Network Working Group
Internet-Draft
Expires: July 30, 2006

L. Toutain
B. Stevant
GET/ENST Bretagne
F. Dupont
CELAR
D. Binet
FT R&D
January 26, 2006

The Point6Box Approach
draft-toutain-softwire-point6box-00.txt

Status of this Memo

Copyright Notice

Abstract

The Point6Box is an add-on equipment which brings IPv6 connectivity to home and SME in a non-intrusive way. It is a deployment tool which will be replaced by IPv6 native service in term.

1. Motivation

IPv6 is nowadays implemented in many components such as core network, operating systems and even in several applications, but end-to-end IPv6 connectivity is still missing, especially because very few Internet Access Providers (IAP) offer for IPv6 connectivity and prefixes allocation. The IETF and some companies have defined and/or developed transitions tools like: 6to4, Tunnel Broker or Teredo, but these tools concern either experimented users or do not offer all the IPv6 benefits (always-on, machine to machine communications,...) to build applications. Furthermore, some of these solutions may also lead to some security threat.

In this document we present the Point6Box and its counterpart the Point6 Provider Edge (PEv6), two equipments that bring IPv6 connectivity to home and SME (Small and Medium Enterprise). This experiment has been launched by the Point6 project in 2005 and fills some of the requirements of the "hub and spoke" problem described by the Softwires working group [ID.problemstatement]. This document gives a short overview of the motivation, architecture and protocols used to solve the problem.

The Point6Box is an add-on equipment that can be connected to any CPEv4 or router in order to bring IPv6 connectivity and functionalities in a non-intrusive way. It is important to note that our goal is to fill missing gaps and not to specialize an equipment for IPv6 connectivity. Progressively, when IAP routers and CPE (Customer Premise Equipment) will become IPv6 aware, these functionalities will be included into equipments.

Several usages and objectives have been identified in this project:

- allow IPv6 connectivity for devices connected in a SME and Home network, in a very easy way, nearly without configuration from the user,
- locate IPv6 functionalities on stand-alone and cheap equipment to avoid to rely on desktop computers. Since IPv6 implies to be always-on, the Point6Box has not to be switched off.
- allow the introduction of IPv6 demonstrators on existing IPv4 network infrastructure. For instance, this allows an R&D division to add features to existing products and to make demonstration to business units.
- anticipate new usages. The connectivity offered by the Point6Box is very close to native access. Currently, new applications such as machine to machine communication relying on auto-configuration features and service discovery can be tested.
- manage an IPv6 network to discover missing features and debugging existing software to improve quality and reduce exploitation costs. Experiences learned during the transition phase must be

directly reused when IPv6 will be run on native infrastructures.
- o use open source software for CPE and PE and extend functionalities when needed.
- o use only fully standardized protocols, such as L2TP [RFC2661], PPP, etc.
- o be able to run over any IPv4 infrastructures (any NAT solutions) to provide a a transition tool to IAPs compliant with future native access architecture.

2. Technical description

Technically, the Point6Box can be viewed as an IPv6 router with only one Ethernet port plugged into an IPv4 router. Through this port, the Point6Box will establish connectivity to an IPv6 Provider Edge. The tunnel is made over L2TP, which provides three main characteristics:

- o L2TP messages are carried over UDP to offer NAT-traversal capabilities,
- o PPP is used to carry IPv6 frames, so we can rely on built-in authentication and configuration mechanisms, and have very easy interaction with AAA servers.
- o LPC sub-protocol may be used to detect when a tunnel is down, for instance due to an IPv4 address renumbering

The Point6Box removes the L2TP encapsulation and forwards incoming IPv6 packets on the link. Generally SME or Home routers interfaces are bridged with an IEEE 802.11 network, so every equipment connected to that network will receive Router Advertisements. IPv6 traffic generated by these equipments will be routed through the Point6Box. IPv4 traffic will continue to be NATed by the IPv4 edge router.

The Point6 Provider Edge is connected to the IPv6 backbone. It includes the server part and can be connected to an AAA database to allow authorization and monitoring. The following picture describes the service architecture.

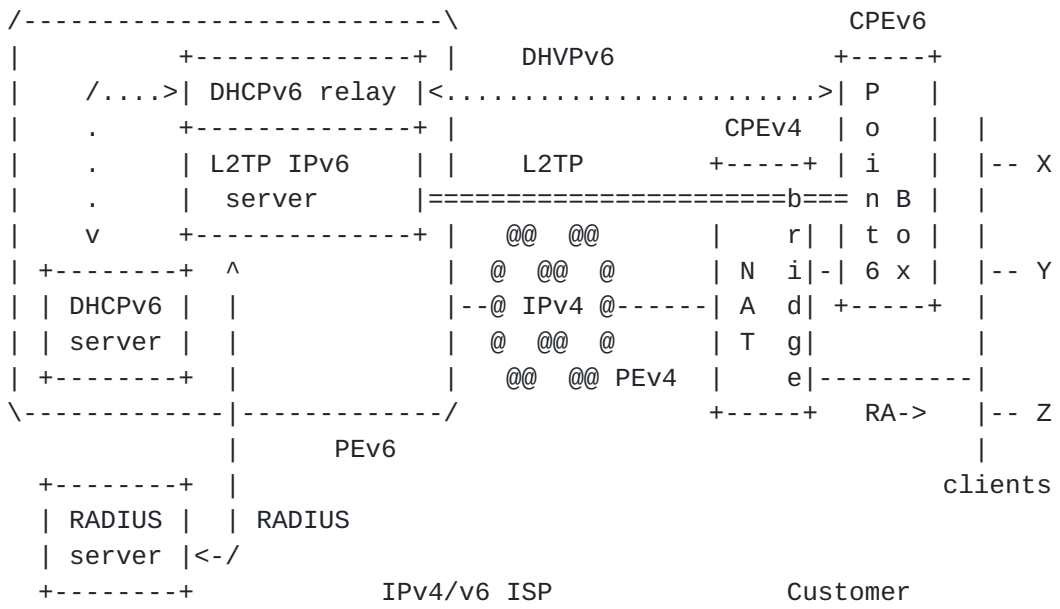

Figure 1: Service Architecture

During the initialization part, the Point6Box establishes a PPP peering with the PEv6 through the IPv4 Internet. Parameters required for the configuration of the Point6Box are the IPv4 address of this PE and a login/password. The PEv6 replies with a PPP/CHAP challenge and the Point6Box authenticates itself. The PEv6 queries an AAA server to validate the user authorization.

AAA and DNS servers will play an important role in network management. Since only the end system will create addresses, a provider must offer an IPv6 network with prefixes. The AAA server is used to centralize information concerning the user. When the AAA server authenticates the user, it returns a positive acknowledgment and the information concerning the account. We have currently identified three main parameters:

- Delegated prefix [ID.delegated]: It is allocated by the provider to the site network. The minimal length can be a commercial agreement between the user and the provider. It may vary between 48 and 64 bits regarding the SME/home network topology or the policy the user has with its provider. The prefix allocation is centralized on the AAA server. This allows the provider to get a centralized vision of the mapping between users and allocated prefixes, but the allocation made by the AAA server must have the following properties: stability over time and aggregation in the provider core network.
- DNS service: It is used in the traditional way to find the address from name and vice-versa.

- DNS domain: In this domain the user can register some equipments through DNS Dynamic Update. The default name could be something like user-login.provider.net.

Both ends of the IPv6 tunnel are configured with link-local addresses, and global addresses (for administration purposes). Then, the Point6Box sends a DHCPv6 [RFC3315] request to get the account parameters. The reply contains a prefix (64 bit long (aka. /64) or shorter) [RFC3633] and other parameters previously returned by the AAA server.

Auto-configuration of the SME/Home network is a major feature to rapidly spread IPv6. If the SME/Home network includes several routers configuration for IPv4 requires technical skills. We have study several approaches to offer internal routers configuration (see [AINA2005]). In this proposal, we focus on DHCPv6 because it does not require any modification, even if this approach is less efficient in case of multi-homing .

The Point6Box includes a DHCPv6 server to answer the requests inside the domain. The static parameters such as DNS resolver and the DNS domain are given to other routers and a pool of /64 prefixes is a constructed based on the prefix received from the provider. An internal router will execute the following algorithm, when one of its interface gets configured through the Neighbor Discovery (ND) [RFC2461] [RFC2462] protocol:

- The router sends DHCPv6 requests for a /64 prefix (the interaction with ND as explained in [AINA2005] is used to detect loops or dual prefixes allocation),
- The router waits for answers from the Point6Box containing the prefix and other parameters,
- The router assigns prefixes to interfaces. It starts unicast and multicast routing and a DHCPv6 relay. The relay functionality is used to allow downstream routers to talk with the DHCPv6 server.

At this point, the internal routers are configured, the equipment addresses can be setup through standard Neighbor Discovery protocol and other parameters through DHCPv6. Names and services discovery becomes an important feature in auto-configured networks since addresses cannot be a priori guessed. It is not clear if DNS is the appropriate answer, more experimentation have to be done. In a first approach, we propose to study the Dynamic Update, and offer this service in the provider network. Every host wanting to register to the DNS, has received through DHCPv6 the domain name and the resolver address and can run a script to register its addresses in the direct and reverse DNS. The provider may prevent misleading usage by filtering prefixes.

3. PEv6 Architecture overview

On the CPEv6 equipment, the interaction between different protocols is relatively simple and in sequence. The L2TP tunnel is open, then a response to the challenge is sent, followed by a ND router solicitation and a DHCPv6 request. The interactions between protocols are more complex on the PEv6 equipment.

The PEv6 waits for L2TP connection. The L2TP service is not protected by a shared secret, since this secret will have to be shared between all the customers and will not prevent from a DoS attack.

When a CPEv6 opens a tunnel, PPP is activated on that tunnel and a challenge is sent and a response is expected. The response contains the challenge, the answer to the challenge and the customer identity. The PEv6 forwards these values to an AAA (RADIUS [RFC2865] today) server. Currently on our experimentation, the response from the AAA server is just used to accept or not the connection. This should be enhanced in the future and the AAA will return more attributes like delegated prefix and other parameters.

Note that the value of the delegated prefix must be as stable as possible, but must depend on the PE location to allow aggregation in the IPv6 core network. So if a customer moves its Point6Box from one place to another, he may not receive the same delegated prefix.

The PEv6 receives user-specific IPv6 parameters from the AAA server during access authentication. It cannot send them directly using the PPP/IPv6CP protocol since only Link Local prefixes are negotiated. The PEv6 has to save information returned by the AAA server and to provide them later to the client during DHCPv6 negotiation

When the CPEv6 requests DHCPv6 parameters, a mapping must be established between the DUID used by DHCPv6 to identify CPE and information returned by AAA identified by user name. To allow this mapping, a DHCPv6 Relay function is added for each active L2TP tunnel. This relay adds RRAO (Relay agent RADIUS Attribute Option [ID.rrao]) information containing user name to the request anf forwards it to the DHCPv6 server.

Since the Point6Box service should maintain for a prefix a mid-term stability, prefix assignments to users are saved in a lease database. The DHCPv6 server may also use attributes provided by RRAO to decide which prefix pool is to be used for this particular user based on information from AAA.

The PEv6 needs to know what prefixes are allocated, for instance for

route injection. Today the information is snooped by the DHCPv6 relay because the right mechanism [ID.notagent] was published after the code was developed.

4. Transition

As stated before, the goal of the Point6Box is not to install IPv6 services on a new equipment. The goal of the Point6Box is to disappear when full connectivity will be established. During that time, the Point6Box will have helped to debug existing implementations, to explore new ways of managing IPv6 networks and to develop missing applications. One possible transition scenario is the integration of Point6Box software into existing CPE, and continue to tunnel IPv6 until all the provider network has been updated to manage natively IPv6. At this time, complete transition will mean merging of IPv4 and IPv6 AAA databases.

5. Scenarios and future plans

Several scenarios have been identified for a current use of the Point6Box:

- offer an easy IPv6 connectivity. The non-intrusive introduction of IPv6 in existing network, will help to demonstrate the benefits of IPv6 (global addresses, auto-configuration, always on,...) without modifying existing architecture. In France, lots of providers are offering triple play services. IPv6 access is incompatible with this offer due to implementation limitation. Using an IPv6 CPE instead of the provider box currently implies loosing television or telephony offers. Point6Box approach allows users to continue to access to all their services and to get an IPv6 connectivity. In that way, the user and the provider may test new services.
- deploy the IPv6 in a private network. A company specialized in digital signages has to install display devices in hotels, shops and supermarkets. The use of IPv4 is complex since display equipments are behind a NAT. The media server, which contains the contents update, cannot contact directly the equipments. With IPv6 each equipment has a global and stable address. The media server can send in real time the contents updates. The Point6Box approach will simplify the deployment of such services:
  1. an authenticated tunnel will be set to the media server
  2. IPv6 auto-configuration routers and hosts properties will allow equipments to be simply plugged on the network without special configuration.

  This scenario does not require a full Internet connectivity, since it focuses on a closed group of users. Security features are not blocking, since the Point6Box can strongly authenticate itself to the PEv6.

- Experiment new usages: IPv6 network will not be managed in the same way as an IPv4 networks: providers will allocate prefixes instead of addresses, equipments like television set will have an IPv6 address, ... This will lead to other paradigms on networking. The Point6Box may help to find innovative usages, adapt or develop new protocols and services. We currently investigate in network auto-configuration, service discovery, securing auto-configuration and automatic filtering of IPv6 Point6Box is a good experimental platform to implement research results.

We are also working in mobility features especially in header compression to limit the impact of tunneling overhead on low bandwidth links as wireless networks. This could help to demonstrate new services even when the wireless infrastructure is IPv4 only.

6. Acknowledgments

The Point6Box development has been made on by a Point6 team (founded by the Brittany Region Council, GET/ENST Bretagne and IRISA/INRIA). This work will not have been possible without the support of Etienne Gallet de Santerre, Herve Le Goff, Yannick Skrzypacz. We would also like to thank the Point6Boxes used by some of the authors to edit this document with IPv6.

7. Security Considerations

The Point6Box approach uses only already existing protocols so should not introduce new security issues.

8. References

8.1 Normative References

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633,

December 2003.

8.2 Informative References

[AINA2005]
Chelius, G., Fleury, E., and L. Toutain, "No Administration Protocol (NAP) for IPv6 Router Auto-Configuration", AINA 2005 IEEE 19th International Conference on Advanced Information Networking and Applications, March 2005.

[ID.delegated]
"RADIUS Delegated-IPv6-Prefix Attribute".

[ID.notagent]
Droms, R., Volz, B., and O. Troan, "DHCP Relay Agent Assignment Notification Option", draft-ietf-dhc-dhcpv6-agentopt-delegate-00.txt (work in progress), July 2006.

[ID.problemstatement]
Li, X., Durand, A., Miyakawa, S., Palet, J., Parent, F., and D. Ward, "Softwire Problem Statement", draft-ietf-softwire-problem-statement-00.txt (work in progress), December 2005.

[ID.rrao] Wing Cheong Lau, "DHCPv6 Relay agent RADIUS Attribute Option", draft-ietf-dhc-v6-relay-radius-01.txt (work in progress), August 2005.

[RFC2461] "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2462] "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC4057] Bound, J., "IPv6 Enterprise Network Scenarios", RFC 4057, June 2005.

Authors' Addresses

Laurent Toutain
GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: Laurent.Toutain@enst-bretagne.fr

Bruno Stevant
GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: Bruno.Stevant@enst-bretagne.fr

Francis Dupont
CELAR

Email: Francis.Dupont@point6.net

David Binet
FT R&D

Email: David.Binet@francetelecom.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.