broadband forum

TECHNICAL REPORT

# TR-187
## IPv6 for PPP Broadband Access

**Issue: 1**
**Issue Date: May 2010**

**Notice**

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE TECHNICAL REPORT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

**Issue History**

| Issue Number | Issue Date | Issue Editor | Changes |
|---|---|---|---|
| 1 | May 2010 | David Miles, Alcatel-Lucent,<br>Roberta Maglione Telecom Italia,<br>Mark Townsley, Cisco Systems | Original |

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.


| | | |
|---|---|---|
| **Editors** | David Miles | Alcatel-Lucent |
| | Mark Townsley | Cisco Systems |
| | Roberta Maglione | Telecom Italia |
| **A&T WG Chairs** | David Allan | Ericsson |
| | David Thorne | BT |
| **Vice-Chair** | Sven Ooghe | Alcatel-Lucent |
| **Chief Editor** | Michael Hanrahan | Huawei Technologies |

**TABLE OF CONTENTS**



  

  

**List of Figures**



  

**Executive Summary**

TR-187 updates PPP-Based Broadband Forum Architectures with details necessary for the deployment of IPv6 Internet Access alongside IPv4 (a.k.a. “dual-stack” IP access). This augments TR-59, TR-101, and other documents that describe PPP-Based IPv4 access.

Using the IPv6 connectivity described in this document, Service Providers will be able to provide basic IPv6 services like tiered internet access, but unable to support more advanced IPv6 based services like IPTV. Future Broadband Forum documents will contain more information on rolling out more advanced IPv6 services.

  

# 1 Purpose and Scope

## 1.1 Purpose

With finite IPv4 address space, calculations as far back as the 1990's revealed consumption was far in excess of what could be afforded, and initiatives such as Classless Interdomain Routing (CIDR) and Network Address Translation (NAT) were started to prolong IPv4 until the next-generation IP protocol (IPv6) could be completed. The IPv6 specification is now complete and projections by scientists in the Internet community indicate that the free pool of Global IPv4 addresses is likely to be exhausted very soon (2011-2012).

While IPv6 was created to meet the requirements of the ever-growing demand for public IP addresses, during its development a number of changes were made, incorporating many lessons from IPv4 deployment. The end result is that IPv6 is not backwards compatible with IPv4. The protocols are instead intended to be operated alongside one another, until the time IPv4 access can begin to be phased out.

This Technical Report is intended for service providers who wish to adopt IPv6 by building on the capabilities of Point-to-Point Protocol (PPP) to support both IPv4 and IPv6 in order to provide basic IPv6 services like internet access.

## 1.2 Scope

TR-187 outlines how basic PPP based IPv6 access can be added to the existing Broadband Forum Architectures.

The following methods for providing IPv6 services to the consumer at the U and T reference are described in this document:

- PPP-based IPv6 Access terminated on the Broadband Network Gateway (BNG):
  - PPP sessions initiated by an IPv6-aware, routed RG;
  - PPP sessions initiated by an end host behind a bridged RG
  - PPP sessions initiated by an end host behind an IPv4-aware RG using PPPoE pass-through
- PPP-based IPv6 Access to LAC extended to LNS over L2TP, in order to be able to cover wholesale/retail scenario.

This document specifies the nodal requirements for RGs and BNGs; there are no new requirements for either Access or Aggregation Nodes.

The following topics are out of scope:

- IPv6 over Ethernet in the Access Node or Access/Aggregation Network
- Service Provider NAT
- IPv4-to-IPv6 inter-working functions (NAT-PT, mNAT-PT, NAT64, etc)
- IPv6 multicast

  

- Tunneling techniques (Softwires, 6rd, DS-lite, etc.)
- Coordination between IPv6 PPP access and Video multicast VLAN, as described in TR-101

  

# 2 References and Terminology

## 2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [1].

| | |
|---|---|
| **MUST** | This word, or the term "REQUIRED", means that the definition is an absolute requirement of the specification. |
| **MUST NOT** | This phrase means that the definition is an absolute prohibition of the specification. |
| **SHOULD** | This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course. |
| **SHOULD NOT** | This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label. |
| **MAY** | This word, or the adjective "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option. |

## 2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.
A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.


| | | | |
|---|---|---|---|
| [1] RFC 2119 | *Key words for use in RFCs to Indicate Requirement Levels* | IETF | 1997 |
| [2] TR-059 | *DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services* | Broadband Forum | 2003 |
| [3] TR-101 | *Migration to Ethernet-Based DSL Aggregation* | Broadband Forum | 2006 |


  

| | | | | |
|---|---|---|---|---|
| [4] | TR-124 Issue 2 | *Functional Requirements for Broadband Residential Gateway Devices* | Broadband Forum | May 2010 |
| [5] | TR-156 | *Using GPON Access in the context of TR-101* | Broadband Forum | 2008 |
| [6] | RFC 1332 | *The PPP Internet Protocol Control Protocol (IPCP)* | IETF | May 1992 |
| [7] | RFC 1334 | *PPP Authentication Protocols* | IETF | October 1992 |
| [8] | RFC 1661 | *The Point-to-Point Protocol (PPP)* | IETF | July 1994 |
| [9] | RFC 1877 | *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses* | IETF | December 1995 |
| [10] | RFC 1994 | *PPP Challenge Handshake Authentication Protocol (CHAP)* | IETF | August 1996 |
| [11] | RFC 2460 | *Internet Protocol, Version 6 (IPv6) Specification* | IETF | December 1998 |
| [12] | RFC 2516 | *A Method for Transmitting PPP Over Ethernet (PPPoE)* | IETF | February 1999 |
| [13] | RFC 3162 | *RADIUS and IPv6* | IETF | August 2001 |
| [14] | RFC 3193 | *Securing L2TP using IPSec* | IETF | November 2001 |
| [15] | RFC 3315 | *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* | IETF | July 2003 |
| [16] | RFC 3633 | *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6* | IETF | December 2003 |
| [17] | RFC 3736 | *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6* | IETF | April 2004 |
| [18] | RFC 4241 | *A Model of IPv6/IPv4 Dual Stack Internet Access Service* | IETF | December 2005 |
| [19] | RFC 4818 | *RADIUS Delegated-IPv6-Prefix Attribute* | IETF | April 2007 |
| [20] | RFC 4861 | *Neighbor Discovery for IP version 6 (IPv6)* | IETF | September 2007 |


  

| | | | |
|---|---|---|---|
| [21] RFC 4862 | *IPv6 Stateless Address Autoconfiguration* | IETF | September 2007 |
| [22] RFC 5072 | *IP Version 6 over PPP* | IETF | September 2007 |
| [23] draft-ietf-radext-ipv6-access-01 | *RADIUS attributes for IPv6 Access Networks* | IETF | Work in progress |
| [24] draft-ietf-v6ops-ipv6-cpe-router-05 | *Basic Requirements for IPv6 Customer Edge Routers* | IETF | Work in progress |

## 2.3 Definitions

The following terminology is used throughout this Technical Report.

**BNG** The Broadband Network Gateway is an IP Edge Router where bandwidth and QoS policies may be applied.. The BNG may encompass any or all of the functionality of a BRAS. BNG is defined more completely in Broadband Forum TR-101 [3].

**BRAS** The Broadband Remote Access Server is the aggregation point for the subscriber traffic. It provides aggregation capabilities (e.g. IP, PPP, ATM) between the Regional/Access Network and the NSP or ASP. AS well as aggregation, it is also the injection point for policy management and IP QoS in the Regional/Access Networks. BRAS is defined more completely in Broadband Forum TR-059 [2].

**RG** The Residential Gateway is a device at the customer premises that connects the customer's Local Area Network (LAN) to a broadband Wide Area Network (WAN). It may route or bridge between these two networks.

## 2.4 Abbreviations

This Technical Report uses the following abbreviations:

**AAA** Authentication, Authorization, and Accounting

**ASP** Application Service Provider

**BNG** Broadband Network Gateway

**BRAS** Broadband Remote Access Server

**CHAP** Challenge-handshake Authentication Protocol

**CIDR** Classless Interdomain Routing

**DHCP** Dynamic Host Configuration Protocol

**DHCPv6** Dynamic Host Configuration Protocol version 6

  

| | |
|---|---|
| **DNS** | Domain Name System |
| **DR** | Delegating Router |
| **EAP** | Extensible Authentication Protocol |
| **IANA** | Internet Assigned Numbers Authority |
| **IETF** | Internet Engineering Task Force |
| **IP** | Internet Protocol |
| **IPCP** | Internet Protocol Control Protocol (for IPv4) |
| **IPv4** | Internet Protocol – Version 4 |
| **IPv6** | Internet Protocol – Version 6 |
| **IPV6CP** | IPv6 Control Protocol (PPP) |
| **L2TP** | Layer 2 Tunneling Protocol |
| **LAC** | L2TP Access Concentrator |
| **LAN** | Local Area Network |
| **LNS** | L2TP Network Server |
| **NAT** | Network Address Translation |
| **NAT** | Network Address Translation |
| **ND** | Neighbor Discovery |
| **NSP** | Network Service Provider |
| **PAP** | PPP Authentication Protocol |
| **PD** | Prefix Delegation |
| **PPP** | Point-to-Point Protocol |
| **PPPoA** | PPP over ATM |
| **PPPoE** | PPP over Ethernet |
| **RADIUS** | Remote Authentication Dial In User Service |
| **RFC** | Request for Comment |
| **RG** | Residential Gateway |
| **RR** | Requesting Router |
| **SLAAC** | Stateless Address AutoConfiguration |
| **TR** | Technical Report |
| **ULA** | Unique Local Addresses |
| **WAN** | Wide Area Network |

  

# 3 Technical Report Impact

## 3.1 Energy Efficiency

In normal operation, incremental energy expenditure only occurs when the packets are forwarded through the access infrastructure. This is not expected to create any significant increase in energy expenditure compared to the equivalent IPv4 traffic transiting the existing access infrastructure. Also, while an IPv6 header is larger than an IPv4 header, IPv6 deployment allows for connectivity to more devices with less state in network equipment (for example, it eliminates the need for Network Address Translation) vs. IPv4. In this regard, IPv6 has the potential to increase overall energy efficiency.

## 3.2 IPv6

TR-187 leverages existing IETF RFCs for IPv6 capabilities. No extensions of IPv6 protocols are defined in this document. TR-187 also references draft-ietf-radext-ipv6-access-01 [23] and draft-ietf-v6ops-ipv6-cpe-router-05 [24] as work in progress. This work may lead to IANA action for attribute standardization.

This document updates PPP-Based IPv6 Internet access to the suite of services specified in TR-59 and TR-101.

## 3.3 Security

User authentication methods that rely on PPP and the associated layer-2 security models are unchanged between PPP for IPv4 and PPP for IPv6.

As IPv6 does not require Network Address Translation (NAT), LANs that have a NAT function today may wish to enable a firewall in the RG for IPv6.

  

# 4 Basic IPv6 concepts

## 4.1 IPv6 addressing principles

IPv6 introduces an IP address of 128-bits (compared to IPv4's 32-bits). A subnet prefix and an interface identifier make up an IPv6 address. For most unicast addresses the interface identifier is 64 bits.

There are three different types of unicast IPv6 addresses:

- Link-local addresses (FE80::/10)
- Global Unicast Addresses;
- Unique Local Addresses (ULAs) (FC00::/7)

Every IPv6 host that communicates over the Internet is configured with both a Link-local address that is used on a single link and at least one Global Unicast Address for accessing the IPv6 Internet. There are different techniques to provide an IPv6 Global Unicast Address to a host. The following sub-sections describe the possible approaches.

With IPv4 access services, a single unicast address is typically assigned to a Residential Gateway (RG), which then utilizes private addresses and NAT to provide Internet connectivity to host devices. In an IPv6 access service, the address assignment will be an allocation of a larger address block (prefix) and no NAT function is required at the RG. Further, rather than configuring IP-related parameters such as DNS within PPP IPCP (as is the case with IPv4), IPv6 does not have link-specific parameter configuration mechanism, but uses the same mechanism for PPP as for other link types.

Note that the Broadband Forum architecture does not use the DHCPv6 Temporary Address (IA_TA option).

### 4.1.1 Stateless Address Autoconfiguration (SLAAC)

The IPv6 Stateless Address Autoconfiguration mechanism defined in RFC 4862 [21] allows a host to generate its own addresses using a combination of locally available information on the host and information advertised by routers.

### 4.1.2 DHCPv6 for Global-Unicast Address assignment

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6), defined in RFC 3315 [15], can be used to provide a device with both an IPv6 Global Unicast Address (assigned by the DHCPv6 server, using the IA_NA option) and other configuration information, which are carried in specific options.

### 4.1.3 DHCPv6 Prefix Delegation

The Prefix Delegation options defined in RFC 3633 [16] provides a mechanism for automated delegation of IPv6 address blocks using DHCPv6. This mechanism is intended for delegating a long-lived prefix from a Delegating Router (DR) to a Requesting Router (RR), across an administrative boundary, where the Delegating Router does not require knowledge about the topology of the links in the network to which the prefixes will be assigned.

  

According to RFC 3633 [16] the router that acts as a DHCPv6 client and is requesting prefix(es) to be assigned is called the "Requesting Router" (RR), while the router that acts as a DHCP server, and is responding to the prefix request is called the "Delegating Router" (DR) In this case, the BNG/BRAS would be the DR and the RG would be the RR.

An RG that does not acquire an address through either SLAAC or DHCPv6 IA_NA option takes an address from the delegated prefix to use as a source address for its own IP applications.

### 4.1.4 Guidelines to Service Providers for IPv6 prefix delegation

TR-101 [3] and TR-59 [2] allow for the use of Network Address Translation (NAT) between the Home Network and Provider Network, i.e. the U interface. This technique is employed to conserve IPv4 address resources through the re-use of a common private address pool for each home.

IPv6 was designed to allow every IP-capable host in the home to obtain a globally unique address and to avoid the use of NAT between the Home Network and Provider Network. In order to achieve this, it is recommended that the broadband service provider delegate an IPv6 address block to the home. If hosts are connecting directly to the service provider, then it is recommended that the service provider support hosts acquiring an IPv6 address through SLAAC.

In order to allow routing in the home network, the Broadband Forum suggests a size for the delegated prefix of least a /60 for home network or SOHO environments with a recommended prefix length of /56. The delegated prefix may be extended to a /48 for larger organizations.

## 4.2 Assignment of Domain Name Servers (DNS)

The DNS protocol operation is independent of whether it is transported over IPv4 or IPv6. In a dual-stack deployment, this allows a host to communicate with the Internet over IPv6 (or IPv4, as available), while making DNS queries solely over IPv4. Thus, while support of DNS over IPv6 is necessary for IPv6-only deployments, it is not for dual-stack. This is an important detail as there are widely deployed operating systems which, while fully IPv6 capable, have no way to dynamically configure IPv6 DNS server addresses. These operating systems will work in a dual-stack environment, but not an IPv6-only environment.

  

# 5 Architectural models

PPP methods for IPv6 services to the consumer at the U and T reference points are described in this Section. Figure 1 shows the PPP tunnels carrying IPv6 to the home network entities across the U and T reference points from the BNG.

The IPv6 service provided through the tunnels is delivered across the A-10 reference point as native IPv6 either from the Application Service Provider (ASP) or Network Service Provider (NSP).

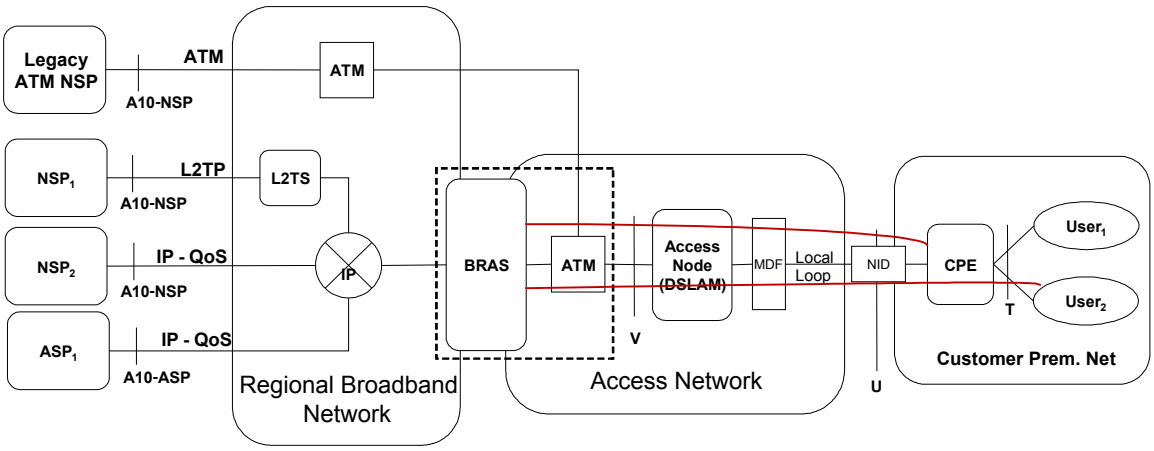


**Figure 1: IPv6 in PPP Tunnel**

Figure 1 shows an example of a PPP tunnel carried over ATM aggregation network, based on the TR-59 architecture, but the same concept also applies for Ethernet aggregation network, based on the TR-101 architecture.

## 5.1 The U reference point

The PPP-based U reference points (Figure 2) gain IPv6 capability through PPP

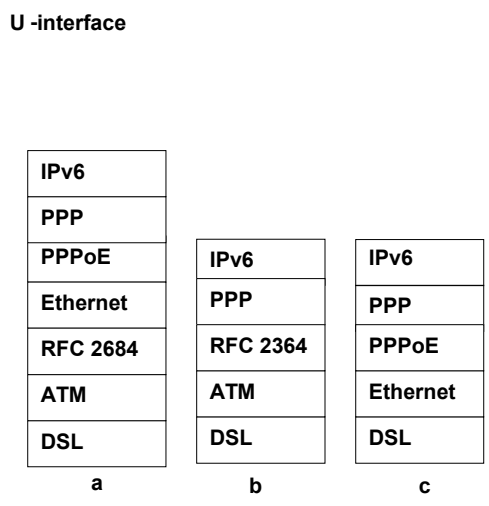


**Figure 2: Protocol Stacks at the U Reference Point**

  

### 5.1.1 Single PPP dual stack IPv4/IPv6 Session

In the case of a dual-stack session, the mechanism adopted to provide IPv4 and IPv6 connectivity to the customer is based on the architecture described in RFC 4241 [18]. It combines the use of the PPP protocol for the session establishment and the use of DHCPv6 and DHCPv6 Prefix Delegation for the configuration of the IPv6 prefixes, addresses and specific parameters. A single PPP session is used to carry both IPv4 and IPv6 traffic; the device that initiates the PPP session will get both an IPv4 address and at least one IPv6 prefix. The details related to the protocol stack and the message flows required to negotiate and configure IPv4 address and IPv6 prefix(es) will be described in the next sections.

### 5.1.2 IPv6 only PPP Session

An IPv6 only PPP session is an alternative to the PPP dual stack model; in this scenario a customer gets IPv6 only connectivity using the PPP Session.

This model can be used to allow hosts inside the LAN to establish their own IPv6 PPP sessions, while still receiving IPv4 connectivity from the Residential Gateway (RG). The RG in such a case would not need to be upgraded to support IPv6, although it would need to bridge PPPoE.

Another use for this model would be to allow existing BNGs to continue to support IPv4, while new BNGs are used for IPv6 PPP sessions.

## 5.2 Overview of the IPv6 over PPP model

The Point to Point Protocol (PPP) supports IPv6 per RFC 5072 [22]; PPP defines both encapsulation of the IPv6 datagram and a control protocol (IPV6CP) for establishing IPv6 modules at both ends of the PPP link. PPPoE is designed to establish a WAN connection to a remote client. PPPoE extends PPP to Ethernet, providing for authentication, authorization, accounting and network layer configuration (RFC 2516 [12]).

A PPP session is initiated and the PPPoE session discovery phase is performed using the traditional mechanism described in TR-59 and TR-101. The PPP session is established using the Link Control Protocol that is independent of the network layer protocol that needs to be carried over PPP. LCP allows for the transport of both IPv4 and IPv6 at the same time over the same (single) PPP session.

In contrast with IPCP which provides other configuration information, IPV6CP only negotiates an interface identifier. Other configuration information is provided via Neighbor Discovery and DHCPv6.

The 64-bit interface identifier is used to derive the Link-local address on the WAN interface. Given that the Link-local address is derived by the RG for its WAN interface, Duplicate Address Detection is not required for the link-local address or any address derived from the interface identifier on the PPP link.

  

During the PPP optional authentication phase using PAP, CHAP or the EAP protocol the subscriber is authenticated with his credentials by the AAA RADIUS. The Access-Accept message sent by the AAA Radius Server to the BNG may contain an indication related to the prefix that needs to be delegated to the PPP client, in addition to the usual IPv4 parameters (for dual-stack sessions). After successfully completing the authentication phase the network layer configuration phase needs to be performed, as two different Network level protocols (IPv4/IPv6) may be carried over a single PPP session. This means two separate protocols are used as the PPP Network Connection Protocol:

- For dual-stack sessions, IPCP is used as Network Connection Protocol for IPv4;
- IPV6CP is used as the Network Connection Protocol for IPv6, but only to negotiate the interface identifier option (type 1).

In the case of dual-stack sessions IPCP and IPV6CP can run in parallel over a single PPP connection. The differentiation between IPv4 and IPv6 traffic is done by the protocol field contained in the PPP header (0x0021 for IPv4 and 0x0057 for IPv6 [22]).

The main difference between IPCP and IPV6CP is that IPCP is able to complete the configuration procedure for the client and to allocate an IPv4 address to the client, while IPV6CP is only used to configure the link-local address. In order to configure an IPv6 Global Unicast Address an additional mechanism is required. This mechanism can be SLAAC or DHCPv6.

The PPP link can be unnumbered (i.e. only using link-local addresses) or the BNG can assign IPv6 addresses to the remote peer via SLAAC or DHCPv6. The BNG end of the PPP interface will typically only have a link-local IPv6 address.

In all cases, the BNG generates Router Advertisement messages toward the PPP peer. These messages are used by the PPP client to populate its Default Routers (RFC 4861) list and to optionally construct SLAAC addresses on the WAN interface. Whenever the Framed-IPv6-Prefix attribute is returned from RADIUS, the BNG includes this prefix as On-Link and Autonomous in the Router Advertisement Prefix Information Option. If this attribute is omitted, the BNG will not send a Prefix Information Option. DHCPv6 is used to delegate prefixes.

Note that PPP interfaces do not use Neighbor Discovery mechanisms for Link-layer address resolution. In PPP there is no concept of link-layer addresses, so all IPv6 on-link datagrams are sent to the PPP peer (the BRAS/BNG) for processing. Note that the Link-local scope is always on-link. Router Solicitations and Router Advertisements are still required on PPP links for the purpose of router discovery as are other functions of Neighbor Discovery.

The functions that are specifically needed on the BNG to support this architecture are listed in Section 9.2.

### 5.3 Considerations about the Addresses and Prefixes Provisioning Model

This section describes how the BNG obtains the IPv6 prefix(es) for numbering both the WAN interface link, if needed, and the subnets and devices located in the home network.

  

The BNG selects the IPv6 addresses and prefixes to be allocated and delegated to the Residential Gateway in the following ways:

- Selection based on an external authority such as a RADIUS server or DHCPv6 Server (in the latter case the BNG acts as a DHCPv6 Relay Agent);
- Dynamic assignment from a pool of available prefixes;
- Statically configured on the BNG

### 5.3.1 AAA RADIUS Integration

RFC 3162 [13], RFC 4818 [19] and draft-ietf-radext-ipv6-access-01 [23] describe different RADIUS attributes that can be used for the deployment of IPv6 in a Broadband access environment. The attributes can be configured on a RADIUS server and downloaded to access servers where they can be applied to access connections.

If a BNG needs to delegate both a prefix to a remote user's network and to select a prefix for numbering the WAN link interface, the prefix used for prefix delegation is placed in the *Delegated-IPv6-Prefix* attribute (RFC4818) and the prefix used for a SLAAC-derived WAN link is placed in the *Framed-IPv6-Prefix* attribute (RFC3162). Both attributes (the one for prefix delegation and the one for address assignment), if applicable, may be sent by a RADIUS Server to the BNG in the RADIUS Access-Accept, thus a single exchange between the BNG and the AAA subsystem is required.

When the WAN link of the RG has an IPv6 address assigned by DHCPv6 the full 128-bit address needs to be provided by the RADIUS server; draft-ietf-radext-ipv6-access-01 [24] specifies a new RADIUS attribute for IPv6-Address to be used for this purpose.

### 5.3.2 DHCPv6 Relay Agent in the BNG

The BNG can embed a DHCPv6 Relay Agent in order to assign addresses and prefixes allocated by an external DHCPv6 server. For the assignment of the delegated prefix (IA_PD option), the BNG acts as a Delegating Router for the RG and as a Requesting Router for the DHCPv6 server.

### 5.3.3 Dynamic assignment from a pool of available prefixes

By analogy with the IPv4 scenario, the IPv6 Prefix used for DHCPv6 Prefix Delegation to number the devices in the home network, can be extracted from a pool of prefixes statically configured on the BNG. The function of prefix pools in IPv6 is similar to that of address pools in IPv4; the main difference is that IPv6 assigns address blocks rather than a single address. As for IPv4, the name of the pool can be configured locally on the BNG or it can be retrieved from an AAA RADIUS server. In the case where the pool is retrieved from the RADIUS Server the *Framed-IPv6-Pool* attribute is used. This is a per-user attribute that contains the name of an assigned pool that should be used to assign an IPv6 prefix to the RG.

The functions that are specifically needed on the BNG to support all these models are listed in Section 9.1.

  

## 5.4 Customer Premises Connectivity Models

This Technical Report describes two basic models that allow users to connect IPv6 devices to the service provider network:

- IPv6 Routed Home Network – an IPv6 Residential Gateway (RG) provides routed IPv6 connectivity to the premises and establishes an IPv6 connection to the service provider network
- IPv6 Host Termination – each host device establishes its own IPv6 connection to the service provider

### 5.4.1 IPv6 Routed Home Network

In this case the RG is the IPv6 router on the home LAN segment. An IPv6 RG in the home network will provide native IPv6 connectivity to any IPv6-capable host. The IPv6 host devices in the home connect to the Service Provider network through this RG. The RG is responsible for establishing the PPP session with the BNG. In addition to providing IPv6 connectivity, the RG can be dual stack and will continue to provide IPv4 connectivity to the home. An example of this architecture is shown in Figure 3.

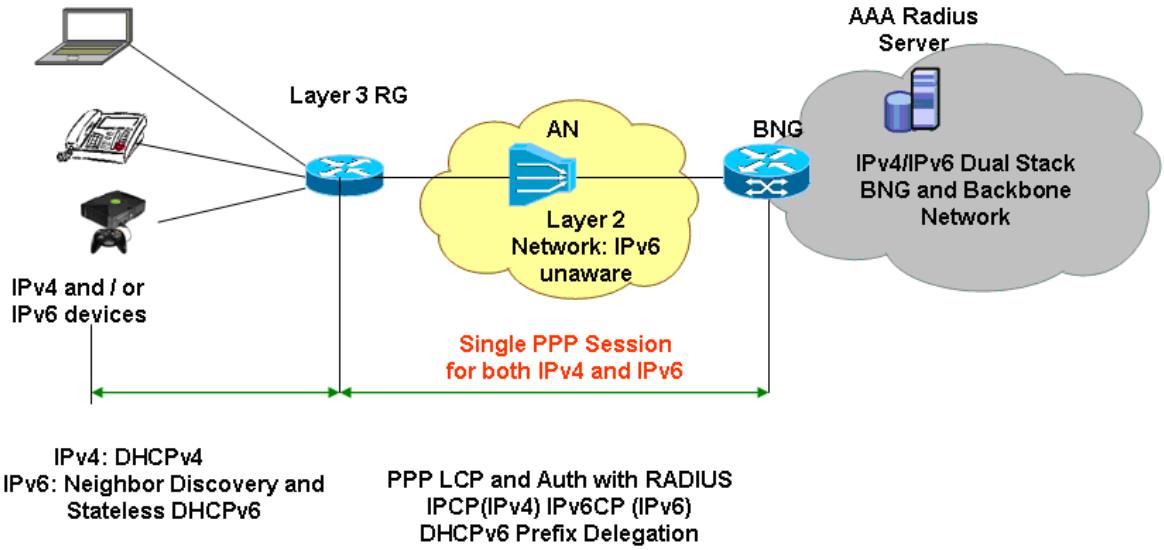


**Figure 3: Example IPv6 Connectivity with PPP Session Initiated by the RG**

#### 5.4.1.1 IPv6 Hosts

Host behavior is independent of access network architecture, and is not under the control of the access network provider. Hosts will, for the most part, conform to a variety of IETF RFCs that specify node behavior and host transition behavior (e.g., RFC 4294). These RFCs, in turn, reference IETF RFCs relating to address assignment, router discovery, domain name service (DNS), DHCPv6, etc. (e.g. RFC 3315, RFC 4862, RFC 3363).

Because the access network provider cannot control the behavior of hosts in a routed home network, no requirements for such hosts are included in this document. In general, it is expected

  

that hosts will support RFC 4862 (IPv6 Stateless Address Autoconfiguration), and may also support DHCPv6 RFC 3315 for IPv6 address configuration. To support SLAAC, the RG will advertise available IPv6 prefixes, including prefix(es) that the service provider network delegates to the RG.

#### 5.4.1.2 Residential Gateway (RG)

The RG will act as the IPv6 router that supports routed IPv6 connectivity inside the customer premises, and between the customer premises and the service provider network. Towards the LAN, the RG will need to act as an IPv6 router and support SLAAC and stateless DHCPv6 (RFC3736) (for example to provide the addresses of DNS servers). Towards the WAN, the RG will need to support IPv6 over PPP, SLAAC (as a host) and DHCPv6 (IA_NA, IA_PD and other information). The PPP session can have just IPv6, or both IPv4 and IPv6, and can be over either PPPoA or PPPoE. PPPoA can only be used if ATM encapsulation is used on the WAN interface. Regardless of whether the RG uses PPPoE or PPPoA for the link-layer, the PPP phases are identical.

In general, the RG is expected to support IPv6 LAN and WAN functionality as described in *TR-124 Issue 2* [4]. The functionality that is specifically needed to support this architecture is listed in Section 6.1.

### 5.4.2 IPv6 Host Termination

An alternative to operating an IPv6 home network is to allow IPv6 links over PPPoE to terminate directly onto end hosts. In this way, individual hosts can be IPv6-enabled without supporting native IPv6 traffic on the home network. PPPoE is used to encapsulate the IPv6 traffic. Examples of this architecture are shown in Figure 4 and
Figure 5.

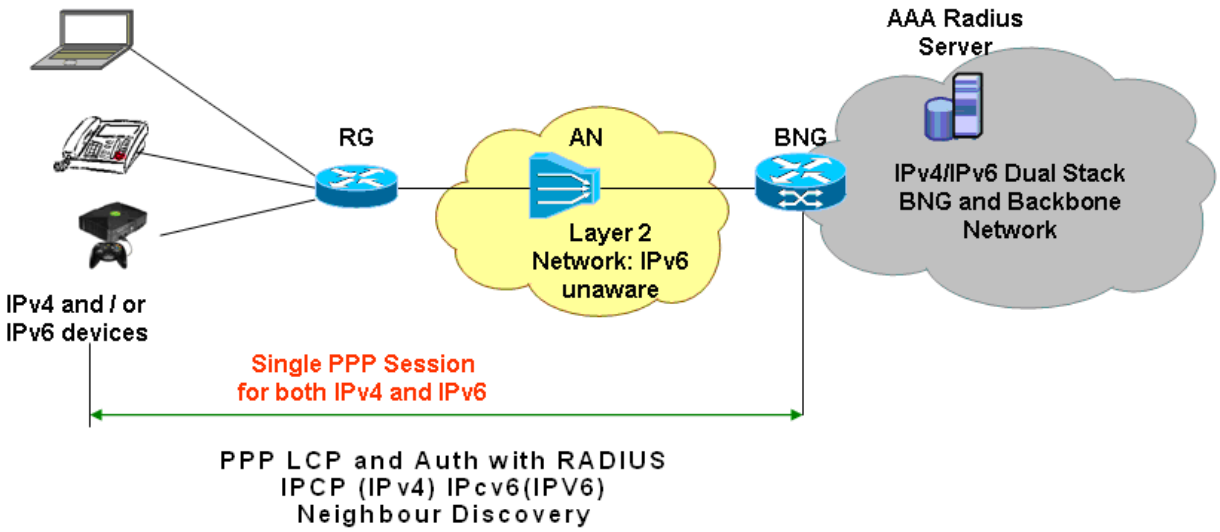


**Figure 4: Example IPv6 Connectivity with PPP Session Initiated by a Host behind the RG**

  

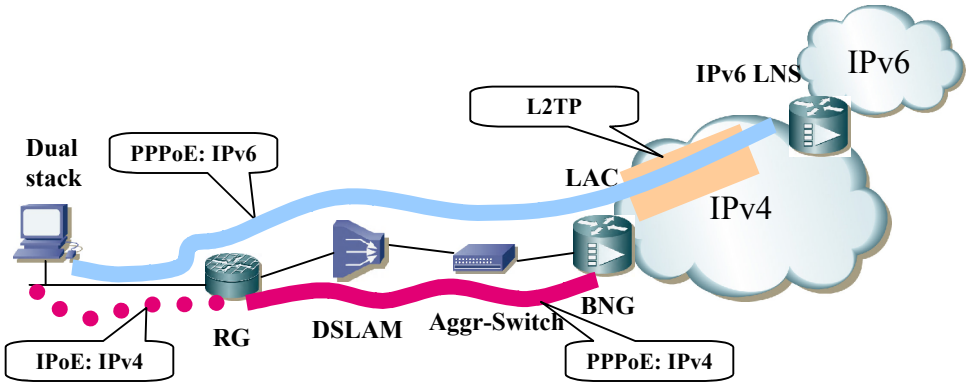


**Figure 5: Example IPv6 Connectivity with IPv4 from RG and PPP for IPv6 from Host**

Host-based access is limited in scale and does not support IPv6 connectivity inside the home network. IPv6 Host Termination is provided here as a transition mechanism in lieu of an IPv6-enabled home network with an RG.

As hosts would not typically implement a routing function, there is no prefix delegation occurring. Note that a host that is configured to act as a router (Internet Connection Sharing or similar) is considered to be a RG in the context of TR-187, and would behave as the RG described in Section 5.4.1.

#### 5.4.2.1 IPv6 Hosts

In general, hosts will operate in a dual-stack environment where they have both IPv4 and IPv6 connectivity and IP addresses. The methods described in this section allow for two distinct scenarios.

- The Host accesses IPv4 and IPv6 Internet resources over the PPPoE connection; LAN resources are directly accessible.
- The Host only accesses IPv6 Internet resources over the PPPoE; IPv4 Internet and LAN resources are directly accessible.

To support IPv6 Host Termination, each IPv6 host that needs IPv6 connectivity will need to support PPPoE. In addition, the PPPoE client will need to use a PPP client that supports IPv6 over PPP. The service provider will determine whether the PPP session can do both IPv4 and IPv6 or just IPv6. Where a service provider is already using PPPoE to connect host devices directly to the network for IPv4, adding IPv6 support to that existing session may be a desirable approach.

Some IPv6 hosts will support stateless DHCPv6 (RFC 3736 [17]) to acquire additional information. While the access network cannot assume such support, it will need to be able to at least provide IPv6 DNS server information by stateless DHCPv6. IPv6 hosts that do not support stateless DHCPv6 will use IPv4 DNS resolvers to request AAAA DNS records.

  

It should be noted that in the scenario where the host and RG use separate PPP sessions, the number of sessions in the network is increased. Thus this approach may have some impact on the scalability of the overall solution.

#### 5.4.2.2 Residential Gateway (RG)

To support IPv6 Host Termination, the RG needs to bridge PPPoE traffic to the WAN interface. This capability currently exists in most RGs and other home routers.

  

# 6 Residential Gateway and IPv6 Host Requirements

This section contains the RG requirements for both the IPv6 Routed Home Network and IPv6 Host Termination scenarios, as described in Section 5.4 It also describes which functions should be supported by IPv6 hosts for the IPv6 Host Termination scenario.

## 6.1 RG Requirements for IPv6 Routed Home Network

**R-1** The RG MUST support IPv6 over PPP (RFC 5072) on its WAN interface.

**R-2** The RG MUST use IPV6CP to negotiate the interface identifier of the RG WAN interface, by using the option Interface-Identifier (type 1). The RG MUST use this identifier to construct the IPv6 Link-local address of this interface.

**R-3** The RG MUST have a PPPoE client (RFC 2516) and/or PPPoA client (RFC 2684) that uses the IPv6-capable PPP client. The type of client that is appropriate for the RG may depend on the access technology.

**R-4** The RG MUST be capable of being configured to simultaneously carry IPv4 and IPv6 traffic over a single PPP connection.

**R-5** The RG MUST be capable of being configured to carry IPv6 over a dedicated PPP connection.

**R-6** The RG MUST support TR-124 [4] WAN.PPP module.

**R-7** The RG MUST support SLAAC (RFC 4862) for address assignment on a PPP session.

**R-8** The RG MUST NOT act as a router for Neighbor Discovery protocols (RFC 4861) on a PPP session.

**R-9** The RG MUST support DHCPv6 client (RFC 3315) for IA_NA (address assignment) on a PPP session.

**R-10** The RG MUST support DHCPv6-PD (RFC 3633) as a client (requesting router) on a PPP session.

**R-11** The RG MUST support the use of RFC 4638 to accommodate 1500 bytes MRU/MTU

**R-12** The RG MUST comply with IPv6 CE Router requirements in draft-ietf-v6ops-ipv6-cpe-router-05 [24].

## 6.2 RG Requirements for IPv6 Host Termination

**R-13** The RG MUST be capable of forwarding PPPoE from LAN devices to its WAN interface.

## 6.3 IPv6 Hosts Requirements for IPv6 Host Termination

**R-14** The IPv6 Host MUST support IPv6 over PPP (RFC 5072 [22]).

  

**R-15** The IPv6 Host MUST have a PPPoE client (RFC 2516) that uses the IPv6-capable PPP client.

**R-16** The IPv6 Host MUST be capable of being configured to simultaneously carry IPv4 and IPv6 traffic over a single PPP connection.

**R-17** The IPv6 Host MUST be capable of being configured to carry IPv6 over a dedicated PPP connection.

**R-18** The IPv6 Host MUST support PPP per IETF RFCs, RFC 1332, RFC 1334, RFC 1661, RFC 1877 and RFC 1994.

**R-19** The IPv6 Host MUST support SLAAC for address assignment on a PPP session.

**R-20** The IPv6 Host SHOULD support stateless DHCPv6 (RFC 3736).

  

# 7 Access Node Requirements

No changes to TR-59 and TR-101 Access Nodes need to be made to support IPv6 over PPP.

# 8 Aggregation Node Requirements

No changes to TR-59 and TR-101 Aggregation Nodes need to be made to support IPv6 over PPP.

# 9 Broadband Network Gateway Requirements

## 9.1 Address assignment and prefix delegation requirements

**R-21** The BNG, when acting as DHCPv6 Server, MUST be capable of using the DHCPv6 IA_NA option for the assignment of addresses to the host or WAN interface of a RG.

**R-22** The BNG, when acting as DHCPv6 Server, MUST be able to assign a single IPv6 /128 address to the WAN interface of the RG when using DHCPv6 for address assignment.

**R-23** The BNG MUST be able to support DHCPv6-Prefix Delegation, RFC 3633 [16], to delegate a prefix to the RG.

**R-24** The BNG MUST send periodic and solicited Router Advertisements (RFC 4861) to populate the default routers list of the host or the RG.

**R-25** The BNG MUST support the IPv6 RADIUS attributes defined in RFC 3162.

**R-26** The BNG MUST support the IPv6 RADIUS attributes defined in RFC 4818.

**R-27** Whenever the Framed-IPv6-Prefix attribute is returned from RADIUS, the BNG MUST include this prefix, with the Autonomous bit set (RFC 4861), in the Router Advertisement Prefix Information Option. If this attribute is omitted, the BNG MUST NOT send the Prefix Information Option.

**R-28** Whenever the Delegated-IPv6-Prefix attribute is returned in Access-Accept messages from RADIUS, if the BNG acts as Delegating Router, it MUST delegate (via the DHCPv6 IA_PD option) the prefix contained in that attribute.

**R-29** When SLAAC is used to number the WAN link, the prefix contained in the *Framed-IPv6-Prefix* attribute MUST be sent by the BNG to the RG in router advertisements (RAs.) These prefixes MUST be /64.

**R-30** Whenever the IPv6-Address RADIUS attribute specified in draft-ietf-radext-ipv6-access-01 [23] is returned in Access-Accept messages from RADIUS, if the DHCP IA_NA option is used to number the WAN link, the BNG MUST offer the IPv6 Address contained in that attribute by putting it in the DHCPv6 IA_NA Option.

**R-31** When the IPv6 pool method is used for DHCPv6 Prefix Delegation, the BNG MUST be able to retrieve the pool name from the *Framed-IPv6-Pool* attribute sent by the RADIUS in the Access-Accept and the BNG MUST be able to delegate a prefix extracted from the specified pool to the Requesting Router.

**R-32** If the RADIUS server includes a *Framed-Interface-Id* attribute (RFC 3162) in the RADIUS Access-Accept, the BNG MUST decline (with a ConfNak) the tentative Interface-Id received in the IPV6CP ConfReq message from the customer and suggest the value of *Framed-Interface-Id*.

**R-33** The BNG MUST be able to retrieve the content of the IPv6-DNS-Server-Address sent by RADIUS in the Access-Accept and insert it into the appropriate DHCPv6 option.

  

**R-34** The BNG MUST support IPv6 anti-spoofing on any delegated prefix contained in a DHCPv6 Prefix-Delegation message. Anti-spoofing MUST allow any IPv6 address within the prefix.

**R-35** The BNG MUST support IPv6 anti-spoofing on any host or WAN interface address assigned through the DHCPv6 IA_NA option. The anti-spoofing entry MUST match the exact 128-bit IPv6 address.

**R-36** The BNG MUST support IPv6 anti-spoofing for any prefix contained in a Router Advertisement Prefix Information Option.

**R-37** The BNG MUST support DHCPv6 stateless operation (RFC 3736 [17]) to provide DNS Recursive Name Server options to the host or RG, and MUST set the Other configuration flag bit to true (1) in all router advertisements.

**R-38** The BNG MUST NOT share a /64 prefix across multiple PPP sessions.

**R-39** When the DHCPv6 Relay Agent implemented in a BNG receives a downstream Relay-Reply message containing a Reply message including an IA_PD option, it MUST add a route (allocated IPv6 prefix contained in the IA_PD, next hop contained in the peer-address field) to the relevant BNG routing table.

**R-40** When the DHCPv6 Relay Agent implemented in a BNG receives an upstream Release message (or a Relay-Forward message containing a Release message) including a IA_PD option, it MUST delete the route corresponding to the delegated prefix(es) indicated in this option.

**R-41** When the DHCPv6 Relay Agent implemented in a BNG or the DHCPv6 server implemented in a BNG notices that the lease related to a delegated prefix has expired, it MUST remove the corresponding route from the BNG routing table.

**R-42** When the DHCPv6 server implemented in a BNG sends a downstream DHCPv6 Reply message including an IA_PD option, it MUST add a route (allocated IPv6 prefix contained in the IA_PD, next hop contained in the destination address of the DHCPv6 Reply) to the relevant BNG routing table.

**R-43** When the DHCPv6 server implemented in a BNG receives an upstream Release message (or a Relay-Forward message containing a Release message) including a IA_PD option, it MUST delete the route corresponding to the delegated prefix(es) indicated in this option

### 9.2 PPP related requirements

**R-44** The BNG MUST support IPV6CP negotiation of the interface identifier of the RG WAN interface, by using the option Interface-Identifier (type 1). The RG MUST use this identifier to construct the IPv6 Link-local address of this interface.

**R-45** If the BNG is to terminate IPv6 over PPP sessions directly, it MUST support IPV6CP and the transport of IPv6 over PPP.

**R-46** The BNG MUST generate Router Advertisement messages toward the PPP peer.

  

**R-47** When the PPP link-layer is up, the BNG MUST allow for the immediate sending of an IPV6CP ConfReq without waiting for the client.

**R-48** If the BNG does not receive the PPP interface identifier for a subscriber via RADIUS (attribute Framed-Interface-Id), it MUST assign a different Interface Identifier (via IPV6CP) to each RG.

**R-49** The BNG MUST be able to carry IPv4 and IPv6 PPP traffic within a single PPP session.

**R-50** The BNG MUST be able to carry IPv6 PPP traffic within a dedicated PPP session.

**R-51** The BNG MUST independently negotiate IPCP and IPv6CP for a common PPP session.

**R-52** When a PPP session is ended, the BNG MUST remove all the routes associated with that session from the routing table, for both addresses and delegated prefixes.

**R-53** If the BNG provides a PIO (SLAAC numbered model) in the Router Advertisements, this option MUST contain a unique global-scope IPv6 /64 prefix for each PPP session. The BNG MUST set the PIO A-Flag (autonomous) bit to true (1).

**R-54** The BNG MUST treat each PPP session as a separate IPv6 link, using the definition of link from RFC 2460.

**R-55** The BNG MUST be able to ignore IPCP in PPP sessions.

**R-56** The BNG MUST support the use of RFC 4638 to accommodate 1500 bytes MRU/MTU.

**R-57** The BNG MUST send Router Advertisement messages at regular intervals with a non-zero router lifetime.

**R-58** The BNG MUST support all ND functions.

### 9.3 LAC/LNS Requirements for Wholesale scenario

As an alternative to direct termination of the PPP session on the BNG, L2TPv2 can be used to tunnel the PPP session to a remote L2TP Network Server (LNS). In this scenario, the BNG acts as an L2TP Access Concentrator (LAC).

**R-59** The BNG MUST support L2TPv2 LAC functions for IPv6 packets.

If a single combined PPP session is used for IPv4 and IPv6, the entire session is tunneled over L2TP to the nominated LNS. However, if unique PPPoE sessions are used for IPv4 and IPv6 these can be processed independently and optionally terminated on different LNSs.

### 9.4 Additional BNG requirements

The BNG might support a mix of IPv4 and IPv6 traffic in any single queue thus allowing for any existing QoS policy to be maintained irrespective of whether the customer is generating or receiving IPv4 or IPv6 traffic. The BNG must also be able to support separate queues for IPv4 and IPv6 traffic, as they may be used to offer IPv4 and IPv6 services with different policies.

  

**R-60** The BNG MUST support forwarding IPv6 and IPv4 traffic in common traffic classes.

**R-61** The BNG MUST support forwarding IPv6 and IPv4 traffic in separate traffic classes.

**R-62** The BNG MUST support input and output octet counters that are the combination of IPv6 and IPv4 traffic (used with Input-Octets and Output-Octets RADIUS accounting).

**R-63** The BNG MUST support input and output packet counters that are the combination of IPv6 and IPv4 traffic (used with Input-Packets and Output-Packets RADIUS accounting).

**R-64** The BNG MUST support input and output octet counters that are separate for both IPv6 and IPv4 traffic.

**R-65** The BNG MUST support input and output packet counters that are separate for both IPv6 and IPv4 traffic.

**R-66** The BNG MUST support sending the counts defined in R-63 and R-64 to RADIUS, in Interim accounting and Stop accounting messages by using IPv6 specific RADIUS attributes.

For operating IPv6 sessions via PPP, prefix related information in RADIUS accounting is necessary. Therefore RADIUS accounting messages for IPv6 sessions have to include PIO related information. Two network scenarios are described below.

Scenario 1: a single Start Accounting message that contains both the IPv6 Delegated prefix and in the case where the numbered model is used either the SLAAC prefix or the IPv6 address assigned via DHCPv6;

**R-67** When IPv6 address and prefix assignment is complete the BNG MUST be able to send a single accounting-start message containing the IPv6 Delegated prefix (/56 IA_PD) and in the case where numbered model is used either the SLAAC prefix (/64 PIO) or the IPv6 address assigned via DHCPv6 (DHCPv6 IA_NA).

Scenario 2: a single Start Accounting message without any IPv6 prefix information (WAN link: /64 prefix (PIO) and delegated Prefix) is sent to the RADIUS Server followed by Interim Accounting messages

**R-68** When the first PPP NCP completes the BNG MUST send a RADIUS Accounting-Start message.

**R-69** When any subsequent NCP completes the BNG SHOULD send a RADIUS Interim-Accounting message.

**R-70** When IPCP completes, the RADIUS accounting message in R-68 or R-69 MUST include the IPv4 address assigned to the subscriber.

**R-71** When IPv6CP completes, the RADIUS accounting message in R-68 or R-69 MUST include IPv6 SLAAC Prefix (/64 PIO).

**R-72** When an IPv6 address is assigned via DHCPv6, the RADIUS interim accounting message MUST include the assigned IPv6 address.

**R-73** If the delegated prefix is provided via DHCPv6-PD to the client, the RADIUS interim accounting message MUST include the delegated prefix (IA_PD, e.g. /56).

  

End of Broadband Forum Technical Report TR-187