TECHNICAL REPORT

TR-025

Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL

Issue: 1.0
Issue Date: September 1999

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies.

Issue History:

Version 1.0	February 1999	Created new document
Version 1.1	April 2, 1999	Modified text to reflect comments received from Washington D.C meeting
Version 1.2	April 29,1999	Review
Version 2.0	May 3, 1999	Update the scope of the document
Version 2.1	May 25, 1999	Ready for ATM working group review
Version 3.0	June 18, 1999	Updated based on the comments received from review meeting on May 27, 1999.
Version 4.0	June 28, 1999	Straw Ballot
Version 5.0	September 16, 1999	Updated based on Straw Ballot comments and ready for Letter Ballot

Technical comments or questions about this Technical Report should be directed to:

Editor: Ray Wang 3Com Corporation ray_wang@3com.com

CONTENTS

LIST OF FIGURES

ABSTRACT

This document presents the Core Network architecture for ADSL service access to legacy data networks. The content of the text is derived from several The Broadband Forum architecture contributions and other references.

1 Introduction and Scope

This document recommends a set of interoperable Core Network Architectures to support broadband service over ADSL systems, and specifies minimum requirements for each. This document is an extension of TR-012, "Broadband Service Architecture for Access to Legacy Data Networks over ADSL". Therefore each of the network architecture is based on the PPP over ATM (over ADSL) model. The scope of the text is limited by the contributions related to this subject. Documents that are referenced are listed in Section 11. The principal objectives of this document are to provide a number of references Core Network architectures that will support access to legacy data network and are consistent with TR-012.

2 Definitions

The following definitions apply for the purposes of this document:

Access Network – The ADSL access network encompasses the ADSL modems at the customer premises and the Access Node at the central office.

Access Node – It is referred to as the concentration point for Broadband and Narrowband data. The Access Node may be located at the central office or the remote site. A remote Access Node may subtend from a central access node. Access Node is also referred to, in TR-012 [1], as DSL Access Multiplexer in the access network.

ADSL – One of the copper access-transmission technologies with data rate of 1.5 – 9 Mbps for downstream and 16 – 640 kbps for upstream. Specific line coding is not assumed.

Architecture Coexistence – One or more network dependent protocols, e.g., ATM and Frame Relay coexist in the Core Network architecture.

Core Network – One or more network entities inter-working together to provide the differential transport services between ATU-C and Service Providers. Thereby the Core Network contains the Access Node or DSL Access Multiplexer (DSLAM) and the Regional Broadband Network. The Regional Broadband Network may institute different transport protocols such as ATM, Frame Relay or IP.

CPE Architecture – An architecture that defines the access behavior within the customer premises network and the interface to the access and the Core Network. Both S and T reference points are considered to be within the CPE architecture.

Downstream – The direction of transmission from the ATU-C to the ATU-R

Legacy Data Network – Refers to the Service Provider Network, which may include the ISP POP, content provider networks, corporate networks and regional operation center (ROC).

Network Access Provider – A Company providing access network services, in particular, the ADSL facilities.

Network Service Provider – A collective terminology for Internet Service Provider, Corporate network and Locally Hosted Content provider.

PPP over ATM or **PPP over ATM over ADSL** – A mechanism for an ADSL end user(s) to access ATM-based broadband services using the PPP protocol [7] in a way that is compatible with the authentication, the authorization and the accounting procedures used in today's ISP dial-up model.

Small Office Home Office (SOHO) – Refers to a small business unit located either remotely or at home. The size is usually smaller than a branch office.

Upstream – The direction of transmission from the ATU-R to the ATU-C.

3 Terminology of Requirements

This section defines the terminology for complying with the requirements imposed upon the Core Network Architecture.

MUST	This word, or **REQUIRED**, means that the requirement is fundamental to this recommendation.
MUST NOT	The phrase means prohibition is absolute.
SHOULD	This word, or **RECOMMENDED**, means that there may exist valid reasons in particular circumstances to ignore this requirement, but the full implications must be understood and carefully weighed before choosing a different course.
MAY	This word, or **OPTIONAL**, means this requirement is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

4 Network Services and Applications

The principal requirements of the Core Network Architecture are defined in TR-012 [1] and TR-018 [2]. TR-012 recommends PPP over ATM (over ADSL) as the user plane protocol independent of transmission layer line code at the U-interface and TR-018 specifies the references and the requirements for CPE architectures to access legacy data services through the U-interface.

Therefore, this document recommends a set of the Core Network architectures that are compatible with TR-012 and also support the connectivity requirements for applications specified by TR-018. Thereby, the scope of this document is to specify recommendations as to the Core Network infrastructure, its associated protocols and interfaces beyond the U-interface to support the customer premises for application to access the legacy network.

TR-018 states that there are two key issues in development of a CPE Architecture solution. One is whether multiple PCs will be interconnected sharing a common high-speed data pipe or if it is only a single PC connected to the high-speed data access, and the other is the type of applications the end user is expected to use. These two variables generally separate residential and SOHO data accesses to the Core Network into the following scenarios:

- Sessions to individual applications
- Multi-homing of individual applications
- Multiple sessions to single NSP
- Simultaneous sessions to multiple NSPs

Support for sessions to individual applications is accomplished by transporting PPP from the end system (e.g., PC) across the U-interface (see Figure 2) to enter the Core Network. One VC is mapped to one PPP session.

Multi-homing of individual applications is a mechanism whereby an individual end system may support more than one PPP session while remaining compatible with TR-012. In this scenario, the corresponding VCs are provisioned for each PPP session. Nevertheless, it may be desirable for the Core Network, at some point, to support the termination function of multiplexed PPP sessions over a shared VC[1].

Multiple sessions to a single NSP allow multiple end systems to share a common link to an NSP through an aggregation function (bridging or routing [8]) function in either the B-NT or a proxy. This means that one or more subnets in the premises on the same Layer 3 network all have logical connectivity with an external Layer 3 network, i.e., NSP. Therefore, it is desirable for the Core Network to support the aggregation function where the PPP session is terminated in the Core Network.

[1] Recognizing that services carrying multiple PPP sessions over the U-interface has now been offered by network service providers, hence it is a need for contributions to address this issue and to update this document in the near future.

Simultaneous sessions to multiple NSPs allow a single user or multiple end systems on a CPE network to have active sessions with different NSPs simultaneously. Some form of Layer 2 multiplexing may be performed at the premises in order to allow multiple Layer 3 domains to be simultaneously supported. In this scenario, it is desirable for the Core Network to be able to support the session aggregation function to interface to multiple NSPs. However, there is a potential security problem, especially when one of the NSPs is a corporate network.

The access scenarios described above demand that a Core Network support:

- Interworking between the 'V' and the 'A10' NSP interfaces. This may occur at the ATM or the PPP layer.
- Bulk provisioning.
- Mechanisms to ensure privacy of user data.

In addition, the Core Network may support:

- Aggregation of traffic from multiple Access Node and delivery of the aggregated traffic to the NSP. The aggregation may or may not involve statistical multiplexing.
- Proxy Authentication, Accounting, Addressing and Authorization on behalf of the NSP.
- Quality of Service objectives and/or service level agreements.

5 Access Configuration

The ability to provide services to a large population of customers plays a key role in deploying ADSL services including Internet access, corporate network access, local content and peer-to-peer communications.

The Core Network operator **MUST** be equipped with effective tools to support the service provisioning and selection between the Service Provider and the user as depicted in Figure 1. The service provisioning **MUST** exist between Service Provider and end user. The mechanism of transporting the service provisioning information to a user **SHOULD** be automatic without the user's intervention, so that user can access a service offered by an NSP based upon the received service provisioning information.

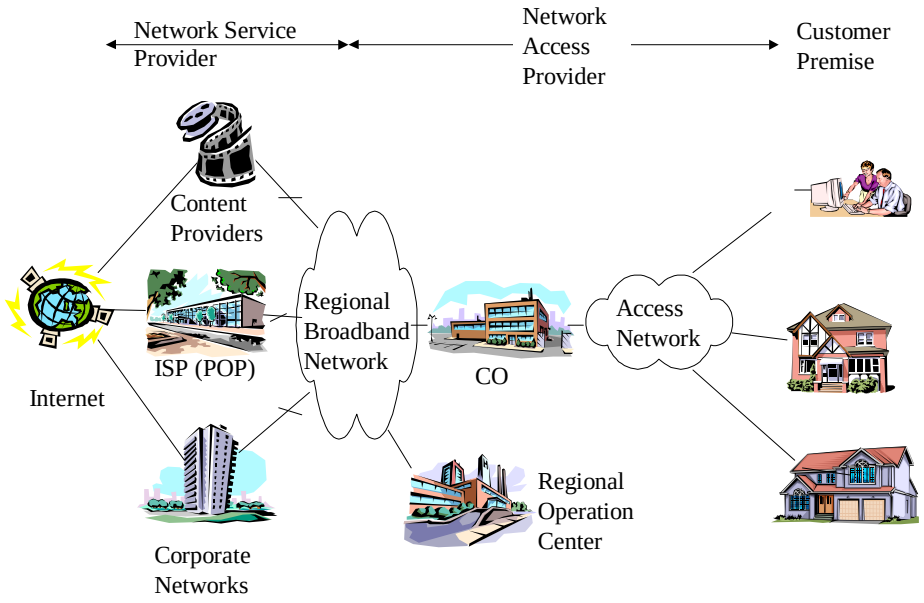

Figure 1 - Access Configurations

Sections 5.1 through 5.4 illustrate categories of Network Service Providers.

5.1 Internet

Providing high-speed Internet access is valuable for both home users and small businesses. The Internet is accessed through one or more ISPs that are connected through the Regional Broadband Network to the Access Network. The Regional Broadband Network can be a combination of ATM, Frame Relay or IP based networks. A "path" or virtual circuit between the user and ingress service point MUST be presented before access by the user is possible. The mechanism of transporting the service provisioning information to a user SHOULD be automatic without requiring user intervention. For example, use of ATM ILMI PVC auto-configuration of PVCs (The ATM Forum Technical Committee, af-nm-0122.000, May 1999).

5.2 Corporate Networks

Two approaches are recommended for access to corporate networks. The first uses tunneling (i.e., IPSec [10] or L2TP [6]) across an IP network, possibly the Internet to the corporate network. This approach replaces dial-up modems by using a virtual private network across the Internet. In the case of L2TP, which is referred to as a "compulsory" tunneling model, the tunnel is created without any action from the user, and without allowing the user any choice in the matter. The L2TP tunneling model can be on top of IPSec if the security is required.

The second approach is to use the Regional Broadband Network to provide direct high-speed connectivity to the corporate network. This has the advantages of being able to offer higher speed, QoS guarantees and greater security. Nevertheless, a "path" or virtual circuit between the user and the ingress service point MUST be established. The provisioning data SHOULD include the relationship between the service and the virtual circuit and the security policy in case of IPSec or tunneling end-to-end.

5.3 Local Content and Services

Locally hosted content and services may be located in a content provider that is connected to the regional broadband network; or located in Network Access Provider facilities (e.g., a central office). Local content can be originated locally (such as merchant services for retailing) or originated remotely (e.g., Web content from the Internet cached in local servers).

5.4 Peer-to-peer communication

The ability to interconnect consumers at high speed enables high quality peer-to-peer communication applications such as video telephony or interactive gaming. As with connections to corporate networks, the end points could be connected through a NSP network or the Internet, or directly through the Core Network. If connected through the Core Network, a "path" or virtual circuit between peers **MUST** be established.

6 Functional Requirements

The network model for ADSL is based on the widely deployed dial-up model, which uses PPP to support the network services described in Section 5. Therefore, a Core Network architecture that is consistent with TR-012 and meets these service demands has the following requirements:

- It **MUST** have the ability to transport one or more network layer protocols through either the PVC or the SVC setup.
- It **MAY** interwork one or more network layer protocols, e.g., Frame Relay and ATM.
- It **MAY** support simultaneous access to multiple Network Service Providers.
- It **SHOULD** have simultaneous multiple class of service or QoS support.

- If SVC service is offered, it **MUST** support Q.2931 procedures for SVC establishment as consistent with TR-017.
- If SVC service is offered, the Broadband Lower Layer Interface (B-LLI) information element **MUST** be transported transparently between ATM end systems to permit the end system to specify PPP and the encapsulation to be used.

7 Core Network Reference Model

The end-to-end ADSL network reference model is depicted in Figure 2.

The Core Network reference model is a subset of the end-to-end architecture; it is composed of two functional blocks and three reference points. The Access Node and the Regional Broadband Network are the two functional blocks. U, V and A10 are the three reference points.

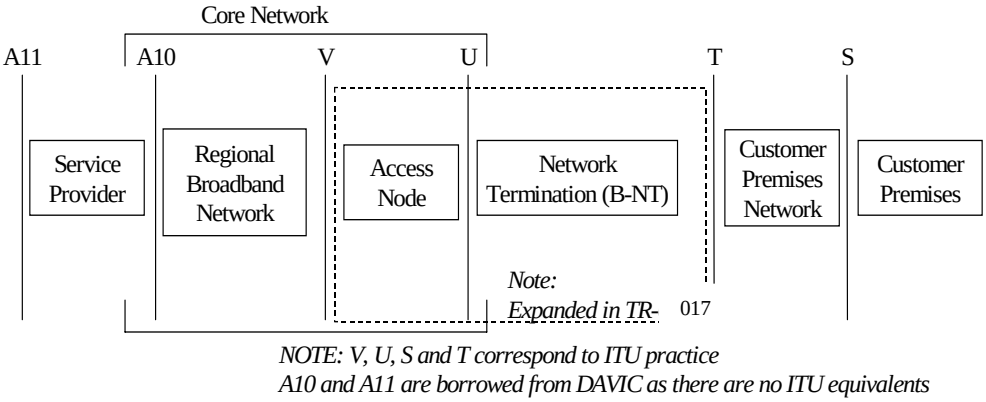

Figure 2 - Architectural reference model

Sections 7.1 through 7.5 describe the significant features of the Core Network reference model.

7.1 Access Node

The Access Node is the concentration point for broadband and narrowband data. The Access Node may be located at a central office or a remote site. The Access Node serves as an ATM layer multiplexer/concentrator between the ATM Core Network and the Access Network. In the downstream direction it may perform routing/ demultiplexing, while in the upstream direction it may perform multiplexing/concentration and higher layer functions, e.g., co-location with Core Network functions.

The Access Node contains a Core Network Interface Element that performs the ATM and PHY layer functions to interface to the ATM Core Network. Non-ATM core networks are not precluded. The VPI/VCI translation and higher-layer function performs the multiplexing/demultiplexing of the VCs between the Access Network interfaces (ATU-Cs) and the Core Network interface on a VPI and/or VCI basis. This block may also perform other higher layer protocol functions. The Access Network side ATM layer functions, if present, support the ATU-Cs, which terminate the Access Network lines in the Access Node. If an ATU-C supports both 'Fast' and 'Interleave' channels two ATM TC sublayer functions may be needed. Traffic management functions should be performed to support rate matching between V and U interfaces. [3]

7.2 Regional Broadband Network

The Regional Broadband Network interconnects the access nodes in a geographical area. This text does not assume ATM is the only transport technology, although ATM has been increasingly deployed in this infrastructure to provide broadband connectivity among COs. A service interworking function is required if the Regional Broadband Network includes multiple transport technologies such as ATM, Frame Relay or IP.

7.3 U Reference Point

This reference point lies between the B-NT (ATU-R) and the Access Node. PPP-over-ATM-over-ADSL has been identified by TR-12 as the Layer 2 protocol over the U-interface to access legacy data networks.

7.4 V Reference Point

A logical interface called V-C, as defined in T1.413 [4], connects the individual ATU-C functions to the corresponding ATM layer functions.

7.5 A10 Reference Point (NSP POP Interface)

This reference point is between the Regional Broadband Network and the Network Service Provider POPs. Multiple PPP sessions may be multiplexed over a single VCC at this interface.

8 Core Network Architecture

This section provides service and functional architectures. The service architecture focuses on the architectural abstraction; the functional architecture provides protocol and interface recommendations.

8.1 Core Network Service Architecture

The Core Network (solid line block in Figure 3) contains the Access Node or DSL Access Multiplexer and the Regional Broadband Network. The Regional Broadband Network may use different transport technologies such as ATM, Frame Relay or IP. An ATM Core is shown in Figure 3.

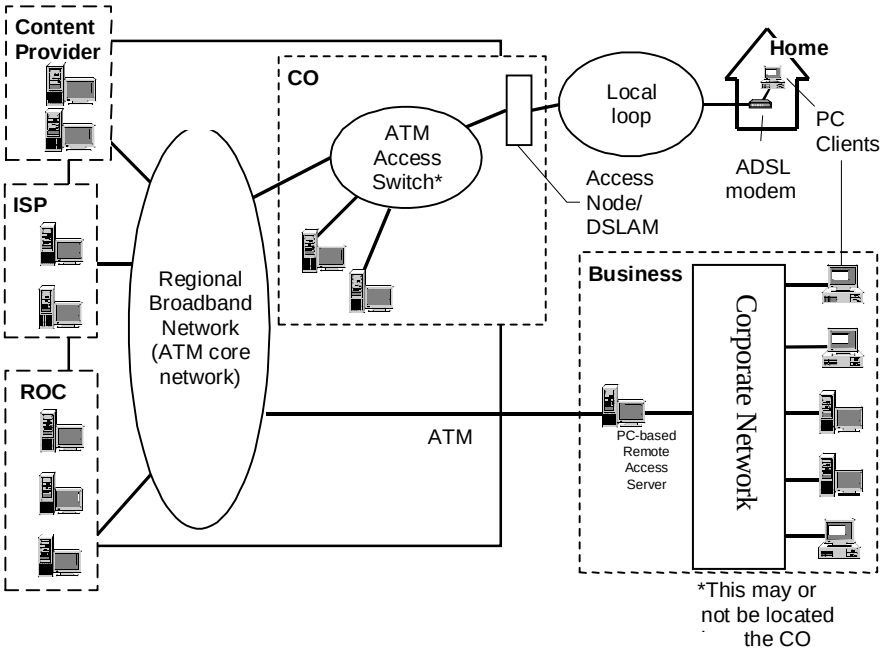

Figure 3 - Service Architecture – abstract view

Sections 8.1.1 and 8.1.2 describe the major components of the Core Network service architecture.

8.1.1 Access Node

The Access Node hosts the following functions:

- Provide termination of the ADSL user lines.
- Provide concentration and multiplexing of the ADSL user lines towards the Regional Broadband Network. The concentration ratio between user lines and single network interface is an important cost factor in service deployment.
- **MAY** provide termination of customer ATM signaling channels. This is desirable in order to provide a standard yet scalable mechanism for supporting switched virtual circuit service to an ADSL customer.
- Provide service configuration of PVCs to ATU-R.

When the service model includes SVC and the Access Node does not terminate signaling channels, then a signaling proxy is required in the Regional Broadband Network. Given the current state of the art, a proprietary system management is required between the Access Node and the proxy in order to support concentration in the Access Node.

8.1.2 Regional Broadband Network

The Regional Broadband Network (RBN) interconnects Access Networks and Network Service Provider networks. Although ATM is being deployed over the SONET infrastructure to provide broadband connectivity among COs, other transport protocols also exist and should not be excluded from end-to-end ADSL services. Frame Relay and IP are examples. The RBN does the following functions:

- Provides service provisioning and backbone bandwidth allocation.
- MAY provide aggregation of PPP traffic.
- MAY provide signaling and service interworking.

- MAY provide Proxy authentication, Accounting, Addressing and Authorization.

8.2 Core Network Functional Architecture Recommendations

In order to support the requirements set by TR-018 and to be compatible with TR-012, four architectures are recommended: the Transparent ATM Core Network architecture, the L2TP Access Aggregation (LAA) architecture, the PPP Terminated Aggregation (PTA) architecture, and Virtual Path Tunneling Architecture (VPTA).

8.2.1 Transparent ATM Core Network

In the Transparent ATM Core Network architecture, all protocols above the ATM layer are carried transparently across an ATM-based Regional Broadband Network between the V and A10 interfaces. There is no service interworking function in the core network. Once the ATM layer connectivity is established between the customer premises and the Network Service Provider network, the session setup and release phases at the link level and network level are established as specified by the NSP. All functionality above the ATM layer is delegated to the NSP. See RFC 2364 [5] for connectivity procedures and encapsulation format for PPP over ATM. This architecture and its protocol stack are depicted in Figure 4.

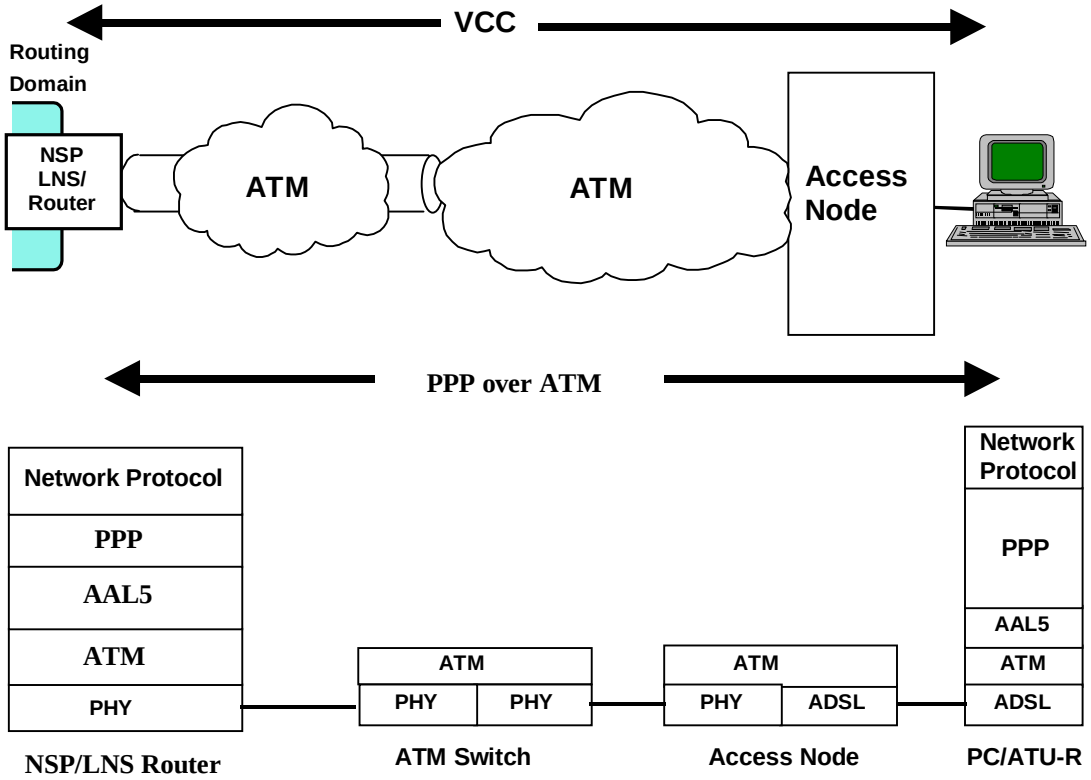

Figure 4 - Transparent ATM Core Network

8.2.2 L2TP Access Aggregation (LAA)

Layer 2 Tunneling Protocol (L2TP) [6] is a protocol for extending PPP sessions over an arbitrary network[2] to a remote network server known as the *L2TP Network Server* (LNS). L2TP was originally designed to support

[2] Currently L2TP is specified over UDP/IP; work is in progress for direct transport over Frame Relay and ATM.

roaming operations, where the user does not dial directly into his destination ISP or Corporate dial server. Instead, the user dials into an *L2TP Access Concentrator* (LAC) which extends the PPP session to the LNS. The capabilities of L2TP can readily be leveraged to support dynamic service selection for PPP over ATM VCCs in the ADSL space.

The basic principle behind the L2TP Access Aggregation architecture is to "tunnel" PPP through the Regional Broadband Network. There are two functional components that are required in order to do this. The first is the L2TP Access Concentrator (LAC). The second is the L2TP Network Server (LNS). The functions of the LAC are performed in equipment connected to the Regional Broadband Network side of the Access Node. The functions of the LNS reside in the NSP network.

Each user has an ATM VCC that originates at the ATU-R is cross-connected in the Access Node and terminated at the LAC. PPP-over-ATM is employed within the ADSL Access Network. The LAC and LNS can be connected over any network supporting the L2TP protocol; for example, it may be either an IP network or a leased line service (e.g., ATM or Frame Relay) depending on the infrastructure and requirements of the Network Service Providers.

The PPP link is then tunneled from the LAC over the Regional Broadband Network to the LNS at the NSP. The placement of the LAC function may change as deployment evolves. Early deployment is expected to use one LAC to support many Access Nodes, but, as ADSL service increases, the number and the location of LAC functions may change. The Access Node may be a candidate for functional migration. The network topology and protocol stacks for the LAA architecture are shown in Figure 5. The Access Node and ATU-R are part of the ADSL Access Network. The Core Network **MUST** be able to accept PPP over AAL5 at the 'V" interface. The Access Node is connected to LAC via ATM interfaces. When permanent connections are used either PVCs or PVPs can be provisioned between Access Nodes and LACs. Bulk pre-provisioning of permanent connections (with, for example PVPs) simplifies the service activation process. An automated service provisioning mechanism **SHOULD** be employed. A UNI 4.0 ILMI-based Auto Service Provisioning **MAY** be a candidate (ATM Forum Technical Committee, af-nm-0122.000, May 1999).

The LAC tunnels the PPP session to the NSP. The LAC interfaces to the Regional Broadband Network using a network technology agreed between the Network Access Provider and the NSP. The NSP employs LNS to strip off the L2TP encapsulation and terminates the user's PPP connection. The LNS also provides conversion from the Regional Broadband Network technology to that used by the NSP. This provides connectivity to the NSP in a manner similar to that which dial-up modem access provides today. PPP provides a Link Control Protocol (LCP) and a Network Control Protocol (NCP) to negotiate link layer and network layer options. These options can be negotiated on the end-to-end link between the CPE and the destination router.

8.2.2.1 Session Establishment

The user initiates a session by establishing a PPP connection between the user's CPE and the LAC. In the case where the PPP session originates from the user's CPE, the user will employ a dialer application on the CPE to initiate a session. Upon initiating a session, the CPE will send a *PPP LCP Configuration-Request* to the LAC. The LAC responds with a *PPP LCP Configuration-ACK*. The PPP at the CPE responds with a *PPP LCP Configuration-ACK* to end the configuration and enter the state of *LCP Opened*.

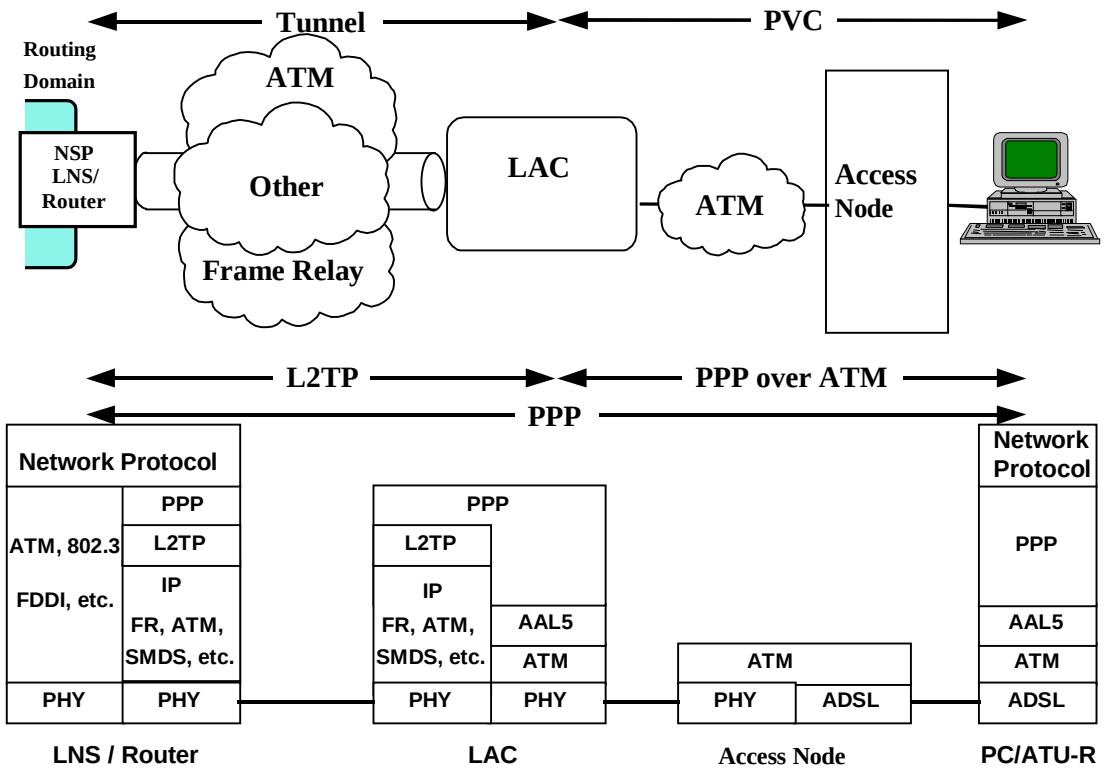

Figure 5 - L2TP Access Aggregation

PPP allows for the specification of options to be placed in the Configuration-Request and for the negotiation of any unacceptable options. PPP also allows for authentication to be requested during the negotiation. For this application to work, the LAC must be informed of the user's intended NSP. A user name along with a fully qualified domain name entered during the PPP authentication phase can provide such information. Once the option negotiation is complete and the user is identified, a PPP connection exists between the LAC and the CPE. The next phase is to extend the PPP session from the CPE to the chosen LNS.

Based on the user-name and domain information provided in the authentication phase of the PPP establishment, the LAC determines the destination. For example, if the user enters *Joe@ nsp.net* for the user-name, the LAC knows that *nsp.net* is the destination NSP.

The LAC determines if a tunnel already exists to the proper LNS. If it does not exist, the LAC establishes one. In order to establish a tunnel it is assumed that there is a path or route between these two entities. This path or route can be supported over a variety of network technologies, including IP, Frame Relay, or ATM.

8.2.2.2 Packet Trace Through Network

An upstream packet from a user is encapsulated in PPP and sent across the ADSL link to the LAC. The LAC associates a user's PPP link with a tunnel and Call-ID. The LAC will encapsulate the PPP data in L2TP and forward it across the appropriate tunnel. The LNS will strip off the L2TP encapsulation and terminate the PPP. The LNS will extract the payload of the PPP frame (which may be IP, IPX, etc.) and handle it appropriately.

In the downstream direction, the LNS encapsulates user data in PPP then encapsulates the PPP packet into L2TP and forwards it to the appropriate LAC. The LAC will know the user to which the data is destined by the tunnel and Call-ID in the L2TP encapsulation. The LAC will terminate the L2TP and send the PPP packet across the appropriate ATM VC.

8.2.2.3 Tear Down

The user disconnects a session using the PPP virtual dialer (controlling the PPP Stack). In doing so, the dialer will issue a *PPP LCP Terminate-Request.* The LCP packet, like other packets from the user, is encapsulated in L2TP at the LAC and sent to the LNS. The LNS will receive this packet, and respond by sending a *PPP LCP Terminate-Reply* packet to the user. The LNS, knowing the user has ended the session, then sends an *L2TP Call-Disconnect-Notify* control packet to the LAC in order to release that session (Call-ID) in the tunnel, and the session is terminated. The LAC and/or the LNS may implement a time-out feature to automatically tear down a session if no data is transmitted for a certain length of time. This will ensure that the L2TP session is terminated even if the user shuts down their CPE without issuing a *PPP LCP Terminate-Request.*

8.2.3 PPP Terminated Aggregation (PTA)

The PPP Terminated Aggregation (PTA) architecture also allows carriers to leverage the suite of PPP protocols in the ADSL Access Network. However, in this case, instead of being tunneled all the way to the NSP, the PPP sessions are terminated in a Broadband Access Server (BAS). Network layer packets are extracted and forwarded over a Regional Broadband Network to the proper NSP. Although this architecture does not necessarily assume an ATM infrastructure to the NSP, the network **MUST** be able to accept PPP-over-ATM (AAL5) at the V-interface. Any network technology (e.g. Frame Relay, ATM, SMDS, private lines, etc.) which encapsulates network layer packets can be used between the NSP and the ADSL Access Network. The user initiates a session by establishing a PPP connection between the user's CPE (e.g. PC) and the BAS. The BAS terminates PPP and forwards the user's network layer traffic to the appropriate NSP to which the user is associated on a session-by-session basis. The NSP need not understand or support PPP functions.

The PTA network topology and protocol stack is shown in Figure 6 and Figure 7 respectively. The Access Node and the ATU-R are part of the ADSL Access Network. It is assumed that PPP over ATM over ADSL is used in this portion of the network. The Access Nodes are connected to the BAS through an ATM network. Each user requires either a provisioned or signaled VCC to the BAS. Just like for the LAA model, this provisioning is purely driven by the subscription process of the access provider, and does not involve the NSP.

The BAS by definition is a network layer device and may be required to provide network and higher layer services. The BAS interacts with both the user and the NSPs 'AAA' infrastructure to provide functions such as IP address configuration and user authentication, user authorization and NSP accounting using the PPP suite of protocols and proxy transactions to the NSP. In the case of an IP network as shown in Figure 6, an IP address and other configuration information for the user are also obtained from the NSP during this query. On the outbound side, the BAS provides an IP router interface to the NSPs. It is configured to support any physical layer transport of IP packets to the NSPs. After the BAS has established a PPP session with the user, it maps a user-identifier to the NSP port. This user identifier can be a session identifier or a user port identifier. This unique mapping will be used to forward the user's network layer packets to the destined NSP. It is important to note that in the upstream direction the BAS behaves as a session-driven policy router. The BAS forwarding engine does not rely on destination IP addresses to determine the NSP, but purely on the session-by-session association between users and NSPs. The NSP on the other hand employs an IP router that receives these packets and forwards them accordingly. When the user wants to initiate a connection to the NSP, he establishes a PPP session to the BAS. The user and the BAS exchange IP packets over the PPP link. The BAS and the NSP exchange IP packets over the Regional Broadband Network using the particular network technology indicated by the NSP. When the user wants to terminate the connection to the NSP, he terminates the PPP session to the BAS. The BAS deletes the user-NSP mapping in its routing tables and returns the IP address to the NSP.

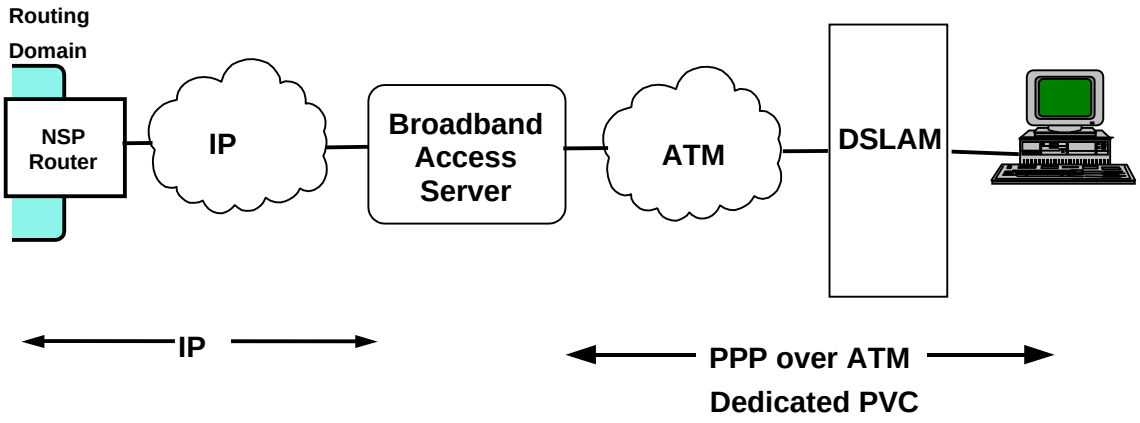

Figure 6 - Network Topology for PPP Terminated

The protocol stack for PPP Terminated Aggregation is shown below in Figure 7. Similar to today's dial-up remote networking, PPP is used to encapsulate IP packets. The Access Network employs PPP over ATM over ADSL. Each user employs ATM SVC service or is pre-provisioned with an ATM VCC to the BAS. From the BAS, the users' network layer packets are extracted from the PPP frames and sent to the NSPs over potentially different network technologies. In the case of ATM, one or more ATM VCCs will exist between the BAS and the NSP.

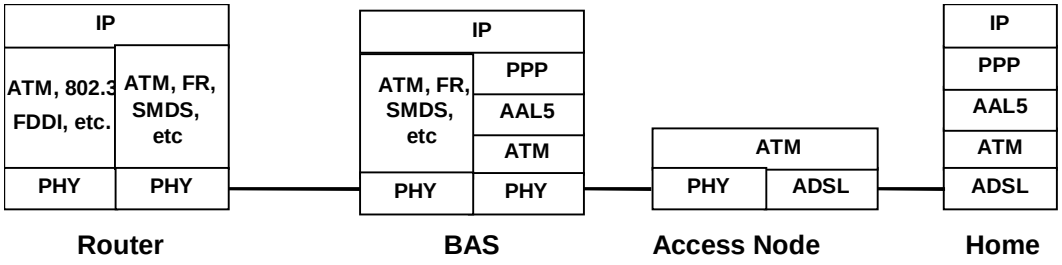

Figure 7. Protocol Stack for PPP Terminated Aggregation

Figures 6 and 7 show a representation of the equipment and protocol needed to implement this architecture. In the Access Network, the equipment is similar to the L2TP architecture discussed in Section 8.2.2. The customer premise equipment is connected to an Access Node in the central office via an ADSL loop. The Access Node provides the termination of the ADSL signal. The Access Node does not process any higher layer protocols. It multiplexes the PPP over ATM signals from end users onto DS1, DS3 or SONET WAN facilities. Instead of terminating at a LAC, the ATM connections are terminated at a BAS.

The BAS terminates the PPP on the incoming, extracts the network layer packets and forwards them to the NSP associated with the session. It implements the basic PPP session management functions and supports the basic NCP functions for IP transport over PPP. Its connections to the various NSPs can be based on different networking technologies; ATM, Frame Relay, SMDS, private lines, etc. Each NSP's port on the BAS requires some amount of the NSP's IP address space. This information can be pre-configured into the BAS or can be dynamically obtained from the NSP. The mapping of the domain portion of the user-name to a destination NSP router can be stored in a local database (as in the case of LAA).

8.2.3.1 Session Establishment

This architecture requires minimal changes to the client's desktop. The user initiates a PPP session to the BAS over an ATM VCC. In the case when the user's CPE initializes the PPP session, the user will rely on a virtual dialer program on their CPE. The virtual dialer program will be similar to a dialer commonly used today and will facilitate PPP negotiation and login ID and password entry. Upon initiating a session, the virtual dialer will send a *PPP LCP Configuration-Request* to the BAS. The BAS responds with a *PPP LCP Configuration-ACK*. The PPP dialer responds with a *PPP LCP Configuration-ACK* to end the configuration. Once the link is established, the BAS initiates the authentication stage and challenges the user for the user-name and password. As with the LAA model, the user will reply with a user-name along with a fully qualified domain name (e.g. *Joe @ nsp.net)*. The BAS extracts the domain string portion of the user-name and sends off a query to NSP to authenticate and obtain address information (e.g., DNS server's address). In the case of IP network, The NSP replies with an IP address and other IP configuration information (e.g. DNS server's address). This information is passed along to the user during the NCP phase for configuring IP transport (based on IPCP). The BAS maps a user identifier (e.g. port, session identifier, etc.) to the outgoing NSP port.

Using PTA, multiple CoS can be supported with multiple logical connections between the BAS and the NSP. As is the case with the LAA model, the desired CoS can be determined by user-name login. In order to connect to the same NSP with different CoS, it would be necessary to require two different structured user-names (e.g. *Joe @ gold.nsp.net* versus *Joe@silver.nsp.net*). The CoS supports differentiated services between the BAS and the NSP router. The Access Network and the NSP's network will also need to provide differentiated service capability to support this feature end-to-end. The diagram in Figure 8 depicts the basic protocol sequences when a customer initiates a session. The sequence is shown with CHAP used for authentication, however, PAP could also be used. The use of CHAP or PAP is negotiated in the PPP LCP phase.

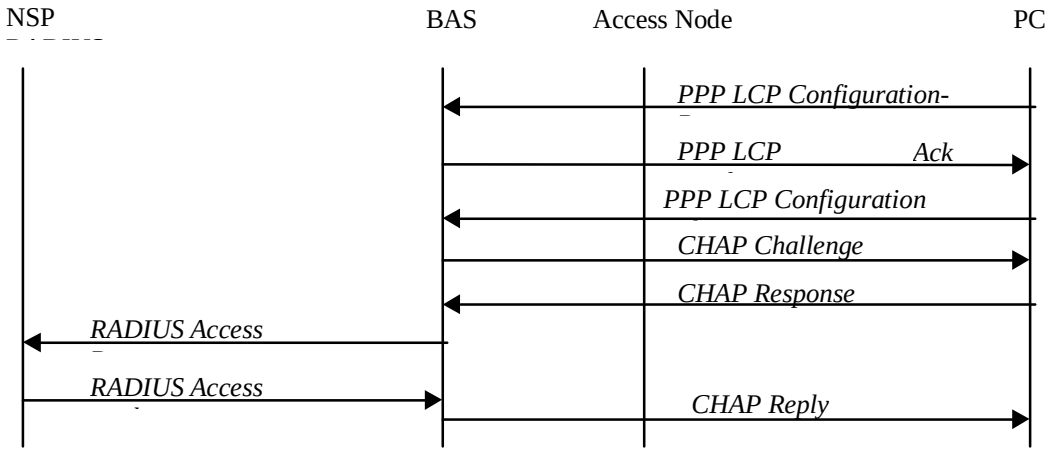

Figure 8. Example Session Establishment Sequence

8.2.3.2 Packet Trace through Network

A packet from a user is encapsulated in PPP and sent across the ATM link to the BAS. In case of an IP network between BAS and NSP, the BAS terminates the PPP on the incoming extracts the network layer packet and forwards them to the NSP associated with the session. In the downstream, IP packets arrive at the BAS from the NSP. The BAS examines the destination IP address to determine which user it is destined for. The BAS encapsulates the packet in PPP and forwards it over the appropriate ATM VCC to the user. Only those users that are connected to that NSP are considered, so there is no possibility of traffic being delivered to a user that has not been authenticated with the NSP and there is no problem if different NSPs have overlapping (private) IP address spaces.

8.2.3.3 Tear Down

When a user wishes to end a session, he can select disconnect on his virtual dialer. In doing so, the dialer issues a *PPP LCP Terminate-Request* to the BAS. The BAS responds with a *PPP LCP Terminate-ACK* and the session will be terminated. The BAS should return the IP address to the NSP for re-use. Optionally, an idle-time-out feature can be implemented to automatically tear down a session if no data is transmitted for a certain length of time. This will ensure that the session is terminated even if the user shuts down their CPE without issuing a *PPP LCP Terminate-Request.*

8.2.4 Virtual Path Tunneling Architecture (VPTA)

VP Tunneling is similar to the Transparent ATM model, except that the end-to-end PPP session uses a SVC established between CPE and the Access Node or a proxy signaling device. Therefore, the use of this architecture, shown in Figure 9, is predicated on the widespread availability of Q.2931 ATM signaling stacks in customer CPEs. A single Virtual Path Tunnel (VPT) is established between the network proxy device and NSP; similar to a single VC from the Network Access Provider to an NSP as used in the LAA and PTA except that no LAC or BAS function is installed by the Network Access Provider. When a customer wants to connect to their NSP of choice, all of their traffic is routed over the VPT and PPP can be used to encapsulate the traffic between the customer and NSP but other protocols could also be used. PPP over ATM (AAL5) **MUST** be supported at the V-interface.

The client-CPE initiates a session with the NSP by effectively invoking the Q.2931 signaling stack on their CPE or set-top box and providing the ATM address of the chosen NSP. A network proxy device terminates the ATM signaling and selects the VC that is connected to the selected NSP and that meets the QoS attributes specified by the customer. The network proxy device then cross-connects all user traffic from this session with that VC. The VC is selected from a pool of VCs at the NSP and it can carry one active session between the NSP and an active customer for the duration of the user session. The VC returns to the pool when the user session is torn down via Q.2931 disconnect.

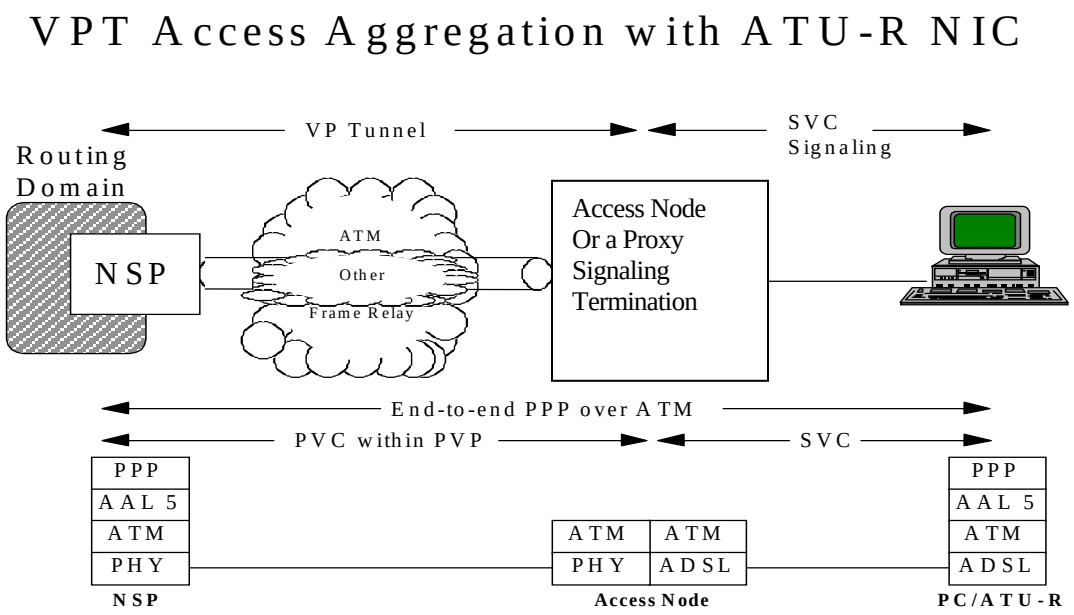

Figure 9. Virtual Path Tunnelling Architecture

9 Core Network Management

This section describes how the architecture addresses critical network management functions to support ADSL service end-to-end.

9.1 Circuit Configuration and Service Selection

Each of the four architectures presented in section 8 requires a virtual circuit to be established between the ATU-R and the Access Node as part of end-to-end connectivity. PVC configuration of the end-system can be done either manually or automatically. Manual configuration involves human interaction and is not recommended for mass ADSL service deployment. Automation can be done by either of two methods:

- Use a default virtual circuit ID and configuration[3]
- Use ILMI based auto-configuration MIB (ATM Forum Technical Committee, af-nm-0122.000, May 1999).

Either method requires no human intervention; the virtual circuit and associated traffic parameters are downloaded from the Access Node to the ATU-R automatically when the user initiates the request. The result of that is a list of connected provider names displayed to the user.

In the PPP over ATM model, when the user wishes to connect to a particular ISP, she (he) just selects the name and then starts the PPP session directly with the ISP via PPP over AAL5.

In a LAC or BAS model, when a user connects to the LAC or BAS, the user must have a method for indicating which NSP they wish to connect to. Both LAA and PTA will allow users to select the desired NSP through a user login employing a structured user name. During the PPP negotiation between the user and the LAC or BAS, the LAC or BAS can require a user name and password. The user name will be implemented as a structured user name in the form user-name@nsp.com. The LAC or BAS will examine the domain portion of the structured user name to determine the proper NSP. It is expected that all structured user names will follow DNS domain ownership rules (e.g., you need to manage the domain "nsp.com" to use tunnel names ending in "nsp.com"). If a given NSP supports more than one CoS, the desired CoS can be indicated in the structured user name.

9.2 Authentication, Authorization and Accounting

In the Transparent ATM, VPTA and LAA architecture, a PPP link is established directly to the NSP. The NSP is free to specify the desired authentication method during the PPP configuration. The LAC may gather authentication information while determining the proper tunnel. The LAC should forward this information to the NSP so that user does not need to re-enter the login information. The NSP is also free to implement additional stages of authentication across the PPP link. In the PTA architecture, a PPP link is established to the BAS. A user enters an ID and password. The BAS verifies the ID and password with the proper NSP through a proxy RADIUS query. The NSP still maintains authentication information. Note that both the NAP and the NSP are able to authenticate and gather accounting information with this architecture. In VPTA architecture, a PPP link is also established directly to the NSP.

Accounting can be handled with the RADIUS authentication server. After a user "logs-in" to the BAS or LAC, the BAS or LAC sends a RADIUS Accounting-Request to the RADIUS Server of the Network Access Provider, indicating the start of a user session along with all other pertinent information (e.g., user name, NSP, CoS, Session ID, etc.). This information may also be sent to an NSP's server via proxy RADIUS. When a user ends a session (through log-out or through a time-out), the BAS or LAC sends a second Accounting-Request to the RADIUS Server of the Network Access Provider, indicating the end of a user session. If the BAS or LAC counts the number of bytes sent to and from a user, this information can be sent to the RADIUS Accounting Server at this time.

[3] A default VCC for VPI=1 VCI=32 has been proposed, but no final decision is made at the current time.

9.3 IP configuration

In the Transparent ATM, the LAA architectures and the VPTA, a PPP link is established directly to the NSP. The user obtains IP configuration directly from the NSP via IPCP. IPCP supports the dynamic assignment of the user's IP address. In the PTA architecture, the user obtains his IP address from the BAS, again via IPCP. The BAS obtains the IP address from the NSP either dynamically or via delegation of an address range to the BAS. Scalability is enhanced if the addresses assigned to a BAS may be aggregated in routing advertisements.

9.4 Aggregation of customers

Both LAA and PTA provide aggregation of users on the interface to the NSP. In the LAA architecture, the current industry standard uses IP addresses to identify a tunnel. Simple mapping of IP addresses to ATM VCC, Frame Relay connection or leased line allow a variety of technologies when connecting with the NSP. Multiple users are aggregated into each tunnel. In the PTA architecture user data is interleaved to the NSP on one IP route.

9.5 Encryption, compression and security

PPP supports many link-level encryption and compression schemes. These schemes can be supported end-to-end in the VPTA, LAA model and Transparent ATM core model and can be supported between the user and the BAS in the PTA model. IPSec technology provides encryption and authentication schemes that do not rely on link-level mechanisms ubiquitously across all models. These tools can operate to provide end-to-end security over both the LAA and PTA models.

9.6 Link and performance monitoring and isolation

PPP supports link quality monitoring (RFC 1333). This can be supported end-to-end for the Transparent ATM, LAA and VPTA model and can be supported between the user and the BAS in the PTA model.

9.7 Resource allocation and traffic management

In the LAA architecture, the LAC (access provider policy) and the LNS (NSP policy) may perform the admission control for tunnels. If the number of users in a tunnel exceeds what the NSP deems is appropriate; the LNS will refuse to accept any more users until some of the existing sessions are terminated.

In the PTA architecture, the BAS will need to enforce any admission control policies on behalf of the NSP. The BAS can provide the NSP a report of the number of sessions rejected due to too many active sessions.

It is desirable for the LAC and BAS architectures to support differentiated services. This is a traffic engineering design issue that may require manipulation of the IP or tunnel mapping to the transport technology used between the NSP and the LAC/BAS and that between the LAC/BAS and the user. Nevertheless, it is outside the scope of this document to outline all the mechanisms that can be used.

However, the primary point of congestion is in the downstream direction (from NSP to CPE) at the LAC or BAS. The structured user-names allow traffic into the LAC and BAS to be segregated to support priority scheduling within the LAC and BAS as depicted in Figure 10 below.

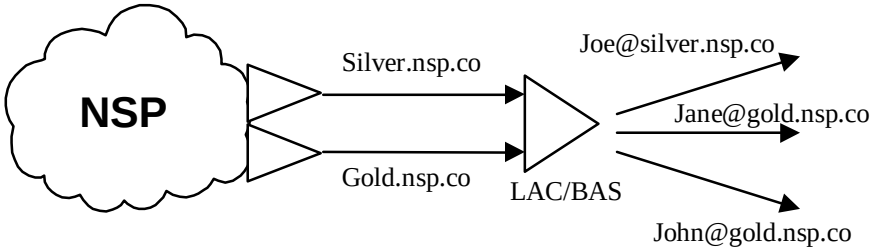

Figure 10. Logical Downstream Partitioned by the NSP

10 Architecture Coexistence

Depending on the network infrastructure on which the network Service Provider is deploying services, one or more network dependent protocols, e.g., ATM and Frame Relay may coexist in the Core Network Architecture. Figure 5 and Figure 6 demonstrate such coexistence. This requires interworking between transport protocols when circuits traverse heterogeneous networks.

This will impose a requirement on interoperability – even more so for a switched environment when end-to-end QoS must be sustained. The impact of this coexistence on the network architecture is outside the scope of this document.

11 Reference

The following Broadband Forum technical recommendations and other references contain provisions that, through reference in this text, constitute provisions of this Working Text. All references are subjected to revision although at the time of publication the editions indicated were valid. A list of currently valid documents referenced here is published:

[1] Broadband Forum TR-012, Broadband Service Architecture for Access to Legacy Data Network over ADSL Issue 1, June 1998

[2] Broadband Forum TR-018, References and Requirements for CPE Architectures for Data Access, March 1999

[3] Broadband Forum TR-017, ATM over ADSL Recommendation, March 1999

[4] ANSI, Network and Customer Installation Interface – Asymmetric Digital Subscriber Line (ADSL) Metallic Interface, T1.413 issue 2, T1E1.4/98-007/R5 1998

[5] IETF RFC 2364, PPP Over AAL5, July 1998

[6] IETF-PPPEX-L2TP-15.TXT, Layer Two Tunneling Protocol “L2TP”, March 1999

[7] IETF RFC 1661, The Point-to-Point Protocol (PPP), July 1994

[8] IETF RFC 1483, Multiprotocol Encapsulation over AAL5, July 1993

[9] ATM Forum, UNI Signaling, Version 4.0, July 1996

[10] IETF RFC 2401, Security Architecture for the Internet Protocol, November 1998

12 Acronyms

For the purpose of this Working Text, the following acronyms are used:

AAL	ATM Adaptation Layer
AAL5	ATM Adaptation Layer 5
ABR	Available Bit Rate
ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
ATM	Asynchronous Transfer Mode
ATU-R	ADSL Terminal Unit – Remote
ATU-C	ADSL Terminal Unit – Central
B-LLI	Broadband Lower Layer Interface
BAS	Broadband Access Server
B-NT	Broadband Network Termination
CBR	Constant Bit Rate
CHAP	Challenge Handshake Authentication Protocol
CO	Central Office
CPE	Customer Premises Equipment
DNS	Domain Name System
DS1	Digital Signal Level 1 (1.544 Mbps)
DS3	Digital Signal Level 3 (45 Mbps)
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
IETF	Internet Engineering Task Force
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
ISP	Internet Service Provider
LAA	L2TP Access Aggregation
LAC	L2TP Access Concentrator
L2TP	Layer 2 Tunneling Protocol
LCP	Link Control Protocol
LNS	L2TP Network Server
NSP	Network Service Provider
NT	Network Termination
PAP	Password Authentication Protocol
PC	Personal Computer

POP	Point of Presence
PPP	Point-to-Point Protocol
PTA	PPP Terminated Aggregation
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
RADIUS	Remote Access Dial In User Service
ROC	Regional Operation Center
QoS	Quality of Service
SOHO	Small Office Home Office
SVC	Switched Virtual Circuit
TR	Technical Report
UBR	Unspecified Bit Rate
UNI	User-Network Interface
VBR	Variable Bit Rate
VC	Virtual Circuit
VCC	Virtual Circuit Connection
VCI	Virtual Circuit Identifier
VPI	Virtual Path Identifier
VPTA	Virtual Path Tunneling Architecture
WAN	Wide Area Network