Service Provisioning in an ATM-over-ADSL Access Network

Reuven Cohen
Dept. of Computer Science
Technion, Haifa 32000, ISRAEL

Abstract

Asymmetric Digital Subscriber Loop (ADSL) technology is a new platform for delivering broadband services to homes and small businesses, thus bringing the information highway to the mass market. Successful deployment of an ADSL-based access network is not only a matter of delivering faster rates, but also offering solutions that are cost-effective and easy to use and to manage. As deregulation and competition spread globally, an ADSL-based access network should also enable end users to choose their service providers dynamically, and to switch from one provider to another easily and rapidly, even on a real-time basis. In light of these requirements, the paper addresses the issue of service provisioning in an ATM-over-ADSL access network. It concentrates on the provisioning of services using the PPP protocol. PPP is the common protocol for service provisioning in circuit-switched telephone networks. However, it is also considered as a good choice for the delivery of broadband services since it has built-in mechanisms for IP address assignment, layer-2 security and AAA (Authentication, Authorization and Accounting). The paper presents the problem of initiating a PPP connection at an Ethernet-based host. It presents several solutions for this problem and discusses the advantages and disadvantages of each solution.

1 Introduction

Asymmetric Digital Subscriber Loop (ADSL) technology is a new platform for delivering broadband services to homes and small businesses, thus bringing the information highway to the mass market. ADSL can be implemented on most of the existing copper infrastructure, enabling the rapid and near ubiquitous offering of new high-speed data access services with minimal expense. ADSL supports a wide variety of high-bandwidth applications, such as high-speed Internet access, telecommuting, virtual private networking, and streaming multimedia content. Most of these applications follow a typical client-server model, where the majority of information is sent downstream toward the client. Depending on line quality, distance, and other physical parameters, ADSL downstream rates range between 1.5 to 8 Mbit/s, whereas upstream rates range between 16 and 640 Kbit/s.

Due to the need to protect Internet Service Providers (ISPs) and other enhanced services providers from anti-competitive practices by the Network Access Providers (NAPs) – the local Telcos that own and operate the access networks – there is a technical distinction between the former, collectively known as Network Service Providers (NSPs), and the latter. The NAPs provide data transport between the customer premises and the NSP's facilities. The NSP is usually responsible for "upper layer" activities such as security, name resolution and application servers. NSPs can be classified into three main categories:

1. Internet Service Providers, that provide the resources required for efficient surfing the Internet through the access network. Examples for these resources are the bandwidth to the Internet backbone, DNS (domain name system) service, IP addresses, Web caching etc.

2. Corporations that provide their employees direct (i.e. not through an ISP) remote access to their Intranet for telecommuting. Small corporations will provide indirect access to their networks, through an ISP. Such corporations do not have a point-of-presence (POP) in the access network, and therefore are not considered as NSPs.

3. The providers of other broadband services, like video on demand, online shopping, distance learning etc.

Real-time audio and video applications have become increasingly popular, especially over the Internet. These applications require Quality of Service (QoS) support to ensure their performance. Therefore, most NAPs prefer to use ATM rather than frame-based technology in their access network With ATM over ADSL, a connection can be established from the end user to any endpoint on the ATM network. Though it is most likely that in the near future the ATM connection will terminate at the NAP, ATM will allow future end-to-end connectivity with quality of service (QoS) support between the end users and their NSPs. In such a configuration, the equipment within the NAP network will perform only cell transport, aggregation and switching across various media.

However, successful deployment of an ADSL-based access network is not only a matter of delivering faster rates. It also involves offering solutions that are cost-effective and easy to use and to manage. The NSPs and end users will only adopt solutions that leverage their current infrastructures and protect past investments. Specifically,

- Since ISPs and corporations already have an infrastructure to support dial-up access based on PPP, an ADSL-based access should support PPP between end users and NSPs.

- End users want solutions that let them use their existing hardware and software, or to buy a standard and cheap configuration. In most of the cases, this means a PC with an Ethernet NIC and MS Windows operating system.

As deregulation and competition spread globally, in addition to the support of these two requirements, an ADSL-based access network should enable end users to choose their NSPs dynamically, and to switch from one NSP to another (e.g. from the corporate Intranet to an ISP) easily and rapidly, even on a real-time basis, without costly and time-consuming intervention from the NAP.

This paper addresses the issue of service provisioning in an ATM-over-ADSL access network. Section 2 describes the architecture of such a network. Section 3 describes the problem of setting up a PPP connection over a MAC layer (Ethernet) rather than over a point-to-point physical or virtual line. This section also presents several approaches for solving this problem. Section 4 describes the proxy-PPP solution for this problem. This solution seems to have many advantages over those described in Section 3, especially if it is employed in conjunction with a web-based service selection scheme that allows users to change NSPs dynamically and rapidly. Finally, Section 5 concludes the paper.

2 An "ATM over ADSL" Access Network Architecture

A typical "ATM over ADSL" access network is presented in Figure 1 [1, 2]. The user side of the ADSL link is implemented in a device called ATU-R. This device also has the functionality of upper layers, including ATM, Ethernet and IP. In most cases the customer premise network will contain

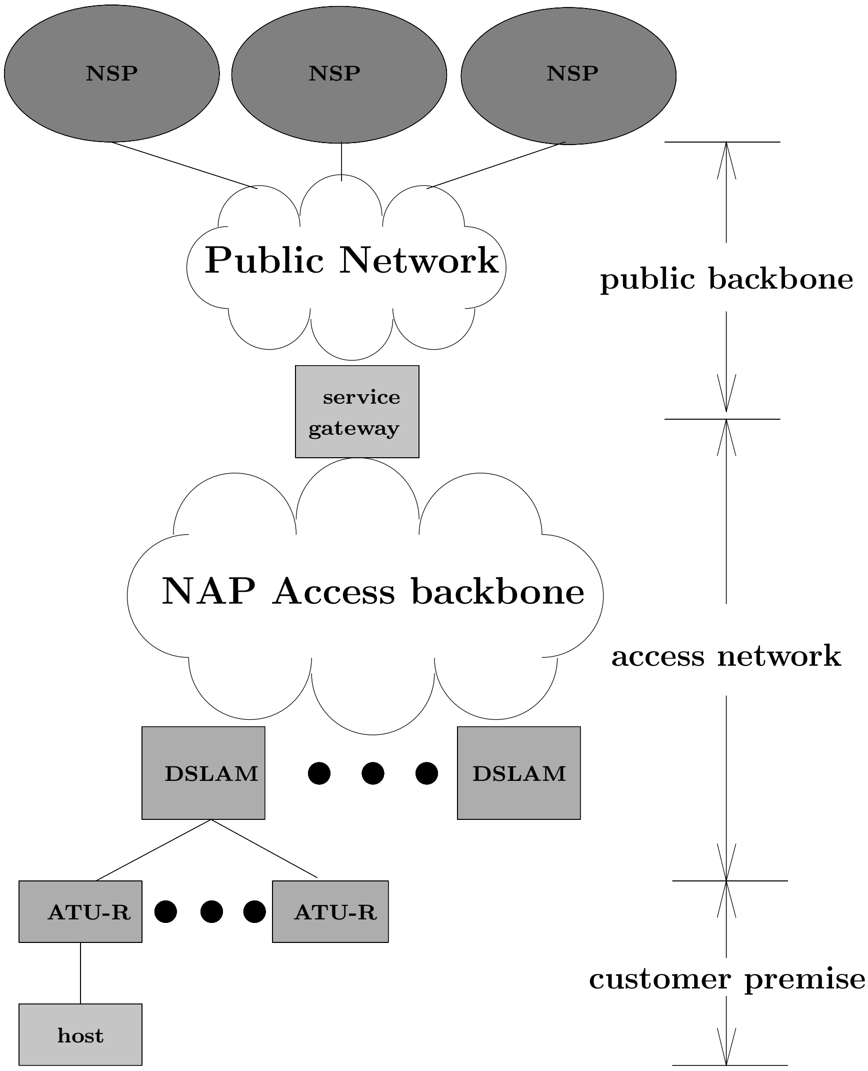
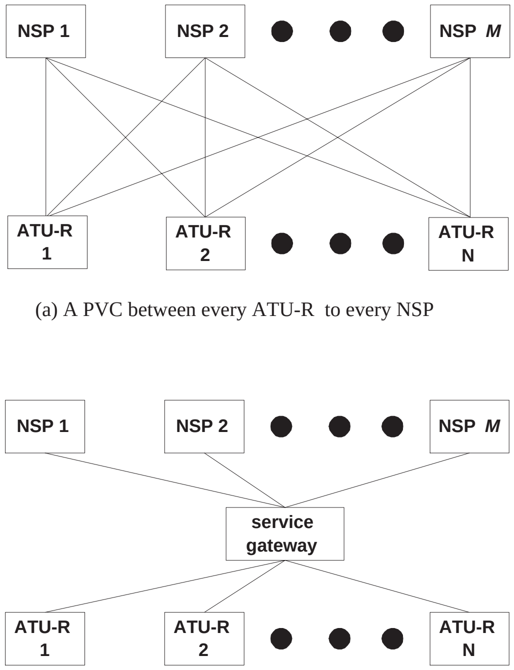


Figure 1: A Typical ADSL-based Access Network

a single host connected to the ATU-R. However, in a typical SOHO (small office, home office) there might be several hosts connected to the same ATU-R by means of a hub or a switch.

The ATU-R is connected to the access network. This network is owned and managed by the NAP (Network Access Provider – usually a Telco company). The main component in the access network is the ADSL Access Multiplexer (DSLAM). Each DSLAM connects several hundreds of ATU-Rs to the access backbone. The DSLAM implements the network side of the ADSL link. However, it also has ATM functionality, as well as some capability of higher layer protocols. In dense neighborhoods, the access network will be hierarchically structured, such that multiple DSLAMs in the same geographical area will be connected through an ATM switch.

Each Network Service Provider (NSP), that provides broadband services to the users of the



(a) A PVC between every ATU-R to every NSP

(b) A PVC from every ATU-R and NSP to the service gateway

Figure 2: PVC Layout With and Without a Service Gateway

access network, is assumed to have a Point of Presence (POP) in the access network. In most cases, today's ATM backbones and ATU-Rs do not yet have the Switched Virtual Circuit (SVC) capability that would allow flexible operation like in a conventional telephone network. Instead, the backbones use Permanent Virtual Circuits (PVCs) that act as static pipes. With this model, providing each of the users the capability of getting connected to each of the NSPs would require setting up and maintain $O(N * M)$ PVCs (Figure 2(a)), where N is the number of users and M is the number of NSPs. To support a more scalable solution, a new networking device is installed in the regional backbone, usually on the border with the access network. This device is referred to as a "service gateway" (see Figure 1), a "broadband access server" [2] or an "access router". With a service gateway, in order to allow each user to connect to every NSP, it is sufficient to set up a single PVC between every customer premise and the service gateway, and between every NSP and the service gateway. Therefore, the number of PVCs is reduced from $O(N * M)$ to $O(N + M)$. This PVC layout is shown in Figure 2(b).

The role of the service gateway is to dynamically bind between the customer PVCs and the NSP PVCs, based on the customer service requirement. As already indicated, it is expected that at least in the first stage users will get IP connectivity to their NSPs using PPP. This is mainly because PPP satisfies most of the requirements associated with remote connectivity to an NSP, like IP address assignment, security and AAA (authentication, authorization and accounting). In addition, since ISPs and corporations are familiar with PPP-based connectivity, easy migration from existing ISP infrastructure is expected.

The set up of a PPP connection over an ATM VC is addressed in [7, 8]. However, in order to extend a PPP connection from PVC to another, and in order to allow multiple PPP connections to be multiplexed over the PVC between the service gateway and the NSP, a new protocol called L2TP (Layer 2 Tunneling Protocol) has been defined [5]. When a user initiates a PPP call, data is transported from the user premises over a PVC to the service gateway. After momentarily terminating the call, the service gateway "extends" the PPP through an L2TP tunnel ending at the target NSP. Since L2TP allows multiple PPP calls to be multiplexed over each tunnel, there is no need to set up a tunnel or a PVC between the service gateway and the NSP for every user. Rather, one tunnel over one PVC, as shown in Figure 2(b), is sufficient. More tunnels can be established over one or multiple PVCs in order to satisfy different Quality of Service (QoS) levels or for security considerations.

Since an NSP only needs to replace the underlying layers for carrying the PPP session, from an analog modem bank to an L2TP tunnel(s), the majority of the ISP infrastructure is maintained. Moreover, with this model, users can easily terminate the PPP session with one service provider, and establish a new session with another provider dynamically, without costly and time-consuming intervention of the NAP.

3 The "PPP Over Ethernet" Problem

It is expected that at least at the beginning of ADSL deployment, the connectivity between the user PC and the ATU-R will be based on Ethernet. This is mainly due to the following reasons:

- An Ethernet NIC is cheap, and available in almost every LAN PC. ATM NICs are much less prevalent due to their cost and configuration complexity.

- An Ethernet-based ATU-R provides an economical and simple solution for SOHO (Small Office Home Office) networking, as shown in Figure 3. SOHO networking enables families and small offices to share important computing resources, like printers, files and remote access capability. For clarification, this figure distinguishes between the ATU-R and the Ethernet hub. However, some ATU-R vendors incorporate the hub functionality into the ATU-R.

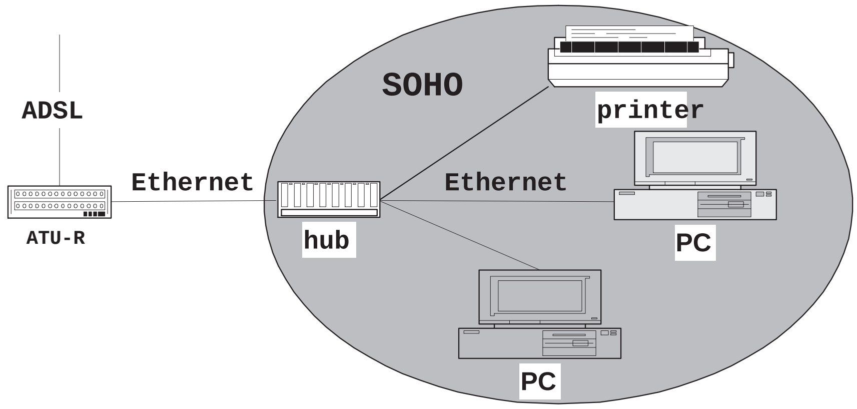


Figure 3: A SOHO Connected to the World Through an Ethernet-based ATU-R

However, an Ethernet-based connectivity between user equipment and the ATU-R imposes a new challenge, of initiating a PPP connection at a host with a Ethernet-based TCP/IP networking stack. Several solutions have been proposed so far for addressing this problem. These solutions are presented in what follows.

The PPPOE solution defines a new layer, called PPPOE, at the host protocol stack. This layer glues the PPP layer to the Ethernet layer (see Figure 4). In this solution a PPP packet is encapsulated in an Ethernet frame and transmitted to the ATU-R. The Ethernet frame is then forwarded over the ATM VC until reaching the service gateway. At the service gateway, the PPP packet is extracted and forwarded over the appropriate L2TP tunnel to the target NSP. Before data transmission, the PC's PPPOE initiates a search protocol in order to detect the MAC address of a "PPPOE server". In this scenario, the functionality of the PPPOE server resides at the service gateway (see Figure 4). However, another option is to implement this functionality in the ATU-R. In such a case, the ATU-R sends to the service gateway IP packets rather than Ethernet frames, over the ATM PVC.

As Figure 4 shows, the IP layer in a PPPOE-based networking stack has an interface to both PPP and Ethernet. Hence, PPPOE allows the PC to send IP packets both to local hosts, through Ethernet, and to remote hosts, through PPP over Ethernet. The decision whether to encapsulate the IP packet in an Ethernet frame or in a PPP frame (and then in an Ethernet frame) is made based on a the network address part of the destination IP address. If the network address is equal to the local network address, the packet is sent through Ethernet directly to the destination. If they are different, the packet is sent through PPP to the NSP, provided that a PPP connection is indeed open.

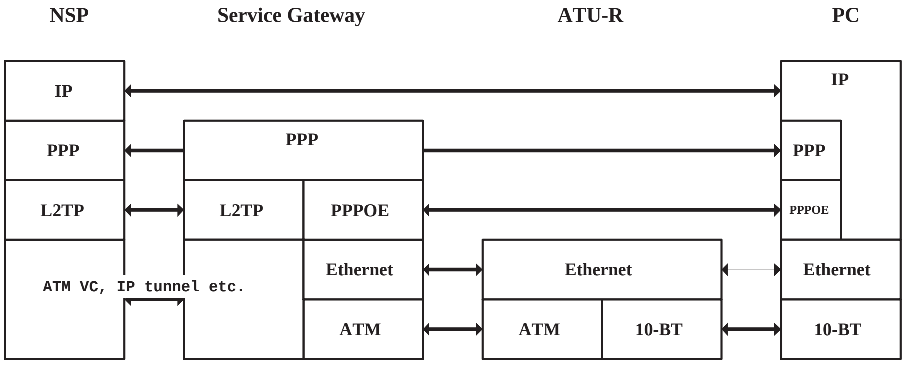


Figure 4: Protocol Stack for PPPOE

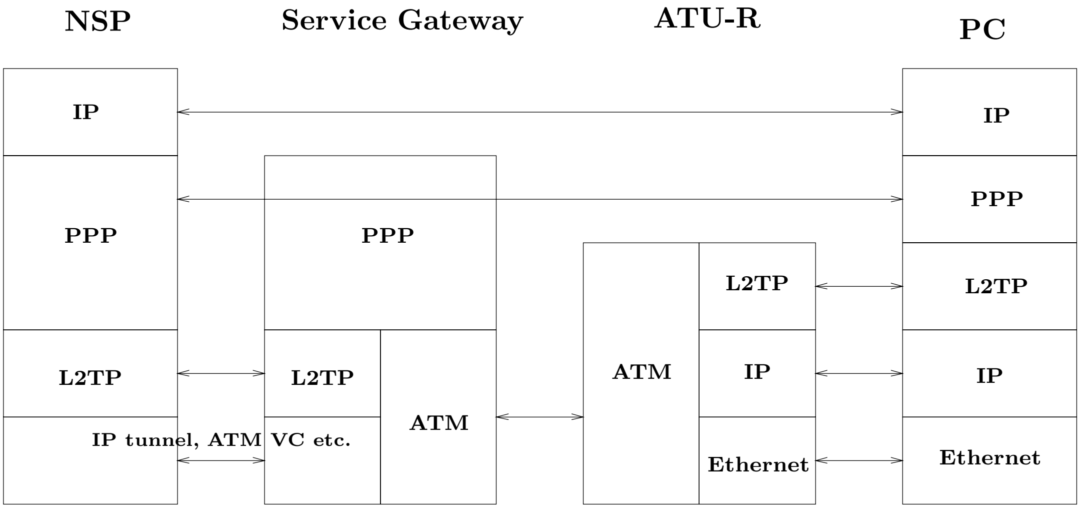


Figure 5: Protocol Stack for L2TP

Another possible solution for the PPP over Ethernet problem is to tunnel the PPP connection between the PC and the ATU-R, or between the PC and the service gateway, through an L2TP tunnel. The first configuration is shown in Figure 5. The main advantage of this solution over a PPPOE-based solution is that L2TP is not a new protocol. However, it was defined in the context of VPN (Virtual Private Network) rather than for solving the PPP over Ethernet problem. For solving the PPP over Ethernet problem, a not-yet-standardized version of L2TP needs to be employed. L2TP is more complicated than PPPOE. In particular, it requires another IP layer in order to build a tunnel between the PC and the ATU-R (see Figure 5).

A third solution for solving the PPP over Ethernet problem is BMAP (Broadband Modem Access Protocol) [6]. Unlike the PPPOE- and the L2TP-based solutions, the network stack of the PC also contains ATM layers (Figure 6). The main idea is that the PPP frame is segmented at

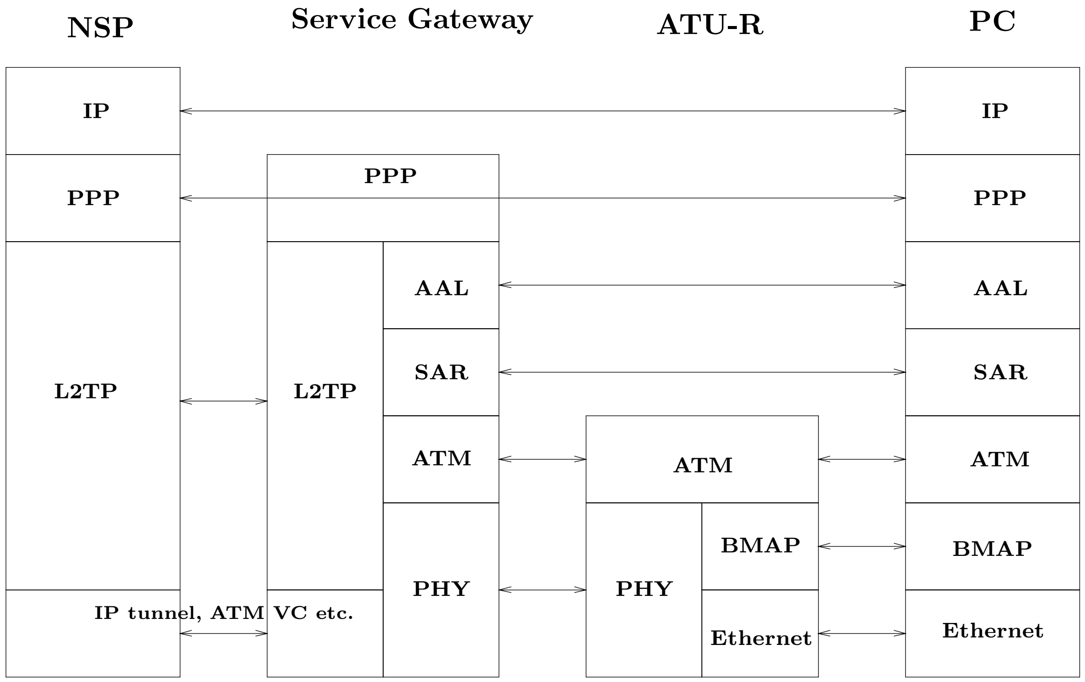


Figure 6: Protocol Stack for BMAP

the PC into ATM cells which are then encapsulated into one or more Ethernet frames and sent to the ATU-R. To reduce the encapsulation overhead, BMAP allows to encapsulate several ATM cells in a single Ethernet frame. The main advantage of this approach is that the ATM functionality needed at the ATU-R is simplified. In particular, there is no need for the ATU-R to perform signaling, SAR (Segmentation and Reassembly), and traffic management. Beside the complexity of the PC network stack, the main problem of BMAP is that if more than one PC wishes to access the ATU-R at the same time, one PC must act as a “server” for all other PCs. This is because at every time the ATU-R can be bound only to one particular PC, and only this PC is allowed to send data through the ATU-R. The traffic from a non-server PC must be sent first to the server PC and then is forwarded to the ATU-R. This is of course a non-efficient way to support SOHO inter-networking.

4 The proxy-PPP Approach

Solutions based on PPPOE, L2TP and BMAP have one major drawback in common: they require to change the standard Ethernet/IP/TCP networking stack at the user PC. Telcos want to avoid the expenses associated with installing and maintaining new software at their customers' PCs.

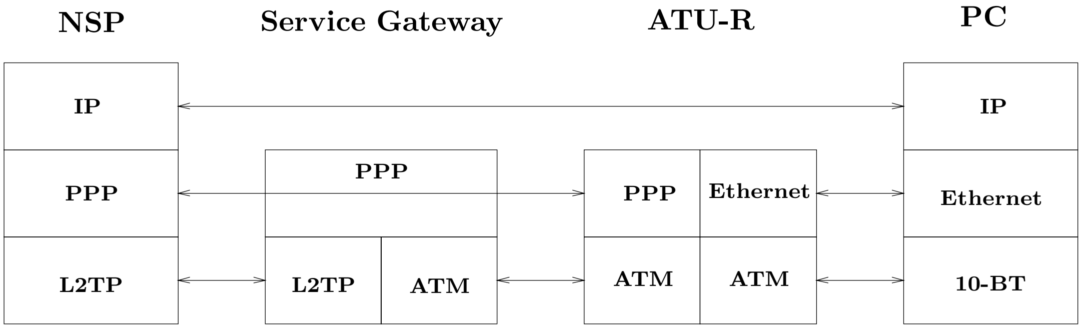


Figure 7: Protocol Stack for Proxy-PPP

Therefore, a solution for the PPP over Ethernet problem that require no change to the standard Ethernet/IP/TCP networking stack is preferable in most cases.

In this section we present the proxy-PPP approach. The main advantage of this solution is that no change is required at the user PC. As shown in Figure 7, the proxy-PPP architecture requires a standard Ethernet/IP/TCP stack in the PC. Unlike in the previous solutions, in proxy-PPP the PPP connection starts at the ATU-R. The ATU-R receives from the SOHO's PCs IP packets encapsulated in Ethernet frames. It extracts the IP packets, and forwards them over the appropriate PPP connection(s).

A possible implementation of proxy-PPP is as follows. Every SOHO's PC and the ATU-R (on its Ethernet interface) are assigned a private IP address with the same network address. As defined in [9], a private address cannot be used in the Internet because it is not globally unique. The ATU-R is defined as the default router for every PC. This can be done automatically, without user intervention, using DHCP [3]. Consequently, every packet sent by a PC to a non-local destination is sent to the ATU-R. The ATU-R locates the NSP with which the PC is associated, changes the source IP address from the local address of the sending PC to the address allocated by the NSP, and forwards the packet in ATM cells over the ATM VC connected to the target NSP. When multiple PCs are allowed to share a single PPP connection then port numbers may also have to be translated by the ATU-R.

There are several possible ways to configure the ATU-R with the parameters needed for setting up the PPP connection(s) associated with every calling PC. However, it seems that a web-based interface is the most attractive approach. In this approach, the ATU-R serves also as a lightweight web server. When a user wants to connect to an NSP, the user first connects to the ATU-R web server in order to get a menu of possible NSPs. The menu can be achieved, either in advance or on-line, by the ATU-R from a remote service controller. The menu is presented to the user as an HTML FORM page. The user selects an NSP, types the parameters needed for setting up a PPP connection to the selected NSP, like user name and password, and then presses the "submit" button. Consequently, an HTTP GET message with the parameters typed by the user is sent to the ATU-R. The ATU-R decodes the message, sets up a PPP connection to the selected NSP, and completes the HTTP session by sending the calling PC a status message.

The main advantages of the proxy-PPP solution are as follows:

- A standard networking stack at the PC: This is the most attractive advantage of the proxy-PPP solution. Users continue using their standard networking software. There is no need to install new software and the network operator does not have to configure and maintain user software. This is a unique property of proxy-PPP. All the other solutions, including PPPOE, L2TP and BMAP, require a change in the user networking stack. A bi-product advantage is that proxy-PPP supports any operating system with a standard Ethernet/IP/TCP networking stack. This includes Unix, Linux, and Macintosh. Other solutions require new software which is currently available only for MS Windows.

- Dynamic and flexible service selection model is supported: Since in other solutions the PPP starts at the PC, the user usually needs to configure an icon which will invoke the PPP connection to every possible NSP. This could be a bothersome process, especially if there are many potential NSPs. In the proxy-PPP solution with web-based service selection, users may use a standard HTML browser in order to get the service menu. Hence, with proxy-PPP solution the following holds:

  - No configuration is needed. All the NSPs are accessible by clicking on the service menu HTML page.
  - Users get an on-line information regarding the available NSPs at every time. If an NSP is not available or the service cannot be provided for any reason (e.g. lack of network resources), users will get an appropriate notification.
  - The network operator can attract new NSPs to the network, because new services can be pushed to the user through the service menu HTML page.
  - The network operator can make revenues from advertisements incorporated into the menu page.
  - Service selection based on QoS considerations can be supported. As an example, suppose that a user uses a CBR VC that consumes all of the ADSL bandwidth. Then, when another

user within the same SOHO asks for the service menu in order to connect to some NSP, or the same user wants to get simultaneous connectivity to another NSP as explained later, the menu provided by the service controller will not present any of the services that require a CBR PVC, but only those that can be provided over a UBR PVC. This mechanism does not require the user to be familiar with QoS considerations. Rather, at any time, the user simply views the dynamic menu in order to know which services are available and which services are denied.

- No need to standardize any new protocol: The proxy-PPP solution uses well known protocols and concepts, including HTTP and DHCP. There is no need to define any new protocol. A bi-product of this advantage is that proxy-PPP works with every service gateway. This is because the gateway is required to run "PPP over ATM", and is not required to perform any not-yet-standardized protocol.

- Supporting multiple simultaneous PPP sessions per user: Another unique property of proxy-PPP is that a PC may connect to several NSPs at the same time. For example, a user may connect simultaneously to the corporate network and to an ISP. The interesting part of this feature is that no support is required from the PCs operating system. This feature is based on the ability of the ATU-R to associate a received IP packet with an outgoing PPP connection based on the source IP address and destination IP address found in the packet. To allow this option, the service controller needs to know the list of network addresses of the servers reachable through every non-ISP NSP (for an ISP such a list is not available, because it provides access to *all* the Internet servers). When a user selects connectivity to such an NSP, the information is "downloaded" from the service controller to the ATU-R, e.g. through the menu page, and stored at the ATU-R‘s table of active connections. When a user‘s application sends a packet, the destination address field contains the IP address of the contacted server. When the ATU-R receives the packet, it looks in the table for an NSP with which the calling PC has an active connection, and whose list of network addresses includes the network address of the destination IP address. If such an NSP is found, the packet is forwarded over the appropriate PPP connection. If such an NSP is not found, and the user has an active connection to an ISP, the packet is forwarded to the ISP. Otherwise, the packet is silently dropped.

- Excellent support for SOHO networking: Using proxy-PPP, the same PC can be connected to a SOHO (small office home office) and to a selected NSP. Moreover, each PC may have connectivity to a different NSP. This feature is actually supported by most of the other solutions, except those that require the PC to have an ATM rather than an Ethernet NIC. However, a unique feature of proxy-PPP is that a group SOHO's PCs may share a single PPP connection. As an example, consider a small office with several PCs. As long as traffic is sent between internal hosts, the ATU-R is not involved. However, when some user needs to send a packet outside, the packet is received by the ATU-R. The ATU-R can be configured to open a PPP connection with an ISP, over which every packet to an external address will be forwarded. The network administrator can determine a time-out period of silence, after which the PPP connection is taken down. Moreover, the ATU-R can be configured with an alternate ISP, with which a PPP connection is established if the first ISP does not respond. In this configuration, the PPP connection from the ATU-R is not associated with a single PC. Rather, all PCs (or a set thereof, as can be defined by the SOHO administrator) can have their external traffic forwarded to the ISP through a single PPP connection. To support such a configuration, the ATU-R needs to implement Network Address Translation (NAT) [4] and Port Address Translation (PAT). NAT allows the hosts to have different local IP addresses, while sharing the same external IP address. PAT guarantees that each local host uses a different port number when multiple local hosts contact the same external server simultaneously. This allows the ATU-R to have a unique association between local hosts and received packets.

Proxy-PPP has two apparent drawbacks. The first is added complexity at the ATU-R due to the need to establish and maintain PPP connections for the end users, and due to the implementation of a lightweight web server that allows users to configure their PPP connections. However, it seems that even if this added complexity is translated into higher cost, this extra cost will be negligible compared with the labor cost associated with solutions that require the Telcos to configure and maintain a new networking stack at every PC. The second drawback is the CPU cycles required at the ATU-R for encapsulating IP packets in PPP frames. However, since this encapsulation requires no CRC computation, because CRC is added by the ATM hardware to AAL-5 frames, the extra CPU power required by proxy-PPP is usually not an issue.

5 Conclusions

The paper has addressed the issue of service provisioning in an ATM-over-ADSL access network. It has described the architecture of such a network and discussed the "PPP over Ethernet" issue.

It has presented several solutions for addressing this issue, namely PPPOE, L2TP, BMAP and proxy-PPP. The paper has shown that proxy-PPP has many advantages over the other approaches, the most important of which is that no modification is needed in the users' hosts, and that no new protocol has to be defined.

The paper has also shown that proxy-PPP solution works extremely well in conjunction with a web-based service selection scheme. In such a scheme, the ATU-R serves also as a lightweight web server. A user that needs connectivity to an NSP gets from the ATU-R an HTML service menu through an HTTP session. The selection of the user, along with the associated parameters, is then forwarded to the ATU-R using another exchange of HTTP messages. The ATU-R then has all the information needed in order to set up a PPP connection to the target NSP. Such a web-based service selection scheme may help to promote new services and to attract new NSPs to offer their services. Moreover, no configuration is needed at the user host, users can get an on-line information regarding the available NSPs at every time, and service selection based on QoS considerations can be supported.

References

[1] K. Asatani and Y. Maeda. Access network architectural issues for future telecommunication networks. *IEEE Communications Magazine*, 36(8), August 1998.

[2] A. Azcorra, D. Larrabeiti, E. Hernandez-Valencia, and J. Berrocal. IP/ATM integrated services over broadband access copper technologoes. *IEEE Communications Magazine*, 37(5), May 1999.

[3] R. Droms. Dynamic host configuration protocol. RFC-2131, March 1997.

[4] K. Egevang and P. Francis. The IP network address translator (NAT). RFC-1631, May 1994.

[5] A. Valencia et. al. Layer Two Tunneling Protocol (L2TP). Internet Draft, October 1998.

[6] C. Tai et. al. BMAP: Extending PPP/ATM services accross Ethernet/USB/IEEE 1394. ADSL Forum 98-018R2, September 1998.

[7] G. Gross, M. Kaycee, A. Lin, A. Malis, and J. Stephens. PPP Over AAL5. RFC-2364, July 1998.

[8] T. Kwok. Residential broadband architecture over ADSL and G.Lite (G.992.2): PPP Over ATM. *IEEE Communications Magazine*, 37(5), May 1999.

[9] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. de-Groot Groot, and E. Lear. Address allocation for private internets. RFC-1918, February 1996.