Technical Report
TR-010

Requirements & Reference Models for ADSL Access Networks: The ÒSNAGÓ Document

June 1998

Abstract:

This document outlines architectural requirements and reference models for ADSL services and service providers. In specific, it defines target applications, various domain ownership, and requirements of different architectures.

Requirements & Reference Models for ADSL Access Networks: The 'SNAG' Document

June 1998

1. Introduction

1.1 Objective

The Service Network Architecture Group (SNAG) was formed at Orlando meeting on June 18, 1996. The objectives of this group were to

- compile architecture options, requirements and reference models for several key ADSL applications, and
- identify various issues associated with each architecture.

It was not expected that this group could identify the optimal architecture, for it is recognized no architecture would be universally optimal for all carriers. Carriers choose architectures based on not only technical issues but also such considerations as business strategy, economics and regulatory concerns that are outside the expertise of SNAG membership and outside the scope of this document.

In addition, it became increasingly clear as the work of the ADSL Forum continued that there was significant overlap between what the SNAG was attempting to do and the work of the packet and ATM groups. The board of directors thus made a decision to merge the packet and cell based work of the SNAG into the packet and ATM groups respectively. The requirements and model work, which the SNAG team had developed, would be issued as a separate document. This is that document.

1.2 Terminology Used

In this document several words are used to signify requirements which 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, which does not include this option, MUST be prepared to inter-operate with another implementation, which does include the option.

1.3 Document Organization

The current section is an introduction. Section 2 defines the target applications that will be used to examine each architecture option and provides a generic reference model. Section 3 defines requirements for evaluations of architectures.

1.4 Revision History

Date (M/D/Y)	Version	Major Changes.
8/1/96	0.1	First skeleton draft.
9/1/96	0.2	Extended options and limited discussion on issues.
10/1/96	0.3	Added text from London meeting.
2/1/97	0.4	Very minor edits after the Seattle meeting.
4/21/97	0.5	Several rewrites agreed to in Amsterdam.
6/17/97	0.6	Agreements from Boston meeting.
9/17/97	0.7	Final Agreements from Brussels meeting
1/26/98	0.8	Abstract and cover logo added.

2. Target Applications

SNAG chose to consider the most likely applications for ADSL services as 1) Internet access and 2) remote LAN access. However, it was decided to not to preclude a richer set.

Internet access can be for either business customers with multiple PCs or residential customers with one or two PCs. Typically one Internet service provider (ISP) that is selected at the service subscription time services an ADSL subscriber. Dynamic connections to multiple destinations are supported with the regular Internet technology through the ISP.

Similar to the Internet access case, remote LAN access may be required by residential subscribers for telecommuting or by a business LAN for corporate private network. Multiple concurrent connection is a requirement for remote LAN access. For instance, three branch offices need to be connected in a mesh topology. Both Internet and remote LAN access may be required simultaneously by ADSL subscribers.

It should be noted that in the scenarios described above, where multiple connections are simultaneously open from one user access point, a potential security issue exists. This is due to the fact that traffic from one service provider access point can be funneled to the other either knowingly or unknowingly by the user's end system. See the section on security for further notes on this potential."

To provide a reference perspective within which to specify a set of requirements and describe interactions, a SNAG Logical Reference model [5] was developed by the members of the SNAG group as shown below:

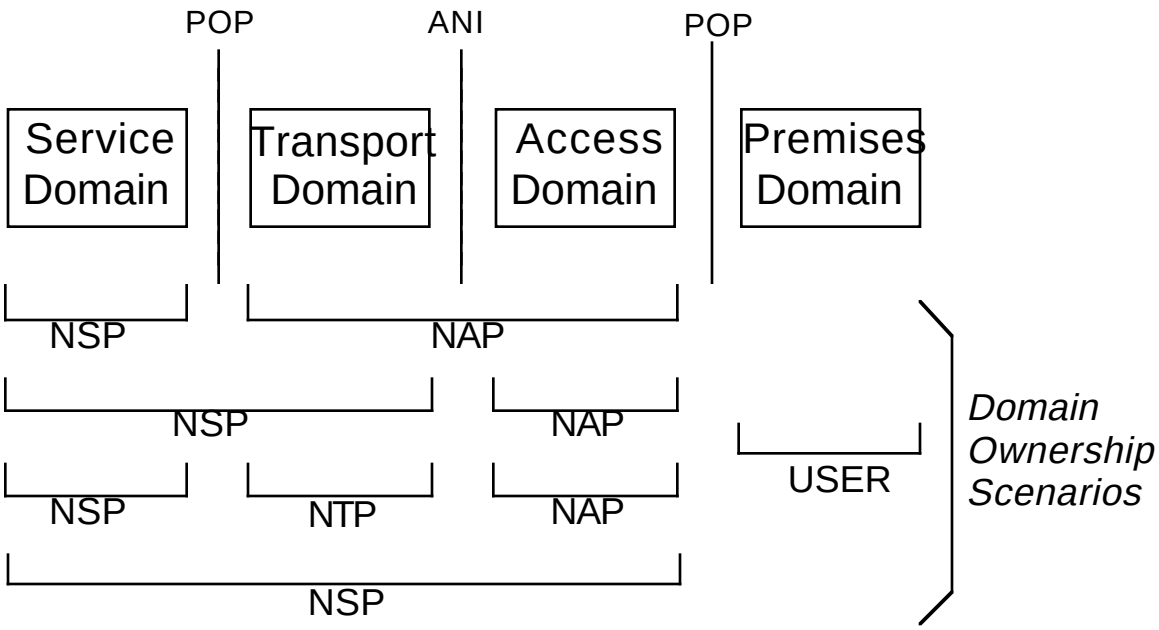

Figure 1. SNAG Domain Reference Model

In this model there are several ÒviewsÓ of an architecture based on the domain ownership, e.g. who owns the components of the architecture outside the user perspective. In this reference model, the ATU-R is located in the premises domain and the ATU-C is located in the access domain.

Here, the acronyms used above are described:

NAP	Network Access Provider
NSP	Network Service Provider
NTP	Network Transport Provider
ANI	Access Network Interface
POP	Point Of Presence

3. Requirements For ADSL Architectures

This section lists the generic requirements of an end-to-end ADSL network. Each requirements is described and then further broken down in terms of how the requirement specifically affects the User, NAP, NTP and NSP.

3.1 Privacy

Privacy needs to be a key attribute of the access and backbone domains. The existing narrowband world typically defines privacy as that provided by the PSTN via circuit switching and a unique physical connection between the central office and the home.

3.1.1 User Specifics

Traffic directed to one User premise network MUST NOT be present on another User premise network.

3.1.2 NAP Specifics

A NAP MUST provide a unique and private connection between a User and an NSP but otherwise be un-involved in implementing privacy policy. A NAP MUST NOT be prohibited from offering value added services such as private user groups.

3.1.3 NSP Specifics

The NSP needs flexibility in its ability to specify and implement a privacy policy. At a minimum this encompasses interconnect, premise to premise, and NSP to NSP.

3.2 Ability to Support Private Address Plans

A User may have business relationships with multiple NSPs. Each NSP may have its own address plan and the User network may also have a private address plan.

3.2.1 User Specifics

Users with private local address plans MUST NOT be prohibited from connecting to an NSP with a separately administered address plan. In addition, switching service sessions between separately administered NSP domains MUST be seamless to the user.

3.2.2 NAP Specifics

A NAP MUST seamlessly and transparently support sessions between separately administered user and NSP domains.

3.2.3 NSP Specifics

An NSP MUST have the ability to serve Users with private address plans. Previous sessions of users with separately administered NSPs MUST not affect a session with a new NSP.

3.3 Service Selection

Service selection deals with the User's ability to seamlessly access an NSP.

3.3.1 User Specifics

A User MUST have the ability to seemlessly select and connect to multiple NSPs. It should be noted that multiple simultaneous connections to NSPs can expose a potential security risk. See section 3.7.1 for further notes.

3.3.2 NAP Specifics

3.3.3 NSP Specifics

3.4 Regulatory Compliance

Access frequently, but not always, occurs across a regulated domain. In this scenario, a mechanism whereby a User can choose a destination must be provided. There is an expectation that the network interface at the ATU-R including all communication to realize a connection to a service providers point-of-presence must be able to be disclosed.

3.4.1 User Specifics

A user MUST be able to connect to an NSP in a standard way.

3.4.2 NAP Specifics

A regulated NAP must comply with local regulatory requirements. These are outside the scope of this document.

3.4.3 NSP Specifics

3.5 Session Control

Given that a session between a User and an NSP access may involve the consumption of scarce resources on the NSP's part, and business and billing models may reflect this, the User should have a mechanism to signal intent to the NSP to initiate and terminate a session.

3.5.1 User Specifics

A User MUST have a method of explicitly setting up and tearing down a session. The User SHOULD be notified when a session is terminated by a NAP or NSP. This notification may be generated by mechanisms local to the premise.

3.5.2 NAP Specifics

A NAP MUST be able to detect if a contracted session service between a User and an NSP is being delivered and where appropriate perform resource recovery.

3.5.3 NSP Specifics

An NSP MUST know when a user is attempting access and have the ability to accept or reject the connection.

3.6 Session Negotiation and Configuration

An end-to-end connection between a User and an NSP may require negotiation and configuration. For example, temporary network addresses and server information may have to be exchanged. Such negotiation and configuration should be supported.

3.6.1 User Specifics

A User MUST have the ability to negotiate and configure session parameters with an NSP. This capability MUST be available on a session by session basis.

3.6.2 NAP Specifics

3.6.3 NSP Specifics

An NSP MUST be able to negotiate and configure session parameters with a User. This capability MUST be available on a session by session basis.

3.7 Simultaneous Access to Multiple NSPs

In some situations, it is expected that multiple Users on a premise network will share a single ADSL link. An ADSL network should allow for multiple sessions over the ADSL link to the same or different NSP.

3.7.1 User Specifics

A User on a premise network MUST be able to access an NSP destination via the ADSL link regardless of whether one or more Users on the same premise network are simultaneously accessing the same or another NSP destination. A single User MAY be able to access more than one NSP at a time. This is commonly known as Ò multi-homing.Ó

3.7.2 NAP Specifics

The NAP must be able to provide multiple connections to the same user domain.

3.7.3 NSP Specifics

The NSP must be able to terminate more than one connection from the same user.

3.8 Minimal Interworking

Maximizing throughput of intermediate systems requires that a minimum of massaging of the data and a minimum of frame/packet hops occurs between the home domain and the service domain.

3.8.1 User Specifics

3.8.2 NAP Specifics

It is desirable that the service offered by the NAP be as transparent as possible in order to not be an impediment to services offered by the NSP.

3.8.3 NSP Specifics

3.9 Service Independence

The premise to POP protocol may vary over the different sessions carried by a NAP.

3.9.1 User Specifics

3.9.2 NAP Specifics

The NAP MUST be transparent to the actual network protocol supported by the User and the NSP.

3.9.3 NSP Specifics

3.10 Service Tiering

The NAP, NTP and NSP require the ability to differentiate the transport and access services they provide to the user. This would be in the form of bandwidth and transit guarantees within the backbone and access domains. Ideally this could be dynamically administered to provide different grades of service on a per-service or flow basis.

3.10.1 User Specifics

The user SHOULD be able to administer their service quality.

3.10.2 NAP Specifics

The NAP SHOULD be able to provide differentiated services.

3.10.3 NSP Specifics

The NSP SHOULD be able to provide differentiated services.

3.11 Authentication

The mechanisms must be provided whereby the User, NAP and NSP can both have a high degree of confidence in whom they are dealing. The existing narrowband world supports mutual authentication via: the Users access an NSP via a well known network identifier (telephone number) which uniquely identifies the service accessed

3.11.1 User Specifics

A User SHOULD connect to an NSP via a well known, unique network identifier.

3.11.2 NAP Specifics

A NAP may or may not want to do authentication. Authentication in the NAP MUST NOT be artificially prohibited.

3.11.3 NSP Specifics

An NSP MUST be provided with a mechanism to identify and authenticate a user. For session oriented access, this typically done through a user name and password for Òalways onÓ authentication the authentication is coupled to the physical or logical connectivity (e.g. PVC vs copper).

3.12 NAP and NSP Accounting Needs

Flexible billing options are necessary at both the NAP and NSP. Both parties should be able to extract appropriate information to authoritatively bill their end-users with a minimum of customer service issues.

3.12.1 User Specifics

3.12.2 NAP Specifics

A NAP MUST have the ability to bill a user or NSP for usage. The type of billing should be flexible (time billing, throughput billing, etc.).

3.12.3 NSP Specifics

An NSP MUST have the ability to bill a user for usage. The type of billing should be flexible (time billing, throughput billing, etc.). An NSP SHOULD be able to reconcile billing from a NAP with the billing of the NSPÕs subscribers.

3.13 Scaleability

A public ADSL network MUST have the ability to scale to a large number of end-users and MAY be required to scale to a suitably large number of service providers.

3.13.1 User Specifics

3.13.2 NAP Specifics

A public ADSL network NAP MUST be able to support a large number of Users and MAY need support a large number of NSPs with possibly multiple POPs.

3.13.3 NSP Specifics

An public ADSL NSP point of presence MUST have the ability to logically or physically scale to support a large number of users.

3.14 Operational Simplicity

Provisioning at both initial service offering and also over the course of the network's lifetime should be minimal. In addition, an ADSL network should be simple to user. End-to-end connections should be able to be made in a straight forward manner. This serves the needs of both Users and NSPs.

3.14.1 User Specifics

A user MUST NOT need special training and MUST NOT have to specially configure the end user system, such as the local PC. An end user system MUST NOT have to be rebooted to connect to an NSP. Ther user should not have to be aware what the ADSL link protocol is (layer 2).

3.14.2 NAP Specifics

The churn of Users from one NSP to another MUST NOT require provisioning on the part of the NAP. The addition of new NSPs MUST require minimal provisioning on the part of the NAP.

3.14.3 NSP Specifics

The addition of Users or deletion of Users from an NSP's service MUST NOT require significant provisioning on the part of the NSP or significant coordination with the NAP.

3.15 Compatibility with Existing Resources

Many resources that will use and ADSL network already exist. The ADSL network should coexist and interoperate with these resources.

3.15.1 User Specifics

Any proposed architecture MUST coexist gracefully with existing PC protocol stacks and no special no special configurations should be necessary.

3.15.2 NAP Specifics

Any proposed architecture MUST be capable of utilizing existing backbone structures. An example an existing backbone structure is an ATM PVC network.

3.15.3 NSP Specifics

Any proposed architecture MUST coexist gracefully with existing NSP infrastructures, including the authorization, provisioning, network address assignment and billing methods.

3.16 Evolution Path

The service set offering should not be constrained such that the first deployment maxes out capability. Note: the Network Migration group is producing standards documents that apply here.

3.17 Security

The Infrastructure of all Domains must be secured against the subversion of its function and unauthorized access to privileged information. Security is affected if the end user system provides multiple simultaneous connections between NSPs. For example, if a user has an IP connection to an ISP and also an IP connection to a Corporate Network simultaneously, irrespective of the underlying transport protocol being used, there is a potential security breach."

This is due to the fact that two different IP links are simultaneously established to the user's end system and there is no fail safe way to prevent the end system from be subverted into routing traffic from one open connection to the other. Although there are situations where multiple simultaneous connections are desirable these must be weighted against the potential security risks they impose.

4. References

Many of the following references are examples of various ADSL architectures and concepts as presented at the ADSL Forum which served as the inspiration for this document.

[1]. D. Veeneman and R. Olshansky, "ADSL IP Concentration", GTE Labs contribution ADSL Forum 96-046, June 1996.

[2]. ITU-T Telecommunication Recommendation I.432, "B-ISDN User-Network Interface Physical Layer Specification"

[3]. T. Starr, "Business Data Services Platform", 1996 DSL Technologies Summit, 27-28th March, 96

[4]. ATM Forum, Packet Mode Report Working Text.

[5]. R.Brown, Minutes of the ADSL Forum - Services Network Architecture Group (SNAG), Seattle, December 1996.