Technical Report
TR-018

References and Requirements for CPE Architectures for Data Access

March 1999

1. Introduction

ADSL and other high speed data access solutions enable subscribers to access the Internet and other data sources at much higher speeds. However, in order to take advantage of this, there is a need for an effective and efficient means of connecting the end-user's PC (or other device) to the ATU-R or other network termination device. Furthermore, as the market for PCs and Internet access continues to grow, there is an increasing need for a means to interconnect PCs in the home.

This document has been developed to support CPE device and computer manufacturers in developing customer premise equipment for the ADSL market. This document presents requirements for extending the high-speed access provided by ADSL through a home distribution network. This home distribution network extends the ADSL Access System to the customer's PC and is critical to enable users to take advantage of ADSL.

This document is meant to provide a framework for which to examine different CPE network architecture proposals against. It presents a set of requirements to clarify the network architecture issues and the needs of the CPE network architecture.

2. User Scenarios

There is significant diversity within the customer's premise and the expected usage of high speed data access services. One common way of describing usage patterns contrasts the SOHO (business) user versus the residential Internet Access user.

A key issue in the development of a CPE Architecture solution is whether multiple PCs will be interconnected sharing a common high-speed data pipe or if it is only a single PC connected to the high-speed data access. Another key issue is the type of applications the end user is expected to use. With these two variables, four usage scenarios[1] have been:

- SOHO (Small Office/Home Office) — These are small offices or branch offices with multiple interconnected PCs used for business purposes. They most likely will want an always-up connection to a single destination. For example, a branch office may want to always be connected to the main office and a small office may always want to be connected to the Internet for web presence

- WAH (Work at Home) Only — These are residential users who use the high-speed access for telecommuting only. Their key concern is that their home environment is indistinguishable from their office environment. They have only a single PC and connect only to their corporations network.

- Internet Access Only — These are residential users who have a single PC and only access the Internet. They may have accounts with multiple ISPs, but do not plan on accessing the different ISPs simultaneously.

- Multi-purpose Residential User- These are the more technologically sophisticated residential users. They typically have multiple PCs at home and access both ISPs and their corporate networks. Members of the household may be accessing different NSPs simultaneously.

Table 2.1: Usage Scenarios

	Single PC	*Multiple PCs interconnected*
SOHO		X
WAH Only	X	

[1] Note that multiple usage scenarios may be present in a single customer premise.

Internet Access Only	X	
Multi-purpose Residential		X

3. Reference Architecture

There are a number of potential configurations for interconnecting a PC with the Broadband Network Termination (B-NT) within a customer's premise. These configurations are driven by the number of PCs (single vs. multiple) and the physical interconnection methods (10BaseT, USB, IEEE1394, ATM25, etc). It is desirable to not preclude support for as many physical interconnection methods as possible.

The ATU-R acts as the demarcation point, and provides an interface to the U-Reference point outside of the customer's premise. An optional hub or switch allows multiple devices to be connected to the B-NT. The hub could be integrated as part of the B-NT, or it may be advantageous for a single PC to act as a gateway to the other PCs in the home.

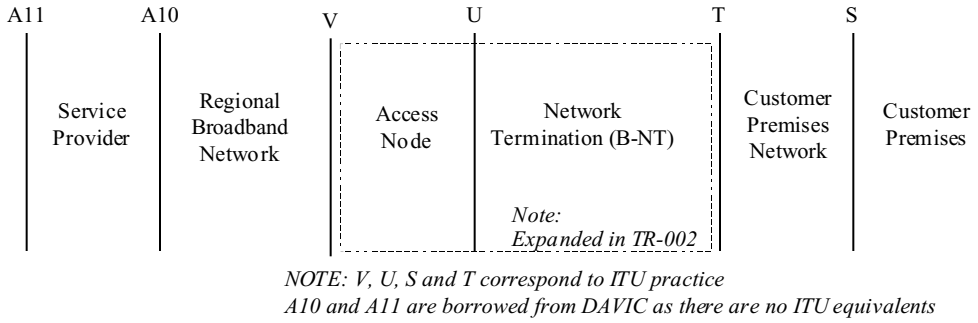

Figure 3.1: Reference Diagram

Figure 3.1 shows the reference model for an ADSL access system. The B-NT corresponds to the Network Termination between the U and T interface in this diagram.

There are a number of potential configurations for implementing the CPN to interconnect a PC(s) with the B-NT within the customer's premise. These configurations include:

- Single PC with B-NT NIC (Network Interface Card) - The B-NT is an internal card in the PC and the ATM session is terminated directly at the PC
- Single PC with external B-NT - The B-NT is external to the PC but connected to a single PC only through one of a number of potential alternatives (USB, 10BaseT, ATM25, etc.).
- Multiple PCs with external B-NT - B-NT connects to a hub or switch which connects a number of PCs. Note, the hub or switch could be integrated into the B-NT.
- Single PC acting as a gateway - B-NT connects to a single PC. This PC is connected to other PCs via a hub. The PC acts as a gateway to other devices on the network.

4. Requirements Overview

4.1 Terminology Definition

This section enumerates the requirement needs of the aforementioned CPE network architecture. As these requirements appear throughout the remainder of this document the reader will find the following designations assigned to each.

- **Highly Recommended** — A requirement that is deemed **necessary** to satisfy the needs of the service configuration. Failure to meet the requirement may cause the application restrictions, or result in improper functioning of the product. Such a requirement is flagged by the letters ÒHRÓ
- **Optional** - Feature or function that is desirable to satisfy the needs of the service configuration. Failure to meet the requirement **should not** cause the application restrictions, or result in improper functioning of the product. An optional requirement is flagged by the letter ÒOÓ
- **Suggested** — A feature or function that is desirable and may become a requirement in the future. However, at this time, because of the state of the technology and market, it is not required for early solutions although it is highly recommended. A suggested requirement is flagged by the letter ÒSÓ

4.2 Structure of Document

Each remaining section of this document explains the requirements for premise networks. Since the requirements may be different for the different Usage Scenarios defined in section 2, the requirements are summarized in table format by Usage Scenario at the end of each section. The earlier subsections explain what the meaning of each feature is.

5. Connectivity Requirements

Section 5 is focused on specific styles of basic connectivity, ability to get a message from ÔAÕ to ÔBÕ otherwise known as reachability. This is independent of latency, quality or any other communication attributes.

In general there are many types of connectivity but for residential and SOHO applications the most common form will be Òstub Ónetworks which have a single point of attachment to the NSP. This is opposed to meshed networks requiring routing protocol exchange and possibly bandwidth brokerage between the network and the premises such that local path optimization can be performed.

Stub networks can be considered in two forms, simple point to point to the outside world (single end system to single VC on the WAN mapping to a single POP), and aggregation (multiple end-system to single VC on the WAN mapping to a single POP). Both may coexist, and both may be overlaid on top of the premise network. More complex scenarios can be built up by overlaying multiple instances of these two models to create service multi-homing scenarios.

5.1 Sessions to individual appliances

Sessions to individual appliances is accomplished by transporting PPP from the end system (e.g. PC) across the premise network to the NT. The premises network may be NULL in the single PC case and may involve tunneling where shared media is concerned. For non-ATM premise networks, the PPP session is then mapped to an individual VC at the NT.

5.2 Multi-homing of individual appliances

This is similar to 5.1, however there is a mechanism whereby an individual end system may support more than one PPP session (and the NT must be able to support a corresponding number of VCs if it is consistent with TR-012). The transport between the PC and the NT must be able to support some form of multiplexing in order to carry multiple PPP sessions.

5.3 Multiple sessions to single NSP

As described above, the number of homes with multiple PCs is already approaching a critical mass. In addition, there are a significant number of small or home offices (SOHO) which are expected to have multiple devices. This trend of multiple devices within a home will only increase. A CPE network architecture must connect these devices within a home and allow them to share a common link to an NSP.

In this scenario, the NT or some proxy must perform an aggregation function (bridging or routing) such that one or more subnets in the premises on the same Layer 3 network all have logical connectivity with an external Layer 3 network (i.e. NSP). PPP, as mandated in TR-012, could most likely be terminated where the aggregation function is located. It is assumed that there is only one L3 port at the NT and the premise media only supports a single L3 instance.

5.4 Simultaneous sessions to multiple NSPs

It may be desirable for a single user or multiple users on a single CPE network, to have active sessions with different NSPs simultaneously. While there is a potential security problem here, especially when one of the NSPs is a corporation, the CPE network architecture should not preclude this capability.

This scenario is similar to 5.3, however the premises media permits some form of layer 2 multiplexing in order to permit multiple Layer 3 domains to be simultaneously supported. Each layer 3 interface may be combined with an aggregation function (e.g. routing) to permit the interface to be used by more than one hostÓEach interface would typically resolve to either an ATM VC, layer 3 tunnel, or other point to point form of connectivity across the Ô/Õnterface.Ó

5.5 Administer and control network connectivity

Service providers m ay choose to deploy PVCs, SVCs or PVCs and SVCs side by side. The CPE network architecture must support the ability for the end user to control SVC signalling in an SVC environment or to choose the proper PVC in a PVC environment.

5.6 Support intra-premise networking

The CPN must support PC to PC communication within the home without traversing the access network. In addition, connectivity to the outside world should not interfere with the premise network. In the case of a branch office, the premises network is just an extension of the corporate network. In the case of a WAH or IAO or MFR scenario, separate logical connectivity to services in the premises (e.g. printer, local server etc.) may be separately administered or predate connectivity to the NSP network. When transient single PC connectivity to an NSP is required, it should not require re-configuration of other devices in the premises.

5.7 Simultaneous access via multiple access providers

The premises may have more than one broadband access port. In this scenario, meshed access to a single NSP is possible (which requires either exchange of routing information and/or a bandwidth brokering function as alluded to in the section introduction) or specific ports may have specific NSP associations and connectivity to a specific NSP may also require a discovery mechanism .

5.8 Requirements Summary by Usage Scenario

Table 5.1 Connectivity Requirements				
Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Sessions to Individual Appliances (5.1)	O	O	HR	HR
Multi-Homing of Individual Appliances (5.2)	S			HR
Multiple sessions to a single NSP (5.3)	O	O	O	S
Simultaneous sessions to multiple NSPs (5.4)	O			HR
Administer and Control Network Connectivity (5.5)	HR	HR	HR	HR
Support Intra-premise networking (5.6)	HR	S	S	S
Simultaneous access via multiple access providers (5.7)	O			O

6. Simultaneous sessions to multiple NSPs

When there is simultaneous access to multiple L3 domains, there are a number of issues to be resolved. This section presents requirements for this situation only.

6.1 Domain isolation/binding

Layer 3 domains may be separately administered which means that inconsistencies in network numbering plans may cause mis-directed data. The premises system requires a mechanism to keep connectivity to separate L3 domains logically separate.

6.2 Security

L3 domains may require mechanisms to prohibit deliberate attempts to permit cross domain reachability, such as reaching the corporate network from the public network.

6.3 Requirements Summary by Usage Scenario

Table 6.1 Multi-Domain Requirements				
Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Domain isolation/binding (6.1)	HR			HR
Security (6.2)	HR			HR

Notes:
- *WAH and Internet Access Only scenarios will not have simultaneous sessions to multiple NSPs so these requirements do not relate to them.*
- *SOHO optionally supports simultaneous sessions to multiple NSPs. The requirements only apply to the cases where this is supported.*

7. Service Transparency

7.1 Supports at least one layer 3 protocols

The premise architecture should be capable of supporting multiple layer 3 protocols. This does not suggest that specific products that are compatible with the architecture are prohibited from only implementing a single layer 3 protocol. In addition, non-routable protocols may have limited connectivity. This would be reflected in the connectivity options that could be employed.

7.2 Does not interfere with layer 3 service set

Connectivity to the NSP should not preclude services. For example, the use of IP network address translation has implications for e-commerce and multi-player gaming which may not be acceptable for recreational broadband access.

7.3 Access technology agnostic

While current work efforts are focusing on high-speed data access via ADSL, the CPE network architecture solution should not be ADSL centric. In order for a CPE network architecture solution to be successful and adopted by the industry and consumers, it must allow the consumers to choose and change their access technology while retaining the functionality of their CPE network architecture.

7.4 Premises technology agnostic

There are a number of technologies that can support the connection between a subscriber's PC and the ATU-R or other high-speed access equipment. Home networking technologies differ in the bandwidth they support, the number and type of devices they can network together, and the physical media that they operate over. It is likely that all of these technologies and others will exist within subscribers' homes. As such the CPE architecture should not preclude connection between in-home devices and the high-speed data network with any of these technologies. The premises networking technology should be transparent to the architecture.

This may be a difficult requirement . Generalized attributes may have to be considered or specified such as layer 2 multiplexing, broadcast and multicast capability, latency management etc.

7.5 Compatible with AAA services

The CPN should be compatible with the authentication, authorization, and accounting mechanisms utilized by the NSP

7.6 Does not preclude side by side with non data services

The premise architecture should not preclude other, non-data centric services from being offered by the same access link

7.7 Support Standard Interfaces in the Premise

The premise network should be based on open, standard interfaces.

7.8 Information Appliance Agostic

The premise architecture will not make assumptions as to the nature of the information enabled devices deployed on the home network, and further, there is no assumption that such devices require other services than local connectivity

7.9 Requirements Summary by Usage Scenario

Table 7.1 Service Transparency Requirements

Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Support at least one layer 3 protocol (7.1)	HR	HR	HR	HR
Does not interfere with layer 3 service set (7.2)	S	S	HR	HR
Access Technology agnostic (7.3)	S	S	S	S
Premise technology agnostic (7.4)	S	S	S	S
Compatible with AAA services (7.5)	HR	HR	HR	HR
Does no preclude side by side w/ non-data services (7.6)	S	S	S	S
Support standard interfaces in the Premise (7.7)	S	S	S	S
Information Appliance Agnostic (7.8)	HR	HR	HR	HR

8. Access Transparency

8.1 Access network isolation from premises configuration

Premise configuration should have no impacts on access network provisioning. The premise configuration should also have no impact of network scalability. Premise network configuration may have impacts on network service provisioning (e.g. network address administration).

8.2 Fault isolation capability for access/premises boundary

The NT should have sufficient functionality to permit fault isolation between the premise network and the access network.

8.3 Requirements Summary by Usage Scenario

Table 8.1 Access Transparency Requirements				
Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Access network isolation from premise configuration (8.1)	HR	HR	HR	HR
Fault isolation capability for access/premise boundary (8.2)	HR	S	S	S

9. Reliability

9.1 Minimize single points of failure

The CPN should minimize the pieces of equipment that are critical to network wide data communications.

9.2 Isolation of premise from access network faults

An access network failure should not be able to impact private intra-premise networking.

9.3 Premise is not dependent on the access network

The premise network should not be dependent on elements within the access/service provider network (e.g. DHCP server) to enable intra-premise networking.

9.4 Requirements Summary by Usage Scenario

Table 9.1 Reliability Requirements				
Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Minimize single points of failure (9.1)	S	S	S	S
Isolation of premise from network faults (9.2)	HR	S	S	HR
Premise not dependent on the network (9.3)	HR	S	S	HR

10. Configuration

10.1 Simple installation, administration. and management

The complexity of setting up and managing corporate LANs is viewed as requiring experts and a dedicated department. If such technology is going to migrate to the home, the administration must be simplified. ÒPlug and PlayÓ is necessary if typical consumers are going to adopt home networking technology.

A minimum of administration in the premise should be required for local networking. Connectivity services to the outside world should not impact administration of the premise network. The user should not be obligated to manually replicate any information on access services that is automatically known to or manually provisioned at any system on the premises network.

10.2 Provide Configuration Information

The CPN should provide a mechanism to distribute necessary network configuration information to the end devices.

10.3 Requirements Summary by Usage Scenario

Table 10.1 Configuration Requirements				
Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Simple Installation, Administration and Management (10.1)	S	S	HR	HR
Provide Configuration Information (10.2)	S	HR	HR	HR

11. Connectivity Administration

11.1 Dynamic NSP selection

The premise architecture should permit the user to dynamically select an NSP with which to establish a session.

11.2 Subscriber Initiated session

The premise architecture should permit any end system to initiate a connectivity instance to an NSP. This may require interworking at an NT2 between the premise network and the termination of signalling from the access network.

11.3 Always Accessible

There is two aspects to this. The premise architecture should permit peer networking such that other end systems may initiate a connectivity instance with the premise network (subject to local policy), and the premise architecture should permit a degree of continuous network presence without impacting access network scalability.

11.4 Requirements Summary by Usage Scenario

Table 11.1 Connectivity Administration Requirements				
Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Dynamic NSP selection (11.1)	S	S	HR	HR
Subscriber Initiated Selection (11.2)	S	HR	HR	HR
Always Accessible (11.3)	HR	HR	HR	HR

12. Quality Capability

12.1 Traffic prioritization

Ability for CPN to give preferential treatment to traffic with high prioritization

12.2 Flexible Bandwidth reservation & management

Ability for CPN to dynamically allocate available bandwidth resources according to the user or users demands.

12.3 Latency appropriate for Voice

Ability to control latency in premise on an application basis

12.4 Select VC based on QoS or CoS parameters

For architectures which use PVCs, the ATU-R must be able to select a PVC for upstream traffic based on QoS, and CoS attributes required by the CPE's application, in addition to the destination network address.

12.5 Requirements Summary by Usage Scenario

Table 12.1 Quality Capability Requirements				
Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Traffic prioritization (12.1)	S	S	S	S
Flexible bandwidth reservation and Management (12.2)	S	S	S	S
Latency appropriate for voice (12.3)	S	S	S	S
Select VC based on QoS or CoS parameters (12.4)	S	S	S	S

13. Evolution

13.1 Native ATM services not precluded

The CPN should not prevent native ATM services from being offered to some or all end systems in the premise.

13.2 Independent evolution of PC and ATU-R

The software drivers on the PC and ATU-R should be able to evolve independently and upgrades to one should not risk isolation of communication.

13.3 Requirements Summary by Usage Scenario

Table 13.1 Configuration Requirements				
Feature	**Usage Scenario**			
	SOHO	**WAH Only**	**Internet Access Only**	**Multi-purpose Residential**
Native ATM Services not Precluded (13.1)	O	O	O	O
Independent evolution of PC and ATU-R (13.2)	S	S	S	S