Technical Report

DSL Forum
TR-102

Service Interface Requirements for TR-058 Architectures

December 2005

Produced by:
The DSL Forum

Editor:
Tom Anschutz, BellSouth

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

Abstract:

This Technical Report supports the business requirements prescribed in TR-058 and outlines a service framework for mass-market DSL service providers to deliver multiple levels of bandwidth and QoS-enabled services to DSL subscribers. In support of this service evolution, a reference architecture and supporting usage cases are included that exemplify the interface specifications needed from a subscriber or a service provider to access these new services.

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 consensus of members of the DSL Forum. This document is not binding on the DSL Forum, any of its members, or any developer or service provider involved in its making. The document is subject to change, but only with approval of members of the Forum.

Table of Contents

Table of Figures

1. PURPOSE AND SCOPE

1.1 Purpose

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

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

While adopting an architecture, like TR-059 or others, may partially fulfill these needs, there is also a critical need to provide a standard message interface among service providers in order to request changes in these variable services.

This technical report specifies a set of interface interactions among service providers in order to facilitate the variability desired in many of the network services. It also exemplifies and justifies the interface capabilities with a set of typical, exemplary application usage cases. While the cases are not expected to be complete or exhaustive, it is believed that they represent a complete set of functionality and suggest a typical usage pattern that should improve interoperability and commonality across various service providers as well as various potential supporting architectures.

Therefore, The purpose of this work and the usage cases is to provide a common set of service interfaces and interactions to address the critical needs described earlier. Adhering to this specification and to the services and service models set forth both here and in TR-058 simplifies and unifies the way for all types of service providers to obtain ADSL end-user customers whether they sell access to networks, applications, or content.

The anticipated outcome for employing this specification, as well as others that build from it, is that it will:

- Reduce the number of alternative interfaces to ISPs/ASPs and end users, in order to reduce costs through common interconnection.
- Establish guidelines for developers and suppliers, so they can build equipment and services that support common interactions.
- Improve the ability to introduce end-to-end services and applications worldwide, so that similar services can interwork across various service providers' networks.

1.2 Scope

This document presents an architecture for evolving DSL deployment and interconnection including the L2TP Access Aggregation (LAA) and PPP Terminated Aggregation (PTA) architectures defined in TR-25. It outlines a common methodology for delivering QoS-enabled applications to DSL subscribers from one or more Service Providers. The business framework and drivers justifying this architectural evolution are described, in part, in TR-058. In the largest sense, the scope of this architecture is to provide IP-QoS and more flexible service arrangements to millions of users and thousands of service providers. And to do this to a useful extent, while pursuing only economic enhancements to existing ADSL networks.

While ADSL is useful for mass markets, segments and niches – this architecture addresses the mass market specifically. The approach, service models, and architecture are intended to scale to thousands of service providers, and many millions of end-users. The architecture does not detail approaches and techniques that might be appropriate to segments and niches, but does recognize that they might also be used in concert with this approach. Similarly, local regulations, e.g. wiretapping, might apply to this and any architecture, but are beyond the scope of this document.

Many of the requirements levied on network elements and management systems are collected in this architecture, but they should not be taken as an exhaustive list of requirements for such elements. It is expected that other documents and standards will come forward to collect the requirements here, as well as those from other markets, segments, and niches in order to provide complete requirements for elements and systems that wish to be suitable in the DSL industry.

This architecture provides a high-level, evolving view of ADSL access. Because of this it provides more details about things that will happen sooner and fewer details about things that are several years and phases from fruition. Also, unlike a design, this architecture does not provide exhaustive instructions on how to develop and deploy networks or elements that adhere to the architecture. In fact, it identifies the need to develop and standardize new functions, features, and protocols in many later-phase areas.

1.3 Requirements

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

MUST This word, or the adjective “REQUIRED”, means that the definition is an absolute requirement of the specification

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighted before choosing a different course.

MAY This word, or the adjective “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2. INTRODUCTION

This Technical Report follows up on capabilities prescribed in TR-058 and follows the following format.

First Section 3 provides context for the framework, including business models, session types, flow classification, bandwidth sharing and QoS business models.

Next, Section 4 provides five exemplary usage cases demonstrating the operational application framework: Videoconferencing, Video on Demand, Turbo Button, Gaming, and VoIP.

In Section 5, the high level application flows from the usage cases in Section 4 are broken down into a common set of detailed network flows showing how the activities involving the Regional/Access Network (RAN) might be accomplished. This includes new information on the involvement of network elements (DSL Service Manager, database, etc.). Clearly, this is exemplary – as many different network management frameworks are possible. In particular, the message interface is seen as a simple and accessible interface to a potentially more complex policy management framework, like IMS (IP Multimedia Subsystem – defined by 3GPP)

Finally, Section 6 defines the message interfaces and a basic set of QoS and bandwidth capabilities in conjunction with the A10 interface to get at the variable services provided by TR-058.

3. OPERATIONAL APPLICATION FRAMEWORK CONTEXT

The following section provides a context for application services, including Internet access. It documents assumptions and considerations taken into account by the usage cases and provides a broad set of potential approaches to providing variable services at the demand of the customer. First, a set of business models is described, and then the sessions and participants are re-described from TR-058. Following this, the methods by which IP QoS (flows, applications) are categorized is detailed, and then the types of QoS are described including precedence and bandwidth sharing.

3.1 Access Session Types

The TR-059 architecture advances the types and number of access sessions that a subscriber would typically establish to a service provider. Where previously there had been just one access session to an ISP, there are now multiple access sessions with three basic types:

Community NSP – Shown in Figure 1 as the 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 1 as the dashed line between $User_1$ and NSP_2, this type of access session is established between a device within the Customer Premises Network and an NSP. It passes through the RG at the Ethernet (PPPoE) level. 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.

ASP – Shown in Figure 1 as the 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 not a 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. Clearly, ASPs can also have relationships with NSPs – however those relationships and their interactions are beyond the scope of TR-059 as well as this document.

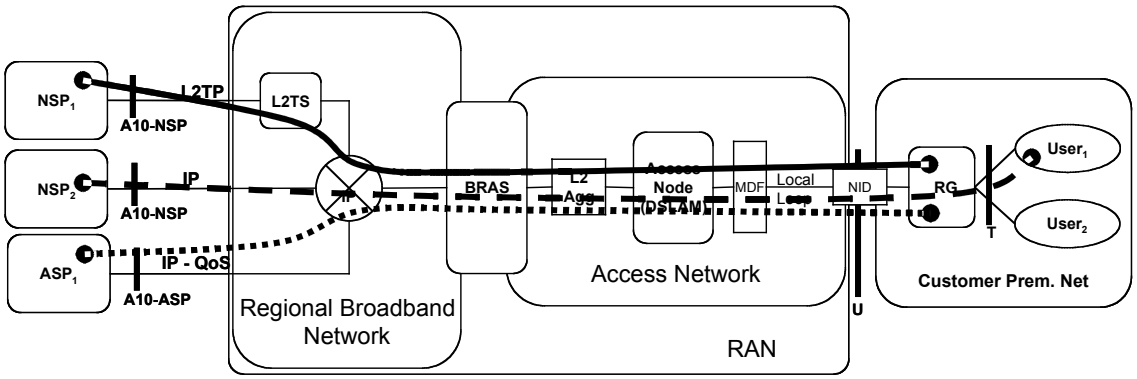


Figure 1 – Access Session Types

3.2 Business Models

The business models that might be supported by the application framework include the following:

1) If a given application were trusted by the RAN provider 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 model, but that it might be 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 RAN provider.

2) If the application were independent of the RAN provider, then a business model would need to be supported with a Bandwidth and/or QoS sales arrangement. This type of arrangement would (theoretically) measure or allocate the bandwidth-QoS to the ASP's systems and would result in models typical of 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. 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 excluded 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 implication 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 assessing a limitation, using an *a la carte* arrangement after that point. This is not unlike many existing cellular telephony business models.

3) For completeness, it should also be noted that 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 and widespread 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 RAN provider for the necessary data transport support to provide that application effectively. For the purposes of the following usage cases, the end-user direct approach will not be considered except as an Internet access feature where bandwidth is applied to any and all applications. Since this approach is independent of the application, it is more easily considered as a separate application and usage case, *Turbo Button.*

3.3 Flow Classification

In the multi-service multi-access architecture defined by TR-059 it will be necessary to identify applications according to their distinct traffic flows. It will also be necessary to identify the access sessions that flows may traverse, and it may be required to identify an application piece-part, or microflow. As sessions, applications, or microflows are given different treatments it will become necessary to assign them to various QoS Classes of service.

In general, these usage cases will assume that applications will be classified as described in *Configuration Guidelines for DiffServ Service Classes* [draft-ietf-tsvwg-diffserv-service-classes-00].

The approach of these usage cases will be to demonstrate that it is possible for the ASP to push packet classifier information into the DSL network at provisioning time so as to configure the DSL network for proper placement of packets from the desired data streams into the appropriate queue(s) in the various network elements that need to support the application flows. Provisioning in this instance relates to the initial setup of the ASP, and is a required first step prior to allowing end users to gain access to the ASPs product offerings.

At the time that the service provider establishes service in the ASP network, they register a profile that describes the treatment that their application should receive. This profile would indicate how to identify their traffic (using IP ports, protocols, and addresses), what treatment their traffic should receive (service class – see draft-ietf-tsvwg-diffserv-service-classes-00), maximum bandwidth, and the business model for that treatment (all-you-can-eat, a la carte, fixed menu). It is possible for ASPs to choose to enhance or limit a specific user, or group, of users. In this case the ASP would initiate a post initial provisioning request to have the specific user or users bandwidth, QoS, or both, modified. This would come over the same A10 interface, but the data elements within the request would be defined to identify said user/users.

Possible characteristics that could be used to identify traffic for treatment include:

- DSCP
- Incoming port/interface
- Source IP address
- Source FQDN

- Destination IP address
- IP Protocol
- Source TCP/UDP port
- Destination TCP/UDP port

In addition to these traditional identifiers, there is also the possibility to classify traffic using an Application Layer gateway (ALG). This approach follows complex protocols (like SIP) and matches the variable ports and addresses that occur in such applications dynamically as they are selected. ALGs are a naturally follow-on to state-ful NAT implementations and are most likely to be available in the RG.

Note that using the IP addresses to identify traffic flows allows for both user-specific as well as default behaviors. For example, if the ASP chose to identify their flows simply by matching the source or destination against their server, then traffic would be provided a default treatment – regardless of the end user that was associated with a flow. Alternately, if the ASP chose to identify the traffic by specifying both the source and destination addresses for traffic both to and from their server, then they would establish per-user classifications, and could specify different values for different customers[1]. In the case where the ASP server is the only attribute known, it is expected that the ASP handles authorization for end users, and blocks any unauthorized users. This would ensure they are not charged for bandwidth associated with these users.

3.4 Business Models for Supporting Concurrent NSP and ASP access sessions

Several economic drivers create the emergence of new business models in addition to the new technology approaches for ADSL.

1. There is an imperative to define new revenue opportunities in the existing technology base without undertaking extensive network renovations.
2. There is a desire to use the ASDL access loop for more than one purpose or connection. The idea is that several NSPs and many ASP applications can all share a single ADSL access line.
3. There is a desire to enhance current wholesale business models so that the Regional / Access Service provider can share in the revenue (as opposed to only the cost) for provisioning the facilities to support high bandwidth applications, like audio and video streaming.

In order to show the business model options, Figure 2 shows several bandwidth relationships that can exist on an ADSL access loop. Note that for the sake of clarity, only a pair-wise relationship is discussed between an ASP application and an NSP access session. In reality, there may be one or more additional Personal NSP access session(s) as well as ASP applications. The principles, however, remain the same.

1 It is appreciated that the user's IP address in this discussion will be variable over long periods of time, and that the method of identifying the user should actually be a reference that remains static – yet gets bound to an IP address when one is assigned. This is a typical BRAS capability that allows mapping user profiles to their interface when it is created – typically at PPP session establishment and using RADIUS.

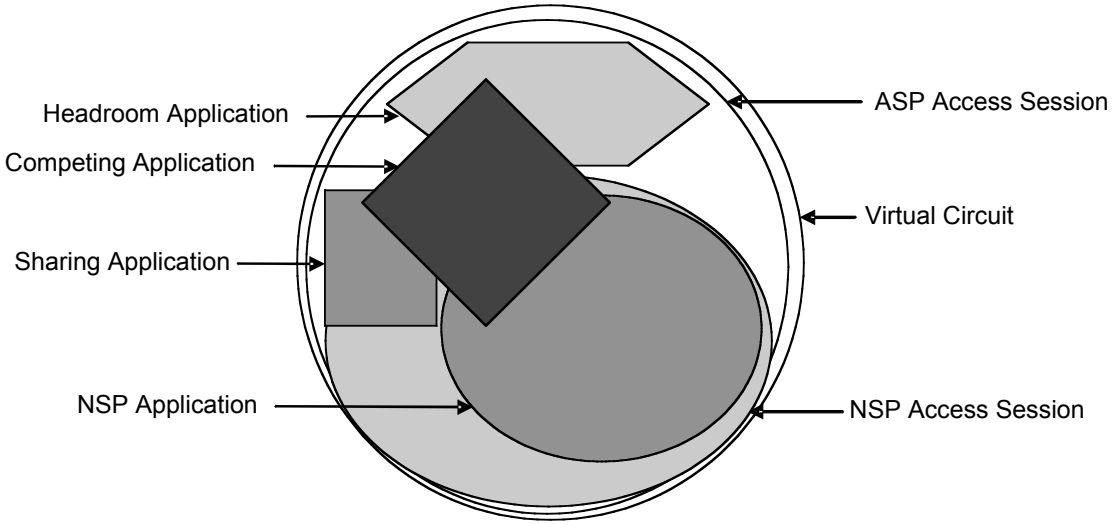


Figure 2 – Bandwidth Business Models

In Figure 2, the outer circle represents the total bandwidth that is available within a VC on an ADSL line after the modems have been allowed to sync to a higher rate than they do today. 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 Virtual Circuit bandwidth. This indicates that the NSP access session is not allowed to access the total bandwidth on the Virtual Circuit. In the past, the NSP Session and the Virtual Circuit would have been the same bandwidth. By increasing the sync rate on the DSL modems, additional bandwidth was 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 ADSL 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.

3.4.1 Simple Bandwidth Partitioning

The first example is the Headroom Application and is shown as a light grey hexagon at the top. This application is allowed to make use of only that bandwidth which the NSP could never access. In this type of model an NSP is provided a dedicated amount of bandwidth on the access loop – even if there is not dedicated bandwidth through the access network. In such an arrangement, ASP applications (or additional NSP access sessions) would only receive bandwidth to which the modems could sync that was over and above the rate sold to the NSP. In this arrangement, if the sync rate were at or below the rate sold to the NSP, no additional applications or access sessions could be provided. This arrangement is unnecessarily restrictive, difficult to implement, and should be strongly avoided.

The second example is the Sharing Application (shown as a dark grey square on the left of the figure). This application has access to all the bandwidth described by the headroom application, but also has access to 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 VC, but can only use the "NSP" bandwidth when the NSP session is not using it. Unlike the previous model, this application can receive bandwidth even when the sync rate is at or below the rate sold to the NSP. However, if the NSP applications are making use of all their bandwidth, then the result is similar to the arrangement described in the Headroom application. This arrangement could be described as work conserving, and should be

the preferred business model for simple bandwidth partitioning.

3.4.2 Priority and Dynamic Bandwidth Sharing

The third example is the Competing Application (shown as a black diamond). In this example, 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. Several cases of competing applications exist:

1. The first case is when a competing application has the same precedence as that of the NSP application(s). In this case, bandwidth is shared fairly according to a typical algorithm, like round-robin, or Weighted Fair Queuing (WFQ). Also, inter-application congestion avoidance mechanisms, like those that are part of TCP can decide how applications would share bandwidth.
2. A second case is when a competing application has greater precedence than that of the NSP application(s). In this case, bandwidth is given to the competing application in strict priority – only "left-over" bandwidth is provided to the other applications. This is the highest QoS level, and is always provided with an upper bound on the bandwidth that the application can obtain: a rate limit. If the application exceeds the upper bound, its traffic will be dropped. This case is the most applicable to a VoIP application because it provides very low latency and because VoIP is not bursty to the point that the rate limit would be exceeded.
3. A third case is when a competing application has a combination of higher precedence and equal precedence. A rate, CIR, is set and the application gets the same treatment as described in case 2 up to that rate. If the application bursts above CIR, then that traffic which bursts is treated differently; it must compete with the other applications as described in case 1.
4. A fourth case is when a competing application has a combination of higher precedence and lower precedence. A rate, CIR, is set and the application gets the same treatment as described in case 2 up to that rate. If the application bursts above CIR, then that traffic which bursts is treated differently; it is treated like a sharing application – only receiving the leftover bandwidth that the NSP application does not use.
5. A fifth case is when a competing application has a combination of higher precedence, equal precedence and a strict rate limit. A rate, CIR, and a second, higher rate, PIR, is set. The application gets the same treatment as described in case 3 up to the PIR rate. If the application bursts above PIR, then that traffic will be dropped.
6. Finally[2], there is a case when a competing application has a combination of higher precedence, equal precedence and lower precedence. As in case 5, a rate, CIR, and a second, higher rate, PIR, is set. The application gets the same treatment as described in case 3 up to the PIR rate. However, if the application exceeds PIR, then that traffic is treated like a sharing application – only receiving the bandwidth that the NSP does not use.

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

4. EXEMPLARY USAGE CASES

The goal of these usage cases is to demonstrate that a TR-058 compliant architecture, like TR-059, and a simplistic policy-oriented operational application framework is sufficient to support many services and to provide the justification for the interface primitives found in Section 6.3. The remainder of the section will

[2] Note that the case where the "competing" application has a lower precedence is equal to the Sharing Application case from the previous section.

show the data flows that are needed among the ASP, DSL Network Provider, and Subscriber locations. Clearly, many similar and dissimilar usage cases are possible – but this TR has included a minimal set that represent both the most popular applications requested by various marketing inputs as well as a set to demonstrate the complete set of A10 network interface interactions.

It should be further noted that some references are provided to near real time updates of policy in the RAN and that these are intended to be accomplished within a few seconds, and, from marketing input, should not take more than 6 seconds to take effect. Most policy updates do not require such stringent times, and can be accomplished during more typical provisioning events. Furthermore, the standard protocols and frameworks for managing policy profiles are just emerging in the DSL Forum and elsewhere, so many of these examples should be taken as requirements for such frameworks and protocols. Finally, in the absence of widespread availability of policy-oriented protocols in the policy enforcement points (RG and BRAS/BNG) it is desirable to leverage existing management and authentication protocols in an ad-hoc manner until proper policy protocols emerge. In this TR, RADIUS, COPS, or LDAP might be used for the BRAS/BNG and TR-068, or SNMP might be used for the RG.

4.1 Videoconferencing

This section details a 3-way videoconference among DSL subscribers with dissimilar access capabilities.

4.1.1 Model

The videoconferencing model used will be a simple provisioned-QoS SIP-driven service implemented by an ASP with a centralized control/mixing conference server. This is the tightly coupled model being developed by an IETF Sipping WG design team[3] that uses four logical entities: focus, conference state notification service, conference policy server element, and stream mixers. This model assumes that an ASP implements all of the logical entities in the video conferencing application, while the DSL network provider just concentrates on the transport and QoS issues. In other words -- the ASP handles all of the mixing as well as the application layer control. A reference diagram for the service with three users is shown in Figure 3. Furthermore, this case makes the simplifying assumption that all the VC users reside in a single RAN provider's network.

3 http://www1.ietf.org/html.charters/sipping-charter.html

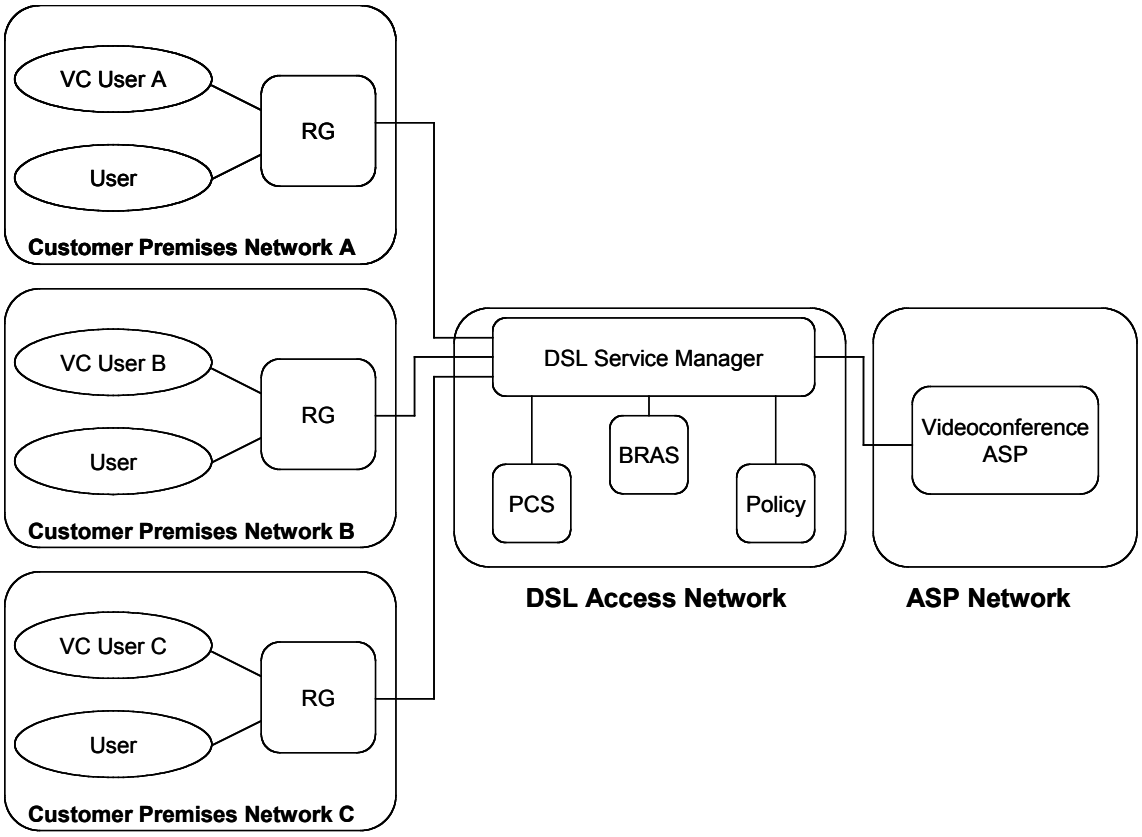


Figure 3 – Videoconference Model

The videoconferencing service has the following very basic capabilities (see Section 4.1.4 for an overview of more sophisticated conferencing capabilities that are beyond the scope of this section).

- Creation/Activation: The user can call the server and either request a reserved conference (without pre-designated participants) or activate a previously reserved conference
- Termination: The conference ends at a pre-designated time
- Adding participants: All users are designated in advance
- Dropping Parties: No parties are dropped.
- Stream Mixing: Basic audio and video mixing are provided. Each participant receives all of the other participants' audio and receives video from the participant with the loudest current audio.

A static provisioning model might impose some restrictions on videoconferencing that desired to send data streams directly among the participants. Fortunately, this example makes use of a centralized mixing function, and it is possible to statically provision a BoD or QoS component for all ASP users communicating with the mixing function. It should also be noted that while it may be inefficient, the mixer could also be present in 2-way calls in order to support this static QoS arrangement. No reservations with network-based BoD or QoS are required before the start of the conference when the QoS provided is relative. If exclusive use of a service class is desired, then there would be a need to provision (or signal) such reservations in the appropriate time-window before a conference started. Similarly, the availability of exclusive resources could also dictate whether real-time adjustment of the schedule (such as adding time to a lengthy conference) is possible.

4.1.2 User Experience

In this application, three users – A, B, and C – set up a videoconference. User A goes to the VC ASP's website and establishes an account. At the website, user A is offered a premium option for the VC app, and chooses to buy it. Users B and C also go to the VC ASP's website, but do not register, only download the required software to participate in videoconferences.

User A reserves a videoconference timeslot on Tuesday from 3:00 to 4:00 and receives a conference ID and access PIN. They then email this information to users B and C.

On Tuesday around 3:00 all three users establish a conference. User A receives the premium experience, and all the users discuss a DSLF usage case, then terminate the conference. Everyone was pleased with application and agree that they will be repeat customers of the VC ASP.

4.1.3 Application Flows

Figure 4 shows the following sequence of events that would occur in the process of registering the ASP VC service, reserving a particular conference, establishing it, and tearing it down once it's over. Assume that three users A, B, and C will be involved in the videoconference and that A will be the *originator*. Numbers in square brackets [1] help coordinate the following descriptive text with the sequential steps in the figures. They are also linked to example network internal operations in section 5.

I. The VC ASP establishes an ASP network presence and, using an *ASP Request* message [3], sets a default conference behavior for all users in the RAN. There may be authentication required for the ASP to set their profile information [1]. Furthermore, several defaults are set for different ASP addresses that support videoconferences at different resolutions and frame rates. Additionally, different business models might be supported, and their salient features might need to be indicated in this step.

II. On the Videoconference ASP website, User A registers to be able to set up videoconferences by setting up their user profile, billing options, etc [8]. They may also obtain, configure, or download the videoconference client application. {Users B and C also gain the ability to videoconference through registration / download [19].}

III. The VC ASP, as part of the registration process for A, queries the RAN for A's capabilities, including maximum bandwidth available [9]. The VC ASP then offers A a premium, high-bandwidth option to see all other participants in a conference at the same time.

IV. In order to exemplify the per-user setting, the VC ASP also sets a profile specifically for user A – again using the *ASP Request* message [11], which establishes a higher maximum bandwidth – just for A.

V. The RGs of users A, B, and C establish PPP sessions between their RG's and the RAN's [5, 6, 7]. This may have occurred long in advance of any conferencing activity, but after the VC ASP has established their defaults. Notably, the RG for user A obtains a VC-specific profile setting from the RAN[4].

VI. User A decides to hold a videoconference with users B and C on Tuesday 3:00-4:00 and arranges this with the VC ASP[5] [16].

---

[4] Alternate mechanisms could be used to obtain the profile, and there is no requirement for PPP to be the access protocol. It is selected for the example because of the TR-059 requirement to use PPPoE for access. Furthermore, initial or simplistic approaches to RG provisioning might include several pre-positioned profiles that do not need to be fetched from a policy server.

[5] This step shows the ongoing need for identity coordination among service providers. While it is not a problem for the VC ASP to identify A using their IP address, B may not be online, and A probably does not know B's IP address. Therefore, there is a need to provide a static, long term identifier for users in the RAN. Possible identifiers include phone numbers (of the DSL line) and user@FQDN. Naturally, these identifiers and the application logic itself will need to be enhanced to support nomadic users.

VII. The ASP checks the availability of local resources to provide the conference at that time. It also queries the capabilities of the other conference parties and offers appropriate VC resolutions and frame rates [17]. The videoconference stream facilities are available and the ASP confirms the conference reservation.

VIII. The videoconference starts at 3:00 on Tuesday. The streams from the users are placed appropriately in the queues by the classifiers, are mixed by the VC ASP, and appropriately mixed streams are distributed to the participants [21, 22].

IX. At 4:00 on Tuesday, the conference is scheduled to end. The VC ASP releases its internal resources for the mixers and conference control, and the videoconference streams are disconnected at the ASP's end.

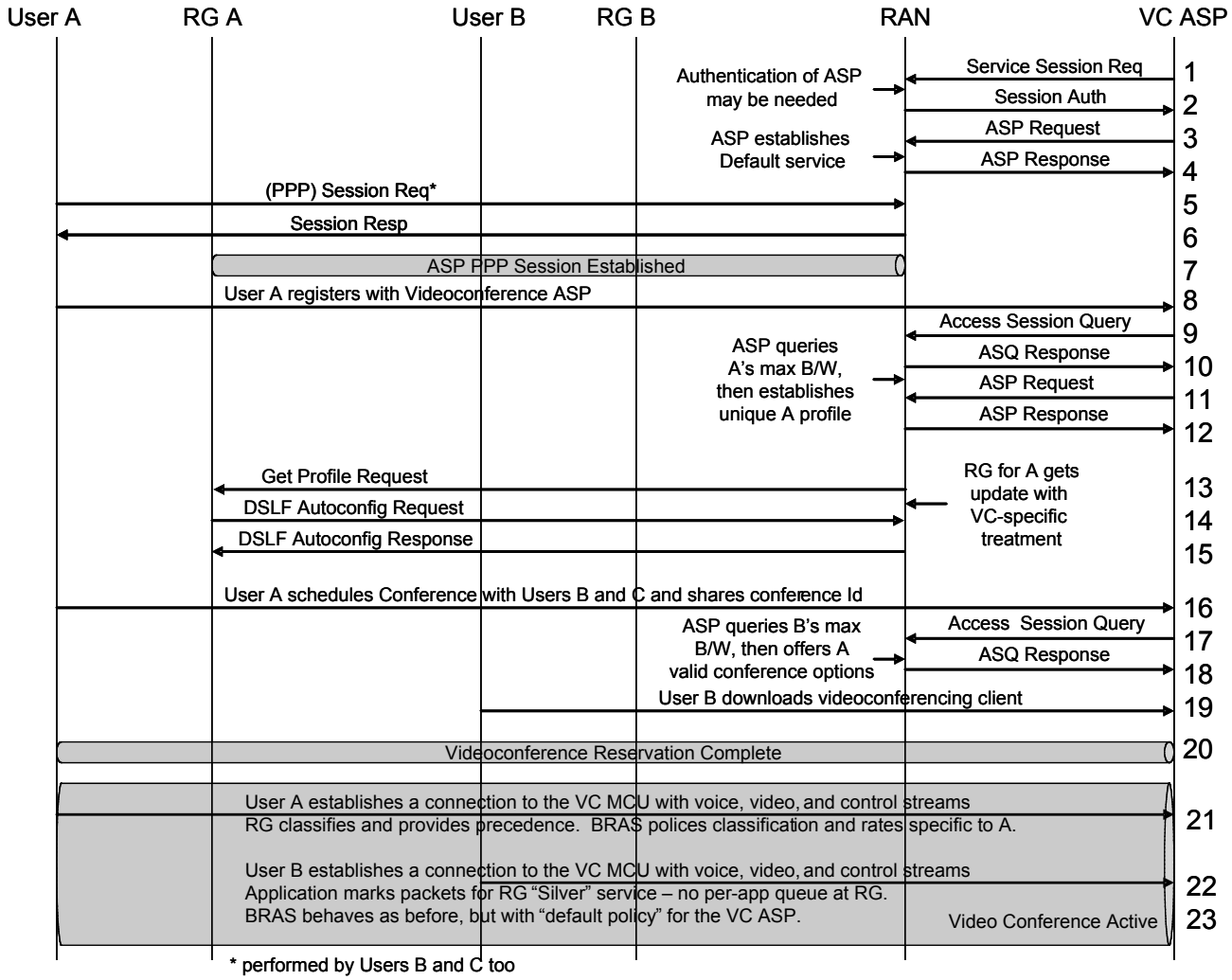


Figure 4 – Videoconference Application Flow

4.1.4 More Advanced Capabilities

In this section, a brief overview of more sophisticated videoconferencing features is provided that was not detailed in this usage case for the sake of brevity; however, analysis shows that these additional features could be supported using the demonstrated approach.

A moderate set of enhancements beyond the minimal subset might include the following capabilities that would require modest application extensions – but no foreseen RAN impacts.

- Privacy: Conference server can add a user without announcing the user's presence and/or identity.
- Conference State: The user can receive full or partial conference state information (i.e., a list of current participants, join announcements, leave announcements, time left, …) either periodically or on demand.
- Recording the conference: This includes the capability to bookmark significant points in the proceedings, e.g., 'here's where we voted Nick off the team").
- Floor control: The conference leader can designate a single current speaker. Only the speaker's video is broadcast. Participants can hear the conference leader and the current speaker.
- Announcement server (human operator access, participant name recording, roll calls)
- Camera control – pan and tilt
- Voting on a proposal raised by a participant
- Collaborative meeting notes, issues list, action item list
- Application sharing
- Focus role migration (no, only needed if conference server is hosted by a participant that wants to hand that role off to another participant).
- Ad hoc termination: The leader can disconnect all of the parties at any time and free up the associated resources.
- Ad hoc dropping of parties: A party can drop out of an active conference. In addition, the leader can ask the server to drop 1 or more parties
- Enhanced video: Multiple streams can be broadcast for "virtual presence"

The following enhancements to the basic viable conference service can use the same model as demonstrated above, but may require that the performance of the ASP request-response transactions approach real time. Specifically, near real time changes in policy and bandwidth queries are required.

- Ad hoc creation/activation: A user can call server and request/activate an ad hoc conference
- Ad hoc adding of participants: (1) A user can "dial into" an active conference; (2) A third party can ask the conference server to add a particular user or users; and (3) The conference server can dial a user and add them (needed for designated participants in reserved conference)
- Side-bar conferences: A participant can start a sidebar. The Subleader can ask the server to add a party to the sidebar. Any party can leave the sidebar. The Subleader can close the sidebar or ask the server to drop a party.

4.2 Video on Demand

This section provides a usage case for Video on Demand (VoD).

4.2.1 Model

The architecture model for VoD is shown in Figure 5.

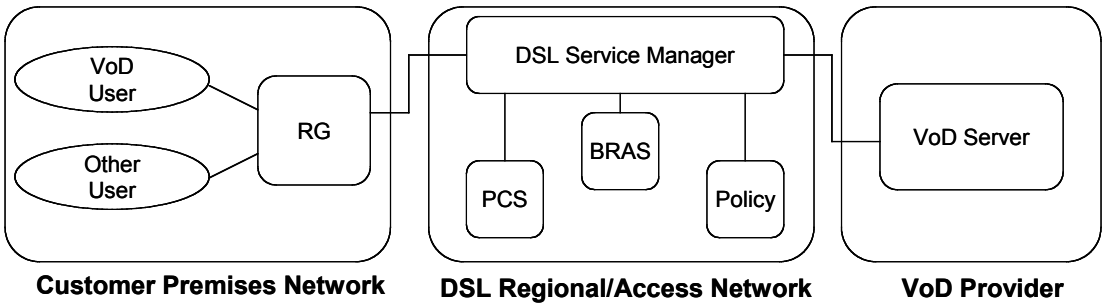


Figure 5 – Video on Demand Model

Initially, the VoD ASP sets up a default VoD profile for all potential customers served by the RAN – this profile will be adequate for effective delivery of the majority of movies to be rendered in regular or high resolution using the buffer and play model. When the end-user requests a movie, the VoD ASP queries the RAN provider to determine the capabilities for that user.

New downstream policies pushed to the RAN will be implemented in the BRAS. In the upstream direction, policy is needed to accommodate the video control and higher layer video ack streams (a worst case estimate for the bandwidth needs in the upstream direction might be 10% of the flow in the downstream direction). Such upstream policies will be implemented in the BRAS; however, it is desirable from the RAN provider's perspective to have the RG perform this shaping first to avoid spoiling the service through shaping the upstream to a potentially lower internet access rate than that needed to support the VoD.

4.2.2 User Experience

VoD allows the end-user to access video content in network servers through their broadband pipe on a transactional basis. The user can choose from a large variety of content without needing to leave the residence or resort to usage of a mail-order service.

This usage case will not discuss the CPE needs of VoD beyond mentioning the need for devices such as home networking, Set Top Boxes, a Personal Video Recorder, etc. that could be used as part of delivering VoD content to any of the 2 to 4 television sets and possibly multiple PC monitors that are present in typical (U.S.) household.

The usage case will involve a simple example of a user requesting the delivery of a movie and, beginning in near real time, viewing it using the buffer & play model. The user will have limited access to VCR-like controls including Rewind, Fast Forward, and Pause. In the buffer & play model, the CPE begins to play out the movie before the entire content file has been downloaded. All that is needed is for a sufficient amount of the movie to have been received for the download of the remainder of the content to be delivered in a time period less than the time it takes to view the entire movie. Later portions of the content sequence are delivered and buffered as an earlier portion is playing. This method typically allows for playback to begin within a few seconds of the beginning of the download. Although this model assumes the immediate viewing of the content rather than storage for future viewing, the viewing rights may be in place for several days, for example.

4.2.3 Application Flows

Descriptions of the VoD application flows for the VoD usage case shown in Figure 6 are as follows:

I. The VoD ASP selects an "all you can eat" business model that provides access to the ASP network via a single Gigabit Ethernet interface (perhaps for a fixed monthly fee to the RAN provider) and allows the ASP to use up to the maximum synch rate for each subscriber.

II. The ASP establishes communication with the ASP network by sending a *Service Session Request* [1, 2]. As part of this step, there may be authentication required for the ASP to set their profile information.

III. Using an *ASP Request* message[6] [3, 4], the VoD ASP sets a default VoD behavior for all potential VoD users served by the RAN. Note that several defaults may be set for different ASP addresses that support VoD at different resolutions and frame rates.

IV. The RAN derives appropriate profile information for usage at all RGs, and sends appropriate information to each RG when they next perform a *PPP session request* [5, 6] to the RAN. At this point, the ASP PPP session is established with default upstream policies in place [7].

V. On the VoD ASP website, User A registers for VoD by setting up their user profile, billing options, etc. [8]. They may also obtain, configure, or download the VoD client application for the STB and/or PC.

VI. At 8:50 PM on Tuesday, User A decides to view "The Matrix Reloaded" in high definition video and requests this from the VoD ASP [16].

VII. The ASP checks the availability of local resources to provide the movie. It queries the RAN for A's capabilities [9, 10], and determines that the resources are adequate for delivery of this movie. Note that different resolution or quality options could be offered depending on the Sync rate of user A – or alternately, user A could be informed of the expected "buffer time" before the movie will start playing. Typically this type of informative mechanism is built into the application itself and is not a function of the RAN.

VIII. At 9:00 PM on Tuesday, the VoD ASP begins sending the necessary audio and video streams to User A [21].

IX. At 11:00 pm on Tuesday, the movie ends. Had this been a different business model, the RAN might process usage information for eventual billing (e.g., number of Kilobytes transported on behalf of VoD ASP / End-user). The default VoD profile for User A is left in place in case they decide to view additional movies.

6 Note that in initial or simplistic deployments, this may also be accomplished using a RAN provider work order or other legacy means.

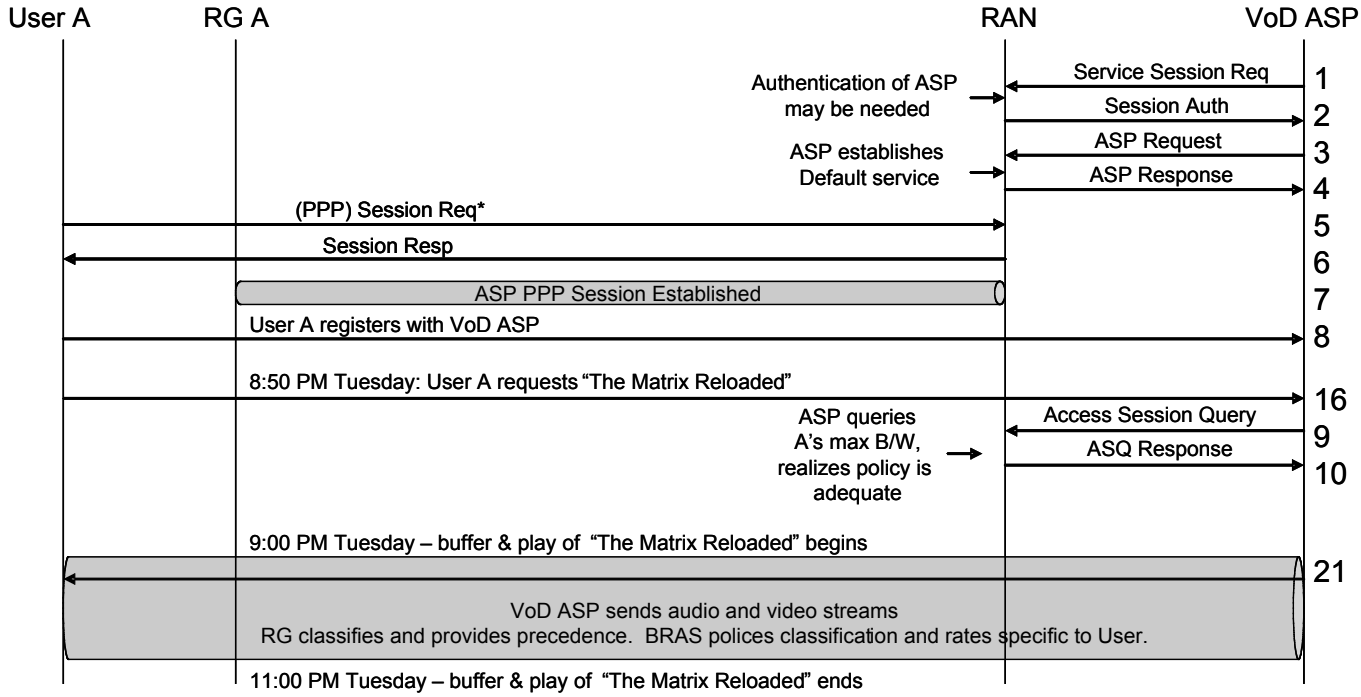


Figure 6 – Video on Demand Application Flow

4.2.4 More Advanced Capabilities

A number of more advanced VoD capabilities have been discussed in the industry that benefit one or more of the stakeholders (end-users, content providers, VoD ASP, RAN provider), including:

- Integration with PVR functionality
- Trickle downloading of likely-to-be-requested content based on usage patterns (using "scavenger class" priority). Scheduling of this activity could be provided through various back-end servers.
- Digital Rights Management enhancements (e.g., unlimited viewing of a movie for up to 10 days; restrictions on copying to secondary storage devices).
- Back Office enhancements (e.g., charging based on movie length or download time; RAN provider wholesale billing of ASP for download bandwidth)

4.3 Turbo Button

A source of frustration for DSL subscribers is that data rates supported by entry-level services (e.g., 256Kb/s downstream and 128Kb/s upstream) are often not properly matched with some application requirements. Although TR-058 allows ASPs to offer their applications at speeds independent of traditional Internet access and could address this issue in that way, many applications (e.g., content download such as large MS Office service packs or movie trailers, and on-line gaming) might not be an ASP, or might not have considered adding value using TR-058. In these cases, the end-user may be interested in using a service that would provide a higher access speed at the times they need it most. This is often called a "Turbo Button" service (TBS). The higher access speed limit provides a higher speed tier or potentially eliminates or lessens artificially imposed limits on the achievable speed altogether. This is applied to the end user's NSP PPP session – so it will affect all the applications and activities that make use of that connection. Note that when the turbo button is pressed on a personal ISP connection – only applications on that "PC" are affected, and if the turbo button is invoked for the community ISP, then all users attached to the home network of the customer receive the advantage of Turbo Button service. The former might be ideal for downloads, and the latter for gaming or LAN parties.

4.3.1 Model

As indicated in the User Experience section, many implementations of a Turbo Button service are possible. For the purposes of this usage case, a simple implementation is presented in which the service is offered by an NSP called myNSP.com. The user requests the turbo button service at the NSP's web site during a browsing session at normal speed.

The NSP will request both the start and stop of turbo service – that is this service will be of the type, "Click-on, click-off" rather than "click for 10 minutes."

The architectural model for Turbo Button service is shown in Figure 7.

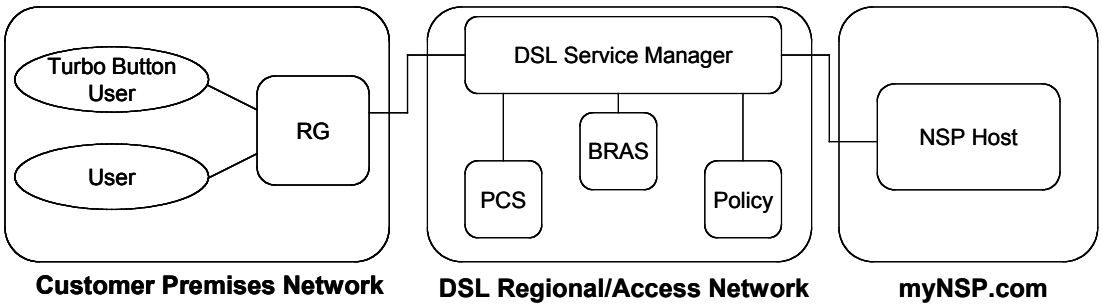


Figure 7 – Turbo Button Model

Once the user requests the turbo service, the NSP queries the RAN to find out what turbo options can be presented to the user. The NSP may map the available upgrades to marketing categories (e.g., fast, faster, wickedly fast). The user selects one of the options, and the NSP requests the profile from the RAN that supports the requested speed. The RAN in turn pushes new policy (e.g., classifiers, rate limiters, priority) into the BRAS and into the user's RG that will support the higher speed. It is important to note that the service is still "Best Effort"; i.e., there is no assumption of a QoS guarantee in this example. A version of turbo button service with QoS support is, of course, possible.

In a typical business model, the NSP might bill the user for usage of the turbo button service. In turn, the DSL network provider would bill the NSP for carrying traffic across the RAN at turbo speeds.

4.3.2 User Experience

Turbo Button service has several possible implementation flavors, each of which would provide a significantly different experience for the end user and other involved players (i.e., the access network provider, the NSP, and the ASP). The following list details some (but not all) of the ways that Turbo Button could be offered.

1. Ordering Method: The user may be offered a choice of ways to order Turbo Button service, e.g., separately from their DSL session with a phone, by using a mass-distributed CD, or within a current DSL session. For the purposes of this document, assume that the user clicks on an advertisement on a web page while in their DSL session and are then taken to a subscription page supported by the NSP.
2. Transience: The Turbo Button service can be permanent (P-TBS) or temporary (T-TBS). In P-TBS, the enhancement would last until the user requests a return to the original access rate (and billing plan). In T-TBS, the enhancement would last only for a certain fixed period of time, after which the default service rate would be re-established.
3. Immediacy of Effect: Depending on how the service is implemented, the time interval of time before the effect of Turbo Button service is manifested might be (1) Negligible, i.e., near real-time invocation within a few seconds; (2) Timed, i.e., to start at a prescribed time that might correspond with a gaming tournament or a "free weekend' for turbo access; (3) Next-Session.

Note that (1) is the only implementation that makes sense for T-TBS while any approach makes sense for P-TBS.

4. Service Level: It may be possible to offer the user a choice of Turbo Button service levels. Gold, Silver, and Bronze levels of service would be offered if multiple speed limits are achievable in the DSL network.

The implementation selections that are made from the above list drive the descriptions of the user and network perspectives of Turbo Button service.

Subscription

Subscribers may be expected to sign up for Turbo Button service after seeing an advertisement online or in the printed/broadcast media. In addition, new DSL subscribers should be able to sign up for Turbo Button service at the time that they subscribe to DSL. The advertisements offering Turbo Button service to new and existing customers must clearly explain how the service is invoked, cancelled, and billed.

The subscriber is billed for Turbo Button service by the NSP (not by the RAN Provider) according to one of several models depending on the billing options in the service profile.

Invocation

Once authenticated by the NSP (using the transport of and possibly with the assistance of the RAN Provider), eligible users of Turbo Button service are permitted to invoke Turbo Button service.

- Permanent Turbo Button service has a merged subscription/invocation operation: the service is invoked at or very soon after subscription (i.e., there is no logical separation between subscription and invocation). The change made to the service profile is in effect until the user unsubscribes.
- In Temporary Turbo Button service however, subscription and invocation are completely different operations since the user subscribes to have the capability to invoke Turbo Button service. Thus, for T-TBS, a means must be established for the user to "push the Turbo button", which may happen multiple times in one session. Each invocation of the service would last some prearranged time after which the service profile would revert to the default settings unless/until the user invokes Turbo Button service again. As indicated above, only users that have subscribed to Turbo Button service would be eligible to invoke the service.

Cancellation

T-TBS invocations would not require canceling since the service cancels itself after a fixed interval of time. However, it should be possible to cancel a T-TBS subscription if the user determines that they are no longer interested in using the service – this would make sense to the user if they are being billed some fixed monthly rate even if they have no usage for a particular month.

4.3.3 Application Flows

Figure 8 shows an example of the sequence of events occurring with using the Turbo Button Service to access sites via a network service provider called "myNSP.com". For simplicity, the details of the RAN (DSL Service Manager, A10 protocol handler, PCS[7], BRAS, etc.) are not shown. The step numbers shown in the figure correspond with the list provided below.

I. The NSP host authenticates itself with the RAN in order to be able to access the customer profiles it wants to update [1, 2].

II. The PPP access session for user A is established in the typical way [5, 6, 7].

III. The user clicks an advertisement to reach the NSP's Turbo Button subscription menu [8].

[7] PCS refers to Policy Configuration System, and is used to mitigate the requirement for an ACS to be able to manage configuration of policy-related information in an RG in near real time. A PCS might be embodied in an ACS or it might be a stand-alone system with similar capabilities dedicated to policy management.

IV. The NSP then queries the RAN for available options for the user's access session connection [9]. It uses the response to this query to put together a set of options for presentation to the customer [10, 8a].

V. The user selects one of the options [16].

VI. The NSP requests the RAN to change the session bandwidth associated with the access session [3, 4]. This change is completed within a few seconds after the end user pushes the turbo button.

VII. Using *Get Profile Request*, the RAN pushes new policy to the RG that will support the turbo speed [13, 14, 15].

VIII. Once the new policy is in place, the user is able to enjoy turbo speed access to sites served by the NSP. Note that all users connected to the access session (i.e., other PC users on the household LAN) would also enjoy the benefits of the turbo button service [21].

IX. Later, the user decides to cancel turbo button service [16].

X. Steps V and VI are repeated with the profile and policy put in place being those needed for default access session speeds [3, 4].

XI. The network has returned to its previous state and the user's PPP session is no longer turboed [21].

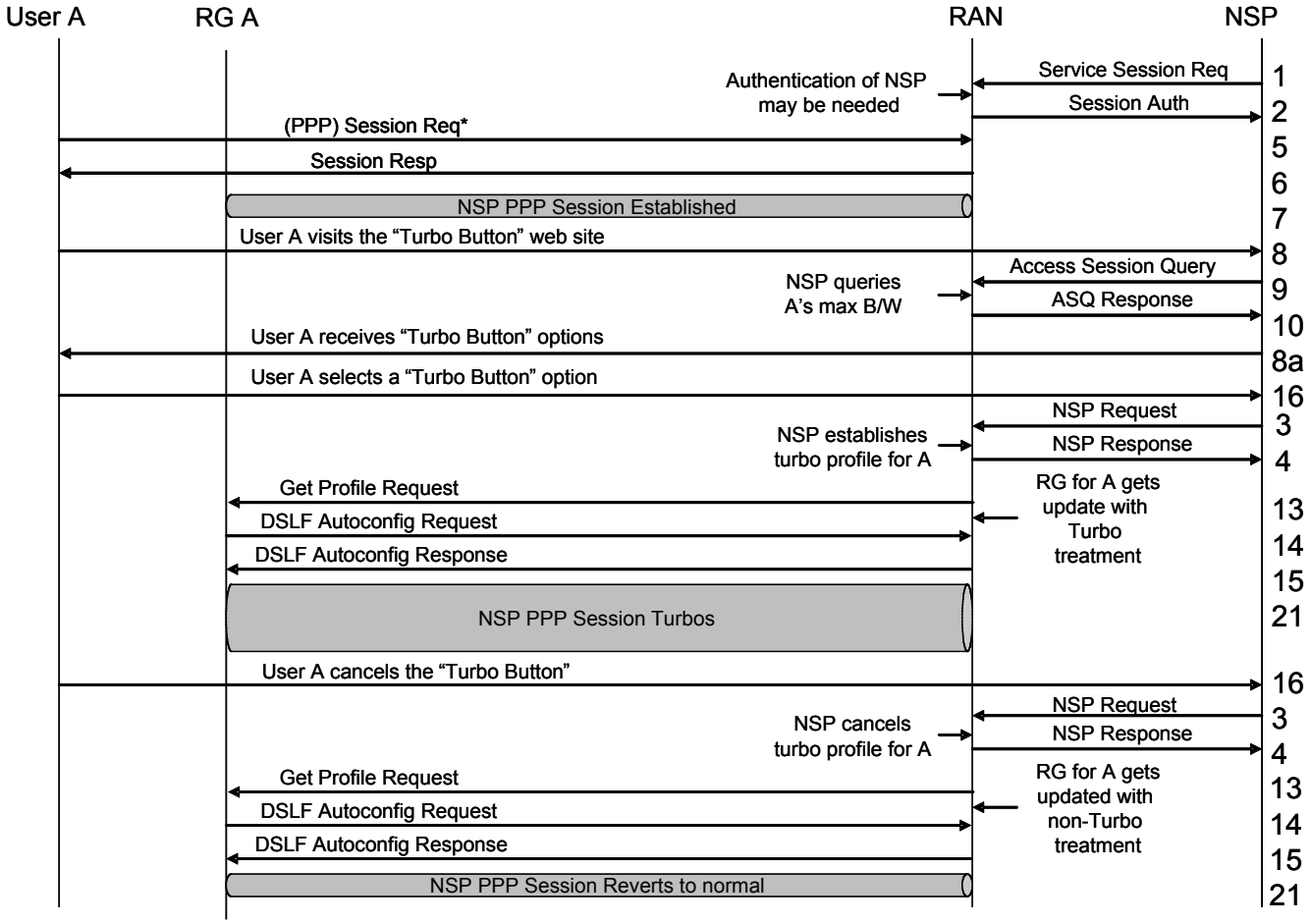


Figure 8 – Turbo Button Application Flow

4.4 Gaming

4.4.1 Model

This section provides an additional illustration of the use of the TR-058 services by showing its application to online gaming. While networked games are not new [9], the confluence of device capabilities and network infrastructure is enabling online gaming to emerge as a significant category of networked applications. Online games can also be generalized as a context [3], [5] for merging interactive communications and entertainment.

Though there are many different models for game play and delivery, this usage case looks at a particular class of games known as “massively multi-player interactive” games. Such games are characterized by substantial numbers of players (greater than 10 and up to the 1000s) and real-time or near real-time interactions. Such games place the significant demands on network and game server infrastructures. Other classes of games that are not discussed here include turn-based games, single player (turn based or real time interactive), and head to head interactive games. Though each of these classes represents a significant number of games available to users, their network requirements are not nearly as complex as those of multi-player interactive games.

In this usage case, a Client-Server architecture for the online game application is being used for the purposes of establishing a concrete example. Other architectures are also possible for this category of applications, but Client-Server has the practical advantage of existence proofs at scale (e.g., [1]), and some analysis of the traffic characteristics [6]. Architectural options and requirements are considered further in [7], [8].

In the client server topology, the client (game workstation) and game server exchange information that is directly relevant only to a specific player. For the purposes of this usage case it does not matter whether the game workstation is a traditional multipurpose workstation (like a PC), or a dedicated entertainment device (like a game console). The game workstation is responsible for such tasks as managing user interactions, rendering, and audio feedback, while the server is responsible for maintaining a consistent view of the game universe and communicating changes to the view to player workstations.

To improve scalability, the client server model may be extended, by, for example, a hierarchy of servers. The difference between the two topologies is one of segmentation. In the hierarchical topology, a server is only responsible for maintaining the state of a portion of the universe. If a player connected to a particular server is interacting with a portion of the universe outside the scope of their immediate server, that server must coordinate with other servers in the network. This partitioning provides significantly more scalability than a simple client server topology. For the purposes of this usage case, a simple client-server architecture is used in order to focus on the interactions across the access network described by TR-59. This service model is show in Figure 9.

Basic game server functionality and auxiliary functions represent a gaming service that could be offered in an ASP model. The game server and servers for auxiliary functions would be connected to the ASP network. Client workstations would access a game server or auxiliary function server through their ASP network connection.

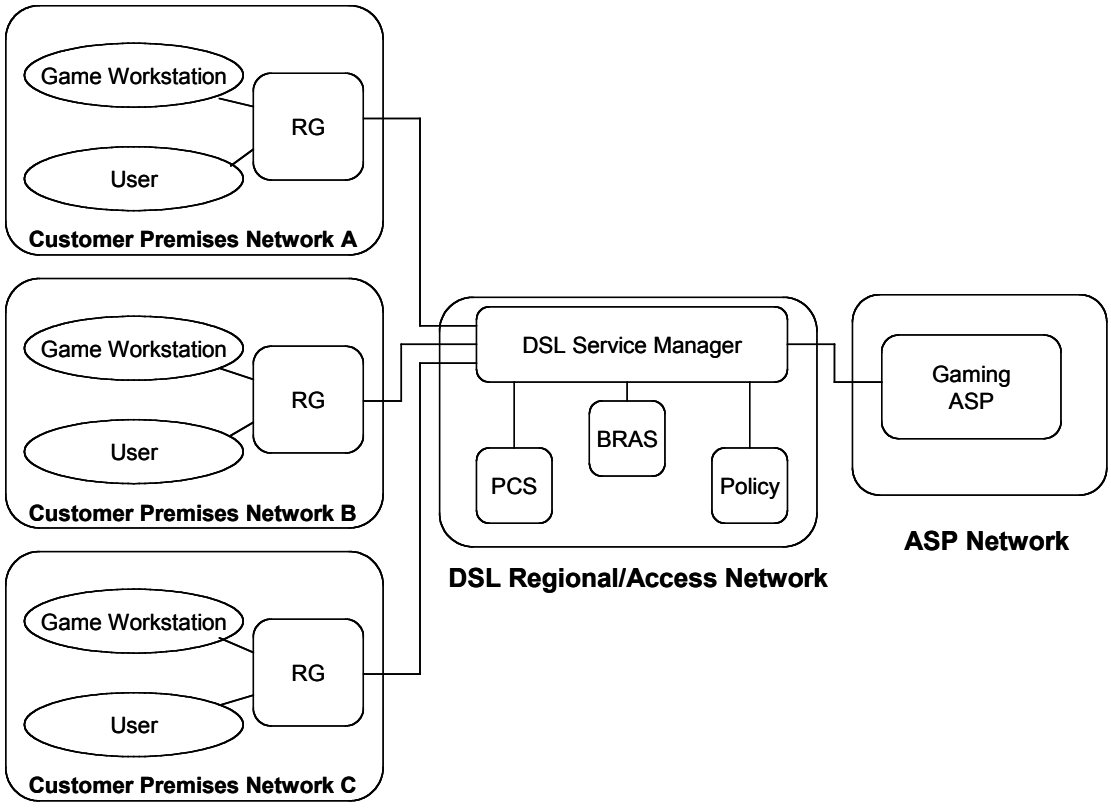


Figure 9 – Gaming Model

From an IP QoS perspective, what is more important is that the online game must be able to coexist with other user applications (e.g. web browsing, e-mail etc.) and permit both applications to receive appropriate QoS treatments.

The goal of this usage case is to demonstrate that TR-059 and a simplistic policy-oriented operations framework is sufficient to support a basic online game service and to suggest areas for further work to establish a complete system. The remainder of the section will show the data flows that are needed among the ASP, DSL Network Provider, and Subscriber locations.

4.4.2 User Experience

In a client/server multiplayer gaming service, the game server and player workstation must communicate state change and play event information in real time. In order to consider the traffic requirements of online games further it helps to further particularize the type of online game. While there are many types of games, one of the more popular forms is generally known as a “First–Person-Shooter” (FPS) games. In an FPS game, the user has a first person perspective of a virtual world and navigates that environment while performing various actions e.g. shooting at bad guys. The workstation must inform the server of player triggered events including the following:

- Player moves.
- Player takes a shot.
- Player changes rooms.
- Player picks up an object.

In a real-time game, the server reconciles these play event messages as they are received from each workstation or peer server. It then communicates state change information to each client workstation. These state change messages contain only information relevant to the particular player – only information about objects currently visible to the player is communicated. Examples of this information include:

- Movement of other objects within the player's current view.
- Hits made by the player.
- Damage incurred by the player.
- Death of the player or other players.
- Communication from the server or other players.

While some standardized gaming data formats and protocols may emerge (e.g., [4] or perhaps MPEG 4/7/21), currently each gaming system seems to define its own methods of communication, but the basic characteristics, seem to be similar. While communication from the workstation to the server is typically event driven, server to workstation communication is often continuous. Servers often send state change messages in frames at a defined rate – 10, 20, 30 frames per second. Frames tend to be significantly larger than voice or video frames, as they need to communicate the current state of the virtual world to the user.

The total time required to send a user event, reconcile its impact on the game universe and communicate state change back to the game workstation becomes the limiting factor in player reaction time. The longer the total time, the less reactive a player can be and the less interactive the gaming experience becomes. Reconciliation time is driven entirely by server capacity and load. Message delivery times are driven by network limitations. For many games, a total round trip "ping" time of 200-350ms is considered acceptable while 100ms is considered exceptional. Anything greater than 500ms starts to become very obvious to the player and is perceived as sluggishness. For an xDSL access network with no queuing delays, the latency is dominated by the packet transit times. As latency increases it becomes more likely that players do not share a consistent view of the universe.

For a "typical" DSL line with 1Mb/s down and 100kb/s up, this corresponds to a latency of ~ 12mS down and ~120mS up for a 1500byte packet, yielding a round trip time of about 132mS. While the specific latency limits will vary with deployment details, TR-59 networks should be capable of excellent performance.

In summary, game play related traffic can be characterized as follows:

- Steady frame rate
- Large frame size (relative to voice or video)
- Latency sensitive

Auxiliary services do not share these characteristics. They are similar or identical to traditional Internet Web based services and do not suffer from significant impacts due to latency.

The bandwidth requirement for game play related traffic is generally lower than for video services, but the latency sensitivity of game play traffic necessitates better than best-effort treatment. Flows related to game play should be placed in an assured forwarding queue at a minimum. Auxiliary services can probably be handled on a best effort basis. Play related traffic and auxiliary service traffic are typically carried in different flows.

For the purposes of this usage case, online game traffic is allocated to AF2 class, and the auxiliary services such as web browsing or email to the BE class.

It is conceivable that traffic within a game play flow could be further differentiated. For example, within the context of a particular game certain events may be treated with higher priority than others. Allowing the application to use and set multiple diffserv code-points could support this. Such use, however, could only be permitted if there was a trusted relationship between the ASP gaming host and the RAN.

4.4.3 Application Flows

The approach of this usage case will be to demonstrate that it is possible for the ASP to push packet classifier information into the DSL network at provisioning time so as to configure the DSL network for

proper placement of packets from the three streams into the appropriate queue as mentioned above in the various network elements that need to support the application flows.

At the time that the online game service provider establishes service in the ASP network, they register a profile that describes the treatment that their application should receive. This profile would indicate how to identify their traffic (using IP ports, protocols, and addresses), what treatment their traffic should receive, maximum bandwidth, and the business model for that treatment (all-you-can-eat, a la carte, fixed menu).

At the time that an end-user of the online game service wants to reserve an online game service instance, the user needs to get a online game session identifier/PIN from the online game service ASP. The user will use this conference identifier to get into the correct service instance, and will give the conference id to the other participants for the same purpose. For the purposes of this usage case, it is assumed that the conference identifier does not need to show up in the data model since it is strictly between the users and the ASP and somehow transferred without concern to the DSL network provider.

The call flow for gaming is simple and similar to Turbo button. The game provider simply needs to negotiate bandwidth profiles between the game server and the player workstation for the purposes of game play traffic. The steps in this scenario are as follows:

I. Subscriber establishes PPP session between RG and DSL network provider [7].

II. Subscriber accesses ASP gaming providers web site and registers for game play [8].

III. ASP gaming provider queries subscriber bandwidth profile and determines current profile to be insufficient for game play [9, 10]. Note that this requires the ASP to authenticate to the RAN [1, 2].

IV. ASP creates application bandwidth/QOS profile at RAN [3].

V. ASP acknowledges subscription [4].

VI. RAN pushes new flow qualifier and bandwidth info for game service to routing gateway [13, 14, 15, 20].

VII. Subscriber joins game using QOS enabled session [21].

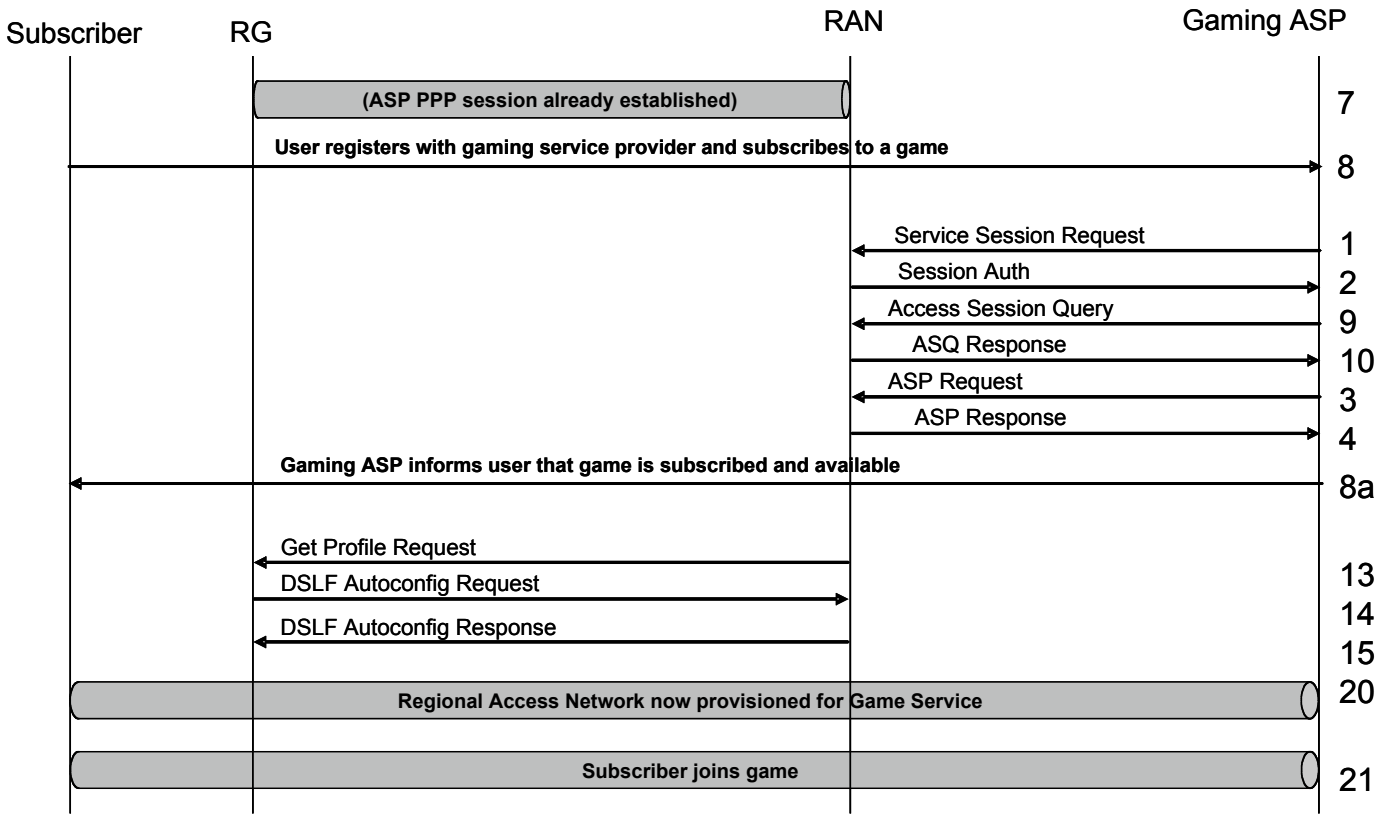


Figure 10 – Gaming Application Flow

4.4.4 More Advanced Capabilities

In addition to maintaining game universe state at communicating state changes to players, a gaming service might provide other auxiliary functions including the following:

- Session Management: manages active player lists, supports ability to invite participants to join a game.
- Presence and availability management: supports the ability of players to locate and determine if opponents are available for play.
- Authentication: verify player identities and validate that players are using correctly licensed software on their workstation.
- Interactive chat and bulletin board: provides a forum for discussion of gaming topics. Can also be used during game play to allow for intra-team communication.
- Content downloads: provides software update and new game delivery services.

However, not all these details are necessarily directly relevant to the TR-059 architecture, some pertain to the game application architecture, while others impact the network flows and require additional functionality within the operational framework of the access network.

4.5 VoIP

This section provides an additional illustration of the use of the TR-059 Architecture by showing its application to Voice over IP (VoIP). VoIP is generally considered the migration of narrow band voice services into an IP network. Once voice is provided though an IP network, it can be integrated with other IP services providing capabilities not achievable or cost effective in the PSTN.

4.5.1 Model

VoIP can take on many different service models. This usage case focuses on a service provider centric (ASP) model rather than a completely decoupled peer-to-peer model. Additionally, the use of SIP as the application protocol is assumed. Figure 11 depicts an exemplary VoIP service architecture used in this usage case. A centralized SIP proxy device is deployed in the service provider's network that handles endpoint registration and authentication, feature activation, and call routing. For connectivity to the PSTN and audio conferencing capabilities, the ASP has also deployed media server/gateway for this function.

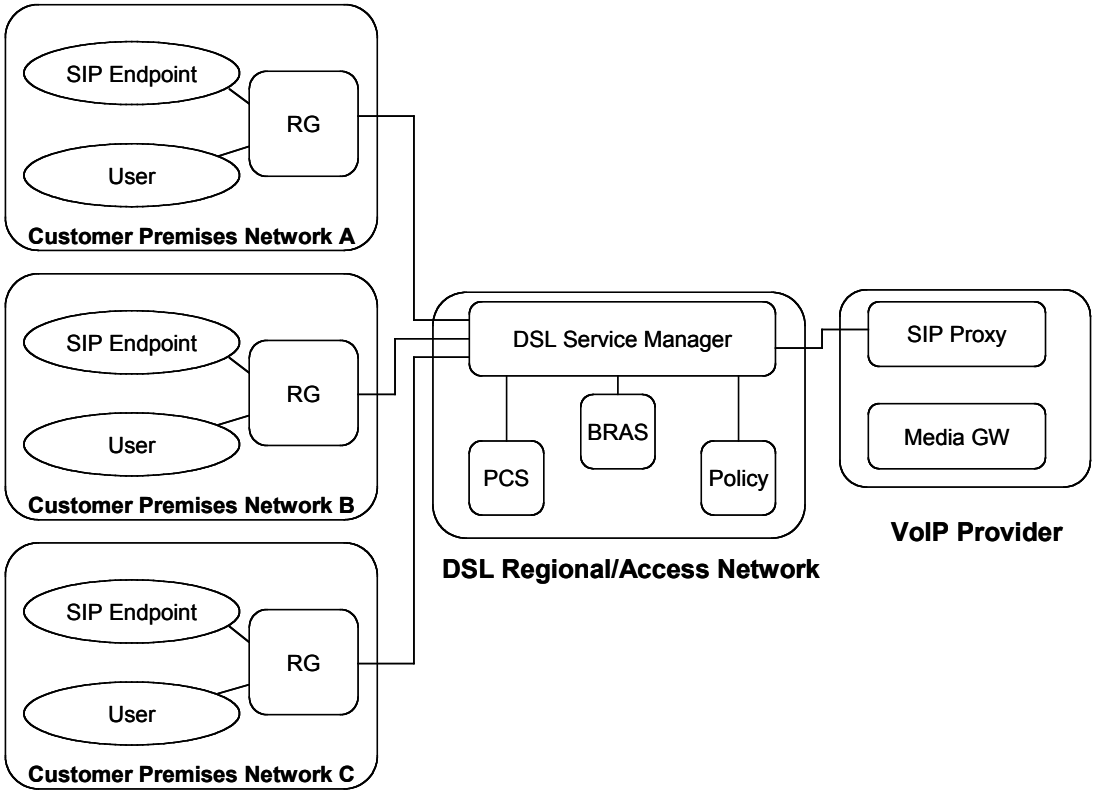


Figure 11 – VoIP Model

The specifics of the calling features associated with the VoIP service are not discussed. Instead a focus on describing the underlying network capabilities that will enable basic call establishment is taken.

Providing QoS and Bandwidth with network based services is rather straightforward. However, VoIP can combine aspects of a network service as well as a peer-to-peer service (signaling vs. Bearer). Similar to the previous SIP based video conferencing example, a VoIP service will use randomly assigned RTP ports to transport the bearer traffic. Call signaling follows a client network server paradigm but the bearer traffic can be either peer-to-peer (SIP phone to SIP Phone) or client to network server (SIP Phone to media gateway). Client to network server flows can be simply classified per Section 3.3 using the destination address of the SIP proxy or media server/gateway. Peer-to-peer traffic cannot be so easily classified given that the dynamic nature of RTP. In the video conferencing scenario, the assumption was made that a network-based mixer (MCU) is required for multi-party calls and that 2-way calls would be configured to use the mixer as well. For VoIP, a similar assumption can be made as well. Presumably, multi-party audio conferencing will be a feature of the VoIP service and as a result a media server (mixer) is required. 2-way calls between SIP users could be routed to the conference bridge providing a well-known IP address that can be used for classification. Alternatives to this approach include:

- Route peer-to-peer calls through a well known network proxy device (presumably less expensive than a mixer because the are no DSPs required)

- Allow the CPE to mark the traffic as VoIP (using the differentiated services code point) and in the network police the bandwidth allocated to that class (i.e. EF) on a per subscriber basis.

For simplicity, this usage case will assume that the CPE will mark the traffic and be policed in the network.

The CPE could be a SIP phone, Analog Terminal Adaptor (ATA), or an Integrated Access Device (IAD) that has a built in xDSL modem. In the non-integrated scenario it is assumed that the RG has ALG capabilities for NAT, firewall, and QoS.

4.5.2 Application Flows

Figure 12 shows the following sequence of events that would occur in the process of registering the ASP VoIP service with a specific user. It is assumed that two users A and B will be involved in a VoIP call. Numbers in square brackets [1] help coordinate the following descriptive text with the figures.

I. The VoIP ASP establishes an ASP network presence and, using the service session request establishes a connection with the RAN enabling it to make policy changes to users that subscribe to its service [1,2]. Given that the RAN will not support the typical voice centric minutes of use paradigm, billing options include:

   a. The RAN charging the VoIP ASP based on the amount of premium bandwidth provisioned in the RAN. For example, a monthly charge per 100Kb/s of configured EF traffic.

   b. A single flat connection recurring connection fee based on the facilities purchased to connect to the RAN (e.g. Gigabit Ethernet).

II. On the VoIP ASP website, the user A registers and creates their user profile, billing options, etc [8]. The user may also obtain, configure, or download the VoIP client application. Other business models might include the ASP drop shipping CPE to the user (IP Phone, ATA, etc). [User B also gains the ability to use the VoIP service through registration/download]

III. The VoIP ASP, as part of the registration process for A, queries the RAN for A's capabilities, including maximum bandwidth available [9]. The VoIP ASP then offers user A different package options (number of simultaneous lines, voice quality options per line, etc).

IV. Once the user selects their desired application package, the VoIP ASP sets a profile specifically for user A –using the *ASP Request* message [11], which establishes a bandwidth and QoS for A's VoIP traffic. Additionally, if the ASP is in the pay by the bandwidth provisioned model, then a billing record would also be generated to capture the amount of bandwidth requested by the ASP.

V. The RGs of users A and B establish PPP sessions between their RG's and RAN [5, 6, 7]. This may have occurred long in advance of any VoIP activity (subscription or call initiation). Notably, the RG for user A obtains a VoIP-specific profile setting from the RAN [13, 14, 15].

VI. User A decides to call user B using the VoIP ASP's service [21].

VII. The ASP verifies that users A and B have active accounts and performs telephone number to IP address mapping and informs B of an inbound call.

VIII. The RTP streams from the users are placed appropriately in the queues by the classifiers in the RG and the BRAS [21, 22, 23].

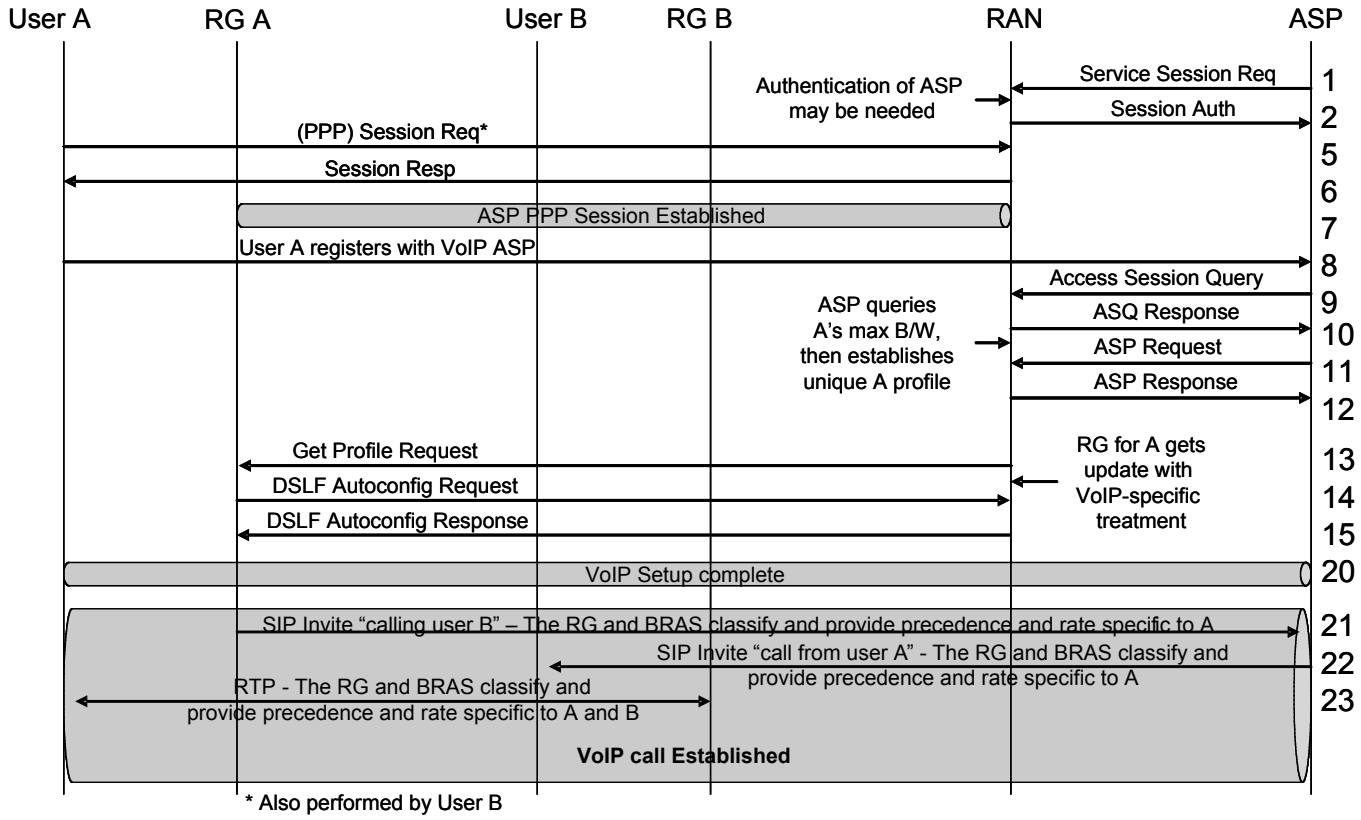


Figure 12 – VoIP Application Flow

4.5.3 More Advanced Capabilities

In this section, a brief overview of more sophisticated VoIP features is provided that were not detailed in this usage case for the sake of brevity; however, it is believed that these additional features could be supported using the demonstrated approach.

A moderate set of enhancements beyond the minimal subset might include the following capabilities that would require modest application extensions – but no foreseen RAN impacts.

- Calls to and from the PSTN
- IP to IP calls across service providers
- N-way audio conferencing. The addition of a conference bridge server would be just another network address associated with the ASPs VoIP service and used for classification.
- Voice mail
- Announcement server (network announcements, human operator access)
- Interactive Messaging or Unified Messaging integration

4.6 Multicast Video

This section provides a usage case for Multicast Video (MV).

4.6.1 Model

The architecture model for MV is shown in Figure 5.

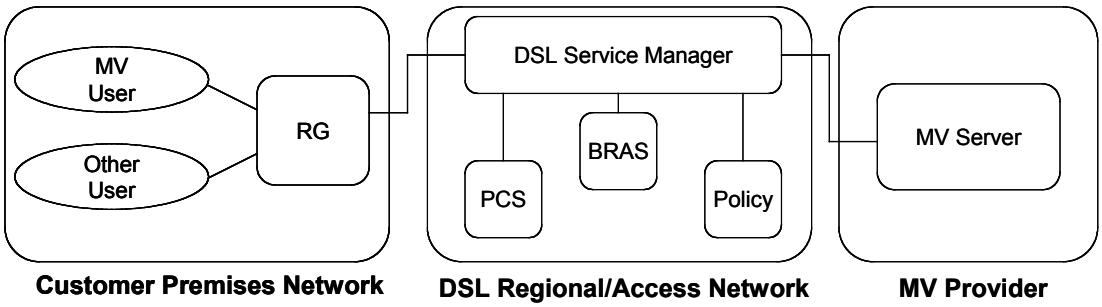


Figure 13 – Multicast Video Model

Initially, the MV Provider (ASP) requests a set of multicast addresses (groups) and establishes their source address as a valid source for the RAN. Then it sets up a default MV profile for all potential customers served by the RAN – this profile will be adequate for effective delivery of the majority of movies to be rendered in regular or high resolution using a multicast streaming model. When the end-user requests a movie, the MV ASP queries the RAN provider to determine the capabilities for that user.

New downstream policies pushed to the RAN will be implemented in the BRAS. These will include provisioning of the newly established multicast group information – including its bandwith. In the upstream direction, policy is also needed to provide QoS for IGMP, the video control and higher layer unicast control traffic – for example DRM exchange and program information.

4.6.2 User Experience

MV allows the end-user to access video content in streaming network servers through their broadband pipe on a (typically) subscription basis. The user can choose from a large variety of content without needing to leave the residence or resort to usage of a mail-order service.

This usage case will not discuss the CPE needs of MV beyond mentioning the need for devices such as home networking, Set Top Boxes, a Personal Video Recorder, etc. that could be used as part of delivering MV content to any of the 2 to 4 television sets and possibly multiple PC monitors that are present in typical (U.S.) household.

The usage case is a simple example of a user subscribing to a multi-channel movie service and watching the movies according to the schedule set by the MV ASP. The delivery of a movie and switching among available movies happens in real time using a streaming multicast model. Unlike VoD, The user will not have access to VCR-like controls from the service. In the streaming model, the CPE begins to play out the movie (actually channel) within about a second of the request. Also unlike typical VoD, the users are able to switch channels without having to subscribe or incur cost. Although this model assumes the immediate viewing of the content rather than storage for future viewing, the DRM and viewing rights may be in place for several days, for example to use a PVR either to obtain VCR functions or to time-shift the movie.

4.6.3 Application Flows

Descriptions of the MV application flows for the MV usage case shown in Figure 6 are as follows:

I. The MV ASP selects a “fixed menu” business model that allows sending 15 multicast channels at a time via a single Fast Ethernet interface (perhaps for a fixed monthly fee to the RAN provider) and allows the ASP to use up to the maximum synch rate for each subscriber. Note that with this arrangement it is extremely unlikely that the ASP can also select an assured bandwidth QoS type.

II. The ASP establishes communication with the ASP network by sending a *Service Session Request* [1, 2]. As part of this step, there may be authentication required for the ASP to set their profile information.

III. Using an *ASP Request* message[8] [3, 4], the MV ASP requests 15 multicast groups for their ASP server address[9] and sets a default MV behavior for all potential MV users served by the RAN. Note that several defaults may be set for different ASP addresses that support MV at different resolutions and data rates.

IV. The RAN derives appropriate profile information for usage at all RGs, and sends appropriate information to each RG when they next perform a *PPP session request* [5, 6] to the RAN. At this point, the ASP PPP session is established with default upstream policies in place [7]. In this usage case, there may be little to set in the RG. (Optionally, the PCS can update RGs that haven't restarted in an off-hours time.)

V. On the MV ASP website, User A registers for MV by setting up their user profile, billing options, etc. [8]. They may also obtain, configure, or download the MV client application for the STB and/or PC.

VI. The MV ASP begins sending all the necessary multicast streams for its "channel" lineup to the RAN for multicast distribution to all its subscribers [23].

< Days might pass >

VII. At 8:55 PM on Tuesday, User A decides to watch a movie by starting the STB or video client. It, in turn requests the MV service [16]. The MV ASP queries the user capabilities [9,10] in order to determine how many simultaneous streams it can offer and whether to include high-definition content. The MC ASP then provides the client with an appropriate program guide and DRM information needed to decode the streams [11].

VIII. At 9:01 PM on Tuesday, User A selects the channel for *Gegen die Wand.* The STB sends an IGMPv3 membership report to join this group to the RAN, and the report is sent to the ASP for application billing and tracking purposes [24]. This join is also used by the RAN in order to start replicating the proper multicast group to User A's STB [25].

IX. At 9:30 PM on Tuesday, User A decides to change the channel to *Lola Rennt.* The STB sends an IGMPv3 membership report that leaves the established multicast group and joins the group for *Lola Rennt*. Once again, the membership report is sent to the ASP for application billing and tracking purposes [24]. This report is also used by the RAN in order to stop and start replicating the associated multicast groups to User A's STB [25].

< Various IGMP reports and queries might happen in the RAN during streaming >

X. At 10:30 pm on Tuesday, the movie credits are rolling, and User A turns off the STB. A final membership report is sent to leave the multicast stream [24]. Had this been a different business model, the RAN might process usage information for eventual billing (e.g., number of Kilobytes transported on behalf of MV ASP / End-user). The default MV profile for User A is left in place in case they decide to view additional movies.

8 This may also be accomplished using a RAN provider work order.

9 Note that this arrangement describes an IGMPv3 enabled capability of using the combination of multicast group as well as unicast source to uniquely identify a desired multicast group. This enhances the scalability of multicast services.

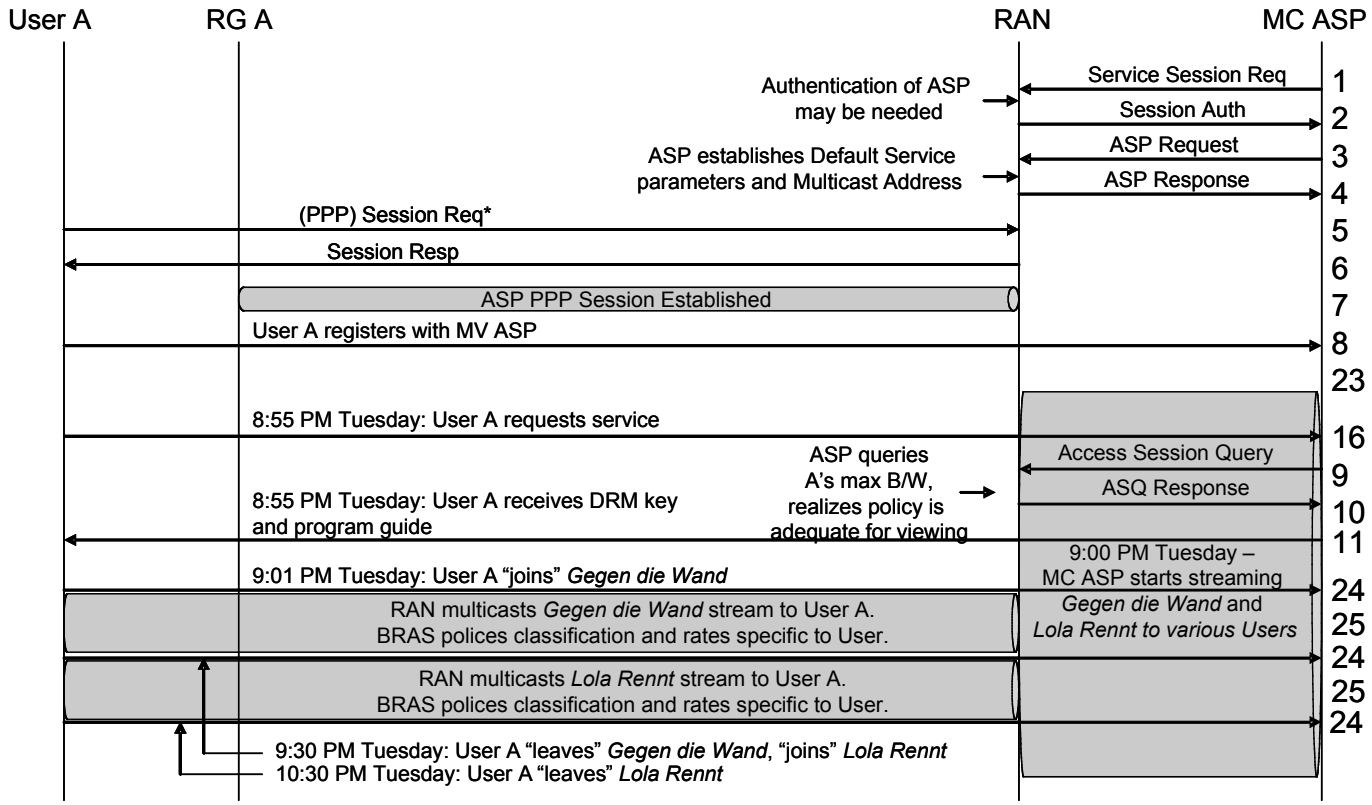


Figure 14 – Multicast Video Application Flow

4.6.4 More Advanced Capabilities

A number of more advanced MV capabilities have been discussed in the industry that benefit one or more of the stakeholders (end-users, content providers, MV ASP, RAN provider), including:

- Integration with PVR functionality
- Smart ad insertion based on ASP Session Query information.
- Digital Rights Management enhancements (e.g., unlimited viewing of a movie for up to 10 days; restrictions on copying to secondary storage devices).

Back Office enhancements (e.g., charging based on movie length; RAN provider wholesale billing of ASP for download bandwidth)

5. NETWORK FLOWS

The network messages and information flows needed to support the application flows from the usage cases in Section 4 are detailed in this section. The subheadings that follow detail the various aspects of network flows needed to support several distinct functions provided by the network. This section will detail the network messages, communications among functional elements, and accounting arrangements that are needed to support the applications with respect to authentication with the RAN Network.

It should be noted that this section provides only one example of possible arrangements of network functional entities, and that the example was chosen in order to minimize complexity. Notably, an overall coordination function, sometimes called "business logic," has been included with the moniker of *DSL Service Manager*. It is expected that typical network deployments would have much more complex set of functions and systems that coordinate business logic. However, the applications and information capabilities can be taken as a litmus test for various policy and management frameworks' suitability to support the business models set forth in TR-058, and refined in this TR.

The numbered lists that follow aligns with the numbered interactions at the far right of their associated figures. The numbering in the figures below also align with the same numbers in previous figures, however, add internal network flows to the previous figures, with outline numbering representing sub-steps within the network.

5.1 ASP Authentication

1 ASP authenticates to the A10 Protocol Session manager (A10-PSM). This functional element will co-ordinate ASP requests with various other network elements and will generate accounting records (log) for positive and negative results to support non-repudiation of access.

1a The A10 PSM retrieves authentication information from the database.

1b The database provides the authentication information, which may be a simple yes or no, or may be a challenge token that the A10 PSM can use to ensure that the ASP is valid.

1c This step shows the optional challenge handshake – envisioned much like CHAP.

1d The response from the challenge.

2 The ASP granted access for service requests.

2a This activity is logged for all the reasons that customer interactions are logged.

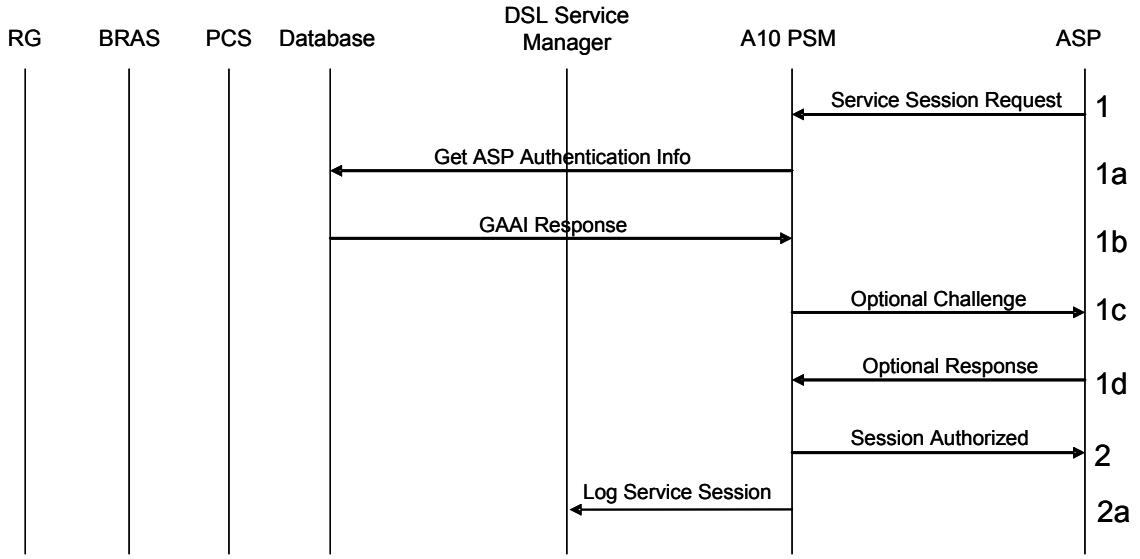


Figure 15 – ASP Authentication

5.2 NSP Authentication

The NSP authentication is similar to the ASP Authentication described above, but will likely differ from the set of capabilities exposed to an ASP. For example the RAN provider would likely restrict the ability to control the overall bandwidth allocated to a PPP session to only the NSP. Given that multiple ASPs will likely share the same PPP session, the RAN provider would not want to allow any one ASP access to that parameter.

1 NSP authenticates to the A10 PSM. This functional element will co-ordinate NSP requests with various other network elements and will generate accounting records (log) for positive and negative results to support non-repudiation of access.

1a The A10 PSM retrieves authentication information from the database. Many protocols could be used, but LDAP may be particularly suited for performance reasons.

1b The Database provides the authentication information, which may be a simple yes or no, or may be a challenge token that the A10 Protocol Session Manager can use to ensure that the NSP is valid.

1c This step shows the optional challenge handshake – envisioned much like CHAP.

1d The response from the challenge

2 The NSP is granted access for service requests.

2a This activity is logged for all the reasons that customer interactions are logged.

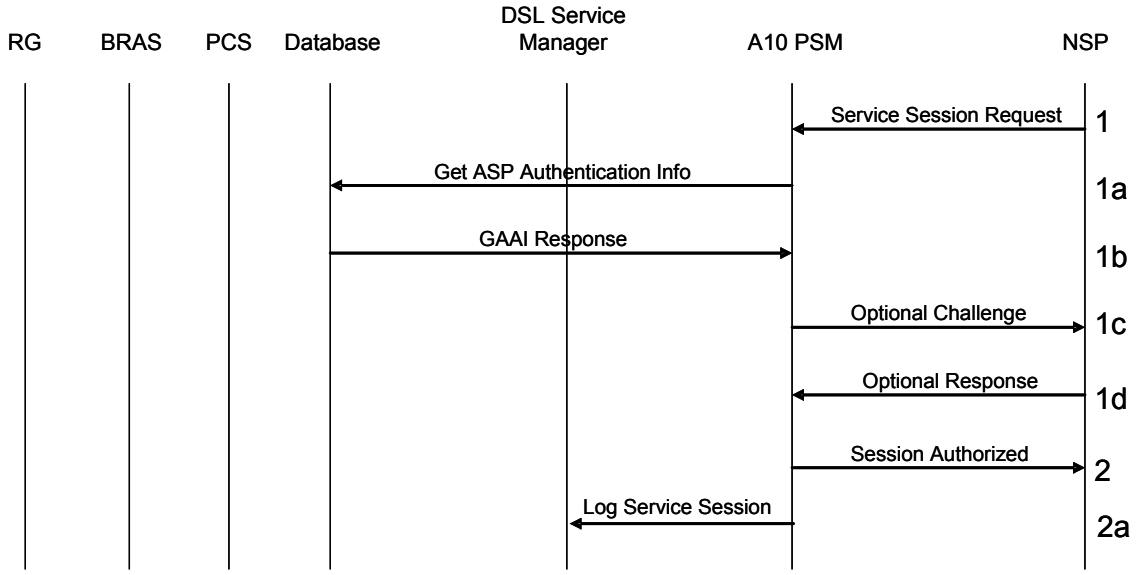


Figure 16 – NSP Authentication

5.3 ASP Application Flow Request

3 The ASP establishes a global policy for their service through an *ASP Request*.

3a The A10 PSM ensures that the request was received within an authenticated Service Session and parses the request. The request is then forwarded to the DSL Service manager

3b The DSL Service Manager accepts the authenticated request from the A10 PSM and runs the business logic that decides if and how to embody the request. In order to establish the current service levels, business models, and authorized capabilities for the ASP, the DSL Service Manager queries the Database for that information.

3c The database provides the requested information to the DSL Service Manger.

3d The DSL Service Manager has established that there is a need to provide a global policy in order to instantiate the service request. The DSL Service manager places the updated global policy information into the Database.

3e For network elements that need to support the global policy the DSL Service Manager pushes a network modified policy profile into the network element. This steps shows the BRAS accepting an updated policy, but it should be noted that other elements, notably the router that serves the ASP, might also need the new policy to be instantiated. Also, while this step shows the DSL Service Manager pushing policy directly into the BRAS, it is also possible that the policy would be delivered indirectly through a policy management or element management system. The policy will include how to identify their traffic for the desired treatment as well as the business model that is desired. All You Can Eat would be easy, so let's say that the overall business model here is a la carte. This means that the ASP has selected a QoS treatment for their traffic, and will be billed

according to the amount of traffic that they offer to the RAN in terms of bytes or seconds. Naturally, the policy will either need to add the capability or the network elements already have the capability to keep byte counts or duration counts of the traffic that is delivered on behalf of this policy. For this capability it might be more likely to involve the router that serves the ASP directly, rather than all the various BRAS distributed in a RAN.

3f If the Service Request is end-user specific, and must change policy in the CEP then, the DSL Service Manger would apply additional logic (otherwise, the default behavior would be for the CPE to fetch the new policy on the next after the next PPP establishment). As shown in this step, it would query the database for information about the access policies already in place for user A.

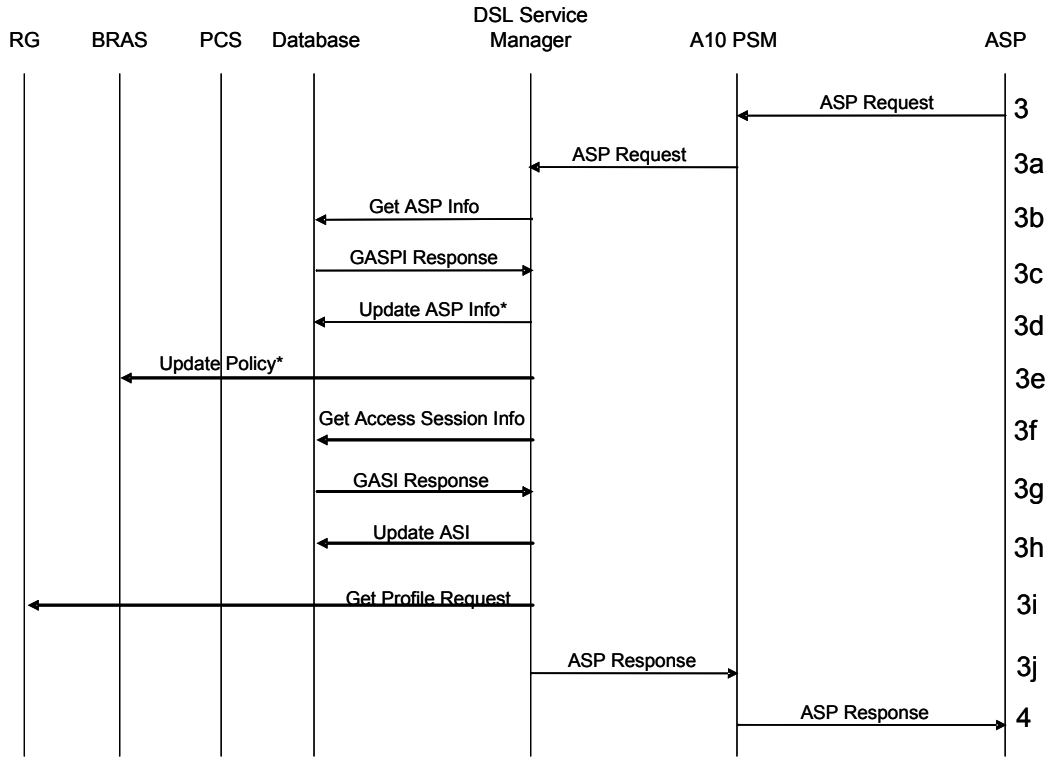
3g The database would return the information available, including existing conditions, and user-specific policies already in effect on the subscriber access.

3h The DSL Service Manager would create or modify the policy for that subscriber's ASP access and update the database with the information.

3i After providing the new policy, the DSL Service Manger would inform user A's RG that there was a new policy in place and that it should go and fetch it.

3j Once all the steps are done to instantiate the new policy, a record is logged (by the DSL Service Manager at the DSL Service Manager – so it's not shown in the diagram). The DSL Service Manager tells the ANI PSM that the request was fulfilled.

4 The acknowledgement is forwarded to the ASP by the A10 PSM and may include a billing reference identifier to help co-ordinate the ASP's activities with the billing itemizations they might see from the RAN.



* *Update Policy* may push policy into other devices in addition or instead of BRAS

Figure 17 – ASP Request

These same capabilities could also be exposed to NSPs through the A10 PSM.

5.4 Establishing Access Session to the RAN Network

End users will establish PPP sessions to the RAN as a matter of course. When these sessions are established, a profile for traffic classification is provided to both the BRAS as well as the RG. These profiles would include (potentially) the policy element that enable a rate limit and QoS level for the ASP's request in step 3. This is a more sophisticated approach and would require more policy information to be deployed to more elements. It is also possible that a standard QoS and bandwidth policy would be leveraged for many ASP applications that share a common genre. For example, a single treatment may be available as a default for *all* the different ASPs that exist in the RAN.

5 The first step is a PPP session establishment request from the RG to the BRAS.

5a The BRAS may add additional information about the request (as is typical) and send a RADIUS authentication request to the RADIUS Proxy (which is another type of Protocol Manager in this example usage case). The RADIUS Proxy will look at the desired network for the PPP session. (If this had been an NSP request, it might have launched a RADIUS authentication request to the NSP, but in either case…)

5b The RADIUS Proxy will pull the profile information from the database for the BRAS.

5c The database provides the profile or potentially a "reference" to a common profile already provisioned or cached in the BRAS.

5d Then the RADIUS Proxy provides the results to the BRAS along with the RADIUS response for authentication.

5e At this point the RADIUS Proxy will log the access to the DSL Service Manger.

6a At some point after establishing connectivity to the ASP network, the RG launches its DSLF auto-config request – aimed at the PCS, which in this example usage case is yet another type of Protocol manager.

6b The PCS queries the database for the RG's particular config info (and also potentially queries one or more NSPs for their contribution to the RG's configuration).

6c The database provides the results, and

6d The PCS responds to the RG's auto-config request with the desired data.

6e Finally, the configuration establishment is logged as available.

Once all the PPP sessions are established, the end users have access to all the various ASPs that are hosted by the RAN. Basic policies are in place, and a special route table in the RG will direct traffic to the ASPs to this PPP session. The mechanism for providing the route table could include PPP session establishment parameters, TRIP protocol, Auto-configuration protocol parameters, or something else.

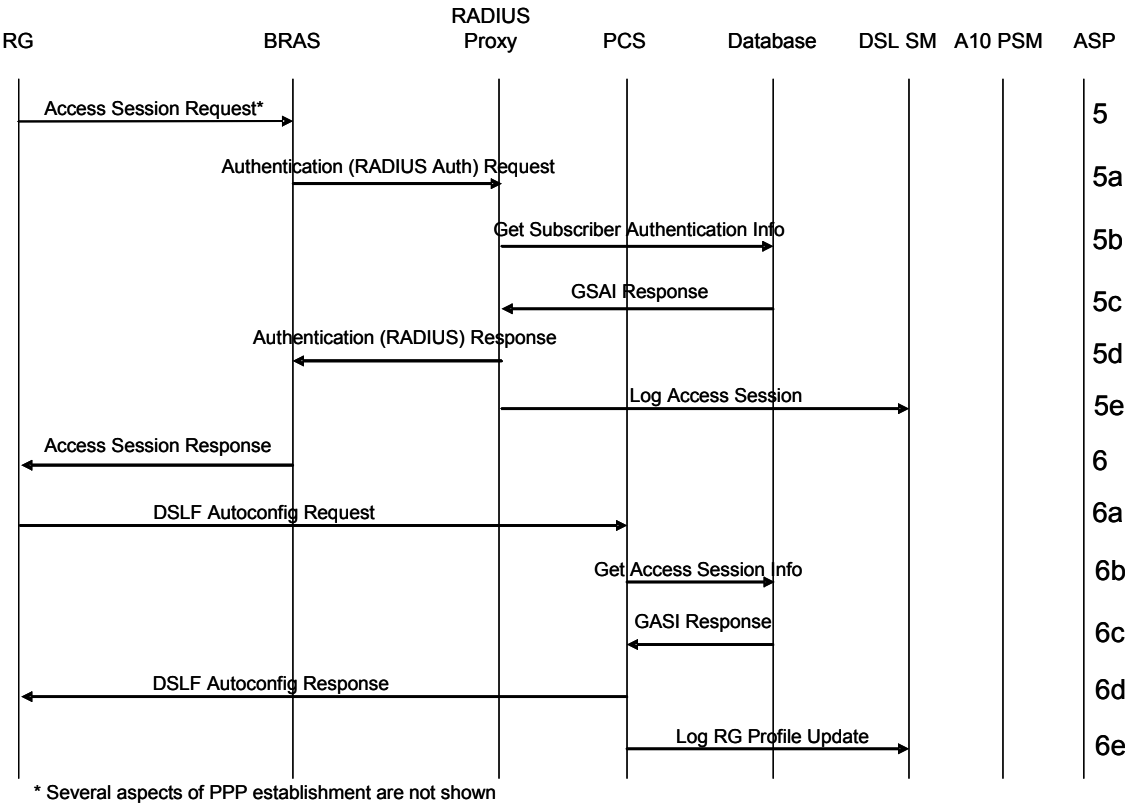


Figure 18 – Access Session Establishment

5.5 Access Session Query

User A forms a business relationship with the ASP. Some sort of billing arrangement is established so that the ASP can bill for providing service to user A.

9 As user A establishes the billing relationship, the ASP queries the RAN to determine the bandwidth and QoS availability for user A.

9a The A10 Protocol Session Manager handles queries by requesting information from the database directly.

9b The database response includes the available bandwidth, and potentially a list of existing committed priority flows that might interfere with new ones. Note that maximum bandwidth may depend on many factors, not just the sync rate. The database response can also include a list of the Olympic class service levels that are supported by the end user. Note that in actual implementation, QoS may be provided in a phased approach – appearing quickly for end users that are two or fewer ATM hops from the BRAS, and adding additional users as they are re-homed in a way that reduces their number of hops and enables hierarchical scheduling to provide QoS.

10 The A10 Protocol Session Manager provides the (potentially reformatted) response to the ASP. The response might also include a transaction ID that would assist the ASP in reconciling a future bill for services.

10a Finally, this interaction is logged, and there may (or may not) be a charge associated with querying a user's capabilities.

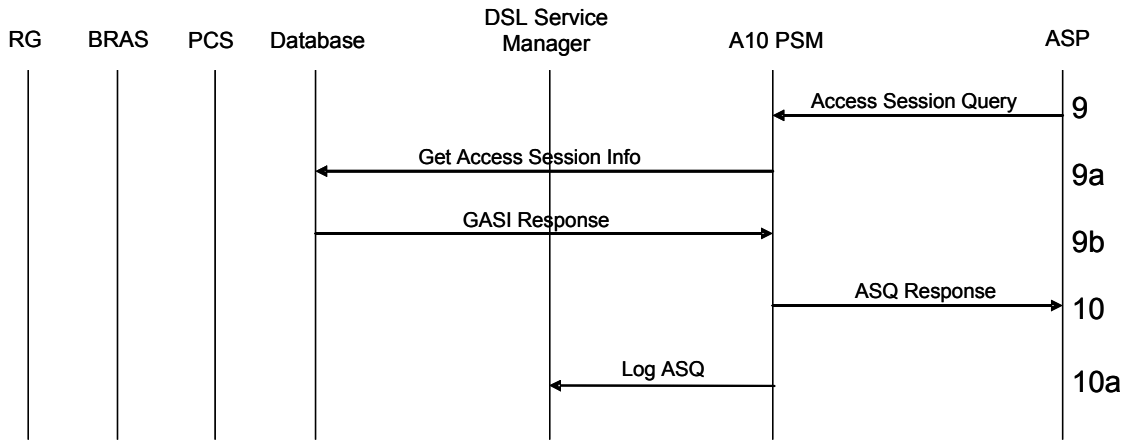


Figure 19 – Access Session Query

These same capabilities could be exposed to NSPs through the A10 PSM.

5.6 RG Profile Update

An example of a profile update is an ASP that sells a premium arrangement to a user – based on a high bandwidth capability, and then requests a different profile for A than the default. This profile might be user-specific, but is probably not - in favor of a profile common to all users that opt into the higher bandwidth tier. This interaction is logged and also will create a billing element for this treatment. The usage case assumption is that the profile for this class of user requires some special treatment on the RG, and the RG needs to update its profile information. Updates of RG profiles and policies are not expected to happen in real time, but are expected to happen on the order of a few seconds rather than minutes or hours.

13 As part of the ASP Application Flow Request, the RG is told that new profile information (a new profile) is available to be fetched from a policy server.

14 The RG requests the new profile from the policy server using TR-069 or a derivative thereof.

14a In this usage case, it is assumed that the policy server is another sort of “protocol handler,” much like the A10 PSM or RADIUS proxy, and does not encompass a database function. Therefore the policy server takes the autoconfig request and queries the database in order to fetch the new profile information. As a protocol handler it is quite possible that the policy server could query other data (like a NSP database) in order to compile a more complete configuration profile for the RG.

14b The database responds to the request with the information needed to configure the RG

15 The policy server provides the configuration details to the RG as prescribed in TR-069. The response to the request will include a new profile that includes the element for the ASP and potentially ALG code or configuration.

15a Successful reconfiguration will be logged, and may be used to create billing elements – especially if the profile required the consumption of scarce resources, like ALGs or QoS queues in the RG.

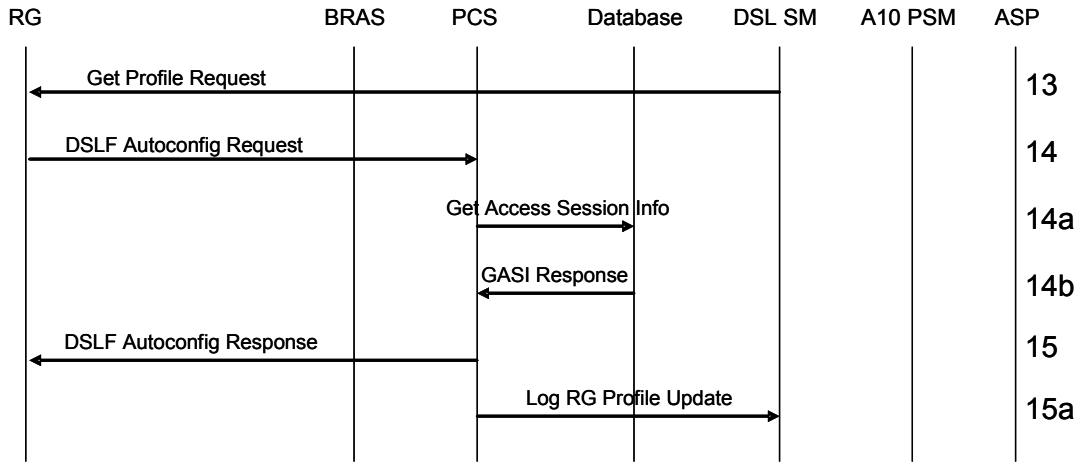


Figure 20 – Profile Update

These same capabilities could be exposed to NSPs through the A10 PSM.

5.7 Multicast Control

Multicast is established using IGMP from the client. Note that IGMP is not sufficient for providing a commercial service, and must typically be enhanced with network-based filters and application layer DRM and access controls. Also, as this is not a novel or new protocol, it will not be described here, except to indicate that IGMP messages may be provided to the ASPs in order to facilitate their accounting and to allow them to collect statistics. Clients should be prepared to use IGMPv3, although some networks might support IGMPv2 for a time before they are upgraded.

5.8 Application Accounting

Figure 13 indicates multiple sources that can accessed to collect accounting information. These sources include:

- A10 or A10 Protocol Session Manager – This functional element could provide records based on the number of events that have transpired during a given time period. These events could include the number of bandwidth queries or bandwidth/QoS requests.
- ASP Router – This device situated in the ASP Network could report usage information on aggregate for the ASP.
- BRAS – The device could provide metrics on the number of bytes used in the access network for a particular user.

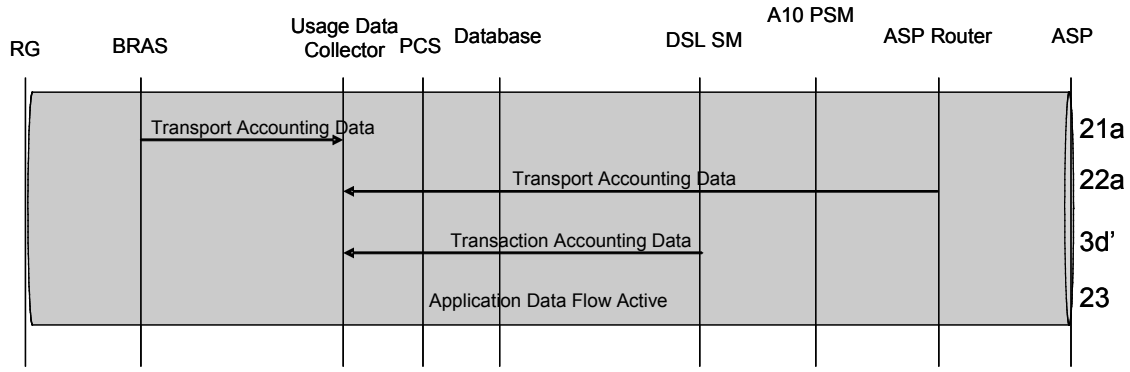


Figure 21 – Collecting Accounting Data

6. NORMATIVE A10 PROTOCOL SPECIFICATION

6.1 Service Provider Protocol Interface

For an ASP or NSP to make requests of the RAN, there needs to be a protocol interface to support communications between the entities. The natural interface point for such a protocol to be supported is the A10 interface described in TR-059 and elsewhere. TR-059 defines the physical characteristics of such an interface up to the network layer (IP)[10]. There also needs to be a set of capabilities and syntax for requesting those capabilities defined at the application layer of such an interface.

The capabilities that such an interface would have MUST include:

- Authentication of peers,
- Ability to reference subscribers, classes of subscribers, or meaningful groups (like all),
- Ability to query capabilities of a given subscriber,
- Ability to request BoD/QoS to a meaningful reference, and
- Ability to pass accounting data to support the billing and non-repudiation of services rendered.

6.2 BoD and QoS Capabilities

There is a broad cross-section of available bandwidth and QoS configuration options that might be used in a RAN – however in practice it is not practical to provide access to all the possible points. In order to make the network more manageable, and to make the selections of the ASPs and NSPs more manageable, bandwidth and QoS subsets are more typically provided. As mentioned earlier in Section 4, it is expected that changes in BoD and QoS take effect on various time scales, and under the most stringent cases take effect within 6 seconds.

6.2.1 Bandwidth on Demand (BoD)

Bandwidth on demand (BoD) is basically the ability to specify and to change the maximum rates for access. It can be further subdivided within the TR-059 context to the following:

1. NSP access can be set to receive various maximum bit rates. These changes affect their entire access session, and so all the applications within the session receive access to the new rate. The NSP could request this for a single subscriber, for all subscribers, or for a pre-defined tier of service. For example, all NSP access subscribers that have elected 256x128Kb/s service might be provided a “free weekend” of 3Mx512Kb/s in a promotion to entice them to upgrade service. This weekend change in that service tier is a prime example of BoD.
2. ASP applications can be set to receive various maximum bit rates. Similarly to the NSP service, but focused on a single application rather than the entire access session, BoD for ASP traffic would support setting both a universal speed limit to all customers as well as customer-specific speed limit for single customers.

Turbo [button] is another term often used to describe the capability for both NSP accesses as well as ASP applications can change their maximum bit rates.

An important aspect of BoD is that it is not a bandwidth guarantee – just a maximum for the service class. If BoD were offered in conjunction with a service class that guaranteed precedence over all other traffic, that would constitute a bandwidth guarantee. Having said this, there is still an expectation that the ASP or NSP gains something from the BoD service – even when it applies to best effort Internet. Also, there is an additional expectation met in these usage cases that the NSP and ASP can query for a line rate maximum and can query for how much is already “committed” to other traffic.

[10] See TR-059 Sections 4.2.2 and 4.2.4 for the A10 interface specifications up to layer 3.

BoD may persist until it is specifically changed again – in other words it may look like a provisioning function. Alternately, it may be requested for a specific interval, predefined interval, or perhaps until an access session is torn down.

6.2.2 Quality of Service (QoS)

The usage cases presented were based a subset of the overall set of available QoS types that might be offered. Within the possible set of QoS capabilities that are possible, it is interesting to categorize applications into 3 distinct categories:

1. No (special) treatment. This is the typical "best effort" internet service class. Most of the applications are assumed to be part of this class, and will interact as they do today in an otherwise undifferentiated access arrangement.
2. Aggregate treatment. This case will cover most QoS apps, and may be the only option in an initial QoS phase. In this QoS arrangement applications self-select from several shared priority levels. There are no bandwidth guarantees, and applications that select the same class may contend for that class' resources, but this should be OK, because there are few concurrent QoS applications envisioned at the outset of providing service. In this approach, applications need not "register" for a class a-priori, so they probably should be billed by bytes or buckets. Many levels are possible – and this document will consider three.
3. Individual treatment. This case will cover a select few applications with demanding requirements. It is likely to be supported in a later phase, and likely to be very limited. In this QoS arrangement applications must register for a limited resource for a given time. These applications may have bandwidth expectations, and the TR-059 approach will be to cater to these expectation through prioritization. To prevent undesired interactions among applications at the same priority of service, it is expected that per-application treatment, and possibly queuing, will prevent contention among apps. In this resource reservation approach, resources are set aside whether the app is in use or not, so probably should be billed both monthly and possibly by bytes or buckets over time periods - or by the minute.

More specifically, this set of application usage cases assumes that there are 4 precedence levels of Applications, and that applications that need special bandwidth assurance (like a required information rate) are allocated from bandwidth dedicated to this type of service from one of the top two tiers. The precedence tiers are:

1. Strict priority service or *Expedited Forwarding.* Basically, this traffic dominates all other traffic. It could be called a Platinum Olympic Class, and best current practice reserves this class for VoIP and control traffic. For this class to retain its integrity, applications are not allowed to self-select into the class. They must be admitted in a provisioning role and with limitations on the amount of bandwidth they are allowed to consume. Typically that bandwidth would be set to small fraction of the overall network capacity, and less than the total access line capacity so that other applications are not totally starved out.
2. Higher priority service or *Assured Forwarding.* In this class, the traffic comes after EF, but before most other traffic. It could be called a Gold Olympic Class, and most applications that require some form of QoS might share one or more queues in this class. The key points are that the class of service can be shared, and queues dedicated to this level might police each application's capability to use the class. Policers could allow committed rates, and mark bursts so that each app gets what it needs, and has a fair chance at bursting into uncommitted bandwidth.
3. Standard priority service or *Best Effort.* In this class the traffic is part of the crowd. This usage case will boldly assign this the Silver Olympic Class, and it is expected to be shared by the overwhelming number of apps. In terms of fairness - applications get "whatever," but can clearly grab bandwidth when competition is absent. And to be fair, "whatever" is typically understood and applied in predictable ways as is found on the Internet. This service class supports non QoS-enabled applications, and is basically what is done today almost everywhere for DSL.

4. Lower priority service or *Lower Effort*[11]. This class is the background task or bulk mail service. In this class traffic is dominated by all other classes. This TR will kindly call this a Bronze Olympic Class – although opinions may vary. While this seems like a completely undesirable and underserved approach to networking, it can provide cost-efficient value to certain apps. Notably peer-to-peer can be provided a "break" on bandwidth and download limits by self-selecting to step out of the way of more interactive applications, like e-mail and web surfing. Similarly, backup and subscription services that want to move a lot of data, but don't want to get in the way of more interactive uses of the DSL access can get their job done through this class.

6.3 Service Provider Protocol Syntax

For an ASP or NSP to make requests of the RAN, there needs to be a protocol interface to support communications between the entities. The natural interface point for such a protocol to be supported is the A10 interface described in TR-059. TR-059 defines the physical characteristics of such an interface up to the network layer. There also needs to be a set of capabilities and syntax for requesting those capabilities defined at the application layer of such an interface.

6.3.1 General Requirements

6.3.2 ASP Authentication Request

This message is sent from a ASP to the Regional/Access Network as a request for establishing a communication session. All the ASPs need to be authenticated by the Regional/Access Network before the network bandwidth and QoS service capabilities can be accessed.

`ASPAuthenticationRequest (SP_ID)`

Argument Name	Data Type	Allowed Value	Description	Default Value
SP_ID	String	Max size = 64	Service Provider Identification. This value would have to be agreed upon between the ASP and Regional/Access Network ahead of time.	N/A

6.3.3 ASP Authentication Response

This message is sent from the Regional/Access Network to the ASP as a response for the ASP Authentication Request. The Regional/Access Network returns an authorization code and indicates what actions are authorized for the service provider to perform.

`ASPAuthenticationResponse (ReturnCode, TimeFrame, AuthorizationCode)`

Argument Name	Data Type	Allowed Value	Description	Default Value

[11] Lower Effort (LE) is described in RFC 3662. Past contributions to this service class have used the term *scavenger class*.

ReturnCode	Boolean	True = ASP is authorized to perform the actions listed in the Authorization parameter False = ASP was not authenticated to do anything.	Is the ASP authorized to do anything ?	N/A
Timeframe	Int	Max Value = 1440	The number of minutes the ASP has left that it does not have to re-authenticate itself.	60
AuthorizationCode	String	Max chars = 32	A code that the ASP can use to avoid future authorizations	N/A

6.3.4 ASP Application Flow Request

An ASP can send this message to the Regional/Access Network as a request for changing an application to the desired QOS, Precedence, and Bandwidth

`ASPApplicationFlowRequest (AuthorizationCode, DslLineId, AppClassifier, AppQos, AppPrecedence, MaxAppBandwidth, Min AppBandwidth, AppDuration, MCSource, MCRequest)`

Argument Name	Data Type	Allowed Value	Description	Default Value
AuthorizationCode	String	Max char = 32.	The code the ASP has obtained from a previous ASPAuthenticationRequest call	N/A
DslLineId	String	Max char = 32	This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN.	N/A
AppClassifier	List of Strings.	5-tuple value of IP and port source and destination, plus protocol id.	The classification that the Application has. This is how the network determines that a packet will get the desired QOS and BW treatment. Should be a 5-tuple value listing IP and port source and destination, plus protocol id. May include wild-card (e.g. don't care) values as well as ranges.	N/A
AppQos	String	One of possible values: None Aggregate Individual	A code that an ASP can use to denote one of the valid QoS definitions or classes.	N/A

AppPrecedence	String	One of possible values: Expedited Forwarding, Assured Forwarding, Best Effort, Scavenger	Defines the Precedence marking this application's packets are to receive.	Best Effort
MaxAppBandwidth	List of integers	Two integer values defining the up and down bandwidth.	The bandwidth that this application will not exceed. Includes both up and down bandwidth in Kbps. Values can be predefined by the RAN.	N/A
MinAppBandwidth	List of integers	Two integer values defining the up and down bandwidth.	The bandwidth that this application is supposed to get in AF. Includes both up and down bandwidth in Kbps. Values can be predefined by the RAN	N/A
AppDuration	Integer	0-1440	Number of minutes for the application flow request to live. If zero, then another request is needed to stop the policy.	0
MCSource	String	ASP IP address	Address to enable as multicast source.	0
MCRequest	Integer	0-1024	Number of Multicast groups requested.	0

6.3.5 ASP Application Flow Response

This message is sent from the Regional/Access Network to the ASP as a response for the ASP Application Flow Request.

`ASPApplicationFlowResponse (DslLineId, ReturnCode, MCResponse)`

Argument Name	Data Type	Allowed Value	Description	Default Value
DslLineId	String	Max char = 32	This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN. Must match what was provided in request	N/A
ReturnCode	Boolean	True = ASP was successful in changing the applications QOS/BW parameters False = ASP was not successful in changing the applications QOS/BW parameters	Was the request successful	N/A

MCResponse	List of Strings	Valid Class D IP Addresses	Multicast Group addresses assigned to ASP	N/A

6.3.6 ASP Access Session Query

An ASP can send this message to the Regional/Access Network as a request for finding out an application's QOS, Precedence, and Bandwidth values.

`ASPAccessSessionQuery(AuthorizationCode, DslLineId, AppClassifier)`

Argument Name	Data Type	Allowed Value	Description	Default Value
AuthorizationCode	String	Max char = 32.	The code the ASP has obtained from a previous ASPAuthenticationRequest call	N/A
DslLineId	String	Max char = 32	This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN.	N/A
AppClassifier	List of Strings.	5-tuple value of IP and port source and destination, plus protocol id.	The classification that the Application has. This is how the network determines that a packet will get the desired QOS and BW treatment. Should be a 5-tuple value listing IP and port source and destination, plus protocol id.	N/A

6.3.7 ASP Access Session Query Response

The RAN will respond to the ASPAccessSessionQuery message with this message.

`ASPAccessSessionQueryResponse (DslLineId, AppClassifier, AppQos, AppPrecedence, AppBandwidth, SessionQoS, SessionBandwidth)`

Argument Name	Data Type	Allowed Value	Description	Default Value
DslLineId	String	Max char = 32	This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN.	N/A
AppClassifier	List of Strings.	5-tuple value of IP and port source and destination, plus protocol id.	The classification that the Application has. This is how the network determines that a packet will get the desired QOS and BW treatment. Should be a 5-tuple value listing the address and port source and destination, plus protocol id.	N/A

AppQos	String	One of possible values: None Aggregate Individual	A code that the ASP can use to avoid future authorizations	N/A
App Precedence	String	One of possible values: Expedited Forwarding, Assured Forwarding, Best Effort, Scavenger	Defines the Precedence marking this applications packets are to receive.	Best Effort
AppBandwidth	List of Integers.	Two integer values defining the up and down bandwidth.	The classification that the Application has. This is how the network determines that a packet will get the desired QOS and BW treatment. Should be a 5-tuple value listing source, destination, and protocol id.	N/A
SessionQoS	List of Integers.	Two integer values defining the up and down bandwidth.	The integers reflect the (remaining) available bandwidth for CIR applications to request.	N/A
SessionBandwidth	List of integers	Two integer values defining the up and down bandwidth	The integers reflect the maximum bandwidth available on the line.	N/A

6.3.8 NSP Authentication Request

This message is sent from a NSP to the Regional/Access Network as a request for establishing a communication session. All the NSPs need to be authenticated by the Regional/Access Network before the network bandwidth and QoS service capabilities can be accessed.

`NSPAuthenticationRequest (SP_ID)`

Argument Name	Data Type	Allowed Value	Description	Default Value
SP_ID	String	Max size = 64	Service Provider Identification. This value would have to be agreed upon between the NSP and Regional/Access Network ahead of time.	N/A

6.3.9 NSP Authentication Response

This message is sent from the Regional/Access Network to the NSP as a response for the NSP Authentication Request. The Regional/Access Network returns an authorization code and indicates what actions are authorized for the service provider to perform.

`NSPAuthenticationResponse (ReturnCode, TimeFrame, AuthorizationCode)`

Argument Name	Data Type	Allowed Value	Description	Default Value
ReturnCode	Boolean	True = NSP is authorized to perform the actions listed in the Authorization parameter False = ASP was not authenticated to do anything.	Is the NSP authorized to do anything ?	N/A
Timeframe	Int	Max Value = 1440	The number of minutes the NSP has left that it does not have to re-authenticate itself.	
AuthorizationCode	String	Max chars = 32	A code that the NSP can use to avoid future authorizations	N/A

6.3.10 NSP Access Session Request

An NSP can send this message to the Regional/Access Network as a request for changing the session bandwidth.

`NSPAccessSessionRequest (AuthorizationCode, DslLineId, SessionBandwidth, SessionDuration)`

Argument Name	Data Type	Allowed Value	Description	Default Value
AuthorizationCode	String	Max char = 32.	The code the NSP has obtained from a previous NSPAuthenticationRequest call	N/A
DslLineId	String	Max char = 32	This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN.	N/A
SessionBandwidth	List of integers	Two integer values defining the up and down bandwidth.	The bandwidth that this access session is supposed to get. Includes both up and down bandwidth in kbps	N/A
SessionDuration	Integer	0-1440	Number of minutes for the application flow request to live. If zero, then another request is needed to stop the policy.	0

6.3.11 NSP Access Session Response

This message is sent from the Regional/Access Network to the NSP as a response for the NSP Access Session Request.

`NSPAccessSessionResponse (DslLineId, ReturnCode)`

Argument Name	Data Type	Allowed Value	Description	Default Value

DslLineId	String	Max char = 32	This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN.	N/A
ReturnCode	Boolean	True = NSP was successful in changing the applications BW parameters False = NSP was not successful in changing the applications BW parameters	Was the request successful ?	N/A

6.3.12 NSP Access Session Query

An ASP can send this message to the RAN as a request for querying to found out an applications Bandwidth values.

`NSPAccessSessionQuery(AuthorizationCode, DslLineId)`

Argument Name	Data Type	Allowed Value	Description	Default Value
AuthorizationCode	String	Max char = 32.	The code the NSP has obtained from a previous NSPAuthenticationRequest call	N/A
DslLineId	String	Max char = 32	This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN.	N/A

6.3.13 NSP Access Session Query Response

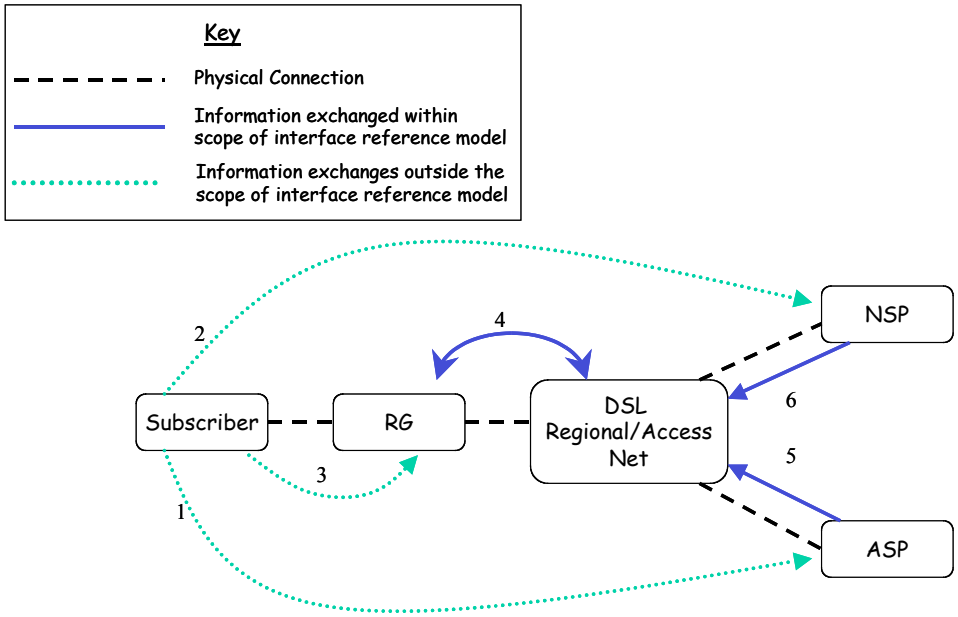
The RAN will respond to the NSPAccessSessionQuery message with this message.

`NSPAccessSessionQueryResponse (DslLineId, SessionBandwidth, SessionMaxBandwidth)`

Argument Name	Data Type	Allowed Value	Description	Default Value
DslLineId	String	Max char = 32	This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN.	N/A
SessionBandwidth	List of integers	Two integer values defining the up and down bandwidth	The bandwidth that this session is supposed to get. Includes both up and down bandwidth in kbps	N/A
SessionMaxBandwidth	List of integers	Two integer values defining the up and down bandwidth.	The integers reflect the maximum bandwidth available on the line.	N/A

A INFORMATIVE ANNEX ON REFERENCE DATA MODEL

In this section a description of the data required in each of the functional domains of the architecture (Regional/Access Network, RG, ASP, NSP, and subscriber) is presented. Figure 22 illustrates a high level representation of the relationships between the different domains.



1,2: The subscriber exchanges information with the A/NSP when signing up for a service
3: The subscriber configures the RG. This may only be for the initial install. The ACS located within the Regional/Access Network may handle all subsequent conf changes
4: The RG initiates access sessions that are terminated in the DSL network. The ACS communicates with the RG for configuration updates.
5,6: The NSP communicates with the DSL network to establish a DSL connection. The ASP and NSP also communicate bandwidth and QoS changes per session or application.

Figure 22 – Inter-Domain Relationships

Based on this abstract view of the domains involved in providing an end-to-end service, a data model can be constructed. Figure 23 depicts a UML model capturing the type of data needed to support bandwidth and QoS management. This model is provided for illustration purposes only and is not intended to represent a complete deployment implementation, which may need to capture information beyond bandwidth and QoS.

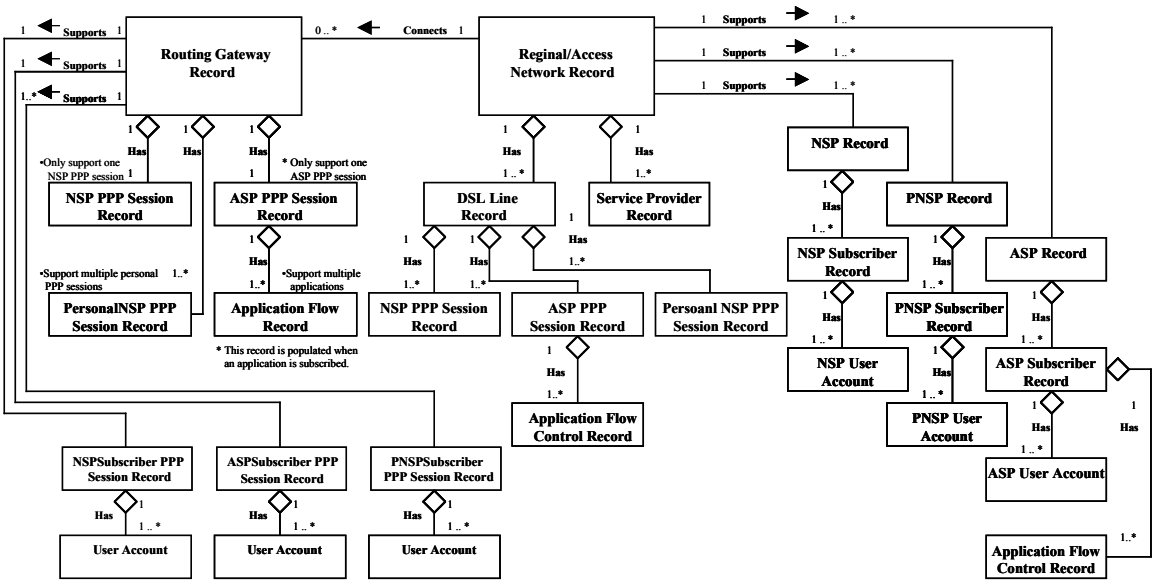


Figure 23 – High Level UML Model

Figure 24, Figure 25, and Figure 26 provide additional details within the main domains and are described below. The remainder of this section provides a detailed description of the data records and attributes captured in the presented UML model.

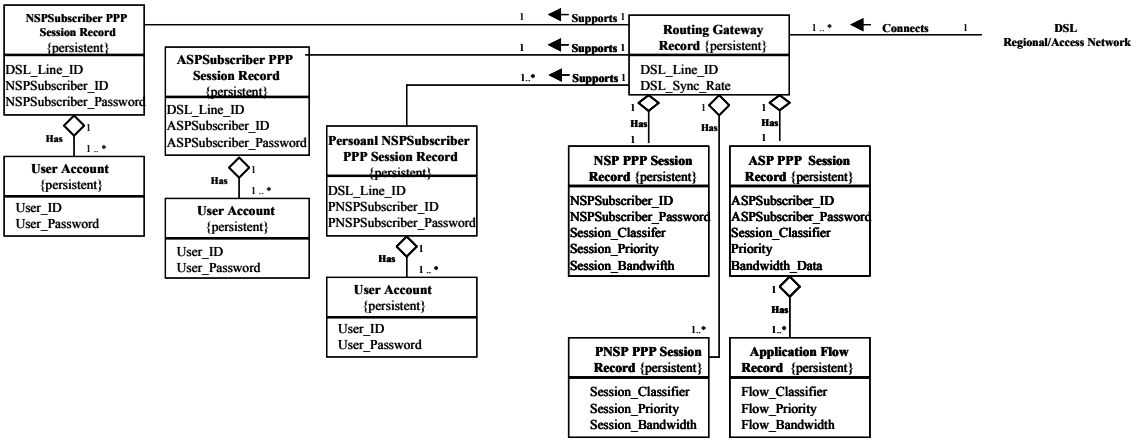


Figure 24 – Detailed UML Representation (RG and Subscriber Maintained Data)

A.1 Subscriber Maintained Data

The following data elements are maintained at Subscriber Premises: (This record is maintained by the subscriber - it could be stored on a PC or any other storage device/media) Also note that there can be multiple instances of this data and that records and sub-elements can occur in multiples. For example, a user may have more than one user ID – each associated with a separate e-mail account.

Record Type	Elements	Description	Source
NSPSubscriber PPP Session Record		The subscribers need to know their DSL_line_ID, NSPSubscriber_ID and NSPSubscriber_Password for accessing their NSP networks. Only a single NSP PPP session record can exist.	
	DSL_Line_ID	DSL_Line_ID is a unique identifier for the DSL line. This is the identifier the Regional/Access Network uses to identify a subscriber line. Could be a phone number, IP address, or FQDN.	DSL_Line_ID is provided by the Regional/Access Network Provider at subscription time.
	NSPSubscriber_ID	This ID is used for accessing the NSP networks.	Assigned by the NSP at the time of subscription
	NSPSubscriber_ Password	Subscriber_Password is initially set by the NSP, later it can be changed by the Subscriber. It is used together with the NSPSubscriber_ID to access the NSP networks.	Initially assigned by the NSP at subscription time. Can be changed by the subscriber.
Personal NSPSubscriber PPP Session Record		The subscribers need to know their DSL_line_ID, PersonalNSPSubscriber_ID and Personal NSPSubscriber_Password for accessing their Personal NSP network. Multiple records can exist.	
	DSL_Line_ID	As defined **Error! Reference source not found.**	As defined **Error! Reference source not found.**
	PersonalNSP Subscriber_ID	This ID is used for accessing the Personal NSP networks.	Assigned by the Personal NSP at the time of subscription.
	PersonalNSPSubscriber_ Password	It is used together with the PersonalNSPSubscriber_ID to access the PNSP networks.	Initially assigned by the PNSP at the time of subscription. Can be changed by the subscriber.
ASPSubscriber PPP Session Record		The subscribers need to know their DSL_line_ID, ASPSubscriber_ID and ASPSubscriber_Password for accessing their ASP services. For each application they subscribe to, they need to maintain their User_ID and Password. Only one ASP PPP session record can exist.	
	DSL_Line_ID	As defined**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found. Error! Reference source not found.**	As defined **Error! Reference source not found.**
	ASPSubscriber_ID	This ID is used for accessing the ASP networks.	Provided by ASP at the time of subscription
	ASPSubscriber_	It is used together with the ASPSubscriber_ID	Initially assigned by ASP at the time of

	Password	to access the ASP networks.	subscription. Can be changed by the subscriber.
User Account Record		This record is maintained by user/users of services provided over the Regional/Access Network. A user account is tied to a subscriber account. Multiple user accounts can be associated with a single subscriber account. Note: There is one or multiple User Account Record under each of the NSPSubscriber PPP Session Record, Personal NSPSubscriber PPP Session Record, and ASPSubscriber PPP Session Record.	Created at the time of subscription to ASP services
	User_ID	This ID is used for accessing the given service.	Assigned by a given ASP to a particular user at the time subscription
	User_Password	It is used together with the User_ID to access a given service,	Initially assigned by a given ASP to a particular user at the time of subscription. Can be changed by the subscriber.

A.2 Routing Gateway

Routing Gateway is a customer premises functional element that provides IP routing and QoS capabilities.

The main functions of RG include:

IP routing between the CPN and the Access Network
Multi-user, multi-destination support: Multiple simultaneous PPPoE sessions (started from the RG or from devices inside the CPN) in conjunction with non-PPP encapsulated IP (bridged) sessions.
Network Address Port Translation (NAPT)
PPPoE pass though
Multiple queues with scheduling mechanism
IP QoS

The following data elements are maintained at RG:

Record Type	***Elements***	**Description**	**Source**
Routing Gateway Record		Routing Gateway Record is maintained by RG.	It is initialized with the initial configuration by the manufacturer or configured by the user during the install process. The ACS or PCS can also update this record during and after the initial install.
	DSL_Line_ID	As defined **Error! Reference source not found.**	As defined **Error! Reference source not found.**
	DSL_Sync_Rate	DSL_Sync_Rate is the current physical layer synch rate of the DSL line. This record includes both upstream and downstream metrics. It also includes what	It is populated by RG during modem training.

		is the maximum obtainable synch rate	
NSP PPP Session Record		NSP PPP Session Record is maintained by the RG to store information specific to the community NSP access session. This session is launched by the RG and provides the CPN with a default route. Only one community NSP record can exist.	
	NSPSubscriber_ID	This ID is used for accessing the DSL and NSP networks.	Assigned by NSP at subscription time.
	NSPSubscriber_Password	It is used together with the Subscriber_ID to access the DSL and NSP networks.	NSPSubscriber_Password is initially set by the NSP, later it can be changed by the Subscriber.
	Session_Classifier	This parameter contains classification parameters to identify the NSP PPP session (i.e. Ethertype and FQDN).	This value is populated based on configuration data received from the PCS.
	Session_Priority	Optional - Indicates the priority level of the NSP PPP connection relative to the other PPP sessions present – only required if DSL bandwidth is shared across PPP sessions and need to establish a priority relationship across the PPP sessions	This value is populated based on configuration data received from the PCS.
	Session_Bandwidth	The Session_Bandwidth contains information about the maximum bandwidth assigned to this NSP PPP access session.	This value is initialized based on a default value or on the Profile Data received from the PCS.
ASP PPP Session Record		ASP PPP Session Record is maintained by the RG to store information specific to the ASP access session. This PPP session is launched by the RG and receives routes, via RIP, to the ASP network. Only one ASP record can exist.	
	ASPSubscriber_ID	This ID is used for accessing the ASP network (and potentially ASP applications although the RG would not be involved).	Assigned by ASP at subscription time
	ASPSubscriber_Password	It is used together with the ASPSubscriber_ID to access the Regional/Access Network. (and potentially ASP applications although the RG would not be involved)[12]	Initially set by the ASP, later it can be changed by the Subscriber
	Session_Classifier	This parameter contains classification parameters to identify the ASP PPP session (i.e. Ethertype and FQDN).	This value is populated based on configuration data received from the PCS.
	Session_Priority	Optional - Indicates the priority level of the ASP PPP connection relative to the other PPP sessions present – only required if DSL bandwidth is shared across PPP sessions and need to establish a priority relationship across the PPP sessions	This value is populated based on configuration data received from the PCS.
	Session_Bandwidth	The Session_Bandwidth contains information about the maximum bandwidth (upstream and downstream) assigned to this ASP PPP access session.	This value is populated based on configuration data received from the PCS.
Application Flow Record		The Application Flow Record is maintained by the RG for each application	

[12] RG is not required to store UserId/Password for applications, which are expected to be maintained by the ASP

		service that subscriber or users of the DSL line subscribe to. It is used to store application specific data. Multiple application records can exist.	
	Flow_Classifier	Flow_Classifier contains classification parameters to identify the application flow (IP 5 tuple). It may include Class D addresses to support multicast.	This value is populated based on configuration data received from the PCS.
	Flow_Priority	Indicates the priority level of the application within the ASP PPP connection. This parameter indicates the treatment of the application flow (what queue it should be placed in) as well as any marking requirements (DSCP).	This value is populated based on configuration data received from the PCS.
	Flow_Bandwidth	Flow_Bandwidth parameter is assigned to the given application based on the negotiated value between the ASP and the Regional/Access Network. It indicates the maximum upstream and downstream bandwidth. It is used by the RG to shape and police the application flow.	This value is populated based on configuration data received from the PCS.
Personal NSP PPP Session Record		Personal NSP PPP Session Record is maintained by the RG to store information specific to the Personal NSP access session. Multiple records can exist.	
	Session_Classifier	This parameter contains classification parameters to identify the PNSP PPP session (i.e. Ethertype and FQDN).	This value is populated based on configuration data received from the PCS.
	Session_Priority	Optional - Indicates the priority level of the PNSP PPP connection relative to the other PPP sessions present – only required if DSL bandwidth is shared across PPP sessions and need to establish a priority relationship across the PPP sessions.	This value is populated based on configuration data received from the PCS.
	Session_Bandwidth	The Session_Bandwidth contains information about the maximum bandwidth assigned to the PNSP access service.	This value is populated based on configuration data received from the PCS.

A.3 Regional/Access Network

The primary function of the Regional/Access Network is to provide end-to-end transport between the customer premises and the NSP or ASP. The Regional/Access Network will also provide higher layer functions such as QoS and bandwidth management. QoS will be provided by tightly coupling traffic-engineering capabilities of the Regional Network with the capabilities of the BRAS.

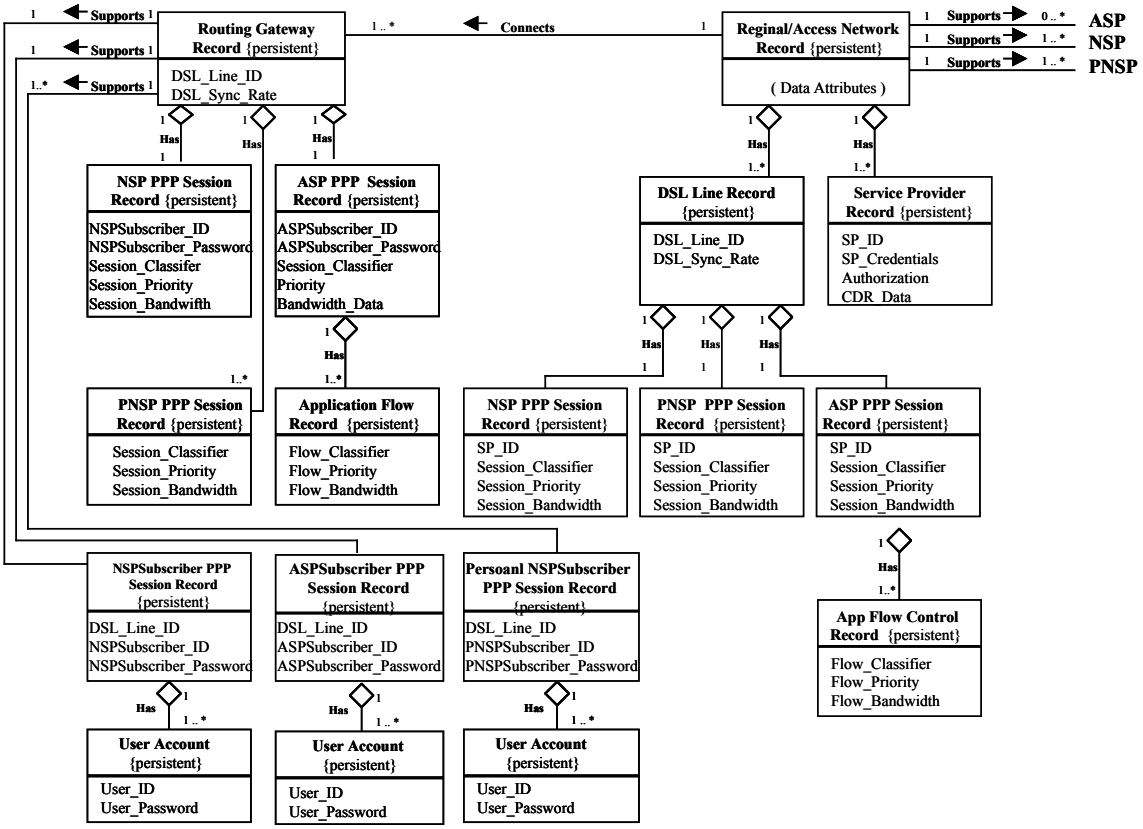


Figure 25 – Detailed UML Representation (Regional/Access Network)

The following data elements are maintained at the Regional/Access Network:

Record Type	*Elements*	**Description**	**Source**
DSL Line Record		The DSL line record is maintained in the Regional/Access Network and is unique to each DSL line. It maintains data specific to a DSL line and the sessions that traverse it.	
	DSL_Line_ID	As defined **Error! Reference source not found.**	As defined **Error! Reference source not found.**
	DSL_Sync_Rate	DSL_Sync_Rate is the current physical layer synch rate of the DSL line. This record includes both upstream and downstream metrics. It also includes what are the maximum obtainable data rates in either direction.	This data is obtained from the DSLAM EMS and the RG
NSP PPP Session Record		NSP PPP Session Record is maintained by the Regional/Access Network to store information specific to the community NSP PPP access sessions. The NSP access record is tied to the DSL Line Record. Only one can exist.	
	SP_ID	Uniquely identifies the NSP that the subscriber has a relationship with. Used to cross reference users to NSPs who make turbo/QoS requests.	Assigned by the Regional/Access Network Provider when a wholesale relationship is established with the NSP
	Session_Classifier	This parameter contains classification parameters to identify the NSP PPP session (i.e. Ethertype and FQDN).	Provided by the NSP at subscription time.
	Session_Priority	Optional - Indicates the priority level of the NSP PPP connection relative to the other PPP sessions present – only required if DSL bandwidth is shared across PPP sessions and need to establish a priority relationship across the PPP sessions	The Regional/Access Network Provider initializes this value at subscription time based on the business model and type of wholesale access that is being sold to the NSP and its relationship to the ASP or the PNSP sessions.
	Session_Bandwidth	The Session_Bandwidth contains information about the maximum bandwidth (upstream and downstream) assigned to this NSP PPP session.	This value is set by the NSP.
PersonalNSP PPP Session Record		PersonalNSP PPP Session Record is maintained by the Regional/Access Network to store information specific to the Personal NSP PPP access sessions. Multiple records can exist.	
	SP_ID	As defined above	As defined above
	Session_Classifier	This parameter contains classification parameters to identify the PNSP PPP session (i.e. Ethertype and FQDN).	Provided by the NSP at subscription time.
	Session_Priority	Optional - Indicates the priority level of the PNSP PPP connection relative to the other PPP sessions present – only required if DSL bandwidth is shared across PPP sessions and need to	The Regional/Access Network Provider initializes this value at subscription time based on the business model and type of wholesale access

		establish a priority relationship across the PPP sessions	that is being sold to the NSP and its relationship to the ASP or the PNSP sessions. Assigned by PNSP and passed to Regional/Access network via NNI message interface.
	Session_Bandwidth	The Session_Bandwidth contains information about the maximum bandwidth (upstream and downstream) assigned to this PNSP PPP session.	This value is initially set by the PNSP,
ASP PPP Session Record		ASP PPP Session Record is maintained by the Regional/Access Network to store information specific to the ASP PPP session. The ASP PPP Record is tied to the DSL Line Record. Only one ASP record can exist.	
	SP_ID	As defined above	As defined above
	Session_Classifier	This parameter contains classification parameters to identify the ASP PPP session (i.e. Ethertype and FQDN).	Provided by the ASP at subscription time
	Session_Priority	Optional - Indicates the priority level of the ASP PPP connection relative to the other PPP sessions present – only required if DSL bandwidth is shared across PPP sessions and need to establish a priority relationship across the PPP sessions	The Regional/Access Network Provider initializes this value at subscription time based on the business model and type of wholesale access that is being sold to the NSP and its relationship to the ASP or the PNSP sessions. Assigned by ASP and passed to Regional/Access network via NNI message interface.
	Session_Bandwidth	The Session_Bandwidth contains information about the maximum bandwidth (upstream and downstream) assigned to this ASP PPP session.	This value is initially set by the Regional/Access Network Provider, but could be modified by individual ASPs that request more bandwidth for their application. An alternative model is that this value is set to the max value initially and ASPs only affect their allotment of bandwidth within the PPP session.
Application Flow Record		The Application Flow Record contains specific details about an application within the ASP session. This record is tied to the ASP account record. Many application records can be associated with an ASP account record.	
	Flow_Classifier	Flow_Classifier contains classification parameters to identify the application flow (IP 5 tuple). It is used by the BRAS & the RG. It may include Class D	Values provided by the ASP.

		addresses to support multicast.	
	Flow_Priority	Indicates the priority level of the application within the ASP PPP connection. This parameter indicates the treatment of the application flow (what queue it should be placed in) as well as any marking requirements (DSCP). It is used by the BRAS and the RG	Provided by the ASP. Regional/Access Network Provider provides available options to select.
	Flow_Bandwidth	Flow_Bandwidth parameter is assigned to the given application based on the negotiated value between the ASP and the Regional/Access Network. It indicates the maximum upstream and downstream bandwidth. It is used by the BRAS & the RG to shape and police the application flow.	These values are provided by the ASP to meet the needs of the application.
Service Provider Record		The service Provider Record is used to authenticate service providers (NSPs, ASPs) who wish to query the Regional/Access Network for information and make bandwidth and or QoS requests.	
	SP_ID	As defined above	As defined above
	SP_Credentials	Used to authenticate this service provider together with SP_ID when connecting to the Regional/Access Network.	Assigned by the Regional/Access Network Provider
	Authorization	Represents what records the SP has access to (DSL line records can it make queries/modifications to.	Assigned by the Regional/Access Network Provider
	CDR_Data	Stores billing data for wholesale access to Turbo and QoS controls	This data is generated by the Regional/Access Network Provider

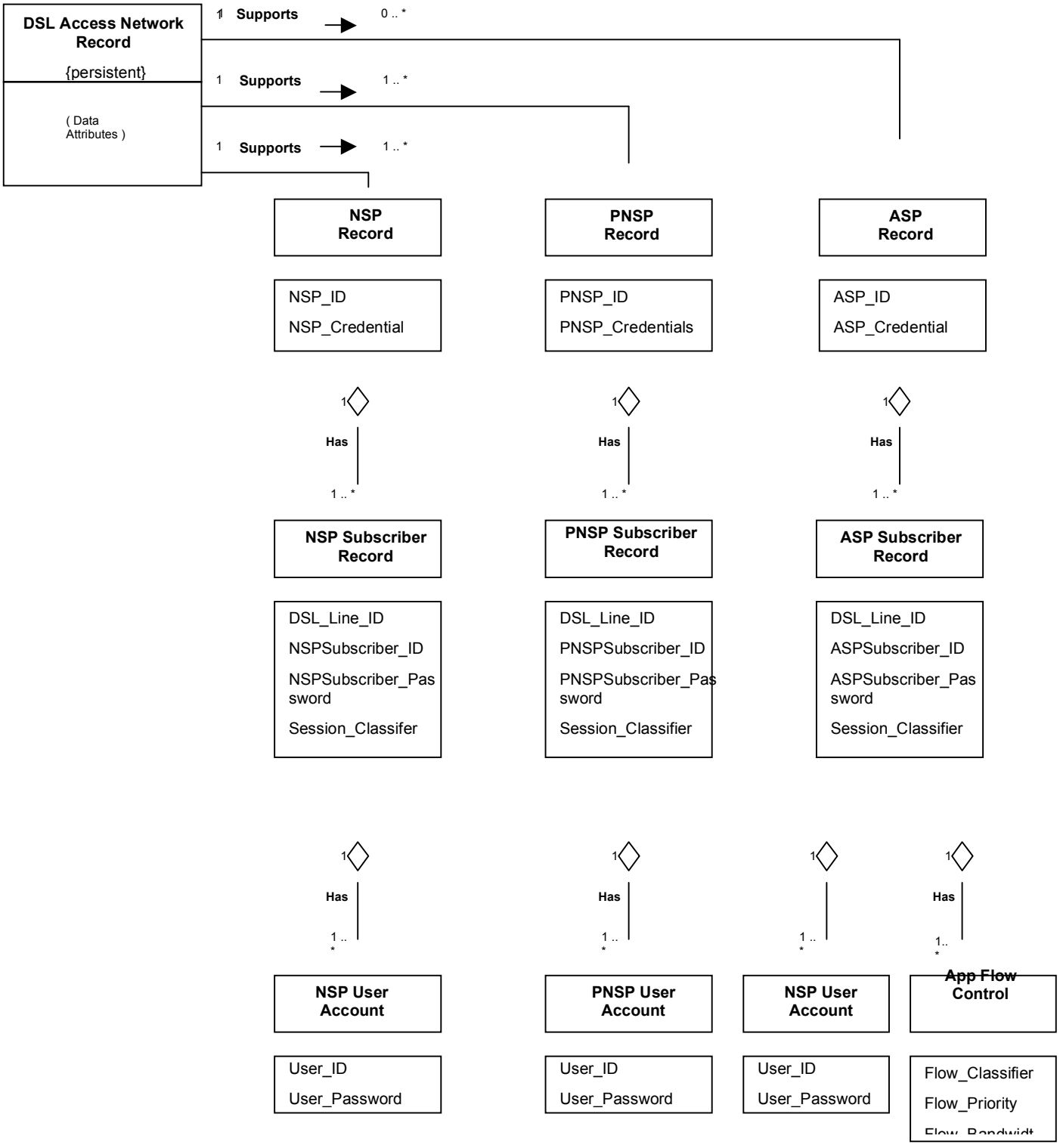


Figure 26 – Detailed UML Representation (ASP, NSP, PNSP)

A.4 Application Service Provider

The Application Service Provider (ASP) is defined as a Service Provider that shares a common infrastructure provided by the Regional/Access Network and an IP address assigned and managed by the Regional Network Provider.

Provides application services to the subscriber (gaming, video, content on demand, IP Telephony, etc.)
Is responsible for the service assurance relating to this application service
Responsible for providing to subscribers additional software or CPE which specific services may
Provides the subscriber contact point for all subscriber problems related to the provision of specific service applications and any related subscriber software.
Does not provide or manage the assignment of IP address to the subscribers

The following data elements are maintained at the ASP:

Record Type	*Elements*	Description	Source
ASP Record		ASP Record is maintained by each service provider. This record contains the service provider's name, password, and other related information that identifies this unique ASP and is used to communicate with Regional/Access Network Provider.	
	ASP_ID	Used to uniquely identify an ASP that has a business relationship with Regional/Access Network Provider.	Assigned by Regional/Access Network Provider at the time of connecting the ASP to the ASP network.
	ASP_Credentials	Used to authenticate an ASP together with ASP_ID when a service session is established with a Regional/Access Network Provider.	Assigned by Regional/Access Network Provider at the time of connecting the ASP to the ASP network.
ASP Subscriber Record		ASP Subscriber Record is maintained by ASP that provides the application service. This record uniquely identifies the subscriber and service related data.	
	DSL_Line_ID	As defined **Error! Reference source not found.**	As defined **Error! Reference source not found.**
	ASPSubscriber_ID	This ID is used for accessing the DSL and ASP networks.	Assigned by the ASP at the time of subscription.
	ASPSubscriber_Password	It is used together with the ASPSubscriber_ID to access the ASP application. Note: The ASP Subscriber ID and Password are only used by ASP for its own purpose and will not be used or referenced by Regional/Access Network for authentication purpose. It is just for maintaining ASP data integrity.	Assigned by the ASP at the time of subscription.
	Session_Classifier	Local copy of Regional/Access Network ASP PPP Session Classification info.	Acquired from the Regional/Access Network through the ANI interface.
	Session_Priority	Local copy of Regional/Access Network ASP PPP Session Priority info.	Acquired from the Regional/Access Network through the ANI interface.
	Session_Bandwidth	Local copy of the Regional/Access Network ASP PPP Session Bandwidth Info.	Acquired from the Regional/Access Network through the ANI interface.

Application Flow Control Record		This record is maintained by the ASP and used to store application specific information such as bandwidth arrangement and QoS settings. This record is tied to the ASP bandwidth Record. Multiple Application Record can be associated with one single ASP bandwidth record.	
	Flow_Classifier	This record is maintained by the ASP and used to store application specific information such as bandwidth arrangement and QoS settings. This record is tied to the ASP bandwidth Record. Multiple Application Records can be associated with one single ASP bandwidth record. It may include Class D addresses to support multicast.	Values provided by the ASP.
	Flow_Priority	Indicates the priority level of the application within the ASP PPP connection. This parameter indicates the treatment of the application flow (what queue it should be placed in) as well as any marking requirements (DSCP). It is used by the BRAS and the RG	Provided by the ASP. The Regional/Access Network Provider specifies available options to select.
	Flow_Bandwidth	Flow_Bandwidth parameter is assigned to the given application based on the negotiated value between the ASP and the Regional/Access Network Provider. It indicates the maximum upstream and downstream bandwidth. It is used by the BRAS & the RG to shape and police the application flow.	These values are provided by the ASP to meet the needs of the application.
ASP User Account		This record is maintained by the ASP. An ASP user account is tied to an ASP subscriber account. Multiple user accounts can be associated with a single subscriber account.	
	User_ID	This ID is used for accessing the given service.	Assigned by a given ASP to a particular user.
	User_Password	It is used together with the User_ID to access a given service.	User_Password is initially assigned by an ASP. Can be changed by the user.

A.5 Network Service Provider

The Network Service Provider (NSP) is defined as a Service Provider that requires extending a Service Provider-specific Internet Protocol (IP) address. This is the typical application of DSL service today. The NSP owns and procures addresses that they, in turn, allocate individually or in blocks to their subscribers. The subscribers are typically located in Customer Premises Networks (CPNs). The NSP service may be subscriber-specific, or communal when an address is shared using NAPT throughout a CPN.

Includes Internet Service Providers (ISPs) and Corporate Service Providers (CSPs)
Is responsible for overall service assurance
May provide CPE, or software to run on customer-owned CPE, to support a given service
Provides the customer contact point for any and all customer related problems related to the provision of this service
Authenticates access and provides and manages the assignment of IP address to the subscribers

The following data elements are maintained at the NSP:

Record Type	*Elements*	Description	Source
NSP Record		NSP Record is maintained by each NSP. This record contains the service provider's name,	

		password, and other related information that identifies this unique service provider and is used communicate with access NSP.	
	NSP_ID	Uniquely identifies the NSP that the subscriber has a relationship with. Used to cross reference users to NSPs who make turbo/QoS requests	Assigned by Regional/Access Network Provider at the time of connecting the NSP.
	NSP_Credentials	Used to authenticate this NSP together with NSP_ID when a service session is established with a DSL access network for requesting a network service.	Assigned by Regional/Access Network Provider at the time of connecting the NSP.
NSP Subscriber Record		NSP Subscriber Record is maintained by NSP that provides the network service. This record uniquely identifies the subscriber and service related data.	
	DSL_Line_ID	As defined **Error! Reference source not found.**	As defined **Error! Reference source not found.**
	NSPSubscriber_ID	This ID is used for accessing the DSL and NSP networks.	Assigned to a DSL subscriber by the NSP.
	NSPSubscriber_Password	It is used together with the NSPSubscriber_ID to access the NSP application. Note: The NSP Subscriber ID and Password are only used by NSP for its own purpose and will not be used or referenced by Regional/Access Network for authentication purpose. It is just for maintaining the NSP data integrity.	Assigned by the ASP at the time of subscription.
	Session_Classifier	Local copy of Regional/Access Network NSP PPP Session Classification info	Acquired from the Regional/Access Network through the NNI interface.
	Session_Priority	Local copy of Regional/Access Network NSP PPP Session Priority info.	Acquired from the Regional/Access Network through the NNI interface.
	Session_Bandwidth	Local copy of the Regional/Access Network ASP PPP Session Bandwidth Info.	Acquired from the Regional/Access Network through the NNI interface.
NSP User Account		This record is maintained by the NSP. A NSP user account is tied to an NSP subscriber account. Multiple user accounts can be associated with a single subscriber account.	
	User_ID	This ID is used for accessing the given service.	Assigned by a given NSP to a particular user.
	User_Password		User_Password is initially assigned by a NSP. Can be changed by the user.

B REFERENCES

[1] Chan, H., R.Chang, “Strifeshadow Fantasy: A Massive Multi-Player Online Game”, Proc. IEEE Consumer Communications and Networking Conference, 2004

[2] DSL Forum, “DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services”, TR-59 Rev 1, September 2003.

[3] Funkhauser, T., “Network Services for Multi-User Virtual Environments”, IEEE Network Realities, Boston MA, Oct 1995

[4] IEEE 1278.2-1995 IEEE Standard for Distributed Interactive Simulation- Communication Services and Profiles, IEEE, New York, NY, USA, April 1996

[5] Manninen, T., “Interaction in Networked Virtual Environments as Communicative Action: Social Theory and Multi-Player Games” Proc. of IEEE CRIWG2000 Workshop, Oct 18-20 Madeira, Portugal.

[6] Pellegrino, J., C. Dovrolis, “Bandwidth Requirement and State Consistency in Three Multiplayer Game Architectures”, Proc. of ACM NetGames 2003, May 22-23, 2003

[7] Smed, J., T. Kaukoranta, H. Hakonen, “Aspects of Networking in Multiplayer Games” Proc. of International Conference on Application and Development of Computer in the 21st Century, pages 74--81, Hong Kong SAR, China, Nov. 2001

[8] Wright, S., S.Tischer, “Architectural Considerations in Online Game Services over DSL Networks”, paper accepted for IEEE ICC2004

[9] Zimmerman, D., B. Rothstein, Y. Kaganovich, K. Pham, “Constructing Client-Server Asynchronous Networked Games using a Single-Computer Model”, California Institute of Technology Computer Science Report #256-80

C GLOSSARY

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding
API	Application Program Interface
ASP	Application Service Provider
BE	Best Effort
BoD	Bandwidth on Demand
BRAS	Broadband Remote Access Server
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
Diffserv	Differentiate Services
DNS	Domain Name Service
DRM	Digital Rights Management
DSCP	Differentiated Services (Diffserv) Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EF	Expedited Forwarding
FQDN	Fully Qualified Domain Name
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Secure Internet Protocol
ISP	Internet Service Provider

L2TP	Layer 2 Tunneling Protocol
LAA	L2TP Access Aggregation
LAC	Layer 2 Access Concentrator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LNS	L2TP Network Server
MPEG	Motion Pictures Expert Group
NAPT	Network Address Port Translation
NSP	Network Service Provider
OSPF	Open Shortest Path First
PC	Personal Computer
PHB	Per Hop Behavior
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PTA	PPP Terminated Aggregation
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAN	Regional / Access Network
RFC	Request For Comments
RG	Routing Gateway
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLO	Service Level Objective
TCP	Transmission Control Protocol
TE	Traffic Engineering
TR	Technical Report (DSL Forum)
TV	Television
UDP	User Datagram Protocol
VC	Virtual Circuit
VoD	Video on Demand
VP	Virtual Path
VPC	Virtual Path Connection
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol
WFQ	Weighted Fair Queuing