DSL FORUM

TECHNICAL REPORT

TR-144

Broadband Multi-Service Architecture & Framework Requirements

Issue Number: 1.00
Issue Date: August 2007

© 2007 DSL Forum. All rights reserved.

Notice:

The DSL Forum is a non-profit corporation organized to create guidelines for DSL network system development and deployment. This Technical Report has been approved by members of the Forum. This document is not binding on the DSL Forum, any of its members, or any developer or service provider. This document is subject to change, but only with approval of members of the Forum.

This publication may incorporate intellectual property. The DSL Forum encourages but does not require declaration of such intellectual property. For a list of declarations made by DSL Forum member companies, please see www.dslforum.org.

©2007 Digital Subscriber Line Forum. All Rights Reserved.

DSL Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only. The text of this notice must be included in all copies.

Notwithstanding anything to the contrary, the DSL Forum makes no representation or warranty, expressed or implied, concerning this publication, its contents or the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by the DSL Forum as a result of reliance upon any information contained in this publication. The DSL Forum does not assume any responsibility to update or correct any information in this publication.

Version History

Version Number	Version Date	Version Editor	Changes
Issue 1.0	August 2007	Anna Cui, AT&T	Original

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

Editor	Anna Cui	AT&T	zc1294@att.com
Architecture and Transport WG Chairs	David Allan David Thorne	Nortel Networks BT	

© 2007 DSL Forum. All rights reserved.

TABLE OF CONTENTS

© 2007 DSL Forum. All rights reserved.

TABLE OF FIGURES

Summary:

This document describes the DSL Forum business requirements for a Multi-Service Architecture & Framework. These requirements include the need for network interconnection standards for broadband access, QoS support and Bandwidth on demand, increased overall bandwidth and higher network reliability and availability. The requirements also include support for a broader range of market segments including both business and residential markets, wholesale and retail, and finally a better user experience.

1 SCOPE

1.1 Background

TR-058, published in September 2003, addressed the marketing requirements of a Multi-Service DSL architecture and evolution from then deployed DSL architectures. With the advent of TR-059 and TR-101 based architectures, the regional access network has become packet aware. TR-059 overlays IP awareness on top of an existing legacy ATM access network. TR-101 is the next evolutionary step where the access network is upgraded to support Ethernet transport and switching capabilities. TR-101, which provides the architectural/topological models and requirements to support the marketing requirements in TR-058, was deliberately limited in scope and only focused on the migration of ATM based DSL aggregation to Ethernet based aggregation and point to POP connections to address the urgent market need. Finally, ongoing work (e.g. WT-134) is addressing the need for a Policy Control Framework on top of the network layer, and the linkage to the application layer and service-oriented architectures. In parallel with DSL forum architectural evolution, we have seen several generic NGN architectures being developed in other standardization organizations (ITU-T NGN and ETSI NGN). This requirements document will strive to align the network architecture requirements with the other standardization efforts.

1.2 Scope of TR-144

The scope of TR-058 is extended from a DSL centric architecture to a generic converged Broadband Multi-Service network architecture. This converged broadband architecture is required to support a broader range of services, including both emerging and legacy services, with an extension to the degree of nomadism support; as well as a broader range of market segments in addition to the current residential and retail focused view. In particular the needs of the business and wholesale markets will be addressed. In addition, some services, like IPTV, require end to end Quality of Service, whereas business VPN services may drive the need for higher network reliability and availability. While many of the applications and services described in TR-058 are still valid and must continue to be supported, new applications and services also drive the need for a new architecture.

The Broadband Multi-Service network architecture defined in this document encompasses the Transport Layer including transport resource and admission control objects that participate in the delivery of transport functionality to the access network, aggregation network, and edge routing. The Home network is in the scope of this document to the extent needed to deliver the end to end services described in this document.

This document presents an overall architectural framework and business requirements for this converged Broadband Multi-Service architecture.

1.3 Relationship to Other TRs and Working Texts (WTs)

The relationship of this document to companion documents which will describe the architecture implementation details is shown in Figure 1.

© 2007 DSL Forum. All rights reserved.

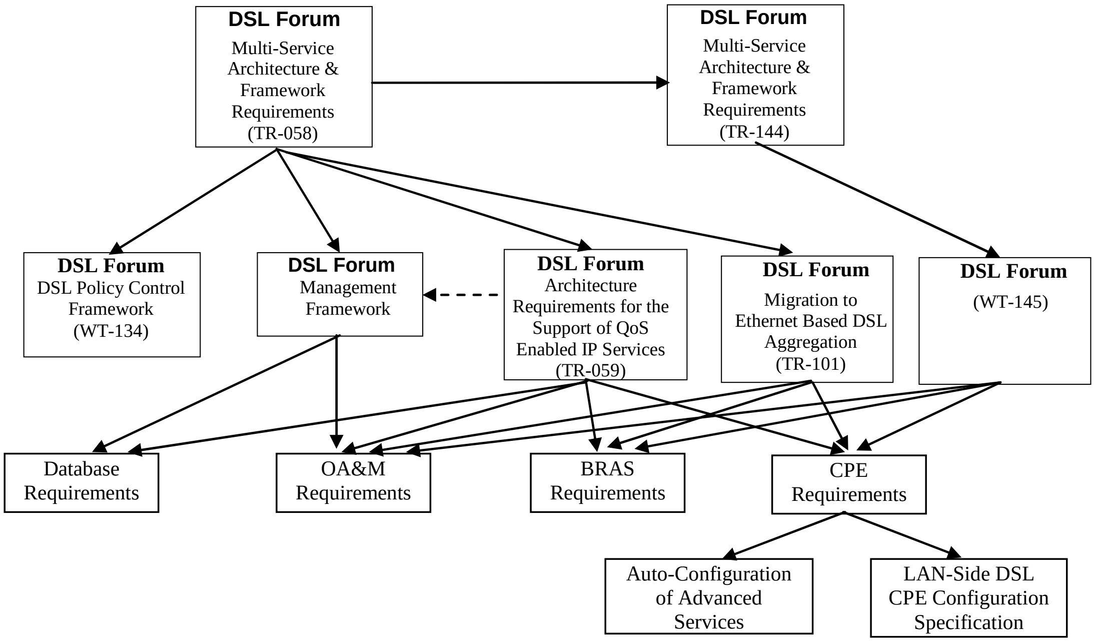

DSL Forum
Multi-Service Architecture & Framework Requirements (TR-058)
DSL Forum
Multi-Service Architecture & Framework Requirements (TR-144)
DSL Forum
DSL Policy Control Framework (WT-134)
DSL Forum
Management Framework
DSL Forum
Architecture Requirements for the Support of QoS Enabled IP Services (TR-059)
DSL Forum
Migration to Ethernet Based DSL Aggregation (TR-101)
DSL Forum
(WT-145)
Database Requirements
OA&M Requirements
BRAS Requirements
CPE Requirements
Auto-Configuration of Advanced Services
LAN-Side DSL CPE Configuration Specification

Figure 1 – Relationship to Other Documents

1.4 Purpose

Service providers are currently motivated to expand their existing services to support triple (and quadruple) play and other value added services to protect or increase both market share and revenue. There is also a move towards a converged network supporting residential, voice and business services. To do this they must address several critical needs, particularly:

- The Broadband Multi-Service architecture must make it easier and quicker to provision services for end-users and wholesale and retail partners.
- The Broadband Multi-Service architecture must address both business and residential markets by means of:
  - Variable bandwidths,
  - Higher bandwidths – to deliver both residential video and high bandwidth business services,
  - Some applications and traffic types taking precedence over others,
  - Some applications needing minimum bandwidth and QoS guarantees, either on per user session or a per flow basis,
  - Specific support for IP applications (e.g. VPNs and multicasting),
  - Service Level Management,
  - Security of user and management interfaces,
  - Support for new business models that can include more types of service providers,
  - Support for these new service parameters across multiple connections to different service providers from a single subscriber,

© 2007 DSL Forum. All rights reserved.

- Support for flexible and scalable topologies.

- The Broadband Multi-Service architecture must provide high reliability and availability, e.g. to support business and voice services.

The purpose of this work and the new service models is to provide a common architecture and set of service interfaces to address these critical needs. 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), or emergency service support (e.g. NENA). However, the scope of legal intercept in this document is limited to awareness rather than specification. This should be taken in account in the implementation of architectures that meet these requirements.

In this document the terminologies user, subscriber and customer are defined as follows:

- **user** the person consuming the service
- **subscriber** the entity that has entered a contractual relationship with the Service Provider
- **customer** the general term covering both user and subscriber. In the context of “Bandwidth on Demand (BoD)”, QoS on Demand, or policy control, customer also includes ASPs/NSPs.

1.5 Terminology of Requirements

In this document, several words are used to signify the requirements of the specification. These words are always capitalized when used in this sense.

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 able to inter-operate with another implementation that does include the option.

2 DRIVERS

In this section, the drivers for the migration of existing networks to a Broadband Multi-Service architecture are discussed.

Network convergence

The architecture needs to support the entire range of service types and market sectors (as opposed to the current multiplicity of service specific networks). This is to reduce both CAPEX and OPEX.

Support for different access types

The architecture needs to support other access types in addition to DSL in order to allow providers to offer services to non-DSL connected customers, use technologies which offer higher bandwidths (such as fiber), or provide support for nomadism (e.g. via wireless). Examples of these access technologies are given in APPENDIX C.

Additional connectivity

© 2007 DSL Forum. All rights reserved.

The current TR-058 architecture is based on (multi) point to pop connectivity to a limited number of services edges. There is a need to support a wider range of connectivity, in particular point to point, multipoint to multipoint, and multiple service edges.

Support for both L2 and L3 NT devices

Some business services require L2 connectivity; therefore L2 NTs must be supported in addition to the L3 devices commonly used as RGs (note however that in this architecture an RG can also be a L2 device.)

Support for a wider range of market segments

The following market segments need to be addressed:

- Residential
- Multi-Dwelling Unit (MDU)
- Work at home
- SOHO
- Nomadic users
- Small business
- Medium business
- Major corporations

Support for both wholesale and retail business models

Support for wholesale market drives the need for specified interconnect points**.** Interconnect can be at Layer 1, Layer2 and Layer3. This market is driven both commercially and in some cases by regulation. Support for Wholesale interconnect requires a new set of network management and accounting interfaces.

Support for both residential and business customers

While there are some common services between residential and business customers, other services are more tailored to one than the other, for instance, interactive gaming is more for residential than business customers, while VPN access or video conferencing are more likely to be used by business customers. Typically, there will be higher availability requirements and more quantified and stringent SLAs for business customers.

In addition, business customers are likely to be more self-managed such that service providers have less control over their end user equipment, and the need to provide management portals to allow the customers to manage and monitor aspects of their network services directly.

Simultaneous business and residential use across the same access line

The boundaries between business and residential are blurring due to the emergence of telecommuters (e.g. using a remote access VPN), or the possible use of low-speed DSL services for small business sites and SOHOs. There will be a requirement for simultaneous support of some business and residential services across the same access line to support teleworking at the same time as domestic use.

Support for new applications and network services in addition to existing ones

There is a need to support new services such as IP Telephony and IPTV in addition to legacy voice and TDM services. In some cases there is a need to interwork between new and legacy services (in particular for voice).

Support for nomadic access

© 2007 DSL Forum. All rights reserved.

A triple play offering is becoming common for many service providers. Adding a degree of mobility to the fixed triple play services will enable a provider to offer quadruple play value added services and find new ways of revenue generation and reducing churn. Nomadism gives the ability for a device to access services at places other than the primary location as well as the ability for a customer to utilize different devices to use the same or similar services.

Fixed-mobile convergence

There is increasing interest in fixed mobile convergence (FMC), which for example allows a single device to be used for both fixed and mobile access, and cost saving when 'mobile' calls are diverted on to a fixed access line. The broadband multi-service architecture must be able to support FMC.

High availability

Some services require high availability which in order to cope with infrastructure failures will involve resilient connections with alternative paths (e.g. rings or multi-homing) and automatic switchover.

More scalable and flexible topology

Penetration levels of broadband services are increasing at a fast pace. The move to end-to-end IP Telephony will further increase such penetration by taking IP services to homes or business sites that may not have used broadband services in the past. Penetration levels may ultimately approach those of the PSTN. In addition, the need for high bandwidth for some applications (e.g. video) may lead to access loops being shortened by installing Access Nodes deeper in the network leading to a more distributed architecture. Over-subscription engineering rules are also quickly evolving, as a consequence of such changes and the broader support of services with minimum bandwidth guarantees. Therefore the architecture needs to support monitoring and configuration which will allow rapid re-dimensioning.

All those factors imply more flexibility in the access and regional network topology, and supporting the distribution of more IP capabilities to some locations, while maintaining economies of scale for the overall network.

3 HIGH LEVEL REQUIREMENTS

Based on these drivers, a set of architectural requirements has been derived that need to be supported in a Broadband Multi-Service architecture. The high level requirements are as follows: (the more detailed requirements can be found in Section 7).

- Support for new business models (in addition to the existing service models) and associated network interconnect points;
- Support for network features to be used with the new service model, including:
  - IP-based services and QoS;
  - Bandwidth and QoS on Demand – including session control;
  - Customer self-configuration;
  - Simplification of operations & provisioning;
  - Distinct network and application control planes interfacing with a common data repository;
  - Alternative (to DSL) access network transport technologies;
  - Nomadism;
  - Resilient network options.

© 2007 DSL Forum. All rights reserved.

- Support for integration into multiple types of Service-Oriented architecture, including ETSI NGN, ITU NGN, IMS, and Web services.

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

While this document does address Application Service Provider (ASP) network drivers for information purposes, the standards related to ASPs (e.g. digital rights management, content security, etc.) are not covered by this framework.

4 APPLICATIONS DRIVING NETWORK EVOLUTION

4.1 Application Definition

Definition of application – In this document “applications” are Layer-7 entities from the ISO OSI communications model. Applications are typically software offerings experienced by end-user customers via a device with a user interface (e.g. audio, visual display screen, joystick, and remote control). Applications also typically make use of communication associations among themselves to add value.

The number and variety of applications have grown substantially in recent years. Some of the reasons for this include:

- The number and frequency of high-bandwidth applications are growing;
- The content delivery industry is growing and innovating;
- Internet applications will continue to dominate the application space, including an increasing proportion of streaming applications;
- Video and audio compression technologies continue to improve, providing better quality over lower bandwidth connections, and enabling streaming of video content at quality levels that were unavailable before;
- Maturation of Digital Rights Management (DRM) is reducing the risk for content owners to use digital distribution without losing control of their content;
- Many markets with competition from cable companies require a video, data, and voice bundle in order to remain competitive;
- Digital Broadcast Satellite and cable have produced a user appetite (and expectations) for channel surfing and a large number of channels;
- Consumers are increasingly requiring content to be provided on-demand rather than on a predetermined schedule;
- End user appliances, like mp3 players and digital set top boxes (STBs), are having content delivered over a broadband infrastructure;
- There is an increasing trend towards supporting multi-services on a single terminal; e.g. video programs are downloaded from a set top box or PC, such that they can be watched later on any device, anywhere;
- Applications are evolving towards becoming more distributed (e.g. peer to peer) and using web services (web2.0).

© 2007 DSL Forum. All rights reserved.

Some of the applications defined in TR-058 are still important and will continue to be drivers for a broadband multi-service architecture. These applications include:

- Video, including but not limited to:
  - Linear/Broadcast IPTV: (Applies largely to residential market)
    This is an emulation of traditional cable TV, but delivered via IP. The content provider and TV provider decide which programs to show and when to show them. Due to the multicast/broadcast nature of the service, the Multi-Service architecture needs to provide a multicast capability to optimize the bandwidth usage.
  - Pay Per View: (Applies to residential market)
    Pay-per-view (PPV) allows a user to purchase a specific TV program. This program is shown at the same time to everyone who has ordered it, as opposed to a Video on Demand services. The PPV program can be purchased using an on-screen guide or by phone. The Multi-Service architecture must be able to deliver the PPV content to the user as a multicast stream.
  - Video on Demand (VoD): (Applies to residential market)
    VoD offers subscribers more control over selecting content and viewing times from a Service Provider/Content Provider offered list.
  - Push VoD: (Applies to residential market)
    Push VoD is the download of a complete logical content element (a program, an episode of a program series etc.) to local storage that then enables the user to view the video content at a later time. Push VoD has been called *trickle charging* of the set-top-box in previous DSL Form documents but the two are not synonymous.
  - Internet TV: (Applies to residential market)
    This is a simple Internet Unicast video download - often to various devices such as PCs, handheld gaming devices, single-purpose video players, etc. The content can be provided by individual users, content aggregators, etc. The End user has control over what to watch, when to watch, and where to watch.
  - Remote Education: (Applies to both business and residential market segments)
    Remote Education delivers educational media to students who are not physically "on site." It allows interactive communication between students and teachers in real time.
  - Video calling and conferencing (Applies to business and residential markets)
    IP-based Video calling and conferencing enables customers to initiate video conversations on their PCs, laptops, STBs, or dedicated hardware.
  - Consumer originated TV: (Applies to residential market)
    Consumer originated TV is the sourcing of video and audio from the subscriber and acting as a content source to a service provider. The content may be made available to a specific subscriber (e.g. for home security or babysitting) or to the general public (e.g. video blogging).
  - Interactive Program Guide (IPG): (Applies to residential market)
    An IPG allows the user to scan or search for programs of interest. This is distinguished from a simple EPG by way of providing additional applications such as reviewing.
  - Video Trick modes: (Applies to both business and residential market segments)
    This term refers to the use of control signaling similar to the controls of a VCR, e.g. Play, Pause, Record, and Stop.

    - Regulated video services: (Applied to both business and residential market segments)
      Regulations require the carriage of emergency alerts issued by national, state or local authorities. These regulations were originally targeted at linear/broadcast services. In general, they operate by the insertion of the emergency alert message as audio and/or video messages into the downstream IP stream. Regulations may also require local, government, educational, or public access programs to be made available.
    - Closed captioning: (Applies to both business and residential market segments)
      Closed captioning is a technology to assist hearing disabled users by displaying the audio portions of a television signal as text on the television screen. It may also be used to show informational services such as stock tickers, emergency alerts and other crawler type information.
    - Advertising (targeted and otherwise): (Applies to residential market)
      Advertising can be inserted into the IP stream at various places which allows targeting on the basis of geography (for local advertisements) or to groups of subscribers based on a specific, predetermined interest category.
- Mass market Internet:
    - Business Internet Applications
      This includes various forms of Internet applications and enablers, such as, Email, HTTP, HTTPS, IPsec and FTP.
    - Residential Broadband Internet Applications (might have different level services).
      This includes various forms of Internet applications, such as, Email, HTTP, HTTPS and FTP.
- Games download (Applies to residential market)
- Interactive gaming: (Applies to residential market)
    - Multi-Player games
      Gamers utilize network connectivity to play games against other users.

In addition, the following application areas, not addressed in TR-058, will also drive the broadband multi-service architecture. Note that some of these are in fact new transport mechanisms to support existing services.

- Voice:
    - IP Telephony: (Applies to both business and residential market segments)

      Analog and digital telephone services are still substantial constituents of the service provider market. It is in the service provider’s interest to deliver analog / digital voice over an integrated packet network infrastructure to save network equipment and management cost. The Multi-Service architecture needs to support both end-to-end VoIP and to provide media and signaling conversion where the voice is not already in VoIP format. To ensure the success of VoIP, it is very important to provide end users with a telephony experience comparable with existing POTS/ISDN from both a quality and service availability perspective.
    - PSTN interconnect to legacy voice network): (Applies to both business and residential market segments)

      Since the PSTN still represents the largest segment of the voice market, the Multi-Service architecture must support interconnect to the PSTN network.

© 2007 DSL Forum. All rights reserved.

- TDM: (Applies to business markets)
    - Digital T1/E1-style TDM access for private line or special services are still important parts of the market. It is in the service provider's interest to deliver TDM service over an integrated packet network infrastructure to save network equipment and management cost.

- Peer to Peer (P2P) (distributed) applications (Applies to both business and residential market segments)
    - P2P Software download / file exchange
    - P2P conversational services (VoIP or videoconference, Instant Messaging)
    - P2P streaming video
    - Collaborative work
- Other applications required by law:
    - Lawful Intercept: (Applies to both business and residential market segments)
      This application intercepts the 1 or 2 way data associated with an access, end user, or company subscriber. It can be applied to all data, or just to data associated with a certain application (e.g. VoIP). That intercepted data may be required to be copied and delivered to a law enforcement agency in real time.
    - Emergency Services: (Applies to both business and residential market segments)
      Emergency Service support is the notion that contact with an emergency assistance center should be allowed under all conditions and should take precedence over other types of application. In the past, this applied to PSTN and then cellular voice. It is currently applied to VoIP, and standards and regulations are working on requirements to allow other types of applications to "connect" with emergency service centers, including Instant Messaging (IM), chat, e-mail, and web browsing. A unique aspect of this application is that access to the emergency service is desired even when the user is not a subscriber or would otherwise not be allowed to use the network. Another is that once a user has contacted the emergency service center, there is a need to provide the physical location of the user (i.e. the street address where emergency response vehicles need to go) and to be able to keep the connection or session to the response center established irrespective of end-user action.
    - Network Neutrality: (Applies to both business and residential market segments)
      There are emerging regulations that specify that Internet access should not interfere with or differentiate among the sites, hosts, or domains of the Internet. In other words, the access provider should not make choices on behalf of the customer about which sites are available – including the notion of providing differentiated QoS to certain Internet sites.

Driven by the evolving application needs described above as well as competition, there is a constant trend in the industry to provide more total bandwidth and greater per-application throughput over time. This is most pronounced when a network operator decides to support delivery of high-quality video to a significant degree. The additional bandwidth needs of video applications, when added to the other applications, cause a significant addition to the bandwidth that must be provisioned in the access and aggregation network. Multicast support can mitigate some of the effects when video is presented as the traditional broadcast-like set of channels, but can also be useful in a download, store and play context.

As broadband networks mature and as compression technology progresses, the need to offer high-definition video, multiple concurrent program streams and other high-bit-rate content to subscribers arises. Emerging networks are being planned with sufficient capacity and capabilities to support several streams of high-definition television content per user, and legacy networks are being used to compliment this with over-the-air and satellite delivered content. In order to deliver this combination of content, special network considerations are required.

4.2 Benefits to Stakeholders

The value propositions to the various stakeholders are:

- Network Operators: Increases demand and value of broadband access services while increasing bandwidth efficiency
- End-Users: Enhances end-user experience (e.g. shorter download time). Enables new content services (e.g., VLOGs, Podcasting, etc).
- Application and Content Providers: New delivery "channels" for content and applications. Alternatives to revenue lost from time shifting and PVR commercial skipping.

4.3 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. QoS applications necessitate predictability from the network, which in turn requires various related functions in the network. This section describes the QoS enabled applications. The detailed QoS requirements are captured in section 7.13.

There are new applications in both the residential and business areas which drive the need for bandwidth significantly above that which is currently provided by ADSL. Examples of these are:

- Multi-channel standard definition TV
- High definition television
- High speed business connectivity and VPN access
- Ethernet services

Some applications such as distance learning drive the need for upstream bandwidth beyond that originally provided by ADSL.

Customer applications will also be the main drivers for the Bandwidth on Demand and QoS. Residential and business customers requiring basic Internet access will continue to be provided a best effort broadband service, while enhanced applications, such as video, interactive games, remote education, etc., require broadband service with additional QoS. SME and SOHO customers will have requirements for multiple channel voice and large file transfers both upstream and downstream which drive the need for increased bandwidth or Bandwidth on Demand. Initially, the main devices to which new applications will be delivered are the PC and STB, but it is expected that home networking when combined with broadband access will lead to an increase in the number of connected devices in the customer premises (e.g. gaming consoles, mp3 players, printers, scanners, cameras, telephones, web appliances, home automation equipment, etc).

Access providers will also require the broadband technologies, bandwidth, and QoS to deliver new business services that are increasingly Ethernet-oriented, as well as continuing to provide legacy services over the new converged network.

5 NETWORK FEATURES TO SUPPORT APPLICATION EVOLUTION

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

5.1 Goals

Broadband services have historically been bounded by the limitations specified when the service was first established. Subscribers placed orders for service based on a 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 was required in the Access Node and a new broadband termination device in the Customer Premises Network (CPN). This type of service change is not easy. It takes time to place, review, and process these service orders and involves some degree of service downtime before the subscriber is able to benefit from the increased bandwidth.

These marketing requirements require an increase in the number of service configuration parameters available (such as speed or broadband type), and that service configuration is more dynamic. Apart 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 the 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 broadband 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. By leveraging the ASP service delivery, these applications going through the same broadband network 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 choose connectivity provider and application provider.

5.2 Network Feature Definition

This section outlines a set of network features, which will become the foundation for other new applications and services.

The prevalent existing service model, where subscriber connections are delivered point-to-point in a best effort fashion, 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 and Bandwidth on

© 2007 DSL Forum. All rights reserved.

Demand. Where feasible, network operators desire the ability to support legacy connectivity types on new infrastructure. This typically involves tunneling or other types of protocol encapsulation. Therefore, new service models for interconnection are required.

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 single, common 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 features, the broadband service must be more than just a basic transport mechanism. New architectural requirements will be needed to enable these network features. The following is a list of some of the new capabilities of these network features.

New Business Models

The ability to support the metering, access control, and generation of accounting information to support the business models described in section 7.1.

Broadband Access Type

The ability to support the broadband access types as described in section APPENDIX C.

Bandwidth on Demand

The ability to change the access bandwidth allocated in response to applications, specific network connectivity, or the user's desire to upgrade his/her bandwidth. This network feature permits the subscriber to typically use a lower bandwidth for Internet access and to request an increase in bandwidth as required.

Note that Bandwidth on Demand does not, by itself, provide QoS (i.e. the increased bandwidth is still best effort), but may be combined with mechanisms that do provide QoS.

IPv6

The ability to support IPv4, IPv6, and appropriate interworking – especially as required to support applications that traverse both broadband and wireless networks.

Quality of Service (QoS)

Quality of Service or QoS refers to the nature of the different types of traffic delivery 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 two different types of QoS mechanisms:

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 RSVP. Other sets of bounds may be contractual, such as those defined in service level agreements (SLAs).

© 2007 DSL Forum. All rights reserved.

NOTE: Within this document (and 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 to request the QoS capabilities described above in an on-demand fashion. This includes both relative and guaranteed QoS.

Multicast: The ability to provide multicast groups to achieve optimized multipoint delivery for multicast applications, like audio and video distribution, to improve efficiency of network resources.

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 operator connections or the core network.

Traffic Aggregation: The ability to aggregate NSP, ASP, or wholesale-specific traffic together into logical traffic groupings (e.g. L2TP tunnels, MPLS LSPs, 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 and efficiency, and with the option to improve the resiliency and availability.

Multi-homing and ring-based aggregation may also be used in cases where enhanced reliability and availability are desired.

Improved Transport: Support higher application and service related traffic volumes over more scalable and cost-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, and Packet over SONET (POS). In addition, it is also important to support network optimization for P2MP and MP2MP topologies.

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 common aggregation system, it should be easier to migrate subscribers from one ISP to another, with little or no downtime. Finally, there is a strong desire to further enable customer self-provisioning.

Increased Access: In pre-TR-059 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 ASPs 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, an ASP that can offer a unique service no longer needs to go through a costly

© 2007 DSL Forum. All rights reserved.

acquisition process to become an end user’s sole supplier – it can offer its services to the entire installed based of subscribers.

Standard Connections: The architecture with standard, common interfaces for NSPs and ASPs benefits service providers such that the service provider need only develop a single interface, using a common suite of protocols and signaling mechanisms, to access all of these network 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.

Flexible Function Distribution: The new architecture should allow flexible content distribution, either centralized to reduce the number of service nodes or a more distributed CDN. This will allow the operator flexibility in adding or optimizing the delivery of such applications.

Reliable Network: Typically each service offered over a broadband network will have its own service availability and reliability requirements. These will vary from the very high reliabilities and availability required by emergency services down to the lowest reliability and availability a customer can make use of. These requirements are described in section 7.17 and TR-126 *Triple-play Services Quality of Experience (QoE) Requirements and Mechanisms*. Services will also use metrics relevant to the nature of the Quality of Experience desired for the service. Service architectures to meet these requirements will include end user applications, data centre designs, application servers as well as network architectures. The network architecture contributes only a portion of the overall reliability and availability of the service.

L2 and L3 VPNs: Wholesale and business services such as L2 and L3 VPNs will also drive the evolution of broadband access and/or aggregation networks, more specifically in terms of bandwidth and in terms of how many connections need to be multiplexed across access and/or aggregation nodes. This again will have its ramifications in how Quality of Service is accomplished and how Service Instances are identified.

Nomadism: The ability to allow a user to access services at places other than their primary location. When changing the network access point, the user's service session is completely stopped and then started again, i.e. nomadism does not imply session continuity per se.

Fixed-Mobile Convergence: The ability to allow a user to use a single device for both fixed and mobile access - often with seamless handoffs between the two networks.

Interwork TDM to Packet Network: The ability to migrate TDM services (e.g. POTS, TDM service) over broadband multi-service packet networks. This will affect the evolution of the broadband access, aggregation and edge nodes, mostly in terms of how it will provide PSTN-like voice quality, service features, lawful intercept and Emergency Services support.

Network Management: Support for these above 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

© 2007 DSL Forum. All rights reserved.

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 network features and signaling their specific needs.

6 NETWORK INTERFACE DESCRIPTIONS

The reference model in Figure 2 supports the following service types and functionality:

- Basic Internet Access
- Multi-media, multi-service
- Business and residential services
- Wholesale and retail connectivity
- Policy control and management

Figure 2 depicts the broadband multi-service reference model. This reference model shows that residential and business end users can be served by several A10 reference points for different services or applications. The relationships need not be provisioned, and as an example, it may be possible that the A10 reference point to be used for a multimedia flow is determined only at the time of the service delivery. Wholesale and retail services are differentiated largely by the ownership of the elements in the Service Provider Domain. Connection-oriented services[1], where address management traverses the A10 boundary, are provided by A10-NSP.

[1] These connection-oriented access services are often mistakenly referred to a layer-2 access, but include both layer 2 as well as layer 3 technologies.

© 2007 DSL Forum. All rights reserved.

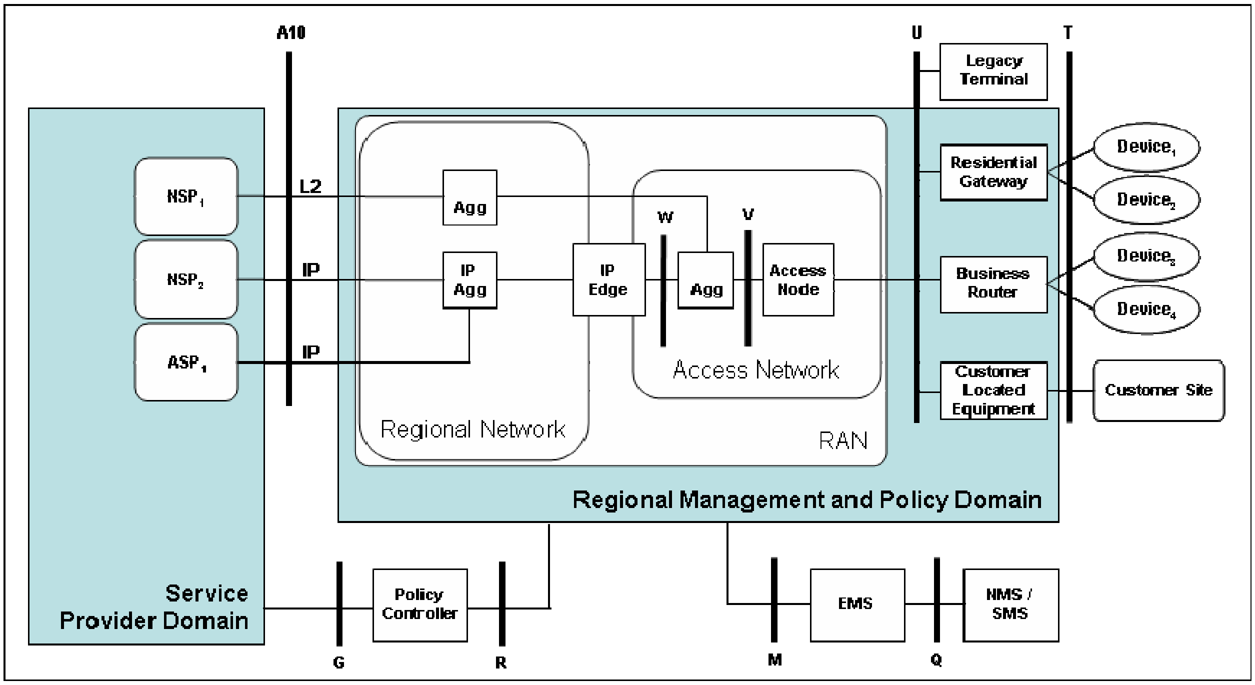


Figure 2 Broadband Multi-service Reference Model

Note, in the reference model, the Legacy Terminal includes the POTS phone, fax, dial-up modem and ISDN phone. The Customer Located Equipment (CLE) is used to provide interworking or native delivery of TDM or ATM services at the customer site. The CLE can be located at the business premises to offer for example PABX services (using DS1/E1 supporting N x 64 kbps), or can be located at a radio site to offer 2G Base Transceiver Station (BTS) connectivity or 3G Node-B connectivity (using T1/E1 or T3/E3 interfaces).

6.1 U Reference Point

The U reference point is located at the subscriber premise between the Access Node and the Residential Gateway for residential service or between the Access Node and the Routing Gateway for business services. Control information and multimedia flows can be distinguished, allowing segregation to different destinations (i.e. controllers and Service/Content providers).

6.2 W Reference Point

The W reference point serves to denote the handoff from the aggregation function in the access network to the IP Edge function. Note that the model also supports omission of the aggregation function, and that results in the V and W reference points being adjacent.

6.3 A10 Reference Point

The A10 reference point serves as the handoff between the access network and ASP and/or NSP as specified in TR-101. The A10 reference point also serves as the handoff between the access network and the Wholesale NSP. This reference point needs to support end-to-end service to both residential as well as business customers. The A10 reference point should support standard transport options. A single instance

© 2007 DSL Forum. All rights reserved.

of the A10 reference point may serve multiple instances of U and V reference points (i.e. point of aggregation or statistical sharing).

6.3.1 A10-ASP Reference Point

This reference point is between the Regional/Access Network and the ASP’s Points of Presence (POPs). 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.

6.3.2 A10-NSP Reference Point

This reference point is between the Regional/Access Network and the NSP’s POPs. In the case of ATM, multiple sessions may be multiplexed over a single VCC at this reference point. 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 broadband service, trouble reports, and other issues from the subscriber are typically addressed to the NSP. Handoff protocols could include ATM VP/VCs, L2TP tunnels, Ethernet VLANs, MPLS LSPs, and routed protocols using IP-VPNs.

6.4 G and R Control Reference Points

The policy control and management interfaces provide the intelligence to facilitate the orderly delivery of the services. A “Policy Controller” would interact with the network by means of an interface to one or more of the network elements. In TR-059 and TR-101, the elements that were controlled with such an interface were the BRAS / BNG and the RG. In the future the “Policy Controller” could control even more elements.

Two types of policy control interface are of interest. One is between the network element and the Policy Controller just described, and is labeled as the R reference point. The other is the “Policy” interface denoted with the G reference point over which policy inputs are made. Like A-10, the G reference point can be an inter-provider reference point. The Policy Controller should be able to generate messages (primitives) across the U reference point to the RG and/or other network termination devices. It must have the capability to distinguish individual U reference instances, and should also be able to address multiple users or service invocations at the same U reference point. The Policy Controller should be able to exchange certain primitives with the BNG, and possibly other network elements as well.

7 EVOLUTION DRIVERS AND ARCHITECTURAL REQUIREMENTS

The evolution of broadband networks is driven by the business case to deploy and maintain a new network, coupled with the need to create and support new services. This section is dedicated to capturing some of the catalysts for network evolution.

- Current generation systems may not have enough capacity to scale to the bandwidth demands of services being envisioned for the future.
- Current generation networks/systems may not support 5-9s type service availability.

© 2007 DSL Forum. All rights reserved.

- Reduction in the number and type of network elements. The number of systems required for multiple services is burdensome from a maintenance perspective, and a reduction in the number of elements, whenever possible, should reduce the management system burden if many services can be supported on fewer elements. For instance, instead of having two NEs for a GPON OLT and DSLAM, both functions could be implemented in a single NE. Similarly, three aggregation switches used for DSL, GPON, and Metro Ethernet access could be combined into one switch that aggregated all three access types.
- Current systems / networks may not allow providers enough flexibility to create the services that are being demanded by their customers.
- Current systems / networks may not adequately address providing broadband to all lengths of access lines that exist in a carrier network.

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

7.1 Business Models

Several economic drivers create the emergence of new business models:

- There is an imperative to find new revenue opportunities using the existing technology base without undertaking extensive network renovations.
- There is a desire to use the broadband access loop for more than one purpose or connection. The idea is that several NSPs and many ASP applications can all share usage of a single access line across the U Reference Point.
- There is a desire to enhance current wholesale business models so that the network operator can share in the revenue (as opposed to only the cost) of provisioning the facilities to support high bandwidth applications, like audio and video streaming, and so the network operator can engage with more types of wholesale business partners.
- There is a trend in wholesale business models to “outsource” subscriber management to the Regional and Access service provider. The wholesale customer then focuses on providing the portal and related applications. This arrangement is sometimes referred to as “bring your own portal,” and it can be selected by a customer with or without specific cooperation between the ISP and the RAN provider.
- There is a desire to offer Open/Equal Access Network involving a horizontal model comprised of Infrastructure Providers, Network Operators, Content Brokers, and Service Providers.

7.2 Billing Models

The Broadband Multi-Service architecture defines the following billing models:

1) **Trusted:** If a given application were trusted by the network operator then application instance records or call detail records (start and stop times for the various applications and participants) could be used in order to derive a bill based on supporting applications in a “Number of instances” x “duration” x “network resource billing amount” model. It should be noted that this is not expected to be a very likely wholesale model, but that it might be

© 2007 DSL Forum. All rights reserved.

appropriate for communications services in which the ASP is the same company as the RAN provider. End users would pay the ASP, who would in turn pay the network operator.

2) **Application as customer:** If the application were independent of the network operator, yet connected to the operator's network, then a business model needs to be supported with a Bandwidth and/or QoS sales arrangement. This type of arrangement will (theoretically) measure or allocate the bandwidth-QoS to the ASP's systems and results in models typified by the following:

a. *All you can eat*: a given ASP might be able to establish application instances limited only by the amount of data that their ASP connection could support. No data throughput or amounts would need to be collected to provide a bill, as the bill would simply be a fixed, recurring monthly amount. Naturally, this model can be refined to establish different rates for different QoS and maximum bandwidths that could be supported.

b. *A la carte*: a given ASP might, again, be able to provide applications only limited by their connection to the RAN. However, instead of a fixed monthly fee, it is possible to measure the amount of data or time that the ASP actually consumes in terms of QoS level, maximum bandwidth, and overall data transported. Naturally, various billing schedules could be developed that include elements from each of these.

c. *Fixed menu*: a given ASP might be required to select a data model with various QoS, maximum bandwidth, and data transport limits – at a fixed cost, but with a fixed duration or with a shut-off if the parameter is exceeded. In this case, an ASP might be given maximum rate limitations less than their network connection size, might be prevented from emitting packets with certain QoS markings, or might even be limited in the total amount of data they could transport in terms of bytes or duration of use. While the billing is simple, like *all you can eat*, the network controls would need to be more sophisticated - not just measuring usage, but policing it according to the business plan.

Finally there can also be hybrid approaches among these, such as a *fixed menu* arrangement up to the point of its limitations, and then instead of reassessing the limitation, using an *a la carte* arrangement after that point. This is not unlike many existing cellular telephony business models.

3) **Subscriber as customer:**

a. The Subscriber purchases bandwidth/QoS from a Network operator, shared by all NSPs and ASPs: there exists a business model where end-users pay for QoS, bandwidth, and total data transport as discussed in the various arrangements in 2) – either in whole or in part. So, for example, an end user might purchase a block of high-bandwidth and/or QoS-enabled transport that could be used with any ASP or even to the Internet using an NSP session. This might preclude or lessen the need for the ASP to bill the end-users directly. However, general opinion holds that end-users will not want to participate in a model where they purchase QoS; and that they might be confused about the required capabilities that they need. Most ASP models are expected to be of the form where an end-user pays an ASP for a valuable application service, and in turn the ASP pays the network operator for the necessary data transport support to provide that application effectively. Nevertheless, this model has one important bandwidth-only instantiation, the *turbo button*.

© 2007 DSL Forum. All rights reserved.

b. The Subscriber purchases time and/or volume based service from a particular NSP, but relies on the network provider to measure the time and/or volume consumed by the pre-paid subscriber.

R-01 Broadband Multi-Service architecture MUST support the metering, access control, and generation of accounting information appropriate to the billing models described in this section.

7.3 Legacy Application Support

NGN migration of voice services currently offered over the PSTN (e.g. POTS, ISDN BRI) will also affect the evolution of the broadband access, aggregation and edge nodes, mostly in terms of how it will provide PSTN-like voice quality, service set, lawful intercept and Emergency Services support.

R-02 Broadband Multi-Service architecture MUST support the voice services currently offered over the PSTN.

R-03 Broadband Multi-Service architecture MUST support TDM services used for business customers, cellular backhauling, and other business applications.

R-04 Broadband Multi-Service architecture MUST provide proper QoS treatment as well as high availability to the voice and TDM services (referred in R-02 and R-03) in the packet network infrastructure, as defined in Section 7.17.

R-05 Broadband Multi-Service architecture MUST be able to provide a media and signaling gateway function between a network-facing PSTN interface and a customer VoIP client that uses VoIP signaling.

R-06 Broadband Multi-Service architecture MUST be able to provide a media and signaling gateway function between a customer-facing TR-08/GR-303/V5 interface to a DLC and a network-facing VoIP client.

R-07 Broadband Multi-Service architecture MUST be able to provide a media and signaling gateway function between a customer-facing POTS/ISDN BRI interface and a network-facing VoIP client that uses VoIP signaling.

R-08 Broadband Multi-Service architecture MUST be able to provide interworking between a customer-facing TDM interface (e.g. T1/E1) and a network-facing packet interface.

R-09 Broadband Multi-Service architecture MUST be able to provide a network-facing TDM Interface to the PSTN network to support PSTN backhaul.

R-10 Broadband Multi-Service architecture MUST support a cost-effective way of supporting legacy services.

The transport of TDM services (e.g. business services, wireless services) over the broadband multi-service architecture must take into account the strict synchronization requirements of those services. In hybrid multi-service environments it is critical to ensure that an acceptable level of quality is being maintained for the TDM services and for proper interworking between different network domains.

TDM networks today provide accurate frequency distribution. Many TDM network elements and services are typically traceable to Primary Reference Clocks (e.g. ITU-T Recommendation G.811 or Stratum1) via a distributed hierarchy of clocks (ITU-T G.811, G.812, and G.813). Such a hierarchy (e.g. ITU-T G.803) of clocks needs to be preserved when transporting TDM services over a multi-service architecture. The requirements are dependent on the TDM service. For example ITU-T G.826 slip rate objectives for voice services must be met while ITU-T G.823/G.824 E1/T1 wander requirements must be met at wireless base stations.

© 2007 DSL Forum. All rights reserved.

Some services might resolve their timing issues within higher layers (e.g. RTP) while other services rely on the timing support provided by the lower layers (e.g. physical layer). The requirements on synchronization in packet networks are currently being addressed in ITU-T SG15/Q13. ITU-T G.8261 Recommendation released in May 2006 addresses synchronization aspects in packet networks for applications such as Circuit Emulation and Synchronous Ethernet where it specifies the maximum network limits of jitter and wander that shall not be exceeded at traffic interfaces, minimum equipment tolerance to jitter and wander and minimum requirements for the synchronization function (interworking function) of network elements.

R-11 Some TDM services require network synchronization. The Broadband Multi-Service architecture MUST be able to provide a mechanism to support such synchronization.

7.4 IPTV application support

In addition to traditional analog and digital broadcast video, an IPTV service is delivered over packet transport, which also provides the additional functionality allowed by bi-directional communications. IPTV can use unicast or multicast to deliver video services as appropriate. It is a basic business requirement that the user quality of experience of IPTV must be comparable with other offerings such as digital cable and digital satellite delivered video services. Channel change time is one factor which impacts the user experience of a TV service. Note that typical digital cable channel change times can range from 1 – 2.5 seconds and digital satellite times are in the range of 2 – 4 seconds.

R-12 Broadband Multi-Service architecture MUST support the delivery of any services to any types of device.

R-13 Broadband Multi-Service architecture MUST support hybrid access systems, e.g. DSL + satellite.

7.5 Other real time application support

Voice and Gaming, etc., are value added services that are of importance to the broadband architecture. They are characterized as low latency applications.

R-14 Broadband Multi-Service architecture MUST support low latency applications, e.g. voice, gaming etc.

7.6 Multi application / multi destination

There is a need for users *on the same access line* to simultaneously access different NSPs and ASPs. Additional destinations can be to other NSPs (e.g. a corporation) or to ASPs. This connectivity will permit a user to maintain an ISP relationship, yet allow these users to have access to other networks and applications that may not be available from their current ISP’s network. The user should be able to select a new service or destination using a form of tunneling and controlled via a user interface if needed, or the access network may simply route traffic appropriately without the need for user intervention or special tunneling arrangements. For example, an access provider may support an ISP as well as a common IP network for ASPs. In this arrangement, both networks are public and reachable from anywhere. However, bandwidth and QoS features offered to ASPs probably vanish when the traffic follows arbitrary paths through the Internet – as would be typical if the ASP traffic were routed to the ISP. An access network operator, however, can instantiate routes in their access network that shunt ASP traffic identified for QoS and BoD treatment directly to the ASP network without otherwise affecting the traffic destined for the ISP.

© 2007 DSL Forum. All rights reserved.

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 network features such as Bandwidth on Demand and QoS on Demand.

R-15 Broadband Multi-Service architecture MUST support the same set of A10 interfaces to NSPs and ASPs**.**

R-16 Broadband Multi-Service architecture MUST allow users to simultaneously access different NSPs and ASPs over a common access connection.

R-17 Both residential and business access MUST be supported by the same access node.

R-18 Broadband Multi-Service architecture MUST provide mechanisms for the classification of traffic according to application type.

R-19 Broadband Multi-Service architecture MUST provide mechanisms for the distinct handling of traffic based upon classification described in R-18.

R-20 Broadband Multi-Service architecture MUST support the following types of arrangements:

Community NSP – Shown in Figure 3 as the pink solid line between the RG and NSP_1, this type of access session is established between an RG and an NSP. It is called the *Community* NSP connection because all the devices within the Customer Premises Network share the connection to the NSP using the NAPT feature of the RG. Because the Community NSP connection is given the *Default Route* at the RG there can be only one. This connection is typically set up to an ISP in order to provide Internet access to all the devices in the Customer Premises Network.

Personal NSP – Shown in Figure 3 as the blue dashed line between $Device_1$ and NSP_2, this type of access session is established between a device within the Customer Premises Network and an NSP. It may be supported with a separate PPPoE session or with a tunneling protocol, like L2TP, Teredo [RFC4380] or IPsec. It is called the *Personal* NSP connection because only the device within the Customer Premises Network from which the connection was established can access the NSP. This avoids using the NAPT feature of the RG. This connection is typically set up to an ISP or a corporation in order to provide private or personalized access, or any access that cannot traverse the NAPT sharing mechanism at the RG.
Note the Community NSP and Personal NSP concepts can also apply to the wholesale market, where the NSP1 and NSP2 in the figure can also be Wholesale NSPs.

ASP – Shown in Figure 3 as the green dotted line between the RG and ASP_1, this type of access session is established between an RG and the ASP network. It is always a single connection and is always shared by all the ASPs. Because the Community NSP connection is given the *Default Route* at the RG, the ASP connection must provide the RG with a list of routes to the ASP network. Also because there is no default route to the ASP network, it is not possible to provide typical Internet access through the ASP connection. This connection is typically set up to the ASP network in order to provide application-specific and QoS-enabled access among all the applications in the ASP network and all the devices in the Customer Premises Network. Note that it is possible to establish a session between a device and the ASP network, for instance, between $Device_4$ and ASP_1, as the orange dotted dash line shown in Figure 3. Clearly, ASPs can also have relationships with NSPs – however those relationships and their interactions are beyond the scope of this document.

© 2007 DSL Forum. All rights reserved.

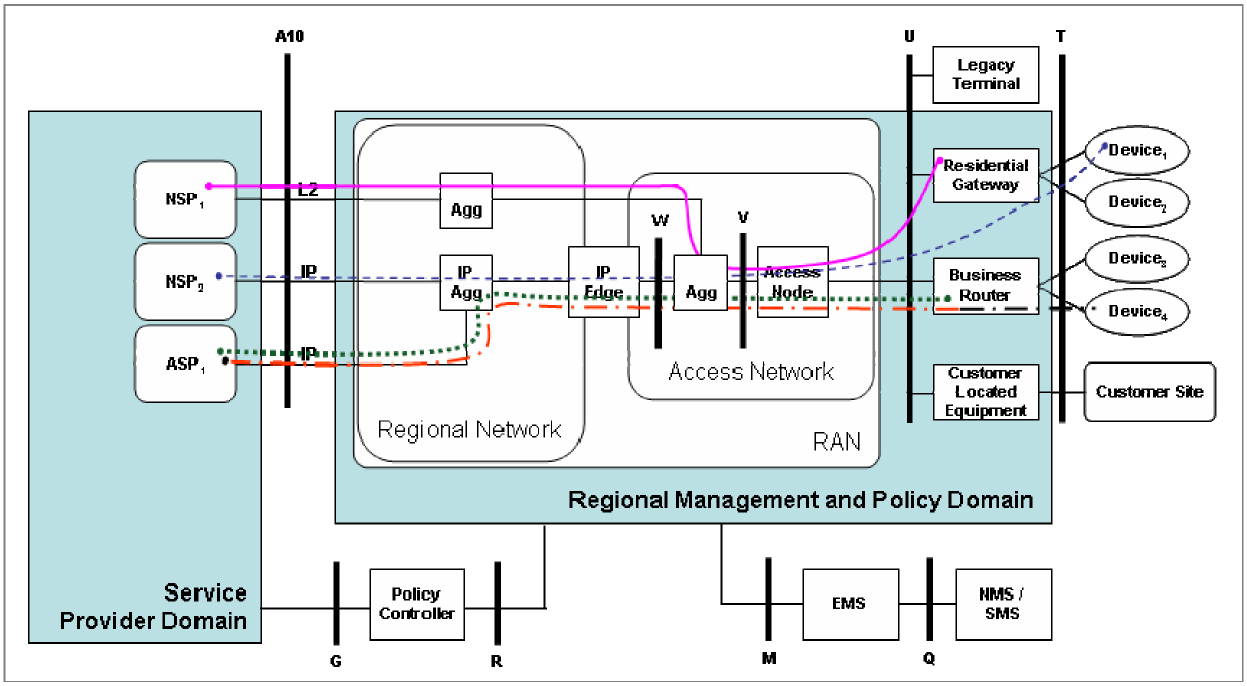


Figure 3 – Access Session Types

R-21 Broadband Multi-Service architecture MUST support both P2MP and MP2MP topologies.

7.7 L2 and L3 VPNs

R-22 Broadband Multi-Service architecture MUST support L2 and L3 VPNs, in particular the high bandwidths and large number of connections that may need to be multiplexed across the access and/or aggregation nodes.

R-23 Broadband Multi-Service architecture MUST support dynamic tunneled access to VPNs.

R-24 The VPN architecture MUST support point-to-point, point-to-multipoint, multipoint-to-point and multipoint-to-multipoint network topologies. This includes the support for uni-directional and bidirectional communication models.

R-25 The VPN architecture MUST support Multi-NSP VPNs.

R-26 The VPN architecture MUST support multicast traffic in an efficient way.

R-27 The VPN architecture MUST support:

- At least 500,000 P2P VPNs
- At least 100.000 MP2MP L2 & L3 VPNs
- At least 10.000 sites per VPN for multipoint-to- multipoint
- Up to 10.000 stations per site for L2

The number of VPNs is based on a typical provider area with a provider edge and could be distributed over a different number of machines.

R-28 Configuration changes to the network MUST NOT be unintentionally service impacting.

R-29 The Broadband Multi-Service architecture MUST be able to provide secure and authorized access to VPN for nomadic users.

R-30 The Broadband Multi-Service architecture MUST support dynamic tunneled VPN access over shared media.

R-31 Broadband Multi-Service architecture MUST include QoS support for both L2 and L3 VPNs.

7.8 Traffic Aggregation

R-32 Broadband Multi-Service architecture MUST support the ability to aggregate NSP, ASP, or wholesale-specific traffic together into logical traffic groupings (e.g. L2TP tunnels, MPLS LSPs, MPLS VPN, VLANs) at the V interface, and across the RBN and A10 interfaces at both Layer 2 (L2) and Layer 3 (L3).

7.9 Improved Transport

R-33 Broadband Multi-Service architecture MUST support high speed L2 technologies at the V interface, across the RBN and at the A10-NSP and A10-ASP interfaces. These include 100Mbps and Gigabit Ethernet and Packet over SONET (POS).

7.10 More Bandwidth

With some access technologies the positioning of the Access Node must be closer to the customer so that the loop lengths can be kept to distances that support higher speeds. For example, in order to achieve symmetric 100Mbps access rates using VDSL2 a network operator would have to position access nodes within 1000 feet of the subscribers. Alternatively the network operator could choose PON or pt-pt Ethernet technology and position ONTs or Ethernet termination points at the customer premises.

R-34 Broadband Multi-Service architecture MUST support locating appropriate access technologies in outside plant Access Nodes.

Note that this will impact the sizing and powering of the Access Node.

7.11 Bandwidth on Demand

Bandwidth on Demand results in a dynamic or semi-dynamic behavior of the actual throughput over the broadband access network.

R-35 Broadband Multi-Service architecture MUST support bandwidth on demand, i.e. the ability to change the effective access line bandwidth based on the application, destination selected, or explicit user request.

Note that such a change does not, by itself, provide QoS (i.e. the increased bandwidth is still best effort), but may be combined with mechanisms that do provide QoS.

R-36 Bandwidth on Demand MUST provide near real time fulfillment of Bandwidth changes requested by either client or application.

R-37 Bandwidth on Demand MUST be able to coordinate with resource admission control.

Figure 4 is used to show a possible bandwidth business model. In the figure, the outer circle represents the total bandwidth that is available to a VC (or VLAN) on an access line. Within this total bandwidth there are two access sessions shown: ASP Access Session and NSP Access Session. The NSP Access Session, shown as a large, light grey oval, occupies a smaller space than the whole access line (VC) bandwidth. This indicates that the NSP access session is not allowed to access the total bandwidth on the

© 2007 DSL Forum. All rights reserved.

loop. In the past, the NSP Session and the Virtual Circuit would have been the same bandwidth. By increasing the data rate on the access loop, additional bandwidth is created that exceeds that which the NSP has purchased.

The ASP Network session is shown as a white circle just inside the VC bandwidth and is essentially the same bandwidth as the Virtual Circuit. This would indicate that some set of conditions exist where the ASP session could occupy all the bandwidth on the access line.

Several Applications are shown overlaid on the sessions and within the bandwidth limits assigned to the NSP and ASP. The NSP application (dark grey oval) is a strict sub-set of the NSP Session and is using a large fraction of the NSP's allowed bandwidth. The three other applications, however, show three salient relationships and business models that can exist between applications in the ASP network and both applications as well as the access session for the NSP. These relationships will be described in the sections that follow.

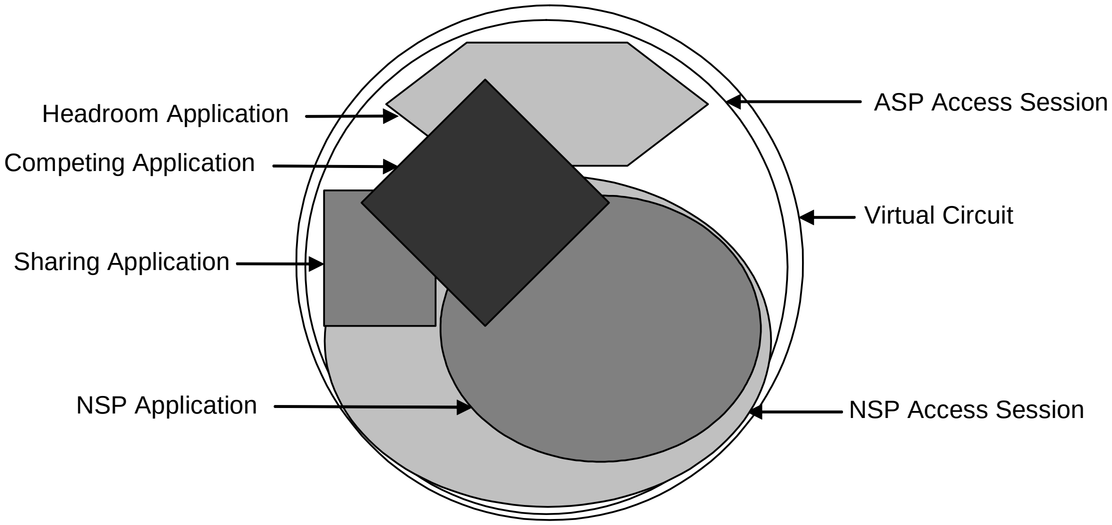


Figure 4 Bandwidth Business Models

7.11.1 Simple Bandwidth Partitioning

In this model, the application has access to all the bandwidth which the NSP could never access, as well as the additional bandwidth sold to the NSP, but not currently in use by applications in the NSP Session. A Sharing application can make use of all the bandwidth on the Virtual Connection, but can only use the "NSP" bandwidth when the NSP session is not using it. This arrangement could be described as work conserving, and may be the preferred business model for simple bandwidth partitioning.

R-38 BoD MUST support the Simple Bandwidth Partitioning model that the application can make use of all the bandwidth on the Virtual Connection, but can only use the "NSP" bandwidth when the NSP session is not using it.

7.11.2 Priority and Dynamic Bandwidth Sharing

In this model, the application may have access to some or all of the bandwidth used by the NSP and it may have access to that bandwidth with greater, equal, or lesser precedence than the NSP applications. Similarly, this application may also be able to pre-empt bandwidth that other ASP applications are attempting to use. This is the most complex arrangement, and the most flexible. A competing application can compete for the bandwidth that NSP applications are attempting to use.

© 2007 DSL Forum. All rights reserved.

R-39 BoD MUST support the Priority and Dynamic Bandwidth sharing model that the application may have access to some or all of the bandwidth used by the NSP and it may have access to that bandwidth with greater, equal, or lesser precedence than the NSP applications. Similarly, this application may also be able to pre-empt bandwidth that other ASP applications are attempting to use.

These treatments can also be provided among ASP applications and with finer granularity among multiple applications.

R-40 Bandwidth on Demand MUST be able to coordinate 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 ensure that the additional bandwidth can be made available on a dynamic basis when requested by applications or end users.

7.11.3 Support of Variable Access Rates

Minimum Line Rate

The Minimum Line Rate is the line rate that is always guaranteed when there is service. A line that is not in a fault condition will always provide at least the minimum line rate.

Maximum Line Rate

The Maximum Line Rate is the maximum data rate desired by the operator in bit/s or the highest data rate permitted by the operator. Therefore the Maximum Line Rate is used to bound the marketed rate for connection tiers.

Attainable Data Rate

The Attainable Data Rate is the Maximum data rate which can be achieved.

Actual Line Rate

The ALR is the instantaneous line rate. The effective bandwidth is bounded by the Actual Line Rate.

R-41 Broadband Multi-service network MUST be able to support the Minimum, Maximum, Attainable, and Actual Line Rates as boundary conditions for traffic management.

7.12 IPv6

R-42 Broadband Multi-Service architecture MUST support IPv4, IPv6, and the appropriate interworking between these. Interworking is particularly appropriate where applications traverse both broadband and wireless networks.

7.13 QoS support

When an ADSL service was first offered, most of the applications were simple web browsing and email. These applications, in general, do not require high quality of service. However, since then, many real-time applications and services have been introduced. Examples are VoIP, video on demand, and interactive gaming. These applications are either time sensitive, or packet loss sensitive, or both. To satisfy customers of these applications, the network service providers must support QoS in their networks.

R-43 Broadband Multi-Service architecture MUST have the ability to differentiate between various service classes at the network level, for both upstream and downstream traffic.

R-44 When marking traffic, Broadband Multi-Service architecture must have the ability to differentiate between various service classes at the application level.

R-45 Broadband Multi-Service architecture MUST support Relative QoS, i.e. class-based traffic priority with no absolute bounds on the achieved bandwidth, packet delay or packet loss rates.

R-46 Broadband Multi-Service architecture MUST support guaranteed QoS, i.e. a packet delivery service with specified values for some or all of the QoS parameters, which may or may not be used as part of contractual SLAs.

R-47 Broadband Multi-Service architecture MUST have the ability to offer relative QoS for some service classes and guaranteed QoS for other service classes.

R-48 Broadband Multi-Service architecture MUST support both signaled and pre-provisioned QOS.

R-49 Broadband Multi-Service architecture MUST provide network QoS support for existing as well as new applications.

R-50 Broadband Multi-Service architecture MUST have the ability to provide and where appropriate enforce QoS for the different services by allocating resources in the access, regional and core networks, or by interworking with other NGN functions to provide the requested QoS.

R-51 Broadband Multi-Service architecture MUST be able to honor ingress QoS markings.

R-52 Broadband Multi-Service architecture MUST be able to remark traffic when configured so as not to honor ingress markings or to perform re-classification for its own purposes.

R-53 Broadband Multi-Service architecture MUST have the ability to preserve traffic markings, yet not honor those received markings.

R-54 Broadband Multi-Service architecture MUST be capable of providing QoS support to applications which dynamically assign port numbers.

R-55 Broadband Multi-Service architecture MUST be capable of providing QoS support to traffic where source and/or destination address are not known ahead of time.

R-56 Broadband Multi-Service architecture MUST be able to collect QoS and service related statistics from the network.

Since not all users are expected to concurrently use their maximum bandwidth at all times, operators involved in delivering QoS-enabled services over these networks want to share network resources between different users.

R-57 Broadband Multi-Service architecture MUST support statistical over-booking of all QoS resources, including guaranteed QoS.

Since many ASPs can be connected to the access and aggregation network, the way in which ASPs use this network must be controlled.

R-58 Broadband Multi-Service architecture MUST allow the operator to divide the bandwidth between the applications delivered by the ASPs.

R-59 Broadband Multi-Service architecture MUST support resource reservation control both within traffic for a given ASP and across ASPs.

R-60 The network resource controls MUST include a feedback function that can inform the requester whether or not the requested bandwidth or QoS is available.

© 2007 DSL Forum. All rights reserved.

R-61 Broadband Multi-Service architecture MUST be able to provide service based accounting on the basis of both time and volume.

In addition to QOS, high availability and reliability in networks is growing in importance. Detailed requirements are defined in section 7.17.

Achieving end-to-end Guaranteed QoS requires the appropriate mechanisms to be in place in each of the networks involved, i.e. the access network, the Regional Broadband Network (RBN) and the core network. These mechanisms may include request or reservation schemes to dynamically support 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. In some access types, like WiMAX and WiFi, it may not be feasible to provide these types of guarantees.

Relative QoS can be used for applications that can cope with an occasionally degraded perceived service behavior. Relative QoS allows the network to give certain classes of traffic a better or worse traffic delivery service than other classes.

Network QoS and QoS related parameters include:

- Bandwidth (See section 7.10 and 7.11)
- Packet transfer delay: The time it takes for the network to deliver a packet from the source to the destination.
- Packet transfer delay variation: The variation of the packet transfer delay from packet to packet. It is also called jitter.
- Bit Error rate: The rate at which the transport mechanism experiences unrecoverable bit-errors. The distribution of bit errors is also important.
- Lost packet rate: The percentage of packets lost in the network during the delivery or discarded because they experienced bit-errors.

Support of QoS can be achieved at (a) Network level, (b) Flow level, and (c) Packet level. At the network level, all customer traffic in the network is affected. At the flow level, only certain customer flows are affected. At the packet level, the QoS treatment is supported at a packet-by-packet granularity. Approaches to support QoS are as follows:

Capacity Planning and Traffic Engineering:

Service Providers use Capacity Planning and Traffic Engineering to deploy/utilize appropriate capacity in the network based on forecast and trending.

R-62 Broadband Multi-Service architecture MUST support Traffic Engineering.

Resource Reservation and Session control:

R-63 Broadband Multi-Service architecture MUST support the ability to reserve (or deny) the bandwidth requested for a session or flow.

R-64 Broadband Multi-Service architecture MUST support the ability to admit or reject resource requests using knowledge of available resources and/or policy.

© 2007 DSL Forum. All rights reserved.

Attempts to change the QoS and bandwidth for a given application must check end to end path across the aggregation, access network, and the subscriber lines to ensure that the QoS and bandwidth requested can be supported. The network also needs to make sure that the changes will not degrade the performance of other applications and other customers' applications.

R-65 Resource Reservation MUST take into account both unicast and multicast traffic both separately and in combination.

The challenges of multicast specific CAC include: various locations of multicast replication points, lack of knowledge of bandwidth, and the ability for CAC to fulfill requests in real time, the statistics to be reported, and coordination between unicast and multicast CAC mechanisms when different,

R-66 Resource Reservation systems MUST be independent of the application and form of IP transport.

Metering and Marking:

R-67 Broadband Multi-Service architecture MUST support Marking in conjunction with Metering to monitor the number of packets received.

Packet Treatment, Queuing and Scheduling Discipline:

R-68 Broadband Multi-Service architecture MUST support queuing and scheduling to achieve the relative and absolute QoS required. This may include shaping of the traffic.

Inter-layer mapping:

R-69 Broadband Multi-Service architecture MUST support Inter-layer mapping to provide end-to-end QoS and bandwidth control in both IP and non-IP networks (e.g. ATM or Ethernet hybrid access networks) requires a mapping from QoS to CoS as well as the appropriate overhead calculation for interconnecting two different layer 2 technologies.

When DSL service was first offered, in general, business customers required higher QoS than residential customers. However, with the introduction of services, such as VoIP, VoD and interactive gaming, residential customers will also require QoS support for some of their services.

R-70 Broadband Multi-Service architecture MUST support QoS for both business and residential customers.

R-71 Different applications may have different QoS requirements. The network MUST be able to support QoS profiles.

7.14 QoS on demand

Many customers subscribe to a broadband service to access applications that only require basic bandwidth and no explicit QoS, such as email and Internet access. However, these customers may occasionally want to use applications that need higher bandwidth and/or a certain QoS level. These applications, such as video on demand and interactive gaming, require high bandwidth and a good QoS but only for a certain period of time. When the customer terminates these applications, they may no longer need the high bandwidth and QoS level. If the high bandwidth and QoS are reserved permanently, the network would need to be over-dimensioned. An alternative approach is to deploy dynamic QoS on demand and bandwidth on demand capability. With this capability, the network resources can be utilized more efficiently.

R-72 Broadband Multi-Service architecture MUST support QoS on Demand i.e. the ability for individual application sessions to request traffic delivery characteristics according to their needs, and to change the desired traffic delivery service for both relative and guaranteed QOS.

To offer QoS on Demand requires signaling capability from ASPs, users, or both. It also needs additional intelligence in the network, which enables dynamic allocation of network resources and dynamic assignment of QoS treatment (e.g. scheduling and queuing disciplines) to certain packets at the time the application is requested, and then to release these resources and QoS assignment at the time the application is terminated. This means that at some point(s) in the network, Resource Reservation and session control needs to be implemented.

Alternatively, QoS on demand can be supported by using a capacity plan for a pool of bandwidth for a given class, with the use of resource monitoring.

R-73 The Broadband multi-service architecture MUST provide support for near real time QoS changes.

7.15 Multicast

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

Applications that may benefit from a multicast service are:

- Bringing broadcast-type high bandwidth multimedia information to residential and business users via a regional/access network.
- Efficient content distribution. A small content server can only send scores of copies of its content to multiple clients or redistribution servers that are located closer to the end-users. This communication is one-to-many and can be facilitated by multicast to improve the scaling characteristics needed by the content server. The applications can vary from Internet Radio to PodCasting to software updates.

Multicast had been extensively addressed in TR-101. It is the intention of this document to extend multicast support to business applications.

R-74 Broadband Multi-Service architecture MUST support multicast for both residential and business customers**.**

R-75 The multicast control MUST support subscriber management and AAA accounting**.**

R-76 Broadband Multi-Service architecture MUST support unified multicast and unicast resource admission control.

R-77 Broadband Multi-Service architecture MUST support time/volume based accounting as well as pre-paid/post-paid multicast service delivery.

R-78 The multicast control MUST be able to dynamically determine the resources required for the delivery of a multicast content request.

R-79 The multicast control MUST include a method to return request failures to the application or client.

R-80 The multicast control MUST be able to override subscriber multicast controls.

© 2007 DSL Forum. All rights reserved.

R-81 The Broadband Multi-Service architecture MUST allow multicast membership accounting for audience measurement.

7.16 Content Distribution

R-82 Broadband Multi-Service architecture MUST support content caching at the edge of the network.

R-83 Broadband Multi-Service architecture MUST support flexible content distribution strategies, i.e. both centralized and distributed.

7.17 Network Availability

The nature of network availability

Network availability is best described in terms of unavailability events having three dimensions:

- Event frequency: how often does the event occur
- Event duration: how long does it take to restore normal operation either in terms of the average or more usefully in terms of a distribution or percentile threshold
- Event scope: how much impact does a single event have (i.e. how many customers are affected at one time or how large is the geographic region affected)

The combination of event frequency and duration and scope information can be used to derive availability percentages and other more service specific figures of merit such as lost call minutes etc.

Event Duration and the sources of unavailability

Unavailability events can be classified into one of five types based on event duration and cause. While these are not exhaustive or very precise they do provide a reasonable framework for setting availability requirements.

The event types are as follows:

Event Type	Description and examples	Typical duration and MTTR
1. Transport network	Transport network switching events, e.g. MPLS Fast Re-Route events in the regional broadband network or SDH APS events in the aggregation network.	<100msec (say MTTR =0, i.e. these events do not materially affect service availability)
2. Network Re-convergence	Network recovery e.g. router re-convergence in the regional broadband network.	< 10 seconds. (say MTTR = 10 sec)
3. Restart events:	Software restart events e.g. re-start or software version update to a network node.	< 5 minutes (say MTTR = 5 min)
4. Hardware replacement events	Hardware replacement events e.g. unprotected interface card failure on network elements.	< 4 hours (say MTTR = 4 hours)
5. “Outside plant” events	“Outside plant” events e.g. unprotected fibre or copper cable	> 4 hours (say MTTR = 24 hours)

© 2007 DSL Forum. All rights reserved.

	failure, or failure of a Residential Gateway.	

Availability can be calculated from this information as the weighted sum of MTTR and event frequency i.e.

$$AverageAvailability = 1 - \sum_{foralleventtypes} MTTR * frequency \qquad \textbf{(Equation 1)}$$

$$TypicalAvailability = 1 - \sum_{foralleventtypeswherefrequencyis \geq 1} MTTR * frequency \qquad \textbf{(Equation 2)}$$

Note that the calculations focus on network-wide availability (especially for event types 1 and 2), rather than node-specific availability.

Events of less than 100msec (i.e. transport network switching events) do not contribute significantly to overall availability percentages, but can have a major impact on QoE (e.g. for video streaming); so it is still important to include these short events in our requirements.

Event Scope and the sources of unavailability

Unavailability events affect more or less customers depending on where they occur in the system. Networks and systems probably have similar structures and so the typical scope of events should be similar and relate to similar event types.

The scope categories are as follows:

Name	Description	Typical Impact
1. Individual fault	Residential Gateway, single line or line card failure. Typically events around the U reference point.	1 – 50 customers.
2. Local fault	Copper cable or Access Node failure. Typically events affecting the Access Node or the V interface.	50-2000 customers.
3. Regional Fault	BNG or aggregation node failure.	2000 – 50,000 customers.
4. Mass Impact Fault	Core application server complex. Typically events beyond the A10 interface or major site infrastructure failures e.g. power.	Over 50k customers.

These categories for event scope can be used in setting availability requirements.

A Note on Planned Outages

The focus of the discussion above is the total of Planned and Unplanned Outages. Planned Outages may justify a different treatment; however, the architecture should not focus exclusively on unplanned events because:

1. Planned events will have less impact over time as node software is improved (e.g. hitless software upgrades).
2. The main distinguishing feature of a planned outage is that because it is scheduled it is possible to take steps to minimize the impact in advance. In other respects it is similar to an unplanned event but with smaller scope.

© 2007 DSL Forum. All rights reserved.

3. The windows of significantly reduced impact suitable for planned outages are becoming less easy to identify as usage patterns change and usage becomes more constant over the course of the day.

R-84 Broadband Multi-service architecture MUST support any combination of the following redundant topologies:

- Redundant links between an Access Node and an aggregation switch, see scenario 1 in Appendix B as an example implementation.
- Redundant links between a subtended Access Node and a primary Access Node, see scenario 2 in Appendix B as an example implementation.
- Ring of Access Nodes, see scenario 3 in Appendix B as an example implementation.
- Redundant aggregation switches connected to an Access Node, see scenario 4 in Appendix B as an example implementation.
- Redundant BNGs, see scenario 5 in Appendix B as an example implementation.

Note: all the redundant topologies mentioned above are expected to support load balancing, so that when Access Node is connected through two, for example, GigE links, it would benefit from 2 Gbps bandwidth.

R-85 Broadband Multi-service architecture MUST support detection and switchover mechanisms to allow services with very high availability requirements to be supported.

R-86 Broadband Multi-service architecture MUST support Multi-homing and ring-based aggregation where enhanced reliability and availability are required.

7.18 Nomadism

The triple play offering is becoming common for many service providers including both phone providers and cable providers. Adding a degree of mobility to the fixed triple play service will enable a provider to offer quadruple play value added services and find new ways of revenue generation and reducing churn.

From the user perspective, nomadism will add the possibility for a user to access services at places other than his home location. For instance, it will allow a user to access from the primary residence (home), from a secondary residence, from a neighbor’s or friend’s residence, from the office, using public access (e.g. WiFi hot-spot), and using mobile/cellular device.

There are many levels of nomadism, such as at a device level, user level, and application level. The scope of Nomadism in this document is limited to device and user nomadism. Nomadism gives the ability for a device to be moved to different access points and access networks (which may or may not belong to the same access network provider) as well as the ability for a user to utilize different device to retrieve the same or similar services. This will include access to services according to the user service profile, authentication and authorization for access services and location update, i.e. to locate where the user is.

The definition of Nomadism given by ETSI/TISPAN is referenced below. For completeness, some related terms given by ETSI/TISPAN are listed as well:

Nomadism: “Ability of the user to change his network access point on moving; when changing the network access point, the user's service session is completely stopped and then started again, i.e. there is no session continuity or handover possible. It is assumed that normal usage pattern is that users shutdown their service session before moving to another access point.” *Definition from ETSI/TISPAN*

Roaming: This is the ability of the users to access services according to their user profile while moving outside of their subscribed home network, i.e. by using an access point of a visited network. This requires the ability of the user to get access in the visited network, the existence of an interface between home network and visited network, as well as a roaming agreement between the respective network operators." *Definition from ETSI/TISPAN.*

Session Continuity: "The ability of a user or terminal to change the network access point while maintaining the ongoing session. This may include a session break and resume, or a certain degree of service interruption or loss of data while changing to the new access point." *Definition from ETSI/TISPAN.*

Continuous Mobility: "The ability of a mobile user/terminal/network to change location while media streams are active". *Definition from ITU-T* For sessions where session breaks are not allowed Continuous Mobility is used.

It must also be noted that in nomadism scenarios, more than one player taking on the different roles may be involved. For example, the network access provider connecting the summer house or hot spot may not necessarily be the same as the one providing the access to the home (primary residence). This implies some kind of "roaming relationship". However, the common scenario is that service is provided by the "home" ASP.

R-87 Broadband multi-service architecture MUST support nomadism i.e. allow a user to access services at places other than their primary location. This will not usually require application session continuity, except for some voice services.

R-88 Broadband Multi-Service architecture MUST support roaming and nomadicity for appropriate wireless devices.

7.19 AAA Requirements

This section contains the AAA requirements. A common AAA system for multiple access types is desired.

R-89 The AAA architecture MUST allow the network to authenticate the use of an access circuit.

Note: Access circuits are typically provided to a subscriber under a contract with the provider, and therefore can be billed, authorized, and traced accordingly. An access circuit can be authenticated by means of a circuit identifier that is generated by network equipment controlled and trusted by the service provider, and that terminates the access circuit.

R-90 The AAA architecture MUST allow the network to authenticate a subscriber session, where a subscriber session is defined as a PPP session, IP session, or dynamically tunneled VPN session.

R-91 The AAA architecture MUST allow the network to authenticate device attachment, in particular for wireless access (e.g. WiMAX or 802.11).

R-92 The subscriber session can be initiated from a RG or from a terminal, and it MUST be possible to authenticate both of these types of session.

Note: For example, a subscriber's login and password may be configured permanently or temporarily into an RG and are used for authentication every time an access session is established. Another example is authentication of a PC-originated access session at a WiFi Hotspot using Login & password.

© 2007 DSL Forum. All rights reserved.

R-93 Broadband Multi-Service architecture MUST allow the network to determine device types.

Note: Device types can be determined by means of device type identifiers, in order for the network to distinguish between devices of different types, for example, to give authorization to particular types of RGs or STBs.

R-94 Broadband Multi-Service architecture MUST support a mechanism to logically locate where a subscriber session has originated or to physically locate where a device is.

R-95 The NSP, potentially after exchanging information with other players, MUST be able to correlate each device IP address authorized on the network with the identity of a subscriber, and to the credential information given by this device at the authentication stage.

R-96 The AAA architecture MUST allow network level authentication to dynamically perform the necessary authorizations between the customer and some existing and predefined network resources, according to the customer' service subscription profile returned by the AAA servers while processing the customer's credential information.

R-97 The AAA architecture MUST allow the different actors involved to interact properly so as to control nomadism for a user connecting from different places in the access network.

R-98 The AAA architecture MUST allow the different actors involved to interact properly so as to control roaming for a user connecting to or from a visited network.

7.20 Wholesale Access and L2 connectivity

Today a number of different types of access unbundling exist. The most common types are (PHY) L1 and L2 unbundling. Additionally, access providers are finding more opportunities to provide services to network providers based on wholesale relationships that are both mandated as well as freely contracted.

R-99 Broadband Multi-Service architecture MUST support wholesale access connectivity.

There is also a strong desire to be able to continue to offer the most popular network services of the legacy networks on newly deployed infrastructure.

R-100 Broadband Multi-Service architecture MUST support a cost-effective way of supporting legacy wholesale services.

R-101 Broadband Multi-Service architecture MUST be able to provide individual aggregation characteristics for wholesale, L2, and other access types.

This allows the various NSPs and applications to specify differing levels of over-subscription – even when they are only using best effort QoS characteristics. Thus, two ISPs may offer differentiated Internet access that depends on the amount of congestion that their subscribers experience – even when those subscribers and the service is supported on the same access network.

7.21 Access Technologies

There are many access technologies and variations for each technology. APPENDIX C details the access technology for most markets.

R-102 The Broadband Multi-Service architecture MUST be able to support the following access types:

- PON
- P2P Fiber Access

© 2007 DSL Forum. All rights reserved.

- ADSL1 and 2
- SHDSL
- VDSL1 and 2
- Ethernet
- Wireless access

R-103 The Broadband Multi-Service architecture must support pair bonding.

7.22 Management

Management is defined as the set of mechanisms for provisioning new subscribers and service providers, controlling network feature delivery, detecting and addressing networking and application troubles, advertising new services and applications and collecting the accounting data necessary to generate bills. These mechanisms need to interface with a well-defined data repository.

Service-Oriented Architecture (SOA) is an application framework that allow for modularity of applications and their support infrastructure. It can promote reuse of common capabilities among applications. For example a VoIP application and a chat application may share subscription, profile repositories, address book, and other capabilities. These capabilities can be part of a framework that allows their reuse across applications. Similarly, applications may offer benefits directly to one another, as would be the case if the VoIP application were usable stand-alone or as a component of the chat application – to support voice chat.

Many of the management and policy functions that a network operator must perform in order to provide their access services are also useful functions that can be exposed to other NSPs and ASPs that share business relationships with the operator. Furthermore, exposing these capabilities can create better integration among applications and network features as well as new potential revenue opportunities for the network operator that exposes them.

R-104 The management features and functions MUST be architected and provided in a modular way so that some or all of them can be made available to 3rd parties. Thus, management interfaces and features are no longer simply support infrastructure, but can become part of the set of features (services) offered by a network provider to their customers.

R-105 The management features and functions MUST be made available as parts of an SOA framework.

Two competing approaches to SOA exist within the typical broadband access provider infrastructure: IMS and non-IMS including Web Services.

> *IMS* is the IP Multimedia Subsystem defined by the 3GPP organizations and is focused on SIP signaling and cross-provider profile capabilities and in managing communications-oriented applications. It is primarily used in wireless and PSTN networks, and is arguably incomplete for some types of applications.
>
> *Web-services* is the mechanism defined by the Internet community and used by Enterprise and Web-centric service providers like Amazon and Google.

Many broadband operators will have the need for a SOA that integrates and supports both systems. There is a general requirement that the applications, management infrastructure, and network features be provided as SOAs with the capabilities exposed in both the IMS and Web-services-centric ways – as appropriate.

To support new services and their underlying network features requires a new set of network management and control interfaces. In this document the term "network management" applies to the provisioning of services, which typically happens on a relatively long time-scale. "Network control" refers to a real-time or near-real-time capability of the network to react to specific requests. ASPs, NSP, Wholesale NSP, and subscribers will all use these network control interfaces to affect policies in the network. 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 network 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 network features and services usage. These billing records will need to be created for static as well as dynamic usages.

A three-layer management model can be used to model the network, SOA/middleware, and applications. This approach is sufficiently generic to support a wide range of use cases. Figure 5 shows the three-layer logical architecture for support of services such as media-on-demand or gaming. It identifies the following layers:

- **The network layer:** This layer models basic communications. The capabilities required from the Regional/Access Network Provider to support these features are described throughout section 7. The Access/Aggregation/Regional Network provider facilitates the connections between subscribers and NSP/ASPs, as well as to the Wholesale NSPs.
- **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 as part of a larger SOA ecosystem. 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 5, 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 Resource and Admission Control (RAC) subsystem and Network Attachment subsystem (NAS) defined by TISPAN NGN, as well as 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.

© 2007 DSL Forum. All rights reserved.

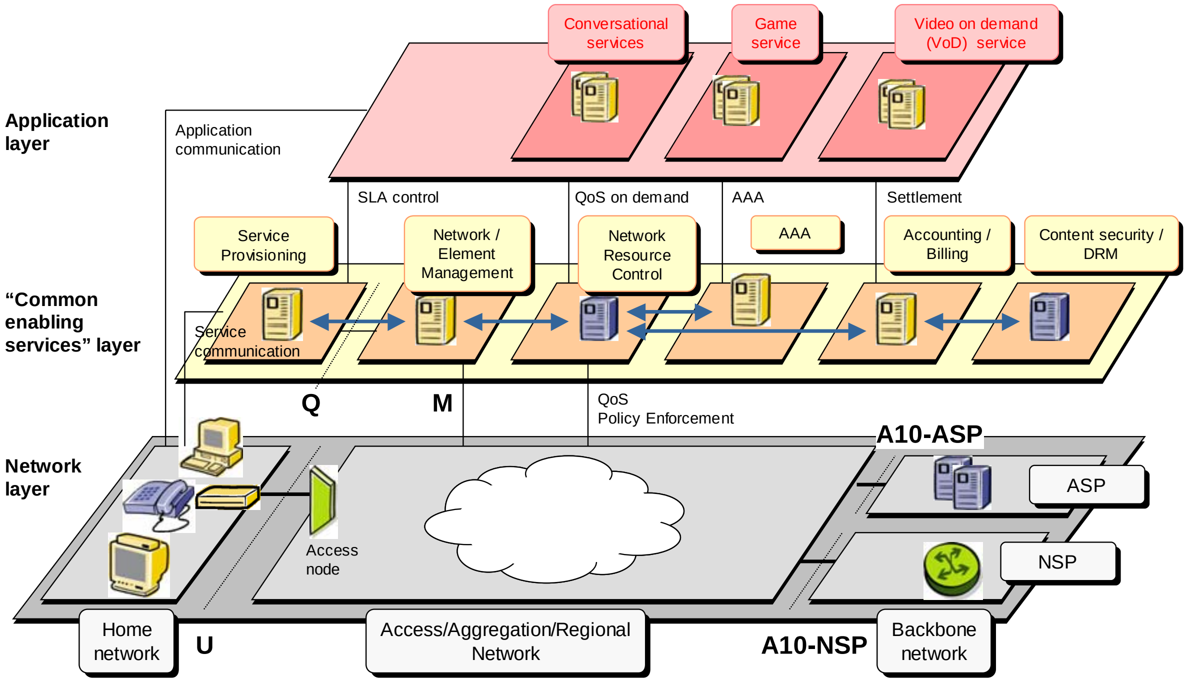


Figure 5 – Three-Layer Management Model

The three-layer model is logical, showing the mandatory and optional functions present in each layer of the architecture for advanced QoS-enabled services delivery. The model does not mandate the implementation of any of these functions in any specific physical network element.

R-106 Broadband Multi-Service architecture MUST support the three-layer logical management model, which includes Application Layer, Common Enabling Service Layer, and Network Layer.

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

7.22.1 Mandatory "common enabling functions" for the Regional/Access Network Provider

R-107 The Common Enabling Service Layer in the Management model of Figure 5 MUST support a Network and Element Management function, that is essential 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, and to the wholesale partners. Additionally, QoS monitoring and SLA verification can be expected to become even more important, especially for the business applications.

R-108 Provisioning individual subscribers MUST NOT necessarily require a per-subscriber L2 construct in the wholesale interface (e.g. per subscriber VLAN).

R-109 Broadband Multi-Service architecture MUST support simple migration of subscribers from one ISP to another, with little or no downtime.

R-110 Broadband Multi-Service architecture MUST support customer self-provisioning.

© 2007 DSL Forum. All rights reserved.

R-111 The Common Enabling Service Layer in the Management model MUST support setting of policy rules for traffic coming from different ASPs.

R-112 The Common Enabling Service Layer in the Management model MUST support management of Accounting and Billing.

R-113 Network Resource Control must be able to generate triggers for accounting purposes.

R-114 Network resource control must be able to interact with accounting and billing functions as part of resource reservation policy decisions.

R-115 Broadband Multi-Service architecture MUST support a new set of network management and billing interfaces which can be used by both service providers and subscribers.

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.

R-116 The Common Enabling Service Layer in the Management model MUST support a Common Data Model for managing the service including keeping track of the parameters associated with subscribers and service providers.

R-117 Broadband Multi-Service architecture MUST support service providers being able to query the network and see how their subscribers are provisioned.

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 access 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 section 7.22.4 for more examples of the types of data expected to reside in the data repository. Much of its value-add is enhanced through the adoption of the same data model by many RANs and many network operators.

7.22.2 Optional "common enabling functions" 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;

© 2007 DSL Forum. All rights reserved.

- **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. Addition of network features that support applications also requires the ability to be able to authenticate the end-devices used to support an application as well as the end-users. Thus, 3 types of AAA must be considered – Network, Device, and User/Application (or content). The emphasis is expected to increase on the latter over time, and mechanisms are needed to enhance the current capabilities of protocols in this area;
- **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, 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.

There are currently diverse requirements for the level of optional features network operators will implement in the near future. Moreover, various ASPs 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 of focusing initially on the features that a network provider must provide in order to deliver the QoS-enabled applications. Without any doubt, the differentiation and enforcement of the new QoS-enabled services brings some new challenges; specifically, the Network Resource Control feature is a crucial piece to cater for the different applications and/or ASPs and to perform accounting if required.

The goal of defining management features is to enable a Regional/Access Network Provider to deploy a flexible mix of the enabling services. This mix can be different depending on the applications considered and therefore, this framework must accommodate different business models applicable to different ASPs.

7.22.3 Policy and Control

Management of the Broadband Multi-Service Architecture is extended beyond the traditional mechanisms to include policy management and control. This approach allows the use of a policy framework to provide flexibility in the management and control planes. Policy can loosely be defined as dynamic configuration based on a set of inputs and/or stimulus plus the ability to resolve the outcome based on the application of a set of rules. This general definition of policy would allow it to apply to almost anything; however this document will narrow the scope of policy to the management and network features. Thus, policy control and management of software applications and their support infrastructure is not in the scope of this document except at the intersection where those applications or their infrastructure overlap with network features or management of the network.

Drivers for policy include, but are not limited to:

- The need to support a policy-enabled NGN.
- The need to change the evaluation rules often or on-the-fly.
- When network interactions need to be guided by user preference.
- When the interactions among application resource requests cannot be determined a priori.
- When tight coupling is desired between application and network, but they remain separate entities.
- When the inputs and preconditions to determine rules are physically and/or temporally distributed.
- When an outcome is based on rules rather than simple settings.
- When an outcome is based on a distributed state.
- When a system is blending otherwise separate applications or capabilities.

In this document, the A10 reference point is extended to support policy control information exchange between SPs, such as ASPs/NSPs, and policy server, the "controller". This allows policy to be pushed from or managed by Service Providers.

R-118 Broadband Multi-Service architecture MUST support policy control and management.

R-119 Broadband Multi-Service architecture MUST support an information model that abstracts various network instantiations from the application layer.

R-120 Broadband Multi-Service architecture policy framework MUST support development of rules that allow the expression of preferred behavior as established by the RAN provider, ASPs, NSPs, and the end-user.

R-121 Broadband Multi-Service architecture policy framework MUST support capabilities that support NGN capabilities.

7.22.4 End-to-End Service Provisioning

7.22.4.1 Users

Many of the optional middleware functions may distinguish between end-users at the application layer. A classic example is that a single broadband access line may support many users – each with individual e-mail accounts.

The provisioning data that applies to each user includes:

- User Name
- Authentication credentials (e.g. password)
- Access account
- User-specific policy, including:
  - Permitted destinations

7.22.4.2 Access Lines

The provisioning data that applies to each access line includes:

- Access line ID

© 2007 DSL Forum. All rights reserved.

- Maximum bandwidth
- Minimum bandwidth
- Access technology type
- Access Line Policy, including:
  - Maximum number of sessions allowed
  - Permitted destinations (ASPs, NSPs) and associated policy (7.22.4.3 below)

7.22.4.3 Access Sessions

The provisioning data that applies to each access session includes:

- Destination (ASP or NSP)
- Access Session Policy, including:
  - Maximum bandwidth
  - Minimum bandwidth
  - Default protocol
  - Single host or subnet needed

7.22.4.4 Application Service Providers (ASPs)

The provisioning data that apply to each ASP include:

- ASP ID
- IP Address(es)
- Authentication credentials (e.g. certificate)
- ASP-specific policy, including:
  - Bandwidth Characteristics
  - QoS Characteristics
  - Allowed multicast groups

7.22.4.5 Network Service Providers (NSPs)

Because of the changes in how broadband is provisioned and managed, there are more details needed per Network Service Provider. When various choices are 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

© 2007 DSL Forum. All rights reserved.

- Subscriber protocol (e.g. IP, PPPoE)
- A10 Protocol (e.g. IP, L2TP, ATM, Ethernet, TDM)
- Authentication
- IP address assignment
- Transport
- Maximum simultaneous sessions

7.22.4.6 L2 Network Service Providers (off Aggregation Network)

The provisioning data that apply to each Wholesale NSP include:

- Minimum bandwidth needed
- Minimum QoS characteristics
- Various services offered
- Encapsulation Mechanism
- Protocol (e.g. IP, L2TP, ATM, Ethernet, TDM)
- Authentication
- IP address assignment
- Transport
- Maximum simultaneous sessions

7.22.5 OAM Functionality

A part of service level management, OAM functionality used to determine and test network connectivity between the IP edge (BNG) and CPE is of critical importance, and additional business requirements are provided here. Historically, when ATM was used as network transport between a BNG and the CPE application, OAM loop-back-cells were used to check the connection status, support error tracing and to perform similar tasks. The user was identified using the PVC, and for this reason no specific Loop-back Terminal Address was needed. A default address was used that was typically the same for all terminals. This simplified the operations, since Loop-back Terminal Addresses did not have to be configured for every user.

R-122 With the introduction of both hybrid and end-to-end Ethernet technology between BNG and CPE, the traditional ATM-based OAM test capabilities are lost. Similar capabilities MUST be made available for Ethernet technologies, and there is a strong desire that the operational model for using the new capability be very similar to the previous model.

R-123 The architecture MUST support the generation and collection of performance data.

7.23 Service Level Management

Service Level Management is the combination of those processes/actions that make sure that the application will experience the desired behavior, i.e. making sure the requested Service Level Agreement

© 2007 DSL Forum. All rights reserved.

(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 especially important for business services.

R-124 Broadband Multi-Service architecture MUST support Service Level Management that makes sure the requested SLA is met.

R-125 Broadband Multi-Service architecture MUST make provision to support management of service levels as described below.

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 is 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.

7.23.1 Network Performance Metrics

Network Availability - The percentage 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.

Network Reliability - The frequency that the network is down.

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 specified in milliseconds and can be a one-way or round-trip delay.

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.

Packet Loss – The measurement of packets lost in transit through a network as a percentage of the total number of packets offered to the network. Related to message delivery.

Network Jitter – The variance of network latency. Jitter is specified in milliseconds.

7.23.2 Operational Metrics

Mean Response Time - The time it takes the Regional/Access Network Provider to respond to submitted reports of trouble.

Mean Time to Restore Service – The measurement of the Regional/Access Network Provider’s ability to restore service within the negotiated interval.

Ordering System Reliability – The measurement of the consistent availability of the ordering system.

© 2007 DSL Forum. All rights reserved.

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

R-126 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.

R-127 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 policy management mechanism.

7.24 Security in 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 architecture. 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 its potential for exposing security flaws in the network to a large number of potential antagonists or automated agents.

R-128 Broadband Multi-Service architecture MUST be able to provide security functions to its users, to connected providers, and to the carrier’s network itself.

R-129 Regional/access networks SHOULD include security functions at appropriate points in the network, to ensure a scalable security solution. These security functions SHOULD prevent such known actions as denial of service, distributed 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 function balances several competing requirements:

R-130 Security SHOULD be controlled by the entity best able to secure the function.

In a network with divided responsibilities, such as that discussed in this document, 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 the quality of the security occurs whenever the information needs to cross a jurisdictional boundary and be manipulated by another entity.

R-131 Security methods MUST be appropriate for the risk, i.e.:

a. They cannot 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.

© 2007 DSL Forum. All rights reserved.

R-132 The different entities MUST be able to sustain the trust models they represent to their peers.

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 access session 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 access session 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.

R-133 The security functions MUST be flexibly defined in any architecture.

7.24.1 Security functions of the regional network

- 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.
- Security functions inherent in the architecture.
- 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.
- Facilities for specialized security services that Regional Network could provide to the User or NSP/ASP using the architecture.
- Security Information that the Regional Network must provide its partners, or that the partners must provide the Regional Network.

7.24.2 Security Functions of ASP/NSP

- 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.
- The security interactions on the Network/Application Service – the transactions between CPN and NSP/ASP and the Role if any of the regional network.
- Information that the ASP/NSP must have from the Regional Network to do its security functions.

© 2007 DSL Forum. All rights reserved.

7.24.3 Security Functions of CPN

- 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. Notably, there are new business requirements to be able to authenticate the placement and configuration of CPN elements that are associated with applications. For example, there is an emerging business need to confirm the integrity of a set-top-box used to deliver valuable content to televisions.
- 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.
- Information that the CPN must have from the Regional Network to do its security functions.

8 DEFINITIONS

AAA	Authentication, Authorization, and Accounting
ADSL	Asymmetric Digital Subscriber Line
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
B-NT	Broadband Network Termination
BE	Best Effort
BNG	Broadband Network Gateway
BoD	Bandwidth on Demand
BRAS	Broadband Remote Access Server
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
DHCP	Dynamic Host Configuration Protocol
Diffserv	Differentiate Services
DLC	Digital Loop Carrier
DS1	Digital Signal level 1 (1.544 Mbps)
DSCP	Differentiated Services (Diffserv) Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Secure Internet Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Technical
L2TP	Layer 2 Tunneling Protocol
LSP	Label Switched Path
MAC	Medium Access Control
MPEG	Motion Pictures Expert Group
MPLS	Multi-Protocol Label Switching
MS/MD	Multi Session / Multi Destination Service
NAPT	Network Address Port Translation
NG-DLC	Next Generation Digital Loop Carrier
NGN	Next Generation Network
NSP	Network Service Provider
OSPF	Open Shortest Path First
PC	Personal Computer
PHY	Physical Layer

© 2007 DSL Forum. All rights reserved.

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
PVC	Permanent Virtual Circuit
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RBN	Regional Broadband Network
RFC	Request For Comments
RG	Routing Gateway or Residential Gateway
RSVP	ReSource reserVation Protocol
RT-DSLAM	Remote Digital Subscriber Line Access Multiplexer
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLO	Service Level Objective
SOA	Service-Oriented Architecture
SONET	Synchronous Optical Network
TE	Traffic Engineering
TR	Technical Report (DSL Forum)
TV	Television
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
VoIP	Voice over Internet Protocol
WFQ	Weighted Fair Queuing
WT	Working Text

© 2007 DSL Forum. All rights reserved.

9 REFERENCES

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

[TR-039] "Requirements for Voice over DSL", DSL Forum Technical Report, TR-039, March 2001;

[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;

[TR-058] "Multi-Service Architecture and Framework Requirements", DSL Forum Technical Report, TR-058, September 2003;

[TR-059] "DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services", DSL Forum Technical Report, TR-059, September 2003;

[TR-092] "Broadband Remote Access Server (BRAS) Requirements Document", DSL Forum Technical Report, TR-092, August 2004;

[TR-101] "Migration to Ethernet-Based DSL Aggregation", DSL Forum Technical Report, TR-101, February 2006;

[TR-102] "Service Interface Requirements for TR-058 Architectures", DSL Forum Technical Report, TR-102, December 2005;

[G.114] ITU-T Rec. G114, International telephone connections and circuits – General Recommendations on the transmission quality for an entire international telephone connection, May 2000.

[TR-126] "Triple-play Services Quality of Experience (QoE) Requirements and Mechanisms", DSL Forum Technical Report, TR-126, December 2006.

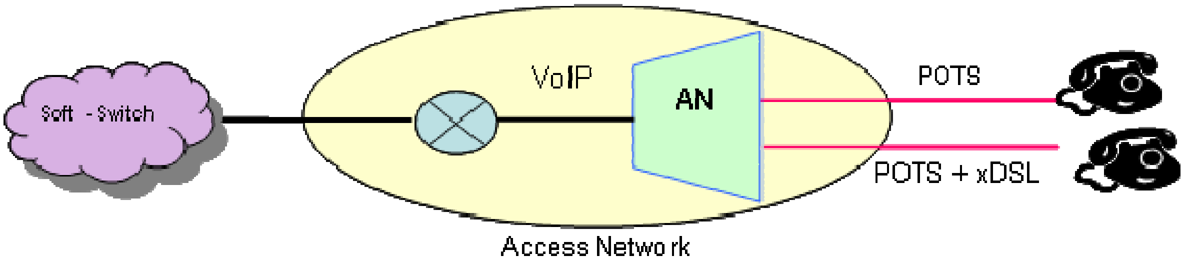
© 2007 DSL Forum. All rights reserved.

APPENDIX A Informative Example of Legacy services

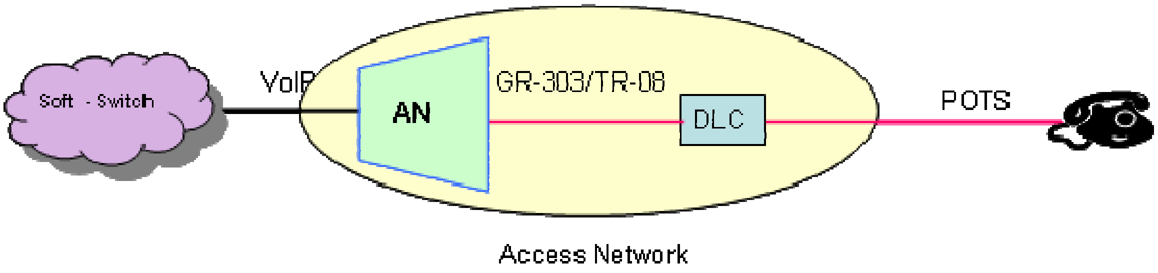
A.1 Voice Services

This section provides some example network scenarios for supporting Voice Services:

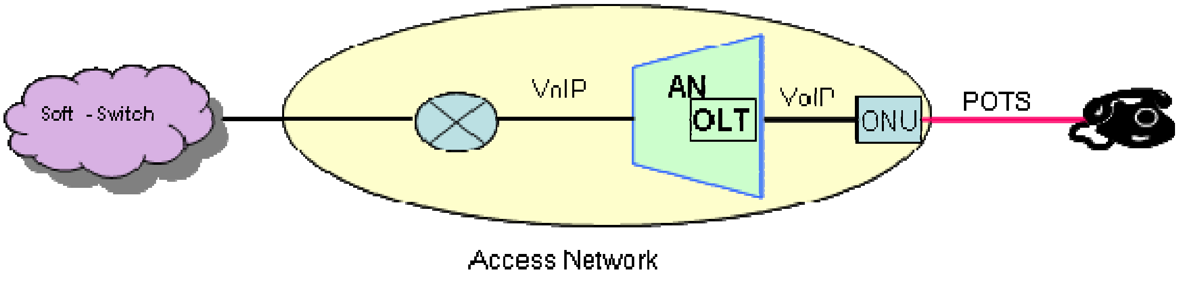
Case a: Connecting POTS to Soft-Switch network: AN performs Edge Packetization function



Case b: Connecting POTS DLC to Packet network: AN performs Edge Packetization function

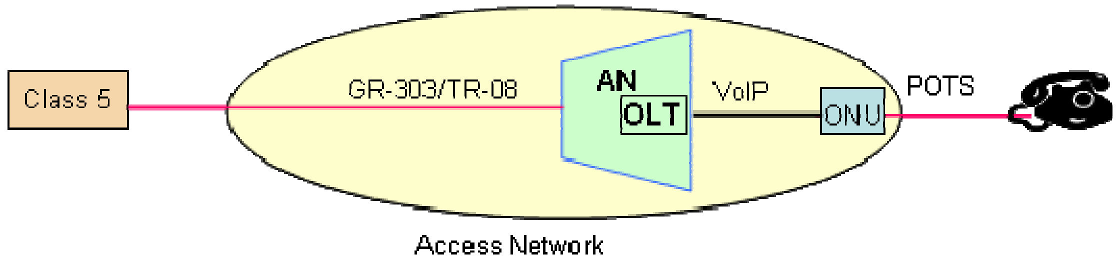


Case c: Connecting POTS to Soft-Switch network: ONT performs VoIP function

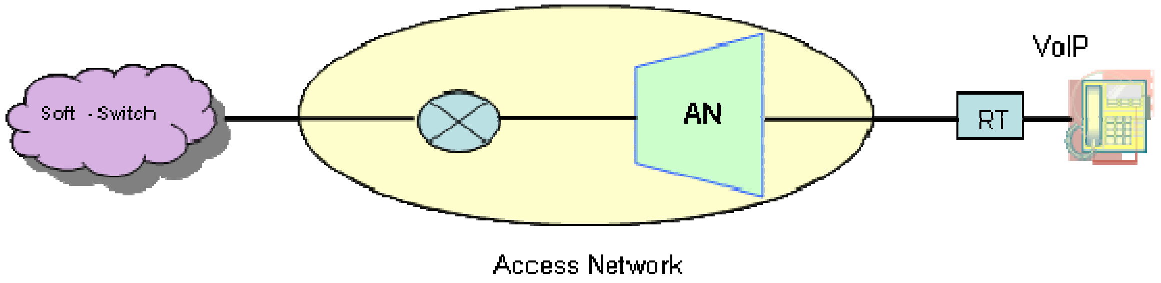


© 2007 DSL Forum. All rights reserved.

Case d: Connecting POTS to TDM network with PON connection (AN can be located at RT or CO)



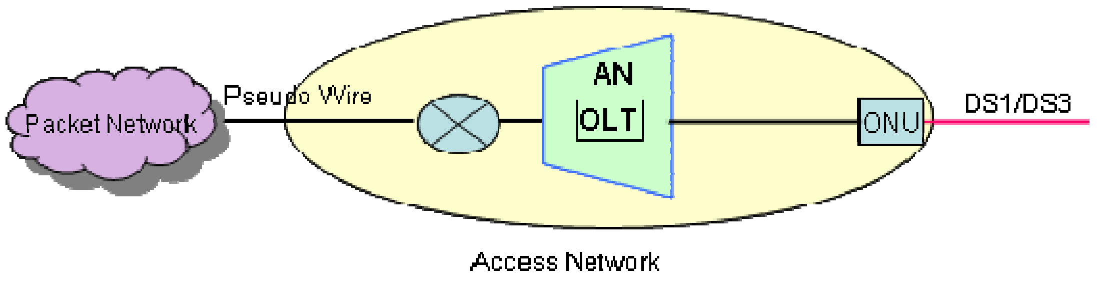
Case e: VoIP End-to-End



A.2 TDM Services

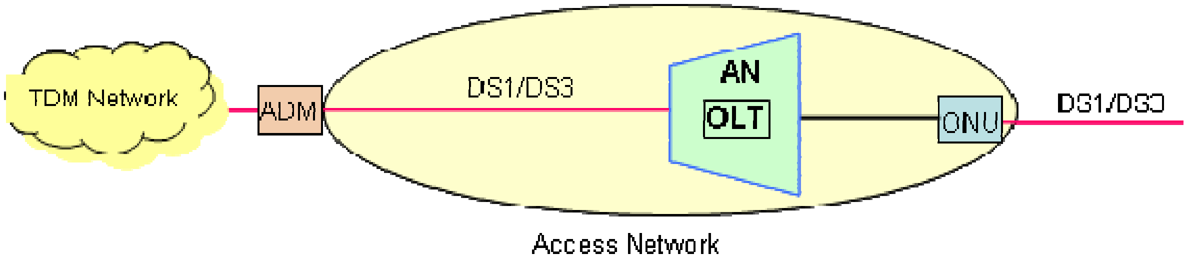
This section gives some example network scenarios for supporting TDM Services:

Case a: Connecting DS1/DS3 to packet network: ONU performs CES over GEM function

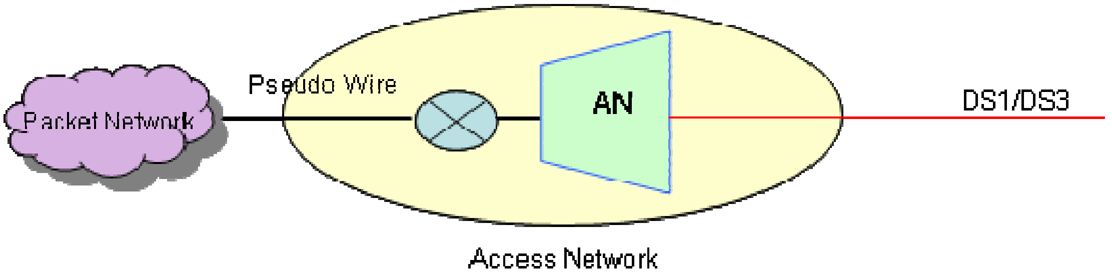


© 2007 DSL Forum. All rights reserved.

Case b: Connecting DS1/DS3 to TDM network: ONU performs TDM over GEM function; and OLT provides TDM network connectivity



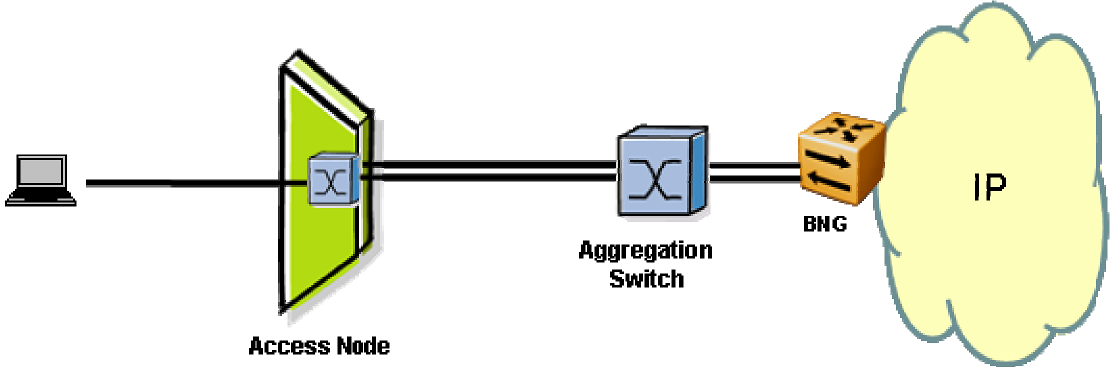
Case c: Connecting DS1 to packet network: AN performs Circuit Emulation function



APPENDIX B Informative Example of Redundant Topologies of Regional and Access network

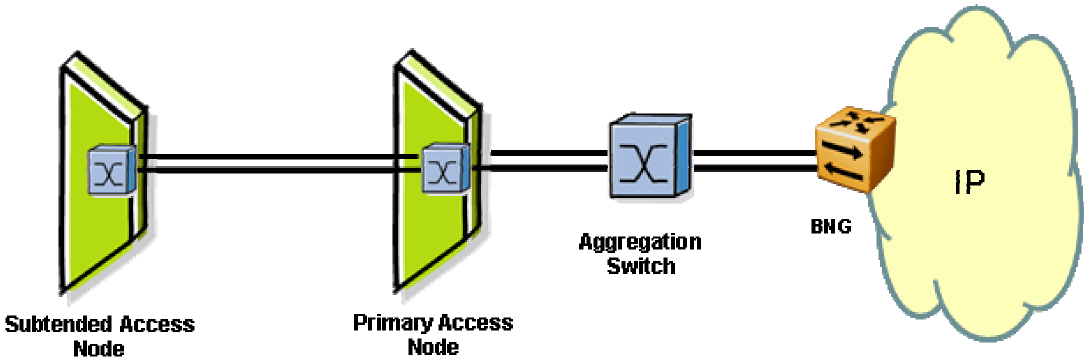
This Appendix offers some example scenarios of redundant topologies. Please note this appendix does not intend to show all the possible scenarios and nor to exclude any other implementations.
Note: in the context of the following scenarios, "Aggregation Switch" represents a function that may be instantiated in a switch or switches, or distributed in the Access Node and/or BNG.

Scenario 1: Redundant links between an Access Node and an aggregation switch

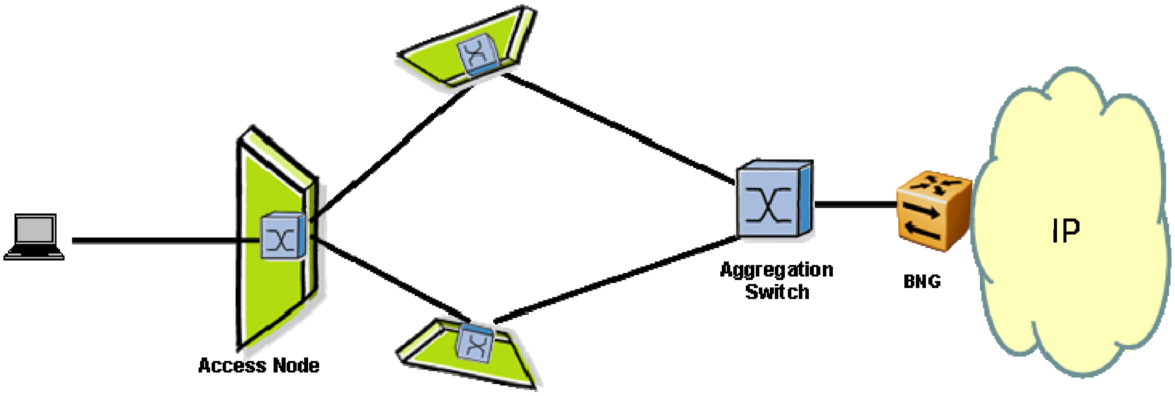


© 2007 DSL Forum. All rights reserved.

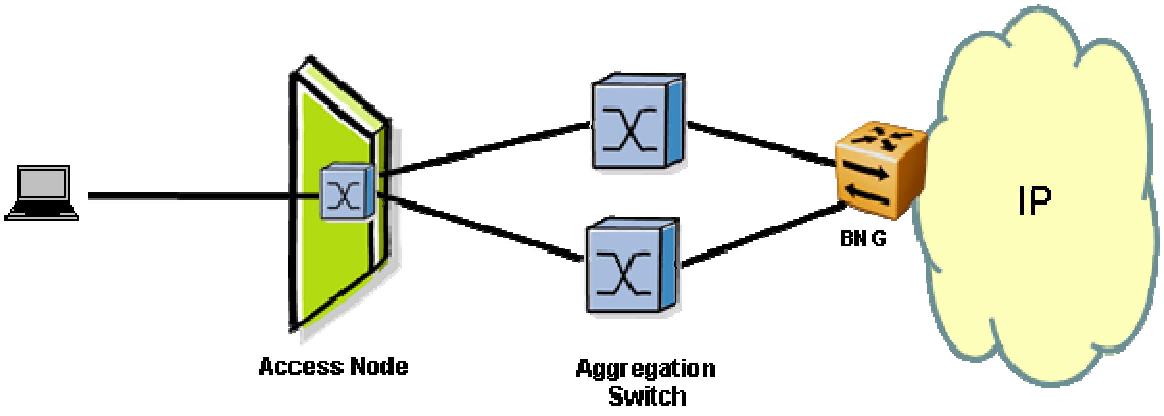
Scenario 2: Redundant links between a subtended Access Node and a primary Access Node



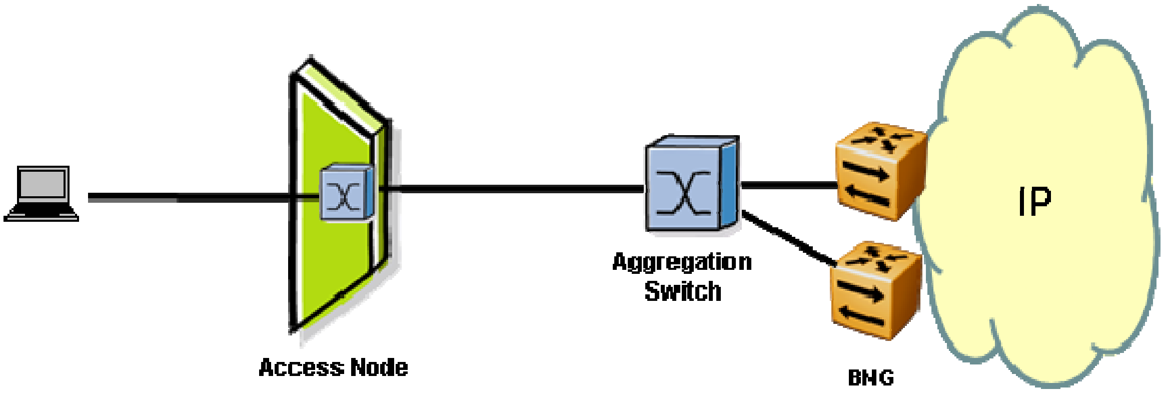
Scenario 3: Ring of Access Nodes



Scenario 4: Redundant aggregation switches connected to an Access Node



Scenario 5: Redundant BNGs



APPENDIX C Informative Access Technologies

C.1 Various DSL technologies

ADSL1 - G.992.1

ITU-T G.992.1describes an asymmetric transmission method for data transport at frequencies above the traditional analog voice service. Compliant modems are typically capable of supporting downstream user data rates up to 7 Mbps and upstream user data rates up to 800 Kbps, using a DMT line code.

ADSL2 - G.992.3

ADSL2 was specifically designed to improve the rate and reach of ADSL, largely by achieving better performance on long lines in the presence of narrowband interference. ADSL2 accomplishes this by improving modulation efficiency, reducing framing overhead, achieving higher coding gain, improving the initialization state machine, and providing enhanced signal-processing algorithms. As a result, ADSL2 provides 5% to 10% higher bit-rates than ADSL1 for both upstream and downstream transmission on most loops, and an even greater improvement for some loops with bridged taps.

ADSL2plus - G.992.5

The ADSL2plus recommendation doubles the downstream bandwidth by extending the usable transmission band up to 2.2 MHz and achieving rates up 24 Mbps downstream. The upstream capacity of ADSL2plus is the same as ADSL2, up to 800Kbps.

SHDSL - G.991.2

G.991.2 SHDSL transceivers are capable of supporting selected symmetric user data rates in the range of 192 Kbps to 5.696 Mbps, using a Trellis Coded Pulse Amplitude Modulation (TC-PAM) line code. G.991.2 modems can be configured to operate at longer ranges than most of the existing DSL technologies, while maintaining spectral compatibility with all other DSL technologies when regional spectral deployment guidelines are followed.

VDSL1&2 - G.993.1 and G.993.2

The ITU-T consented the VDSL2 recommendation G.993.2 in 2005. The VDSL2 recommendation borrowed the best from the ADSL2 and VDSL1 (ITU-T G.993.1) recommendations. To address the distinct needs for markets in different parts of the world, G.993.2 (VDSL2) contains several profiles. One profile (30a) specifies a transmission bandwidth up to 30 MHz that can provide up to 100 Mbps downstream and upstream on very short lines. Another profile (17a) enables services for street cabinet installation with bandwidth up to 100 Mbps downstream and 50 Mbps upstream. The 12a profile provides up to 50 Mbps downstream and 30 Mbps upstream, and is intended for intermediate length lines. The 8a profile provides up 50 Mbps downstream and 12 Mbps upstream while providing service on lines as long

© 2007 DSL Forum. All rights reserved.

as 6,000 feet at lower bit rates. With DMT modulation, trellis coding, and larger error correction capacity, VDSL2 provides high performance for short to medium length lines. Notably, VDSL2 allows operator selection of ATM or Ethernet native transport. With many operators eager to use Ethernet end-to-end, it is expected that VDSL2 will be used in deployments where an ADSL technology could also work, but doesn't provide the desired native Ethernet transport.

G.Bond

G.BOND is used to increase the data rate in proportion to the number of pairs that are bonded. This means that applicable to all DSL technologies, the standard series allows a service provider to multiplex various data streams via ATM transport (G.998.1), Ethernet transport (G.998.2) or TDM (G.998.3) over multiple DSL links.

C.2 Fiber Technologies

B-PON

The ITU G.983 standard, based on ATM technology, specifies symmetric transport at 155 Mbps, and asymmetric transport of up to 155 Mbps upstream and 622 Mbps downstream bandwidth shared by up to 32 individual optical network terminals (ONTs) by using a passive splitter. Depends on the business model on how deep a service provider wants to deploy fiber to the network, different variations of FTTx systems, such as fiber to the home or Premise (FTTH/FTTP), fiber to the node (FTTN), and fiber to the curb (FTTC), etc., have been considered.

E-PON

One of the outgrowth PON technologies of BPON is Ethernet-based PON (EPON). In June 2004, the IEEE ratified EPON as the IEEE802.3ah standard supporting 1 Gbps of bandwidth.

G-PON

The other outgrowth PON technology of BPON is Gigabit PON (GPON), developed as a migration path from the BPON standard to next generation networks. GPON standard defines the downstream bit rate at 1.244 Gbps and 2.488 Gbps, while upstream rates are 155 Mbps, 622 Mbps, 1.244 Gbps, and 2.488 Gbps. In addition to the bandwidth improvement, GPON also enables the transport of multiple services, specifically data and TDM, in native formats and with extremely high efficiency.

Point to Point FTTx

Point to Point FTTx uses point-to-point fiber connection to the premise, to the curb, or to the node instead of using passive splitters in the field. It uses various drop technologies, such as, xDSL or Ethernet to bring the connectivity to the subscribers. Using Point-to-Point FTTx, instead of sharing bandwidth among multiple subscribers, each end user enjoys the dedicated full bi-directional bandwidth.

C.3 Wireless

The original WiMAX standard, IEEE 802.16, specifies frequencies in the 10 to 66 GHz range. 802.16a added support for the 2 to 11 GHz range, of which most parts are already unlicensed internationally however some still re.quire licenses. The WiMAX specification improves upon many of the limitations of the WiFi standard by providing increased bandwidth and stronger encryption. It also aims to provide connectivity between network endpoints without direct line of sight in some circumstances. It is commonly considered that spectrum under 5-6 GHz is needed to provide reasonable NLOS performance and cost effectiveness for PtM (point to multi-point) deployments.

The most common wireless access technology for broadband services is IEEE802.11 (also known as WiFi/WLAN). It is designed for distribution in flats and houses as first/last meter technology and is connected with a wired technology to the access network.

© 2007 DSL Forum. All rights reserved.

<End of Document>

© 2007 DSL Forum. All rights reserved.