

European IPv6 Task Force Communication

IPv6 on DSL:

The Best Way to Develop Always-On Services

PATRICK COCQUET

6WIND Chairman, www.6wind.com

The deployment of IPv6 has become an issue of strategic importance for many economies, and telecom operators and NSPs play a key role in ensuring the availability of this new protocol on broadband access networks. It cannot be denied that the complexities exist in deploying IPv6 in an IPv4 world. Knowing this, telecom operators and network service providers (NSPs) have to ensure a viable transition strategy that takes into account transparent interoperability and mature integrated functionalities for deploying advanced applications on both IPv4 and IPv6. This potent combination will enable operators and NSPs to exploit the richer services offered by IPv6 while interoperating IPv4 during this long transition period, creating a new business model that will generate return on investment without waiting for the whole world to be fully IPv6 deployed.

Only the use of IPv6 at the end-user site can drive differentiated services, achieving returns in not only investments, but also in services innovation and flexible communication solutions. So both IPv4 and IPv6 protocols have now to be implemented on digital subscriber line access networks. Solutions are mature and are beginning to be deployed.

Keywords—Digital subscriber line (DSL), Internet services, IPv4 to IPv6 transition, IPv6.

I. INTRODUCTION

In coming years, an important factor in business productivity gains will involve the introduction of new applications based on greater mobility of terminals and users.

This growth involves the spread of technologies which at present are not very widespread. The availability of IP terminals using wireless technologies (particularly WLAN), the generalization of high-speed Internet, and the wide scale introduction of peer-to-peer (P2P) applications on IP (telephony, videoconferencing, and push services) are far from being a reality.

These new technologies are interdependent. How can performing applications be deployed without high-speed access or adapted wireless terminals? It is also essential to wonder about the capacity of IP networks to be able to directly connect correspondents for P2P applications, manage the mobility of terminals, and consider plug and play capabilities for terminals and network equipment.

Existing network address translation (NAT)-based IP architectures have too many limitations [1] to be used for wide-scale deployment of network architectures able to generate these new services. IPv6 [2] is the ideal technology for playing a catalyst role in deploying innovative services based on wireless technology and mobility within businesses. IPv6 actually offers solutions adapted for all encountered problems: almost unlimited addressing space, end-to-end secure access for P2P applications, automatic terminal and router configuration, and terminal mobility.

To be able to deploy these highly added-value services, it is first necessary to offer a high-speed IPv6

access to customers (public or private organizations as well as the home) parallel to existing IPv4 access. This involves taking into account intelligently the current service scenarios in order to ensure a harmonious coexistence of IPv4 and IPv6 [3]. Service providers and their customers will, thus, have mechanisms which facilitate a transparent migration for users from IPv4 to IPv6 applications and the capacity to deploy new applications, new terminals, and the associated online services.

This paper outlines the benefits that can be obtained by IPv6 in the local loop, especially in digital subscriber line (DSL) access systems. Section II describes IPv6 benefits. If IPv6 is an issue of strategic importance for countries such as China, where IPv4 address shortage may well halt or slow down the development progress in providing advance information and communication technology (ICT) access to its population, it has to be considered in Europe and the United States as a catalyst for end-user service development and machine-to-machine communications. Section III is dedicated to the use of IPv6 in DSL access networks. To capitalize the explosive development of DSL, telecom operators and NSPs have at their disposal available solutions on the market to associate broadband access with IP address availability. With IPv6, the customer network becomes a subnet instead of just a unique point of connection.

II. IPv6 BENEFITS

IPv6 constitutes the necessary IP evolution cornerstone for new application fields occurring with wireless networks, mobility, and accessibility of terminals. It is not a question of discarding an existing technology that works well, but simply providing IP—as has been already done in the past—some “fuel” for developing new services and applications. The main benefits connected to business services are described below.

A. Addressing Space

The addressing space extension from 32 to 128 b offered by IPv6 is clearly the basis for the evolution of IP networks. It offers up new possibilities for:

- access of countries suffering from a poor IPv4 address allocation to have sufficient addressing space [4];
- deployment of mobile Internet and its billions of terminals [5];

- management of permanent connections (asymmetric DSL (ADSL), cable, etc.) and IP mobility;
- development of new Internet devices for the consumer market [6];
- design of new IP-based systems such as telematics for vehicles, command and control industrial systems, and monitoring of agricultural production, among many others.

In other circumstances, the telephone could not have developed if not for extension of the addressing space. Currently, available services (personal voice mail, call forwarding, etc.) would not have been effectively developed if we had stayed with a single standard number to serve a whole company.

B. Access Simplification

IPv6 addressing space opens a new field that simplifies access for the final user. Consequently, it is no longer necessary to create complex solutions to get around NAT-type mechanisms that no longer have a place.

The scarcity of IPv4 addresses led to the deployment of mechanisms such as NAT, which cleverly hides a very large number of private addresses behind a very small number of public addresses, and which manages the gateway between public and private domains or even between two public domains.

But NAT is only well suited for a client-server type architecture—the server being in the public space and the client in the private space—since communication is solely client initiated. Using IP networks to offer standard end-to-end services such as the one needed for telephony, for remote control, for monitoring, etc., is quite a challenge when you do not use global IP addresses. The use of private addresses with NAT leads to complex and expensive solutions.

C. Simplification of Network Configuration

From its beginning, IPv6 was designed to enable “plug and play,” providing a simple, high-performance

solution for configuring terminals and basic mechanisms to manage IP connectivity. This type of mechanism is well adapted to nomadicy: moving a terminal from an IP sub-network to another IP sub-network without having to maintain running sessions. Mobile IP, on the other hand, as discussed in the following paragraph, addresses the problem of mobility more specifically, without interrupting running communication sessions. Different configuration protocols are shown in Fig. 1.

First of all, IPv6 integrates a stateless auto-configuration mechanism [7]. This means a server is not necessary to connect a terminal. When the terminal arrives in a new network, it simply constructs its address starting from a prefix sent by the local router. So it is no longer useful to install or maintain a dynamic host configuration protocol (DHCP) server.

Configuring the address may not be enough. Movement of the terminal requires updating the name-address correspondence in the domain name server (DNS) (DNS Update).

Anycast addressing—also available in basic IPv6 specifications—compared to traditional multicast techniques, constitutes a very effective way of locating a DNS server and, generally, all types of servers. Communication is indeed established with the first server that responds. Reserved anycast addresses (for example, addresses for DNS) are set.

Additionally, to offer a complete solution for configuring business networks, IPv6 integrates mechanisms used by service providers to configure prefixes in its clients’ routers (“prefix delegation”) [8].

For businesses, it is also possible to quickly redefine a complete addressing scheme (“router renumbering”), using a step-by-step construction of:

- prefixes to be used on the different interfaces of the router, starting from the access router prefix delegated by the operator, the service provider, or the service in charge of the business network administration;
- terminal addresses, thanks to the stateless auto-configuration mechanism using the local router prefix.

For example, this approach resolves the problem of merging private networks, poorly managed by IPv4.

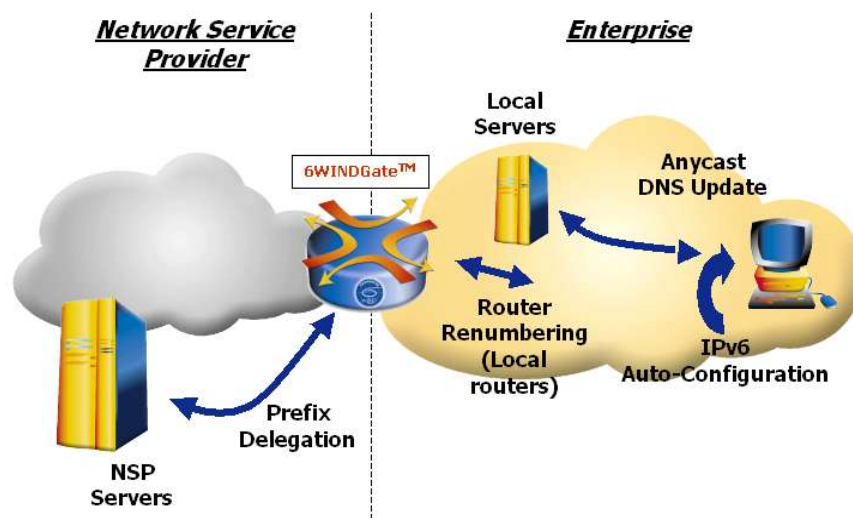


Fig. 1. Network configuration protocols.

D. Security of Exchanges

Improvements to IPv4 architecture security, both at the network layer (IPsec) and in application security (proxies or firewall-type solutions), can be implemented in the same way on IPv6.

IPv6 also brings an immediate solution to end-to-end security of transmission that is not always possible through NAT-based IPv4 architectures.

So IPv6 combines a complete set of mechanisms that maintain the current architectures while proposing end-to-end solutions particularly well suited for P2P applications.

E. A Mature Technology

The basic IPv6 specifications [2] date back to 1998 and were developed after long years of work, implementation, and testing. Today the large majority of router providers (core, aggregation, or access routers) and software publishers offer IPv6-ready solutions. Interoperability sessions that regularly take place demonstrate a high level of maturity of the protocol.

Like all the areas the Internet Engineering Task Force (IETF) handles, new proposals are regularly created to complete existing IPv6 specifications. These practices do not indicate that IPv6 is not fully mature; on the contrary, they prove that lots of activities are ongoing and that working groups have to take into consideration new requirements; it was this type of approach and repetitious work methods that allowed the IPv4 protocol to meet with the success that it did.

III. IPv6 AND DSL—A PERFECT MATCH

A. The Always-On Internet

To concur with the strong development of DSL, the IPv6 protocol is being deployed as part of commercial packages.

- DSL means always-on Internet access, which globally uses a lot more IP addresses than with a switched network access. On these networks, NSPs provide IP addresses on a ratio superior to 1 : 2 and increasing to 1 : 15 (1 address for 15 users). Deploying always-on Internet requires that this ratio be more than 15 : 1 (15 addresses per user).
- DSL is synonymous with broadband Internet access, which encourages the sharing of one access by several terminals, especially when one deploys WiFi behind a DSL modem. NAT devices are generally required, as NSPs do not have the capacity to provide several public IP addresses. This leads to many configuration problems, as some applications are not running well behind a NAT.
- The always-on Internet access provided by DSL creates the ideal environment for developing P2P applications, such as Internet telephony (ToIP) or multimedia file exchanges. IPv6 is a solution that is well suited to P2P applications, since it enables real end-to-end communications

to be made without any address translation devices [NAT or network address port translation (NAPT)] and with stable public addresses.

B. Reference Architecture for IP Services Over DSL

Fig. 2 represents a reference model for IP services over a DSL architecture.

This reference model involves three players.

- The service user (SU). The SU is the one using one or more IP services provided by one or several NSPs. It can be a residential, professional, or corporate user.
- The network access provider (NAP). The NAP provides users with DSL access over the local loop and connects these users with service providers through its transport network.
- The network service provider (NSP). The NSP provides the service to users. The NSP can be an NSP offering an Internet access service to residential and enterprise customers.

The NAP and the NSP can be part of the same organization—for instance, an incumbent carrier that owns the local loop and markets Internet access offers.

The NAP can also be a green-field operator accessing the local loop following an operation of unbundling, and reselling the use of this access network to NSPs.

The NAP can also be the owner/manager of a business center connecting the enterprises hosted in this business center and their respective Internet access providers.

The NSP can also be, for example, the national headquarters of a large corporation that provides its regional offices with access to its IT center.

1) **SU**: In the case of a residential user, Internet access today is the most widely used IPv4 service over DSL, and this mostly for a single terminal. In this case, only one IPv4 address is allocated to the user site, this address being dynamically allocated most of the time by the Internet access provider. The terminal is connected to the DSL network via a modem, mainly through a USB interface or Ethernet.

The difference between the IPv4 access service for a professional and for a resident is minimal. For the professional user, the IPv4 address allocated by the NSP is generally fixed. The provisioned bandwidth on the DSL line might be more important than in the case of a residential user. The modem is replaced by a DSL router (NAT) enabling to share the IPv4 access between several terminals.

In the case of a corporate user, a fixed IPv4 address range is generally allocated instead of a unique address. The maximum bandwidth of the DSL line is more important, and a minimum bandwidth might be guaranteed. Besides, additional v4 Internet access services can be proposed, such as a virtual private network (VPN) service allowing the interconnection of the different sites of the enterprise.

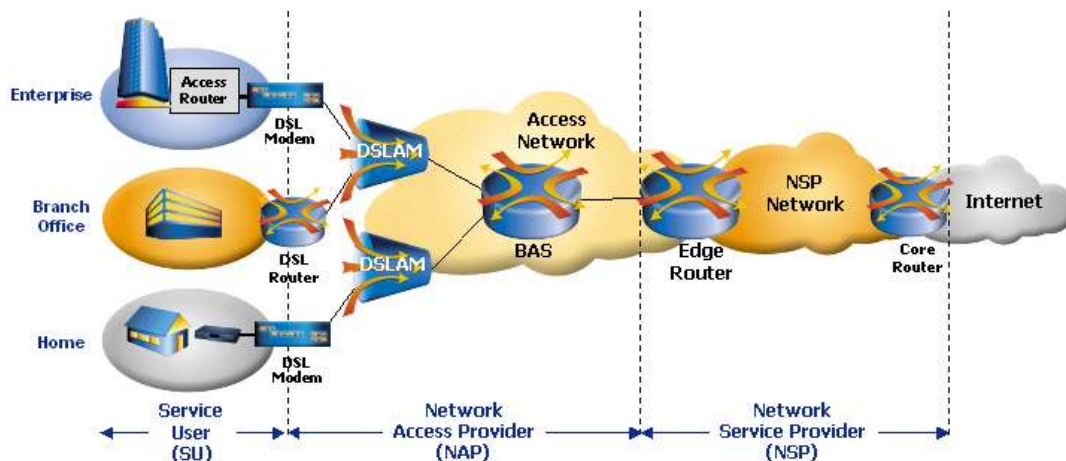


Fig. 2. Reference architecture for IP services over DSL.

2) **NAP**: The NAP has a direct access to users. It “resells” its users to NSPs in different ways. The most widely used are the following.

- Asynchronous transfer mode permanent virtual circuits (ATM PVCs): an ATM PVC is established between the DSL modem installed at the user’s premises and an access server located on the NSP’s site. The NAP commutes ATM PVCs to the NSP’s point of presence through its transport network. In this case, the NAP owns and operates the DSL access multiplexers (DSLAMs) and the ATM transport network up to the NSP’s points of presence. NSPs operate the broadband access servers (BAS).
- PPP over layer 2 tunneling protocol (L2TP) tunnels: a point-to-point protocol (PPP) session is established between the user’s DSL router/modem and an access server located on the NSP’s site. The NAP forwards the PPP sessions into the L2TP tunnels to the NSP’s point of presence through its transport network. In this case, the NAP owns and operates the DSLAMs and the BAS. NSPs operate the edge routers that are L2TP tunnel servers (LNS).

3) **NSP**: The interface between the NSP and the NAP depends on the service offered by the NSP to its users. The “PPP tunnels” interface described previously is perfectly suitable for the provision of basic Internet access services to residential or professionals. The “PVC ATM” interface is used when the NSP wishes to control the quality of the service offered, particularly in a business offer.

C. Deployment Solutions for IPv6 Services Over DSL

The deployment of new IPv6 services over DSL, either concurrently or in place of IPv4 services, relies on the implementation of IPv6 connectivity between the service provider and its customer and on the configuration of this customer’s equipment in order to operate this connectivity.

The deployment solution has to take into consideration the following points.

- The interface between the NSP and the NAP, which can be “level 2” based, for example, on ATM PVCs, or “level 3” based on L2TP tunnels in which PPP sessions are established.
- The management of subscribers, which can, for example, be centralized in a RADIUS server or distributed on several equipment. The allocation of public addresses, which can be more or less automated.
- The type of customer premises equipment (CPE) installed at the user’s location. It can be a DSL modem running like a simple bridge between the customer LAN and the DSL WAN: this solution address mainly the residential market. It can also be an IP router enabling the implementation of advanced functions (IPsec VPN, Firewall, IP quality of service (QoS), Mobile IP, etc.): this solution addresses today’s professionals and enterprises and is going to be more and more implemented in the residential market.

The following part of this paper presents in detail four examples of global solutions allowing IPv6 to be progressively deployed on a service architecture where IPv4 is already present.

1) **LAN/ATM Routed Access**: LAN/ATM routed access is illustrated in Fig. 3. This solution meets the needs of a NSP having a direct ATM access with its professional and corporate customers and wishing to set up a real IPv4 and IPv6 dual access, on which added-value services can be offered such as site-to-site VPN with QoS.

A DSL access router is installed on the customer site. This router may integrate an internal DSL modem or be connected by Ethernet to an external DSL modem. An ATM PVC is established between the DSL modem and the BAS installed at the NSP’s point of presence.

IPv4 and IPv6 packets are forwarded directly over this PVC, using the multi-protocol encapsulation over ATM adaptation layer 5 (AAL5) (RFC 1483/2684) mechanism. There is only one PVC for both protocols.

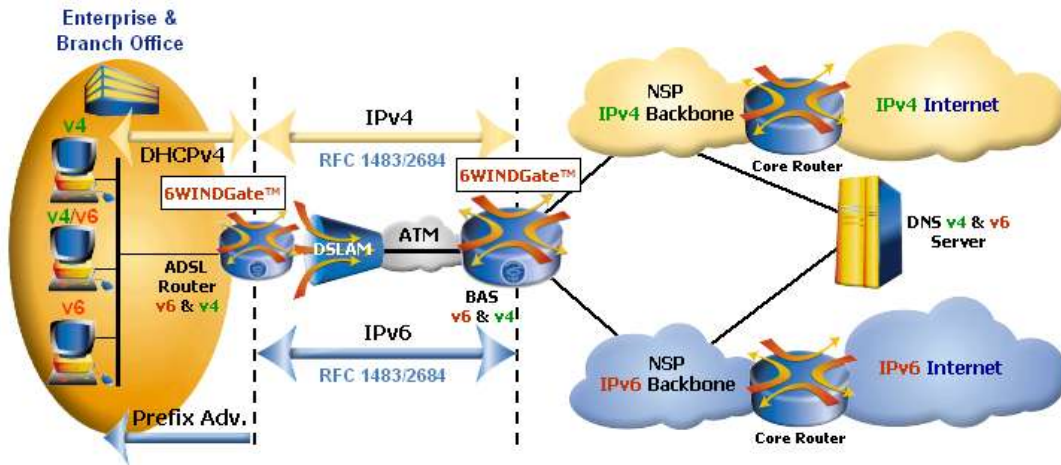


Fig. 3. LAN/ATM routed access.

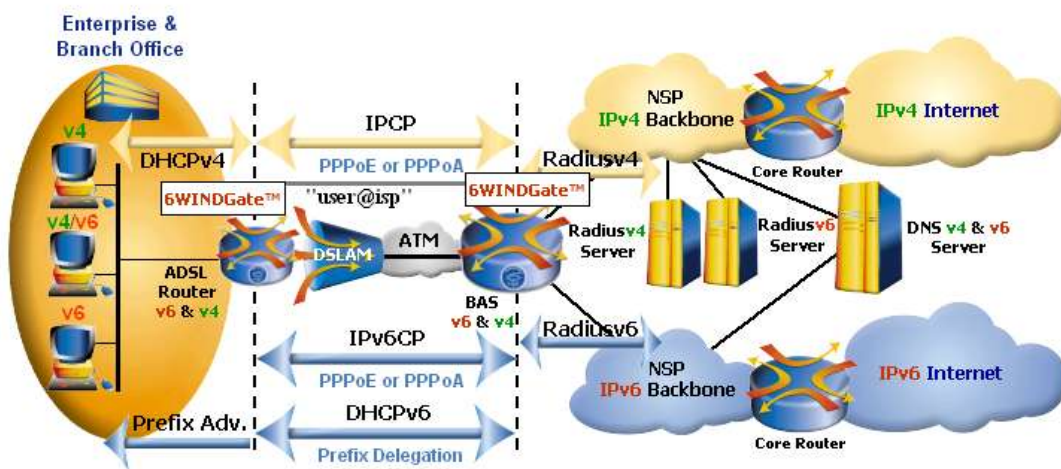


Fig. 4. PPP/ATM routed access.

The BAS is connected to the NSP backbone concurrently in IPv4 and IPv6. The NSP's servers and core routers giving access to the v4 and v6 Internet are also connected to this backbone.

In this solution, the DSL access router configuration is static, meaning the IPv4 public addresses and the IPv6 prefix are defined in the configuration file of the equipment and not at each connection. It has the advantage of simplicity and robustness: no central address allocation server, no PPP encapsulation. A prefix delegation mechanism based on DHCPv6 can be implemented in order to ease the network provisioning.

2) **PPP/ATM Routed Access:** PPP/ATM routed access is illustrated in Fig. 4. This solution is an alternative to the previous one. The set of equipment used, the CPE and the BAS, is the same as in the other solution. However, access between the customer and the NSP is established dynamically over PPP, and IPv4 and IPv6 connection attributes are stored in a centralized RADIUS database.

Only one PPP link [Link Control Protocol (LCP)] is established between the DSL access router and the BAS. A PPPv4 session [IP Control Protocol (IPCP)] and a PPPv6 session [IPv6 Control Protocol (IPv6CP)] are established

on this link. This allows a unique PPP identifier for both IPv4 and IPv6 protocols.

PPP over ATM (PPPoA) (RFC 2364) or PPP over Ethernet (PPPoE) (RFC 2516) is used between the broadband access server (BAS) and the customer site depending whether the access router is directly connected to the DSL line or via an Ethernet–DSL modem.

The BAS is connected to the NSP backbone concurrently in IPv4 and IPv6. The NSP's servers, and especially Remote Authentication Dial-In User Service (RADIUS) servers, are also connected to this backbone.

The BAS sends a request to the RADIUS server while providing the user ID ("user@isp"). There may be only one RADIUS server for both IPv4 and IPv6 or two different servers, one for IPv4 and another one for IPv6. In the first case, when the BAS receives a PPP session open request for a user, it retrieves the user's IPv4 and IPv6 connection attributes from the RADIUS server. Then the BAS is able to establish PPPv4 and PPPv6 sessions with the access router. In the second case, when there are two RADIUS servers, the BAS successively sends requests to the RADIUSv4 server, then to the RADIUSv6 server, and finally establishes PPPv4 and PPPv6 sessions with the access router.

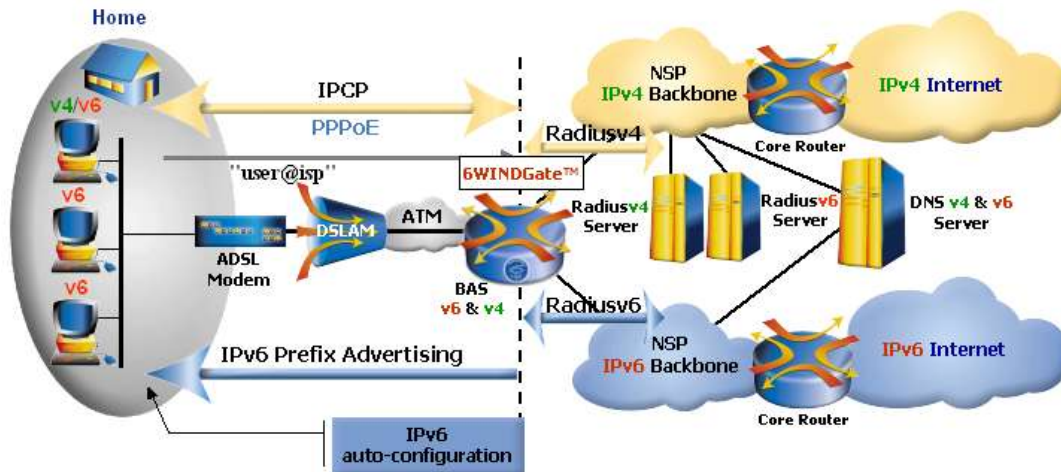


Fig. 5. LAN and PPP/ATM mixed bridge access.

On one hand, the BAS establishes the PPPv4 session and transmits IPv4 configuration information by IPCP to the access router, and on the other hand the PPPv6 session by IPv6CP. An IPv6 local link then exists between the BAS and the access router, and IPv6 configuration parameters are transmitted by DHCPv6. The BAS acts as DHCPv6 server while the access router acts as DHCPv6 client.

The prefix delegation mechanism, based on DHCPv6, is used to allocate an IPv6 network prefix to the access router. This prefix is then advertised on the customer site, thus making it possible for IPv6 terminals to auto-configure.

The main advantage of this solution is to have a homogeneous and centralized subscriber management for IPv4 as well as for IPv6. Moreover, auto-configuration mechanisms for IPv4 by IPCP and IPv6 by prefix delegation make this solution highly suitable for a large scale deployment.

The solution where two RADIUS servers are used, one for IPv4 attributes, the other one for IPv6 attributes, presents the advantage of simplifying the introduction of new IPv6 services, since it is not necessary to modify the existing RADIUSv4 configuration to add IPv6 access to an IPv4 user.

3) LAN and PPP/ATM Mixed Bridge Access: LAN and PPP/ATM mixed bridge access is illustrated in Fig. 5. This solution is adapted for residential users. It meets the needs of a service provider that already offers v4 Internet access over PPPoE to his customers and wishes to supplement its offer with true IPv6 access.

Terminals on the customer site are interconnected by a LAN (Ethernet, 802.11, Bluetooth). This LAN is connected to the DSL network via a bridge modem. This modem is completely transparent to the IP protocol, whether it is IPv4 or IPv6.

IPv4 access works classically by setting up a PPPv4 session on the ATM PVC established between the modem and the BAS.

- The IPv4 terminal sends its identifier ("user@isp") on the PPPoE link to the BAS.
- The BAS uses this identifier to authenticate the user to a RADIUSv4 server.

- After the user authentication, the RADIUSv4 server returns to the BAS the PPPv4 connection parameters and the IPv4 terminal configuration (IPv4 public address, DNS server address).
- The BAS transmits these configuration parameters to the IPv4 terminal.
- The IPv4 terminal auto-configures with the received parameters.

IPv6 access is established simultaneously in the following way.

- The BAS uses the user identifier a second time to question a second RADIUS server containing this user's IPv6 configuration parameters, primarily the network prefix of the user site (a/64, for example).
- The RADIUSv6 server returns to the BAS the IPv6 network prefix assigned to this user.
- The BAS advertises this prefix toward the customer site.
- IPv6 terminals on the customer site use this prefix to auto-configure.

In this architecture, there is only one ATM PVC per customer. IPv4 over PPPoE over ATM and IPv6 over Ethernet over ATM flow simultaneously on this PVC, using the multi-protocol encapsulation over AAL5 (RFC 1483/2684) mechanism in bridged mode.

This solution presents the following major benefits.

- This is a very easy solution to deploy on an existing IPv4 network, since it does not require any truck roll to configure a CPE. It enables the introduction of new services over IPv6 by using the DSL modem already installed at the customer premises.
- Thanks to the wide IPv6 addressing space, it allows a customer to use several terminals with public addresses behind a simple modem, whereas in an IPv4-only architecture, it would have been necessary to install a router on the customer site to be able to support several terminals.

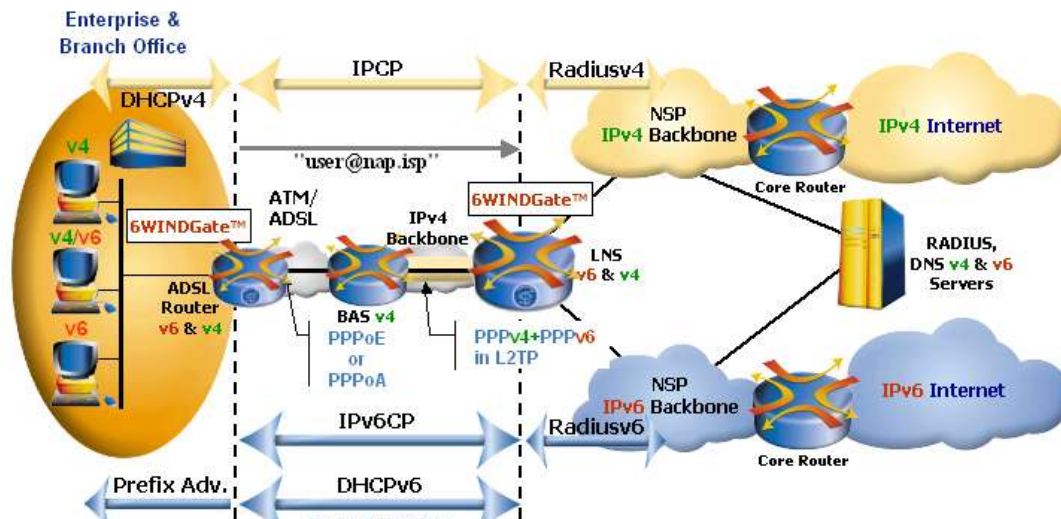


Fig. 6. PPP/L2TP routed access.

- All the IPv6-only terminals, having a global address, are visible by the NSP (they are not hidden behind an NAT) and can, thus, be used as a support to set up new services.

This solution gradually allows the NSP to switch off IPv4 access, as soon as migration solutions are implemented, allowing an IPv6-only terminal to access v4 Internet resources.

4) **PPP/L2TP Routed Access:** PPP/L2TP routed access is illustrated in Fig. 6. This solution is designed for a NSP using PPP sessions collected over L2TP by one or more NAP. It is particularly suited for a NSP offering added-value services to professionals and enterprises on a dual IPv4 and IPv6 access.

In this solution, a double PPPv4 and PPPv6 session is established between the customer access router and the service provider L2TP Network Server (LNS). This double PPP session consists of two sections.

- A first section between the access router and the BAS established over Ethernet (PPPoE) or ATM (PPPoA) according to the router DSL line interface (internal or external DSL modem connected by Ethernet).
- A second section between the BAS and the LNS established over L2TP. The BAS acts as L2TP access concentrator (LAC) making it possible to forward toward the LNS PPP sessions initialized on customer terminals.

The customer site's authentication and configuration parameters are managed in the RADIUS server. DHCPv6 is used on the PPPv6 link between the LNS and the customer site's DSL router, the LNS being DHCPv6 server and the DSL router, DHCPv6 client.

It is important to note that in this architecture, the NAP backbone can remain in IPv4. That means that a NSP can already start offering native IPv6 services, even if the interconnection with the NAP is based on L2TP over IPv4.

IV. CONCLUSION

We have seen that several architectures are available for deploying new IPv6 services over DSL. All of these architectures allow for the gradual introduction of new v6 services on an existing v4 network, thereby enabling a mix of IPv4 and IPv6 users on the same DSL area network and providing the same user with v4 and v6 access.

With the architectures described, there can be a smooth development toward IPv6-only services from using IPv4 and IPv6 protocols independently. In other words, IPv4 access connectivity can be phased out as protocol translation mechanisms, such as NAT-PT [9], are implemented in the service provider's backbone, enabling v6-only terminals to communicate with the v4-only resources on the Internet.

In each of the scenarios studied, several options are available according to the existing setup, in terms of both the hardware already installed and the procedures governing the way in which the network is operated and the subscribers managed. For example, it has been seen that IPv6 can be deployed at the access in addition to IPv4 in bridged mode without touching the modems installed at the user sites. It has also been shown that IPv6 can be maintained for the RADIUS and PPP-based user management systems used for IPv4.

The wide range of features and high levels of flexibility of commercially available solutions favor the implementation of these new architectures. They enable service providers to control the rate at which IPv6 is introduced over DSL and focus on the immediate added-value services for both companies and residential users, whilst keeping the risks and costs of the existing architectures to a strict minimum.

REFERENCES

- [1] M. Holdrege and P. Srisuresh. RFC 3027: Protocol complications with the IP network address translator. [Online]. Available: <http://www.ietf.org/rfc.html>
- [2] S. Deering and R. Hinden. RFC 2460: IPv6 specification. [Online]. Available: <http://www.ietf.org/rfc.html>
- [3] E. Carmès. ISOC member briefing 6: The transition to IPv6. [Online]. Available: <http://www.isoc.org/briefings>
- [4] P. Grossetête, J. Bound, and T. Hain. e-Nations, the Internet for all: An IPv6 business case. [Online]. Available: http://www.nav6tf.org/RIR_eNations/e-Nations-paper.pdf
- [5] A. Yegin and C. Williams. ISOC member briefing 14: IPv6: Necessary for mobile and wireless internet. [Online]. Available: <http://www.isoc.org/briefings>
- [6] A. Williams, B. Haberman, and R. Kermode. ISOC member briefing 7: IPv6 in the home makes sense. [Online]. Available: <http://www.isoc.org/briefings>
- [7] S. Thomson and T. Narten. RFC 2462: IPv6 stateless address autoconfiguration. [Online]. Available: <http://www.ietf.org/rfc.html>
- [8] R. Droms, Ed., RFC 3315: Dynamic host configuration protocol for IPv6 (DHCPv6). [Online]. Available: <http://www.ietf.org/rfc.html>
- [9] G. Tsirtsis and P. Srisuresh. RFC 2766: Network address translation–protocol translation (NAT-PT). [Online]. Available: <http://www.ietf.org/rfc.html>

Patrick Cocquet received the M.S. degree from Ecole Centrale (French Electrical Engineering University), Lille, France, in 1979.

He was Head of the Networks R&D at Thales, leading all strategic research and development projects on IP networking architectures and technologies.

He is currently Co-founder and Chairman of 6WIND, Montigny-le-Bretonneux, France. He has largely been instrumental in shaping the company's vision and direction in advanced IP technology, particularly in the deployment of the new-generation Internet, IPv6. As a result, he has become an acknowledged Internet visionary, highly respected in the industry and the scientific community for his insightful ideas on the Internet and its evolution and impact on the economy as well as the society at large.

He drives multilevel lobbying activities in promoting the benefits of the new-generation Internet among governments, state agencies, industrial players, and international organizations and forums. He is also Vice-President of the IPv6 Forum he founded in 1999 with L. Ladid, President of the French IPv6 Task Force he founded in 2002, and Steering Committee Member of the European IPv6 Task Force. He was also appointed, in 2003, to be Vice-Chairman of the China IPv6 Council, which he co-founded with L. Dong, CEO of Beijing Internet Institute.

About 6WIND

6WIND is the de facto leader and innovator of advanced IP-agnostic networking software for OEM licensing to build new generation networking equipment. 6WIND's flagship technology, the 6WINDGate™, empowers network equipment providers to significantly cut development time and costs, simplify network integration and deliver a leading edge differentiation with advanced IPv4 and IPv6 features. The 6WINDGate solution has been used worldwide by major industrial corporations, ISPs and telecommunication operators, public services, state bodies and the academia in advanced dual protocol IP projects on mobility, WLAN, interoperability, secure broadband access and peer-to-peer applications.

A spin-off of Thales and a contributor to IETF (Internet Engineering Task Force) on IP standardization and protocol definition, 6WIND was the first European company certified IPv6-ready by the global IPv6 Forum and is a European Information Society Technology award winner (EIST 2004). The company is headquartered in France and is present in China and Korea. For more information on 6WIND, visit <http://www.6wind.com>