs.

So introducing MPLS up to the AN, and providing a simple ATM-MPLS L2 cross-connect function, is the natural first step. Potential advantages of the use of MPLS in DSL access networks are:

- MPLS is link-layer independent (not only ATM interfaces but also e.g. Ethernet interfaces may be used).
- MPLS can be implemented in a scalable manner (label stacking with full flexibility on the number of nested labels).
- MPLS can be accompanied with a complete control plane that works in the heterogeneous environment described above.

In a later stage, after the above changes have been made to the BAS, RBN and AN, then MPLS may be introduced in the B-NT. This allows the B-NT to also eventually benefit from the same MPLS advantages. This step still requires significant standardisation in the field of auto-configuration and flow-through service provisioning.

12.4 Options

12.4.1 Description of the reference DSL (ATM-based) access network architecture

The reference architecture consists of a number of customers that are connected via the ADSL technology to an AN. That AN is currently connected to an ATM access network that aggregates the user traffic to a set of service providers / gateways. The most widely spread service available to these customers is web browsing and or email, so IP based services. For that type of service the user traffic is aggregated to a Broadband Access Server (BAS) that interfaces to the IP/MPLS core network. Voice over DSL is a non IP service for which AAL2 PDU's are terminated on a Voice Gateway which interfaces to a PSTN network. These examples are not exclusive and the access architecture is open for the introduction of new services. This situation is shown in Figure 36.

This architecture allows for permanent connections (PVC), soft PVCs (SPVC), and for switched connections (SVCs). In practice, mostly PVCs are deployed.

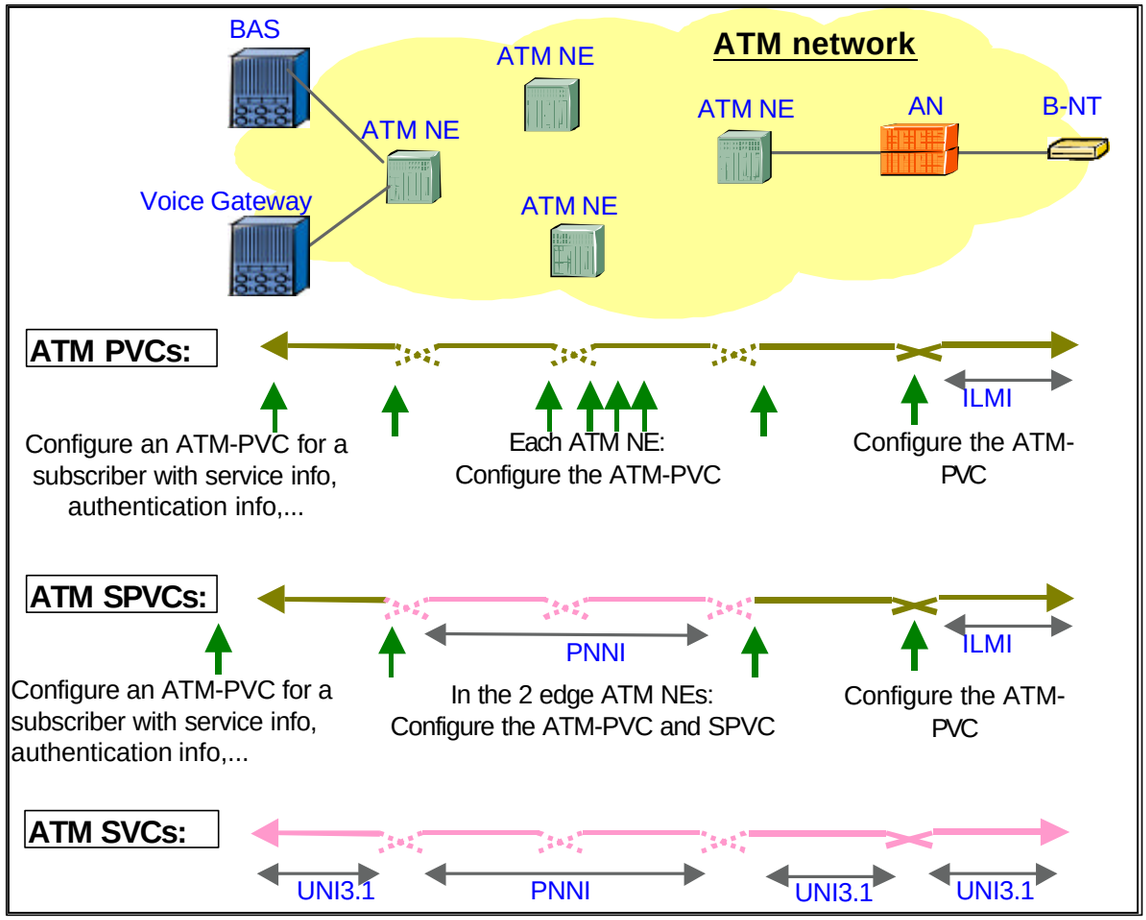


Figure 44: Reference DSL (ATM-based) access network

- PVCs are connections that are configured from a management system in each involved NE. The exception is the end point (the B-NT): the B-NT is not directly configured from a management system but is configured from the AN through ILMI.
- SPVCs are connections that are configured as a PVC in the end point and in some NEs at the edge of the network while signalling is used in the inner part of the network. Variations exist with respect to the PVC segment being larger or smaller.

- SVCs are connections established upon the initiative of an end point using signalling proceduresThere is no involvement of a management system in the establishment of the connection.

12.4.2 Functional diagram of the ATM based AN

The AN SHALL contain ATM & PHY layers to interface the AN to the RBN / Edge ATM Network over the V interface. Some examples of ATM RBN / Edge Network Interface PHY include N x DS1, DS3, and SONET/SDH. Non-ATM Core Networks are not covered in this section. In addition to the PHY functions, this block SHALL perform ATM layer functions as specified in ATM Forum UNI specification 3.1 and Traffic Management 4.0.

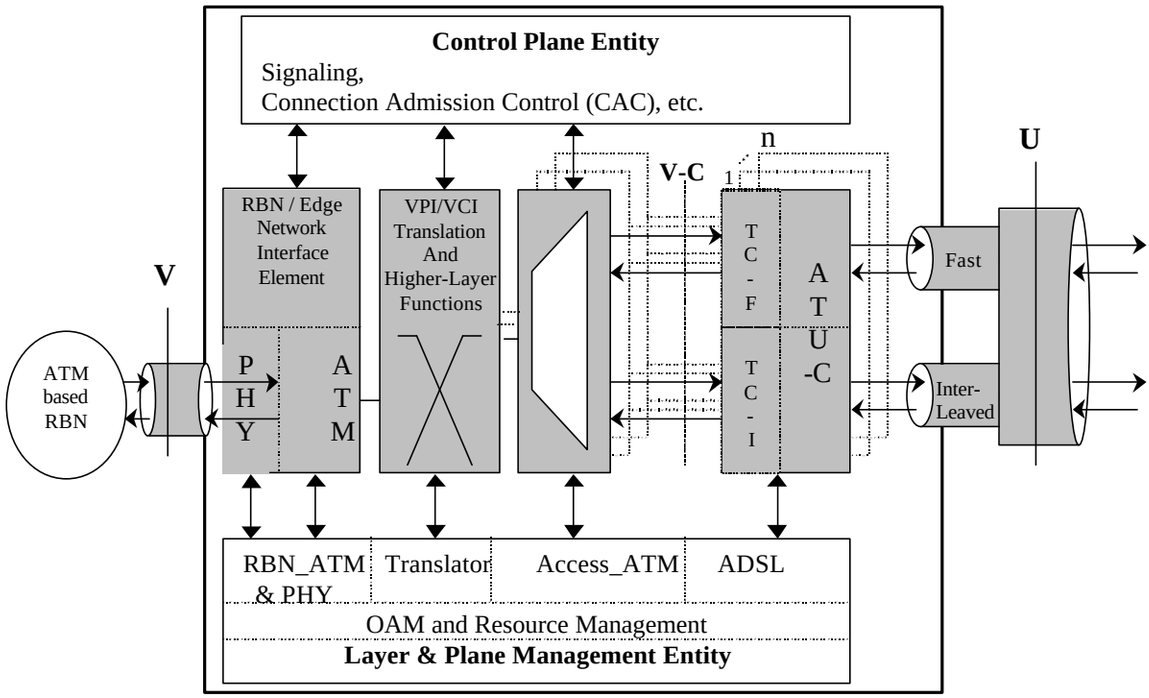


Figure 45 ATM Mode AN, Detailed Logical Reference Model

12.4.3 Description of an ATM-MPLS L2 cross-connect function in the AN

The introduction of MPLS in the access network up to the AN but not up to the B-NT results in the access network architecture shown inFigure 46. Similar as in ATM access networks one may define PVCs, SPVCs, and SVCs. As a first step, only the MPLS PVCs could be introduced. This is the equivalent of an ATM PVC service. This is the logical first step as ATM PVCs are the most commonly deployed feature in today's ATM access networks, and MPLS PVCs can support the same feature in (heterogeneous) MPLS networks.

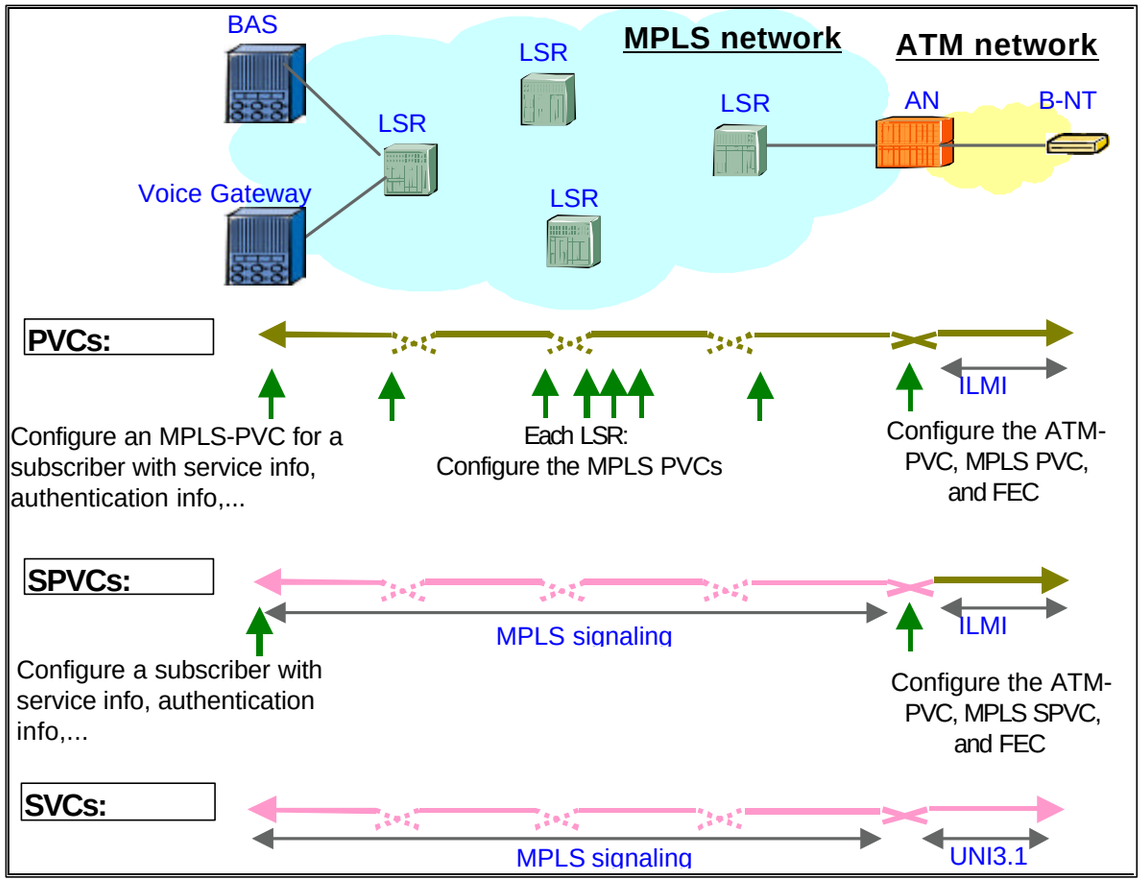


Figure 46: PVCs, SPVCs, and SVCs in an MPLS access network

12.4.4 Functional diagram of the ATM-MPLS L2 cross-connect architecture in the AN

When MPLS is introduced in the access network 'up to the AN', then it is an AN responsibility to interwork between the ATM based B-NT and the MPLS network. Most of the issues related to this architecture can therefore be expected to impact the AN. Further chapters are dedicated to these issues and propose solutions.Figure 47 gives a functional decomposition of this AN with the purpose to give an overview of the functions.

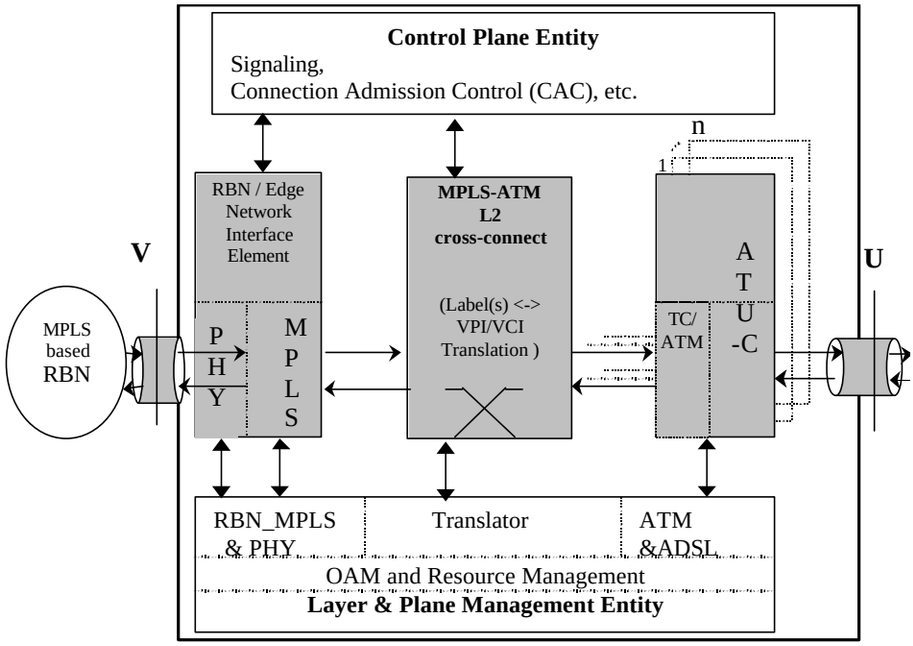


Figure 47: ATM-MPLS L2 cross-connect AN, Detailed Logical Reference Model

Potential issues:
- How to classify traffic in order to forward it between MPLS PVCs and ATM PVCs? See section 12.4.5.
- Which association should be defined between MPLS labels and ATM VPI, VCIs? See section 12.4.6
- What's the relationship between the 'MPLS traffic descriptor' of the MPLS PVC and the 'ATM traffic descriptor' of the ATM PVC? See section 12.4.7,
- The use of the concept of MPLS label stacking in comparison with ATM VP and VC switching. See section 12.4.8.
- How to provide end to end OAM? See section 12.4.9.

12.4.5 PVC connectivity between the B-NT and the BAS / Voice Gateway

In the alternative described in this section, the role of the B-NT remains unchanged with respect to the reference architecture, but an MPLS RBN replaces the ATM RBN. For the B-NT using the PVC feature this means it uses ILMI to exchange information w.r.t. the PVCs. The PVCs on the user (ATM) interface still have to be configured in the AN, inclusive their ATM traffic contract, the layer 2, layer 3, and the service provider information. See document [25] for more information.

The MPLS network, including the AN and the BAS/Voice Gateway (all acting as LERs), is configured with MPLS PVCs.

Figure 5 suggests to define that there is a 1-1 relationship between the ATM PVC on the user interface and the MPLS PVC. This keeps the responsibilities of the various network elements similar as today: the AN and the access network still offer layer 2 access, (only ATM is replaced by MPLS). And the BAS and Voice Gateway support the service provided on top of this PVC, and this includes authentication.

Obviously, if for the upstream traffic 1-1 relationship exists between the ATM PVC on the user interface and the MPLS PVC in the access network, the same 1-1 relationship exists for the downstream traffic.

12.4.6 The user plane: unidirectional or bi-directional PVCs?

The previous chapter explains the need for a rule to map traffic between the user ATM PVC and the MPLS PVC. The proposal is to define a 1-1 relationship between them. Looking into the details one notices that ATM VP and VC connections established in an ATM network are bi-directional and that traditional MPLS LSPs established in an MPLS network are unidirectional. The signalling protocols used to establish SPVCs / SVCs are also defined to establish uni-directional LSPs. Bi-directional LSPs are defined e.g. for optical networks but then the bandwidth is symmetrical.

In the mass market environment bi-directional communication with asymmetric characteristics is assumed. So what type of connection should the 'MPLS PVC' be?

There are two options:
- Option 1: Extend MPLS with the concept of an asymmetric bi-directional LSPs (this means extending the signalling protocols and the management interfaces), or
- Option 2: Extend MPLS with the concept of a 'pair of LSPs' where two opposite direction LSPs between the same end points are paired to offer bi-directional communication between these end points. The two LSPs are established independently in the access network as two uni-directional LSPs. The fact that they are paired is known only in the two end points, being the AN and the BAS / Voice Gateway.

These two options can be further elaborated upon with sub-options::

- use the same label for both directions,
- or keep a separate label space for both directions.

In case the MPLS network is realised by ATM switch technology, then the use of one VPI, VCI as the same label for both directions of traffic flows allows the use of one bi-directional ATM connection to support an asymmetrical bi-directional LSP. When labels are different for both directions, then two ATM connections are required.

It is required that the option selected to solve the uni/bi-directional issue results in the same user plane characteristics for PVCs, SPVCs, and SVCs. It is also required that the selected option can be supported by various technologies. And it is prefered that the option can be supported with a minimum of deviations in the signalling protocols as defined and used in core and access networks.

12.4.7 ATM traffic contract - MPLS class of service

Connections are specified in ATM networks with an ATM Class of Service (CoS) (e.g. CBR, GFR, …) and for each CoS there is a set of corresponding traffic parameters (e.g. PCR, SCR, …). The unit of bandwidth in an ATM network is cells/s.

MPLS networks may be based on ATM, but also on other technologies. This means that the MPLS network may become a heterogeneous network. In MPLS, traffic flows may be specified using a Per Hop Behaviour (in case of DiffServ behaviour) or by explicitly requesting the characteristics during signalling (in case of IntServ behaviour e.g. Guaranteed service, controlled load service) and the traffic parameters are in units of bytes/s. Even when an MPLS network is realised with ATM nodes, it is wise to specify the traffic flows as it is specified in MPLS networks in order not to endanger the evolution to heterogeneous networks.

With other words: the AN that is the LER that interworks between the ATM and the MPLS network shall assure consistency between both types of traffic contract. There are a number of RFCs that specify interworking for these parameters, but the main message is that this interworking leaves options. The mapping of traffic parameters may be AN specific.

12.4.8 Label stacking

One of the problems faced in today's ATM access networks is the amount of PVCs to be managed in the network. A possible solution is to use the concept of ATM VP Connections as a grouping level: establish e.g. one VP Connection in the ATM network between the BAS and the AN, and map the VC Connections of the individual subscribers into this VP Connection. In this way only the AN and the BAS / Voice Gateway are to be configured with a PVC per user.

The same solution is provided by MPLS: i.e. label stacking. The label stacking of MPLS is richer in its implementation:

- The operation at any layer is exactly the same, an LSR does not even need to know whether or not the payload of the switched frames contain additional labels.
- The amount of nested labels does not need to be identical for the various PVCs. Labels may be added / removed inside the MPLS network as appropriate.

Beside the application of bundling traffic to the same destination, label stacking can also be used to bundle traffic of the same CoS. For example it is possible to establish multiple MPLS PVCs between a BAS and an AN in order to separate the traffic based on their CoS requirement.

12.4.9 OAM

Today's ATM networks offer many inband (F4/F5) OAM features such as inband failure detection, … . These features allow the end points to quickly detect failures with the end to end communication, and give an efficient tool to the operator to locate the failure.

MPLS standardisation is not that far yet, but intends to provide similar procedures for the heterogeneous MPLS network.

12.4.10 Potential standardization TOPICS

Section 12.4 leaves some options open for possible DSL Forum work:

- Do we introduce LSP-pairs or asymmetric bi-directional LSPs?
- QOS mapping should be worked out.
- MPLS stacking should be worked out (perhaps MPLS service unbundling between the NAP/NSP is another topic that should be elaborated?)
- MPLS OAM should be worked out.

This list mentions some topics that were introduced in this document but it does not intend to be exhaustive with respect to the standardization work. Other potential topics can be identified by looking into other 'interworking' standardization documents, e.g. "Frame Relay/ATM PVC Service Interworking Implementation agreement", document [26]. This document for example introduces the topic 'optional translation of higher layer protocols'.

13. MPLS Based VPN Network Scenario

13.1 Starting Network Scenario

The following diagram is used to refer to the existing DSL network deployment:

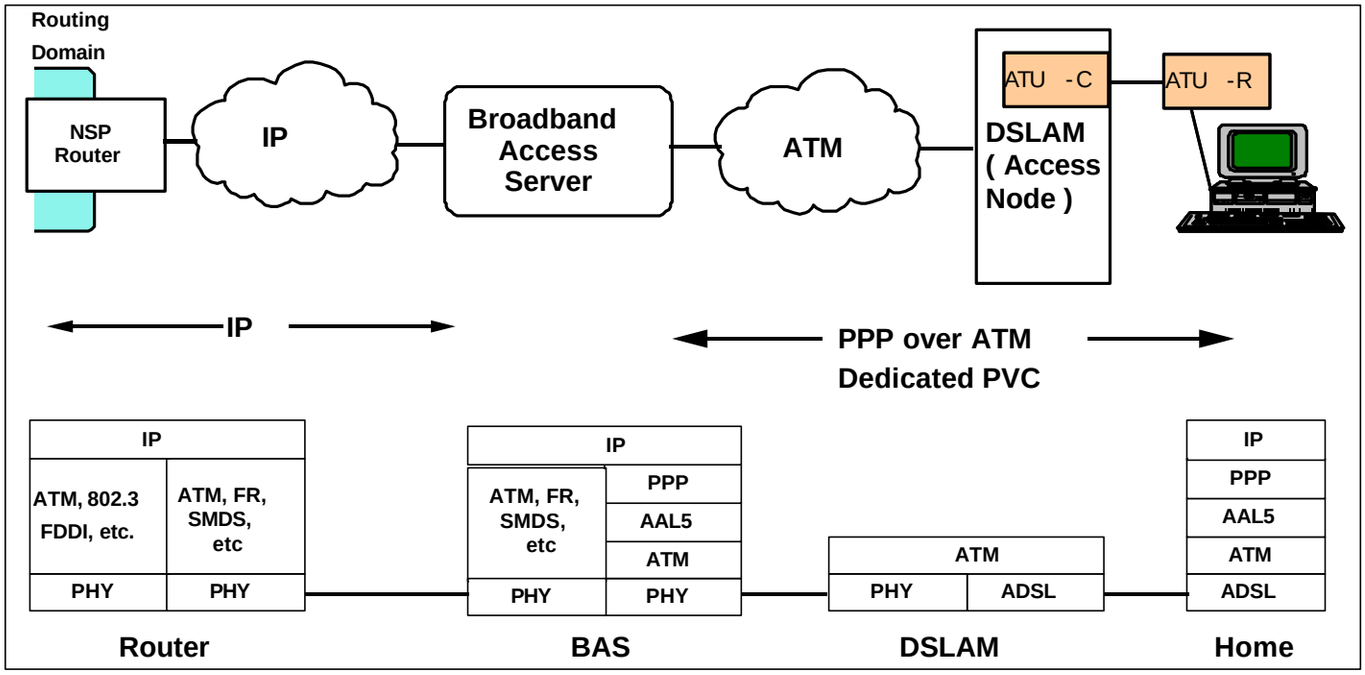


Figure 48 DSL Network Reference Diagram

This network depicts DSL services being deployed to subscribers using ATM as the layer-2 technology from the subscriber (Home) and terminates at a broadband access server (BAS). The subscribers IP data is transported over

PPP from the home end point and terminates at the BAS. The IP datagram then routes over an IP infrastructure carries by various layer-2 technologies that are NAP/NSP specific.

13.2 Proposed target Network Scenario

The proposed target scenario is an MPLS based core network that utilizes RFC 2547 to implement virtual private networks within the core out to the edge of the network. DSL systems reside at the edge of this network. Please refer to Figure 49 MPLS VPN Network.

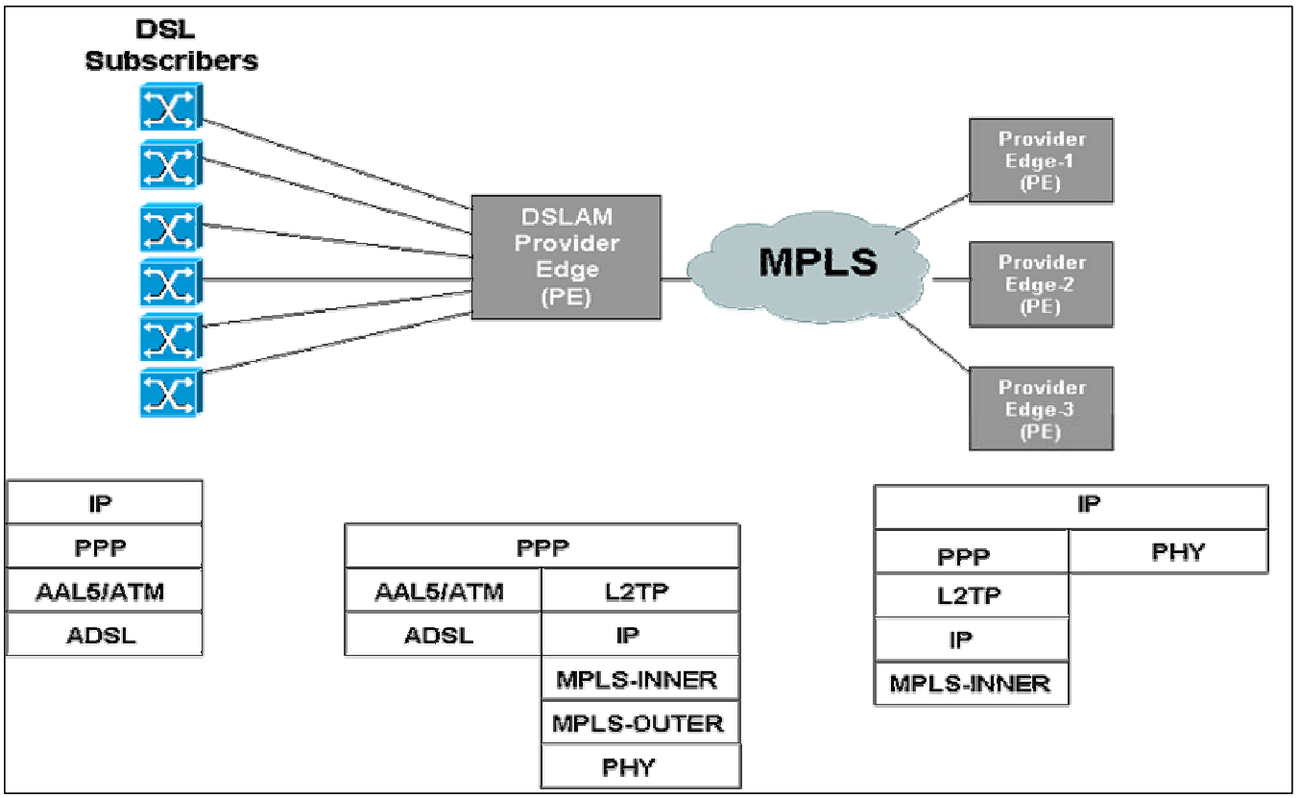


Figure 49 MPLS VPN Network

Per RFC2547, there are several roles a node can play in an MPLS VPN network. The key roles are the Provider Edge (PE) and the Provider (P). The PE is the gateway between non-MPLS based traffic and the MPLS network. The PE is responsible for routing protocols and addressing information on the non-MPLS side. It is also responsible for signaling/creating label switched paths through the MPLS core as well as signaling/creating the VPN labels that only have significance at the edges (PEs). Per the protocol stack in Figure 49 MPLS VPN Network, there are two labels used for MPLS VPNs. The outer label is used to model the label switched path through the MPLS core. The inner label is used to define the VPN. This labeling scheme differentiates MPLS VPNs from other VPN technology, and is touted to scale higher than current VPN technologies. In current VPN technology, the core is aware of the VPN. In an MPLS VPN network, the core has no knowledge of the VPN as it merely passes the packet through based on the outer label. This outer label is removed by the P node that plays the role of the penultimate hop. The PE receives the packet with the inner label in tact. It is this inner label that allows the PE to look up a routing table in order to forward a packet to the appropriate destination.

The ACCESS NODE takes the role of an integrated router with the additional capability of MPLS tagging based on RFC2547. From the starting scenario, PPP would be transported over L2TP inside an MPLS VPN toward the NSP. Additionally, the VPN could be used to transport RFC2684 (obsoletes RFC1483) based bridged or routed PDUs. This gives the NSP additional flexibility within a VPN.

13.3 Drivers

The drivers for the proposed target network depicted are as follows.

13.3.1 Network Access Provider

- Integrates with emerging core MPLS network.
- Provides an aggregation capability for grouped subscribers (service level granularity).
- Provides for an SLA to be applied to the VPN.
- Provides for an aggregated interface toward the NSP (lower management system burden).
- VPN creation signalled throughout the network versus manually provisioned per node.

13.3.2 Network Service Provider

- Integrates with existing routed infrastructure.
- QoS guarantees from NAP based on VPN SLA(s).
- Provides an aggregation capability for grouped subscribers (lower management system burden).
- Standard benefits of a VPN (private addressing, etc).

13.3.3 End User

- Wider array of service offerings, competitively priced based on provider's ability to better manage service offerings (new and old).

13.4 Options/Requirements

This proposal dictates a requirement on the Access Node to support MPLS and VPNs in an integrated fashion. Methods to achieve this evolution leverage off existing proposals to support MPLS and integrated routing (see contribution dslforum2001-266). In other words, the ACCESS NODE terminates the ATM layer, and uses the physical port/VC coupled with the IP header to determine which VPN it belongs to. From a signalling perspective, the ACCESS NODE supports IP routing protocols (RIP, OSPF, etc), MPLS VPN tag distribution protocols (LDP and BGP), and traffic engineering protocols (RSVP and/or CR-LDP). Advantages of this approach can be ascertained from the Drivers section above.

13.5 References

- RFC 2547 – MPLS Based VPNs
- DSL Forum contribution dslforum2001-266
- DSL Forum contribution dslforum2001-348

14. Migration to Ethernet Transport in the Regional Broadband Network

14.1 Starting network scenario

The starting scenario depicted below illustrates the four domains involved in DSL access, and the physical/functional contents of these domains in current generation access systems. Examples of typical protocol stacks are also shown, with optional protocol layers in parentheses. The *Premises Domain* contains the subscribers' equipment, that is, DSL modem or router, analogue filter and one or more subscriber hosts (PCs, for example). The *Access Domain* contains the Access Node and the ATM switch; the latter extends the ATM circuits via the *Transport Domain* to the *Service Domain* where the circuits are terminated. The Service Provider's equipment manages the IP traffic conveyed over

the ATM circuit in order to e.g. verify subscriber identity, perform IP provisioning of subscriber hosts, and provide services such as web access and email.

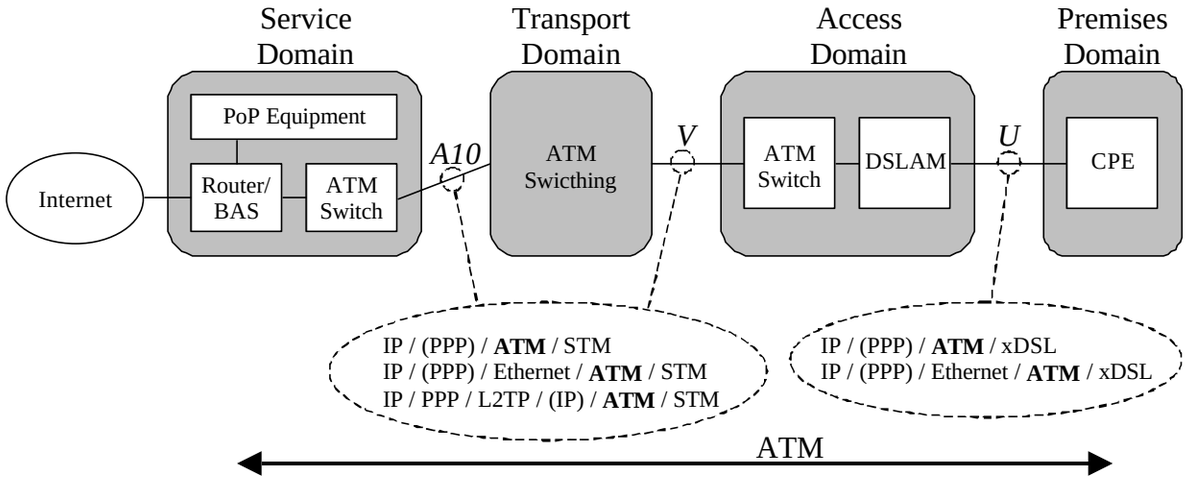


Figure 50: Starting Scenario, Using TR-010 Domain Nomenclature.

As the various protocol stacks in Figure 50 indicate, there are multiple variants of this scenario, some of which include PPP and/or tunneling between the Access Domain and the Service Domain. However, the common denominator for the starting network scenario is the ATM interconnection between the Access Node and the Broadband Access Server. The proposed target network scenario explores using ethernet in the regional broadband network / transport domain.

14.2 Proposed target network scenario

Originally, the term “Ethernet” designated a specific network system developed by Xerox, Intel and DEC. Later, the Ethernet system protocol was used as a basis for specifying the family of IEEE802.3 protocols. Although the IEEE802.3 protocols differ in various degrees from the original Ethernet protocol, the term “Ethernet” is still widely used as a common name for all of the protocols. This section uses the general common meaning of “Ethernet” when using the word Ethernet within this section.

In the proposed target scenario, Ethernet is the primary transport protocol across the regional broadband network and the V and A10 interfaces. The scenario takes advantage of the trend towards interconnecting the subscriber host(s) to the DSL modem using Ethernet. The Access Node becomes Ethernet-centric in the sense that it bridges between the subscribers’ home LAN and an *Access Domain Ethernet*. The traditional tasks of the ATM cross-connect Access Node are retained in the bridging Access Node, that is, termination of the xDSL protocol towards the subscribers, and traffic aggregation.

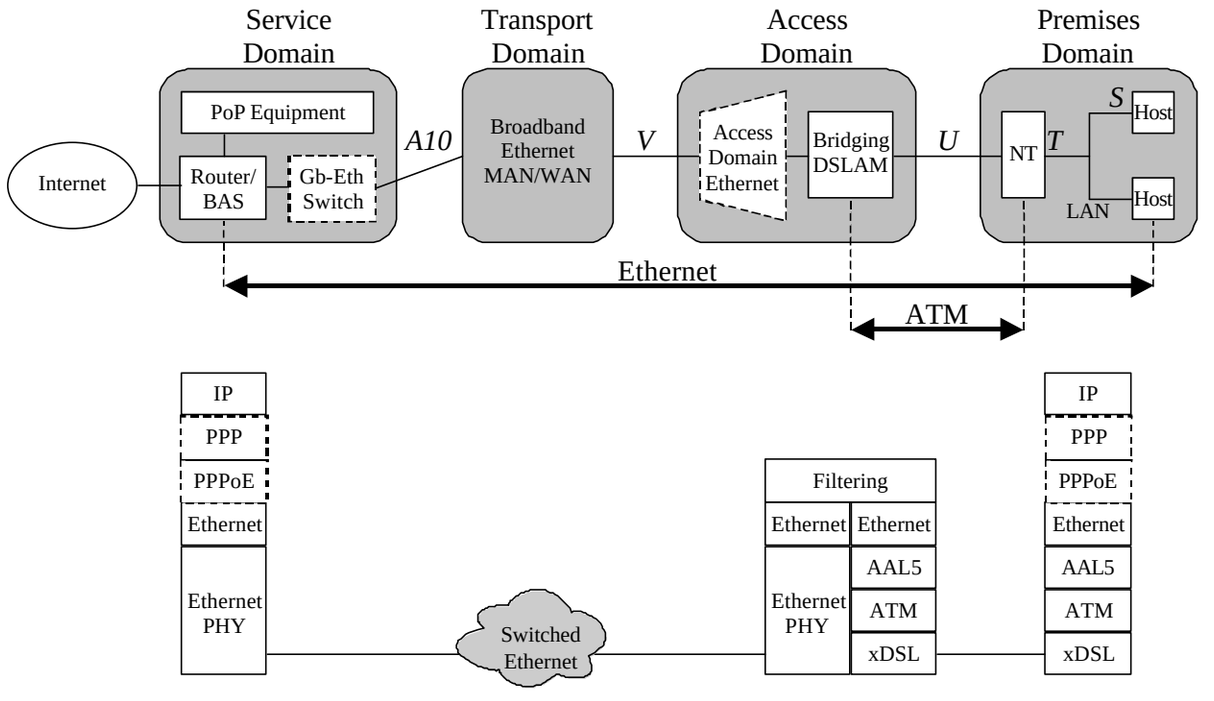


Figure 51: Proposed target Scenario and Example of Associated Protocol Stack.

In addition to the traffic aggregation performed by the Access Node, another level of aggregation can be obtained via one or more layers of Ethernet switches in the Access Domain Ethernet. The relevance of an Access Domain Ethernet depends on the size and number of co-located Access Nodes, and the desired level of aggregation.

The Access Domain is connected to the Service Domain via a Broadband Ethernet MAN or WAN, possibly using Gigabit Ethernet technology. The Service Provider's router/BAS (Broadband Access Server) may interface directly or via a fast switch towards this Broadband Ethernet.

The protocol stack representing the Customer Premises in Figure 51 actually corresponds to various combinations of protocols stacks for the NT (the xDSL modem) and the terminal equipment (the PCs). Figure 52 shows typical protocol stacks associated with different kinds of NTs and with/without the use of PPP. Note the presence of the Ethernet layer as a common denominator for all the stack combinations. The Ethernet layer is encapsulated over AAL5 according to RFC2684.

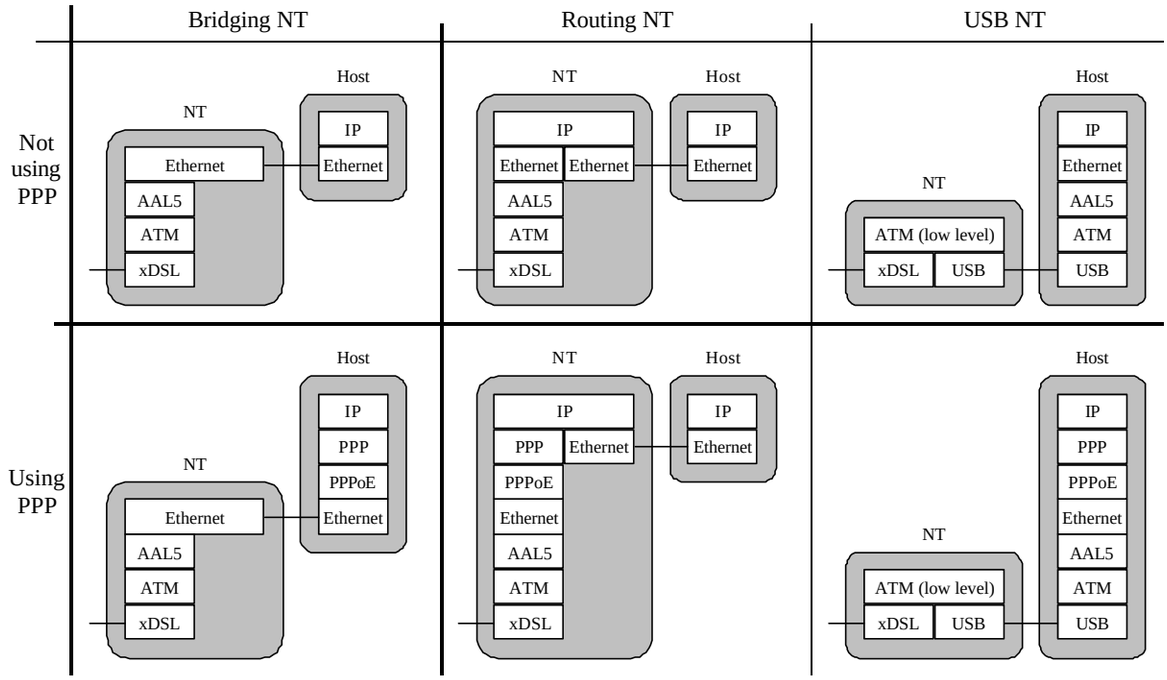


Figure 52: Typical CPE Protocol Stacks for the NT and the Customer Premises Host.

The traditional POTS connection may be retained in the proposed target scenario, using filters/splitters towards the local exchange in the CO. Alternatively, Service Providers can offer high-quality Telephony over IP services as a POTS replacement or as an additional multimedia service. To provide adequate QoS on relatively slow DSL links, such real-time applications require ATM in the local loop. Configuration of ATM circuits only in the local loop is, however, considered far simpler than configuration of end-to-end circuits used in the starting scenario. The mapping between ATM circuit and Service Provider (or just service) is a matter handled solely by the bridging Access Node and controlled by a management system.

The proposed target network scenario provides full support for VoMBN based telephony solutions. Voice services can be supported in the proposed target network scenario using a BLES gateway that is integrated with the Access Node. However if voice services are required using the BLES standard from a Central Gateway then this requires the use of encapsulation of the ATM cells over a packet switched network. This is a topic subject to ongoing standardization within the IETF Pseudo Wire Emulation Edge to Edge (PWE3) Working Group.

14.3 Drivers

Ethernet technology has proven itself very successful in LAN environments where it today is ubiquitous and dominant. This scenario explores taking advantage of Ethernet's success in the LAN and applying it to the DSL access case. At the subscribers' premises, Ethernet is a natural choice for hooking up one or more hosts to the DSL modem in a fast and easy way. The ease of installation at the subscribers' premises is a major requirement posed by operators, causing Ethernet to be the prevailing and most popular DSL modem interface today.

The use of Ethernet as a common transport protocol between subscribers and Service Providers ensures an end-to-end solution with little protocol overhead and minimized protocol conversion, and thus simple interfaces between Access Provider and Service Providers. Ethernet is connectionless, so traffic flows need no prior configuration. Instead, by inspecting the source addresses of incoming frames the network switches quickly builds up knowledge about the network topology in order to direct traffic in the right direction only. This self-configuring feature of a switched Ethernet ensures a simple network installation.

Ethernet technology is currently being widely deployed in other access scenarios, such as fiber access systems (FTTB, FTTH) offering high-speed Ethernet connections to subscribers. These scenarios are often based on Ethernet MANs/WANs, for example Metro Rings. An Ethernet based transport approach to DSL access networks could benefit from metro ethernet MAN/WAN deployments.

14.4 Options

Traditionally, Ethernet has been associated with little security, rudimentary QoS mechanisms, and only limited network management features. This was adequate during the early years of initial, small and localized Ethernet LAN deployment, because there was little or no need for such functionality. However, when Ethernet is considered for use as a WAN transport technology as in the proposed target network scenario, there is a need to ensure high security and adequate QoS. Other important aspects to be considered are handling of Services and Service Selection, and management of Ethernet networks.

The proposed target network scenario depicted in Figure 51 constitutes the basic Ethernet DSL access scenario. By employing different kinds of Ethernet related techniques, this basic scenario can be tailored to various network requirements regarding security, QoS and Service Selection. These techniques include for example the use of virtual LAN (VLAN) techniques, traffic filtering and shaping, and the Point-to-Point Protocol (PPP) over Ethernet.

The following sections describe in more details various functional requirements put forward to the proposed target scenario, and possible solutions to meet these requirements. The resulting scenarios are, however, all based on the basic proposed target scenario (Figure 51), that is, an end-to-end Ethernet across a bridging Access Node.

14.4.1 Security

In general, all IP networks are susceptible to a wide range of attacks from both external and internal parties. The attacks can have many forms, including information theft, denial-of-service attacks, and corruption of programs or information. These threats are a general issue to any IP based access system, including ATM based DSL systems. Additional security issues are, however, imposed to Ethernet DSL Access by the use of Ethernet as the common layer-2 technology. Deploying such a broadcast media for traffic to/from multiple subscribers (and possibly also for management traffic) requires that the system provides features to ensure the privacy and integrity of the transported data, and to protect the equipment owned by subscribers and operators. For the DSL subscribers, the bridging Access Node constitutes the boundary to a network where various flows share the same physical media; therefore the Access Node must play an active role in the protection of data and equipment.

Different traffic types can be separated by employing VLAN techniques. A VLAN is a logically separated broadcast network within an Ethernet. Communication between VLANs must always traverse a layer-3 device, typically an IP router. Thus, an immediate use of VLAN is to separate management traffic and subscriber payload traffic in different VLANs. In this way, malicious subscribers cannot abuse the common Ethernet to tamper with the operators' equipment. The IP routers at the network edge must be configured to prevent traffic in subscriber VLANs from accessing the management VLAN.

Layer-2 visibility between individual subscribers must also be considered. If no restrictions are introduced in the Access Domain all subscribers will have layer-2 visibility of each other, enabling ARP poisoning and similar attacks not associated with traditional DSL access. Two possible techniques for providing layer-2 separation are VLAN and filtering:

Besides separation of traffic types, VLANs may also be used to separate traffic belonging to different subscribers, thus providing a layer-2 separation between them. The Access Node tags upstream traffic, using the VLAN ID associated with the subscriber. Downstream traffic is checked for correct VLAN before it is forwarded onto the DSL link. The use of individual VLAN IDs is, however, somewhat limited by the VLAN standard (IEEE802.1Q), providing a maximum of 4096 VLAN IDs per Ethernet. Alternatively, VLANs may be used to separate groups of subscribers that individually have layer-2 visibility.

Another method to counter the layer-2 visibility issue and resolve a number of other security issues is by filtering in the Access Node. By inspecting the upstream traffic it is possible to remove broadcast traffic (which otherwise may cause broadcast storms); poisoning / spoofing packets (for example ARP poisoning); perform source address filtering

(to avoid spoofing); perform destination address filtering (directing the traffic to a fixed destination, typically the default gateway – see below); and perform Ethertype filtering (i.e. allowing only authorized Ethernet frame types, for example PPPoE frames or IPv4 frames).

Specifically, the layer-2 separation can be ensured by using destination address filtering. By allowing upstream traffic towards the default gateway only, direct communication between subscribers is made impossible. To ensure good IP address utilization multiple subscribers can share the same IP subnet, provided that the Access Node performs ARP proxying of upstream ARP requests, replying with the default gateway as layer-2 destination for traffic between subscribers in the same IP subnet. Downstream ARP requests (from the default gateway) should be filtered by the Access Node in order to forward the request only to the intended subscriber, thus preventing flooding of DSL links with irrelevant ARP requests. Alternatively, the Access Node can act as ARP proxy for the downstream ARP requests.

A third option for ensuring layer-2 separation between subscribers is using PPP over Ethernet (PPPoE). Combined with upstream filtering of Ethernet frame types this ensures that traffic can flow only between the BAS and the individual subscribers.

Other mechanisms can be devised that provide layer-2 separation, but they will not be elaborated upon further in this document. The common denominator for the solutions is that the Access Node must perform filtering and possibly layer-2 modifications of the traffic going through it (for example, VLAN tagging).

14.4.2 Quality of Service

The Ethernet protocol IEEE802.1p supports up to 8 different priority levels (Class of Service). This *Differentiated Services* approach enables preferential treatment of for example management traffic and real-time traffic, as opposed to web browsing traffic and bulky downloads. The actual prioritization of the Ethernet frames is performed by the Ethernet switches used throughout the network, and by the Access Nodes. With a proper planning and monitoring of network capacity, the use of Differentiated Services can provide a scalable solution and can support Service Level Agreements.

The use of ATM in the local loop is considered relevant on relatively slow DSL links that must support real-time applications like for example Telephony over IP. Such applications will experience problems regarding delay and jitter if big Ethernet frames pertaining to other user applications are not segmented. The use of ATM also enables provisioning of ATM PVCs with different QoS profiles and bandwidth. Consequently, it is possible to ensure that the real-time traffic obtains adequate treatment. Thus, on each DSL line a number of ATM PVCs can be established, each corresponding to a certain QoS level, see Figure 53. The Access Node maps between the ATM PVC and the IEEE802.1p priority used within the access network, that is, the Ethernet priority value is a configurable attribute of each ATM PVC. Bandwidth control can be handled on the ATM level; in the downstream direction through traffic shaping, and in the upstream direction through ATM Usage Parameter Control (UPC).

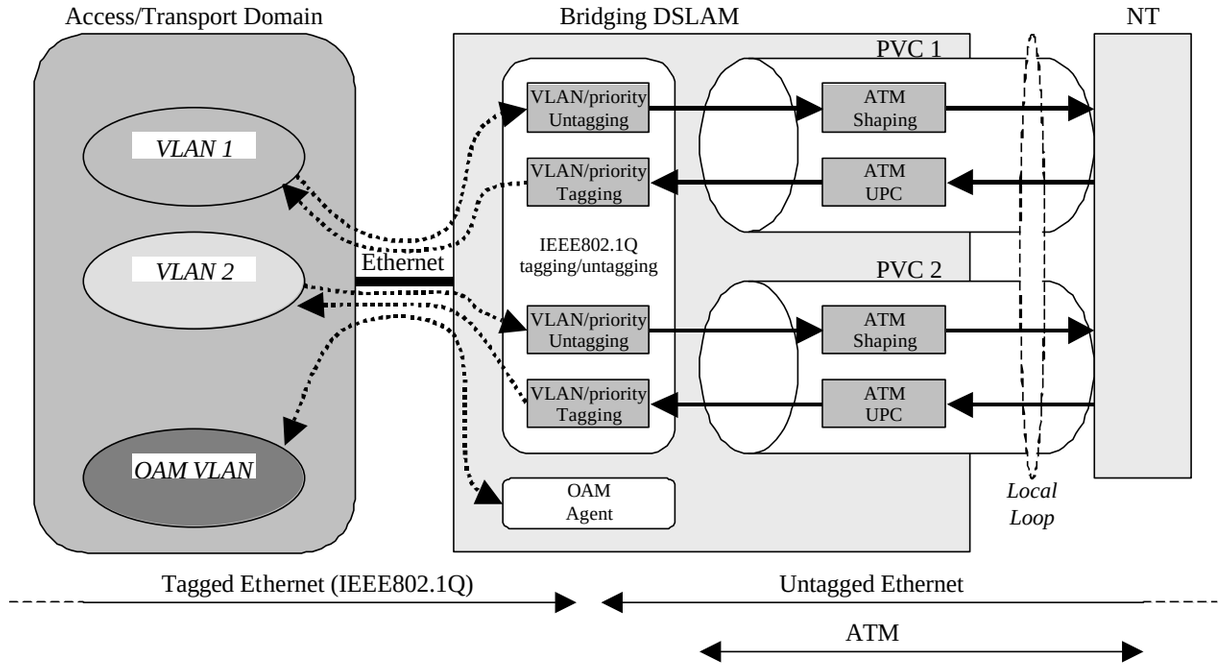


Figure 53: Mapping Between IEEE802.1Q and ATM PVCs for a single subscriber.

The bandwidth provisioned to each subscriber is clearly a chargeable service parameter. With ATM on the local loop the ATM PVC settings define the available bandwidth.

With a single Ethernet covering most domains in the Proposed target Scenario figure, the size of this network must be considered, in order to prevent the network from being flooded with broadcast messages. Here, VLAN techniques can be used as a QoS mechanism. VLANs may be defined simply as a means to limit the size of broadcast domains, ensuring that such traffic will not flood the entire network.

However, VLANs may also serve other purposes; for example, using an Ethernet DSL the Network Access Provider (NAP) may define a unique VLAN for each service. Examples of such services are Telephony over IP, web browsing, and TV broadcasting; each running in different VLANs. The desired quality of each VLAN can then be ensured by configuring the Ethernet switches to reserve a portion of the transmission bandwidth for traffic with that VLAN ID.

Path redundancy can be implemented through use of the Spanning Tree Protocol (STP). STP is a link management protocol used for learning about – and controlling – the topology of an Ethernet network. An Ethernet can always have only one active path between two switches, so if multiple paths exist the STP will force all but one path into a standby state. If a path subsequently becomes unavailable, the STP will automatically reconfigure the topology and activate a possible standby path.

14.4.3 Services and Service Selection

The use of VLAN for different services is a simple means for controlling the subscribers' access to services. Again, there are many different ways of implementing this functionality, depending on the actual access scenario, that is, the types of services offered, unbundling aspects, flavor of access protocols, and much more. If ATM is used in the local loop then it is simple to define different ATM PVCs for different services and let the Access Node handle the mapping between PVCs and VLAN, thereby controlling the service access. Figure 53 illustrates the mapping in the Access Node for a single subscriber. The mapping may be semi-statically defined by operational staff, or it may be performed dynamically as an on-line service selection performed by the subscriber and controlled by the Service Provider's BAS.

Alternatively, the VLANs may stretch all the way to the CPE where it is mapped towards different applications. The Access Node must still provide control of which VLANs that the subscriber has access to.

An important aspect regarding services is the ability to uniquely identify subscribers before granting them access to services. In the ATM based DSL scenario, subscribers may be identified at the Service Provider PoP by inspecting the VPI/VCI values. However, since the bridging Access Node terminates the ATM layer in the Ethernet transport scenario, the VPI/VCI approach cannot be used here for subscriber identification at the Service Provider. Instead, the DHCP protocol may use an option to include circuit identification (that is, VPI/VCI), as described in RFC3046. The option is then inserted by the bridging Access Node, acting as a DHCP relay agent, thus providing the DHCP server with unique subscriber identification. The DHCP server can use this information to determine e.g. if an IP address should be assigned to the requesting CPE host, and what IP address should be used.

A completely different approach to managing service access/selection is the use of PPP over Ethernet, as described in RFC2516. The standard supports the presence of multiple BASs on the same Ethernet, for example representing individual Service Providers. The subscriber's PPPoE client may be located in the CPE modem or at the CPE host. It is possible to start multiple PPPoE sessions over the same DSL connection, for instance from different hosts connected to the CPE LAN. In this way it is possible to access different services simultaneously. Typically, the subscriber must be validated before access to services is granted. Via the PPP protocol the subscriber provides login credentials that the BAS can verify, often supported by a RADIUS server. The login credentials match a certain profile that configures the client (for example IP address and default gateway), and perhaps also authorizes the client to access a certain service. As an alternative to PPPoE the BAS may support HTTP based login.

Using PPPoE provides a solution that fits very well with existing dial-in access systems in terms of AAA and Service Selection, because such system are widely based on using PPP and RADIUS (or similar AAA protocol). This is one of the reasons for the popularity of PPPoE as an access protocol. A potential drawback with PPP is, however, its poor ability to handle multicast. The use of multicast gains more and more attention as a way to distribute multimedia flows, that is, radio, broadcast TV and Video on Demand. But because PPPoE – like the traditional ATM access scenario – creates "virtual circuits" between the CPE and the Service Provider's BAS, the multicast flow must be duplicated in each individual PPPoE session, thus wasting bandwidth in both the Transport Domain and Access Domain.

The task of distributing multimedia flows is solved in the Ethernet DSL access scenario by using other mechanisms, for example by using multicast towards Access Nodes and managing the signal distribution using IGMP, or by using broadcast/multicast in separate VLANs.

The Ethernet technology is also advantageous for local or regional peer-to-peer connections, because the traffic is not necessarily "tromboned" via the Service Provider's PoP but may be switched locally within the Access Domain or Transport Domain. The local/regional traffic is for example Telephony over IP, but also the fast growing area of file sharing and private web servers generate large amounts of peer-to-peer traffic. Yet another application area is transparent interconnection of corporate LANs and telecommuters, isolated within the Access Domain in a separate VLAN. In general, by offloading the Service Provider's PoP the transmission bandwidth is better utilized and the PoP routing requirements are reduced.

14.4.4 Examples of network architectures

As an example of how to use VLANs for different purposes, consider Figure 54.

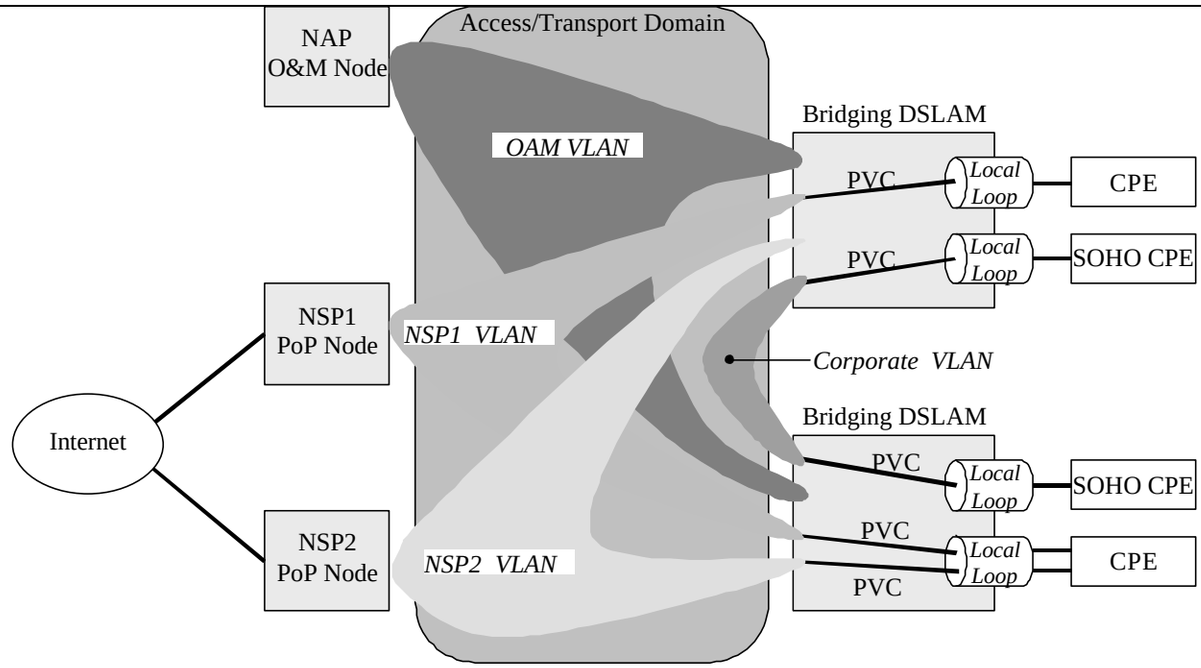


Figure 54: Example of VLAN usage for traffic separation and service selection.

Here, four VLANs are defined: One for each of the Network Service Providers, one for a specific enterprise, and one for Operation and Maintenance (O&M) purposes. Each subscriber PVC is associated with a VLAN, providing a certain service. A subscriber may have multiple PVCs and thus be able to access multiple services. Note that if no traffic restrictions are imposed two subscribers connected to the same VLAN by default have layer-2 visibility of each other. This is utilized in the *Corporate VLAN* shown in Figure 54, which transparently interconnects the Ethernet LANs located at two Small-Office-Home-Office (SOHO) CPEs.

For security reasons, however, some operators require layer-2 separation between individual subscribers. Consequently, one of the previously mentioned techniques must be applied, that is, a unique VLAN per subscriber, traffic filtering, or PPP over Ethernet (PPPoE).

Figure 55 illustrates the use of PPPoE. Each subscriber may establish multiple PPPoE sessions towards one or more Broadband Access Servers (BAS). VLAN can still be applied, for example in order to separate the O&M traffic from the subscriber traffic. Network Service Providers may also have individual VLANs, but the choice of NSP is less dynamic because it is limited by the chosen PVC-to-VLAN mapping.

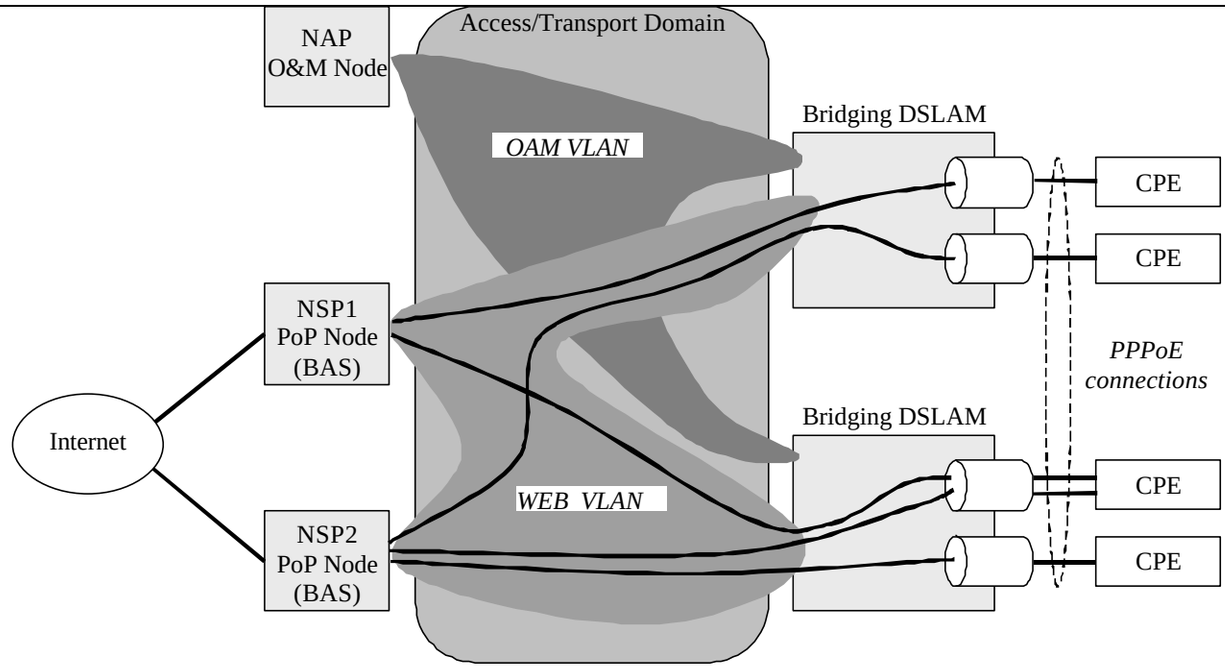


Figure 55: Example of using PPP over Ethernet (PPPoE).

14.4.5 Ethernet management

In general, network management can involve a number of different functions, such as Configuration Management, Performance Management, Fault Management, Accounting Management and Security Management. Traditionally, Ethernet networks have only offered few – but adequate – mechanisms for performing such management tasks. These mechanisms include remote configuration and monitoring of network elements via SNMP, handled by a Network Management System (NMS). The NMS performs periodical interrogations (polling) of each network element's SNMP agent and receives spontaneous events (traps) from the agent, for example if a link is broken. The NMS can also perform auto-discovery of the network to learn about the network topology.

SNMP is described in a number of RFCs, primarily RFC1155, RFC1157 and RFC1213. The protocol may run over UDP/IP, or directly over Ethernet (RFC1089).

Statistical traffic information can provide very useful input to the task of performance management. The RMON MIB standard (RFC1757) defines a large number of statistical parameters to be calculated by an Ethernet device about its operation. Using a monitoring tool these RMON parameters can be retrieved and processed. In this way the load of the network can be monitored, and potential bottlenecks can be discovered and prevented.

For security reasons the management traffic should be conveyed in a dedicated VLAN, separated from the subscriber traffic. Furthermore, the management traffic can be tagged with the highest priority indication, in order to ensure that it is given preferential treatment in case of heavy network load.

However, having acknowledged the limited options for performing management of Ethernet there is now ongoing work within the IEEE802.3ah (Ethernet in the First Mile, EFM) group with the purpose of defining mechanisms for e.g. remote failure indication, remote loop-back and link monitoring.

14.4.6 Options summary

This chapter has discussed several mechanisms that may be applied to the basic Ethernet scenario depicted in Figure 51, in order to tailor the network to specific requirements. The table below provides an overview of possible solution mechanisms that can be applied to meet the major functional requirements for the Ethernet DSL access

scenario. The solutions are all implemented and/or supported by the bridging Access Node. In many cases, several solutions are applied simultaneously in order to provide the desired functionality.

Solution *Requirem.*	*VLAN*	*Traffic Filtering*	*PPP over Ethernet*	*Traffic Shaping and Policing*
Subscriber Security	(✓)	✓	✓	
Network Security	✓	✓	✓	
Quality of Service	✓			✓
Service Selection	✓	✓	✓	

Table: Main functional requirements and possible solution mechanisms.

14.4.7 Additional options

The differences between Ethernet switches and IP routers have narrowed down over the last decade, as the switches have become more and more intelligent. Using L3-switching in the Access Domain (either performed by separate switches in an Access Domain Ethernet, or integrated in the Access Node) can well be integrated into an Ethernet DSL Access scenario. This approach implies, however, that the service provisioning functionality moves to a more distributed model. Even BAS functionality have found its way into the Ethernet switches. Also that fits within an Ethernet DSL Access scenario in which the BAS functionality is partly or totally distributed to the Access Domain.

In a transition phase it may also be relevant for the Access Node to be able to handle advanced protocol conversions, for example as a converter between PPPoA and PPPoE. That will support the base of existing customers with equipment that supports only PPPoA (PPP over ATM), while the NAP and NSP can transit to an Ethernet-centric solution.

As described elsewhere in this report, the use of Ethernet may be combined with MPLS. Inserting this protocol on top of the Ethernet layer provides additional QoS and redundancy functionality to the Ethernet access scenario. However, deploying MPLS involves additional network configuration. Thus, the relevance of MPLS deployment is a trade-off between on one side the wish for a simple network and on the other side the requirements for more advanced Service Level Agreements.

14.4.8 Advantages and disadvantages

The use of Ethernet as primary transport technology for DSL access systems has many advantages:

- Mature, proven and well-known technology
- Flexible provisioning and easy reconfiguration
- Switches are self-learning about network topology
- Scalability issues may be addressed using Ethernet in conjunction with other technologies (e.g., IP, MPLS)
- Little protocol overhead
- Adequate to bursty traffic patterns
- Adequate to IP multicast services
- Compatible with existing CPE modem equipment
- Fast growing Ethernet based infrastructure in MAN/WAN for other access types

- VLANs provide security and options for service selection
- PPP is supported through the PPPoE standard
- Virtual layer-2 connections are possible with e.g. VLAN or Access Node filter functions
- QoS can be provided by IEEE802.1p (Class of Service) or VLAN configuration, extended by ATM functionality on slow DSL links.

As described previously in this section, the Ethernet technology provides a number of different solutions and scenarios to an Ethernet DSL Access system. However, the various solutions are all based on the same basic scenario, namely an end-to-end Ethernet across a bridging Access Node. The Access Node plays an important role in these networks, because it constitutes the boundary between the individual copper lines and the common Ethernet used by all subscribers and for management traffic. Consequently, the bridging Access Node is envisioned to possess functionality that enables it to filter the traffic in both upstream and downstream direction, and possibly also modify the Ethernet frames according to configurations regarding priority and VLAN. It must also be able to control the bandwidth available to each individual subscriber.

The PPPoE protocol can be used as a simple mechanism to provide security and service selection, but it is envisioned that it will get tough competition from access scenarios running pure IP over Ethernet, because the latter has less protocol overhead, does not necessarily require a BAS, and is much more suitable to IP multicast services. As described, there are several options for creating virtual Ethernet connections between subscribers and Service Providers, providing functionality similar to PPP and ATM circuits.

When compared to ATM, the following areas can be considered drawbacks of the Ethernet transport scenario:

- Simpler QoS mechanisms (for example, less options for guaranteed bandwidth)
- Fewer O&M features.
- The mental barrier against using Ethernet for anything else than best-effort LAN traffic with no security requirements.

Furthermore, Ethernet provides no inherent segmentation mechanism that can ensure real-time frames from being delayed over the DSL link more than is acceptable. However, by retaining the ATM layer between the CPE modem and the Access Node the delay can be minimized. For high-speed DSL the delay caused by a long frame is not an issue, so the ATM layer is not required for the purpose of frame segmentation. When standards under development for Ethernet over copper such as: IEEE802.3ah (EFM) and 10MDSL are completed they can be considered for future work in the DSL Forum Architecture & Transport WG.

14.5 Addendum: Some future considerations beyond the Proposed Ethernet Transport Target Network Architecture – possible Ethernet application for higher speed DSL access technolgies:

Note that this section of text is outside of the scope of this network migration document, because ethernet standards IEEE802.3ah (EFM) and 10MDSL are still under development at this time. In general, future standards providing higher upstream bandwidth can reduce the need for frame segmentation, and the ATM layer could potentially be omitted in those areas where these new high speed standards may be deployed. Thus, seen from a QoS perspective ATM can be considered optional in the local loop when the line speed is relatively high in each direction, say 4-5Mbit/s or more. In that case, the worst-case delay caused by a long (1500 bytes) Ethernet frame does not significantly delay the real-time traffic frames. However, a Multi-Service requirement is that even in this case that the Access Node must enforce that the priority settings are correct on upstream traffic. Furthermore, the Access Node must still be able to limit the bandwidth available to subscribers for different services/priorities. This policing functionality could be implemented either on layer 2 (Ethernet frame policing, MPLS policing) or layer 3 (IP packet policing).

The bandwidth provisioned to each subscriber is clearly a chargeable service parameter. With ATM on the local loop the ATM PVC settings define the available bandwidth. Without ATM, the bandwidth control must be performed by similar functionality in the Access Node.

VLANs may stretch all the way to the CPE where it is mapped towards different applications. The Access Node must still provide control of which VLANs that the subscriber has access to. This scenario is particularly relevant when ethernet is exclusively used as the layer 2 technology on the U interface.

15. References

2001.496 Section 7

[1] ITU-T G.991.2, "*Single-pair high-speed digital subscriber line (SHDSL) transceivers*", 2001
[2] ITU-T G.992.1, "*Asymmetrical Digital Subscriber Line (ADSL) Transceiver",* 1999
[3] ATM Forum AF-PHY-0086.001, "*Inverse Multiplexing for ATM (IMA) Specification Version 1.1*", March 1999
[4] ETSI TM6 contribution 013t39, "*IMA support in SDSL Access Environment*", September 2001
[5] IETF RFC 1990, "*The PPP Multilink Protocol (MP)",* 1996
[6] IETF RFC 2686, "*The Multi-Class Extension to Multi-Link PPP",* 1999
[7] DSL Forum Technical Report TR-043*, "Protocols at the U Interface for Accessing Data Networks using ATM/DSL*", August 2001
[8] ITU-T Question 4/15, "G.991.2: Implementor's Guide Draft Text", October 2001

2002.141 Section 10

[9] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.
[10] Bradner, S., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification", RFC 2205, September 1997.
[11] Wroclawski, J., "The Use of RSVP with IETF Integrated Services", RFC 2210, September 1997.
[12] Wroclawski, J., "Specification of the Controlled-Load Network Element Service", RFC 2211, September 1997.
[13] Shenker, S., Partridge, C., Guerin, R., "Specification of Guaranteed Quality of Service", RFC 2212, September 1997.
[14] Garrett, M., Borden, M., "Interoperation of Controlled-Load Service and Guaranteed Service with ATM", RFC 2381, August 1998.
[15] Crawley, E., Berger, L., Berson, S., Baker, F., Borden, M., and J. Krawczyk, "A Framework for Integrated Services and RSVP over
ATM", RFC 2382, August 1998.
[16] Suzuki, M., "The Assignment of the Information Field and Protocol Identifier in the Q.2941 Generic Identifier and Q.2957 User-to-user Signaling for the Internet Protocol", RFC 3033, January 2001.

2001.447 Section 11

[17] "Evolution of DSL to Next Generation Networks", DSLForum 2001-266, G. Young, August 2001.
[18] "ATM transport over ADSL Recommendation (update to TR-017", DSL Forum TR-042, August 2001
[19] "Auto-Configuration Architecture & Framework", DSL Forum WT-60v3, September 2001
[20] "DSL Service Flow-Through Fulfillment Management Interface", DSL Forum WT- 63v3.2, October 2001
[21] "ATM-MPLS L2 cross-connect in DSL access networks", DSLForum2001-449, S.Ooghe, L. Pauwels, P.Nelson November 2001
[22] "BGP/MPLS VPNs", IETF RFC 2547, E. Rosen, Y. Rekhter, March 1999
[23] "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM", DSL Forum TR-037, March 2001

2001.449 Section 12

[24] Contribution DSLForum2001-447, Sven Ooghe, Munich meeting, December 2001
"Next generation network DSL access scenarios using an MPLS architecture"
[25] DSL Forum, TR 037 "Auto-configuration for the connection between the DSL B-NT and the network using ATM"
[26] Frame Relay Forum, FRF.8.1, February 2000 Frame Relay/ATM PVC Service Interworking Implementation agreement