Technical Report
DSL Forum
TR-058

Multi-Service Architecture & Framework Requirements

September 2003

Produced by:
Architecture & Transport Working Group
Editors: Mark Elias, SBC and Sven Ooghe, Alcatel

Working Group Co-Chair: David Allan, Nortel Networks
Working Group Co-Chair: David Thorne, BT

ABSTRACT:

This documents describes the Marketing requirements for Multi-Service Architecture & Framework in the DSL Forum. These requirements include the need for network interconnection standards for DSL accesses, QoS standards, Bandwidth on Demand, QoS on demand and increased bandwidth.

Table of Figures

Table of Tables

1. SCOPE

This document discusses the requirements of a Multi-Service DSL architecture and evolution from currently deployed DSL architectures.

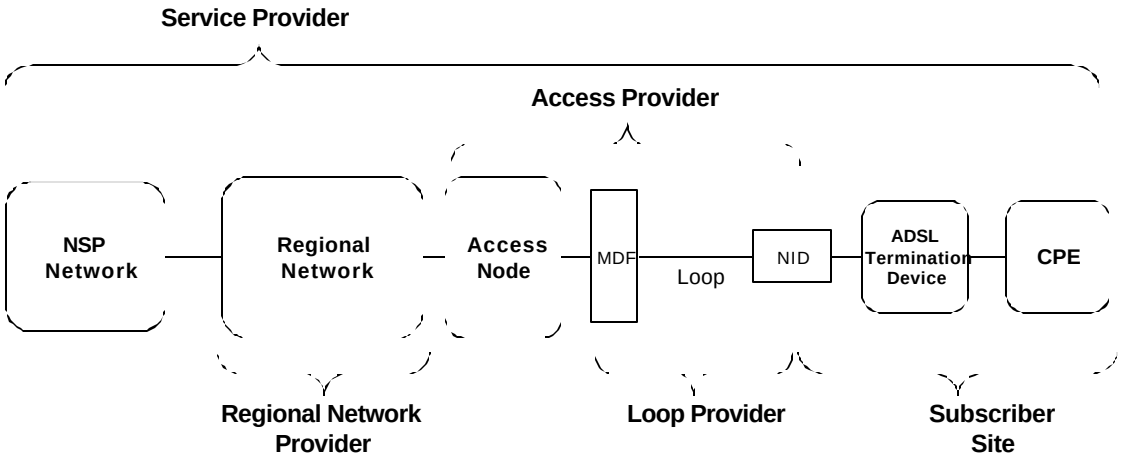

Figure 1 – Example DSL Network Components

First, the current DSL architecture is outlined; then the DSL market requirements that set a target set of capabilities and drive the migration of existing networks to a Multi-Service Architecture are discussed. Based on these drivers, a set of architectural requirements is introduced that need to be supported in a Multi-Service Architecture. These requirements include the following:

- Support for a new service model (in addition to the existing service models) and associated network interconnection standards;
- Support for new service features to be used with the new service model, including:
  - ⇨ IP-based services and QoS;
  - ⇨ Bandwidth and QoS on Demand;
  - ⇨ Distinct network and application control planes interfacing with a common data repository;
  - ⇨ Alternative network transport technologies.

The prevalent service model, where subscriber connections are delivered on a best effort basis over ATM PVCs, will continue to exist. However, the new service model will be able to support the mentioned improvements and benefits.

The new architecture will become the foundation for many new applications and services, such as:

- Interactive gaming
- Voice services
- Video on Demand
- Bandwidth on Demand via a “Turbo” button or per application
- Multicast audio and video
- Remote education

The requirements put forward in this document are intended to address the mass market, and do not preclude additional niche or custom services that could be provided using the same infrastructure. While this document does address the Application Service Provider (ASP) network and the content delivery network drivers for information purposes, it does not expect secondary standards (i.e. digital rights management, security, etc.) to be developed in this framework.

The relation of this document to companion documents describing the architecture implementation details is shown in Figure 2. The standards must satisfy the early adopter customer requirements for an unmanaged service and the basic customer requirement for a fully managed solution. The fully managed solution requires the access provider to be accountable for the customer modem, set top box (STB) or other terminals.

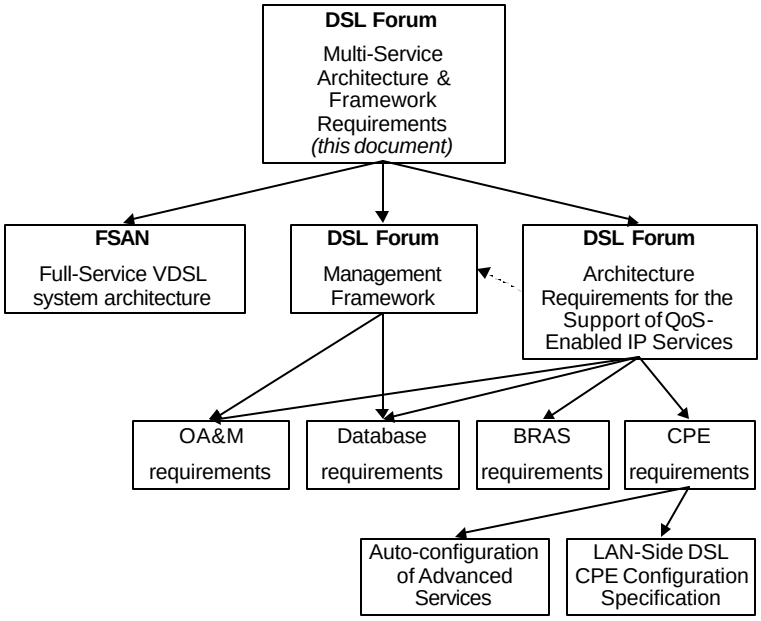

Figure 2 - Relationship to other documents

1.1. Purpose

ADSL service providers are highly interested in advancing DSL to be the preferred broadband access technology by growing their networks, increasing the value provided by those networks, and expanding the market they can address. To do this they must address several critical needs, particularly:

- The service must become more accessible to end-users and to wholesale and retail partners.
- The service must address a wider market with:
  - Variable speeds,
  - Some applications and traffic types having precedence over others,
  - Specific support for IP applications (e.g. IP-QoS and multicasting),
  - Support for new business models that can include more types of service providers, and
  - Support for these new service parameters across multiple connections to different service providers from a single DSL subscriber.
- The service must be competitive with alternative access technologies (e.g. cable).

While VDSL may also fulfill these needs, perhaps even better than ADSL, it is also important to realize that much ADSL has already been deployed, and that the current business imperatives may cause ADSL service providers to try to make more of what they already have than to try massive network upgrades. Therefore, there is also a critical need to provide a standard evolution path for the embedded base of ADSL.

The purpose of this work and the new service models is to provide a more common architecture and set of service interfaces to address these critical needs. Adhering to this architecture and to the services and service models set forth simplifies and unifies the way for all types of service providers to obtain new ADSL end-user customers, irrespective of whether they provide access to networks, applications, or content. It is noted that there might be local regulations about the architecture, for example allowing governments to request legal wiretaps to be made at any level of the network stack (cf. CALEA/FIP security requirements). These should be taken in account in the implementation of such an architecture.

1.2. Terminology of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST	This word, or the adjective "REQUIRED", means that the definition is an absolute requirement of the specification
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighted before choosing a different course.
MAY	This word, or the adjective "OPTIONAL", means that this item 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.

2. WHY THE CURRENT DSL ARCHITECTURE CAN'T PROVIDE WHAT IS NEEDED

While the current DSL architecture is well established, it will not be able to meet all expected future requirements of the new services / applications and the user-service centric architecture.

Local Conversational Applications

Applications such as two-player gaming often occur between friends that live in the same geographic area. After the gaming application has been initiated and the locality relationship has been determined there is no need for gaming traffic to traverse a distant centralized gaming server. Similar applications with typically high local traffic probabilities include fixed voice telephone conversations.

The current client-server architecture for Internet access does not explicitly provide for the necessary local switching / routing required to support local conversational services in an efficient manner.

Flexibility to address new kinds of services

The current installed base is founded on permanent virtual connections which remain static and are provisioned one time only. The typically deployed connection ADSL is one that is predominantly a best effort UBR fixed connections at a preset upstream and downstream speed that cannot meet all possible future service and interconnection requirements.

Increasing flexibility should enable Bandwidth on Demand and/or QoS on Demand in a dynamic manner rather than today's static configurations. In addition, new service activation should be automated and not require a complex or length service order process. Automatic service activation should enable timely configuration of the application, the Routing Gateway (RG), and, where applicable, end-to-end network transport with various levels of service quality.

This means the new architecture will be able to support new high bandwidth services in an efficient manner.

MUST support non-ATM network interfaces

While the current architecture adequately supports ATM based interfaces (e.g. E1/T1/E3/DS-3/STM-1/OC-3c/STM-4/OC-12) it cannot always support other network interface types such as Gigabit Ethernet, 100BaseT, and Packet over SONET (POS). These non-ATM transports MUST also be supported in the new network architecture.

MUST continue to support existing services & applications and future services and applications

While the current architecture adequately supports existing services, in many cases it may not support some future services (see reasons above) in the most desirable manner. The new architecture should be able to support both existing and future services

Service Level Management requirements

Not only is the usage of business services expected to increase, but the number of entertainment applications that require increased bandwidth or differentiated delivery treatment are also expected to increase. The existing architecture does not currently have the functionality to meet future service level management requirements. In addition the move from permanent to dynamic connections for some services means that the OSS back-office will be affected. The new architecture should be able to cope with service level management in the context of dynamic service configuration (see section 5.8).

3. APPLICATIONS DRIVING EVOLUTION

3.1. Content Delivery Networks

This is an architecture discussion for the industry at large and requires sharing of network and investment.
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 applications
- Video compression technologies continue to improve, providing better quality over lower bandwidth connections
- 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 often not an easy near term business proposition (although 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 (i.e. 50%+ decrease in download time) Enables new content services
• Content Providers:	New delivery channel for content offers

3.2. Multicast

Multicast can bring a number of advantages to both the application provider and the network provider. These benefits are related to efficiency of use of resources of various sorts:

- The processing load on the CPU of the application provider equipment decreases: this decrease will be proportional to:
  - the average number of receivers per multicast group
  - the bandwidth of the multicast stream
  - the number of multicast streams

- The bandwidth and forwarding savings in the network provider equipment is proportional to:
  - the average number of hops, i.e. the network size
  - the number of content sources
  - the average number of receivers per multicast group
  - the bandwidth of the multicast streams
  - the access link bandwidth.

Note that all of these parameters have the tendency to grow over time, which shows that the driver to use multicast will also increase over time.

Some applications that can benefit from a multicast service are:

- Bringing **broadcast-type high bandwidth multimedia** information to residential users via an access/regional network. Since terminals are multicast aware, multicast is probably the best candidate to offer this service.
- In a **Content Distribution Network** (CDN) an Origin Server copies its content to multiple Surrogate Servers that are located closer to the end-user. This communication is one-to-many.
- **Software Updates** have the same characteristics as CDNs, except that for the case of updates for end-users the number of receivers can be larger.

3.3. Quality of Service enabled applications

The evolution from high-speed Internet services to QoS-enabled applications is a key part of the network and application providers' strategy going forward. These applications necessitate predictability from the network, which in turn requires various related functions in the network:

- The ability to differentiate between various service classes at the network level, for both upstream and downstream traffic is a necessity.
- The ability to offer relative QoS for some service classes and guaranteed QoS for other service classes, depending on the needs of the application.
- The ability to enforce QoS parameters for the different services (e.g. bandwidth, latency, etc.) by allocating resources in the access, regional and core networks.
- The ability to collect statistics from the network to report on contractual guarantees.
- Since not all users are expected to concurrently use their maximum bandwidth at all times, many of the operators involved in delivering QoS-enabled services over these networks want to share network resources between different users and allocate them only if required.

- Controlling the resources within the network for those applications offered by ASPs that require some form of guaranteed QoS to ensure good perceived service behavior. Since many ASPs can be connected to the access network, the ASPs should use this access network in a controlled way. Therefore, the operator may divide the bandwidth between the applications delivered by the ASPs and perform some admission control onto its network to avoid conflicts between end users and/or applications originating from different ASPs.
- For both cases, some form of network resource control is required.
- These controls also need to include a feedback function that can inform the subscriber whether the requested bandwidth or QoS is available as requested or not and whether it will degrade other services that might be active at the same time.
- Also, high reliability in networks is growing in importance.
- The ability to bill/account for the used services

Customer applications, as identified in Table 1 and Table 2, will be the main drivers for the type of DSL access, bandwidth limitations, Bandwidth on Demand and the QoS needed to provide these applications. Residential and Business Customers requiring basic Internet access will continue to be provided the Best Effort ADSL service, while enhanced applications, such as video, interactive games, remote education, etc., require ADSL or VDSL service with additional QoS characteristics. SME and SOHO customers with requirements for large file transfers, upstream or downstream, require increased bandwidth or Bandwidth on Demand using either ADSL or SHDSL. Initially, the main devices to which new applications will be delivered are the PC and the Television but it is expected that home networking with broadband access will lead to an increase in the number of connected devices in the customer premises network (e.g. DSL gateway, gaming consoles, set-top boxes, printers, scanners, cameras, web appliances, home automation equipment, etc).

Access providers MAY also require the DSL technology, Bandwidth and QoS as an alternative to provision legacy Private line and Frame access.

TV Focused Services	Typical bandwidth (upstream)	Typical bandwidth (downstream)	Delay bound	Packet loss	On demand
Broadcast TV – e.g. MPEG2		2 - 6 Mb/s [1]	~1s	10^{-5}	Yes
High definition TV – HDTV		12 - 19 Mb/s [1]	~1s	10^{-5}	Yes
Pay Per View and NVOD – e.g. MPEG2		2 - 6 Mb/s [1]	~1s	10^{-5}	Yes
VOD – e.g. MPEG2		2 - 6 Mb/s [1]	~1s	10^{-5}	Yes
Navigator and EPG (can be locally launched and updated in non real time)		< 0.5 Mb/s	N/a	N/a	No
Picture in Picture – two MPEG2 channels		Up to 12 Mb/s [1,2]	~1s	~1%	Yes
Picture in Browser – one MPEG2		Up to 9 Mb/s [1,2]	~1s	10^{-5}	Yes
Personal Video Records PVR – replay MPEG2 file off hard disk		2 - 6 Mb/s local [1]	N/a	N/a	Yes
ITV - TV telephony features	< 64 kb/s	< 64 kb/s	<400ms (RTT)	~1%	Yes
- TV browser		Up to 3 Mb/s	N/a	N/a	Yes/No
- TV e-mail	128 - 640 kb/s	Up to 3 Mb/s	N/a	N/a	No
- TV Instant Messaging	128 - 640 kb/s	Up to 3 Mb/s	N/a	N/a	No
- TV Chat	128 - 640 kb/s	Up to 3 Mb/s	N/a	N/a	No
- TV on-screen notification		< 64 kb/s	N/a	N/a	No
- TV interactive games	128 - 640 kb/s	Up to 3 Mb/s	~10ms	10^{-5}	Yes
- TV Audio Juke Box		< 128 kb/s	~1s	<1%	Yes
Notes:					
1) video compression advancements will enable more efficient encoding (1,5 to 3 Mb/s)					
2) more efficient solutions could be available					

Table 1 - TV delivered applications

PC Focused Services	Typical bandwidth (upstream)	Typical bandwidth (downstream)	Delay bound	Packet loss	On demand
High Speed Internet Access (browsing, IM, Chat, FTP, VPN, access, etc)					
- Residential (typically asymmetric)	128 - 640 kb/s	Up to 3 Mb/s	N/a	N/a	Yes/No
- SME/SOHO (typically symmetric)	Up to 6 Mb/s	Up to 6 Mb/s	N/a	N/a	Yes/No
Server based E-Mail	as above	as above	N/a	N/a	No
Live TV on PC		300 - 750 kb/s	~1s	~1%	Yes
Video on Demand		300 - 750 kb/s	~1s	~1%	Yes/No
Video Conferencing	300 - 750 kb/s	300 - 750 kb/s	<400ms (RTT)	~1%	Yes/No
Voice/Video telephony	64 - 750 kb/s	64 - 750 kb/s	<400ms (RTT)	~1%	Yes
Interactive Games	10 - 750 kb/s	10 - 750 kb/s	~10ms	10^{-5}	Yes
Remote Education		300 - 750 kb/s	~1s	~1%	Yes/No

Table 2 - PC Delivered Applications

Definition of application – In this text "applications" are those entities listed in Table 1 and Table 2. Applications are service offerings as experienced by the end-user via a device with a user interface (e.g. audio, visual display screen, joystick, remote control) typically located on or near the customer premises.

Definition of service feature - In this text "service features" are the underlying attributes necessary to support applications. These include (but are not limited to): Type of DSL access, Bandwidth on Demand, QoS on Demand, many-to-many access.

For each application, the ideal QoS requirements are given in terms of bounds on delay and packet loss. Some values are shown as orders of magnitude. For example, "~1s" means "order of seconds". The order of magnitude is sufficient to show the differences in some of the QoS requirements for different applications. For interactive communication services, the delay bound shown is the value as proposed by [G.114]. For each application it is also indicated whether an "on demand" behavior (either Bandwidth on Demand or QoS on Demand) may be beneficial.

The listed applications will drive the adoption of new service features by access network providers, regional network providers, network service providers and application service providers. The introduction of QoS in the network can be done according to two approaches or phases:

- In a first phase, applications are given differentiated traffic treatment, thereby enabling relative QoS differentiation. This approach enables support for new applications in a relatively short timeframe. The levels of QoS offered to applications can either be statically configured, semi-dynamic (i.e. policy based) or "on demand" via Bandwidth on Demand or Relative QoS on Demand.

- A second phase would include the features outlined above, but additionally could provide guaranteed QoS to those applications for which this is beneficial. This can also be done in either a static fashion or "on demand" via Guaranteed QoS on Demand.

The terms Relative QoS and Guaranteed QoS will be described in more details in section 4.2. The individual service features will be discussed in more details in sections 5.2, 5.4 and 5.5.

4. SERVICE FEATURES REQUIREMENTS TO SUPPORT APPLICATION EVOLUTION

4.1. Service Goals

DSL services have historically been bounded by the limitations specified when the service was first established. Subscribers placed orders for service based on a set speed profile purchased for a fixed amount of money recurring on a monthly basis. As newer applications became available, the typical subscriber may or may not be able to access these new applications depending upon how their initial connection was established, the limitations of the technology, and the availability of these new applications through their existing service provider. Further, if the subscriber desired to modify their service to add more bandwidth, a new service profile had to be put into place or, in the worst case, new equipment is required in the Access Node and a new DSL termination device in the Customer Premise Network (CPN). This type of service change is not a dynamic process. It takes time to place, review, and process these service orders and involved some degree of service downtime before the subscriber was able to benefit from the increased bandwidth. Even with these new services there is no ability to prioritize traffic from different providers or applications.

These marketing requirements require an increase in the number of service configuration parameters available (such as Speed or DSL type) and make these service configuration parameters more dynamic. Aside from variable dynamic bandwidth, these new requirements include Quality of Service (QoS) and multi-application/multi-destination selection. Service Providers benefit in that they will only need to develop one set of system interfaces for any and all carriers that adopt the resultant architecture. By subscribing to these interfaces, Service Providers will now be able to develop applications that can take advantage of variable bandwidth and better than "best effort" data traffic delivery and do so in a consistent fashion from one access network to another. Subscribers will be able to realize greater potential of their broadband data connections. This means that a subscriber can still use their Internet access as it exists today; yet additional bandwidth on their DSL line can be used to deliver other applications, potentially even from multiple service providers, such as direct corporate access, video chat and video conferencing, and various content on demand, be it movies, games, software, or time-shifted television programs. Finally, these applications can be given traffic delivery characteristics (i.e. QoS treatment) according to their needs, so that business access, online gaming, and casual Internet access all share bandwidth appropriately. Both subscribers and Service Providers will be able to decide among connections, who provides the best service for a specific application, and what applications add the most value.

4.2. Service Feature Definitions

This document presents a proposal for evolving DSL deployment and interconnection. It will outline a set of requirements for a common methodology for delivering QoS-enabled applications to DSL subscribers from multiple Service Providers. These service features will become the foundation for many new applications and services. These service features and many of the applications using these service features are intended to address the mass market, and do not preclude additional niche or custom services that could be provided using the same infrastructure.Also provided is a set of architectural requirements to support the proposed new service models. Some of the highlights including:

- IP-based services and QoS
- Distinct network and application control planes interfacing with a common data repository.
- The migration of DSL to leverage newer, alternative network transport technologies

The prevalent existing service model, where subscriber connections are delivered in a best effort fashion over ATM PVCs, will continue to exist. However, this service model in its currently deployed form will not be able to support all of the improvements and benefits desired, including IP QoS, Bandwidth on Demand, and nor will service providers be able to utilize newer, alternative transport options for these legacy connections. Therefore, new service models for interconnection are also required. New and emerging service models are expected to provide the benefits as listed.

A new service model is proposed to more efficiently manage scarce IP network address resources. For Service Providers that are more interested in providing their applications (like gaming, content, etc.) rather than a network infrastructure, there will be a common public infrastructure through which addressing and network access mechanisms will be included. Application Service Providers (ASPs) will not need to manage IP addresses, nor authenticate subscriber access to the network, however they will still authorize user access to their applications in conventional ways.

In order to support these new products, the DSL service MUST be more than just a basic transport mechanism.

New architectural requirements will be needed to enable these service features. The following is a list of some of the new capabilities of these service features.

Multi-Service Architecture High Level Service Feature Requirements:

DSL Service Type

The ability to provide the customer with a DSL service that suits their needs. This could include existing (ADSL, SHDSL, VDSL) and future DSL technologies. The DSL technologies MUST include a migration framework with minimal impact to the customer.

Bandwidth on Demand:

The ability to dynamically change the effective DSL line bandwidth based on the application or destination selected. This service feature permits the subscriber to typically use a lower speed connection for functions like Internet access and to occasionally request a dynamic increase in bandwidth based on application, Service Provider, or even a "Turbo" button. Note that Bandwidth on Demand is not, by itself, used to achieve QoS (i.e. the bandwidth increase is still best effort), but may be combined with other QoS mechanisms.

Quality of Service (QoS)

Quality of Service or QoS refers to the nature of the differentiated traffic delivery service provided, as described by parameters such as achieved bandwidth, packet delay, and packet loss rates. Traditionally, the Internet has offered a Best Effort delivery service, with available bandwidth and delay characteristics dependent on instantaneous load.

There are different types of QoS:

Relative QoS : this term is used to refer to a traffic delivery service without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It is used to handle certain classes of traffic differently from other classes;

Guaranteed QoS: this term is used to refer to a traffic delivery service with certain bounds on some or all of the QoS parameters. These bounds may be hard ones, such as those encountered through such mechanisms as an ATM Call Admission Control (CAC) function or RSVP reservation. Other sets of bounds may be contractual, such as those defined in service

level agreements (SLAs) that often typically define a monetary penalty should a certain threshold be crossed or missed.

NOTE: Within this document (and hopefully all derivative documents), the generic terms "QoS" and "QoS on Demand" will be used to describe the general concept of differentiated traffic delivery implemented by means of traffic parameters, without regard to any specific parameter or bound / guarantee. Wherever possible, the qualifying adjectives "Relative" and "Guaranteed" should, at a minimum, be used when describing the needs of a particular service. Ideally, the full definition of the QoS requirements of an application or service should define the various parameters (priority, delay, jitter, etc), any boundaries and the type of boundaries (engineered or contractual) involved.

QoS on Demand: The ability for individual application sessions to request traffic delivery characteristics according to their perceived needs, and to dynamically change the desired traffic delivery service. This allows the network to treat traffic dissimilarly to and from the subscriber based on specific usage characteristics of the product or service. This will permit high priority guaranteed traffic to take precedence over other traffic destined for a specific subscriber. This may also be used to provide an optimized delivery through the Access Network, and may provide different Qualities of Service to different applications. Specifically, the term "Relative QoS on demand" is used to refer to requests to change the relative traffic delivery service, without requiring specific bounds on delay, loss and throughput.

Many-to-Many Access: The ability for multiple users using a single DSL line to access more than one Service Provider simultaneously. Additional destinations can be corporations or ASPs. As shown in Figure 11, this will permit the subscriber to maintain their current ISP relationship, yet allow other users of the same DSL service to have access to other applications that may not be available over their ISP connection.

Content Distribution: The ability to support content storage (caching) and IP multicasting at the edge of the network to reduce backbone resource requirements. This will permit efficient use of network resources without overtaxing the Service Provider connections or the Core Network.

Network Service Providers will be able to benefit from the aggregation capabilities of these new DSL Access Networks. Specifically, the architecture will also permit:

Traffic Aggregation: The ability to aggregate application-specific traffic together into logical traffic groupings (e.g. L2TP tunnels, MPLS label stacking, MPLS VPN, VLAN tagging, etc) at the V interface, and across the RBN and A10 interfaces, ensuring Layer 2 (L2) and Layer 3 (L3) scalability & efficiency.

Layer 2 traffic aggregation has previously been available by aggregating subscriber VCs into a VP permitting upstream ATM switches to switch VPs instead of individual VCs per subscriber. In the proposed architecture a new IP aware network element is deployed at the edge of the access network. This device can function as an ATM switch and continue to support this type of layer 2 aggregation.

L2TP access concentration (LAC) of PPP sessions provides further scalability benefits by combining many subscriber PPP sessions into one or more L2TP tunnels per service provider. These tunnels can be carried over ATM virtual circuits or over IP regional backbones.
The termination of protocols such as PPPoE and PPP at the edge of the network, in addition to permitting aggregation of traffic will also decrease the overall traffic volumes by reducing the number of protocol layers through conversion of end user traffic into basic IP packets.

Improved Transport: Support higher application &service related traffic volumes over more scalable and effective L2 technologies that could be used at the V interface, across the RBN and at the A10-NSP and A10-ASP interfaces. These include such technologies as 100Mbps and Gigabit Ethernet services and Packet over SONET (POS).

Simpler Provisioning: Traffic that has been aggregated into logical application-specific traffic groupings can reduce the level of per subscriber provisioning. Additionally, since subscriber traffic is now going through a centralized aggregation system, it should be easier to migrate subscribers from one ISP to another, with little or no downtime.

Differentiated Services: Up until now, almost all DSL transport has been best effort delivery at a fixed rate. To support differentiated treatment for high priority traffic the new architecture MUST support a traffic management methodology that supports both Relative and Guaranteed QoS.

Increased Access: In previous architectures, Service Providers could only reach those subscribers with whom they had a direct relationship. These new architectures permit a subscriber to connect simultaneously to multiple Service Providers for a variety of services. Service Providers no longer need to enter into complex business relationships in order to be the sole provider for all their subscribers' needs. Likewise, a Service Provider that can offer a unique service no longer needs to go through a costly acquisition process to become an end user's sole supplier – it can offer its services to the entire installed based of subscribers.

Standard Connections: Up until now, each access provider has had their own set of interfaces for Service Providers. This proposal defines common interfaces for NSPs and ASPs. This means that the Service Provider need only develop a single interface, using a common suite of protocols and signaling mechanisms, to access all of these service features from many access providers. Also, subscriber connections will be similar among Access Providers, allowing common CPE to be more widely deployed and to permit the end-user to use existing CPE when moving from one access provider to another.

Support for these new capabilities requires a new set of network management and billing interfaces. Both Service Providers and Subscribers will use these interfaces. Service Providers will be able to examine the network and see how their subscribers are provisioned. NSPs will also be provided an interface to control and troubleshoot subscriber connections.

Subscribers will be provided mechanisms for requesting these new service features and signaling their specific needs.

These service features will support applications like:

- Multicast audio and video media applications
- Video on demand applications
- Voice services
- Interactive gaming
- Remote education
- Variable bandwidth, both on demand ("Turbo" button) and by application

5. EVOLUTION IMPROVEMENT REQUIREMENTS

Evolution of DSL networks is driven by several factors: a) Business case to deploy/maintain, and 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 provides 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 by or created for their customers.
e. Current systems / networks may not adequately address providing DSL to all types of access lines that exist in a carriers network.

In general the new service features needed to support applications described in the previous section are driving the evolution towards a new architecture.

- 5.1 More bandwidth
- 5.2 Bandwidth on Demand (dynamic bandwidth)
- 5.3 Multi application / multi destination selection
- 5.4 QoS support
- 5.5 QoS on demand
- 5.6 User-Service unbundling
- 5.7 Service Management
- 5.8 Service Level Performance
- 5.9 Current DSL Access Technology
- 5.10 Security

5.1. More Bandwidth

Due to the continuously rising DSL uptake, the regional broadband network will gradually become more and more loaded with traffic over time. This trend is even more apparent, since the average bandwidth per user also increases, due to a shift towards more bandwidth hungry services. In order to anticipate this evolution, a capacity increase is required across all interfaces in the access and regional broadband network.

On the other hand, a large amount of the newly offered bandwidth hungry services typically have a relatively short-lived session duration. This means that there is no real need to permanently provision the required resources for all users. Instead, by taking statistical multiplexing into account, the network can be dimensioned in a more optimal way and intelligent QoS mechanisms can be used to control the resource usage in the network.

5.2. Bandwidth on Demand

Bandwidth on Demand results in a more or less dynamic behavior of the actual throughput over the DSL access network. This influences the QoS control mechanisms at higher layers, both for pre-configured connections as well as dynamically changing connections.

Bandwidth on Demand MUST be coordinated with static provisioning of permanent guaranteed services (e.g. virtual leased lines) to enable a coherent connection and session admission control scheme. Provisioning of the access line to the maximum sustainable bandwidth is also necessary to insure that the additional bandwidth can be made available on a dynamic basis when requested by applications or end users.

Bandwidth on Demand MUST also be coordinated with the **dynamic QoS mechanisms** (if present) such that the layer 1 throughput mechanisms are correctly integrated with the higher layer QoS mechanisms (e.g. for session based services). Specifically, in this case, the application driven approach to offer QoS on Demand may be integrated with the application driven approach to offer Bandwidth on Demand.

5.2.1. Use of Line Rates by Connection Access Control (CAC)

Connection Access Control (or CAC) uses the Minimum, Planned and Actual Line Rates as boundary conditions for traffic management. These rules follow principles that are illustrated in the figure below for the most complex case of an ADSL line with Dynamic Rate Adaptation. In many instances operators set a fixed upstream and downstream line rate which is well below the theoretical maximum. In this case a much simpler traffic management scheme exists where the planned line rate (PLR) = actual line rate (ALR). In the figure below GCR means the Guaranteed Cell Rate. This is a general term which means the guaranteed portion of the connection. In case of ATM, the GCR will be the Peak, Minimum or Sustainable Cell Rates depending on the ATM service class. For example GCR is the PCR for CBR, SCR for VBR, MCR for GFR, MDCR for UBR+. The Guaranteed Cell Rate may be generalized to a guaranteed bitrate.

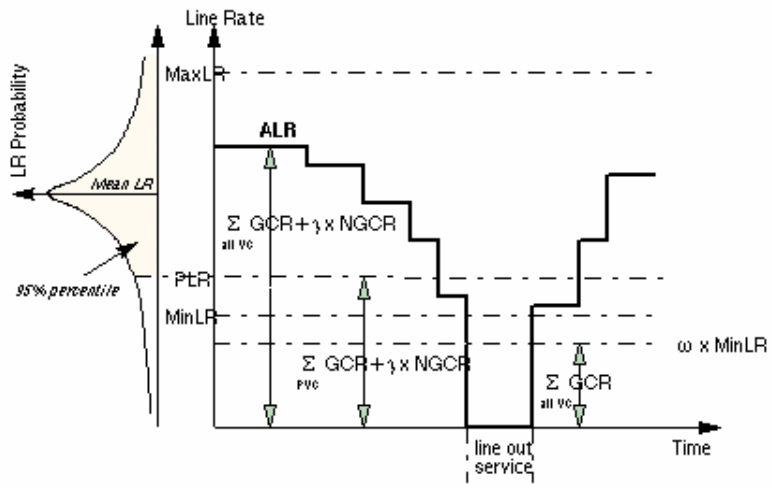

Figure 3 - Line rates, CAC and probability in rate adaptive DSL networks

5.2.1.1. Minimum Line Rate

The MinLR is the line rate that is always guaranteed when there is service. Therefore the Minimum Line Rate is used to bound the guaranteed bit rate. This makes the guaranteed bit rate invulnerable to rate adaptation.

5.2.1.2. Planned Line Rate

The PLR is the line rate that is very likely achieved. Therefore the Planned Line Rate is used to bound the total bit rate for all permanently established connections (e.g. ATM PVCs). The probability that PVCs are affected by rate adaptation is thus very small but not zero. When rate adaptation happens, the non-guaranteed bit rate portion may experience additional loss and a worse jitter.

5.2.1.3. Actual Line Rate

The ALR is the instantaneous line rate. Given the relatively short-term character of dynamically established layer 2 connections (e.g. ATM SVCs), the Actual Line Rate is used to bound the total bit rate for permanent and dynamic connections, if dynamic connections are present. When Dynamic Rate Adaptation happens, the non-guaranteed bit rate portion of the permanent and dynamic connections may experience additional loss and worse jitter. In the case of Rate Adaptation at Start-up, dynamic connections can be released because of line re-initialization. However, the QoS of permanent connections is not affected in this case.

If no dynamic connections are present, provisioning of permanent connections should not normally be restricted by the short-term ALR (which could drop below the PLR); the previous principle is sufficient in this case.

If dynamic connections are present, they may influ ence the provisioning process of permanent connections: new permanent connections should not hinder the QoS contract of existing dynamic connections (i.e. permanent connections have the same priority as dynamic connections, and this priority is based on the normal mechanisms such as service class).

5.3. Multi application / multi destination selection

There is a need for multiple users to simultaneously access different NSPs and ASPs over a common layer 2 connection. Additional destinations can be other NSPs (e.g. a corporation) or ASPs. This will permit the subscriber to maintain their current ISP relationship, yet allow these users to have access to other applications that may not be available from their current ISP connection. The subscriber should be able to select a new service or destination via a user interface.

Each service provider connection can have a fixed set of service parameters that are implemented at session startup such as bandwidth and default QoS. Each session may also take advantage of dynamic service features such as Bandwidth on Demand and QoS on Demand.

5.4. QoS support

The new architecture MUST support those QoS mechanisms that are needed to achieve the desired perceived service behavior for the customers and their applications. QoS is required for applications that require a stable behavior, i.e. for which an occasionally worse behavior cannot be accepted. In other words, QoS is required for those services where the addition of future services MUST NOT disrupt existing services.

Depending on the perceived service behavior that is to be achieved, one or more QoS features need to be supported in the network. These features include relative QoS, guaranteed QoS, QoS on demand (and related Bandwidth on Demand). The introduction of QoS in the network can be done according to two approaches or phases:

- In a first phase, relative QoS is introduced in the network. Using this feature, applications are given differentiated traffic treatment, which allows some applications to have a better behavior than others. As such, this feature allows to support a number of new applications for which best effort behavior is not sufficient. The levels of QoS offered to applications can either be statically configured or semi-dynamic (i.e. policy based). Additionally, some applications may benefit from an “on demand” behavior. This can be done achieved by supporting Bandwidth on Demand and/or Relative QoS on Demand. This approach also permits QoS to be offered without implementing complex signaling and reservations protocols across disparate equipment

- A second phase offers the features outlined above, but additionally provides guaranteed QoS to those applications for which this is beneficial. This allows differentiated traffic treatment and ensures that the QoS requirements of those applications are met. The levels of QoS can be provided in a static fashion, or “on demand”. The latter would be done via Guaranteed QoS on Demand.

Achieving end-to-end Guaranteed QoS requires the appropriate mechanisms to be in place in each of the involved networks, i.e. the access network, the Regional Broadband Network (RBN) and the core. These mechanisms may include request or reservation schemes to dynamically support technical guarantees, or simply data collection algorithms that can be coupled with reporting tools to provide measurements as to whether a contractual guarantee has been met. Clearly, in this model, the end-to-end QoS problem is only as strong as the weakest link.

Relative QoS can be used for applications that can cope with an occasionally degraded perceived service behavior or where there is a conscious decision on the part of the end user to overbook the available bandwidth of their connection. Relative QoS allows the network to give certain classes of traffic a relatively better/worse traffic delivery service than other classes. This can also be beneficial for applications that require a stable behavior, as outlined above.

The network MUST support static provisioning of permanent (very long duration) services and dynamic provisioning of services with finite session times (e.g. gaming, Video on Demand). To deliver the new dynamic service provisioning should be done in a manner which avoids adversely impacting the existing network, and which minimizes the burden on the management system. Dynamic service provisioning should be sufficiently fast to achieve smooth service activation and deactivation.

To date most DSLAMs still carry residential Internet access (UBR) as the main traffic type and (still) remain lightly loaded. New services such as Business Internet Access, VPN (Various types), and Video services are increasingly being deployed. Both require the appropriate mechanisms to be in place such that each customer gets the desired QoS behavior for the entire duration of its service(s).

Since QoS (other than best effort) can be defined part of a new session start-up, and the subscriber line can carry multiple sessions, it is important that there be a feedback mechanism in place to confirm that there is sufficient bandwidth available for delivery of all QoS enhanced traffic. For some QoS levels, this can be an offshoot of an integral CAC mechanism. For other QoS "flavors", the network control mechanisms should be able determine if the requested services exceed the capacity of the access line and inform the requestor if the requested service can be delivered as expected.

5.4.1. QoS differentiation between business and residential customers

Business customers typically require higher QoS guarantees than residential subscribers. Part of the bandwidth offered to business customers may as such be constantly available in the network, and cannot be overbooked for other customers. This can be regarded as an "always on" virtual leased line service.

On the other hand, business customer may also benefit from a best effort service, in which case its traffic will be pooled with the residential best effort traffic in network. This allows efficient use of network resources but also requires the appropriate fairness mechanism to be built in to make correct differentiation between business and residential customers. One way of doing this is to still assign a minimal guaranteed bandwidth to the best effort connection of business customers. This ensures that at times of congestion, they will still experience the minimal bandwidth and as such have a better QoS than residential customers. However, this method has the disadvantage that this guaranteed portion of the bandwidth cannot be overbooked and as such the network may run out resources to offer even this minimal guaranteed bandwidth to a large number of customers.

Another mechanism to ensure appropriate fairness is to make sure that, at times of congestion, traffic is being discarded in an intelligent way. In other words, customers requiring a higher QoS for their best effort connection should experience a smaller packet/cell loss than other customers. This in turn means that at times of congestion, the average throughput for these customers will be better than that for customers with a lower QoS.

Intelligent traffic discard mechanisms should work in combination with fair scheduling techniques such as weighted fair queuing (WFQ) or weighted round robin (WRR). This ensures that customers with the same level of QoS will get their even share of the available remaining bandwidth.

5.5. QoS on demand

Certain types of services (e.g. Video on Demand) require high guaranteed bandwidth for a reasonably short and finite period of time. These services are bandwidth hungry and if bandwidth was permanently reserved and guaranteed for every user or potential user of a given service, then the network would need to be over dimensioned several times. An alternative to over dimensioning a network to ensure Guaranteed QoS is to build in a dynamic QoS capability in the network.

To offer Guaranteed QoS on Demand requires additional intelligence capability in the network, which enables **dynamic allocation of resources** for the service at the time the service is requested, and to release these resources at the time the service is terminated. This means that in some point(s) in the network, resource admission control functionality needs to be present. Although this makes the network more complex, it avoids the static over-provisioning of guaranteed traffic and efficiently uses existing network resources. Dynamic allocation of network resources is necessary if efficient resource usage is to be achieved across a Guaranteed QoS enabled access and regional broadband network.

Other services don't require Guaranteed QoS but could still benefit from a temporary enhancement of the relative service behavior (e.g. temporarily moving from bronze to gold subscription profile for a specific service). This may also be performed by means of QoS on Demand, albeit for Relative QoS. This also requires additional intelligence capability in the network, which will dynamically reconfigure some QoS settings for the requestor and will return to the original configuration once the Relative QoS service is terminated. To some extent, this can be compared to the Bandwidth on Demand feature used to increase the best effort throughput on a DSL line.

Like the basic QoS service feature, attempts to change the QoS for a given service on demand need to also check the subscriber line and see if this change can be implemented without degrading other services. If so, then a feedback mechanism must be in place to inform the requestor about the potential service impact.

5.6. User-service unbundling

Today a number of different types of DSL unbundling exist. The most common types are copper (PHY layer) and ATM PVC L2 unbundling. This new architecture should be capable of quickly enabling new services and applications. To do this unbundling to application service providers requires a new user-service approach to unbundling at the A10-ASP interface. It is envisioned that the ASP environment will have user-level rather than network-access-level identification. To enable user level identification the ASP may interface with a common repository hosted by the Regional/Access Network Provider, providing user identification, line characteristics, and subscriber preferences.

5.7. Service Management

Service Management is defined as the set of mechanisms for provisioning new subscribers and service providers, controlling network feature delivery, advertising new services and applications and collecting the application data necessary to generate billings. These mechanisms need to interface with a well-defined data repository. In addition to standard protocols used within the network to facilitate feature delivery, a set of end user signaling protocols are needed to permit subscribers and service providers to request network features and resources.

The architecture proposed in this document clearly needs management and control systems to configure the underlying network service features or "building blocks".

To support new services and their underlying service features requires a new set of network management and control interfaces. In this working text, we use the term "network management" when talking about the provisioning of services, which typically happens at a relatively long time-scale. "Network control" refers to a real-time capability of the network to react to specific service requests. ASPs, NSP, and subscribers will all use these network control interfaces. Application Service Providers will be able to use these interfaces to agree on service levels offered by the Regional/Access Network providers. Network Service Providers will be able to examine the network and see how their subscribers are provisioned. NSPs will also be provided an interface to control and troubleshoot subscriber connections. Subscribers will use these interfaces to invoke new service features such as Bandwidth on Demand and Multi Application access. In all cases, appropriate billing records will need to be created for a wide variety of service features and services usage. These billing records will need to be created for static as well as dynamic usages.

A **"three-layer logical/functional architecture"** can be used as the base architecture to support the delivery of advanced QoS-enabled services. This approach is sufficiently generic to support a wide range of advanced services. In Figure 4 the three-layer logical architecture for support of services such as media-on-demand or conversational services is shown. It identifies the following layers:

- **The network layer:** This layer has to support predictability, reliability and QoS enforcement. The capabilities required from the Regional/Access Network Provider to support these features are described throughout section 5. To date, most DSL network diagrams, such as those referenced by [TR-025], show four (4) different providers. These include the Loop Provider, the Access Network Provider, the Regional Broadband Network Provider, and the Network (or Application) Service Provider. In this framework described in this document, the Regional and Access Network Providers are believed to be services offered by the same entity. Because of this blurring of the Access and Regional Broadband Networks, this document will now refer to this conglomeration as the Regional / Access Network Provider. As shown in Figure 4, the BRAS is positioned between the Access Network and the Regional Network. Furthermore, it may be beneficial to implement the BRAS as close to the access nodes as possible. In that case there is little or no intervening aggregation between the access nodes (DSLAM or RT) and the BRAS.

- **The "common enabling services" layer:** This layer provides a set of "common enabling services" that can be used by or shared among various applications and/or ASPs. Some of these services may be linked to the Regional/Access Network Provider (and to be provided by them in a mandatory way), while others may be provided by the NSP or ASP, depending on the business model chosen. The services are represented as "logical functional blocks" in Figure 4, without specifying how or where these services are implemented. Various network elements may be used to implement any or all of these services, depending on the specific instantiation of the three-layer architecture. It is at this layer that the common data repository used by the network and application control planes will be found.

- **The application layer:** This layer interacts with the "common enabling services" layer. For example, for conversational services, this layer could be implemented through a SIP server, while for media-on-demand one could implement a video-on-demand portal. Subscribers will directly interact with the application layer through a number of different protocols. Typically, only the ASP is assumed to be aware of the application-layer interaction.

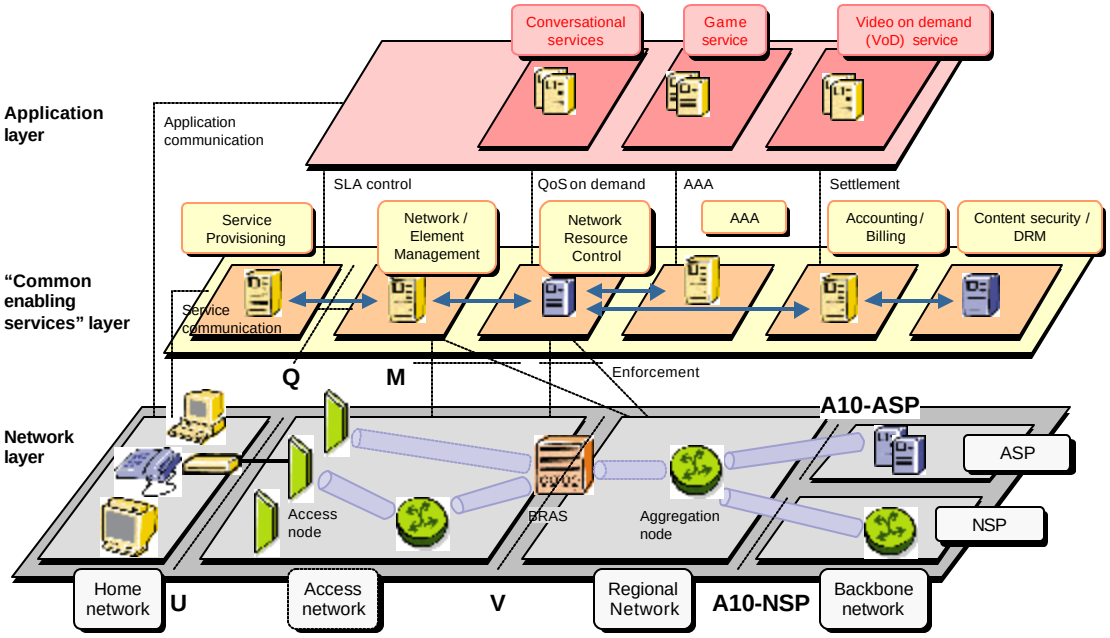

Figure 4 - Three-layer logical/functional architecture for support of advanced services

The three-layer architecture is a logical architecture, showing the mandatory and optional functions present in each layer of the architecture for advanced QoS-enabled services delivery. The architecture does not mandate that the implementation of any of these functions must be done in any specific network element in the actual network instantiation.

In the following paragraphs, the common enabling services are further discussed from the point of view of the Regional/Access Network Provider; some of these services are mandatory, while others are optional:

5.7.1. Mandatory "common enabling services" for the Regional/Access Network Provider

- **Network and element management:** This is an essential service in order to provision and monitor the network. Usually within this realm, the operator may define and provision different classes of traffic that will be available to interconnect subscribers to NSPs and ASPs. Additionally, QoS monitoring and SLA verification can be expected to become even more important.

- **Network Resource Control (NRC):** This is an essential service in order to be able to set policy rules for traffic coming from different ASPs (which in turn allows for enforcement of the business model) and to avoid conflicts in traffic going to and coming from subscribers in a generally bandwidth-constrained environment. Network Resource Control allows support for Bandwidth and/or QoS on Demand. The requests for bandwidth usage can come from multiple sources, e.g. the application layer provided by the ASP, or the subscriber.

- **Accounting/Billing**: Network Resource Control is an active part of the business enforcement process and therefore likely linked to an accounting system that will keep track of the ASP's and/or subscriber's network usage, both from a static (provisioned) and dynamic ("on demand") point of view. It is expected that some services will be offered for a fixed fee, no matter how long the service duration or how many times the service is used in a month (or other fixed timeframe), while other services will be charged on a "per hour" or "per usage" basis. The Accounting / Billing system needs to be capable of capturing and reporting all these events.

- **Common Data Model:** Managing the service includes keeping track of the parameters associated with subscribers and service providers. This can be done by means of a common data model, stored in a data repository. This is a shared resource, controlled by the Regional/Access Network Provider, and accessed by ASPs, NSPs, and end users. It will contain control values used by the all these entities when offering value added services. For example, the end user's maximum sustainable line rate will be stored here and can be used to permit access to high bandwidth applications. If the end user's DSL line is not capable of a sustained bandwidth of 1Mbps, it makes no sense to permit the end user to order a streaming movie that requires 1.5Mbps. Likewise, if there are contractual relationships with one service provider that prohibit an end user from accessing certain other service providers, this will also be tracked in the data repository. Please see the text in section 5.7.3 for more examples of the types of data expected to reside in the data repository.

5.7.2. Optional "common enabling services" for the Regional/Access Network Provider

The following (non-exhaustive) list of services could be provided through either the network provider(s) or the ASPs. The implementation of these services on a given access network could obviously be different for different applications and/or ASPs:

- **Service provisioning**: At this level, the detailed service mix that an end user is subscribed to, will be provisioned. The end user can remain with best-effort service or can choose to upgrade the service package, which then will have to be reflected at the network layer. This service does not relate to application-specific service configurations but will rather make sure that there is an infrastructure that allows for easy flow-through network and element provisioning in line with the end user requirements.

- **Authentication, Authorization, and Accounting (AAA)**: Conceptually similar to AAA used for high-speed Internet access today, but some changes may be needed due to the introduction of QoS-enabled services. Given that many ASPs don't want or need to support IP addressing, the Regional Backbone or Network Access Provider will need to create the infrastructure to provide basic network connectivity, including network authentication and IP address assignment and administration.

- **Accounting and billing**: The network provider could either be accounting for the usage that ASPs are making of its infrastructure (e.g. volume based accounting) or do the billing function on behalf of some of the ASPs (e.g. content-based accounting and billing) that do not wish to engage in that process;

- **Digital Asset Management**: The network provider could choose to include content distribution nodes (e.g. for audio and/or video) in its network and may require to actively manage the content over these nodes;

- **Content integrity and security and Digital Rights Management**: This service makes sure that the content is delivered in a secure way to the end user in an acceptable way for the content owners.

- **Service Level Management**: The data collection portion of an overall service level agreement system is located at this layer. It is this data, coupled with reporting and billing mechanisms that could be used to document network performance in relation to contractual guarantees.

It is currently unsure what level of optional services network providers will commonly implement in the near future. Moreover, various ASPs may have different strategies in teaming up with network providers. Nevertheless, a number of mandatory services are tied to the network provider regardless of the business model. The most realistic approach consists in focusing initially on these services, that a network provider has to bring to deliver the QoS-enabled services. Without any doubt, the differentiation and enforcement of the new QoS-enabled services brings some new challenges; specifically, the Network Resource Control service is the crucial piece to cater to the different applications and/or ASPs and to inform the accounting process if required.

If we split the "common enabling services" layer into its mandatory and optional constituents, we can easily map a few common business models encountered today:

- The Access/Regional Network Provider limits itself to the mandatory services only (element and network management and network resource control). In this case, the ASPs will deliver all optional services described above. We assume that the Network Provider offers either L2 (e.g. ATM), PPP or IP wholesale. Therefore, the AAA server may or may not belong to the Network Provider.

- The Network Provider controls the service delivery, but still some other ASPs can be connected to this service delivery platform. This is the typical deployment in some "walled-garden" multimedia delivery projects.

- Ultimately, the goal of this architecture is to enable an Access/Regional Network Provider to deploy a flexible mix of the enabling services. This mix can be different depending on the application considered and therefore, this framework should ultimately be open to accommodate different business models applicable to different ASPs.

Many of the functionalities required (AAA, billing, resource management) are replicated in each business entity or exist in multiple layers in the architecture and in the supply chain suggesting that an element of recursion may be necessary when a service is requested. An abstract representation of this is shown in the following diagram:

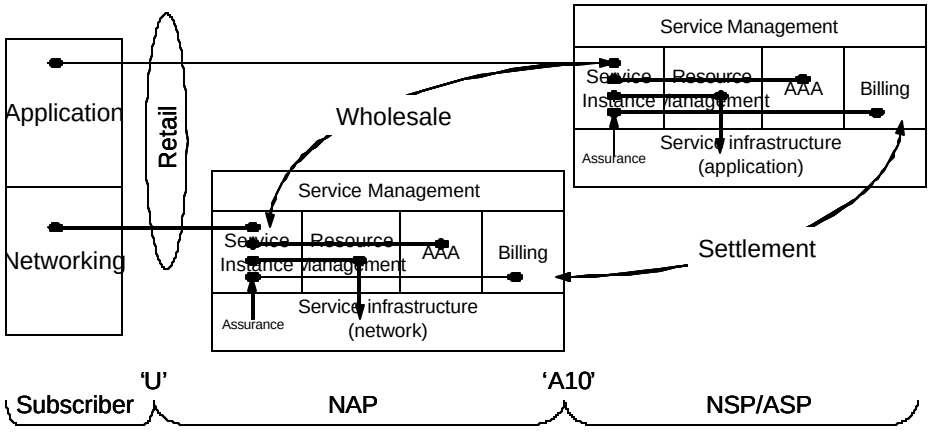

Figure 5 - Service Management Relationships

As the diagram above illustrates, there may be multiple entry points into the supply chain depending on the services that each entity offers. There is can be a retail relationship between the subscriber and the Network Provider. Likewise, the retail relationship may be between the subscriber and the Service Provider, with a corresponding wholesale relationship between the Service Provider and the Network Provider.

This triggers a number of actions (some of which may be null functions).

- The service request is authenticated and authorized.
- Resources to provide the service are allocated. The resource allocation process may recurs as the service entity obtains services from subsidiary entities in the supply chain. This is especially true when the subscriber requests a service from the Service Provider who, in turn, needs to issue a complementary request to the Network Provider.
- Service assurance information is collected from the service infrastructure, and subsidiary service entities.
- Billing information is logged for future billing and settlement.

Understanding how each service entity in the food chain will have common functional requirements for interactions for both initial service invocation, service assurance and billing and settlement will guide the evolution of the requisite interfaces.

5.7.3. End to end service provisioning

5.7.3.1. Definition of Service

- DSL services (ADSL, SHDSL, VDSL)
- Service speeds
- Usage caps

5.7.3.2. Subscribers

Because of the changes in how DSL is provisioned and managed, there are a number of new data points that MUST be tracked for each subscriber. Among these are:

- Maximum sustainable subscriber bandwidth
- Maximum number of sessions allowed
- Permitted destinations
- Default protocol
- Default destination
- Default bandwidth
- Single host or subnet needed
- Restricted subscriber (single destination only)
- Total reserved bandwidth

5.7.3.3. Service Providers

Because of the changes in how DSL is provisioned and managed, there are more details needed per Service Provider. When various choices listed for an option, these are to be considered as examples only and not a definitive list of the choices for a given option.

- Minimum bandwidth needed
- Minimum QoS characteristics
- Various protocol metrics

- Subscriber protocol (e.g. IP, PPPoE)
- Protocol (e.g. IP, L2TP, ATM)
- Authentication
- IP address assignment
- Transport
- Maximum simultaneous sessions

5.8. Service Level Management

Service Level Management is the combination of these processes/actions that make sure that the Application will experience the desired behavior, i.e. making sure the requested Service Level Agreement (SLA) is met. This is achieved by first mapping the SLA to the actual network/device specific configuration parameters, configuring the network with this information and then monitoring that the desired behavior is achieved (i.e. Service Assurance). Service Level Management is likely to be a dynamic process. This is due to the fact that the configuration-monitoring-checking process is inherently a control process with a feedback loop.

Service Level Management is intended to provide 3 levels of benefit – increasing over time:

- To provide a list of the salient network performance and operational metrics that might be used in a Service Level Objective (SLO) or Service Level Agreement (SLA).
- To provide a standard definition of such metrics so that the meaning would be common when used by various providers.
- To provide boundary condition service metrics that are driven by architectural considerations where applicable. For example, while it is NOT the intention of this document to set the SLO or SLA for Network Delay (Latency), any network that purports to support Voice over IP (VoIP) will need to have a maximum delay that is within the bounds necessary to support VoIP.

Network Performance Metrics

1. **Network Availability** - The percent of time that the Regional/Access Network is available for subscribers to connect. This metric is defined on some time basis, such as a month, a week, or a year. An SLA should also specify not the entire network but the section of the network for which the Regional/Access Network Provider is responsible. For example, the Regional/Access Network Provider is not responsible for NSP problems.
2. **Network Delay (Latency) –** The time it takes for a data packet to traverse the Regional/Access Network, from end-to-end or edge-to-edge. Latency is defined in milliseconds and can be a one-way or round-trip delay.
3. **Message Delivery** - The ability of the Regional/Access Network to transmit traffic at the negotiated speed. Some applicable measurements are packet loss. These metrics MUST have a time base as well.
4. **Network Jitter** – The variance of network latency. Jitter is defined in milliseconds.

Operational Metrics

5. **Mean Response Time** - The time it takes the Regional/Access Network Provider to respond to submitted reports of trouble
6. **Mean Time to Restore Service –** The measurement of the Regional/Access Network Provider's ability to restore service within the negotiated interval
7. **Ordering System Reliability –** The measurement of the consistent availability of ordering system.

8. **End-User Installation Guarantee –** The measurement of the Regional/Access Network Provider's ability to meet negotiated order due dates.

Service Level Management functionality MUST gather data from several key network elements. Knowing which element is dropping frames or discarding cells can dramatically reduce the time to repair a network. This data collection effort is also a key to generation of reports that are used to show whether the network has met or failed to meet contractual obligations for service delivery.

SLM for billing purposes MUST know when dynamic service activation starts and ends and MUST be associated with QoS control. Therefore it is natural to have some relationship between the SLM with the centralized intelligent controller.

5.9. Current DSL Access Technology

5.9.1. ADSL

ADSL allows the use of one existing twisted-pair local loop to provide high-bandwidth data and/or video services. It supports two-way transmission of analog voice (POTS) and digital voice (ISDN), a downstream-only digital broadband channel of up to theoretically 8 Mbps for data or video distribution, and an upstream-only digital channel of up to theoretically 640 Kbps. The rates of the digital channels depend on the physical and electrical characteristics of the loop (primarily loop length) and on the ADSL technology that is deployed.

5.9.2. SHDSL (G.991.2)

On its face SHDSL is simply a single line version of HDSL, transmitting T1 or E1 signals over a single twisted pair. However, SHDSL has the important advantage compared to HDSL that it suits the market for individual subscriber premises which are often equipped with only a single telephone line. SHDSL will be desired for any application needing symmetric access such as servers and power remote LAN users.

5.9.3. VDSL

VDSL will be asymmetric transceivers at data rates higher than ADSL but over shorter lines. While no general standards exist yet for VDSL, discussion has centered around the following downstream speeds:

12.96 Mbps	(1/4 STS-1)	4,500 feet of wire
25.82 Mbps	(1/2 STS-1)	3,000 feet of wire
51.84 Mbps	(STS-1)	1,000 feet of wire

Upstream rates fall within a suggested range from 1.6 Mbps to 2.3 Mbps. VDSL will provide the access required to satisfy customer needs for Video, VOD, and increased Bandwidth.

5.10. Security in Evolving DSL Multi-service Architectures

Security is a complex issue that does not lend itself to a list of pre- or proscriptions in providing a framework for network architects. There are, however, many threats that can be easily identified, based on a risk assessment of the network, the history of attacks against similar networks, or a combination of both. This is especially true when the network in question is attached to the public Internet and it's potential for exposing security flaws in the network to a large group of potential antagonists or automated agents.

Any network architecture that provides services to the public MUST be built to provide security functions to its users, to connected providers, and to the carrier's network itself. These security functions should prevent such known actions as denial of service, theft of service, or unauthorized access either to the network or to the information contained in various repositories within the network.

The security functions MUST balance several competing requirements:

1. Security should be controlled by the entity best able to secure the function.

   In a network with divided responsibilities, such that discussed in this recommendation, there are separate realms of responsibility. This is especially true in the area of security. Management bonding between entities is always complicated to provide and is best minimized in any architecture. In the case of security information and configuration, the additional risk of compromising quality of the security occurs whenever the information needs to cross a jurisdictional boundary and be manipulated by another entity.

2. Security methods MUST be appropriate for the risk

   a. They MUST NOT be so complex that users or providers ignore the procedures or short-circuit the methods in order to use the services.

   b. Nor should the security methods be so complex that they discourage the users from using the service.

   c. The resources required to secure the service should be appropriate to the level of risk and the value of the service.

3. The different entities do provide certain security services to each other. For example the Regional Network may provide information about the source of a connection to an NSP or ASP or the architecture of the regional network may provide a certain level of inherent security in its services (e.g. an ATM PVC has certain inherent security properties). It is clearly the responsibility of the receiver of the information to make appropriate use of this information as THEY see fit. Good security architecture does not constrain the receiver of the information to use this information that they do not control. On the other hand, the provider of the information should be able to guarantee the quality of any information they provide to the level that the have promised their partner. Examples of such a security services:

   a. if a Regional Network Provider claims that an ATM PVC will have been securely configured to reach and carry traffic only from a particular destination they are providing some assurance that their provisioning system is secure against tampering and that they can detect attempts to change the configuration or insert unauthorized traffic on the circuit when it is under their control.

b. The regional Network provider may provide protection against certain types of hostile traffic reaching the CPN. In such a case they are indicating that their network architecture, management, and signaling can support such protection and that they can detect violations.

4. The security functions MUST be flexibly defined in any architecture. The requirement that an architecture could support a security function or service is different from a requirement that it MUST. It is service providers, Regional Network or user choice to implement the security functions that they need for their services and environments.

Using the reference model in Figure 1, we can talk about some of the security questions that need to be covered in defining an architecture based on this model.

5.10.1. Security functions of the regional network

a) Security of management interfaces. This is especially true of in-band interfaces that are carried over the same facilities as user data paths or which allow the Users or ASP/NSPs to reconfigure functions on the Regional network.

b) Security functions inherent in the architecture

c) Special security risks inherent in the regional network architecture

Guidance on how these risks would be addressed (by the Regional network or by requirements of the CPN or NSP/ASP.

d) Facilities for specialized security services that Regional Network could provide to the User or NSP/ASP using the architecture

e) Security Information that the Regional Network MUST provide its partners, or that the partners MUST provide the Regional Network.

5.10.2. Security Functions of ASP/NSP

a) Security requirements expectations placed by the ASP/NSP on the Regional network or on the CPN in the architecture. What they expect of these networks.

b) The security interactions on the Network/Application Service – the transactions between CPN and NSP/ASP and the Role if any of the regional network.

c) Information that the ASP/NSP MUST have from the Regional Network to do its security functions

5.10.3. Security Functions of CPN

a) Security requirements expectations placed by the CPN on the Regional network or on the ASP/NSP in the architecture. What they expect of these networks.

b) The security interactions on the Network/Application Service – the transactions between CPN and NSP/ASP as seen by the CPN and the role if any played by the Regional Network.

c) Information that the CPN MUST have from the Regional Network to do its security functions.

6. CURRENT DSL ARCHITECTURES

6.1. Logical Reference Architecture

As noted in Section 1 above, the end-to-end DSL network consists of four providers. Of these providers, the two that this proposal most affects are the Regional Network Provider and the Access Network Provider. Historically the Regional Network has been a network of ATM switches, as shown in Figure 6. This is because the access to most Access Nodes is an ATM based interface. Some Access Networks even have their own ATM switches used to aggregate traffic from multiple Access Nodes.

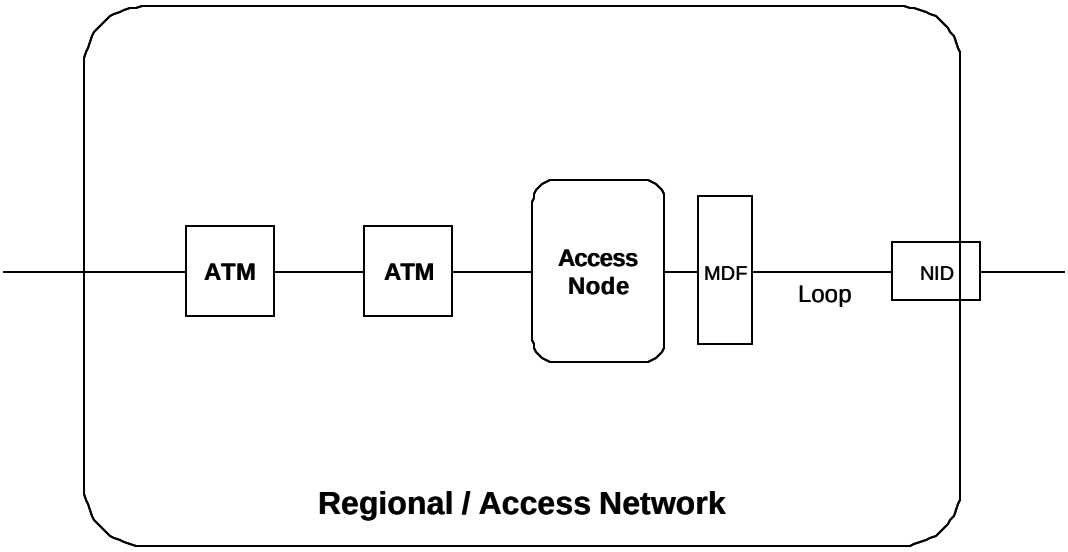

Figure 6 - ATM based Regional and Access Network Providers

Most manifestations of the [TR-025] architecture variations deployed in the field today do not use the available QoS mechanisms and just offer best effort residential Internet access services. Instead the physical DSL line rate profiles are permanently fixed within the Access Nodes and this is used to control TCP traffic peaks. This is because the "Best effort" (e.g. UBR) traffic may not be bounded or even controlled using CAC (i.e. no PCR enforcement). In this uncontrolled case there is no ATM layer congestion deference for the low priority, not guaranteed, remaining bandwidth. As a result of congestion TCP mechanisms provide flow control to adjust the "best effort" traffic throughput to the remaining bandwidth available. In some geographic regions many DSL networks were deployed before the advent of the BRAS. In addition, almost all Access Network Providers use permanently fixed DSL line speed profiles in the Access Nodes to limit upstream and downstream traffic.

Even if the Service Provider sends more traffic to meet an end-user application request the regional broadband network and / or Access Node will police the downstream traffic. Since most Internet-based applications use TCP as the transport protocol, the excess traffic discarded at the Access Node will trigger TCP back off, and this effectively controls the downstream bandwidth. As such, most Service Providers also shape downstream traffic at the subscriber-selected bandwidth. However, the desire to move to a Bandwidth on Demand model means that both the Regional and Access Networks could be vulnerable to traffic overloading. Therefore a means to control upstream and downstream traffic is needed in this new architecture.

Since the IP layer mechanisms can only be used in IP enabled network elements, this implies that upstream traffic should be controlled at the BRAS. In other words, the traffic may have crossed the DSLAM and one or more ATM switches before reaching the BRAS. As such, if guarantees are to be achieved over the ATM network, such an approach is not sufficient; some users may send more traffic in the network than they are allowed, thereby hindering other users' applications. To avoid this from happening, ATM policing mechanisms need to be deployed at the access nodes, or the network needs to be over-provisioned. This makes sure that these users cannot congest the intermediate ATM network.

Many times the physical components of the Access Nodes are daisy-chained, sharing the bandwidth of the aggregating circuit. As shown in Figure 8 in Section 6.2.1, there are numerous ways that DSL access devices can be interconnected to the first ATM switch. Historical measurements have shown that the typical DSL subscriber uses no more than a small fraction of sustained bandwidth. However, network requirements are changing as subscribers are offered more and more attractive high bandwidth applications, the average sustained bandwidth per subscriber over these "mid-mile" connections is expected to increase. As per subscriber bandwidth usage increases, the Regional Network Provider will also need to scale bandwidth and provide per application QoS on a subscriber-level basis.

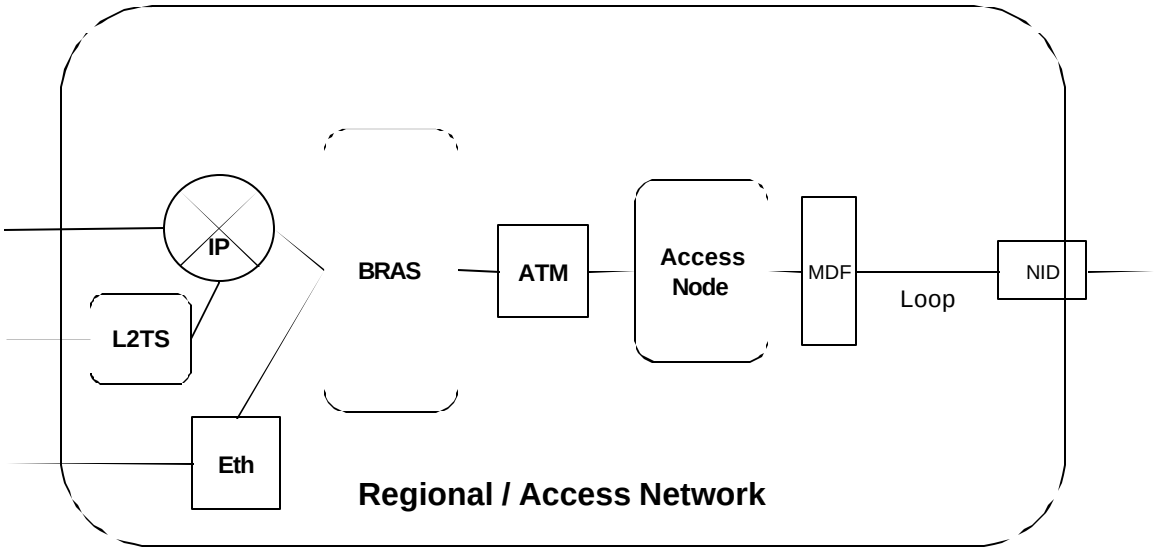

Figure 7 - IP Enabled Regional Network

As a result, other devices need to be added to the Regional Network to provide better aggregation of subscriber traffic. There are several options for doing this, most of which involve IP enabling the Regional Network as shown in Figure 7. Subscribers that use or be converted to native IP, which is a routable protocol, can be aggregated at the IP level into a Virtual LAN (VLAN) or Virtual Private Network (VPN) for handoff to their associated Service Provider.

Typical protocol usage to support PC based services

Those PC-based subscribers that use variations of the Point to Point Protocol (PPP), such as PPPoA (PPP over ATM) and PPPoE (PPP over Ethernet), can be aggregated at either the PPP or the IP layer [TR-044].

If the aggregation is done at the PPP layer, then these PPP sessions will need to be forwarded over a routable protocol such as Layer 2 Tunneling Protocol (L2TP). When the new subscriber aggregation element is functioning in this mode, it is referred to as an L2TP Access Concentrator or LAC. The other option for PPP based subscriber is to also terminate the PPP session and assign IP addresses to the subscribers. This traffic would then be collected into a VLAN or VPN as with native IP traffic. When performing PPP Termination and Aggregation (PTA), the box is typically called a Broadband Remote Access Server or BRAS.

Typical protocol usage to support TV based services

Those TV based services that use DHCP can be aggregated at the IP or ATM layer [TR-044].

The RG either broadcasts the DHCP discover message over all bridged ATM connections, or can intelligently isolate DHCP requests on a specific control channel. Such control channel is statically configured between the RG and the DHCP relay point prior to any service terminal activation. The relay point may be located at the BRAS or at a separate DHCP relay or server location. Here, the DHCP server may interact with the NSP/ASP directly to allocate an IP address, or may wish to provide a local address on the combined NAP/NSP network. This configuration requires pre-established VC connectivity between all RGs and the DHCP server.

QoS support in heterogeneous environments

These new network elements also need to be able to function as the first tier ATM aggregation device, where the Access Node is now directly connected. As such, these devices will also need to handle ATM level aggregation and switching and need to function as an adjunct to the existing ATM network. Since they are IP aware, they can also serve as the Label Edge Router (LER) that is required if the Core Network is to become Multi Protocol Label Switching (MPLS) aware. MPLS enables QoS to be offered across heterogeneous networks with a mix of ATM and non-ATM interfaces (e.g. 100BaseT, Gigabit Ethernet, DS-3, E3, OC3c/STM-1, E1, T1)

6.2. Access Network

Description

The Access Network refers to the network between the xTU-R and the xTU-C/Access Node. The protocols between these devices are well defined and this recommendation does not attempt to alter them.

6.2.1. Access Node

Description

The Access Node contains the xTU-C, which terminates the DSL signal. Physically, the xTU-C can be deployed in the central office in a DSLAM, or remotely in a remote DSLAM (RT-DSLAM), Next Generation Digital Loop Carrier (NG-DLC), or a Remote Access Multiplexer (RAM). A DSLAM hub can be used in a central office to aggregate traffic from multiple remote physical devices, and is considered logically to be a part of the Access Node.

The Access Node provides aggregation capabilities between the Access Network and the Regional Network. It is the first point in the network where traffic on multiple DSL lines will be aggregated onto a single network. Traditionally the Access Node has been primarily an ATM concentrator, mapping PVCs from the xTU-R to PVCs in the ATM core. The role of the Access Node will remain basically the same in the near term.

Various physical Access Node configurations are shown in Figure 8, with brief names for the configurations listed in Table 3.

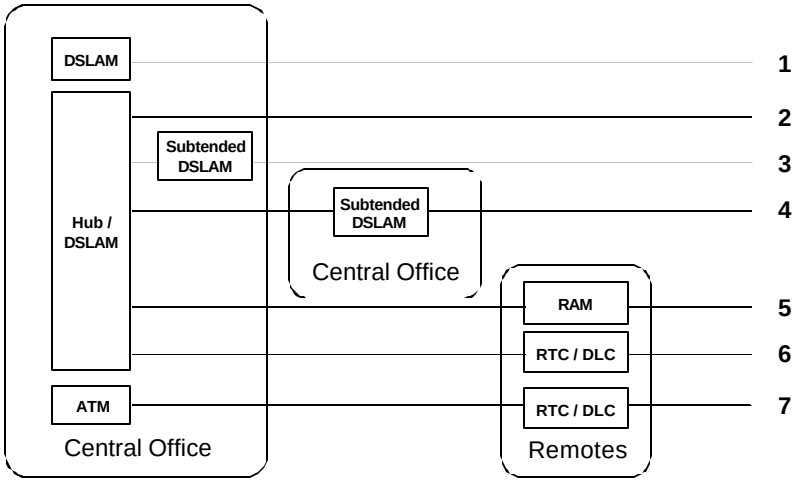

Figure 8 - Access Node Architecture Variations

Table 3 – Access Node Architecture Variation Descriptions

Reference #	Description
1	Access Node
2	Hub Access Node
3	Collocated Subtended Access Node
4	Remotely Located Subtended Access Node
5	Subtended Remote Access Node
6	Subtended DLC Located Access Node
7	Aggregated DLC Located Access Node

6.2.2. U reference point

The U reference point is defined as the interface between the Access Network and the CPN. This interface refers to the area between the CPN where the Routing Gateway (RG) (formerly the xTU-R or DSL Modem) is located and the Access Network where the Access Node is located. The U reference point includes the capabilities and protocols that cross between the Access Network and the CPN.

6.2.3. Customer Premises Network

The Customer Premises Network (CPN) is defined at its highest level as the location where the RG is located and terminates the physical DSL signal, and where the subscriber's computers and other devices are interconnected.. The initial DSL deployments focused on single user architectures where the CPN constituted a single PC connected directly to a DSL modem. This paradigm of service will continue to be supported and improved, but MUST be extended to support advanced features that go beyond the single user model. To support enhanced features (multi-user, gaming, VoIP, video, etc), the CPN MUST evolve to support the networking and management of devices and services within the home or business location.

From a network perspective, the CPN is the ultimate target of the services provided by the Service Provider (NSP or ASP). The CPN includes the networking environment and protocols that are resident in the premises. A CPN may imply coexistence of different link and physical layer technologies such as radio, power line transmission and Ethernet, but is assumed to have access to outside networks (via DSL). The terms devices and appliances refer to the collection of end terminals that can reside on the CPN, either temporarily (laptops, palm pilots, foreign devices etc.) or permanently, such as desktops, security, and climate control systems. Devices may or may not be individually addressable and reachable from other devices, inside or outside the CPN. Some devices may communicate with proxies that then can relay or translate state or configuration information for these end devices.

6.2.3.1. DSL Modem

Description

The DSL Modem contains the xTU-R and terminates both DSL and ATM. It may or may not be integrated with additional Routing functionality. If it is not integrated, it will be used in a mode that is referred to as a simple bridge modem. When integrated with the routing function, it is called the Routing Gateway or RG.

6.2.3.2. Networking Technologies

Description

The CPN will support the transparent transmission of IP packets. It is expected that the CPN will be a hybrid of technologies that may include Ethernet, phone line networking, power line networking, wireless networking, and others.

6.2.3.3. LAN Devices

Description

Devices inside the CPN that are served by the DSL Modem and RG, and connected by the various Networking Technologies are referred to as LAN Devices. These may include, but are not limited to, PCs, laptops, networked set-top boxes, and Internet Appliances.

6.2.4. T reference point

As shown in Figure 9, the T reference point defines the interworking between the DSL modem/RG and the LAN Devices. The other major functional requirement placed on the T reference point includes identifying and supporting "QoS flows" as defined in sections 5.4 and 5.5. The primary goal of this interface is to facilitate seamless transmission of IP packets in both a best effort approach as well as in a QoS enabled approach. QoS can be enforced by maintaining predefined QoS behaviours (Diffserv) or via QoS on Demand using a signalling mechanism (e.g. ATM SVCs, RSVP in Intserv,…), such as dynamically changing the desired traffic delivery service according to the perceived needs of individual application sessions.

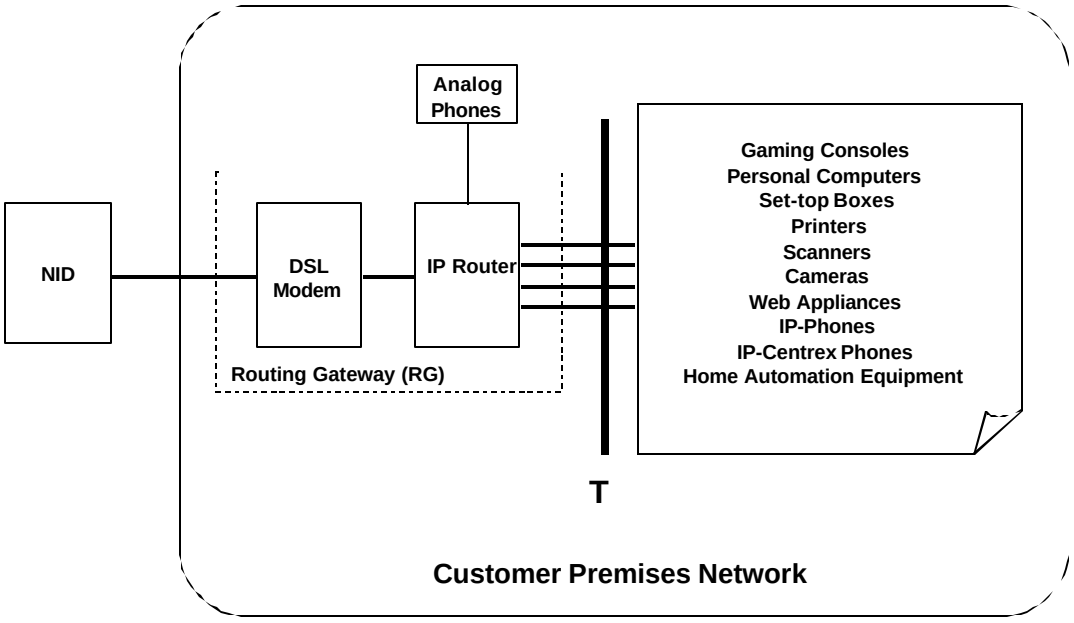

Figure 9 - T reference point

Figure 9 also shows a link with one or more analog phones. This would be the case for an Integrated Access Device (IAD) offering derived voice. There are two possibilities to offer packetized voice to the access network:

- The packetized voice traffic is sent as IP packets towards the BRAS. In this case, the Routing Gateway will handle voice packets together with data traffic;

- The packetized voice traffic is sent as voice over AAL2 towards a Voice Gateway. In this case, the voice traffic will be sent on a dedicated PVC, which is different from the PVC(s) used for connectivity towards the BRAS.

7. SERVICE PROVIDER INTERCONNECTION MODELS

Generally, services over a DSL access-based broadband network will be provided and supported by a number of different operational organizations. These organizations may be part of one company or more than one company. Leaving commercial issues aside, it is necessary to have a clear idea of the roles of the different organizations and how the functionality of equipment, network management, and test equipment can support their ability to discharge their roles for the benefit of the end customers. In order to provide a baseline with which to contrast, this document provides a common architectural view of DSL architecture in Figure 10.

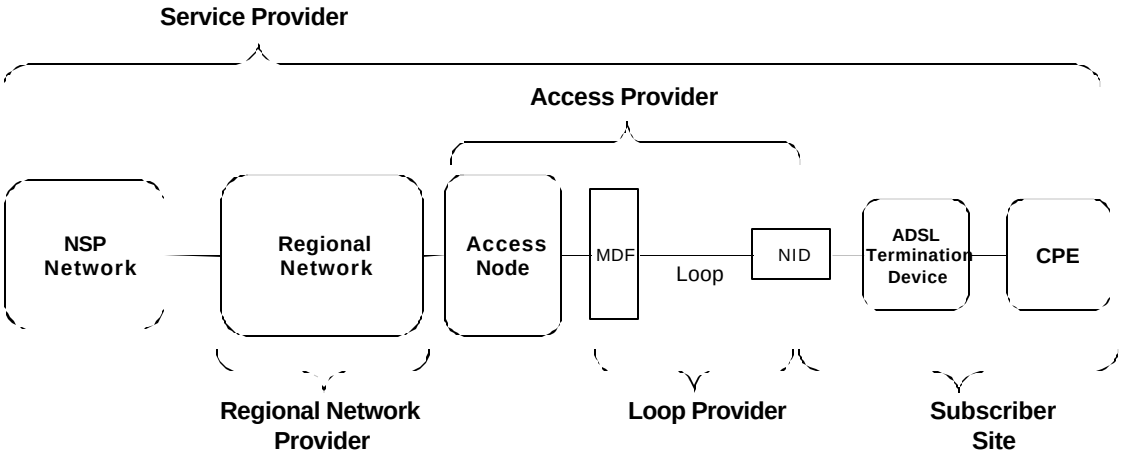

Figure 10 - DSL Network Components (Voice and application components not shown for clarity)

Boxes in the figures represent functional entities – networks and logical components rather than physical elements.

This traditional architecture is centered on providing transport services to a line or a loop. It is desired, however, to be able to provide services that are user-specific. Additionally, more than one subscriber can be present at the same premises and share a single loop. There is a need, therefore, to describe a slightly more complex situation, and hiding the common complexity shared with Figure 10, this description is provided in Figure 11 below. Note that the figure shows many-to-many access through a common Regional/Access network. It is used to simultaneously provide an Application Service$_1$ between an ASP Network$_1$ and User$_1$ at the same time and over the same U interface as it supports a Network Service$_2$ between NSP Network$_2$ and User$_2$.

This service provider interconnection model provides an additional benefit for ASPs. It allows them to be able to aggregate the users from several different NSPs, thereby possibly enlarging their customer base.

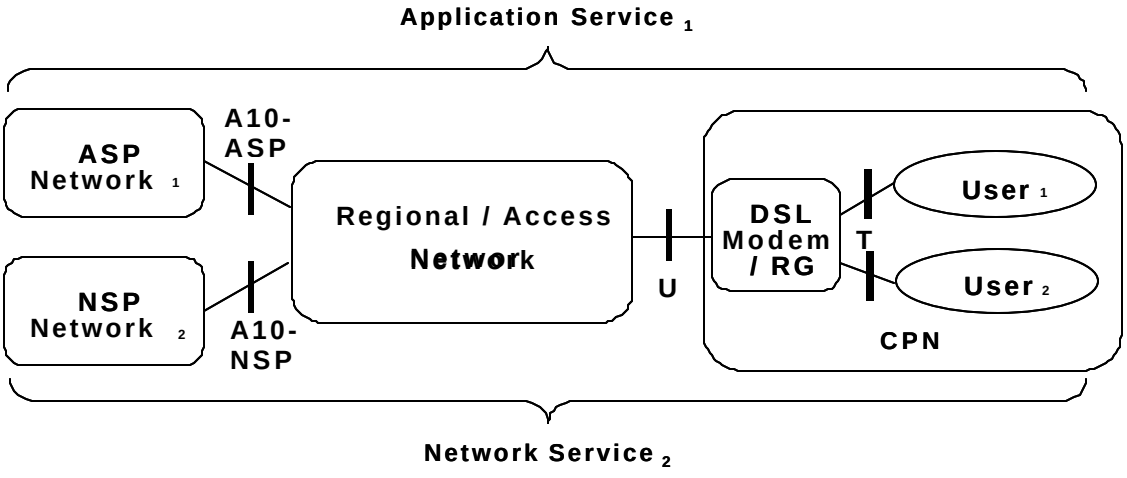

Figure 11 - Many-to-Many Access

It is of paramount importance that there is a sustainable business model in which the new applications can benefit from a predictable network. Indeed, if the Regional/Access Network Provider is to expect no service uptake increase for a substantial implementation effort for these services, it is unreasonable to expect that these providers will offer something better than a best-effort service. In return, a predictable network will enable the various ASPs to provide more advanced applications and drive up the service uptake from end users. Therefore, in summary, QoS-enabled services have to be differentiated and enforced by application requirements but, more importantly, through explicit business-to-business agreements (i.e. an operator can be expected to charge more for this premium quality service than for best-effort services).

The figures show the key components of a DSL access-based broadband network that can be provided by a single organization or several organizations. In the case of several providing organizations, the role of these various providers is indicated below:

The Network Service Provider (NSP):

- Includes Internet Service Providers (ISPs) and Corporate Service Providers (CSPs)
- Is responsible for overall service assurance
- May provide CPE, or software to run on customer-owned CPE, to support a given service
- Provides the customer contact point for any and all customer related problems related to the provision of this service
- Authenticates access and provides and manages the IP address to the subscribers
- Optionally provides a centralized server farm to be used by one or more ASPs (see next)

The Application Service Provider (ASP):

- Provides application services to the application subscriber (gaming, video, content on demand, IP Telephony, etc.)
- May wholesale services (AAA - authentication, authorization, accounting), connectivity, multicast replication etc.) from the Regional/Access Network Provider to complete service offerings and take advantage of the Regional/Access Network Provider network build out
- Is responsible for service assurance relating to this application service (although instrumentation of service assurance may be in collaboration with one or more Regional/Access Network Providers)
- Responsible for providing to subscribers additional software or CPE which specific services may need.
- Provides the subscriber contact point for all subscriber problems related to the provision of specific service applications and any related subscriber software
- Has minimal operational dependencies on the Regional/Access Network Provider from whom the ASP obtains services, e.g. does not provide or manage the IP addresses of subscribers, may employ user based AAA models etc.

The Loop Provider:

- Provides a metallic loop from the Access Network equipment to the customer's premises
- Is responsible for the integrity of the metallic loop and its repair
- May also provide the Access Network Provider aggregated access to remotely deployed DSL equipment owned, operated, and maintained by the Loop Provider

The Access Network Provider:

- Provides digital connectivity to the customer via the metallic Loop
- Is responsible for the performance and repair of the access transmission equipment

The Regional Network Provider:

- Provides appropriate connectivity between the Access Network and the NSPs and ASPs
- Is responsible for Regional Network performance and repair

7.1. Application Service Provider Network

7.1.1. Description of the ASP network

The Application Service Provider (ASP) is defined as a Service Provider that utilizes a common infrastructure provided by the Regional/Access Network and an IP address assigned and managed by the Regional or Access Network Provider. This is a new application of DSL service. The Regional or Access Network Provider owns and procures addresses that they, in turn, allocate to the subscribers. ASPs then use this common infrastructure in order to provide application or network services to those subscribers. For example, an ASP may offer gaming, Video on Demand, or even filtered Internet access, or access to VPNs via IPsec or some other IP-tunneling method. The ASP service may be subscriber-specific, or communal when an address is shared using Network Address Port Translation (NAPT) throughout a Customer Premises Network (CPN). It is envisioned that the ASP environment will have user-level rather than network-access-level identification and that a common repository will assist in providing user identification and preferences [TR-046]. Logical elements used by ASPs typically include routers, application servers, and directory servers. The relationship between the ASP Network, the A10-ASP interface, and the Regional Network is shown in Figure 11.

7.1.2. Capabilities of the ASP network

The capabilities of the ASP should include but are not limited to the following:

- Authenticating users at the CPN
- Assignment of user profile or preference data
- Assignment of QoS to service traffic
- Customer service and troubleshooting of network access and application-specific problems
- Ability to determine traffic usage for accounting purposes and billing

The following mechanisms MUST be available to the ASP:

- ASP administered mechanisms to identify subscribers (operationally decoupled from the NSP)
- Mechanisms to bind subscribers to ASP access points for the duration of service delivery. (e.g. association of subscriber identity with the subscriber's assigned IP address (by the Regional/Access Network Provider))
- Mechanisms to collect usage information, generate billing and perform settlement with Regional/Access Network Providers for services obtained as part of offering application services to subscribers.

7.2. Network Service Provider Network

7.2.1. Description of the NSP network

The Network Service Provider (NSP) is defined as a Service Provider that provides addressing and connectivity to an Internet Protocol (IP) network. This is the typical application of DSL service today. The NSP owns and procures addresses that they, in turn, allocate individually or in blocks to their subscribers. The subscribers are typically located in Customer Premises Networks (CPNs). The NSP service may be subscriber-specific, or communal when an address is shared using NAPT throughout a CPN. This relationship among the NSP, the A10-NSP reference point, and Regional/Access Network is shown in Figure 11. NSPs typically provide access to the Internet, but may provide access to a walled garden, VPN, or some other closed group or controlled access services. For example L2TP and IP VPNs are typical arrangements at the A10-NSP reference point.

7.2.2. Capabilities of the NSP Network

The capabilities of the NSP should include but are not limited to the following:

- Authenticating network access between the CPN and the NSP network
- Assignment of network addresses and IP filters
- Assignment of traffic engineering parameters
- Customer service and troubleshooting of network access problems

Optionally, the NSP may offer a centralized server farm to be used by one or more ASPs. This has the advantage of allowing central environmental control of these servers by the NSP. It may also provide the ASPs the possibility of putting their content closer to their subscribers. This may be beneficial for the perceived service behavior (e.g. reducing traffic delay for content retrieval).

7.3. Regional/Access Network Provider Network

7.3.1. Description of the Regional / Access Network

The Regional and Access Network are used to aggregate subscriber traffic and provide routing or forwarding of this traffic at various levels. Traditionally Access Network Providers have offered layer 2 connections such as ATM PVCs from DSLAMs and Remote Terminals (RTs) with little or no aggregation. When aggregation has been offered, it has usually been in the form of ATM PVPs or L2TP tunnels offered by the Regional Network Provider. These models were not designed to offer the dynamicity of bandwidth and/or QoS that is desired by this framework.

In order to provide the new service features outlined in this framework, the roles of the Regional and Access Network Providers need to change. In addition to their traditional roles, which need to be preserved to provide service to legacy service providers and subscribers, these networks must evolve. In fact, this framework now views this as a combined network, since these changes must be coordinated between both networks.

7.3.2. Capabilities of the Regional / Access Network

In addition to supporting legacy connections, the capabilities of the Regional / Access Networks should include, but are not limited to, the following:

- Access to the full sustainable bandwidth of the DSL Subscribers loop

- Ability to control or limit subscriber bandwidth
- Ability to dynamically change service delivery parameters such as bandwidth and packet precedence
- Common interfaces for ASPs and NSPs
- Aggregation of subscriber traffic to different service providers (via such mechanisms as PPP/PPPoE termination, PPP over L2TP, IP bridging (RFC2684/1483), ATM PVCs, IP VPNs, and VLANs)
- Ability to permit or deny subscriber access to various service providers
- Suitable transport options at the service provider interfaces (such as P acket over SONET (POS) and Gigabit Ethernet)
- IP address allocation and network authentication for subscribers that desire to connect to ASPs
- Data collection capabilities sufficient to support billing for new service features and to provide statistics necessary for service level management reporting

8. NETWORK INTERFACE DESCRIPTIONS

The following reference model is suggested as a baseline for multimedia service delivery. The major addition is the concept of a Controller function, which provides the intelligence to facilitate the delivery of the services. Such a controller (e.g. media gateway controller, back-office server) would interact with the Access/Regional Network by means of some sort of control interface.. The control interface can cross various reference points in the architecture, such as the .U, V or A10 reference points. A general architecture is one that considers the control functions and transport functions independent of each other. The details of such a function and its relation to network management is outside the scope of this document.

The reference model suggests that ADSL end users can select amongst several A10 reference points for different services or applications. Specifically, it may be possible that the A10 reference point to be used for a multimedia flow is resolved only at the time of the service grant.

The Controller function should be able to generate messages (primitives) across the U reference point to the Routing Gateway (RG) and/or the customer premises equipment. A controller entity must have the capability to distinguish individual U reference instances, and should also be able to address multiple users or service invocation at the same U interface.

The Controller function could exchange certain primitives with the Access Node. It is expected that the Access/Regional Network will provide only transport functions, and the mechanics to deliver multimedia flows will be based on standard protocols / signaling schemes wherever possible.

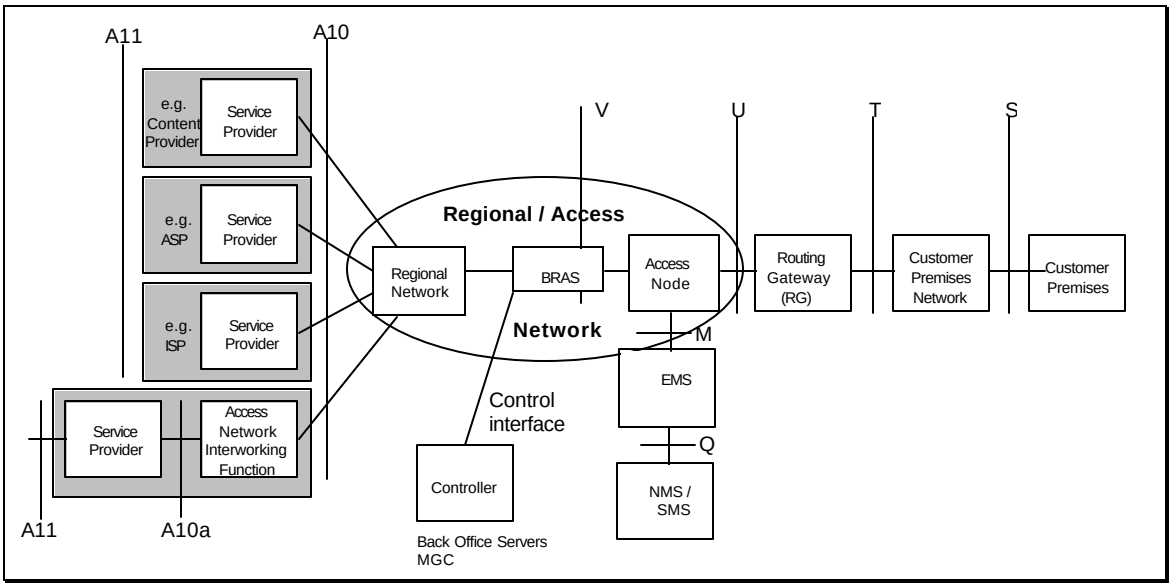

Figure 12 - Multi Service Reference Model

8.1. Requirements at the S and T reference point

The T Interface defines the interworking between the DSL modem/Routing Gateway and other CPE in the Customer Premises Network (CPN). The requirements for new vertical services over DSL require the addition of a Routing Gateway as the intermediate point between the DSL modem and the LAN Devices. The primary goal of this interface is to facilitate seamless transmission of IP packets in both a best effort approach as well as in a QoS enabled approach. QoS can be enforced by maintaining predefined QoS behaviors or via QoS on Demand through a signaling mechanism. The DSL modem and Routing Gateway may or may not be a single device.

It is assumed that real time multimedia services will coexist with pre-configured services at these reference points. Real time multimedia services MUST coexist with provisioned services. The Customer Premise MUST be capable of upgrading the service portfolio from provisioned services to real time multimedia services. This requirement addresses backward compatibility to the present mode of operation.

The reference model MUST allow each instance of the service invocation to be individually distinguished by the controller and to be allocated with a distinct session and bearer. This capability will allow several real time multimedia services to operate simultaneously, each controlled separately.

The S and T reference points MAY overlap in certain RG or customer equipment implementation.

8.2. Requirements at the U reference point

The U Interface is located at the subscriber premise between the Access Node and the Network DSL Termination Device (Routing Gateway or RG). Control information and multimedia flows SHOULD be distinguished flows, allowing segregation to different destinations (i.e. controllers and Service/Content providers). Distinct flows at the U reference point SHOULD be addressed individually for the allocation of bearer service. Multimedia flows at the U reference point MAY be addressed to multiple instances of A10 reference points. DSL specific attributes SHOULD support the different bearer qualities needed for the multimedia flow (e.g. allocating streams to fast and Interleaved channels). One control flow, across the U reference point, SHOULD be capable to address multiple end-points at the S or T reference points.

8.3. Requirements at the V reference point

No special requirements are identified at the V reference point; as such it can be considered as a null interface within this framework. This is because this document views the Regional and Access Networks as a single entity, even though it is possible that subordinate documents may desire to separate these networks back into their component parts. It is assumed that standard bearer signaling and protocol stacks will be utilized across the V reference point for setting on-demand bearer to the multimedia flows.. Bearer and Transport services invoked across the V reference point SHOULD be associated with the real time multimedia services across the U reference point.

8.4. Requirements at the A10 reference point

The A10 reference point serves as the sink for the multimedia service or may serve as a gateway function for service delivery. The A10 reference point SHOULD support standard bearer and transport flows and individual multimedia services SHOULD be able to correlate with distinct end points.. A single instance of the A10 reference point MAY serve multiple instances of U and V reference points (i.e. point of aggregation or statistical sharing). A controller MAY establish control information flow across the A10 reference point, for the purpose of setting the multimedia service.

8.4.1. A10-ASP Interface

This reference point is between the Regional/Access Network and the ASP's Points of Presence (POPs). This interface will consist of a routed IP interface, which may be transported over Fast Ethernet, Gigabit Ethernet, and Packet over SONET (POS), or some other IP interface. The ASP has the end-to-end Service responsibility to the customer for their specific application and is viewed as the "Retailer" of the specific application. Trouble reports for the specific application go directly to the ASP. This interface is a new interface not described in [TR-025].

8.4.2. A10-NSP Interface

This reference point is between the Regional/Access Network and the NSP's POPs. The interfaces could be ATM, Fast Ethernet, Gigabit Ethernet, or Packet over SONET (POS). In the case of ATM, multiple sessions may be multiplexed over a single VCC at this interface. Typically, the NSP has the end-to-end service responsibility to the customer and is viewed as the "Retailer" of the service. As the retailer of the DSL service, trouble reports, and other issues from the subscriber are typically addressed to the NSP. Handoff protocols could include ATM VP/VCs, L2TP tunnels, and routed protocols using IP-VPNs.

8.5. Control interface

The control interface is designed to carry control information to and from the network elements in the Regional / Access Network. The physical, transport and control stacks SHOULD all be based on standard protocols. The information exchanged using the control interface should interact with the end-points and with network element that needs to commit the bearer to the service. The controller may be administered by an independent business entity (which doesn't own other network elements); this requirement implies that security and AAA SHOULD be supported to validate the user requesting a specific service. It also implies that the identification of individual U reference points should be flexible to accommodate several business arrangements.

9. DEFINITIONS

AAA	Authentication, Authorization, and Accounting
AAL5	ATM Adaptation Layer 5
ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding
API	Application Program Interface
ARP	Address Resolution Protocol
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
ATMARP	ATM Address Resolution Protocol
ATMF	ATM Forum
B-NT	Broadband Network Termination
BE	Best Effort
BGP	Border Gateway Protocol
BoD	Bandwidth on Demand
BRAS	Broadband Remote Access Server
CBR	Constant Bit Rate
CO	Central Office
COPS	Common Open Policy Service
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSP	Corporate Service Provider
DHCP	Dynamic Host Configuration Protocol
Diffserv	Differentiate Services
DLC	Digital Loop Carrier
DNS	Domain Name Service
DS1	Digital Signal level 1 (1.544 Mbps)
DSCP	Differentiated Services (Diffserv) Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EF	Expedited Forwarding
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
GFR	Guaranteed Frame Rate
iBGP	internal Border Gateway Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Secure Internet Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Technical
L2TP	Layer 2 Tunneling Protocol
L2TS	Layer 2 Tunnel Switch
L2oMPLS	Layer 2 over MPLS
LAC	Layer 2 Access Concentrator
LAN	Local Area Network
LD	Long Distance
LDAP	Lightweight Directory Access Protocol
LER	Label Edge Router
LLC	Logical Link Control
LSP	Label Switched Path
LNS	L2TP Network Server
MAC	Medium Access Control

MARS	Multicast Address Resolution Server
MASS	Multi-Application Selection Service
MBGP	Multicast Boarder Gateway Protocol
MPEG	Motion Pictures Expert Group
MPLS	Multi-Protocol Label Switching
MS/MD	Multi Session / Multi Destination Service
MTU	Message Transfer Unit
NAPT	Network Address Port Translation
NG-DLC	Next Generation Digital Loop Carrier
NHRP	Next Hop Resolution Protocol
NSP	Network Service Provider
OC3	Optical Carrier 3
OSPF	Open Shortest Path First
PC	Personal Computer
PHB	Per Hop Behaviour
PHY	Physical Layer
POP	Point of Presence
POS	Packet over SONET
PPP	Point-to-Point Protocol
PPPoA	Point-to-point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PTA	PPP Terminated Aggregation
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAM	Remote Access Multiplexer
RFC	Request For Comments
RG	Routing Gateway
RRP	Resource Request Protocol
RSVP	ReSource reserVation Protocol
RT-DSLAM	Remote Digital Subscriber Line Access Multiplexer
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLO	Service Level Objective
SNAG	Service Network Architecture Group (DSL Forum)
SONET	Synchronous Optical Network
SVC	Switched Virtual Circuit
TCP	Transmission Control Protocol
TE	Traffic Engineering
TR	Technical Report (DSL Forum)
TV	Television
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
VBR-nrt	Variable Bit Rate - non-Real Time
VBR-rt	Variable Bit Rate - Real Time
VC	Virtual Circuit
VCC	Virtual Circuit Connection
VLAN	Virtual Local Area Network
VoD	Video on Demand
VP	Virtual Path
VPC	Virtual Path Connection
VPN	Virtual Private Network
VoBB	Voice over Broadband
VoIP	Voice over Internet Protocol
WFQ	Weighted Fair Queuing
xTU-C	xDSL Termination Unit - Central Office (at Access Network end)
xTU-R	xDSL Termination Unit - Remote (at customer end)

10. REFERENCES

[TR-025] "Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL", DSL Forum Technical Report, TR-025, December 1999;

[TR-044] "Auto-Configuration for Basic Internet (IP-based) Services", DSL Forum Technical Report, TR-044, December 2001;

[TR-046] "Auto-Configuration Architecture & Framework", DSL Forum Technical Report, TR-046, February 2002;

[G.114] International Telecommunications Union (ITU). ITU-T-G.114, International telephone connections and circuits – General Recommendations on the transmission quality for an entire international telephone connection, May 2000.