TECHNICAL REPORT

TR-242
IPv6 Transition Mechanisms for Broadband Networks

Issue: 1
Issue Date: August 2012

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	Approval Date	Publication Date	Issue Editors	Changes
1	21 August 2012	22 August 2012	Steven Wright, AT&T Dean Cheng, Huawei	Original
1	21 August 2012	10 September 2012	Steven Wright, AT&T Dean Cheng, Huawei	Editorial update to Figure 6 and Section 7, 7.1 titles

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

Editors	Steven Wright Dean Cheng	AT&T Huawei Technologies
End to End Architecture WG Chairs	David Allan David Thorne	Ericsson BT
Vice Chair	Sven Ooghe	Alcatel-Lucent
Chief Editor	Michael Hanrahan	Huawei Technologies

Table of Contents

List of Tables

List of Figures

Executive Summary

TR-242 describes several IPv6 transitional mechanisms that can be deployed in existing broadband networks based on the TR-101 architecture to deal with the IPv4 to IPv6 migration phase. Some of these mechanisms are in addition to the TR-101 based broadband network architecture and will require new functions and some new node types. TR-242 documents relevant requirements for each of the IPv4 to IPv6 transitional technologies.

Using the mechanisms described in TR-242, Service Providers will be able to provide (unicast) IPv6 connectivity and services to their existing customers, alongside (unicast) IPv4 services for legacy IPv4 hosts and applications behind the RG. Some of these mechanisms would also enable the sharing of Service Provider's existing IPv4 addresses between customers. Note that mechanisms as documented in this version of TR-242 only support unicast services for both IPv4 and IPv6 but multicast support is limited to IPv4.

1 Purpose and Scope

1.1 Purpose

The Broadband Forum has defined a target IPv4-IPv6 dual stack Architecture (assuming native implementation of IPv6 protocols) in TR-177 [6] and TR-187 [7]. TR-187 builds on the capabilities of existing protocols such as the Point-to-Point Protocol (PPP) and Layer 2 Tunneling Protocol (L2TPv2) to provide IPv6 service in addition to today's IPv4 service. TR-177 specifies how to enhance the TR-101 network architecture for supporting Ethernet (e.g. non-PPP) encapsulated IPv6 and IPv4 packet services.

To enable dual stack IPv6 service deployment while guaranteeing IPv4 service continuity for legacy IPv4 devices behind the RG, Service Providers may need additional transition mechanisms, beyond native IPv6 implementations, in order to optimize their infrastructure upgrades in the context of TR-101 [3] architecture. TR-242 identifies several transition mechanisms, explaining what transition issues are solved by each of them and the benefits each transition mechanism offers based on TR-101 architecture.

1.2 Scope

TR-177 and TR-187 describe mechanisms whereby operators can provide IPv6 service in addition to existing IPv4 service. However these involve upgrading existing network equipment which may include the Residential Gateway (RG), Broadband Network Gateway (BNG) and Access Node (AN).

In some cases, these network upgrades may also pose operational and deployment challenges to operators. Some operators may wish to maintain their existing access/aggregation infrastructure in order to reduce the network impact when introducing IPv6. Further, operators may need mechanisms to cope with the exhaustion of IPv4 addresses. Technologies to achieve these goals may be deployed simultaneously or in a phased approach.

The starting point for TR-242 is the TR-101 architecture. TR-242 introduces additional mechanisms, over and above those in TR-177 and TR-187, which enable operators to handle the operational and deployment challenges related to IPv4 address exhaustion, IPv6 introduction and IPv4/IPv6 co-existence.

TR-242 describes different techniques which enable different migration paths:

- Techniques that deal with IPv4 address exhaustion do not simply depend on the introduction of IPv6. These techniques involve some kind of IPv4 address sharing;
- Techniques that ease the introduction of IPv6 by not requiring dual stack End-to-End™;
- Techniques that maintain IPv4 service continuity for IPv4 only hosts and/or applications by not requiring dual stack End-to-End™.

The described mechanisms may either be deployed as upgrades of existing network elements (e.g. the RG or BNG) and/or embodied in additional network elements.

1.3 IPv6 Transition Planning

Planning for the transition to IPv6 services by a Service Provider includes consideration of both commercial and technical aspects. Commercial aspects include identification of specific business requirements in the current context of the Service Provider and then elucidating the associated commercial costs, benefits and risks. Such commercial considerations usually result in the development of a business case and are beyond the scope of this specification.

The ATIS IPv6 Readiness Plane [1] identifies technical readiness steps and characterizes levels of readiness. Technical readiness steps include developing an inventory of IP-aware network elements, and developing a design for IPv6 Transition. For this specification, the inventory of IP aware network elements starts with the TR-101 architecture, and considers Network Services (e.g. DNS, DHCP, AAA, NTP, etc.) and Network Management (TR-069, MIBS, Netflow, MRTG, etc.). Applications (e.g. VoIP, IPTV), Operations Support Systems and Business Support Systems are beyond the scope of this specification.

For TR-242, the design goal is the support of a dual stack environment in the Home Network for connectivity to the public IPv4 and IPv6 Services. A specific design would need to cover IPv6 addressing plans, IPv6 Routing and IPv6 peering as well as mechanisms for security, network management and network services. The IPv6 transport of IPv6 packets may be supported by various tunneling and translation mechanisms described in TR-242.

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 [15].

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 term "RECOMMENDED", means that there could 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 could 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 term "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.

Document	Title	Source	Year
[1] ATIS IPv6 Readiness Plan	*ATIS Readiness Plan for IPv6 Transition*	ATIS	2008
[2] TR-069 Amendment 4	*CPE WAN Management Protocol*	BBF	2011
[3] TR-101 Issue 2	*Migration to Ethernet-Based DSL Aggregation*	BBF	2006

[4]	TR-124 Issue 3	*Functional Requirements for Broadband Residential Gateways*	BBF	2012
[5]	WT-146 *(Work in Progress)*	*Subscriber Sessions*	BBF	2012
[6]	TR-177	*Migration to IPv6 in the Context of TR-101*	BBF	2010
[7]	TR-187	*IPv6 for PPP Broadband Access*	BBF	2010
[8]	TR-181 Issue 2 Amendment 5	*Device data Model for TR-069*	BBF	2012
[9]	RFC 792	*Internet Control Message Protocol*	IETF	1981
[10]	RFC 1191	*Path MTU Discovery*	IETF	1990
[11]	RFC 1661	*The Point-to-Point Protocol (PPP)*	IETF	1994
[12]	RFC 1332	*The PPP Internet Protocol Control Protocol*	IETF	1992
[13]	RFC 1559	*Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*	IETF	1993
[14]	RFC 1918	*Address Allocation for Private Internets*	IETF	1996
[15]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[16]	RFC 2473	*Generic Packet Tunneling in IPv6 Specification*	IETF	1998
[17]	RFC 2663	*IP Network Address Translator (NAT) Terminology and Considerations*	IETF	1999
[18]	RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*	IETF	2000
[19]	RFC 2983	*Differentiated Services and Tunnels*	IETF	2000
[20]	RFC 3022	*Traditional IP Network Address Translator*	IETF	2003
[21]	RFC 3633	*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*	IETF	2003
[22]	RFC 3768	*Virtual Routing Redundancy Protocol*	IETF	2004
[23]	RFC 4241	*A Model of IPv6/IPv4 Dual Stack Internet Access Service*	IETF	2005
[24]	RFC 4443	*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*	IETF	2006
[25]	RFC 4787	*Network Address Translation(NAT) Behavioral Requirements for Unicast UDP*	IETF	2007
[26]	RFC 4861	*Neighbor Discovery for IP version 6 (IPv6)*	IETF	2007
[27]	RFC 5382	*NAT Behavioral requirements for TCP*	IETF	2008
[28]	RFC 5508	*NAT Behavioral Requirements for ICMP*	IETF	2009

[29] RFC 5597	*NAT Behavioral Requirements for DCCP*	IETF	2009
[30] RFC 5625	*DNS Proxy Implementation Guidelines*	IETF	2009
[31] RFC 5905	*Network Time Protocol Version 4: Protocol and Algorithms Specification*	IETF	2010
[32] RFC 5969	*IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)*	IETF	2010
[33] RFC 6146	*Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*	IETF	2011
[34] RFC 6147	*DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*	IETF	2011
[35] RFC 6269	*Issues with IP address sharing*	IETF	2011
[36] RFC 6302	*Logging Recommendations for Internet-Facing Servers*	IETF	2011
[37] RFC 6333	*Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*	IETF	2011
[38] RFC 6334	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Options for Dual-Stack Lite*	IETF	2011
[39] RFC 6346	*The Address plus Port (A+P) Approach to the IPv4 Address Shortage*	IETF	2011
[40] RFC 6519	*RADIUS Extensions for Dual-Stack Lite*	IETF	2012
[41] draft-cheshire-nat-pmp-03.txt	*NAT Port Mapping Protocol (NAT-PMP)*	IETF	
[42] draft-ietf-behave lsn-requirements-06	*Common Requirements for IP address sharing*	IETF	
[43] draft-ietf-pcp-base-26	*Port Control Protocol (PCP)*	IETF	
[44] draft-ietf-softwire-6rd-radius-attrib-03	*RADIUS Attribute for 6rd*	IETF	
[45] draft-ietf-softwire-dslite-multicast-02	*Multicast Extensions to DS-Lite Technique in Broadband Deployments*	IETF	
[46] draft-shirasaki-nat444-05	*NAT444*	IETF	
[47] draft-shirasaki-nat444-isp-shared-addr-07	*NAT444 addressing models*	IETF	

2.3 Definitions

The following terminology is used throughout this Technical Report.

AFTR (Address Family Transition Router):	An AFTR element is the combination of an IPv4-in-IPv6 tunnel end-point and an IPv4-IPv4 NAT implemented on the same node. In the BBF architecture, the AFTR can be either embedded in the BNG or located in a separate node.
B4 (Basic Bridging Broadband element):	The B4 element is a function implemented on a dual stack capable node, either a directly connected device or a Residential Gateway that creates a tunnel to an AFTR. The BBF architecture only considers the case where the B4 element is located in the RG.
CPE	Customer Premises Equipment.
Dual Stack	A network element that supports both IPv4 and IPv6 natively.
IPv4 Address	A 32-bit integer value IP address formed according to RFC 791 for public IPv4 addresses, or RFC 1918 for private IPv4 addresses. IPv4 addresses include both Unicast and Multicast address formats. An IPv4 address is normally represented as 4 octets of decimal digits separated by periods.
IPv6 Address	A 128-bit integer value IP address formed according to RFC 4291. IPv6 addresses include Unicast (including Anycast) and Multicast address formats. An IPv6 Address is normally represented as eight groups of four hexadecimal digits separated by colons.
Public IPv4 Address	An IPv4 address that is globally unambiguous per RFC 1918
Private IPv4 Address	An IPv4 address that is unambiguous within an enterprise (or administrative domain) but may be ambiguous between enterprises (i.e. globally ambiguous) per RFC 1918.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

AAA	Authentication, Authorization, Accounting
AFTR	Address Family Translation Router
AN	Access Node
B4	the Basic Bridging BroadBand element
BBF	The Broadband Forum
BNG	Broadband Network Gateway

BR	Border Router
CE	Customer Edge
CG-NAT	Carrier Grade-NAT
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IGD	Internet Gateway Device
IPCP	Internet Protocol Control Protocol
IPTV	Internet Protocol TeleVision
LAN	Local Area Network
MIB	Management Information Base
MSS	Maximum Segment Size
MRTG	Multi Router Traffic Grapher
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
NAS	Network Access Server
NAT	Network Address Translation
NAT-PMP	NAT Port Mapping Protocol
NTP	Network Time Protocol
PCP	Port Control Protocol
P2P	Peer-to-Peer
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RG	Residential Gateway
TCP	Transmission Control Protocol
TR	Technical Report
UDP	User Datagram Protocol
UPnP	Universal Plug ‘n’ Play
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network
WG	Working Group
WT	Working Text

2.5 Relation to other documents

TR-124 Issue 2, Issue 3 [4]
TR-124 Issue 1 defines requirements for broadband Residential Gateway (RG) devices that are capable of supporting applications including data, voice, broadcast video, video on demand, etc. in broadband networks.

TR-124 Issue 2 updates TR-124 Issue 1 by specifying IPv6 capability with a set of requirements to support dual stack operation on both the LAN side and WAN side of an RG, including several IPv6 specific protocols, as well as some transitional mechanisms.

TR-124 Issue 3 updates TR-124 Issue 2 with additional IPv6 transition requirements regarding DS-Lite, 6rd, and Release Control.

TR-242 must support IPv6 and its transition requirements on RG defined in TR-124, TR-124 Issue 2 and TR-124 Issue 3 by way of reference to TR-124 as a whole.

TR-187 [7]
TR-187 provides updates to PPP-based operation in the Broadband Forum Architecture by including IPv6 over PPP as extensions to TR-59, TR-101 and other documents that originally only supported IPv4 over PPP. TR-187 defines requirements on the Residential Gateway (RG), Access Node (AN), and Broadband Network Gateway (BNG) so that Service Providers can provide both IPv4 and IPv6, i.e. dual stack, Internet services to their customers. TR-242 must support IPv6 over PPP and associated requirements defined in TR-187 by way of reference.

TR-177 [6]
TR-177 provides modifications to the TR-101 architecture in order to support both IPv4 and IPv6, i.e. dual stack operation in broadband networks, so that Service Providers can provide IPv6-based services and applications to their customers along with existing IPv4-based ones. TR-177 defines requirements on the Access Node (AN) and Broadband Network Gateway (BNG). The current TR-177 version only supports IPv6 unicast-based deployment. TR-242 must support the IPv6 over Ethernet under TR-101 architecture and associated requirements defined in TR-177 by way of reference.

WT-146
The Broadband Forum is working on a document WT-146, (Subscriber Sessions) that includes the concepts of separate an IPv4 and an IPv6 session and IP Session grouping for deployment in a TR-101 based architecture. WT-146 re-uses architectural notions introduced in TR-59 and TR-101 architectures, and places requirements on the Residential Gateway (RG) and IP Edge (i.e. the BNG) devices to establish and maintain single (IPv4 or IPv6) or dual stack (IPv4/IPv6) sessions. Note the ultimate goal of TR-242 is to enable Service Providers to provide IPv4/IPv6 dual stack services to their customers and so the WT-146 session architecture and requirements are supported in TR-242.

3 Technical Report Impact

3.1 Energy Efficiency

TR-242 has no impact on Energy Efficiency.

3.2 IPv6

TR-242 leverages existing RFCs for IPv4 and IPv6 capabilities, as well as some IPv6 transition mechanisms. TR-242 also references a number of IETF drafts that are currently under the development at IETF. This Technical Report does not define any new IPv6 protocol.

3.3 Security

The introduction of IPv6 into the home network removes the need of having NAT functions for IPv6 traffic in the RG. As a consequence, best practices may impose additional security requirements on the RG to protect the home network, e.g. use of RG Firewall options.

TR-101[3] provides loop identification in the BNG using RADIUS as one mechanism for authorizing the IPv4 service. TR-101 service authentication, if required, may be provided using 802.1X or PPP. When providing a dual stack or IPv6 service, the same authentication mechanisms can provide authorization for both.

R-1. Native IP services MUST be able to use the authentication mechanisms defined in TR-101, TR-177 and TR-187.

R-2. Overlay IP services MUST be able to inherit the native IP service authorization.

R-3. It MUST be possible to authorize IPv4 and IPv6 services for a subscriber with a single authorization transaction.

R-4. It MUST be possible to authorize IPv4 and IPv6 services for a subscriber with a separate authorization transaction for each of the service.

As for the case of DS-Lite, the AFTR must be configurable to terminate the tunnel for authorized users.

R-5. The AFTR MUST be configurable to limit service only to registered/authorized customers.

As described in RFC 6333 [37], in order to prevent the rogue devices from launching denial-of-service attack, AFTR must forward packets following the requirement below:

R-6. When de-capsulating packets, the AFTR MUST only forward packets sourced by RFC 1918 [14] addresses, an IANA reserved address range, or any other out-of-band pre-authorized addresses. The AFTR MUST drop all other packets.

3.4 Privacy

Some techniques may require logging user's transactions in order to be able to trace back the user's activities. Source IP address and Source Port only or Source and Destination IP address and port may be logged. When destination based logging is used user privacy might be affected.

4 Introduction to IPv6 Transition Options

4.1 Introduction

In the migration from IPv4 to IPv6, the dual stack model is the simplest and most well-understood approach today. Unfortunately the classic dual stack approach alone does not help with the IPv4 address exhaustion problem, as each end-user continues to need a permanently assigned public IPv4 address. In addition this model may not be directly applicable when Service Providers do not have enough IPv4 addresses left to provision the new subscribers.

There is a variety of coexistence or translation techniques being proposed at the IETF to allow continued expansion of the current Internet. The adoption by Service Providers of a specific mechanism in the BBF's architecture may depend on various factors, but a key one is the feature set that needs to be supported by the BNG.

The purpose of TR-242 is to analyze the applicability of different migration approaches and to describe a number of variations of the classic dual stack model that could satisfy the following business requirements:

- Allowing the Service Provider to continue providing access to IPv4 content and services to residential hosts (IPv4-IPv4 communications for dual stack hosts or IPv4-only hosts) when native IPv6 connectivity is offered to the customers;
- Reducing the consumption of global IPv4 addresses;
- Avoiding address family protocol translations (e.g. IPv4<->IPv6 Translations)

4.2 IPv4/IPv6 Migration Options

Service Providers' IPv4 based networks developed under different market and technical conditions. Different AAA architectures, RG deployments and customer authentication models can lead to different IPv6 migration strategies. Some network migration scenarios employ tunneling techniques that facilitate the transport of IP packets through network domains or segments that use the other IP address family. Other migration paths use a homogenous domain approach, and this allows IPv6 to be introduced without fundamental changes to existing protocols. Important milestones for all approaches are the trigger for starting migration (e.g. the date of expected exhaustion of IPv4 addresses for a given Service Provider) and the final target date for completing it. All the techniques listed here have different migration phases. Table 1 gives an overview of the techniques considered, their key features, required extensions and the way in which IPv4 addresses are shared. Figure 1 provides an overview of the temporal relationship between the various phases of each of the different techniques.

	Transport Migration			IPv4 Address Management
Approach	Key & Access Related Features	IP Migration Technique	Extensions	IPv4 Address Sharing capabilities
Dual-Stack with IPv4 Release Control	• Dual-Stack access • Keeping PPP infrastructure • Native IPv4-IPv6 without tunnel • Progressive IPv4 address savings with increasingly to IPv6 migrated services	• Native IPv4-IPv6	• Extended RADIUS communication • Modified RG	• Time based
DS-Lite	• IPv6 only • Use case – if IPv4 addresses already exhausted	• Native IPv6 • Tunneling IPv4 over IPv6	• Modified RG • DHCPv6 and RADIUS attributes	• NAT44 (Port based)
6rd optionally with NAT44	• Derivate of IPv6 to IPv4 tunneling • Access remains IPv4 only.	• Native IPv4 • Tunneling IPv6 over IPv4	• Modified RG • DHCPv6 and RADIUS attributes	• NAT44 (Port based)
Dual-Stack optionally with NAT444	• Dual-Stack access • Native IPv4-IPv6 • Reuse of address base • Impact on application layer	• Native IPv4-IPv6 • NAT44	• NAT44 function	• NAT44 (Port based)

Table 1 Overview of IPv6 Transition Mechanisms

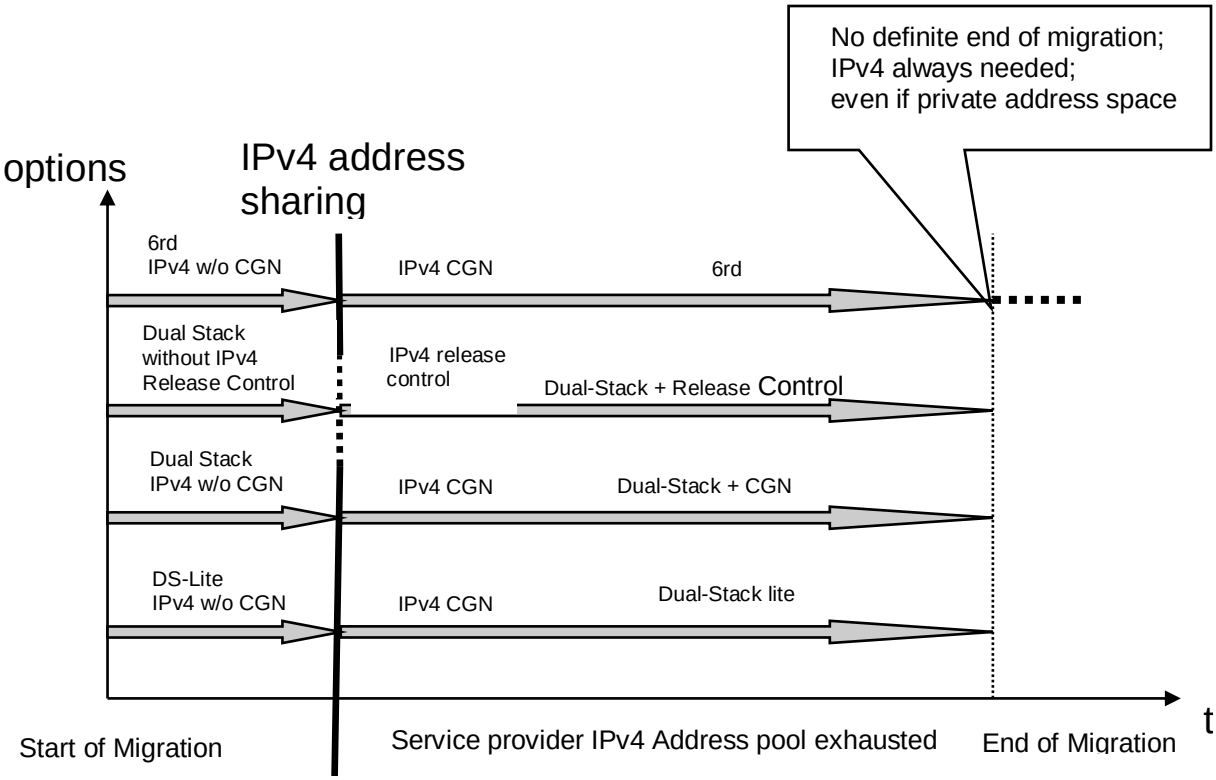

Figure 1 Timeline of IPv6 Transition Options

4.3 IPv6 Transition Mechanisms as Updates to TR-101

TR-101 [3] describes an access architecture based on Ethernet to support IPv4 services where several of the network elements have IPv4 awareness. IPv4-aware nodes are nodes that monitor traffic and rely on detecting IPv4 traffic in order to determine nodal behavior (e.g. routing, multicasting, collecting network management statistics). Figure 2 identifies the nodes that are usually IPv4 aware. These are therefore the nodes that may be impacted by a transition from IPv4 to dual stack or IPv6 support. TR-101 assumes publicly addressed IPv4 unicast and multicast transmission schemes in the access network, with the option of NAT functions in the Residential gateway.

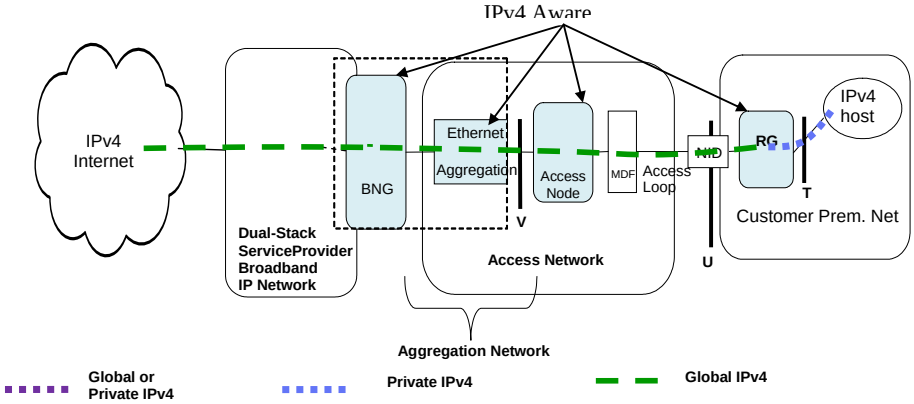

Figure 2 IP Aware Nodes in TR-101

TR-242 proposes several IPv6 transition mechanisms to aid carriers for their process of transitioning their networks to IPv6 as defined in TR-187 [7], TR-177 [6], and TR-124 [4], i.e. before full-bloom IPv6 operation takes place in their networks. One or more of the mechanisms as defined in TR-242 may be used to relieve IPv4 address exhaustion pressure, or provide IPv6-based connectivity and services over existing IPv4-based infrastructure, or both. When implementing one or more of such mechanisms in an existing broadband network, the existing broadband network architecture as defined in TR-101 [3] is unchanged.

The IPv6 transition mechanisms that are documented in TR-242 will require some additional networking functionality in the existing broadband networks and associated network equipments including the BNG and RG. Deploying IPv6 transition mechanisms in a given broadband network is of course optional, but if such mechanisms are deployed, they must not adversely impact the existing broadband networking functionality such as IPv4 multicast, QoS, etc. nor on the existing network equipments.

Therefore all the IPv6 transition mechanisms that are defined in TR-242 are done in the context of TR-101. The highlights of the relevant functions needed to support these IPv6 transition mechanisms mainly impact the following network elements:

- Some mechanisms require special functions on RG.

- Some mechanisms require additional functions (e.g. tunnel termination) to support IPv6 transition on a BNG or in some nodes in the Regional Broadband Network.
- IPv6 services imply IPv6 records on DNS servers.
- Some mechanisms require new RADIUS attributes and DHCPv6 options

Some tunnels (softwires) in the Access Network or/and Regional Broadband Network may also be needed to carry IPv4 or IPv6 packets.

Figure 3 shows a tunnel with its associated endpoints overlaid on the TR-101 architecture. The tunnel endpoints may contain additional functionality, e.g. NAT mechanism, to facilitate the transport of IP packets across an infrastructure supporting a different IP address family. The tunnel endpoint in the home network could exist at the terminal device, but for the purposes of this specification it is assumed to exist in the RG. The tunnel endpoint in the dual stack Service Provider's Broadband IP network could exist in a separate node than the BNG, or it could be integrated into the BNG.

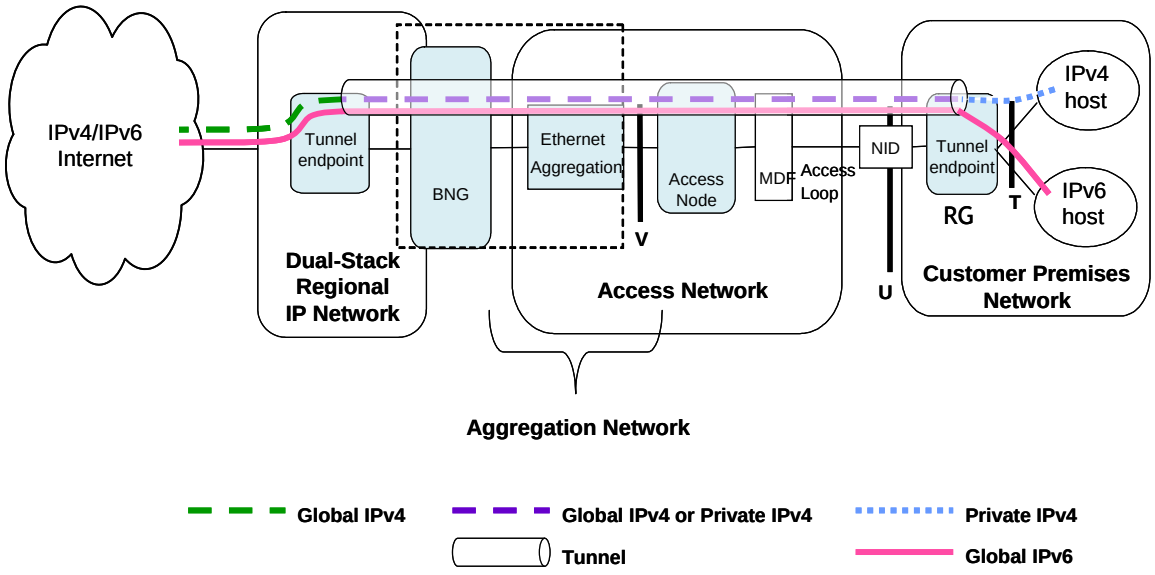

Figure 3 Tunnels and Endpoints Extending IPv4 TR-101

4.4 Operations, Administration and Maintenance during IPv6 Migration

Section 7/TR-101 [3] provides requirements for Ethernet OAM. During the migration to IPv6 these Layer 2 OAM functionalities are expected to continue to be deployed.

In IPv4-only broadband networks, IPv4-based OAM facility such as ICMP (RFC792 [9]) for troubleshooting and traceability has been deployed, and in IPv4-IPv6 dual stack environment, the IPv6-based counterpart, i.e. ICMPv6 (RFC4443 [24]) is also required. In the case of a tunnel, debugging across tunnel layers is not required.

With various IPv6 transitional mechanisms, IP-based OAM facility such as ICMP must be supported. Note in both 6RD and DS-Lite deployment, ICMPv6 and ICMPv4 packets are encapsulated with IPv4 and IPv6, respectively.

R-7. IPv6 ICMP (RFC 4443 [24]) MUST be supported in 6rd-enabled broadband networks.

R-8. IPv4 ICMP (RFC 792 [9]) MUST be supported in DS-Lite-enabled broadband networks.

4.5 Network Management through IPv6 Migration

The starting point of the IPv6 migration is the TR-101 architecture that provides various requirements for managing the access infrastructure using IPv4. The same functionality needs to be provided in the context of the dual stack or IPv6 service.

TR-069 assumes the availability of an IP infrastructure for access to the devices under management, and in the context of TR-101, this is specifically IPv4 connectivity. During IPv6 migration to support of dual stack or IPv6 services, the continued availability of IPv4 access for network management purposes permits the network infrastructure to be upgraded independently of the network management infrastructure.

R-9. The Access Node MUST be able to continue providing management access using IPv4 while providing dual stack or IPv6 services.

R-10. The BNG MUST be able to continue providing management access using IPv4 while providing dual stack or IPv6 services.

R-11. The RG MUST be able to continue providing management access using IPv4 while providing dual stack or IPv6 services.

4.6 General RG Requirement

For each IPv6 transition technology that a RG supports, a configuration knob must be provided in order to explicitly either enable or disable the relevant function associated with that specific technology.

R-12. The RG MUST be able to independently enable or disable native IPv4, Release Control, native IPv6, DS-Lite, and 6rd.

R-13. The RG MUST support the configuration of R-1 using either manual configuration or via TR-69.

R-14. A RG MUST support IPv4 and IPv6 dual stack operations on its LAN interface(s), according to requirements defined in LAN.ADDRESS, LAN.ADDRESSv6, LAN.DHCPS, LAN.DHCPv6S, LAN.DNS, LAN.DNSv6 sections of TR-124 [4].

Specific RG requirements associated with 6rd and DS-Lite are documented in Section 5 and Section 6, respectively. Most requirements on LAN side of a RG are common regardless of transition mechanisms as documented in TR-124 [4].

4.7 Summary

A Service Provider may decide to use different migration mechanisms, and at the same time, in different parts of its own network based on the type of BNG deployed in each single geographic area; these different migrations may or may not be concurrent.

A Service Provider may also then decide to move from one mechanism to another based on different factors such as:

- BNG technology evolution
- Migration from centralized to a more distributed architecture, according to the traffic growth
- Network Architecture Deployment model
- Service Deployment needs

This transition between different transitional mechanisms is not covered in TR-242.

5 6rd

5.1 Introduction – IPv6 Tunneled over IPv4 via 6rd

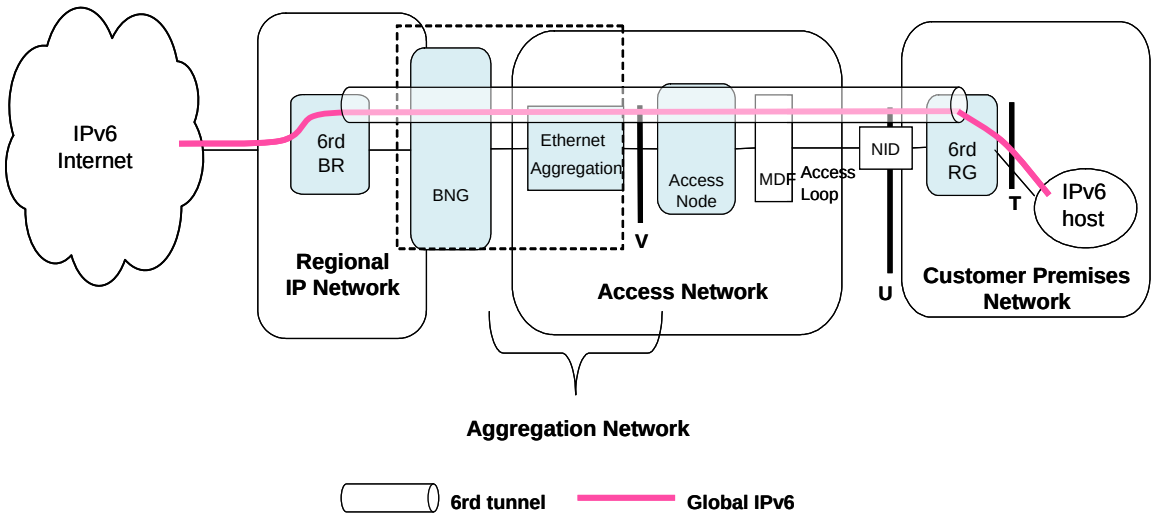

Figure 4 IPv6 Tunneled over IPv4 via 6rd

This approach permits an established IPv4 access infrastructure to introduce IPv6 services (and thus provides dual stack services) through a tunnel overlay. It has the following characteristics:

- Introduction of two components - 6rd RG (Residential Gateway) and 6rd BR (Border Relay)
- Automatic Prefix Delegation on 6rd RG
- Stateless, automatic IPv6-in-IPv4 encapsulation and de-capsulation functions on 6rd (RG & BR)
- IPv6 traffic automatically follows IPv4 Routing
- 6rd BRs addressed with IPv4 anycast for load-balancing and resiliency
- No impact on the Ethernet Aggregation Network

However, the 6rd approach does not specifically address the exhaustion of the public IPv4 address space as the underlying infrastructure remains IPv4.

The 6rd tunnels may be established over an IPv4 infrastructure using Private (RFC1918 [14]) or Public IPv4 addresses.

5.2 Technical requirements: IPv6 Tunneled over IPv4 via 6rd

When implementing the IPv6 tunneled over IPv4 via 6rd, which is defined in RFC5969 [32] (IPv6 Rapid Deployment on IPv4 Infrastructures), the following requirements apply.

5.2.1 6rd Configuration Requirements

6rd operation is limited to a Service Provider network or more accurately, a 6rd domain, where exactly one 6rd IPv6 prefix is required for the operation in that domain. A Service Provider may have more than one 6rd domains.

R-15. An RG MUST only support the assignment of a single 6rd prefix for a given 6rd domain.

R-16. A Border Relay MUST only be configurable with a single 6rd prefix for a given 6rd domain.

NOTE: A Service Provider may have multiple 6rd domains.

R-17. The IPv4MaskLen, 6rdPrefix, 6rdPrefixLen, 6rdBRIPv4Address MUST all be configured on the Border Relay and RGs with the same value, respectively, in a given 6rd domain.

Note that the RG IPv4 address used as a 6rd tunnel endpoint can be provisioned in the RG using a variety of mechanisms. The RG's IPv4Masklen is not sufficient for the 6rdBR though, it must also be provisioned with the implied embedded prefix. For example, assume the RG's IPv4Masklen is 8, and the RFC1918 10/8 space was used. The RG might be assigned an IPv4 address such as 10.1.92.3 and could determine the high order eight bits, but the 6RD BR would need to be provisioned with that 10.0.0.0/8, otherwise the BR does not know the high order bits of the RG address.

The MTU for IPv6 traffic sent over the 6rd tunnel may be configurable to be some value other than the IPv4 MTU adjusted for default tunnel headers. The WAN interface MTU of the RG should be configurable independent of any LAN interface MTU configuration. RG configuration is described in RFC 5969 [32], TR-124 [4] and TR-181 [8].

R-18. The 6rd BR MUST provide a mechanism to configure the MTU of the 6rd tunnel independent of any IPv4 MTU configuration.

5.2.2 Border Relay Requirements

A 6rd Border Relay Router MUST be implemented as per RFC 5969 [32].

The physical instantiation of the 6rdBR functions may be made at various points in a Service Provider's network, but it needs to have at least one IPv4-enabled interface, one 6rd virtual interface acting as an endpoint for the 6rd IPv6-in-IPv4 tunnel, and one IPv6 interface connected to the native IPv6 network.

R-19. The 6rd BR MUST be configured with the same 6rd elements as the 6rd RGs operating within the same domain.

R-20. The 6rd BR MUST be able to be configured with one IPv4 address at the BR for a given tunnel endpoints in a 6rd domain.

The BR IPv4 address may be an anycast address that is shared by multiple Border Relays in a single 6rd domain for the purpose of high availability and scalability.

R-21. The BR IPv4 address MUST be able to be an anycast address that is shared across a given 6rd domain.

For the sake of policy consistency, especially for QoS, it is useful to reflect the value of the IPv6 “Traffic Class” field into IPv4 "Type of Service" field, and vice versa:

R-22. The 6rd BR MUST be configurable to copy the value of “Traffic Class” field in an IPv6 packet into the “Type of Service” field of the corresponding IPv4 packet during the encapsulation process, and vice versa during the de-capsulation process. This behavior SHOULD be able to be configurable as per RFC 2983[19].

5.2.3 RG Requirements

The RG configuration to perform 6rd function is described in RFC 5969 [32], TR-124 [4], and TR-181 [8].

R-23. The RG MUST support 6rd CE (RG) functions per RFC 5969 [32].

R-24. A RG that is configured to perform 6rd CE function per RFC5969 [32] MUST comply with requirements defined in TRANS.6rd section of TR-124.

NOTE: There are several different methods for the RG configuration (Refer to Annex A:).

R-25. It MUST be possible to configure the RG so that all traffic destined to the same 6rd domain is EITHER sent directly OR via the 6rd Border Relay node.

R-26. The RG MUST NOT send multicast packets to 6rd tunnel.

R-27. The RG MUST be able to be configured with the IPv4MaskLen, 6rdPrefix, 6rdPrefixLen, and 6rdBRIPv4Address.

NOTE: The values of the parameters specified in R-27 need to be the same for all RGs in a given 6rd domain.

Per RFC5969 [32], 6rd delegated prefix is used in the same manner as a prefix obtained via DHCP-PD [21] and it is automatically created at a given RG by combining the 6rd prefix and all or part of the RG’s IPv4 address.

Since 6rd delegated prefixes are selected based on both the 6rd prefix and the IPv4 address assigned to a given RG, the registration of 6rd derived IPv6 address should not have a lifetime longer than the remaining lifetime of the IPv4 address from which it is derived

R-28. The RG MUST derive a 6rd delegated prefix based on the 6rd prefix and the RG's IPv4 address, with prefix length as /64 or shorter as specified in RFC5969, and announce it to the LAN via RA.

R-29. The RG's RA announcement of the 6rd delegated prefix to the LAN MUST persist even if the WAN connection goes down. When the WAN connection comes back up, the RG MUST attempt to re-discover the 6rd service. If the 6rd service no longer exists or delegated prefix changed, the RG MUST advertise the previous 6rd delegated prefix with lifetime of zero. If the 6rd prefix has changed, the RG MUST subsequently advertise the new prefix.

A single 6rd RG may be connected to more than one 6rd domain, in which case there would be a separate set of 6rd configuration parameters.

When both native IPv6 and 6rd are enabled and available, this is logically equivalent to multi-homing, and it may occur during a transition from a 6rd overlay to a native IPv6 service.

When both native IPv6 and 6rd are enabled and available, the RG has to be able to select the outgoing interface to use (native or tunnel). Different behaviors are needed for the cases where the two interfaces provide the same IPv6 prefix to the RG, or provide different prefixes.

R-30. When the same prefix is provided the default behavior SHOULD be to route over native IPv6 rather than 6rd.

R-31. If different prefixes are provided, the default behavior MUST be to set a flag to indicate the 6rd prefix is not preferred in the RA sent to the LAN.

For the sake of policy consistency, especially for QoS, it is useful to reflect the value of the IPv6 "Traffic Class" field into IPv4 "Type of Service" field:

R-32. The RG MUST be configurable to copy the value of "Traffic Class" field in an IPv6 packet into the "Type of Service" field of the corresponding IPv4 packet during the encapsulation process, and vice versa during the de-capsulation process. This behavior SHOULD be able to be configurable as per RFC 2983[19].

On LAN interfaces, a RG that supports 6rd must follow the guidelines as defined in TR-124 [4] for the IPv4-IPv6 dual stack operation.

5.3 Encapsulation Requirements

All IPv6 packets transported between a 6rd RG and a BR are encapsulated in IPv4 packets and as such, an RG-BR pair can be seen as two endpoints of a virtual link. When an RG sends an IPv6 packet encapsulated in an IPv4 header, the source IPv4 address is the RG's IPv4 address and the destination IPv4 address is the BR's IPv4 address, and the source and destination addresses are reversed when a BR sends an IPv6 packet encapsulated in an IPv4 header to a RG.

R-33. The RG MUST be able to be configured to send all 6rd traffic to the BR.

R-34. The RG SHOULD NOT send IPv6 Neighbor Reachability Detection (NUD, refer to RFC 4861[26]) packets to the 6rd BR. Note the RG can send packets to itself so as to test the reachability of BR.

R-35. The BR MUST support hair-pinning of 6rd traffic (i.e. traffic received over a 6rd tunnel interface having an IPv6 destination that requires forwarding back over the same 6rd tunnel interface).

5.4 6rd and RADIUS

6rd is used to provide IPv6 connectivity service through legacy IPv4-only infrastructure. 6rd uses DHCP as auto-configuration protocol. The 6rd RG uses an extension to the DHCP options to discover the 6rd BR and to configure IPv6 prefix and addresses (RFC5969 [32]). When the DHCP server is implemented in the BNG, the BNG can pass the 6rd configuration to 6rd RG using theses extended DHCP options.

In many networks, user configuration information is managed by AAA servers, together with user Authentication, Authorization, and Accounting (AAA). The RADIUS (Remote Authentication Dial In User Service, RFC2865 [18]) protocol is usually used by AAA Servers to communicate with network elements. When a BNG hosts a NAS (Network Access Server), i.e. the RADIUS client, it obtains relevant configuration parameters from the RADIUS server.

In these scenarios, it would be useful for the Service Provider to be able to tie together 6rd configuration with the customer profile and to maintain such information on the RADIUS server, so that the 6rd configuration can be passed to the 6rd RG via the RADIUS protocol.

The IETF draft [44] defines a new RADIUS IPv6-6rd-Configuration Attribute to carry the IPv4 address of the 6rd Border Relay for a given 6rd domain, and other configuration information. When the BNG receives such an attribute during the normal RADIUS message exchange with the RADIUS server, it must retrieve the 6rd Border Relay's IPv4 address and then pass it to the 6rd RG using the DHCP 6rd-option defined in RFC5969 [32].

R-36. When acting as a DHCP server, the BNG MUST be able to retrieve the IPv4 address of the 6rd Border Relay sent by RADIUS in the Access-Accept message and insert it into the 6rd-option field of the DHCP message.

5.5 6rd and IPv6 DNS

In the 6rd scenario, both IPv4 and IPv6 hosts and applications may co-exist (i.e. dual stack) behind 6rd RG, which cannot easily get the IPv6 DNS server address along with other 6rd parameters through in-band configuration method (e.g. there is no DHCPv4 option defined for it). Possible approaches to resolve this for the solution to address this issue include:

- IPv6 DNS proxy (over IPv4) on 6rd RG
- Assign IPv6 DNS server address manually or out-of-band (TR-069 [2])

The general RG requirements are described in Section 4.6, the following are additional DNS related requirements for 6rd RG:

R-37. The RG MUST support DNS proxy as per RFC 5625 [30] for IPv6 hosts connected on its LAN side.

R-38. Configuration of the IPv6 DNS server address at the RG via TR-069 SHOULD be supported.

R-39. Manual configuration of IPv6 DNS server address SHOULD be supported.

R-40. If Manual configuration of IPv6 DNS server address is used, it MUST override configurations via other methods.

6 DS-Lite

6.1 Introduction

6.1.1 Problem statement

This problem statement is related to the case of subscribers having a native IPv6 connectivity on the RG WAN interface of an IPv6-enabled RG. During the long transition phase from IPv4 to IPv6 (which could last for a long time), these subscribers still need to send and receive traffic to and from IPv4 hosts.

The assumption here is that all hosts that need to access IPv4 resources are either IPv4-only hosts or dual stack IPv6/IPv4 hosts. This is the case today for IP enabled hosts that are PCs. It is not excluded that in the future IPv6-only hosts will exist (for instance for small machines, sensors, etc.) but it is assumed that they do not need to access any IPv4 resources: for this reason, they are not in the scope of this problem statement. Given this assumption, it is not necessary to support IPv6-IPv4 communications, it is sufficient to support IPv4-IPv4 and IPv6-IPv6 communications.

In this context, it is required to have a technical solution which matches the following business requirements:

1) Continue to provide IPv4 connectivity for Internet service to residential hosts (IPv4-IPv4 communications for dual stack hosts or IPv4-only hosts) even when native IPv6 connectivity is available for Internet, VoIP and unicast IPTV services

2) Limit the consumption of global IPv4 addresses (because of address depletion: this is the main driver for IPv6 deployment)

3) As transparent as possible with regard to access and aggregation networks

4) Limit the use of cascaded IPv4 NAT capabilities because it implies the use of a private addressing scheme in the aggregation network. This can result in increased complexity of management due to:

    - Potential conflicts with private addresses already used by Service Providers in the aggregation network

    - Overlapping addressing schemes in the aggregation network, especially for large Service Providers (e.g. those with more than 16 million subscribers)

    Moreover, cascaded IPv4 NAT capabilities can cause potential issues with some services such as P2P.

5) Support for gradual deployment of the technology, only making it available initially to a small number of IPv6 customers, without needing to deploy the full

set of required functionality in all boxes spread around the Service Provider's networks.

In the case of IPv6oE, DS-Lite requires:

- The AN must support IPv6oE
- The Ethernet Aggregation Network nodes must support IPv6oE

6.1.2 Technical solution: DS-Lite

The technique proposed to meet the business requirements described above is based on the so-called Dual-Stack Lite model, a lightweight IPv4-IPv6 dual stack model currently specified by RFC 6333 [37]. The principle is the use of a tunnel (softwire) established between the RG (the softwire initiator) and a tunnel concentrator (called the AFTR) located somewhere in the Service Provider's network. The RG supports dual stack on its LAN interfaces(s) but ***only*** IPv6 on its WAN interface. The Dual-Stack tunnel is used to transport privately-addressed IPv4 datagrams that are encapsulated in IPv6 datagrams: several encapsulation schemes could be used, but IPv4-in-IPv6 (RFC 2473 [16]) is recommended here.

IPv6 datagrams that encapsulate privately-addressed IPv4 traffic is then forwarded (by the RG) to one of the available AFTR, whereas IPv6 traffic is globally addressed. IPv4 private addresses are assigned to subscriber hosts by the DHCPv4 server embedded in the RG, as it is already done today in many IPv4 architectures. An IPv4 address must be assigned to the B4 element(s) embedded in the RG, so that the B4 element can initiate IPv4 connection towards the network over the DS-Lite tunnel, according to RFC 6333. However there is no need to assign any IPv4 address to the WAN interface of the RG. An IPv4 address could be assigned by the RG to the DS-Lite tunnel as specified in RFC 6333, but this is not strictly necessary. The RG must be provisioned with the IPv6 address or the FQDN name of the AFTR: this can be done via manual configuration, TR-069 or a specific DHCPv6 option, as specified in RFC 6334 [38], note that with the DHCPv6 option, only FQDN name can be configured.

The AFTR is also a CGN device (Carrier Grade NAT) which translates private IPv4 addresses to and from global IPv4 addresses according to a classical NAPT scheme configured by the Service Provider. This means that a given global IPv4 address can be shared by more than one subscriber. The AFTR maintains the tunnel-specific information (such as the IPv6 address used by the RG for the tunnel) in a mapping table that is used and maintained by its CGN function to forward traffic coming from the IPv4 Internet into the right tunnel.

With CGN function, the AFTR supports an extended NAT table. This means that global IPv4 addresses are shared amongst several subscribers while de-multiplexing of users flows relies on the tunnel-specific information (e.g. the IPv6 address used by the RG for the tunnel) maintained in the AFTR's extended NAT table. The AFTR requires a well-known IPv4 address to enable communication from the RG, such as trace routing.

The following diagram shows the functioning of this solution:

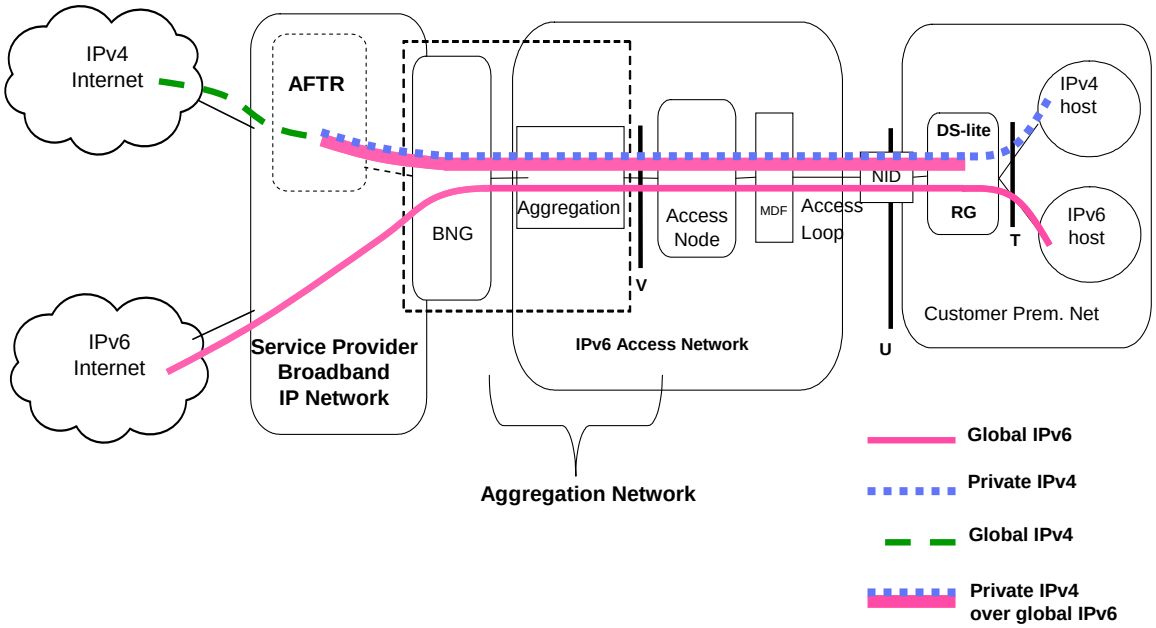

Figure 5 DS-Lite Example

Note: The figure shows the DS-Lite case where the AFTR is implemented outside of the BNG. It is also possible to implement the AFTR within the BNG node.

In Figure 5, the host indicated as "IPv4 host" is an IPv4-only host or a dual stack host that accesses IPv4 contents. Conversely, the host indicated as "IPv6 host" is an IPv6-only host (out of the scope of the DS-Lite solution) or a dual stack host that accesses IPv6 contents.

Note that only a single level of NAT is performed on IPv4 traffic at the AFTR level (meaning that the RG does not activate NAT capabilities anymore). This has the advantage of maintaining an acceptable level of operational complexity while avoiding potential address overlapping situations in the network.

This solution meets all the business requirements described in the corresponding problem statement and has also the following properties:

- There is no need for private IPv4 addresses to be routed within the Service Provider's network
- IPv4 address allocation to the RG is not required.
- There is no need for a DHCP server nor a PPP "server" for IPv4 in the Service Provider's network
- Only one level of NAT in the network is necessary for IPv4 (located at the AFTR)
- It supports a centralized or distributed architecture (several CGN devices can exist, *e.g.* one per POP, and can be incrementally deployed inside or outside the BNG)

Note that this solution is suitable only for IPv4 unicast traffic. The support of IPv4 multicast services to DS-Lite customers is still being specified in an IETF draft [45], so the IPv4 multicast is out of scope of this proposal and its traffic should not be forwarded in the DS-Lite tunnel.

6.2 Technical requirements: IPv4 Tunneled over IPv6 via DS-Lite

6.2.1 RG Requirements

The RG configuration to perform DS-Lite B4 function is described in RFC 6333 [37], TR-124 [4] and TR-181 [8].

As for RFC 6333 a DS-Lite B4 element is a function that is implemented on a dual stack capable device that creates a tunnel to a DS-Lite tunnel concentrator called an AFTR. In the solution defined here the B4 element is implemented in a routed RG that is a dual stack router.

R-41. The RG MUST implement a B4 element as defined in RFC 6333 in order to support DS-Lite.

R-42. A RG that is configured to perform DS-Lite B4 function per RFC 6333 MUST comply with requirements defined in TRANS.DS-Lite section of TR-124.

R-43. When running DS-Lite, the RG MUST deactivate the NAPT function on the DS-Lite interface.

R-44. The B4 element of the RG MUST support IPv4-in-IPv6 encapsulation on its WAN link as specified in RFC 2473 [16].

In order to guarantee interoperability, the RG supports the DHCPv6 option to retrieve the AFTR information. Manual configuration or Remote Configuration (via TR-069) of the IPv6 address or the FQDN of the AFTR element should also be supported.

A RG may be configured with either the IPv6 address or the FQDN name of the DS-Lite AFTR via manual method or TR-069, and in addition, DHCPv6 AFTR_NAME option can carry AFTR FQDN name and that can be conveyed to the RG from a DHCPv6 server.

R-45. The RG MUST comply with the requirements in the WAN.TRANS.DS-Lite 6, 7, 8, and 9 sections of TR-124.

R-46. The RG MUST support configuration of the method whereby the AFTR element (FQDN or IPv6 address), is acquired, i.e. via DHCPv6, TR-069, or manually.

R-47. The RG MUST support configurations of a static IPv4 default route towards the DS-Lite tunnel for the IPv4 traffic.

Using an encapsulation (IPv4-in-IPv6) to carry privately-addressed IPv4 traffic over IPv6 will reduce the effective MTU of the datagram. Unfortunately, Path MTU discovery (RFC 1191 [12]) is not a reliable method to deal with this problem. The best solution is to increase the MTU size

of all the links between the B4 element and the AFTR elements by at least 40 bytes (size of the nominal IPv6 header).

However, this is not always possible in some deployments, because some legacy network devices cannot support an increased MTU and then the end-to-end MTU between the B4 element and the AFTR cannot be big enough, and therefore an alternative solution is required. One method is to tweak the TCP MSS option of IP packets. This solution is widely used today to cope with a similar issue related to the MTU decrease due to PPPoE encapsulation.

R-48. The RG MUST be able to rewrite the TCP MSS option of TCP packets forwarded over the DS-Lite softwire, according to the MTU of that softwire.

Another solution consists of in supporting packet fragmentation:

R-49. The RG MUST be capable of performing packet fragmentation and reassembly as specified in Section 7.2/RFC 2473 [17].

For the sake of policy consistency, especially for QoS, it is useful to reflect the value of the IPv4 "Type of Service" field into the IPv6 "Traffic Class" field:

R-50. The RG MUST be configurable to copy the value of "Type of Service" field in an IPv4 packet into the "Traffic Class" field of the corresponding IPv6 packet during the encapsulation process, and vice versa during the de-capsulation process. This behavior SHOULD be able to be configurable as per RFC 2983[19].

In cases where it is needed, The WAN interface of the RG may need to be configured with an IPv4 address; in such situations the IPv4 address could be assigned to the DS-Lite tunnel as specified in RFC 6333.

When an application running on the RG initiates an IPv4 connection, it needs to send packets with an IPv4 source address configured on the B4 element as specified in RFC 6333.

R-51. The RG MUST be able to be configured with an IPv4 address in the pool 192.0.0.0/29, excluding 192.0.0.1, as specified in RFC 6333.

When both native IPv4 and DS-Lite are enabled and available, the RG must be able to select the right interface for IPv4 traffic forwarding, and this is logically equivalent to multi-homing.

R-52. When both native IPv4 and DS-Lite are enabled and available, the RG MUST be able to be configured with enough adequate IPv4 routing information to select which outgoing interface to use (native or tunnel).

On LAN interfaces, a RG that supports DS-Lite must follow the guidelines as defined in TR-124 [4] for the IPv4-IPv6 dual stack operation.

6.2.2 AFTR Requirements

An AFTR element is the combination of an IPv4-in-IPv6 tunnel end-point, referred to as a softwire concentrator in RFC 6333 and an IPv4-IPv4 NAPT usually implemented on the same node. Since the NAPT function is deployed in the network, it is referred to Carrier Grader NAT (CGN) in current literature. The AFTR element can either live as a standalone network node or it can be embedded on the BNG.

R-53. The AFTR MUST support IPv4-in-IPv6 as specified in RFC 2473 [16] to establish the DS-Lite softwire.

R-54. The AFTR MUST be able to perform packet fragmentation and reassembly as specified in Section 7.2/RFC 2473.

For the sake of policy consistency, especially for QoS, it is useful to reflect the value of the IPv4 "Type of Service" field into IPv6 "Traffic Class" field, and vice versa:

R-55. The AFTR MUST be configurable to copy the value of "Type of Service" field in an IPv4 packet into the "Traffic Class" field of the corresponding IPv6 packet during the encapsulation process, and vice versa during the de-capsulation process. This behavior SHOULD be able to be configurable as per RFC 2983[19].

The NAT44 function implemented on the AFTR conforms to RFC 4787 [25], RFC 5382 [27], RFC 5508 [28], and draft-ietf-behave-lsn-requirements [42] respectively. For further details refer to the CGN (Section 9).

R-56. The AFTR MUST support a MTU increased by at least 40 bytes on RG facing interfaces in order to accommodate both the IPv6 encapsulation header and the IPv4 datagram without fragmenting the IPv6 packets.

Note that the network transited between the RG and AFTR also needs to support the larger MTU size if packet fragmentation is to be avoided.

R-57. The AFTR MUST be capable of rewriting the TCP MSS option of TCP packets forwarded over the DS-Lite softwire, according to the MTU of that softwire.

6.2.3 BNG requirements

DS-Lite AFTR function may be implemented on a BNG.

R-58. When acting as an AFTR, the BNG MUST comply with RFC 6333 [37].

R-59. When acting as DHCPv6 Server, the BNG MUST be able to send the FQDN name of the AFTR element by means of the DHCPv6 option, as defined in RFC6334 [38].

6.3 DS-Lite and RADIUS

Dual-Stack Lite (RFC6333 [37]) is a solution that offers both IPv4 and IPv6 connectivity to those customers who have an IPv6 prefix (i.e. no IPv4 address is assigned to the attachment device). It is a technique that addresses the need for IPv4 service continuity during the forthcoming IPv6 transition period. One of its key components is the IPv4-over-IPv6 tunnel, but a DS-Lite Basic Bridging Broadband (B4) will not know if the network it is attached to offers Dual-Stack Lite support, and if it did, would not know the remote end of the tunnel to establish a connection.

The RFC6334 [38] specifies a new DHCPv6 option, which is used by a Dual-Stack Lite B4 capable RG to acquire the Address Family Transition Router (AFTR) name.

When a DHCPv6 Server receives a DHCPv6 request containing, in the OPTION_ORO, the AFTR_NAME option, the DHCPv6 server must be able to include in its response the DS-Lite AFTR name in the AFTR_NAME option. In order to do so, the DHCPv6 Server must be aware of, for each customer or group of customers, the Tunnel Terminator endpoint Name for each customer or group of customers.

The DHCPv6 server may be configured to send the same or different tunnel endpoint configuration information to B4 elements. In such case, it would be useful for the Service Provider to be able to tie together the Tunnel End-point information with the customer profile and to maintain such information in a single, centralized place, and for an example, the RADIUS Server.

RFC6519 [40] specifies a new RADIUS attribute to carry the Dual-Stack Lite Address Family Transition Router (AFTR) name, called the DS-Lite-Tunnel-Name; this RADIUS attribute is defined based on the equivalent DHCPv6 option already specified in RFC6334 [38].

R-60. When acting as a DHCPv6 Server the BNG MUST be able to retrieve the contents of the DS-Lite-Tunnel-Name sent by RADIUS server in the Access-Accept message and insert it into the DHCPv6 AFTR_NAME option.

6.4 DS-Lite and IPv4 DNS

In the DS-Lite scenario, both IPv4 and IPv6 hosts and applications may co-exist (i.e. dual stack) behind a B4 element, which cannot easily get the IPv4 DNS server address along with other DS-Lite parameters through in-band configuration method (e.g. there is no DHCPv6 option defined for it). Possible approaches to resolve this for the solution to address this issue include:

- IPv4 DNS proxy (over IPv6) on DS-Lite B4 implemented on a RG
- Assign IPv4 DNS server address manually or out-of-band (TR-069)

The general RG requirements are described in Section 4.6, the following are additional DNS related requirements for DS-Lite RG:

R-61. The RG MUST support DNS proxy as per RFC5625 [30] for IPv4 hosts connected on its LAN side.

R-62. Configuration of the IPv4 DNS server address at the RG via TR-069 SHOULD be supported.

R-63. Manual configuration of IPv4 DNS server address SHOULD be supported.

R-64. If Manual configuration of IPv4 DNS server address is used, it MUST override configurations via other methods.

7 Dual-Stack model with private IPv4 address space and CGN implemented on the BNG

7.1 Introduction

The proposed approach is based on the following principles:

- Native IPv6 connectivity is provided to the customers
- A pool of IPv4 globally routable addresses is shared among several subscribers

In this model at least part of the Service Provider network (for example, the access network or the aggregation network) supports IPv6 forwarding capabilities; in addition a Carrier Grade NAT function, responsible for translating the private IPv4 addresses into globally routable IPv4 addresses, is placed within the Service Provider network.

Each RG is assigned at least one global IPv6 prefix, plus one unique or private IPv4 address subnet locally routable in the operator's network, which is then subsequently NAT'ed out to a globally routable IPv4 address by the Service Provider owned Carrier Grade NAT function that occurs on the BNG or elsewhere.

IPv6 packets are natively forwarded within the Service Provider network.

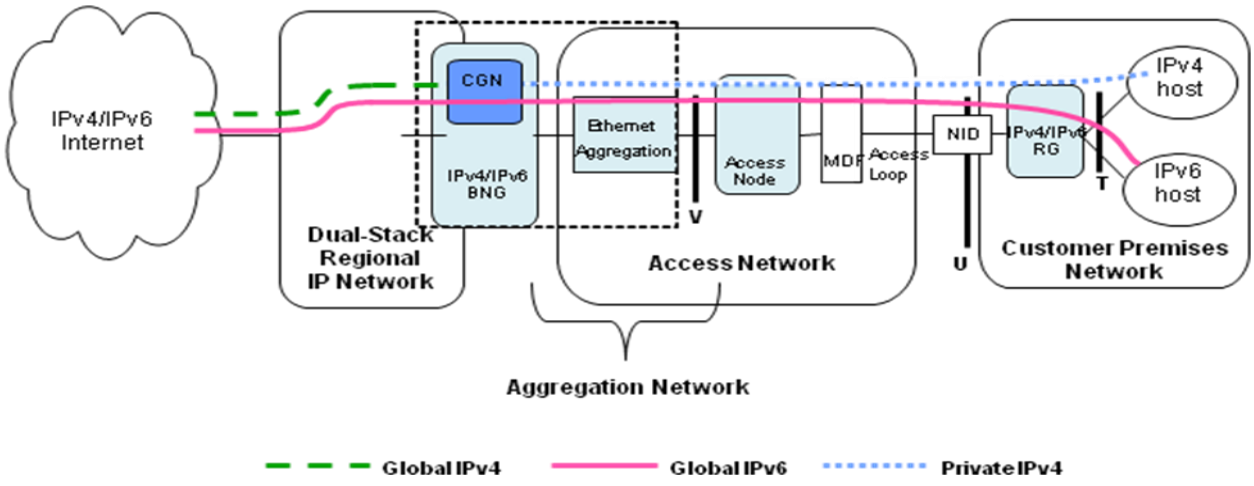

Figure 6 Dual-Stack with Private IPv4 Address

7.1.1 Comparison with DS-Lite model

The model as described in this section has some similarities and presents some analogies with the DS-Lite approach ([37]), for example it makes use of the CGN function, but it differs from DS-Lite in the following key aspects:

1) No need to create an IPv4 over IPv6 tunnel from the RG (simplification on the RG) but at the cost of extra management complexity due to the allocation and forwarding of private IPv4 addresses on RG.

2) There will be extra IPv4 routing complexity compared to DS-Lite if the CGN function is not performed at the BNG.

3) Single device used to terminate both IPv4 and IPv6 traffic sessions: this model simplifies the re-use of AAA/Radius and subscriber management infrastructure for both IPv4 and IPv6 traffic. There will be additional complexity for DS-Lite if the AFTR function is not performed on the BNG, because subscriber management will have to be performed in different places for IPv4 and IPv6.

7.1.2 Avoiding IPv4 over IPv6 tunnel

The possibility of avoiding the IPv4 over IPv6 tunnel is dependent on the placement of CGN function: in this scenario, the CGN is embedded in the BNG, thus it is located in the same Layer 2 domain where the RGs are, and hence the subscribers' private IPv4 addresses are not exposed beyond the NAT/BNG device.

The specific placement of the CGN, on the BNG, allows the native forwarding of subscribers' IPv4 traffic with private IPv4 addresses. However, the extra cost of complexity introduced by double-NAT should be considered by the operator.

In the DS-Lite model, the CGN function is part of the AFTR, which can be physically located in a device anywhere in the Service Provider network. To avoid addressing and routing IPv4 in the Service Provider network, an IPv4 over IPv6 tunnel can be used to carry the IPv4 traffic from the RG to the CGN.

7.2 BNG Requirements

R-65. When implementing CGN on the BNG, the BNG MUST support the CGN requirements specified in Section 9.

8 Support of IPv6 Connectivity with Content Based IPv4 Release Control

8.1 Problem statement

Exhaustion of the IPv4 address space is expected (IANA IPv4 address space allocations were finished in February 2011, RIR allocations are expected to finish in 2012) while dual stack deployment is still ongoing. To decrease the simultaneous IPv4 address demand in a dual stack environment Always-On service like VoIP, Software Update Services and IPTV should be deployed via IPv6-only. To mitigate migration problems, a universal solution for dual stack connectivity (e.g. PPPoE session) for RGs and for PC clients is preferred. The dual stack approach alone will not help to save IPv4 addresses because IPv4 is still at any time used in the session. To achieve address savings Release Control uses IPv4 only limited period of time of the session.

To deal with IPv4 address space exhaustion, techniques such as Large Scale NAT (LSN a.k.a. CGN) or port based routing (IETF: experimental RFC 6346 [39]) are intended to provide a more effective IPv4 utilization. Port based address sharing has issues (documented in RFC 6269 [35]). For comparisons with other solutions see Section 4.2.

The effectiveness of IPv4 address usage has to be increased to perform a smooth migration with the lowest possible customer impact. For this purpose the below described method provides a method to dynamically release IPv4 addresses of dual stack (PPPoE) sessions in order to reuse them as needed. This method allows shaping the IPv4 address demand.

8.2 Technical solution: Dynamically provisioned IPv4 Address

This approach is based on IPv4/IPv6 dual stack IP Edge. By using PPP sessions with dual stack access, end devices in customer networks can communicate via IPv4 and/or IPv6 dependant on the capabilities of the network itself and of the services/endpoints.

Based on the assumption that the Service Provider provides broadband access as well as IP based services, coordination of IPv6 migration between access and backbone networks as well as the services is possible and recommended. Then the access to IPv6 based services will then be possible as soon as IPv6 network connectivity on the customer side is provisioned. As of the preferable and increasing usage of IPv6 when both IPv4 and IPv6 connectivity are available, IPv4 traffic demand will not increase but decrease in the medium-term perspective. Figure 7 illustrates an Internet access architecture where IPv4 and IPv6 are supported, to which the Release Control mechanism is applicable.

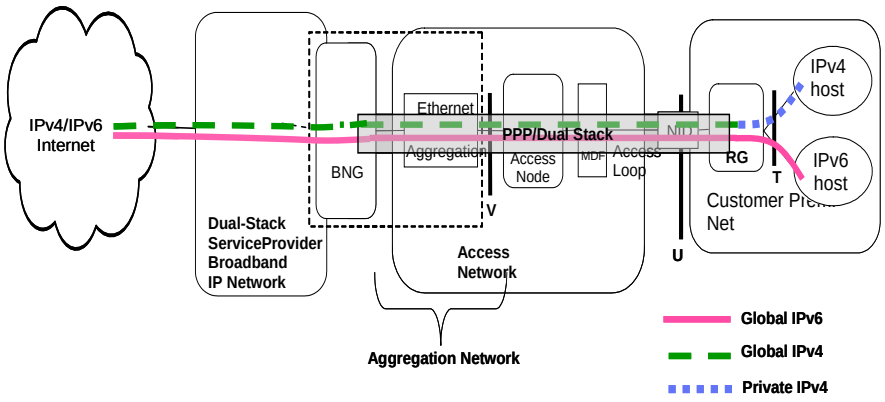

Figure 7 Release Control

This approach is based on the assumption that the customer initiated a session based on IPv6 (see point 1 of Figure 8) and uses IPv4 only if applications or services request IPv4 connectivity. Any services which were available before the migration of the network are continuously supported. When IPv4 connectivity is not needed during the time of network connectivity the continuous providing of a global IPv4 address to the RG is not necessary. The provisioning of IPv4 addresses can then be done dynamically at run-time of the PPP session.

The goal of the solution is to use the IPv4 address resources more efficiently, to decrease the use of IPv4 addresses and limit the size of the used IPv4 address pool. Assuming that always-on services are reachable via IPv6, a dual stack capable RG should request IPv4 address parameters only on demand when sending out IPv4 traffic towards the WAN interface is intended. That means the RG will not start initially a dual stack PPP session but an IPv6-only PPP session. This can be accomplished by using only IPCPv6 in the PPP setup. The IPv4 part of dual stack is only set up on demand in the case of explicit IPv4 communication requests by the RG.

In order to detect IPv4 traffic demand for the WAN interface the RG should detect the different IP protocols. This is very similar to today's behaviour, when IPv4-only traffic demand requests trigger the establishment of the whole PPP session.

The BNG will then request IPv4 address parameters via the RADIUS protocol from the platform controller of the Service Provider. The platform controller will respond with IPv4 address attributes for the RG to the BNG. The BNG then allocates the IPv4 address parameters via IPCP to the RG (due Section 3.3/RFC1332 [12]). With this additional IPCP IPv4 session set up the dual stack PPP session is established (see point 2 of Figure 8).

In order to detect that no IPv4 connectivity is needed anymore the RG needs to sense IPv4 traffic towards the WAN interface. The RG should start a timer if no IPv4 traffic is seen. This is very similar to today's implementation, where the whole PPP session is terminated in the absence of

traffic. After reaching the timer's threshold the RG sends an IPCP termination request message to the BNG to release the used IPv4 address.

When the BNG receives this message it sends an *Interim Accounting* to the platform controller to signal the releasing of the IPv4 address. The platform controller confirms the release of the IPv4 address (see point 3 of Figure 8).

During the lifetime of a PPP session this IPv4 address release/request process can happen several times.

An appropriate message flow is shown in Figure 8.

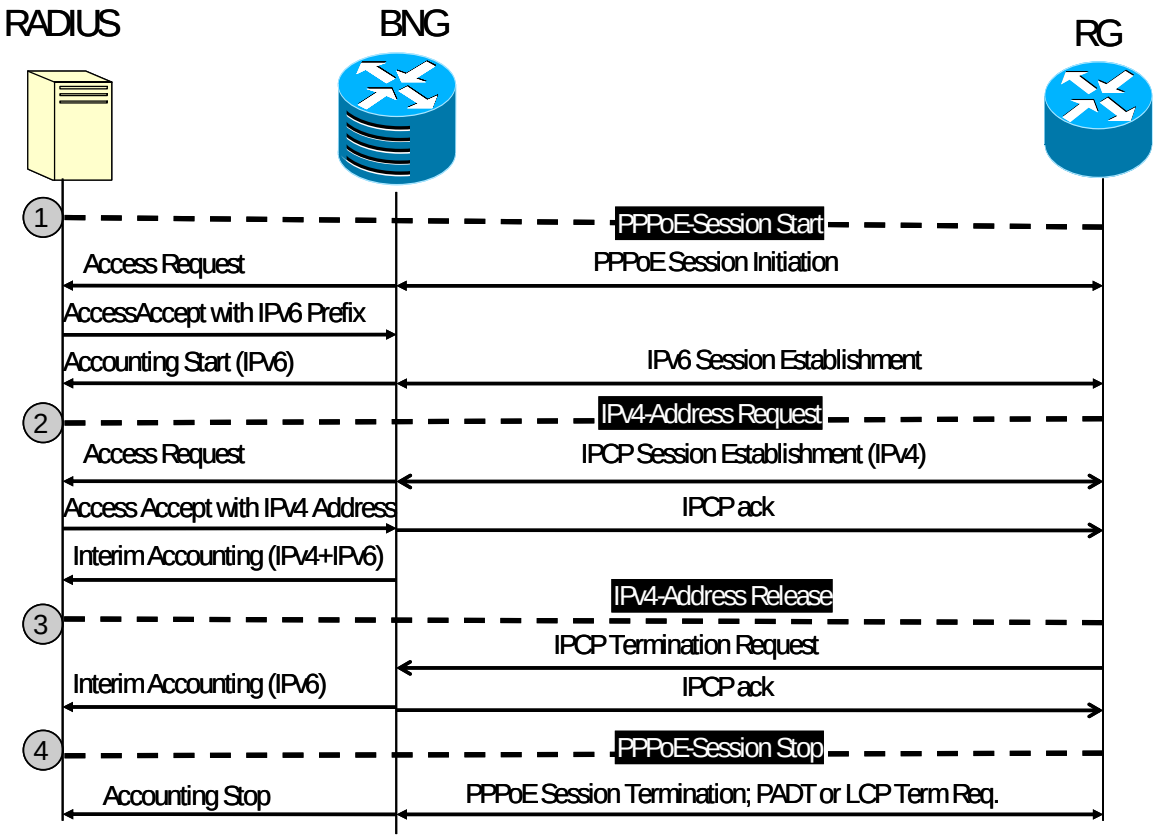

Figure 8 Release Control Signaling Example

8.3 Session/User impact

Establishing a new session with IPv4 while no IPv4 address was assigned to the WAN interface might have some impact on the user experience. A delay is created due to the time it takes to establish IPCP and assign an IPv4 address (or the equivalent DHCP process). In practice, this delay will be shorter compared to the PPP on demand mode as the authenticated PPP session is already established.

All other functions of session establishment, routing, forwarding and NAT are untouched, so that there are no further impacts or incompatibilities expected.

8.4 Technical requirements for: IPv4 Address release control

8.4.1 RG requirements

R-66. The RG MUST provide a mechanism which monitors IPv4 session/traffic.

R-67. The RG MUST provide a timer based trigger for releasing the IPv4 address.

R-68. The RG MUST support PPP according to RFC 1332.

R-69. The RG MUST provide the (re)assignment and release of an IPv4 address inside a PPP session according to the procedures of Section 5/RFC 1661 [11] and Section 3/RFC 1332 [12] independent of the IPv6CP status according to Section 2.1/RFC 4241. The timer which triggers the release of the IPv4 address MUST be configurable in minutes.

R-70. The timer which triggers the release of the IPv4 address MUST be configurable via TR-069.

8.4.2 BNG requirements

R-71. The BNG MUST support the release and the (re)assignment of IPv4 addresses inside the PPP session according to the procedures of Section 5/RFC 1661 [11] and Section 3/RFC 1332 [12] independent of the IPv6CP status according to Section 2.1/RFC4241 [23].

R-72. The BNG MUST be able to report release and (re)assignment of IPv4 addresses to the AAA platform.

9 Network Address Translation Function

9.1 Address Spaces and NAT

The IPv4 address space is divided into Private and Public address spaces (by RFC 1918 [14]). Network Address Port Translation as defined in RFC 2663 [17] is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol and User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. This solution provides a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses. In TR-242, we use the term NAT44 to refer to a NAPT function where the addresses of internal and external realms are IPv4 addresses.

In the migration towards an IPv6 infrastructure, it is expected that all of these address spaces may exist simultaneously. For example, whether the Service Provider uses tunneling of IPv6 packets over the native IPv4 network, tunneling of IPv4 packets over a native IPv6 network, or Native dual stack, the Service Provider is simultaneously supporting IPv4 and IPv6.

NAT44 has been deployed widely for many years, especially in enterprise networks (RFC 3022 [20]) and in customers' home networks; the same technology is likely to be deployed in carrier's networks because of the depletion of global IPv4 addresses. In addition, there are currently new deployments based on other types of NAT technologies, in particular IPv6 to IPv4 translation, i.e. NAT64 (RFC 6146 [33] and 6147 [34]). For the purpose of TR-242, only the NAT44 technology that is currently deployed in carrier's network is included; other types of NAT are out of scope.

NAT44 functions are currently found in RG devices at the boundary between the Home Network and the Service Provider Network. Hosts connected to a Layer-3 RG are assigned IPv4 private addresses while an IPv4 public address is assigned to the RG so that those hosts can communicate with hosts and servers located in the external realm. The NAT44 requirements on a RG are documented in TR-124 [4].

IPv4 address exhaustion will ultimately make transition to IPv6 desirable. However, due to several reasons, the deployment of IPv6, especially at large scale, cannot be done overnight. Existing Internet content will be available via IPv4 for some considerable time. Some solutions are under development at the IETF to accommodate the transitional time required in some carriers' networks where IPv4 and IPv6 operations and services may co-exist. Using NAT44 capabilities in a broadband access network is one of these solutions.

9.2 Carrier Grade NAT44

When a NAT44 function is performed by a node in the broadband access network, the general translation function on these devices is the same as defined in RFC3022 [20], but there are specific carrier class requirements with regard to scalability, reliability, etc. and this approach is therefore referred to as CG-NAT44 (Carrier Grade NAT44, in [47]). In such deployment, a single public IPv4 address is shared by multiple subscribers thus reducing IPv4 address consumption. The intent is to rationalize the management of the remaining IPv4 address blocks to guarantee IPv4 based service continuity during the transition period.

CG-NAT44 is the term used in TR-242 for NAT44 function when it is deployed in a broadband network and then subject to several requirements specified below. Two scenarios are considered in TR-242:

- NAT444: in this scenario, the CG-NAT44 function is implemented in a carrier network and is in addition to the NAT44 function implemented in the RG.

- DS-Lite: in this scenario, the CG-NAT44 function is usually implemented in the device that supports the AFTR capability as per RFC 6333 [37].

Figure 9 and Figure 10 illustrate these two scenarios, respectively.

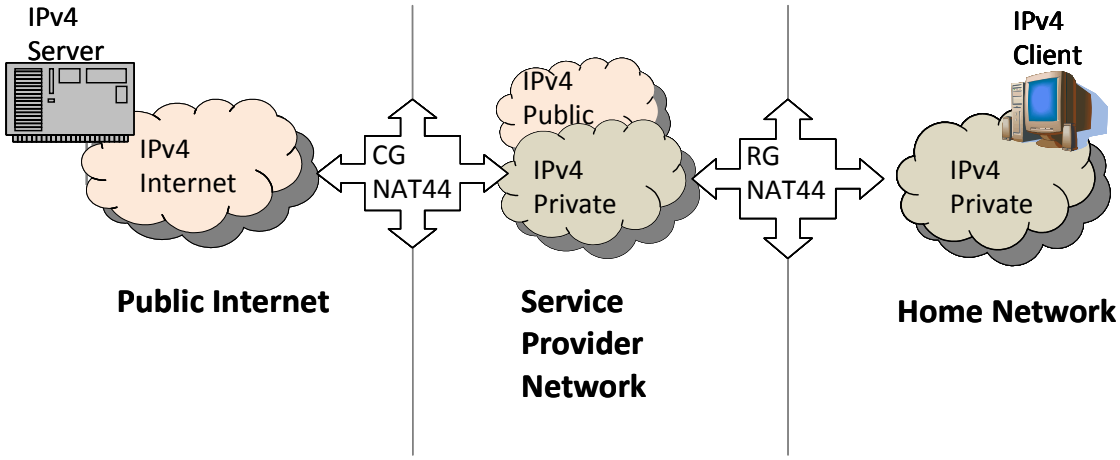

Figure 9 Deployment of CG-NAT44 function within the NAT444 scenario

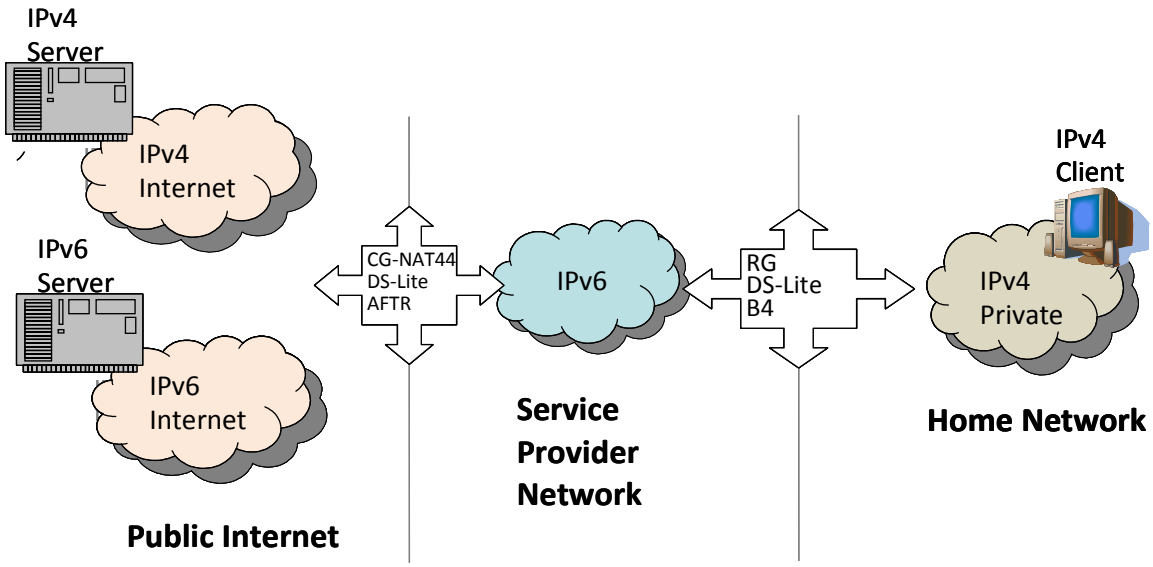

Figure 10 Deployment of CG-NAT44 function within the DS-Lite scenario

In the Broadband Forum architecture, the CG-NAT44 functionality can be placed either in the BNG or in an external device. Note that the CG-NAT44 function, including those implemented according to the IETF draft [47] and DS-Lite RFC 6333 [37], utilizes IPv4 address sharing mechanisms as opposed to assigning a separate global IPv4 address to each individual subscriber as deployed in today's broadband networks. While sharing IPv4 addresses would reduce the consumption of global IPv4 addresses, and make it easier to support the transition phase from IPv4 to IPv6, there exist a number of issues that carriers must be aware of before actual deployment of any address sharing function such as CG-NAT44. Issues with IP address sharing are referred to RFC6269 [35].

The requirements for CG-NAT44 are defined in the following sections. Most of them apply to both NAT444 and DS-Lite scenarios. Some of them are specific to the DS-Lite scenario.

9.3 General requirements

The CG-NAT44 device must implement NAT44 functions as defined in RFC2663 [17] with additional requirements from the Service Provider's perspectives.

R-73. The CG-NAT44 device MUST implement NAT44, based on NAPT as defined in RFC2663 [8].

R-74. The public IPv4 addresses pools maintained by the CG-NAT44 MUST be configurable by the Service Provider.

R-75. The CG-NAT44 device MUST support TCP, UDP, ICMP, DCCP requirements as defined in RFC4787 [27], RFC5382 [28], RFC5508 [28], and RFC5597 [29], respectively.

In addition, it must support all mandatory requirements (with the key word MUST) defined in Section 3 of draft-ietf-lsn-requirements [42] as follows:

R-76. The CG-NAT44 device MUST support all mandatory requirements (i.e. with the key word MUST) as specified in Section 3 of draft-ietf-lsn-requirements [42].

Some of the requirements which are optional in RFC4787 [27] have been made mandatory as follows.

R-77. The CG-NAT44 device MUST have an "Endpoint-Independent Mapping" behavior as specified as REQ-1 in RFC4787.

This requirement means that for the same internal source address and port (X:x), the CG-NAT44 device maintains the same source external mapping (X':x') regardless of the destination IP address (Y1 or Y2).

R-78. The CG-NAT44 device MUST have an "Endpoint-Independent Filtering" behavior as specified as REQ-8 in RFC4787.

The CG-NAT44 device MUST have an IP address pooling behavior of "Paired" whenever there are enough external ports available to do so. The behavior of "Paired" means that only one external address is allocated to one internal address.

R-79. If there are not enough ports available to have an IP address pooling behavior of "Paired", the CGN-NAT44 MUST be able to allocate a new external address to one internal address, i.e. an external address different from the ones already allocated to that internal address.

9.4 Other Requirements

Within the context of CG-NAT44 deployment, a single IPv4 address is shared by more than one subscribers' RG, it is therefore necessary for the ISP to perform an IP session log on CGN device in order to identify individual end-users. In some environments, ISP needs to comply with law enforcement agencies to attribute resources. In such cases, ISP needs to have a way to answer the question "*who was using IPv4 address a.b.c.d port number xyz at date t*?" Such information may have been collected according to guidance provided in RFC6302 [36].

R-80. CGNs MUST provide a way to attribute IPv4 address/source port number/time stamp to a subscriber.

There are many ways to achieve this, ranging from logging of every session on the CGN to logging of port block allocation only, all the way to deterministic NAT where ports are pre-allocated to users and CGNs generate no logs at all.

R-81. A CG-NAT44 device MUST be able to perform NAT44 translation log with appropriate storage and processing capacity.

R-82. Session based logs MUST include at least the following:

- Internal Source IPv4 address
- Internal Source UDP or TCP port
- External Source IPv4 address
- External Source UDP or TCP port
- Timestamp in UTC (for assignment of a NAT44 mapping) accurate to the second from a traceable time source (e.g. RFC 5905 [31])
- In case of DS-Lite: Softwire identifier(e.g. IPv6 source address of the DS-Lite tunnel on RG)

Note that the accuracy of timestamps is very important for the logs to be useful for correlation purposes. Having incorrect timestamps could lead to the attribution of a packet to the wrong subscriber.

In general, the amount of CGN log information is huge due to the dynamic nature of IP flow, the large number of users, etc. resulting in potential problems when dealing with storage, information transfer, management, etc.

R-83. A CG-NAT44 device MUST be able to minimize the amount of information required to trace Internet activity back to its source.

In some environments, it may be useful to perform bulk port allocation for TCP/UDP**,** i.e. a port set that contains multiple ports instead of a single one, to be allocated by the CGN for a given subscriber, and this port set can be consecutive allocated before any IP session to and from that subscriber is established, or scattered. Bulk port allocation scheme reduces the amount of log information on the CGN because the logging is based on individual subscriber, as opposed to each IP session.

Note that if deterministic NAT is used, no logging is required because the bindings are either algorithmically determined or permanently mapped.

R-84. A CG-NAT44 MUST implement mechanisms in order to minimize the amount of the log information including at least the following:

- Bulk Port Allocation. The port set allocated by the CGN can be Consecutive or Scattered.
- Deterministic NAT

When Bulk Port Allocation is used the CG-NAT44 can create one log per range of ports instead of a single log per port. This behavior would reduce the amount of logs created by the CG-NAT44.

R-85. Bulk Port Allocation based logs MUST include at least the following:

- Internal Source IPv4 address
- External Source IPv4 address
- External Source bulk port id (UDP or TCP)
- Timestamp in UTC (for assignment of a bulk port id) accurate to the second from a traceable time source (e.g. RFC 5905 [31])
- IPv6 source address of the DS-Lite tunnel on RG (If a DS-Lite tunnel is used with the RG)

In some environments, it may be useful to pre-allocate some external TCP/UDP ports and ICMP identifiers on a NAT44 device for an individual subscriber. Doing so would save some cost when performing log tasks on the NAT44 device. The pre-allocation may be accomplished through configuration or other means.

R-86. A CG-NAT44 device SHOULD support pre-allocation of external UDP ports for individual subscribers.

The pre-allocated ports, along with the associated external IPv4 address assigned to that subscriber, are used for that particular subscriber during the NAT44 procedure for all UDP connections between that subscriber and hosts in the external realm.

R-87. A CG-NAT44 device SHOULD support pre-allocation of external TCP ports for individual subscribers.

The pre-allocated ports, along with the associated external IPv4 address assigned to that subscriber, are used for that particular subscriber during the NAT44 procedure for all TCP connections between that subscriber and hosts in the external realm.

R-88. A CG-NAT44 device SHOULD support pre-allocation of external ICMP identifiers for individual subscribers.

The pre-allocated identifiers, along with the associated external IPv4 address assigned to that subscriber, are used for that particular subscriber during NAT44 procedure for all ICMP message exchanges between that subscriber and hosts in the external realm.

An operator may want to support port forwarding behavior on a CG-NAT44 device, i.e. allow an IP flow originated from the external realm to be sent to a user behind the CG-NAT44 device

with a specific IPv4 address and port. This port forwarding behavior is useful for some applications such as webcam, P2P, etc.

R-89. A CG-NAT44 device SHOULD support port forwarding behavior that defines NAT44 mapping rule, i.e. how an external IPv4 address and an external port mapped to an internal IPv4 address and an internal port. Port forwarding behavior MAY be achieved by configuration or/and dynamic protocol(s) such as PCP (Port Control Protocol [43]).

By definition, the CG-NAT44 function that is introduced to the broadband network has high availability of carrier grade, and in particular, it must avoid single points of failure during its operation.

R-90. The CG-NAT44 network architecture MUST avoid single points of failure.

9.5 DS-Lite NAT44 Requirements

R-91. A node that implements the DS-Lite AFTR MUST implement both the tunnel termination and the NAT44.

Given the previous requirement, the DS-Lite AFTR is a CG-NAT44 device and in the following requirements it is also called DS-Lite CG-NAT44 device.

R-92. The entries of the NAT binding table of a DS-Lite CG-NAT44 device MUST include the IPv6 address of the DS-Lite tunnel endpoint in the RG (or any other identifier that points to that IPv6 address).

Typically, the entries are composed of at least the following items: {private address, private port, RG IPv6 address (or another identifier), public address, public port, protocol}. The DS-Lite CG-NAT44 device automatically acquires the IPv6 address of the DS-Lite tunnel endpoint in the RG upon receipt of the first incoming IPv6 datagram.

R-93. The DS-Lite CG-NAT44 device MUST provide a means so that the IPv6 address to be used to encapsulate IPv4 traffic into a DS-Lite tunnel is automatically recognized by the CGN.

In order to avoid flooding attacks, the following requirement is necessary:

R-94. The DS-Lite CG-NAT44 device MUST provide a means to limit the number of external ports (for IPv4 traffic) that can be used per IPv6 RG address.

The DS-Lite CG-NAT44 service should only be available to subscribers that are in the same administrative scope as the CG-NAT device (e.g. same Service Provider).

R-95. The DS-Lite CG-NAT44 device MUST support configurable IPv6 Access Control Lists in order to filter incoming IPv6 datagrams, based at least on the IPv6 prefix.

9.6 NAT444 Requirements

As the exhaustion of global public IPv4 addresses has become a reality, many network operators have already started to suffer from the shortage of global public IPv4 addresses, so NAT devices have already been deployed and private IPv4 addresses are used widely. The usage of private IPv4 addresses can only reduce the impact and urgency of the public IPv4 address shortage problem, and it creates many side effects and deployment issues.

However, private IPv4 addresses may be used to provide IPv4 access services. CGN (Carrier Grade NAT) can be deployed in the ISP's network so that public IPv4 address can be shared. As described in the IETF draft draft-shirasaki-nat444 [47], the NAT444 Model uses two Network Address and Port Translators (NAPTs) with three types of IPv4 address blocks.

The first NAPT is in the CPE (RG), and the second NAPT is in a CGN installed in the ISP's network.

The first IPv4 address block is a Private Address space inside the customer's network behind the RG. The second one is an IPv4 Private Address block between the RG and the CGN. The third one is the IPv4 Global Address space used to reach the Internet.

When a RG receives an IPv4 packet from the a host, it translates packet source address from the RG-scope private IPv4 address and transport identifier into a CGN-scope private IPv4 address and transport identifier, and then forwards it towards the CGN. The RG records the IPv4-IPv4 address and transport identifier mapping information and the translation log for inbound packets.

When a CGN receives the IPv4 packet from the RG, it translates the packet source address from a CGN-scope private IPv4 address and transport identifier into a public IPv4 address and transport identifier, and then sends it to the IPv4 Internet core. The CGN records the IPv4-IPv4 address and transport identifier mapping information and translation log for inbound packets.

The NAT444 CGN model is described as in Figure 11.

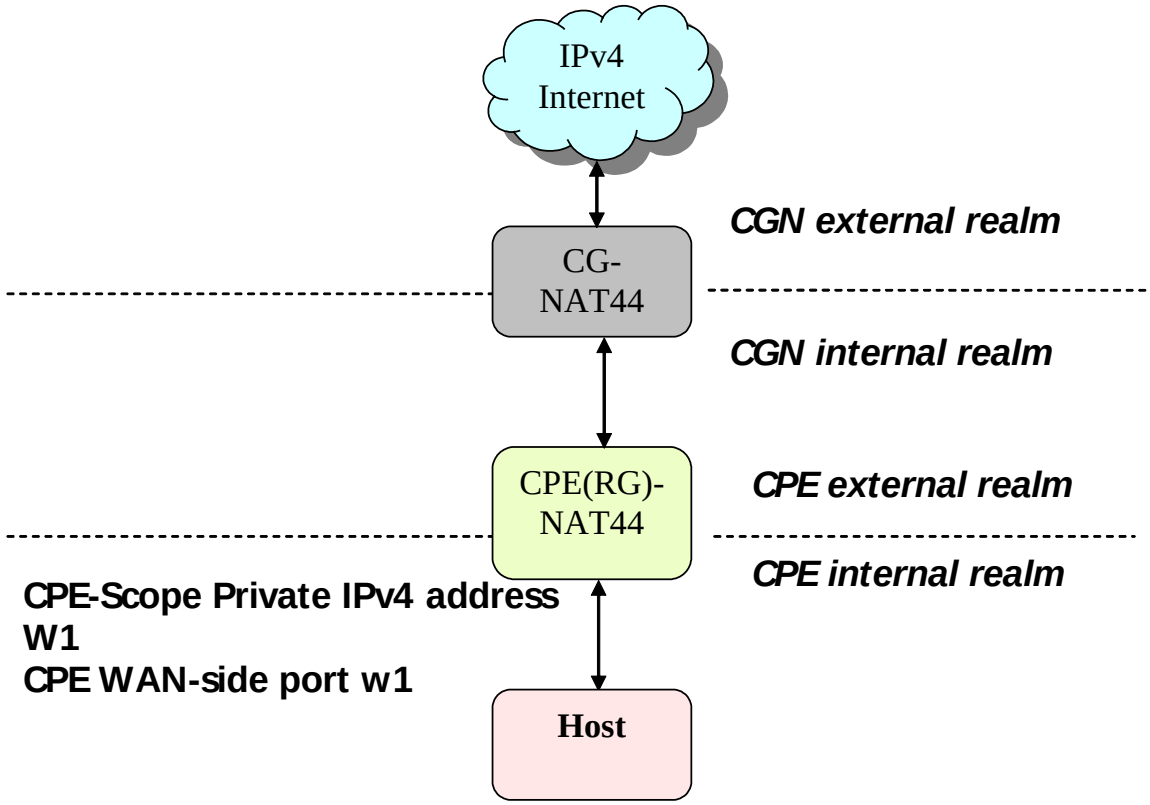

Figure 11 the NAT444 CGN Model

The requirements of CG-NAT44 described in Section 9.3 and Section 9.4 are also applicable to scenario NAT444.

R-96. The RG-NAT44 device MUST comply with the requirements in the LAN.ADDRESS, LAN.DHCPS, LAN.DNS, LAN.NAT, LAN.FWD sections of TR-124 [4].

9.7 Support of Port Control Protocol (PCP)

The Port Control Protocol (PCP) [43] developed at the IETF allows a device to control how incoming IPv6 or IPv4 packets are translated and forwarded by an external network address translator (NAT) or a firewall. PCP allows for the dynamic control of a CG-NAT44 by a PCP server (likely to be collocated with the CGN) so that some IP traffic that comes from the Internet can cross the CGN by means of an address-port mapping, as so-called port-forwarding capability.

There are three use cases of PCP deployment as follows:

1) UPnP IGD (Internet Gateway Device) and NAT-PMP (Port Mapping Protocol, draft-cheshire-nat-pmp-03 [41]) are used in the LAN: an Interworking function is required to be embedded in the RG to ensure interworking between the protocol used in the LAN and PCP.

2) Hosts behind and connected to the RG will either include a PCP client or an UPnP IGD client.

3) The RG includes a PCP client which is commonly invoked by an HTTP-based configuration).

R-97. The device implementing CGN function MUST support Port Control Protocol (PCP) Server behavior as specified in draft-ietf-pcp-base [43].

R-98. The RG MUST support Port Control Protocol (PCP) Client behavior as specified in draft draft-ietf-pcp-base [43].

R-99. The PCP server SHOULD deny the PCP client's request which carries the public IPv4 address and port already used or pre-allocated to other user.

10 Transition Mechanism Applicability

Figure 12 shows the applicability of different transition mechanisms. There are two dimensions that drive the use (and possibly sequence) of particular transition techniques:

- The type of IP services to be supported. This is shown on the vertical axis. Operators may decide to focus on maintaining IPv4 services, introducing IPv6 services or supporting a combination of both.

- The capability of the current access network. This is shown on the horizontal axis. Today most access networks are only able to natively support IPv4 traffic, but over time native IPv6 support will increase.

Depending on the operator strategy, parts of the network may or may not be dual stack enabled. The figure shows that depending on the type of service and the type of access network, there could be a need for tunneling IPv4 over IPv6 (6rd), dual stack, or tunneling IPv6 over IPv4 (DS-Lite).

In addition, there are several techniques that can be used to prolong the lifetime of IPv4 access networks. These include IPv4 Release Control and CGN. The figure shows that CGN can be used either as a standalone technique for IPv4 services, or in combination with the use of a dual stack network.

The figure shows the deployment phases for the different transition techniques. For instance, DS-Lite is not expected to be deployed in access networks that are IPv4 only. Likewise, 6rd is a transition technique for introducing IPv6 services within the existing IPv4 access network. 6rd is not expected to be used in native IPv6-only networks.

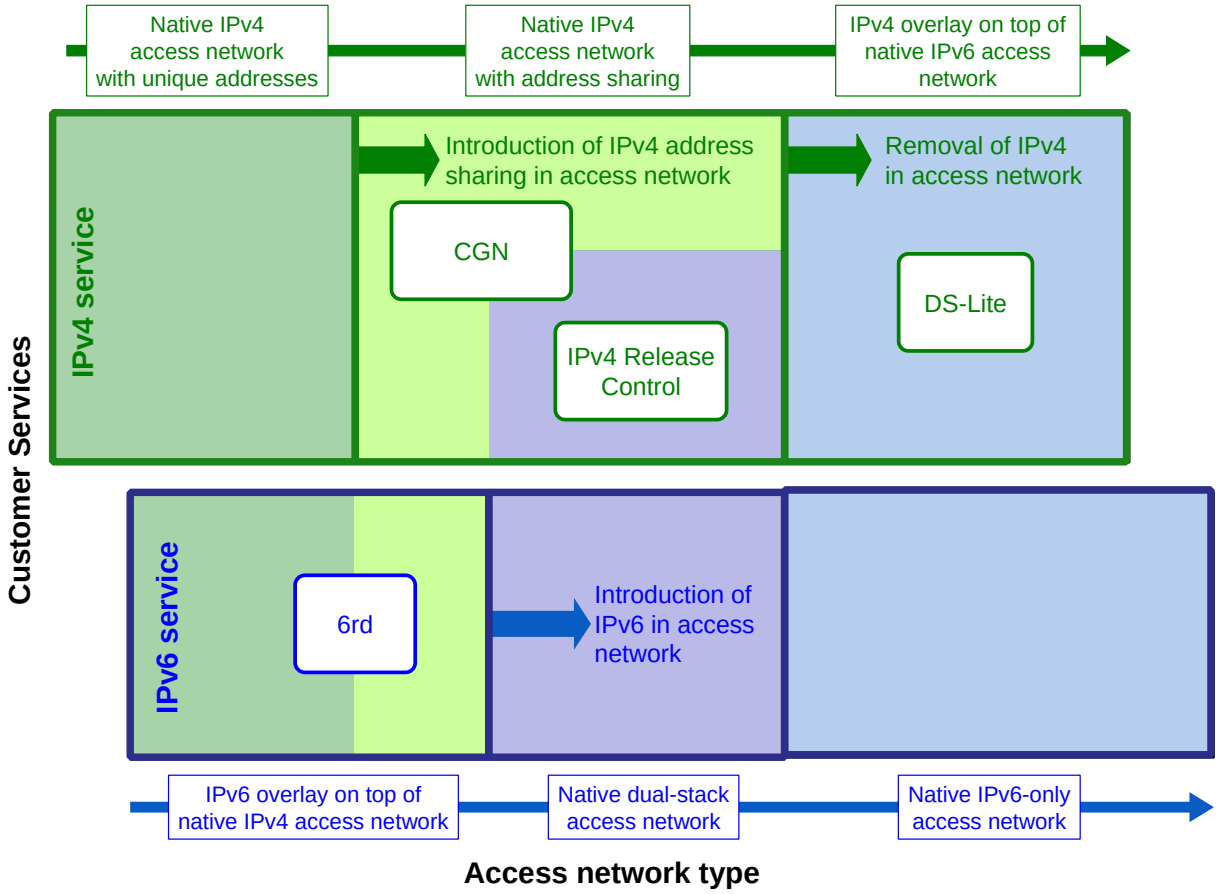

Figure 12 Applicability of Transition Mechanisms

Annex A: Network Attachment Tutorials

TR-101 provides an access architecture that has several different attachment procedures whereby the RG can attach to the access network and obtain an IPv4 address. The RG requirements are identified in TR-181 [8]. To provide dual stack services in the home, the RG must be able to access both IPv4 and IPv6 content.

A.1 6rd cases

In the case of 6rd, the RG first establishes IPv4 connectivity and then establishes IPv6 tunnels using 6rd. There are three options (manual configuration, DHCP configuration and TR-069 configuration) for configuration of 6rd parameters identified in Appendix VI/TR-181 [8]. The 6rd specific parameters include IPv4MaskLen, 6rdPrefix, 6rdPrefixLen, and 6rdBRIPv4Address.

A.1.1 Manual Configuration of 6rd parameters

A 6rd RG obtains its IPv4 address from the access network via IPCP or DHCP. The obtained IPv4 address is also used for the RG to establish the 6rd tunnel. In addition, the 6rd parameters have to be manually configured on the RG. Figure 13 below depicts this scenario.

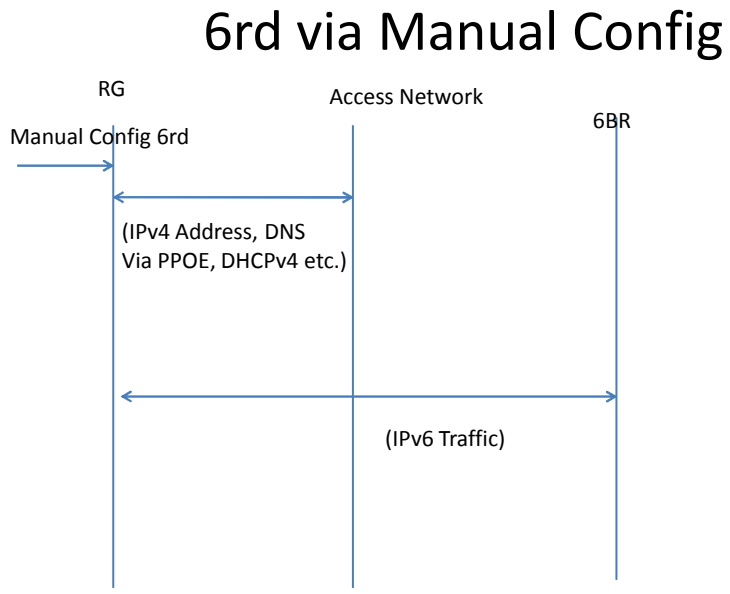

Figure 13 6rd via Manual Configuration

A.1.2 DHCP Configuration of 6rd parameters

In this case, the transactions exchanges with the DHCP server include the provisioning of the 6rd parameters along with the IPv4 address. When the RG obtains its IPv4 address via DHCPv4, the same configuration process can also be used to convey the 6rd configuration parameters. Prior to this configuration, the RG can forward IPv4 and IPv6 traffic on the LAN side only. After the completion of this configuration process, the RG can forward IPv6 traffic to the IPv6 Internet via the WAN side 6rd tunnels. Figure 14 below depicts this scenario.

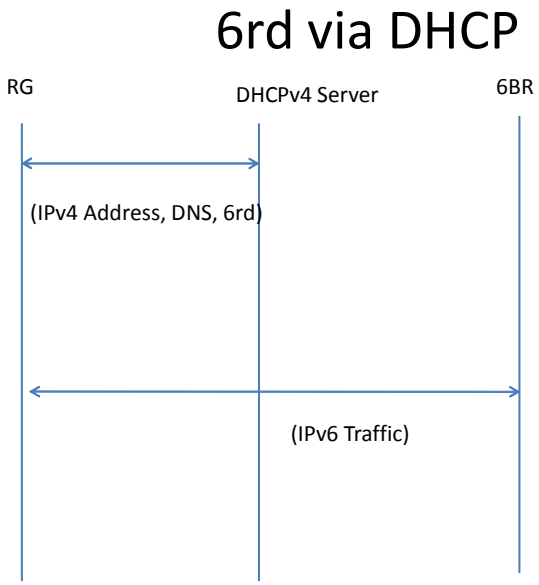

Figure 14 6rd via DHCP

A.1.3 TR-069 Configuration of 6rd parameters

In this case, once the RG is attached to the IPv4 network, the 6rd parameters are configured via TR-069 [2]. The RG is configured initially for IPv4 operation by means of standard mechanisms (e.g. manual, PPPoE, DHCPv4). At some point in time, the RG is then re-configured using TR-069 / TR-181 [8] to acquire the 6rd parameters. The RG can then establish the 6rd tunnels to establish IPv6 routing between the dual stack LAN side and the IPv6 Internet using the 6rd tunnels on the WAN side. Figure 15 below depicts this scenario.

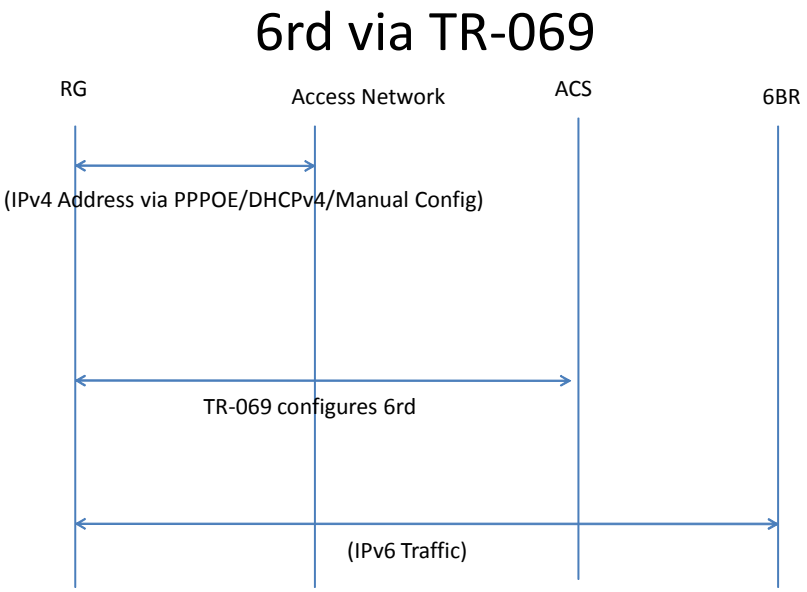

Figure 15 6rd via TR-069

A.2 DS-Lite cases

In the case of DS-Lite, the RG first establishes IPv6 connectivity and then establishes an IPv4 over IPv6 tunnel using the DS-Lite mechanism. There are several options (manual configuration, DHCPv6 standalone configuration, DHCPv6 with RADIUS configuration and TR-069 configuration) for configuring the DS-Lite specific parameters. The DS-Lite specific parameters include either the AFTR Tunnel end-point name, or the AFTR IPv6Tunnel end point address. The AFTR Tunnel end point address is not configurable via DHCPv6.

The following explain the different configuration options.

A.2.1 Manual Configuration of the DS-Lite parameters

A DS-Lite RG obtains its IPv6 prefix(es) and DNS server information from the access network via DHCPv6(-PD). In addition, a DS-Lite RG must obtain the IPv6 address of the AFTR in order to establish the IPv4-over-IPv6 tunnel and there are two ways to achieve this. The IPv6 address of the AFTR can be manually configured on the RG, or the name of the AFTR (FQDN) can be manually configured on the RG. In the latter case, the RG must acquire the IPv6 address of the AFTR via DNS.

Figure 16 below depicts a scenario where the DHCPv6 Server sits on the BNG is a Delegating Router (as per RFC 3633 [21]), a similar flow applies also for the case where the DHCPv6 server is an external device and the BNG supports a DHCPv6 Relay Agent capability.

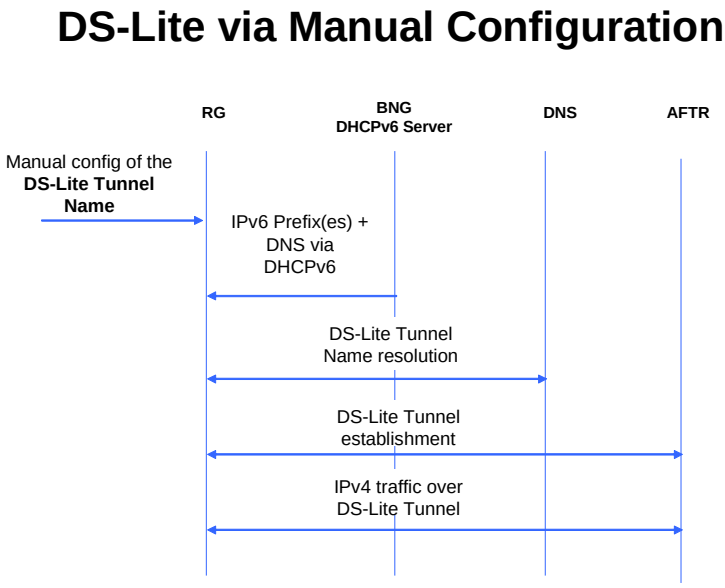

Figure 16 DS-Lite via Manual Configuration

A.2.2 DHCPv6 standalone configuration of DS-Lite parameters

In this case, the DHCPv6 Server provides the DS-Lite parameters (only the FQDN name is available via DHCPv6) along with the IPv6 prefix(es). Where the RG obtains its IPv6 prefix(es) via DHCPv6, the same configuration process can also be used to convey the DS-Lite Tunnel end-point name, by using the OPTION_AFTR_NAME DHCPv6 option specified in RFC 6334 [38]. In this scenario, the DHCPv6 Server needs to be provisioned with the DS-Lite Tunnel end-point name. After obtaining the IPv6 prefix(es) and configuring its own interfaces on the LAN side and optionally on the WAN side, the RG needs to resolve the Tunnel end-point name in order to get the IPv6 address of the AFTR. At this point, the RG can establish the DS-Lite IPv4-in-IPv6 tunnel on the WAN interface with the AFTR and then forward privately-addressed IPv4 traffic into this tunnel.

Figure 17 below depicts a scenario where the BNG is a DHCPv6 Server on the BNG, a similar flow applies also for the case where the DHCPv6 server is an external device and the BNG is acting as DHCPv6 Relay agent.

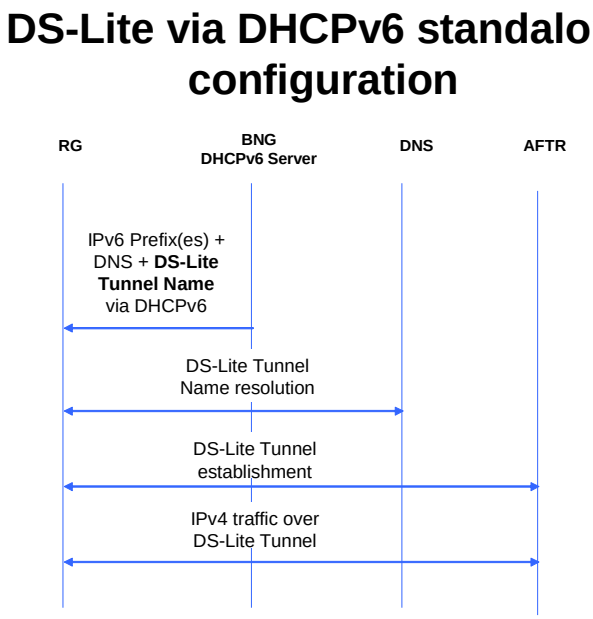

Figure 17 DS-Lite via DHCPv6 Standalone Configuration

A.2.3 DHCPv6 + RADIUS configuration of DS-Lite parameter

This scenario is similar to the previous case, but the DHCPv6 Server does not need to be provisioned with the DS-Lite Tunnel end-point name, because this parameter is configured into the RADIUS server and it is sent by RADIUS Server to the BNG. In this case, the DS-Lite Tunnel end-point name is configured in the customer's profile stored into the RADIUS Server, by using the DS-Lite-Tunnel-Name RADIUS attribute specified in RFC6519 [40]. The RADIUS Server sends the DS-Lite Tunnel end-point name in the Access-Accept message, then the BNG retrieves the DS-Lite-Tunnel-Name from the RADIUS attribute and it inserts it into the DHCPv6 OPTION_DS_LITE_NAME option to be sent to the RG. Next steps are the same as described before. Figure 18 below depicts this scenario.

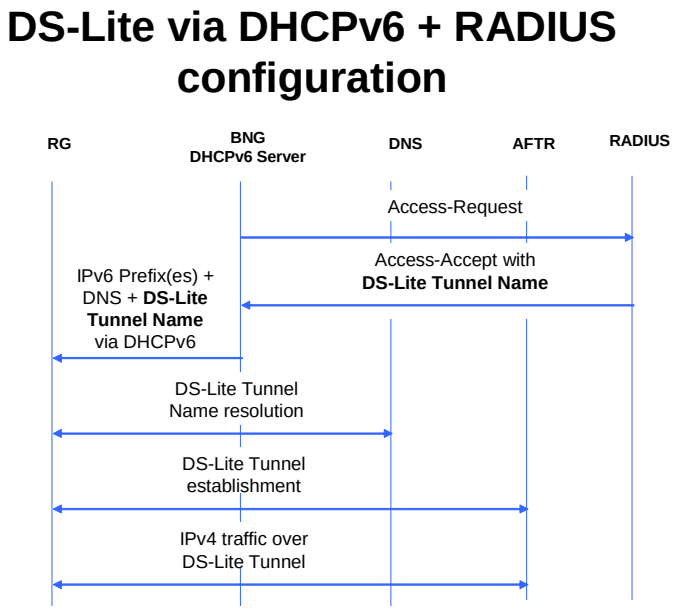

Figure 18 DS-Lite via DHCPv6 + RADIUS Configuration

A.2.4 TR-069 Configuration of DS-Lite parameters

In this case, once the RG is attached to the IPv6 network and the DS-Lite parameter (either the name or the address) is configured via TR-069. The RG gets its IPv6 prefix (es) and DNS via DHCPv6 (-PD) from the access network. After obtaining the IPv6 prefix (es) and configuring its own interfaces on the LAN side and optionally on the WAN side, the RG needs to resolve the Tunnel end-point name in order to get the IPv6 address of the AFTR. At this point, the RG can establish the DS-Lite IPv4-in-IPv6 tunnel on the WAN interface with the AFTR and then forward privately-addressed IPv4 traffic into this tunnel.

Figure 19 below depicts a scenario where the BNG is a Delegating Router (as per RFC 3633 [21]), a similar flow applies also for the case where the DHCPv6 server is an external device and the BNG supports a DHCPv6 Relay Agent capability.

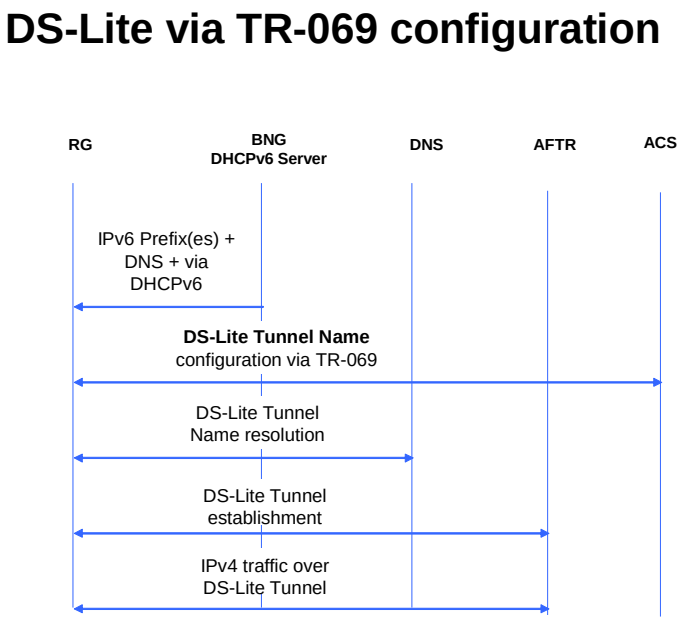

Figure 19 DS-Lite via TR-069 Configuration

End of Broadband Forum Technical Report TR-242