Technical Report

TR-296
IPv6 Transition Mechanisms Test Plan

Issue:1
Issue Date: November 2013

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 Report 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 Editor	Changes
1	11 November 2013	13 December 2013	Dean Cheng, Huawei Daisy Sun, IXIA	Original

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

Editors	Dean Cheng	Huawei
	Daisy Sun	IXIA
E2EArchitecture WG Chairs	David Allan	Ericsson
	David Thorne	BT
Vice Chair	Sven Ooghe	Alcatel-Lucent

Table of Contents

EXECUTIVE SUMMARY **7**

1 PURPOSE AND SCOPE **8**

1.1 PURPOSE 8
1.2 SCOPE 8

2 REFERENCES AND TERMINOLOGY **10**

2.1 CONVENTIONS 10
2.2 REFERENCES 10
2.3 DEFINITIONS 12
2.4 ABBREVIATIONS 13

3 TECHNICAL REPORT IMPACT **14**

3.1 ENERGY EFFICIENCY 14
3.2 IPV6 14
3.3 SECURITY 14
3.4 PRIVACY 14

4 TEST CASES FOR 6RD **15**

4.1 DEVICES UNDER TEST 15
4.2 TEST EQUIPMENT 15
4.3 TEST SETUP 15
4.4 TEST TOPOLOGY 16
4.5 TEST CASES 17
4.5.1 Basic 6rd Encapsulation *17*
4.5.2 Prefix Lifetime *18*
4.5.3 Prefix Length of /64 ..... *19*
4.5.4 Prefix Length shorter than /64 ..... *20*
4.5.5 Mapping of "Type of Service" and "Traffic Class" *21*
4.5.6 Configure 6rd Parameters on RG Manually *23*
4.5.7 Configure 6rd Parameters on RG via DHCP *24*
4.5.8 Configure 6rd Parameters on RG via TR-069 ..... *25*
4.5.9 Forwarding over Native IPv6 vs. 6rd with Same IPv6 Prefix *26*
4.5.10 Forwarding over Native IPv6 vs. 6rd with Different IPv6 Prefix *27*
4.5.11 Hub and Spoke Mode *28*
4.5.12 User-to-User Direct Communication *29*
4.5.13 Maximum Transmission Unit (MTU) *30*
4.5.14 Persistent 6rd Delegated IPv6 Prefix *31*
4.5.15 Lost Service *32*
4.5.16 6rd Prefix Change *33*

5 TEST CASES FOR DS-LITE **36**

5.1 DEVICE UNDER TEST 36
5.2 TEST EQUIPMENT 36

5.3 TEST SETUP 36
5.4 TEST TOPOLOGY 37
5.5 TEST CASES 38
5.5.1 Configure FQDN of AFTR Element on RG via DHCPv6 38
5.5.2 Configure FQDN of the AFTR Element on RG manually 40
5.5.3 Configure FQDN of the AFTR Element on RG via TR-069 41
5.5.4 IPv4-in-IPv6 Tunnel Encapsulation 42
5.5.5 Deactivate NAPT Function on RG 44
5.5.6 Configuring a default IPv4 Route at RG for DS-Lite Tunnel 45
5.5.7 Extended NAT Table on DS-Lite AFTR 46
5.5.8 Mapping between IPv4 TOS field and IPv6 TC field 47
5.5.9 DNS Proxy function for RG 49
5.5.10 PCP server function on DS-Lite AFTR 50
5.5.11 IPv6 Datagram Filter Function for DS-Lite CG-NAT44 53
5.5.12 DS-Lite port Limit function of DS-Lite CG-NAT44 55
5.5.13 AFTR with 40-byte MTU Increment on B4 Facing Interfaces 57
5.5.14 Packet Fragmentation and Reassembly at B4 and AFTR device 58
5.5.15 Rewriting the TCP MSS option of TCP packets by B4 and AFTR 60
5.5.16 PCP - Learning Public IPv4 address of the DS-Lite AFTR 62
5.5.17 PCP - Request an Already Used Port 63

6 TEST CASES FOR RELEASE CONTROL 66

6.1 DEVICE UNDER TEST 66
6.2 TEST EQUIPMENT 66
6.3 TEST SETUP 66
6.4 TEST TOPOLOGY 67
6.5 TEST CASES 68
6.5.1 DSL RG (Residential Gateway) with Release Control Functionality 69
6.5.2 DSL IPv4-only RG 70
6.5.3 RG with Dual-Stack PPP functionality but without Release Control 71
6.5.4 Compatibility with IPv6-only RG 73

7 TEST CASES FOR DUAL-STACK WITH CGN NAT44 74

7.1 DEVICE UNDER TEST 74
7.2 TEST EQUIPMENT 74
7.3 TEST SETUP 74
7.4 TEST TOPOLOGY 75
7.5 TEST CASES 76
7.5.1 Dual-Stack model with shared service provider IPv4 address Function 76

8 TEST CASES FOR CGN (NAT44) 79

8.1 DEVICE UNDER TEST 79
8.2 REQUIRED TEST EQUIPMENT 79
8.3 TEST SETUP 79
8.4 TEST TOPOLOGY 80
8.5 TEST CASES 81
8.5.1 CG-NAT44 Network Address Port Translation Function 81

8.5.2 CG-NAT44 Full cone NAT mode of address translation 83
8.5.3 CG-NAT44 High Availability 84
8.5.4 PCP Server Function Support on CG-NAT44 86
8.5.5 Paired IP Address Pooling Behavior of CG-NAT44 88
8.5.6 TCP port in Bulk Port Allocation mode 90
8.5.7 UDP port in Bulk Port Allocation mode 93
8.5.8 PCP - Learning Public IP address of the CGN 95
8.5.9 PCP - Request an Already Used Port 96
8.5.10 The function of NAT ALG for TCP protocol for CG-NAT44 98
8.5.11 The function of NAT ALG for ICMP protocol for CG-NAT44 99
8.5.12 Pre-allocation of external ICMP identifiers for individual subscribers 100

List of Figures

Figure 1 6rd Test Topology 16
Figure 2 DS-Lite Test Topology 37
Figure 3 Release Control Test Topology 67
Figure 4 PPP States as defined in RFC 1661 68
Figure 5 Dual-stack BNG and CG-NAT44 Test Topology 75
Figure 6 Device and Functions Used in CG-NAT44 Test 80

List of Tables

Table 1 Device and Functions Used in 6rd Test 16
Table 2 Device and Functions Used in DS-Lite Test 37
Table 3 Device and Functions Used in Release Control Test 67
Table 4 Device and Functions Used in Dual-Stack BNG with CGN Test 75
Table 5 Device and Functions Used in CG-NAT44 Test 80

Executive Summary

TR-296 specifies a suite of test cases for verifying the interoperability of the network devices that implement the IPv6 transition mechanisms defined in TR-242; all the transition mechanisms in TR-242 are covered.

The targeted network devices include RG, 6rd BR, DS-Lite AFTR, dual-stack BNG, CGN. The test cases are organized in groups, with each group corresponding to a specific IPv6 transition mechanism defined in TR-242. A generic test topology along with test equipment is defined for each test group. The test methodology including configuration, test procedure and expected results are specified for each test case.

1 Purpose and Scope

1.1 Purpose

The Broadband Forum has defined several IPv6 transition mechanisms for use in conjunction with IPv4 address sharing mechanisms to facilitate the transition from IPv4 to IPv6. This is based on standards developed at IETF along with inputs from carriers for deployment requirements as documented in TR-242. One or more of these mechanisms may be considered by carriers to offer IPv6 service during their transition from existing IPv4-only architecture to IPv4-IPv6 dual stack architecture as described in TR-177 and TR-187 respectively, as an extension to TR-101 based broadband network architecture.

To implement these transition mechanisms, functional enhancement is required on the RG and BNG. Furthermore, some transition mechanisms require additional devices and/or network services in the existing broadband networks. This, together with the variety of IPv6 transition mechanisms, makes it highly desirable to perform interoperability tests on the devices required for any specific transition mechanism before the actual rollout is performed.

The purpose of interoperability testing is to verify that the set of devices required for a given transition mechanism support the required transition features and that the devices can communicate with each other accordingly. TR-296 documents separate test series for each IPv6 transition mechanism that is defined in TR-242. Each series of tests has separate test equipment, configuration, test setup, topology, methodology, procedure and criteria for evaluating test result (pass or fail).

Test cases defined in TR-296 are intended for use by carriers, vendors and testing institutes.

1.2 Scope

The scope of TR-296 is to define a series of test cases that can be used to verify the interoperability of network equipment that implement IPv6 transition mechanisms as defined in TR-242 [6].

The scope of the devices that will be tested is as follows:

- Network devices that implement any of the mechanisms defined in TR-242, including standalone BNG, BNG with additional embedded functions, such as 6rd BR, DS-Lite AFTR, CGN, etc.

- RG that implements any of the mechanisms defined in TR-242.
- Any other new devices that implement any of the mechanisms defined in TR-242, such as a standalone node acting as 6rd BR (Border Relay) or a standalone node acting as DS-Lite AFTR (Address Family Transit Router) tunnel terminators.

The scope of the IPv6 transition implementations that will be tested is as follows:

- 6rd
- DS-Lite

- Release control
- Dual-Stack architecture with CG-NAT44 implemented on the BNG
- CG-NAT44

The following are out of scope of TR-296:

- Conformance testing for IPv6 transition mechanisms
- Any other devices that do not require additional features defined in TR-242, e.g. Access nodes and Ethernet aggregation switches
- Access node specific IPv6 testing in accordance to TR-177 [4] – these tests are defined in TR-254 [7].
- IPv4-IPv6 dual-stack capability of BNG
- IPv6 functions defined in TR-124 [3] other than those referenced by 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 [11].

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]	TR-069 Amendment 4	*CPE WAN Management Protocol*	BBF	2011
[2]	TR-101 Issue 2	*Migration to Ethernet-Based Broadband Aggregation*	BBF	2011
[3]	TR-124	*Functional Requirements for Broadband*	BBF	2012

	Issue 3	*Residential Gateways*		
[4]	TR-177	*Migration to IPv6 in the Context of TR-101*	BBF	2010
[5]	TR-187	*IPv6 for PPP Broadband Access*	BBF	2010
[6]	TR-242	*IPv6 Transition Mechanisms for Broadband Networks*	BBF	2012
[7]	TR-254	*Functionality Tests for Ethernet Based Access Nodes*	BBF	2012
[8]	RFC 1332	*The PPP Internet Protocol Control Protocol (IPCP)*	IETF	1992
[9]	RFC 1661	*The Point-to-Point Protocol (PPP)*	IETF	1994
[10]	RFC 1918	*Address Allocation for Private Internets*	IETF	1996
[11]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[12]	RFC 2473	*Generic Packet Tunneling in IPv6 Specification*	IETF	1998
[13]	RFC 2663	*IP Network Address Translator (NAT) Terminology and Considerations*	IETF	1999
[14]	RFC 2983	*Differentiated Services and Tunnels*	IETF	2000
[15]	RFC 4213	*Basic Transition Mechanisms for IPv6 Hosts and Routers*	IETF	2005
[16]	RFC 4241	*A Model of IPv6/IPv4 Dual Stack Internet Access Service*	IETF	2005
[17]	RFC 4443	*Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*	IETF	2006
[18]	RFC 4787	*Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*	IETF	2007
[19]	RFC 5382	*NAT Behavioral Requirements for TCP*	IETF	2008
[20]	RFC 5508	*NAT Behavioral Requirements for ICMP*	IETF	2009
[21]	RFC 5597	*Network Address Translation (NAT) Behavioral Requirements for the Datagram Congestion Control Protocol*	IETF	2009
[22]	RFC 5625	*DNS Proxy Implementation Guidelines*	IETF	2009
[23]	RFC 5969	*IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)*	IETF	2010
[24]	RFC 6333	*Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*	IETF	2011
[25]	RFC 6334	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Options for Dual-Stack Lite*	IETF	2011

[26]	RFC 6519	*RADIUS Extensions for Dual-Stack Lite*	IETF	2012
[27]	RFC 6887	*Port Control Protocol (PCP)*	IETF	2013
[28]	RFC 6930	*RADIUS Attribute for IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)*	IETF	2013

2.3 Definitions

The following terminology is used throughout this Technical Report.

6rd (IPv6 Rapid Deployment)	An IPv6 transition technology defined in RFC5969 [23].
6rd BR	6rd Border Relay
ACS	Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.
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.
DS-Lite (Dual-Stack Lite)	An IPv6 transition technology defined in RFC6333 [24].
Dual Stack	A network element that supports both IPv4 and IPv6 natively.
Inbound	Data traffic direction from broadband network to its subscribers.
Outbound	Data traffic direction from subscribers to broadband network.
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 [10].
Public IPv4 Address	An IPv4 address that is globally unambiguous per RFC 1918.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

ACS	Automatic Configuration Server
AFTR	Address Family Translation Router
B4	The Basic Bridging Broadband element
BBF	Broadband Forum
BNG	Broadband Network Gateway
BR	Border Router or Border Relay
CGN	Carrier Grade NAT
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DSL	Digital subscriber line
DS-Lite	Dual-Stack Lite
EMF	Equipment management Function
HTTP	Hyper Text Transfer protocol
IPCP	Internet Protocol Control Protocol
LAN	Local Area Network
NAPT	Network Address Port Translation
NAT	Network Address Translation
PCP	Port Control Protocol
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
RG	Residential Gateway
TR	Technical Report
WG	Working Group
WT	Working Text

3 Technical Report Impact

3.1 Energy Efficiency

TR-296 has no impact on Energy Efficiency.

3.2 IPv6

TR-296 specifies a suite of interoperability test cases for network devices that implement IPv6 transition mechanisms defined in TR-242 and also TR-124 for RG specific requirements. In addition, test cases that involve IPv4-IPv6 dual stack also conform to requirements defined in TR-187 and TR-177, for IPv6 over PPP and IPv6 over Ethernet, respectively. The technologies behind all IPv6 transition test cases in TR-296 are based on IETF RFCs.

3.3 Security

For Security requirements on devices under the tests, refer to TR-242, and otherwise, TR-296 does not introduce direct impact on Security.

3.4 Privacy

TR-296 has no impact on Privacy.

4 Test Cases for 6rd

4.1 Devices Under Test

- Two RG (Residential Gateway) with 6rd functionality
- One 6rd BR (Border Relay) device

4.2 Test Equipment

For 6rd interoperability test, the required test equipment is as follows:

- Three IPv6 hosts supporting the IPv6 stack, including handling of ICMPv6, DHCPv6, HTTP and DNS requests over IPv6.
- Four IPv4 hosts supporting the IPv4 stack, including handling of ICMP, DHCP, HTTP and DNS requests over IPv4.
  Note: all IPv4 and IPv6 hosts could be simulated using a Traffic Generator platform that is connected to the 6rd_RG nodes and the 6rd-BR node, respectively. An IPv4-IPv6 dual-stack host may also be used.
- Two IPv4 routers with one capable of providing server functions including DHCP, RADIUS and DNS.
- DNS Server
- RADIUS Server that supports 6rd extensions defined in RFC6930 [28]
- DHCP Server that supports 6rd options defined in RFC5969 [23].
- One TR-069 server (ACS)
- Traffic generator capable of generating IPv4 and IPv6 traffic.
- Protocol analyzer capable of interpreting this list of traffic types
  - IPv4 packets
  - IPv6 packets
  - IPv6-in-IPv4 packets per RFC4213 [15]

4.3 Test Setup

This section describes the requirements of 6rd RG and 6rd BR including their interfaces, configuration, etc. for the test cases. It also describes the associated network services provided by DNS server, RADIUS server, and DHCP server that are required in the test. Finally, it describes the functions of traffic generator and protocol analyzer that are used for the test.

For 6rd interoperability test, two simulated home networks (Network-1 and Network-2 in Figure 1) are needed that support both IPv4 and IPv6, and at each site, there is a 6rd-RG device that is running in the router mode for IPv4 but also capable of receiving and transmitting IPv6 packets that are encapsulated with IPv4 header. The reason for having two simulated home networks is to test customer-to-customer communication.

The 6rd-BR device must have interface facing 6rd-RG devices over IPv4-only access network (Network-3 in Figure 1), and is capable of transporting IPv6-in-IPv4 packets with 6rd-RG device. In addition, it connects to both IPv6-only network (Network-4 in Figure 1) and IPv4-only network (Network-5 in Figure 1) that serve as source and destination of test traffic, respectively.

This test also requires some network service functions such as DHCPv4 server function, RADIUS server function, and DNS server function.

4.4 Test Topology

Figure 1 is the 6rd test topology for all 6rd test cases; note that depending on each test case, test equipment are connected and configured as needed. The connectivity as illustrated between the devices in the figure is at IP layer.

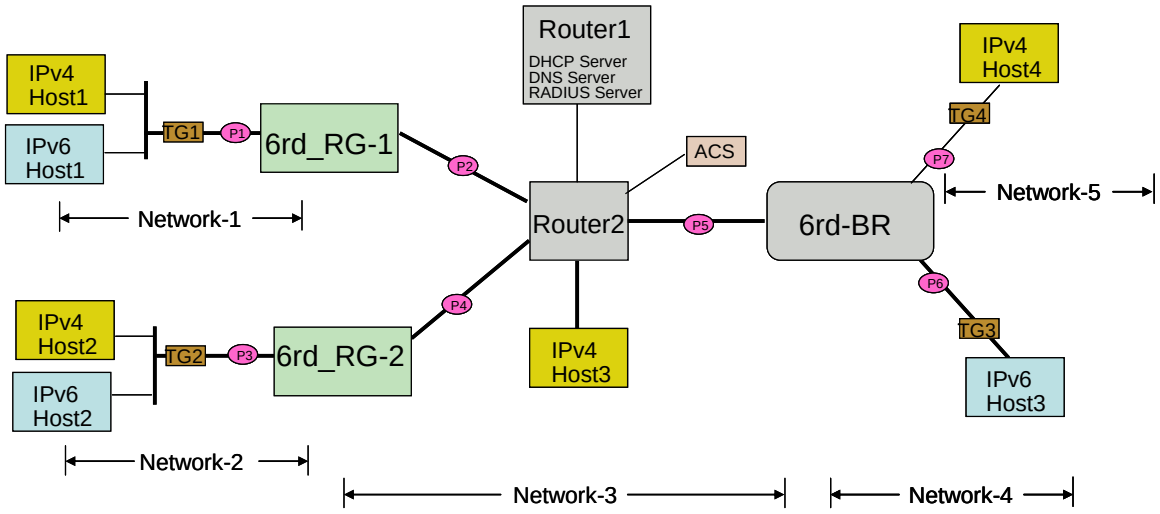

Figure 1 6rd Test Topology

Table 1 Device and Functions Used in 6rd Test

Devices/Functions	Descriptions
6rd_RG_1 6rd_RG_2	The RG supports 6rd functions. At least two units are required in order to allow testing of customer-to-customer traffic.
6rd_BR	The 6rd BR performs the 6rd BR function. It may be located on a BNG or on a separate platform.
Router1	This is an IPv4 router that provides DHCP server function, DNS server function and RADIUS server function. Note alternatively, one or more of these server functions can be realized by other devices including traffic generators.

Router2	This is an IPv4 router that provides IP connectivity between IP devices.
ACS	Automatic Configuration Server that provides TR-069 server function.
IPv4-Host1, IPv4-Host2, IPv4-Host3, IPv4-Host4	These are IPv4 hosts, which are used to test IPv4 communication among the hosts.
IPv6-Host1, IPv6-Host2, IPv6-Host3	These are IPv6 hosts which are used to test IPv6 communication among the hosts and with the traffic generators.
TG1/TG2/TG3/TG4	These are insertion points where traffic generator may be connected in-wire. If connected, traffic generators provide IPv6 traffic source and destination and communicate with IPv6 hosts.
Probe points (p1 to p7)	The probe points may be inserted in different points of the test network in order to verify and monitor the IP packets.
Network-1, Network-2	These are IPv4-IPv6 dual-stack networks.
Network-3	This is IPv4-only network by default. Whenever a test case requires IPv6 support, this will be stated explicitly.
Network-4	This is IPv6-only network.
Network-5	This is IPv4-only network.

4.5 Test Cases

This section lists all test cases for 6rd. Note that the 6rd test cases are organized according to 6rd requirements defined in Section 5/TR-242 [6].

4.5.1 Basic 6rd Encapsulation

4.5.1	Test Basic 6rd Encapsulation
Test Objective	Verify a 6rd Residential Gateway obtains 6rd information and encapsulates and decapsulates packets.
Requirement	TR-242: R-7, R-23, R-24
Requirement Description	TR-242: R-7: IPv6 ICMP (RFC 4443 [17]) MUST be supported in 6rd-enabled broadband networks. R-23: The RG MUST support 6rd CE (RG) functions per RFC 5969 [23]. R-24: A RG that is configured to perform 6rd CE function per RFC5969 MUST comply with requirements defined in TRANS 6rd section of TR-124 [3].
Device Under Test	6RD_RG-1 in Figure 1

Test Configuration	**Test Setup –**Figure 1 **Test Conditions:** 1) Router1 is configured to assign 6rd elements via DHCPv4 or ACS is configured to assign 6rd elements via TR-069. 2) 6RD-BR is configured with 6rd elements. 3) 6RD_RG-1 has 6rd mechanism enabled and is configured with 6rd elements via DHCPv4, TR-069, or manually.
Test Procedure	1) Enable 6RD_RG-1. 2) Capture packets at probe p2. 3) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3.
Expected Result	1) At step 1, 6RD_RG-1 obtains 6rd information through TR-069 or DHCPv4. 2) At step 3, 6RD_RG-1 encapsulates the ICMPv6 Echo Requests in the IPv4 packet with the following values: 2a) Outer IPv4 header source address is 6RD_RG-1 IPv4 address on Network-3 2b) Outer IPv4 header destination address is 6RD_BR IPv4 address on Network-3 2c) Inner IPv6 header source address is IPv6-Host1 address configured from 6rd delegated prefix 2d) Inner IPv6 header destination address is IPv6-Host3 address 3) At step 3, IPv6-Host1 receives ICMPv6 Echo Replies to all ICMPv6 Echo Requests that have been transmitted to IPv6-Host3.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.2 Prefix Lifetime

4.5.2	Verify Prefix Lifetime
Test Objective	Verify a 6rd Residential Gateway assigns lifetimes from 6rd prefix delegation to LAN interfaces.
Requirement	RFC 5969 – Section 4 TR-242: R-23
Requirement Description	RFC 5969 [23] – Section 4: The prefix lifetimes advertised in Router Advertisements or used by DHCP on the CE LAN side MUST be equal to or shorter than the IPv4 address lease time.

	TR-242: R-23: The RG MUST support 6rd CE (RG) functions per RFC 5969.
Device Under Test	6RD_RG-1 in Figure 1
Test Configuration	**Test Setup –** Figure 1 **Test Conditions:** 1) Router1 is configured to assign 6rd elements via DHCPv4 or ACS is configured to assign 6rd elements via TR-069. 2) 6RD-BR is configured with 6rd elements. 3) DHCPv4 server is configured with a lease time of 1 hour for all IPv4 addresses. 4) 6RD_RG-1 has 6rd mechanism enabled and is configured with 6rd elements via DHCPv4, TR-069, or manually.
Test Procedure	1) Capture packets at probe p1 2) Enable 6RD_RG-1 3) Wait for 6RD_RG-1 to obtain 6rd elements
Expected Result	At the step 3, 6RD_RG-1 transmits an IPv6 Router Advertisement with a valid Prefix Information Option that has a valid lifetime equal to or less than 1 hour.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.3 Prefix Length of /64

4.5.3	Verify 6rd delegated prefix length of /64
Test Objective	Verify a 6rd Residential Gateway assigns 6rd delegated prefixes with prefix length of 64
Requirement	RFC 5969 [23] – Section 4 TR-242: R-28
Requirement Description	RFC 5969 – Section 4: The 6rd delegated prefix is created by concatenating the 6rd prefix and a consecutive set of bits from the CE IPv4 address in order. The length of the 6rd delegated prefix is equal to length of the 6rd prefix (n) plus the number of bits from the CE IPv4 address (o). TR-242: 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.
Device Under Test	6RD_RG-1 in Figure 1
Test Configuration	**Test Setup –** Figure 1 **Test Conditions:** 1) Router1 is configured to assign the 6rd elements via DHCPv4 or ACS is configured to assign the 6rd elements via TR-069 as follows: - 6rd prefix 2001:db8::/48 - IPv4MaskLen 16 2) 6RD_RG-1 is configured with an IPv4 address of 10.100.100.1 3) 6RD-BR is configured with 6rd elements. 4) 6RD_RG-1 has 6rd mechanism enabled and is configured with 6rd elements via DHCPv4, TR-069, or manually.
Test Procedure	1) Capture packets at probe p1 2) Enable 6RD_RG-1 3) Wait for 6RD_RG-1 to obtain 6rd elements 4) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3.
Expected Result	1) At the step 3, the 6RD_RG-1 transmits IPv6 Router Advertisements with a Prefix Information Option containing a prefix of 2001:db8:0:6401::/64. 2) At the step 4, IPv6-Host1 receives ICMPv6 Echo Replies to all the ICMPv6 Echo Requests that have been transmitted to IPv6-Host3.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.4 Prefix Length shorter than /64

4.5.4	Verify 6rd delegated prefix length of /56
Test Objective	Verify a 6rd Residential Gateway assigns 6rd delegated prefixes with prefix length less than /64
Requirement	RFC 5969 [23] – Section 4 TR-242: R-28
Requirement Description	RFC 5969 – Section 4: The 6rd delegated prefix is created by concatenating the 6rd prefix and a consecutive set of bits from the CE IPv4 address in order. The length of the 6rd delegated prefix is equal to length of the 6rd prefix (n) plus the number of bits from the CE IPv4 address (o).

	TR-242: 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.
Device Under Test	6RD_RG-1 in Figure 1
Test Configuration	**Test Setup –** Figure 1 **Test Conditions:** 1) Router1 is configured to assign the 6rd elements via DHCPv4 or ACS is configured to assign the 6rd elements via TR-069 as follows: 6rd prefix 2001:db8::/32 IPv4MaskLen 8 2) 6RD_RG-1 is configured with an IPv4 address of 10.100.100.1 3) 6RD-BR is configured with 6rd elements. 4) 6RD_RG-1 has 6rd mechanism enabled and is configured with 6rd elements via DHCPv4, TR-069, or manually.
Test Procedure	1) Capture packets at probe p1 2) Enable 6RD_RG-1 3) Wait for 6RD_RG-1 to obtain 6rd elements 4) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3.
Expected Result	1) At the step 3, the 6RD_RG-1 transmits IPv6 Router Advertisements with a Prefix Information Option containing a prefix in the 2001:db8:6464:100::/56 range. 2) At the step 4, IPv6-Host1 must receive ICMPv6 Echo Replies to all the ICMPv6 Echo Requests that have been transmitted to IPv6-Host3.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.5 Mapping of "Type of Service" and "Traffic Class"

4.5.5	Mapping the value of IPv6's "Traffic Class" field and IPv4's "Type of Service" field.
Test objective	The aim of this test is to check the value of "Traffic Class" field of an IPv6 packet is copied correctly to the "Type of Service" field of an IPv4 packet on a 6rd RG for outbound traffic and on a 6rd BR for inbound traffic, respectively, and vice versa on a 6rd RG for inbound traffic, and on a 6rd BR

	for outbound traffic, respectively.
Requirement	1) RFC5969 [23]: Section 9 2) TR-242:R-33, R-22, R32
Requirement description	Details of IPv6-in-IPv4 encapsulation requirements are referred to Section 9/RFC5969. In addition the following requirements are defined in TR-242: 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 [14]. 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. R-33: The RG MUST be able to configured to send all 6rd traffic to the BR.
Device under test	6rd RG and 6rd BR device referred to Figure 1
Test configuration	**Test Setup –** Figure 1 **Pre-conditions:** 1) 6rd_RG-1 and 6rd_RG-2 are configured in router mode. 2) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv6 address for Network-4 and IPv4 address for Network-3 are configured on 6rd-BR. 2) IPv4 address pool is configured on the DHCP server. 3) 6rd parameters are configured on 6rd_RG1 and 6rd_RG2 manually, or via DHCP, or by TR-069. 4) 6rd function is enabled on 6rd_RG-1, 6rd_RG-2 and 6rd-BR respectively, including the function that maps the value of "traffic class" field in IPv6 packet and "type of service" field in IPv4 packet in both directions. 5) IPv4-Host3 and IPv6-Host3 are configured as FTP or HTTP server respectively.
Test procedure	1) 6rd_RG-1 and 6rd_RG-2 start IPv4 connection. 2) Check via EMF that the IPv6 operation (addressing, communication between IPv6 hosts and also with the RG, etc.) in Network-1 ad Network-2, respectively, is performed correctly.

	3) IPv4-Host1 and IPv4-Host2 try to get access to the FTP or HTTP service in IPv4-Host3. 4) IPv6-Host1 and IPv6-Host2 try to access the FTP or HTTP service in IPv6-Host3. 5) Capture and analyze the packets via the probes p1, p2, p3, p4, p5, and p6.
Expected result	1) At step 1 and 2, the IP connection is established successfully. 2) At step 3, IPv4-Host1 and IPv4-Host2 get access to the IPv4 FTP or HTTP service successfully. 3) At step 4, IPv6-Host1 and IPv6-Host2 get access to IPv6 FTP or HTTP service successfully. 4) At step 5: a) In the packets captured by the probes p2/p4 outbound direction, all the original IPv6 packets are now in IPv6-in-IPv4 tunnel encapsulation format. Verify that the IPv4 header "Type of Service" field has the same value as IPv6 header "Traffic Class" in original IPv6 packet captured at probes p1/p3 outbound direction, respectively. b) In the packets captured by the probes p1/p3 inbound direction, there should be only native IPv6 packet format. Verify that the IPv6 header "Traffic Class" has the same value as IPv4 header "Type of Service" field in IPv6-in-IPv4 packet captured at probes p2/p4 inbound direction, respectively. c) In the packets captured by probe p5 inbound direction, all original IPv6 packets from IPv6-Host3 should be in IPv6-in-IPv4 encapsulation format. Verify that the IPv4 header "Type of Service" field has the same value as IPv6 header "Traffic Class" in original IPv6 packet captured at probe p6 inbound direction. d) In the packets captured by probe p6 outbound direction, there should be only native IPv6 packet format. Verify that the IPv6 header "Traffic Class" has the same value as IPv4 header "Type of Service" field in IPv6-in-IPv4 packet captured at probe p5 outbound direction.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.6 Configure 6rd Parameters on RG Manually

4.5.6	Configure 6rd Parameters on RG Manually
Test objective	The aim of this test is to verify manual provision of 6rd elements on RG.
Requirement	TR-242: R-27, A.1.1

Requirement description	R-27. The RG MUST be able to be configured with the IPv4MaskLen, 6rdPrefix, 6rdPrefixLen, and 6rdBRIPv4Address. Appendix A.1.1: Manual configuration of 6rd parameters
Device under test	6rd_RG-1, 6rd_RG-2 in Figure 1
Test configuration	**Test Setup** – Figure 1 **Pre-conditions:** 1) Reset DUT to unconfigured state. 2) 6rd_RG-1 and 6rd_RG-2 are configured in router mode. 3) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) Set up and verify IPv4 network connectivity in Network-1, Network-2, and Network-3. 2) Set up and verify IPv6 network connectivity in Network-4. 3) Configure 6rd elements on the 6rd-BR. 4) IPv6-Host3 is configured as FTP or HTTP server and reachability is verified.
Test procedure	1) Configure the 6rd elements on 6rd_RG-1 and 6rd_RG-2 manually. Check the 6rd elements via DUT CLI or EMF (Equipment Management Function) 2) IPv6-Host1 and IPv6-Host2 try to access the FTP or HTTP service in IPv6-Host3.
Expected result	1) At step 1, the 6rd elements are configured successfully on 6rd_RG-1 and 6rd_RG-2 respectively. 2) At step 2, the communication between IPv6-Host1/IPv6-Host2 and IPv6-Host3 respectively, is successful.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.7 Configure 6rd Parameters on RG via DHCP

4.5.7	Configure 6rd Parameters on RG via DHCP
Test objective	The aim of this test is to verify provisioning of 6rd elements on RG via DHCP
Requirement	TR-242: R-27, A.1.2
Requirement description	R-27. The RG MUST be able to be configured with the IPv4MaskLen, 6rdPrefix, 6rdPrefixLen, and 6rdBRIPv4Address.

	Appendix A.1.2: DHCP configuration of 6rd parameters
Device under test	6rd_RG-1, 6rd_RG-2 in Figure 1
Test configuration	**Test Setup** –Figure 1 **Pre-conditions:** 1) Reset DUT to unconfigured state. 2) 6rd_RG-1 and 6rd_RG-2 are configured in router mode. 3) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) Set up and verify IPv4 network connectivity in Network-1, Network-2, and Network-3. 2) Set up and verify IPv6 network connectivity in Network-4. 3) Configure 6rd elements on the 6rd-BR and DHCP server accordingly. 4) IPv6-Host3 is configured as FTP or HTTP server and reachability is verified.
Test procedure	1) Configure the 6rd elements provisioning mode as DHCP. Check the 6rd elements via DUT CLI or EMF to make sure that the 6rd parameters are conveyed to 6rd_RG-1 and 6rd_RG-2, respectively, through their DHCP message exchange with the DHCP server. 2) IPv6-Host1 and IPv6-Host2 try to access the FTP or HTTP service in IPv6-Host3.
Expected result	1) At step 1, the 6rd elements are configured successfully on 6rd_RG-1 and 6rd_RG-2. 2) At step 2, the communication between IPv6-Host1/IPv6-Host2 and IPv6-Host3 respectively, is successful.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.8 Configure 6rd Parameters on RG via TR-069

4.5.8	Configure 6rd Parameters on RG via TR-069
Test objective	The aim of this test is to verify provisioning of 6rd elements on RG via TR-069
Requirement	TR-242: R-27 TR-242: A.1.3
Requirement	R-27. The RG MUST be able to be configured with the IPv4MaskLen,

description	6rdPrefix, 6rdPrefixLen, and 6rdBRIPv4Address. Appendix A.1.3: TR-069 [1]Configuration of 6rd parameters
Device under test	6rd_RG-1, 6rd_RG-2 in Figure 1
Test configuration	**Test Setup** – Figure 1 **Pre-conditions**: 1) Reset DUT to unconfigured state. 2) 6rd_RG-1 and 6rd_RG-2 are configured in router mode. 3) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) Set up and verify IPv4 network connectivity in Network-1, Network-2, and Network-3. 2) Set up and verify IPv6 network connectivity in Network-4. 3) Set up the connectivity between the ACS and 6rd-RG-1/6rd-RG-2, respectively. 4) Configure 6rd elements on the 6rd-BR and the ACS, respectively. 5) IPv6-Host3 is configured as FTP or HTTP server and reachability is verified.
Test procedure	1) Configure the 6rd elements provisioning mode as TR-069 on 6rd_RG-1 and 6rd-RG-2 respectively. Check the 6rd elements via DUT CLI or EMF. 2) IPv6-Host1 and IPv6-Host2 try to access the FTP or HTTP service in IPv6-Host3.
Expected result	1) At step 1, the 6rd parameters are configured on 6rd-RG-1 and 6rd-RG-2 respectively, successfully. 2) At step 2, the communication between IPv6-Host1/IPv6-Host2 and IPv6-Host3 respectively, is successful.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.9 Forwarding over Native IPv6 vs. 6rd with Same IPv6 Prefix

4.5.9	Forwarding over native IPv6 vs. 6rd with same IPv6 prefix
Test objective	The aim of this test is to check 6rd RG routing behavior when both native IPv6 and 6rd are enabled with the same IPv6 prefix.
Requirement	TR-242: R-30

Requirement description	R-30. When the same prefix is provided the default behavior SHOULD be to route over native IPv6 rather than 6rd.
Device under test	6rd_RG-1 device in Figure 1
Test configuration	**Test Setup** – Figure 1 **Pre-conditions:** 1) 6rd_RG-1 is configured in router mode. 2) Network-3 is a dual-stack network which supports both IPv4 and IPv6 3) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) 6RD-BR is configured with 6rd elements. 2) 6RD_RG-1 is configured with 6rd elements and has 6rd mechanism enabled. 3) Enable IPv6 on 6RD_RG-1 WAN link on Network-3 and configure IPv6 address with same prefix as 6rd prefix
Test procedure	1) Prepare probe p2 to capture packets. 2) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3
Expected result	1) At step 2, IPv6-Host1 receives ICMPv6 Echo Replies to all ICMPv6 Echo Requests that have been transmitted to IPv6-Host3. 2) At step 2, probe p2 shows that the ICMPv6 Echo Requests and ICMPv6 Echo Reply message are native IPv6 packets.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.10 Forwarding over Native IPv6 vs. 6rd with Different IPv6 Prefix

4.5.10	Forwarding over native IPv6 vs. 6rd with different IPv6 prefix
Test objective	The aim of this test is to check 6rd RG routing behavior when both native IPv6 and 6rd are enabled with different IPv6 prefix.
Requirement	TR-242: R-31
Requirement description	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.
Device under test	6rd_RG-1 in Figure 1
Test	**Test Setup** – Figure 1

configuration	**Pre-conditions:** 1) 6rd_RG-1 is configured in router mode. 2) Network-3 is a dual-stack network which supports both IPv4 and IPv6 3) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) 6RD-BR is configured with 6rd elements.
Test procedure	1) Prepare probe p1 to capture packets. 2) Enable IPv6 on 6RD_RG-1 WAN link on Network-3 and configure IPv6 address with IPv6 prefix-1. 3) Enable 6rd mechanism on 6RD_RG-1 and configure 6rd elements with IPv6 prefix-2 different than IPv6 prefix-1 4) Prepare probe p2 to capture packets. 5) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3
Expected result	1) At step 2, 6RD_RG-1 transmits an IPv6 Router Advertisement with IPv6 prefix-1 with a valid lifetime and with autonomous address-configuration flag set. 2) At step 3, 6RD_RG-1 transmits an IPv6 Router Advertisement with two Prefix Information Options. One option includes IPv6 prefix-1 with autonomous address-configuration flag set. The other option includes IPv6 prefix-2 with autonomous address-configuration flag clear. 3) At step 5, IPv6-Host1 receives ICMPv6 Echo Replies to all ICMPv6 Echo Requests that have been transmitted to IPv6-Host3. The capture at probe p2 shows that the IPv6 prefix-1 is used for the source IPv6 address of ICMPv6 Echo Requests messages and the destination IPv6 address of ICMPv6 Echo Reply messages.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.11 Hub and Spoke Mode

4.5.11	Hub and Spoke Mode
Test objective	Verify a 6rd Residential Gateway supports 6rd hub and spoke mode.
Requirement	TR-242: R-25, R-33
Requirement description	TR-242: 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-33: The RG MUST be able to be configured to send all 6rd traffic to the BR.
Device under test	6RD_RG-1 and 6RD_RG-2 in Figure 1
Test configuration	**Test Setup** – Figure 1 **Test Conditions:** 1) Router1 is configured to assign 6rd elements via or DHCPv4 or ACS is configured to assign 6rd elements via TR-069 or is manually configured with 6rd elements. 2) 6RD-BR is configured with 6rd elements. 3) 6RD_RG-1 and 6RD_RG-2 have 6rd mechanism enabled and are configured with 6rd elements via DHCPv4, TR-069, or manually. 6RD_RG-1 and 6RD_RG-2 are configured to send all traffic to 6RD-BR.
Test procedure	1) Enable 6RD_RG-1 and 6RD_RG-2. 2) Wait for 6RD_RG-1 and 6RD_RG-2 to obtain 6rd elements. 3) Capture packets at probe p2 and p4. 4) IPv6-Host1 transmits ICMPv6 Echo Requests to delegated 6rd address of 6RD_RG-2.
Expected result	At step 4, 6RD_RG-1 and 6RD_RG-2 forward encapsulated ICMPv6 Echo Requests and ICMPv6 Echo Replies, respectively, to 6RD-BR.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.12 User-to-User Direct Communication

4.5.12	6rd User-to-User direct communication
Test objective	Verify a 6rd Residential Gateway supports sending traffic directly within the same 6rd domain.
Requirement	TR-242: R-25
Requirement description	TR-242: 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.
Device under test	6RD_RG-1 and 6RD_RG-2 in Figure 1
Test	**Test Setup** – Figure 1

configuration	**Test Conditions:** 1) Router1 is configured to assign 6rd elements via DHCPv4, or the ACS is configured to assign 6rd elements via TR-069. 2) 6RD-BR is configured with 6rd elements. 3) 6RD_RG-1 and 6RD_RG-2 have 6rd mechanism enabled and are configured with 6rd elements via DHCPv4, TR-069, or manually. 6RD_RG-1 is configured to send traffic directly to 6RD_RG-2, and vice versa.
Test procedure	1) Enable 6RD_RG-1 and 6RD_RG-2. 2) Wait for 6RD_RG-1 and 6RD_RG-2 to obtain 6rd elements. 3) Capture packets at probe p2 and p4. 4) IPv6-Host1 transmits ICMPv6 Echo Requests to delegated 6rd address of 6RD_RG-2.
Expected result	At step 4, 6RD_RG-1 and 6RD_RG-2 forward encapsulated ICMPv6 Echo Requests and ICMPv6 Echo Replies, respectively, directly to each other not via 6rd_BR.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.13 Maximum Transmission Unit (MTU)

4.5.13	Maximum Transmission Unit (MTU)
Test objective	Verify a 6rd Border Relay supports configuration of MTU.
Requirement	TR-242: R-18
Requirement description	TR-242: R-18: The 6rd BR MUST provide a mechanism to configure the MTU of the 6rd tunnel independent of any IPv4 MTU configuration.
Device under test	6RD-BR in Figure 1
Test configuration	**Test Setup** – Figure 1 **Test Conditions**: 1) Router1 is configured to assign 6rd elements via DHCPv4, or the ACS is configured to assign 6rd elements via TR-069 [1]. 2) 6RD-BR is configured with 6rd elements and is configured with an MTU of 1280 bytes on 6rd tunnel interface. 3) 6RD_RG-1 has 6rd mechanism enabled and is configured with 6rd elements via DHCPv4, TR-069, or manually.

Test procedure	1) Enable 6RD_RG-1. 2) Wait for 6RD_RG-1 to obtain 6rd elements. 3) Capture packets at probe p1 and probe p2. 4) IPv6-Host1 transmits ICMPv6 Echo Requests of size 1500 bytes to IPv6-Host3.
Expected result	At step 4, verify the following: 1) 6RD_RG-1 drops the packets. 2) 6RD_RG-1 sends ICMPv6 Error message (Packet Too Big) to IPv6-Host1. 3) IPv6-Host1 fragments subsequent ICMPv6 Echo Requests sent to IPv6-Host3.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.14 Persistent 6rd Delegated IPv6 Prefix

4.5.14	Persistent Prefix
Test objective	Verify a 6rd Residential Gateway continues to advertise a prefix when the WAN connection has gone down. Verify that 6rd Residential Gateway re-discovers the 6rd service after the WAN connection comes up.
Requirement	TR-242: R-29
Requirement description	TR-242: 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.
Device under test	6RD-RG-1 in Figure 1
Test configuration	**Test Setup** – Figure 1 **Test Conditions:** 1) Router1 is configured to assign 6rd elements via or DHCPv4 or ACS is configured to assign 6rd elements via TR-069. 2) 6RD-BR is configured with 6rd elements. 3) 6RD_RG-1 has 6rd mechanism enabled and is configured with 6rd elements

	via DHCPv4, TR-069, or manually.
Test procedure	1) Capture packets at probe p1 2) Enable 6RD_RG-1. 3) Wait for 6RD_RG-1 to obtain 6rd elements. 4) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3. 5) Disable the WAN connection to 6RD_RG-1. 6) Wait for 6rd_RG-1 to send an IPv6 Router Advertisement on Network 1. 7) Enable the WAN connection to 6RD_RG-1. 8) Wait for 6rd_RG-1 to obtain 6rd elements. 9) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3.
Expected result	1) At step 3, 6RD_RG-1 transmits an IPv6 Router Advertisement with a valid Prefix Information Option that has a valid lifetime. 2) At step 4, IPv6-Host1 receives ICMPv6 Echo Replies to all the ICMPv6 Echo Requests that have been transmitted to IPv6-Host3. 3) At step 6, 6RD_RG-1 transmits an IPv6 Router Advertisement with same 6rd delegated prefix as in step 3 with a valid lifetime. 4) At step 9, IPv6-Host1 receives ICMPv6 Echo Replies to all the ICMPv6 Echo Requests that have been transmitted to IPv6-Host3.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.15 Lost Service

4.5.15	Lost service
Test objective	Verify a 6rd Residential Gateway continues to advertise a prefix when the WAN connection has gone down. Verify that when the WAN connection comes up the 6rd Residential Gateway re-discovers 6rd and advertises a different prefix.
Requirement	TR-242: R-29
Requirement description	TR-242: 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.

Device under test	6RD-RG-1 in Figure 1
Test configuration	**Test Setup** – Figure 1 **Test Conditions:** 1) Router1 is configured to assign 6rd elements via DHCPv4, or the ACS is configured to assign 6rd elements via TR-069. 2) 6RD-BR is configured with 6rd elements. 3) 6RD_RG-1 has 6rd mechanism enabled and is configured with 6rd elements via DHCPv4, TR-069, or manually.
Test procedure	1) Capture packets at probe p1. 2) Enable 6RD_RG-1. 3) Wait for 6RD_RG-1 to obtain 6rd elements. 4) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3. 5) Disable the WAN connection to 6RD_RG-1. 6) Wait for 6rd_RG-1 to send an IPv6 Router Advertisement on Network-1. 7) Configure DHCPv4 server or ACS to stop assigning 6rdPrefixes to 6RD_RG-1. 8) Enable the WAN connection to 6RD_RG-1. 9) Wait for 6rd_RG-1 to send an IPv6 Router Advertisement on Network-1.
Expected result	1) At step 4, IPv6-Host1 receives ICMPv6 Echo Replies to all the ICMPv6 Echo Requests that have been transmitted to IPv6-Host3. 2) At step 6, 6RD_RG-1 transmits an IPv6 Router Advertisement with a valid Prefix Information Option that has the old 6rdPrefix with a valid lifetime. 3) At step 9, 6RD_RG transmits an IPv6 Router Advertisement with a valid Prefix Information Option containing the old 6rdPrefix and a lifetime of zero.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

4.5.16 6rd Prefix Change

4.5.16	6rd Prefix Change
Test objective	Verify a 6rd Residential Gateway continues to advertise a prefix when the WAN connection has gone down. Verify that when the WAN connection comes up the 6rd Residential Gateway re-discovers 6rd service and advertises a different prefix.

Requirement	TR-242: R-29
Requirement description	TR-242: 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.
Device under test	6RD-RG-1 in Figure 1
Test configuration	**Test Setup** – Figure 1 **Test Conditions:** 1) Router1 is configured to assign 6rd elements via DHCPv4, or the ACS is configured to assign 6rd elements via TR-069. 2) 6RD-BR is configured with 6rd elements. 3) 6RD_RG-1 has 6rd mechanism enabled and is configured with 6rd elements via DHCPv4, TR-069, or manually.
Test procedure	1) Capture packets at probe p1. 2) Enable 6RD_RG-1. 3) Wait for 6RD_RG-1 to obtain 6rd elements. 4) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3. 5) Disable the WAN connection to 6RD_RG-1. 6) Wait for 6rd_RG-1 to send an IPv6 Router Advertisement on Network- 1. 7) Configure DHCPv4 server or ACS to assign a new 6rdPrefix. 8) Enable the WAN connection to 6RD_RG-1. 9) Wait for 6rd_RG-1 to obtain 6rd elements. 10) IPv6-Host1 transmits ICMPv6 Echo Requests to IPv6-Host3.
Expected result	1) At step 4, IPv6-Host1 receives ICMPv6 Echo Replies to all the ICMPv6 Echo Requests that have been transmitted to IPv6-Host3. 2) At step 6, 6RD_RG-1 transmits an IPv6 Router Advertisement with a valid Prefix Information Option that has the old 6rdPrefix with a valid lifetime. 3) At step 9, 6RD_RG-1 transmits an IPv6 Router Advertisement with a valid Prefix Information Option containing the old 6rd delegated prefix and a lifetime of zero. 6RD_RG-1 transmits an IPv6 Router Advertisement with a valid Prefix Information Option containing the new 6rd delegated prefix and a valid lifetime.

	4) At step 10, IPv6-Host1 receives ICMPv6 Echo Replies to all the ICMPv6 Echo Requests that have been transmitted to IPv6-Host3.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5 Test Cases for DS-Lite

5.1 Device Under Test

- Two RG (Residential Gateway) with DS-Lite B4 functionality
- One DS-Lite AFTR device

5.2 Test Equipment

For DS-Lite interoperability test, the required test equipment is as follows:

- Four IPv6 hosts supporting the IPv6 stack, including handling of ICMPv6, DHCPv6, HTTP and DNS requests over IPv6.
- Three IPv4 hosts supporting the IPv4 stack, including handling of ICMP, DHCP, HTTP and DNS requests over IPv4.
  Note: all IPv4 and IPv6 hosts could be simulated using a Traffic Generator platform that is connected to the DS-Lite B4 nodes and the DS-Lite AFTR node, respectively. Also, an IPv4-IPv6 dual-stack host may also be used.
- Two IPv6 routers with one capable of providing server function of DHCPv6, DNS and RADIUS.
- DNS Server
- RADIUS Server that supports DS-Lite extensions defined in RFC6519 [26].
- DHCPv6 Server that supports DS-Lite options defined in RFC6334 [25].
- One TR-069 server (ACS).
- Traffic generator capable of generating IPv4 and IPv6 traffic.
- Protocol analyzer capable of interpreting this list of traffic types:
  - IPv4 packets
  - IPv6 packets
  - IPv4-in-IPv6 packets per RFC2473 [12]

5.3 Test Setup

This section describes the requirements of DS-Lite B4 and DS-Lite AFTR including their interfaces, configuration, etc. for the test cases. It also describes the associated network services provided by DNS server, RADIUS server, and DHCPv6 server that are required in the test. Finally, it describes the functions of traffic generator and protocol analyzer that are used for the test.

For DS-Lite interoperability test, two simulated home networks (Network-1 and Network-2 in Figure 2) are needed that support both IPv4 and IPv6, and at each site, there is a DS-Lite B4 device that is running in the router mode for IPv6 but also capable of receiving and transmitting IPv4 packets that are encapsulated with IPv6 header. The reason for having two simulated home networks is to test customer-to-customer communication.

The DS-Lite AFTR device must have an interface facing DS-Lite B4 devices over an IPv6-only access network (Network-3 in Figure 2). This network is capable of transporting IPv4-in-IPv6 packets. In addition, the DS-Lite AFTR device connects to both an IPv4-only network (Network-4 in Figure 2) and an IPv6-only network (Network-5 in Figure 2) that provide the source and destination of test traffic, respectively.

This test also requires some network service functions such as DHCPv6 server function, RADIUS server function, and DNS server function.

5.4 Test Topology

Figure 2 is the DS-Lite test topology for all DS-Lite test cases; note that depending on each test case, test equipments are connected and configured as needed. The connectivity as illustrated between the devices in the figure is at IP layer.

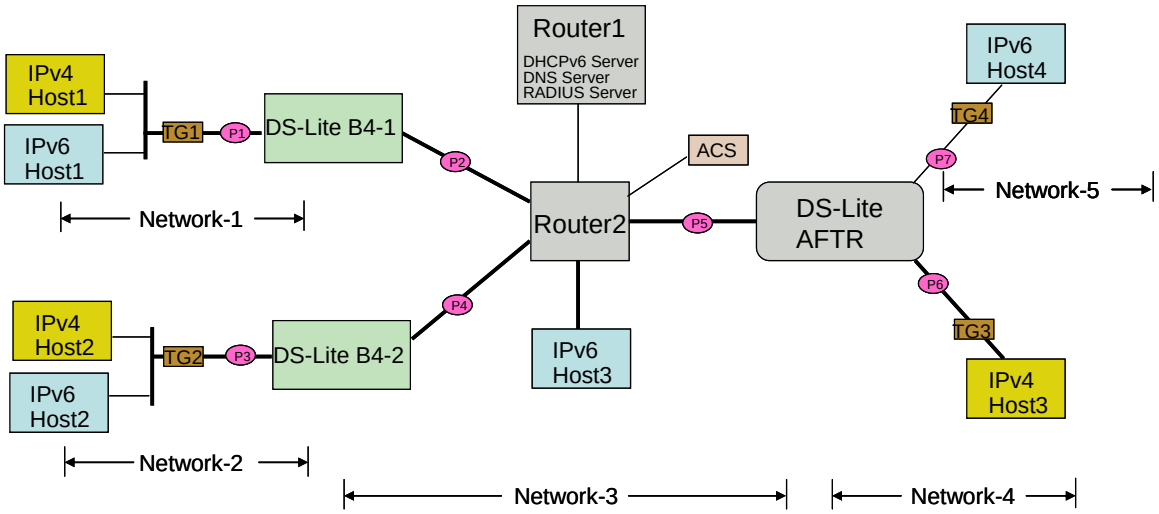

Figure 2 DS-Lite Test Topology

Table 2 Device and Functions Used in DS-Lite Test

Devices/Functions	Descriptions
DS-Lite B4-1 DS-Lite B4-2	The RG supports DS-Lite B4 functions. At least two units are required in order to allow testing of customer-to-customer traffic.
DS-Lite AFTR	The DS-Lite AFTR function may be located on a BNG or on a separate platform.
Router1	This is an IPv6 router that provides DHCPv6 server function, DNS server function and RADIUS server function. Note alternatively, one or more of these server functions can be realized by other devices including

	traffic generators.
Router2	This is an IPv6 router that provides IP connectivity between IP devices.
ACS	Automatic Configuration Server that provides TR-069 server function.
IPv4-Host1, IPv4-Host2, IPv4-Host3	These are IPv4 hosts, which are used to test IPv4 communication among the hosts and with the traffic generators.
IPv6-Host1, IPv6-Host2, IPv6-Host3, IPv6-Host4	These are IPv6 hosts which are used to test IPv6 communication among the hosts.
TG1/TG2/TG3/TG4	These are insertion points where traffic generator may be connected in-wire. If connected, traffic generators provide IPv4 traffic source and destination and communicate with IPv4 hosts.
Probe points (p1 to p7)	The probe points may be inserted in different points of the test network in order to verify and monitor the IP packets.
Network-1, Network-2	These are IPv4-IPv6 dual-stack networks.
Network-3	This is IPv6-only network by default. Whenever a test case requires IPv4 support, this will be stated explicitly
Network-4	This is IPv4-only network.
Network-5	This is IPv6-only network.

5.5 Test Cases

This section lists all test cases for DS-Lite. Note that the DS-Lite test cases are organized according to DS-Lite requirements defined in Section 6/TR-242.

5.5.1 Configure FQDN of AFTR Element on RG via DHCPv6

5.5.1	FQDN of the AFTR element can be conveyed to RG via DHCPv6 [25].
Test objective	The aim of this test is to check FQDN of the AFTR element is conveyed to RG via DHCPv6 correctly
Requirement	TR-242:R-46
Requirement description	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 [1], or manually.
Device under test	DS-Lite B4 devices in Figure 2
Test configuration	**Test Setup -** Figure 2 **Pre-conditions:**

	1) Reset DUT to unconfigured state. 2) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode. 3) The probes are ready to analyze the IP packets. **Test Conditions:** 1) IPv6 addresses are configured on AFTR 2) IPv6 address pool and FQDN (AFTR name) are configured on the DHCPv6 server. 3) The IPv6 address for FQDN of AFTR is configured on DNS server. 4) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode. 5) IPv4-Host3 is configured as FTP or HTTP server and reachability is verified.
Test procedure	1) Configure the FQDN retrieving mode as DHCPv6 on DS-Lite B4-1/ DS-Lite B4-2 to acquire IPv6 address from DHCPv6 server. 2) DS-Lite B4-1 and DS-Lite B4-2 start the IP connection. 3) Check the AFTR-Name DHCPv6 option is requested by DS-Lite B4-1/ DS-Lite B4-2 in the packets via the probes p2/p4 4) IPv4-Host1 and IPv4-Host2 try to access the FTP or HTTP service in IPv4-Host3. 5) Check the specific FQDN of the AFTR element on DS-Lite B4-1/ DS-Lite B4-2 via EMF (Equipment Management Function), or check the AFTR FQDN in DNS Requests from DS-Lite B4-1/ DS-Lite B4-2 in the packets via the probes p2/p4, which should be the same as the specified FQDN configured.
Expected result	1) At step 1, the FQDN retrieving mode is changed to DHCPv6 mode successfully. 2) At step 2, the IP connection is established successfully. 3) At step 3, the AFTR-Name DHCPv6 option is requested in DHCPv6 messages from DS-Lite B4-1/ DS-Lite B4-2 4) At step 4, IPv4-Host1 and IPv4-Host2 get access to the FTP or HTTP service successfully (optional). 5) At step 5, the FQDN entry created on DS-Lite B4-1 and DS-Lite B4-2 is correct. The AFTR FQDN in DNS Requests from DS-Lite B4-1/ DS-Lite B4-2 in the packets via the probes p2/p4 is the same as the specified FQDN configured on the DHCPv6 server.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.2 Configure FQDN of the AFTR Element on RG manually

5.5.2	FQDN of the AFTR element can be conveyed to RG manually
Test objective	The aim of this test is to check FQDN of the AFTR element can be manually configured on RG correctly
Requirement	TR-242:R-46
Requirement description	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 [1], or manually.
Device under test	DS-Lite B4 devices in Figure 2
Test configuration	**Test Setup -** Figure 2 **Pre-conditions:** 1) Reset DUT to unconfigured state. 2) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode. 3) The probes are ready to analyze the IP packets. **Test Conditions:** 1) IPv6 addresses are configured on DS-Lite AFTR device 2) IPv6 address pool is configured on the DHCPv6 server. 3) The IPv6 address for FQDN of the AFTR is configured on DNS server. 4) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode. 5) IPv4-Host3 is configured as FTP or HTTP server and reachability is verified.
Test procedure	1) Configure the FQDN manually on DS-Lite B4-1 and DS-Lite B4-2, and DS-Lite B4-1/ DS-Lite B4-2 acquire IPv6 address from DHCPv6 server respectively. 2) DS-Lite B4-1 and DS-Lite B4-2 start the IP connection. 3) IPv4-Host1 and IPv4-Host2 try to access the FTP or HTTP service in IPv4-Host3. 4) Check the specific FQDN of the AFTR element on DS-Lite B4-1 and DS-Lite B4-2 via EMF (Equipment Management Function). 5) Check the AFTR FQDN in DNS Requests from DS-Lite B4-1/ DS-Lite B4-2 in the packets via the probes p2/p4 is the same as the specified FQDN configured.
Expected result	1) At step 1, the FQDN retrieving mode is changed to manual mode successfully.

	2) At step 2, the IP connection is established successfully. 3) At step 3, IPv6-Host1 and IPv6-Host2 get access to the FTP or HTTP service successfully (optional). 4) At step 4, the FQDN entry created on DS-Lite B4-1and DS-Lite B4-2 is correct. 5) The AFTR FQDN in DNS Requests from DS-Lite B4-1/ DS-Lite B4-2 in the packets via the probes p2/p4 is the same as the specified FQDN configured on t DS-Lite B4-1 and DS-Lite B4-2.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.3 Configure FQDN of the AFTR Element on RG via TR-069

5.5.3	FQDN of the AFTR element can be conveyed to RG via TR-069 [1]
Test objective	The aim of this test is to check FQDN of the AFTR element is conveyed to RG via TR-069 correctly
Requirement	TR-242:R-46
Requirement description	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 [1], or manually.
Device under test	DS-Lite B4 devices in Figure 2
Test configuration	**Test Setup -** Figure 2 **Pre-conditions:** 1) Reset DUT to unconfigured state 2) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode. 3) The probes are ready to analyze the IP packets. **Test Conditions:** 1) IPv6 addresses are configured on DS-Lite AFTR device 2) IPv6 address pool is configured on the DHCPv6 server. 3) The FQDN (AFTR name) is configured on the ACS. 4) The IPv6 address for FQDN of the AFTR is configured on DNS server. 5) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode. 6) IPv4-Host3 is configured as FTP or HTTP server and reachability is verified.

Test procedure	1) Configure the FQDN retrieving mode as TR-069 on DS-Lite B4-1 and DS-Lite B4-2, and B4-1/B4-2 acquire IPv6 address from DHCPv6 server respectively. 2) DS-Lite B4-1 and DS-Lite B4-2 start the IP connection. 3) IPv4-Host1 and IPv4-Host2 try to access the FTP or HTTP service in IPv4-Host3. 4) Check the specific FQDN of the AFTR element on DS-Lite B4-1 and DS-Lite B4-2 via EMF (Equipment Management Function). 5) Check the AFTR FQDN in DNS Requests from DS-Lite B4-1/ DS-Lite B4-2 in the packets via the probes p2/p4 is the same as the specified FQDN configured
Expected result	1) At step 1, the FQDN retrieving mode is changed to TR-069 mode successfully. 2) At step 2, the IP connection is established successfully. 3) At step 3, IPv4-Host1 and IPv4-Host2 get access to the FTP or HTTP service successfully. 4) At step 4, the FQDN entry created on DS-Lite B4-1 and DS-Lite B4-2 is correct. 5) The AFTR FQDN in DNS Requests from DS-Lite B4-1/ DS-Lite B4-2 in the packets via the probes p2/p4 is the same as the specified FQDN configured on t DS-Lite B4-1 and DS-Lite B4-2.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.4 IPv4-in-IPv6 Tunnel Encapsulation

5.5.4	IPv4-in-IPv6 tunnel encapsulation
Test objective	The aim of this test is to check whether IPv4 packets tunneling in IPv6 is complied with RFC2473 [12].
Requirement	TR-242:R-44, R-53
Requirement description	R-44. The B4 element of the RG MUST support IPv4-in-IPv6 encapsulation on its WAN link as specified in RFC2473 [12]. R-53. The AFTR MUST support IPv4-in-IPv6 as specified in RFC2473 to establish the DS-Lite softwire.
Device under test	DS-Lite B4 devices in Figure 2
Test	**Test Setup** - Figure 2

configuration	**Pre-conditions:** 1) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode. 2) The probes are ready to analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv4 address for Network-4 and IPv6 address are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode, and the retrieving mode of IPv6 address is set to DHCPv6 mode if FQDN is configured on the DHCPv6 server (step 3 above). 6) IPv4-Host3 is configured as FTP or HTTP server and reachability is verified. 7) NAT44 is configured on DS-Lite AFTR device.
Test procedure	1) DS-Lite B4-1 and DS-Lite B4-2 start IP connection. 2) Check the IPv4-in-IPv6 tunnel entry on DS-Lite B4-1, DS-Lite B4-2 and DS-Lite AFTR via EMF (Equipment Management Function). 3) IPv4-Host1 and IPv4-Host2 try to access the FTP or HTTP service in IPv4-Host3. 4) Capture and analyze the packets via the probes p2/p4 and p6. 5) Capture and analyze the packets via the probes p5 and p1/p3.
Expected result	1) At step 1, the IP connection is established successfully. 2) At step 2, IPv4-in-IPv6 tunnels establish successfully on DS-Lite B4-1, DS-Lite B4-2, and DS-Lite AFTR. The related tunnel entries are created with the IPv6 tunnel addresses being set according to the tunnel end's IPv6 address. 3) At step 3, IPv4-Host1 and IPv4-Host2 get access to IPv4 FTP or HTTP service successfully. 4) At step 4, in the packets captured by the probes p2/p4 outbound direction, all the original IPv4 packets are now in IPv4-in-IPv6 tunnel encapsulation format with the source IPv6 address being the B4-1's and B4-2's IPv6 address respectively, and the destination IPv6 address being the DS-Lite AFTR's IPv6 address. In the packets captured by the probe p6 outbound direction, all the packets are the same as the packets originally sent by the IPv4-Host1 and IPv4-Host2 respectively, except the source IPv4 address because it is changed by NAT.

	5) At step 5, in the packets captured by the probe p5 inbound direction, all the original IPv4 packets are now in IPv4-in-IPv6 tunnel encapsulation format with the source IPv6 address being the DS-Lite AFTR's IPv6 address and the destination IPv6 address being the B4-1's and B4-2's IPv6 address respectively. In the packets captured by the probes p1/p3 inbound direction, all the packets are the same as the packets originally sent by IPv4-Host3 except the destination IPv4 address because it is changed by NAT.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.5 Deactivate NAPT Function on RG

5.5.5	Deactivate NAPT Function on DS-Lite RG
Test objective	The aim of this test is to check if the RG can deactivate the NAPT function on the DS-Lite interface when running DS-Lite.
Requirement	TR-242: R-43.
Requirement description	R-43 When running DS-Lite, the RG MUST deactivate the NAPT function on the DS-Lite interface.
Device under test	DS-Lite B4 devices in Figure 2
Test configuration	**Test Setup - Figure 2** **Pre-conditions:** 1) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode. 2) The probes are ready to analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv4 address and IPv6 address are configured on DS-Lite B4-1, DS-Lite B4-2, and DS-Lite AFTR device. 2) IPv6 address pool and FQDN (AFTR name) are configured on the DHCPv6 server. 3) The IPv6 address for FQDN of AFTR is configured on DNS server. 4) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode but not NAT44 mode, and the IPv6 address retrieving mode is set to DHCPv6 mode. 5) IPv4-Host3 is configured as FTP or HTTP server and reachability is verified.
Test procedure	1) IPv4-Host1, IPv4-Host2, DS-Lite B4-1 and DS-Lite B4-2 start their

	respective IP connections. 2) Check the IPv4-in-IPv6 tunnel entry both on DS-Lite B4-1/ DS-Lite B4-2 and AFTR. 3) IPv4-Host1 and IPv4-Host2 try to get access to the FTP or HTTP service in IPv4-Host3. 4) Capture and analyze the packets via the probes p1/p3 and p2/p4.
Expected result	1) At step 1, the IP connections are established successfully. 2) At step 2, IPv4-in-IPv6 tunnels establish successfully both on DS-Lite B4-1/DS-lite B4-2 and DS-Lite AFTR and the related tunnel entries are created with the IPv6 tunnel addresses being set according to the tunnel end's IPv6 address. 3) At step 4, in the packets captured by the probes p2/p4 outbound direction, all the packets are with the source address being the DS-Lite B4-1's and DS-Lite B4-2's IPv6 address respectively. The source IPv4 address and port in the tunneled packet are same as the packet sent by the IPv4-Host1 and IPv4-Host2 respectively as observed at probes p1/p3.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.6 Configuring a default IPv4 Route at RG for DS-Lite Tunnel

5.5.6	IPv4 traffic can be routed to DS-Lite tunnel by a static IPv4 default route at RG
Test objective	The aim of this test is to check whether the IPv4 traffic can be routed to the DS-Lite tunnel by a static IPv4 default route.
Requirement	TR-242: R-47
Requirement description	R-47. The RG MUST support configurations of a static IPv4 default route towards the DS-Lite tunnel for the IPv4 traffic.
Device under test	DS-Lite B4 devices in Figure 2
Test configuration	**Test Setup - Figure 2** **Pre-conditions:** 1) DS-Lite B4-1 is configured in router mode. 2) Probe p2 is ready to analyze the IPv6 packets. **Test Conditions:** 1) IPv4 public address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device.

	2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 is configured in DS-Lite mode, the IPv4 prefix for Network-1 and IPv6 address for Network-3 are configured. 6) IPv4-Host3 and IPv6-Host3 are configured as FTP or HTTP server. 7) NAT44 is configured on DS-Lite AFTR device.
Test procedure	1) DS-Lite B4-1 starts IP connection. 2) IPv6-Host1 tries to get access to the FTP or HTTP services in IPv6-Host3. 3) Configure a static IPv4 default route pointing to the virtual interface (tunnel) towards the DS-Lite AFTR (it does not need to be configured if the static IPv4 default route is already configured by default). Check the static IPv4 default route entry on DS-Lite B4-1. 4) IPv4-Host1 tries to access the FTP or HTTP services in IPv4-Host3.
Expected result	1) At step 1, the IP connection is established successfully. 2) At step 2, IPv6-Host1 accesses the FTP or HTTP services successfully. 3) At step 3, the outbound interface of the static IPv4 default route entry is the DS-Lite tunnel on DS-Lite B4-1. 4) At step 4, IPv4-Host1 accesses the FTP or HTTP services successfully.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.7 Extended NAT Table on DS-Lite AFTR

5.5.7	Extended NAT Table on DS-Lite AFTR
Test objective	The aim of this test is to check whether the AFTR support an extended NAT table in DS-Lite scenario
Requirement	Section 6.6 in RFC6333 TR-242 R-93
Requirement description	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
Device under test	DS-Lite B4 devices in Figure 2

Test configuration	**Test Setup -** Figure 2 **Preconditions:** 1) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode and work as gateway for their LAN. **Test Conditions**: 1) IPv4 public address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) FQDN of DS-Lite AFTR is configured on the DHCPv6 server. 3) The IPv6 address for FQDN of AFTR is configured on DNS server. 4) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode, while B4-1's IPv4 prefix for Network-1 is the same as B4-2's IPv4 prefix for Network-2 and B4-1's IPv6 address for Network-3 is different from B4-2's IPv6 address. 5) IPv4-Host3 are configured as a FTP server as well as a web server. 6) NAT44 function with extended NAT binding table is configured on DS-Lite AFTR device.
Test procedure	1) DS-Lite B4-1 and DS-Lite B4-2 start the IP connection 2) The IPv4-Host1 and IPv4-Host2 try to get access to the FTP and Web service in IPv4 -Host3 3) Check the NAT address mapping table on DS-Lite AFTR device via EMF.
Expected result	1) At step 1, the IP connections are established successfully. 2) At step 2, the IPv4-Host1 and IPv4-Host2 successfully accesses the application service in IPv4-Host3. 3) At step 3, the DS-Lite AFTR device successfully completes the address translation, creates two NAT address mapping entries. The first entry for DS-Lite B4-1 includes the IPv6 address of DS-Lite B4-1, and the second entry for DS-Lite B4-2 includes the IPv6 address of DS-Lite B4-2.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.8 Mapping between IPv4 TOS field and IPv6 TC field

5.5.8	Mapping between TOS field and TC field
Test objective	The aim of this test is to check whether the value of the "Type of Service"(TOS) field in an IPv4 packet is copied into the "Traffic Class"(TC)

	field of the corresponding IPv6 packet during the encapsulation process and vice versa during the de-capsulation process in DS-Lite scenario. In particular: this test case is for B4 and AFTR device.
Requirement	TR-242: R-50, R-55
Requirement's description	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 [14]. 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.
Device under test	DS-Lite B4 devices and DS-Lite AFTR device in Figure 2
Test configuration	**Test Setup** – Figure 2 **Pre-conditions:** 1) DS-Lite B4-1 is configured in router mode. 2) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv4 public address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 is configured in DS-Lite mode, the IPv4 prefix for Network-1 and IPv6 address for Network-3 are configured. 6) NAT44 is configured on DS-Lite AFTR device. The IPv4 public address pool of Network-4 is configured on NAT, and only one public IPv4 address A1.B1.C1.D1 is included in the pool of Network-4. 7) The RG and DS-Lite AFTR device enable the mapping function between TOS field in IPv4 packet and TC field in IPv6 packet.
Test procedure	1) DS-Lite B4-1 starts IP connection. 2) TG1 sends a traffic stream, in which the source IPv4 address is a1.b1.c1.d1 of Network-1, the destination IPv4 address is A2.B2.C2.D2 of Network-4, and the value of TOS field in IPv4 packet is set to A. Capture IPv6 packets from B4-1 at probe p2 and check IPv4 packets received by TG3.

	3) Check the NAT address mapping table entry on DS-Lite AFTR device via EMF. 4) Based on the NAT address mapping table information obtained in step 3, TG3 sends traffic stream in which the source IPv4 address is A2.B2.C2.D2 of Network-4 and the destination IPv4 address is A1.B1.C1.D1 of Network-4, destination port number is x1, the value of TOS field in IPv4 packet is set to B. Capture IPv6 packets from DS-Lite AFTR device at probe p5 and check the IPv4 packets received by TG1.
Expected result	1) At step 1, the IP connection is established successfully. 2) At step 2, in the IPv6 packets captured at probe p2, the value of TC field should be A. In the IPv4 packets captured by probe p6, the value of TOS field should be A too. 3) At step 3 on DS-Lite AFTR device, a new NAT address mapping entry should be created as follow: a1.b1.c1.d1: x1 <----> A1.B1.C1.D1: X1 4) At step 4, the IPv6 packets captured by probe p5, the value of TC field should be B. In the IPv4 packets captured by probe p5, the value of TOS field should be B too. Note: 1) an.bn.cn.dn:xn indicates the IPv4 private address and port of Network-1 2) An.Bn.Cn.Dn:Xn indicates the IPv4 public address and port of Network-4
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.9 DNS Proxy function for RG

5.5.9	DNS Proxy function for RG
Test objective	The aim of this test is to check whether the DNS Proxy function is supported by RG.
Requirement	TR-242: R-61
Requirement's description	R-61. The RG MUST support DNS proxy as per RFC5625 [22] for IPv4 hosts connected on its LAN side.
Device under test	DS-Lite B4 devices and AFTR device in Figure 2
Test configuration	**Test Setup –** Figure 2 **Pre-conditions:**

	1) DS-Lite B4-1 is configured in router mode. 2) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv4 public address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) NAT44 is configured on DS-Lite AFTR device. 3) IPv6 address pool is configured on the DHCPv6 server. 4) FQDN (AFTR name) and DNS server address are configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 5) The IPv6 address for FQDN of AFTR is configured on DNS server. 6) The domain name for IPv4-Host3 is configured on IPv4 DNS server. 7) Enable the DNS proxy function on DS-Lite B4-1 if it's not enabled by default. 8) DS-Lite B4-1 is configured in DS-Lite mode, the IPv4 prefix for Network-1 and IPv6 address for Network-3 are configured. 9) IPv4-Host3 and IPv6-Host3 are configured as FTP or HTTP server and reachability is verified, respectively.
Test procedure	1) DS-Lite B4-1 starts IP connection. 2) IPv4-Host1 tries to access the FTP or HTTP services by the domain name of IPv4-Host3.
Expected result	1) At step 1, the IP connection is established successfully. 2) At step 2, IPv4-Host1 should access the FTP or HTTP services successfully.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.10 PCP server function on DS-Lite AFTR

5.5.10	PCP server function on DS-Lite AFTR
Test objective	The aim of this test is to check functionality of DS-Lite AFTR with embedded PCP Server.
Requirement	TR-242:R-44, R-53, R-97
Requirement	R-44. The B4 element of the RG MUST support IPv4-in-IPv6 encapsulation on

description	its WAN link as specified in RFC2473 [12]. R-53. The AFTR MUST support IPv4-in-IPv6 as specified in RFC2473 to establish the DS-Lite softwire. R-97: The device implementing CGN function MUST support Port Control Protocol (PCP) Server behavior as specified in RFC 6887 [27].
Device under test	DS-Lite AFTR device in Figure 2
Test configuration	**Test Setup -** Figure 2 **Pre-conditions:** 1) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode. 2) The probes are ready to analyze the IPv4 and IPv6 packets. 3) The DS-Lite AFTR device embeds a PCP server function. The PCP Server is being enabled. 4) IPv4-Host1 embeds a PCP client function and allows manual configuration for the PCP client. **Test Conditions:** 1) IPv4 address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode, and the retrieving mode of IPv6 address is set to DHCPv6 mode if FQDN is configured on the DHCPv6 server (step 3 above). 6) NAT44 is configured on DS-Lite AFTR device. 7) Make sure that PCP server function is activated on the DS-Lite AFTR device. 8) Make sure that PCP client function is activated on IPv4-Host1. 9) Configure the PCP Server address on IPv4-Host1. 10) IPv4-Host1's IP address is a1'.b1'.c1'.d1' IPv4-Host2's IP address is a2'.b2'.c2'.d2' 11) DS-Lite B4-1's IPv6 address is v6.b4-1. DS-Lite B4-2's IPv6 address is v6.b4-2.
Test procedure	1) DS-Lite B4-1 and DS-Lite B4-2 start IP connection.

	2) Check the IPv4-in-IPv6 tunnel entries on DS-Lite B4-1, DS-Lite B4-2 and DS-Lite AFTR device via EMF (Equipment Management Function). 3) Note the availability of DS-Lite AFTR IPv4 address A1.B1.C1.D1, port X1 on the subnet with IPv4-Host3. 4) Configure TG3 sending IPv4 traffic with destination address A1.B1.C1.D1 and destination port X1. 5) Check the NAT address mapping table on the DS-Lite AFTR device via EMF (Equipment Management Function) or by analyzing the packets via the probe p5 or internal hosts (IPv4-Host1 and IPv4-Host2). 6) Configure on IPv4-Host1 such that the PCP client will communicate with the PCP server on DS-Lite AFTR device to create a mapping: external A1.B1.C1.D1:X1 and internal v6.b4-1:a1'.b1'.c1'.d1':x1'. 7) Check the NAT address mapping table on the DS-Lite AFTR device via EMF (Equipment Management Function). 8) Configure TG3 sending IPv4 traffic with destination address A1.B1.C1.D1 and destination port X1. 9) Analyze the packets via the probes p5, p1 and IPv4-Host1. 10) Analyze the packets via the probes p3 and IPv4-Host2.
Expected result	1) At step 1, the IP connection is established successfully. 2) At step 2, IPv4-in-IPv6 tunnels establish successfully on DS-Lite B4-1, DS-Lite B4-2, and DS-Lite AFTR. The related tunnel entries are created with the IPv6 tunnel addresses being set according to the tunnel end's IPv6 address. 3) At step 5, the NAT address mapping table on the DS-Lite AFTR device should have no entries at this point since there was no connection initiated from the internal hosts nor any PCP Request send yet. Since there is no entry in the DS-Lite AFTR NAT address mapping table all traffic generated by TG3 should NOT be forwarded by the DS-Lite AFTR device: there should be no packets received by probe p5 or internal hosts (IPv4-Host1, IPv4-Host2). 4) At step 7, the NAT address mapping table on the DS-Lite AFTR device should have one entry created as a result of the PCP map request send by IPv4-Host1: external A1.B1.C1.D1:X1 and internal v6.b4-1:a1'.b1'.c1'.d1':x1'. 5) At step 9, the packets captured by the probe p5, (all IPv4 packets generated by TG3) are in IPv4-in-IPv6 tunnel encapsulation format with the source IPv6 address being the DS-Lite AFTR device's IPv6 address and the destination IPv6 address being the DS-Lite B4-1's IPv6 address. The packets captured by the probe p1 are the same as the packets originally sent by TG3 except the destination IPv4 address because it is changed by NAT.

	All the traffic generated by TG3 should be received by the IPv4-Host1 only. 6) At step 10, there should be no traffic received by neither probe p3 nor IPv4-Host2. Note: 1) an'.bn'.cn'.dn':xn' indicates the IPv4 private address and port in Network-1 or Network-2. 2) An.Bn.Cn.Dn:Xn indicates the IPv4 public address and port of Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.11 IPv6 Datagram Filter Function for DS-Lite CG-NAT44

5.5.11	IPv6 datagram Filter Function for DS-Lite CG-NAT44
Test objective	The purpose of this test is to check DS-Lite CG-NAT44 device filter incoming IPv6 datagram based on the IPv6 prefix. The IPv6 packets are filtered based on the IPv6 prefix, which includes the native IPv6 packets from subscribers and the IPv6 packets from DS-Lite tunnel.
Requirement	TR-242:R93,R-95
Requirement description	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. 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 datagram, based at least on the IPv6 prefix.
Device under test	The CG-NAT44 device that is co-located with the DS-Lite AFTR in Figure 2 .
Test configuration	**Test Setup - Figure 2** **Pre-conditions:** 1) DS-Lite B4-1 and B4-2 are configured in router mode. 2) The traffic generator is ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) DS-Lite B4-1 and B4-4 device are configured in DS-Lite mode. The IPv4

	addresses for Network-1 and Network-2 are configured. 2) The IPv6 address of AFTR device is configured on DS-Lite B4-1 and DS-Lite B4-2 device. The IPv6 addresses for Network-1 and Network-2 are configured. 3) The IPv6 address pool is configured on DHCPv6 server, and the IPv6 address IPv6_A1 is allocated to DS-Lite B4-1, the IPv6 address IPv6_A2 is allocated to DS-Lite B4-2 device. 4) The IPv6 address for Network-3 is configured on DS-Lite AFTR device, the NAT44 function and the IPv4 public address pool of Network-4 are configured on DS-Lite AFTR device.
Test procedure	1) DS-Lite B4-1 and DS-Lite B4-2 start the IP connection. 2) TG1 and TG2 send the IPv4 traffic stream simultaneously, the destination IPv4 addresses of the streams are in Network-4. Check the received traffic on TG3. 3) The IPv6 prefix -1 is configured to filter the IPv6 packets from DS-Lite tunnel on the DS-Lite AFTR device. This prefix specifies the packets with the source address IPv6_A1 are permitted, other IPv6 packets are denied. 4) TG1 and TG2 send IPv6 traffic stream simultaneously, the destination IPv6 addresses of both streams are in the Network-5.The source IPv6 address of traffic sent by TG1 is IPv6_S1, and the source IPv6 address of traffic sent by TG2 is IPv6_S2. Check the traffic received on TG4. 5) The IPv6 prefix-2 is configured to filter the native IPv6 packets from subscribers on the DS-Lite AFTR. This specifies that the packets with the source address of IPv6_S1 are permitted, and other IPv6 packets are denied.
Expected result	1) At step 1, DS-Lite B4-1 and DS-Lite B4-2 establish IP connection successfully. 2) At step 2, TG3 receives the IPv4 traffic streams from both TG1 and TG2 successfully. 3) At step 3, TG3 receives the IPv4 traffic stream from TG1 without any packet loss, and the stream from TG2 is discarded. 4) At step 4, TG4 receives the IPv6 traffic streams from both TG1 and TG2 successfully. 5) At step 5, TG4 receives the IPv6 traffic stream from TG1 without any packet loss, and the IPv6 stream from TG2 is discarded.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.12 DS-Lite port Limit function of DS-Lite CG-NAT44

5.5.12	DS-Lite port Limit function of DS-Lite CG-NAT44
Test objective	The purpose of this test is to check that DS-Lite CG-NAT44 device can provide a port limiting function to prevent from occupying excessive port resources.
Requirement	TR-242: R-94
Requirement description	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.
Device under test	The DS-Lite AFTR device in Figure 2.
Test configuration	**Test Setup** - Figure 2 **Pre-conditions**: 1) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode. 2) The traffic generator TG1, TG2 and TG3 are ready to simulate/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv4 address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode, the IPv4 prefix for Network-1, Network-2 and IPv6 address for Network-3 are configured. 6) NAT44 function and the IPv4 public address NAT pool of Network-4 are configured on DS-Lite AFTR device. 7) DS-Lite port number limit function is activated on DS-Lite AFTR device so as to limit the port-number (which is assigned to B4) to 500. The port limit of 500 is just a typical example. Note: the UDP mapping timer MUST be set to a sufficiently large value that the test can be completed, prior to any timeout may occur.
Test procedure	1) DS-Lite B4-1 and DS-Lite B4-2 start IP connection. 2) Check the IPv4-in-IPv6 tunnel entries on DS-Lite B4-1, DS-Lite B4-2 and DS-Lite AFTR via EMF. 3) The traffic generator TG1 sends the traffic with 500 streams:

	Stream 1~500: the source ports of all these 500 streams are different from each other. The destination IPv4 addresses of all these 500 streams are A3.B3.C3.D3 of Network-4. Check the received traffic on TG3. 4) Check the number of the external ports which are used on the DS-Lite AFTR device via EMF. 5) Following the steps above, the traffic generator TG1 adds 100 streams incrementally: Stream 501~600: the source ports of each stream are different from each other. The destination IPv4 addresses of all these 100 streams are A3.B3.C3.D3 of Network-4. Check the received traffic on TG3. 6) Check the number of external ports which are used on the DS-Lite AFTR device via EMF. 7) The traffic generator TG2 simulates another user by sending 500 traffic streams: Stream 1~500: the source ports of each stream are different from each other. The destination IPv4 addresses of all these 500 streams are A3.B3.C3.D3 of Network-4. Check the received traffic on TG3. 8) Check the number of the external ports which are used on the DS-Lite AFTR device via EMF.
Expected result	1) At step 1, IP connections are established successfully. 2) At step 2, two DS-Lite tunnel entries with the IPv6 addresses of DS-Lite B4-1 and DS-Lite B4-2 are created on DS-Lite AFTR device. 3) At step 3, the traffic generator TG3 receives the 500 traffic streams from TG1 successfully without any packet loss. 4) At step 4, the DS-Lite AFTR device completes the address translation successfully. The number of the created NAT entries is 500, and each internal IPv4 address only maps to one external IPv4 address, all 500 external ports are occupied. 5) At step 5, the traffic generator TG3 should drop the new 100 traffic streams from TG1. 6) At step 6, no new entries should be created on the DS-Lite AFTR device, because the number of the external ports which are assigned to DS-Lite B4-1 has reached the port limit. 7) At step 7, the traffic generator TG3 receives 500 traffic streams from TG2 successfully without any packet loss. 8) At step 8, another 500 new NAT entries should be created on DS-Lite AFTR device, and the DS-Lite CG-NAT44 device assigns 500 external ports to DS-Lite B4-2. Note:

	1) an.bn.cn.dn indicates the IPv4 private address in Network-1 2) An.Bn.Cn.Dn indicates the IPv4 public address in Network-4
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.13 AFTR with 40-byte MTU Increment on B4 Facing Interfaces

5.5.13	AFTR with 40-byte MTU Increment on B4 Facing Interfaces
Test objective	The aim of this test is to check whether the DS-Lite AFTR device supports a MTU increased by at least 40 bytes on B4 facing interfaces.
Requirement	TR-242: R-56
Requirement description	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.
Device under test	DS-Lite B4 devices and DS-Lite AFTR device in Figure 2.
Test configuration	**Test Setup** - Figure 2 **Pre-conditions:** 1) DS-Lite B4-1 is configured in router mode. 2) The traffic generator TG1 and TG3 are ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv4 public address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 is configured in DS-Lite mode, the IPv4 prefix for Network-1 and IPv6 address for Network-3 are configured. 6) NAT44 is configured on DS-Lite AFTR device. The IPv4 public address NAT pool of Network-4 is configured. Only one public IPv4 address A1.B1.C1.D1 is included in the pool. 7) Configure the IPv6 MTU on the DS-Lite AFTR device facing DS-Lite B4-1 to 1440 bytes. 8) Enable FTP or FTTP server function on IPv4-Host3.

Test procedure	1) B4-1 starts IP connection. 2) TG1 sends a traffic stream, in which the source IPv4 address is a1.b1.c1.d1 of Network-1, the source port number is x1, the destination IPv4 address is A2.B2.C2.D2 of Network-4, and the packet size is 1400 bytes. So the packet size of the IPv4-in-IPv6 packets is 1440 bytes. Capture IPv4-in-IPv6 packets originated from TG1 at probe p2. 3) Check the NAT address mapping table entry on DS-Lite AFTR device via EMF. 4) Based on the NAT address mapping table information (Note that the mapping table entry is: a1.b1.c1.d1:x1 <--> A1.B1.C1.D1:X1) obtained in step 3, TG3 sends a traffic stream, in which the source IPv4 address is A2.B2.C2.D2 of Network-4, the destination IPv4 address is A1.B1.C1.D1, destination port number is X1. Capture IPv4-in-IPv6 packets originated from TG3 at probe p5.
Expected result	1) At step 1, the IP connection is established successfully, and IPv4-Host1 accesses the FTP or HTTP services on IPv4-Host3 successfully. 2) At step 2, IPv4 packets sent by TG1, and captured at probe p2 as IPv4-in-IPv6 packets are not fragmented. 3) At step 3 on AFTR, a new NAT address mapping entry should be created as follow: a1.b1.c1.d1: x1 <----> A1.B1.C1.D1: X1 4) At step 4, IPv4 packets sent by TG3, and captured by probe p5 as IPv4-in-IPv6 packets are not fragmented. Note: 1) an'.bn'.cn'.dn':xn' indicates the IPv4 private address and port in Network-1 or Network-2. 2) An.Bn.Cn.Dn: Xn indicates the IPv4 public address and port in Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.14 Packet Fragmentation and Reassembly at B4 and AFTR device

5.5.14	Packet Fragmentation and Reassembly at B4 and AFTR device
Test objective	The aim of this test is to check whether the DS-Lite B4 and AFTR devices are capable of performing packet fragmentation and reassembly.
Requirement	TR-242: R-49, R-54
Requirement	R-49. The RG MUST be capable of performing packet fragmentation and

description	reassembly as specified in Section 7.2 of RFC 2473 [12]. R-54. The AFTR MUST be able to perform packet fragmentation and reassembly as specified in Section 7.2 of RFC2473.
Device under test	DS-Lite B4 devices and DS-Lite AFTR device in Figure 2.
Test configuration	**Test Setup** - Figure 2 **Pre-conditions:** 1) DS-Lite B4-1 is configured in router mode. 2) The traffic generator TG1 and TG3 are ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv4 public address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 is configured in DS-Lite mode, the IPv4 prefix for Network-1 and IPv6 address for Network-3 are configured. 6) NAT44 is configured on DS-Lite AFTR device, the IPv4 public address NAT pool of Network-4 is configured, only one public IPv4 address A1.B1.C1.D1 is included in the pool. 7) Set IPv6 MTU to 1400 bytes for DS-Lite tunnel on DS-Lite B4 and DS-Lite AFTR device.
Test procedure	1) DS-Lite B4-1 starts IP connection. 2) TG1 sends a traffic stream, in which the source IPv4 address is a1.b1.c1.d1 of Network-1, the source port number is x1, the destination IPv4 address is A2.B2.C2.D2 of Network-4, the DF flag filed in packets is 0, and the packets size is 1400 bytes. Capture IPv4 packets originated from TG1 as IPv4-in-IPv6 packets at probe p2, and check the IPv4 packets received by TG3. 3) Check the NAT address mapping table entry on DS-Lite AFTR device via EMF. 4) Based on the NAT address mapping table information (Note that the mapping table entry is: a1.b1.c1.d1:x1 <--> A1.B1.C1.D1: X1) obtained in step 3, TG3 sends traffic stream, in which the source IPv4 address is A2.B2.C2.D2 of Network-4, the destination IPv4 address is A1.B1.C1.D1 of Network-4, destination port number is X1, the DF flag filed in packets is 0,

	and the packets size is 1400 bytes. Capture IPv4 packets originated from TG3 as IPv4-in-IPv6 packets at probe p5, and check the IPv4 packets received by TG1.
Expected result	1) At step 1, the IP connection is established successfully. 2) At step 2, for IPv4-in-IPv6 packets captured at probe p2, fragmentation is performed and each IPv4 packet resulted in two IPv4-in-IPv6 packets. In the IPv4 packets captured by probe p6, the IPv4 packets are the same as original IPv4 packets sent by TG1. 3) At step 3 on DS-Lite AFTR device, a new NAT address mapping entry should be created as follow: a1.b1.c1.d1: x1 <----> A1.B1.C1.D1: X1 4) At step 4 in IPv4-in-IPv6 packets captured at probe p5, fragmentation is performed and each IPv4 packet resulted in two IPv4-in-IPv6 packets. In the IPv4 packets captured by probe p1, the IPv4 packets are the same as original IPv4 packets sent by TG3. Note: 1) an'.bn'.cn'.dn':xn' indicates the IPv4 private address and port in Network-1 or Network-2. 2) An.Bn.Cn.Dn: Xn indicates the IPv4 public address and port in Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.15 Rewriting the TCP MSS option of TCP packets by B4 and AFTR

5.5.15	Rewriting the TCP MSS option of TCP packets by B4 and AFTR
Test objective	The aim of this test is to check whether the value of the TCP MSS option of TCP packets can be rewritten by B4 and AFTR, respectively, when the value in the MSS option field of TCP packets is larger than the MTU on the DS-Lite softwire.
Requirement	TR-242: R-48, R-57
Requirement description	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. 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.
Device under test	DS-Lite B4 devices and DS-Lite AFTR device in Figure 2.
Test	**Test Setup** - Figure 2

configuration	**Pre-conditions:** 1) DS-Lite B4-1 is configured in router mode. 2) The traffic generator TG1 and TG3 are ready to transmit/analyze the IPv4 and IPv6 packets. **Test Conditions:** 1) IPv4 public address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 is configured in DS-Lite mode, the IPv4 prefix for Network-1 and IPv6 address for Network-3 are configured. 6) NAT44 is configured on DS-Lite AFTR device. The IPv4 public address NAT pool of Network-4 is configured. Only one public IPv4 address of A1.B1.C1.D1 is included in the pool of Network-4. 7) Set IPv6 MTU as 1400 for DS-Lite tunnel on both DS-Lite B4 and DS-Lite AFTR devices. Note: Other value for IPv6 MTU may be used as appropriate.
Test procedure	1) DS-Lite B4-1 starts IP connection. 2) TG1 and TG3 set TCP MSS value as 1500 bytes, then TG1 starts a TCP connection to TG3. 3) Capture the IPv4-in-IPv6 TCP packet originated from TG1 at probe p2. 4) Capture the IPv4-in-IPv6 TCP packet originated from TG3 at probe p5.
Expected result	1) At step 1, the IP connection is established successfully. 2) At step 3, in the IPv4-in-IPv6 TCP packets captured by probe p2, the value in TCP MSS field should be 1320 (1400-20-20-40) bytes. 3) At step 4, in the IPv4-in-IPv6 TCP packets captured by probe p5, the value in TCP MSS field should be 1320 (1400-20-20-40) bytes.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.16 PCP - Learning Public IPv4 address of the DS-Lite AFTR

5.5.16	PCP server function support on DS-Lite AFTR: Learning Public IP address assigned by the DS-Lite AFTR
Test objective	The purpose of this test is to retrieve the external IP address assigned by the DS-Lite AFTR. Note, the DS-Lite AFTR may be configured with a pool of public IP addresses. Only the (shared) address assigned by the DS-Lite AFTR to the requesting host will be returned.
Requirement	TR-242:R-97
Requirement description	R-97: The device implementing CGN function MUST support Port Control Protocol (PCP) Server behavior as specified in RFC6887 [27].
Device under test	The DS-Lite AFTR device in Figure 2. Note-1: DS-Lite AFTR device embeds a PCP server function. The PCP Server is being enabled. Note-2: IPv4-Host1 embeds a PCP client function and allows manual configuration for the PCP client.
Test configuration	**Test Setup** – Figure 2. **Preconditions:** 1) DS-Lite B4-1 is configured in router mode 2) The DS-Lite AFTR device has implemented PCP server function. 3) IPv4-Host1 has implemented PCP client function. 4) Traffic generators and probes are ready to simulate and analyze exchanged IPv4 packets **Test Conditions:** 1) IPv4 address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode, and the retrieving mode of IPv6 address is set to DHCPv6 mode if FQDN is configured on the DHCPv6 server (step 3 above). 6) NAT44 is configured on DS-Lite AFTR device. 7) Make sure that PCP server function is activated on the DS-Lite AFTR device. 8) Make sure that PCP client function is activated on IPv4-Host1.

	9) Configure the PCP Server address on IPv4-Host1. 10) IPv4-Host1's IP address is a1'.b1'.c1'.d1' 11) DS-Lite B4-1' IPv6 address is v6.b4-1
Test procedure	1) IPv4-Host1 starts the IP connection. 2) Establish IP connectivity between IPv4-Host1 and IPv4-Host3. 3) Check the NAT address mapping table on the DS-Lite AFTR device via EMF or by analyzing the packets via probe p6. 4) Note the IPv4 source address received by IPv4-Host3. 5) Process a PCP MAP Request from IPv4-Host1 to PCP Server by requesting a short-lived mapping to the Discard service (TCP/9 or UDP/9). The request lifetime is set to 30 seconds. 6) Record the value returned by the PCP server in the PCP MAP Response observed by probe p2.
Expected result	1) At the end of step 5 of the test procedure (see above) there are two entries in the mapping table on the DS-Lite AFTR device: 1a) external A1.B1.C1.D1:X1 and internal v6.b4-1:a1'.b1'.c1'.d1':x1' 1b) external A1.B1.C1.D1:9 and internal v6.b4-1:a1'.b1'.c1'.d1':9 2) At step 6, the source IPv4 address of the PCP MAP Response from the DS-Lite AFTR is the same as that of data packets sent by IPv4-Host3, both received by IPv4-Host1, i.e., A1.B1.C1.D1. Note: 1) an'.bn'.cn'.dn':xn' indicates the IPv4 private address and port in Network-1 or Network-2. 2) An.Bn.Cn.Dn: Xn indicates the IPv4 public address and port in Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

5.5.17 PCP - Request an Already Used Port

5.5.17	PCP server function support on DS-Lite AFTR : Requesting an already used port
Test objective	The purpose if this test case is to assess the behavior of the PCP Server when a port already in use is required by a PCP client. Two cases will be checked: (1) No PREFIER_FAILURE option is included in the request and, (2) PREFER FAILURE is included in the request.
Requirement	TR-242:R-97

Requirement description	R-97: The device implementing CGN function MUST support Port Control Protocol (PCP) Server behavior as specified in RFC6887.
Device under test	The DS-Lite AFTR device in Figure 2. Note-1: DS-Lite AFTR device has PCP server function. The PCP Server is being enabled. Note-2: IPv4-Host1 and IPv4-Host2 have PCP client function and allow manual configuration for PCP client.
Test configuration	**Test Setup –** Figure 2 **Preconditions:** 1) DS-Lite B4-1 and DS-Lite B4-2 are configured in router mode 2) The DS-Lite AFTR device has implemented PCP server function. 3) IPv4-Host1 and IPv4-Host2 have implemented PCP client function. 4) Traffic generators and probes are ready to simulate and analyze the IPv4 packets **Test Conditions:** 1) IPv4 address for Network-4 and IPv6 address for Network-3 are configured on DS-Lite AFTR device. 2) IPv6 address pool is configured on the DHCPv6 server. 3) FQDN (AFTR name) is configured on the DHCPv6 server (or configured manually if it is not supported on DHCPv6 server). 4) The IPv6 address for FQDN of AFTR is configured on DNS server. 5) DS-Lite B4-1 and DS-Lite B4-2 are configured in DS-Lite mode, and the retrieving mode of IPv6 address is set to DHCPv6 mode if FQDN is configured on the DHCPv6 server (step 3 above). 6) NAT44 is configured on DS-Lite AFTR device. 7) Make sure that PCP server function is activated on the DS-Lite AFTR device. 8) Make sure that PCP client function is activated on IPv4-Host1 and IPv4-Host2. 9) Configure the PCP Server address on IPv4-Host1 and IPv4-Host2. 10) IPv4-Host1's IP address is a1'.b1'.c1'.d1' IPv4-Host2's IP address is a2'.b2'.c2'.d2 11) DS-Lite B4-1' IPv6 address is v6.b4-1 DS-Lite B4-2' IPv6 address is v6.b4-2
Test procedure	The following steps are repeated for each configuration: (1)

	PREFERE_FAILURE option is included in the PCP Request, (2) PREFER_FAILURE is included in the PCP Request. 1) IPv4-Host1 and IPv4-Host2 start the IP connection respectively. 2) Make sure that port X1 for address A1.B1.C1.D1 is available on the DS-Lite AFTR device. 3) Configure on IPv4-Host1 such that the PCP client will communicate with the PCP server on the DS-Lite AFTR device to create a mapping: external A1.B1.C1.D1:X1 and internal v6:b4-1:a1.'b1'.c1'.d1':x1'. 4) Configure on IPv4-Host2 such that the PCP client will communicate with the PCP server on the DS-Lite AFTR device to create a mapping: external A1.B1.C1.D1:X1 and internal v6.b4-2:a2'.b2'.c2'.d2':x2'. 5) Note the value of the assigned port returned by the PCP server in the PCP MAP Response by analyzing IP packet observed by probes p2/p4.
Expected result	(a) PREFERE FAILURE option is not included in the request 1) At the end of step 5 of the test procedure (see above) there are two entries in the mapping table on the DS-Lite AFTR device created by PCP: 1a) external A1.B1.C1.D1:X1 and internal v6.b4-1:a1'.b1'.c1'.d1':x1'. 1b) external A2.B1.C1.D1:X2 and internal v6.b4-2:a2'.b2'.c2'.d2':x2'. 2) The value of the assigned port returned by the PCP server in the PCP MAP Response is equal to X2. 3) IPv4-Host1 is receiving all IPv4 traffic sent by TG3 on A1.B1.C1.D1:X1 4) IPv4-Host2 is receiving all IPv4 traffic sent by TG4 on A1.B1.C1.D1:X2 (b) PREFERE_FAILURE option is included in the request 1) At the end of step 5 of the test procedure (see above) there is only one entry in the mapping table on the DS-Lite AFTR device created by PCP: external A1.B1.C1.D1:X1 and internal v6.b4-1:a1'.b1'.c1'.d1':x1' 2) The PC Server returns an error "CANNOT_PROVIDE_EXTERNAL 3) IPv4-Host1 receives all IPv4 traffic sent by TG3 on A1.B1.C1.D1:X1 Note: 1) an'.bn'.cn'.dn':xn' indicates the IPv4 private address and port in Network-1 or Network-2. 2) An.Bn.Cn.Dn: Xn indicates the IPv4 public address and port in Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

6 Test Cases for Release Control

6.1 Device Under Test

- Two RG (Residential Gateway) with Release Control functionality
- Optional:
  - One DSL RG with Dual-Stack PPP functionality (Chapter 5.1.1 of TR-187 [5])
  - One DSL RG with IPv6-only PPP functionality (Chapter 5.1.2 of TR-187 [5])
  - One DSL RG with IPv4-only PPP functionality (TR-124 [3], TR-101 [2])
- One BNG that supports both IPv4 and IPv6 along with Release Control mechanism

6.2 Test Equipment

For Release Control interoperability test, the required test equipment is as follows:

- Three IPv6 hosts supporting the IPv6 stack, including handling of ICMPv6, DHCPv6, HTTP and DNS requests over IPv6.
- Three IPv4 hosts supporting the IPv4 stack, including handling of ICMP, DHCP, HTTP and DNS requests over IPv4.
  Note: all IPv4 and IPv6 hosts could be simulated using a Traffic Generator platform that is connected to the RG nodes and the BNG node, respectively. Also, an IPv4-IPv6 dual stack host may also be used.
- One Ethernet Switch
- One IPv4-IPv6 dual-stack router capable of providing server functions of DHCP, DHCPv6 (optional), DNS and RADIUS (optional)
- Traffic generator capable of generating PPP packets as well as IPv4 and IPv6 traffic.
- Protocol analyzer capable of interpreting this list of traffic types
  - IPv4 packets
  - IPv6 packets
  - PPP packets

6.3 Test Setup

This section describes the requirements of RG and BNG that support Release Control including their interfaces, configuration, etc. for the test cases. It also describes the associated network services provided by DNS server, RADIUS server, and DHCP, DHCPv6 server that are required (or optional) in the test.

Because address pool and user management can be provided directly on the BNG, the RADIUS and DHCPv6 server are optional.

Finally, it describes the functions of traffic generator and protocol analyzer that are used for the test.

For Release Control interoperability test, all network segments (Network-1, etc. in Figure 3) support both IPv4 and IPv6, i.e., dual-stack.

Two simulated home networks (Network-1 and Network-2 in Figure 3) are needed, so that customer-to-customer communication can be tested. The Network-4 in Figure 3 serves as the source and destination for test traffic.

Both BNG and RG-1/RG-2 must support Release Control mechanisms. This test also requires some network service functions, such as DHCP (IPv4 and IPv6) server function, RADIUS server function, and DNS server function.

6.4 Test Topology

Figure 3 is the test topology for all Release Control test cases; note that depending on each test case, test equipments are connected and configured as needed. The connectivity as illustrated between the devices in the figure is at IP layer.

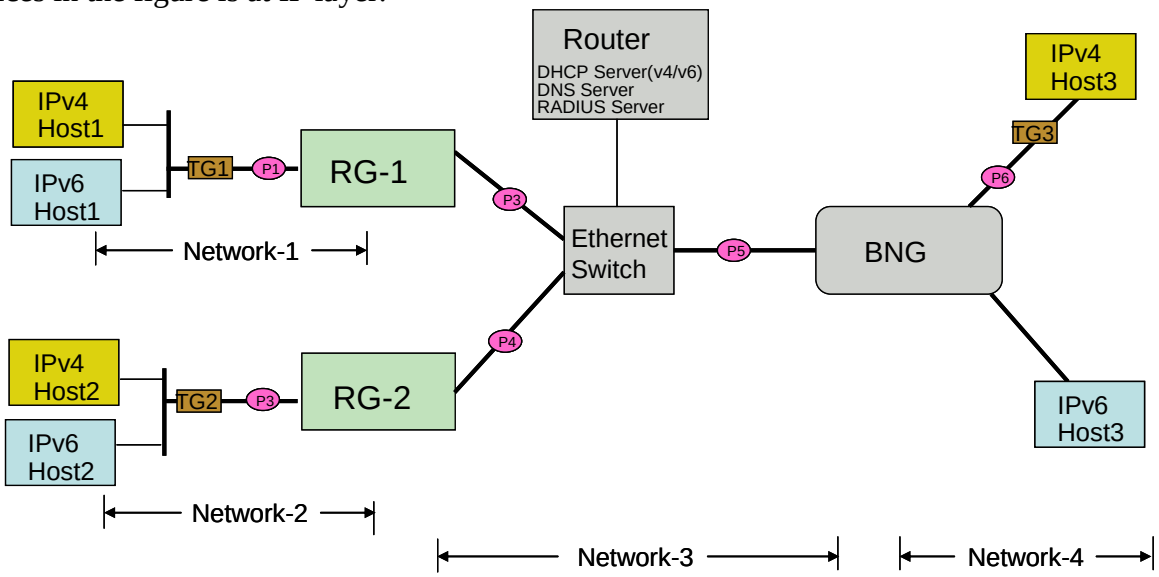

Figure 3 Release Control Test Topology

Table 3 Device and Functions Used in Release Control Test

Devices/Functions	Descriptions
RG1, RG2	The RG1 and RG2 support Release Control function.
BNG	The BNG must support all requirements for Release Control.
Ethernet Switch	This is a layer-2 Ethernet switch that connects all devices used in the test together.

Router	This is an IPv4-IPv6 dual-stack router that provides DHCP/DHCPv6 server function, DNS server function and RADIUS server function. Note alternatively, one or more of these server functions can be realized by other devices including traffic generators.
IPv4-Host1, IPv4-Host2, IPv4-Host3	These are IPv4 hosts in the Release Control test for IPv4 communication among themselves and traffic generators.
IPv6-Host1, IPv6-Host2, IPv6-Host3	These are IPv6 hosts in the Release Control test for IPv6 communication among themselves and traffic generators.
TG1/TG2/TG3	These are insertion points where traffic generator may be connected in-wire. If connected, traffic generators provide IPv4 and IPv6 traffic source and destination and communicate with IPv4 and IPv6 hosts, respectively.
Probe points (p1 to p6)	The probe points may be inserted in different points of the test network in order to verify and monitor the PPP and IP packets.
Network-1, Network-2 Network-3, Network-4	All these networks support both IPv4 and IPv6 simultaneously, i.e., dual-stack.

6.5 Test Cases

This section lists all test cases for Release Control. Note that the Release Control test cases are organized according to Release Control requirements defined in Section 8/TR-242 [6].

Test cases must cover all PPPoE and NCP states involved in Release Control. As Release Control is a part of network transition phase, testing shall be focused on this phase.

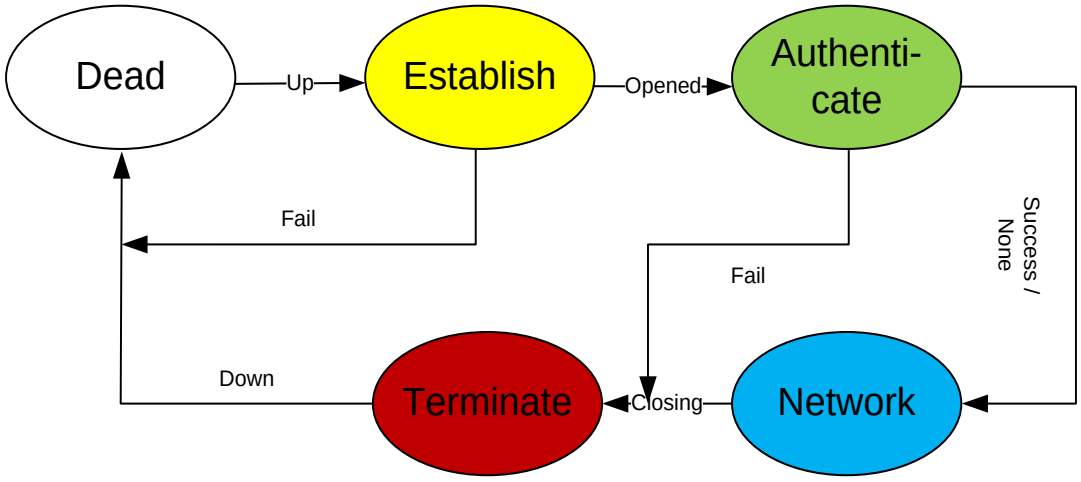

Figure 4 PPP States as defined in RFC 1661

6.5.1 DSL RG (Residential Gateway) with Release Control Functionality

6.5.1	DSL RG (Residential Gateway) with Release Control Functionality
Test objective	Release Control Basic Functionality
Requirement	The RG Must release an IPv4 Address in case of predetermined timer release.
Requirement description	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 [8]. 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 [9] and Section 3/RFC 1332 independent of the IPv6CP status according to Section 2.1/RFC4241 [16]. The timer which triggers the release of the IPv4 address MUST be configurable in minutes. 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/RFC1661 [9] and Section 3/RFC 1332 independent of the IPv6CP status according to Section 2.1/RFC 4241.
Device under test	Refer to Figure 3: RG with PPP Dual Stack capability supporting additional Release Control features per R-66 to R-69/TR-242. BNG with PPP Dual Stack capability supporting additional Release control features per R-71/TR-242.
Test configuration	**Test Setup** - Figure 3 **Test Conditions**: 1) Set up IPv4-Host 1 and IPv6-Host1 2) Set up RG-1 and configure release timer. 3) Set up BNG with address pool for IPv4-Host2 and IPv6-Host2,and optionally DNS entries for IPv4-Host3 and IPv6-Host3
Test procedure	1) Initiate Session Setup with IPv6 and IPv4 address assignment on RG-1 (through sending traffic to IPv4-Host3 and IPv6-Host3, respectively) 2) Send IPv6 Traffic from IPv6-Host1 to IPv6-Host3 3) Send IPv4 Traffic from IPv4-Host1 to IPv4-Host3 4) Stop IPv4 Traffic at IPv4-Host1 and wait for timeout (R-66, R-67) 5) Stop IPv6 traffic and wait for timeout.

Expected result	1) At step 1, PPPoE connection is established and PPP LCP state transits from Dead to Network phase. 2) At step 2 - IPv6 address assignment, pull up IPv6 without IPv4 Session a) IPv6CP setup and messaging b) Configuration of IPv6 parameters via SLAAC and DHCPv6 c) No IPv4 connectivity 3) At step 3, IPv4 address assignment, pull up IPv4 with existing IPv6 session a) IPCP setup and messaging b) Configuration of IPv4 parameters c) No change in IPv6 connectivity 4) At step 4, teardown of IPv4 Session with active IPv6 Session a) IPCP Termination b) No change in IPv6 connectivity 5) At step 5, PPP LCP Terminated after the timeout.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

6.5.2 DSL IPv4-only RG

6.5.2	DSL IPv4-only RG
Test objective	Release Control – Backward compatibility with Dual-Stack RG
Requirement	The dual stack RG without Release Control capabilities must operate on a Release Control capable BNG.
Requirement description	R-66. Not valid for this test case. R-67. Not valid for this test case. R-68. The RG MUST support PPP according to RFC 1332 [8]. R-69. Not valid for this test case. 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/RFC1661 [9] and Section 3/RFC 1332 independent of the IPv6CP status according to Section 2.1/RFC 4241 [16].
Device under test	Refer to Figure 3: RG With PPP IPv4 capability without Release Control functionality,

	supporting R-68/TR-242 BNG With PPP Dual Stack capability supporting additional Release control features R-71/TR-242
Test configuration	**Test Setup** - Figure 3 **Test Conditions:** 1) Set up IPv4 2) Set up RG1. 3) Set up BNG with address pool for IPv4-Host1 and optional DNS entries for IPv4- Host3
Test procedure	1) Initiate Session Setup with IPv4 address assignment (through sending traffic to IPv4-Host3) 2) Send IPv4 Traffic from IPv4-Host1 to IPv4-Host3 3) Terminate IPv4 session
Expected result	1) At step 1, PPPoE connection is established and PPP LCP state transits from Dead to Network phase. 2) At step 2 - IPv4 address assignment, pull up IPv4 without existing IPv4 session a) IPCP setup and messaging b) Configuration of IPv4 parameters 3) At step 3 - LCP and IPCP terminated.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

6.5.3 RG with Dual-Stack PPP functionality but without Release Control

6.5.3	RG with Dual-Stack PPP functionality but without Release Control
Test objective	Release Control – Backward compatibility with Dual-Stack RG
Requirement	The dual stack RG without Release Control capabilities must operate on a Release Control capable BNG.
Requirement description	RG must not support R-66, R-67 and R-69 R-68. The RG MUST support PPP according to RFC 1332 [8]. 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 [9] and Section 3/RFC 1332 independent of the IPv6CP status according to Section 2.1/RFC 4241 [16].

Device under test	Refer to Figure 3: RG With PPP Dual Stack without additional release Control features R-66 to R-69/TR-242. BNG With PPP Dual Stack capability supporting additional release control features R-72/TR-242.
Test configuration	**Test Setup** - Figure 3 **Test Conditions:** 1) Set up IPv4 and IPv6 on IPv4-Host1 and IPv6-Host1 respectively 2) Set up BNG with address pool for IPv4-Host1 and IPv6-Host1, and optionally DNS entries for IPv4-Host3 and IPv6-Host3
Test procedure	1) Initiate Session Setup with IPv4 and IPv6 address assignment (through sending traffic to IPv4-Host3 and IPv6-Host3 respectively) 2) Send IPv6 traffic from IPv6-Host1 to IPv6-Host3 3) Send IPv4 Traffic from IPv4-Host1 to IPv4-Host3 4) Stop IPv4 traffic at IPv4-Host1 and wait for timeout (R-66, R-67) 5) Stop IPv6 traffic at IPv6-Host1 and wait for timeout.
Expected result	1) At step 1, PPPoE connection is established and PPP LCP state transits from Dead to Network phase. 2) At step 2 - IPv6 address assignment a) Pull up IPv6 b) IPv6CP setup and messaging c) Configuration of IPv6 parameters via SLAAC and DHCP 3) At step 3 - IPv4 address assignment a) Pull up IPv4 b) IPCP setup and messaging c) Configuration of IPv4 parameters d) No change in IPv6 connectivity 4) At step 4, no change in IPv4 connectivity. 5) At step 5, LCP session terminated after timeout.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

6.5.4 Compatibility with IPv6-only RG

6.5.4	DSL IPv6-only RG
Test objective	Release Control – Backward compatibility with IPv6-only RG
Requirement	The IPv6-only RG without Release Control capabilities must operate on a Release Control capable BNG.
Requirement description	RG must not support R-66, R-67 and R-69 R-68. The RG MUST support PPP according to RFC 1332 [8]. 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 [9] and Section 3/RFC 1332 independent of the IPv6CP status according to Section 2.1/RFC 4241 [16].
Device under test	Refer to Figure 3: RG With PPP IPv6 capability without Release Control functionality, supporting R-68/TR-242 BNG With PPP Dual Stack capability supporting additional Release control features R-71/TR-242
Test configuration	**Test Setup** - Figure 3 **Test Conditions:** 1) Set up IPv6 2) Set up RG1 3) Set up BNG with address pool and IPv6-Host3, and optional DNS entries for IPv4- Host 3
Test procedure	1) Initiate Session Setup with IPv6 address assignment (through sending traffic to IPv6-Host3) 2) Send IPv6 Traffic from IPv6-Host1 to IPv6-Host3 3) Terminate IPv6 Session
Expected result	1) At step 1, PPPoE connection is established and PPP LCP state transits from Dead to Network phase. 2) At step 2 - IPv6 address assignment, pull up IPv6 a) IPv6CP setup and messaging b) Configuration of IPv6 parameters 3) At step 3 - IPv6 session is terminated; PPP LCP session is terminated.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

7 Test Cases for Dual-Stack with CGN NAT44

7.1 Device Under Test

- Two RG (Residential Gateway) with NAT44 function
- One BNG that supports both IPv4 and IPv6, and with an embedded NAT44 function

7.2 Test Equipment

For dual-stack with CGN NAT44 interoperability test, the required test equipment is follows:

- Three IPv6 hosts supporting the IPv6 stack, including handling of ICMPv6, DHCPv6, HTTP and DNS requests over IPv6.
- Three IPv4 hosts supporting the IPv4 stack, including handling of ICMP, DHCP, HTTP and DNS requests over IPv4.
  Note: all IPv4 and IPv6 hosts could be simulated using a Traffic Generator platform that is connected to the RG nodes and the BNG node, respectively. Also, an IPv4-IPv6 dual stack host may also be used.
- One Ethernet Switch
- One IPv4-IPv6 dual-stack router capable of providing server function of DHCP/DHCPv6, DNS and RADIUS
- Traffic generator capable of generating PPP packets as well as IPv4 and IPv6 traffic.
- Protocol analyzer capable of interpreting this list of traffic types
  - IPv4 packets
  - IPv6 packets

7.3 Test Setup

This section describes the requirements of RG and dual-stack capable BNG with embedded CGN (NAT44) function including their interfaces, configuration, etc. for the test cases. Note the CGN functions and requirements are according to those in Chapter 7/TR-242 [6]. Note also the CGN function is only applicable to IPv4 networking in a broadband network.

For dual-stack BNG and CG-NAT44 interoperability test, all network segments (Network-1, etc. in Figure 5) support both IPv4 and IPv6, i.e., dual-stack.

Two simulated home networks (Network-1 and Network-2 in Figure 5) are needed, so that customer-to-customer communication can be tested. The Network-4 in Figure 5 serves as the source and destination for test traffic.

This test requires a CGN-NAT function co-located on the BNG.

This test also requires some network service functions, such as DHCP (IPv4 and IPv6) server function, RADIUS server function, and DNS server function.

7.4 Test topology

Figure 5 is the topology for all dual-stack with BNG and CG-NAT44 test cases; note that depending on each test case, test equipment is connected and configured as needed. The connectivity as illustrated between the devices in the figure is at IP layer.

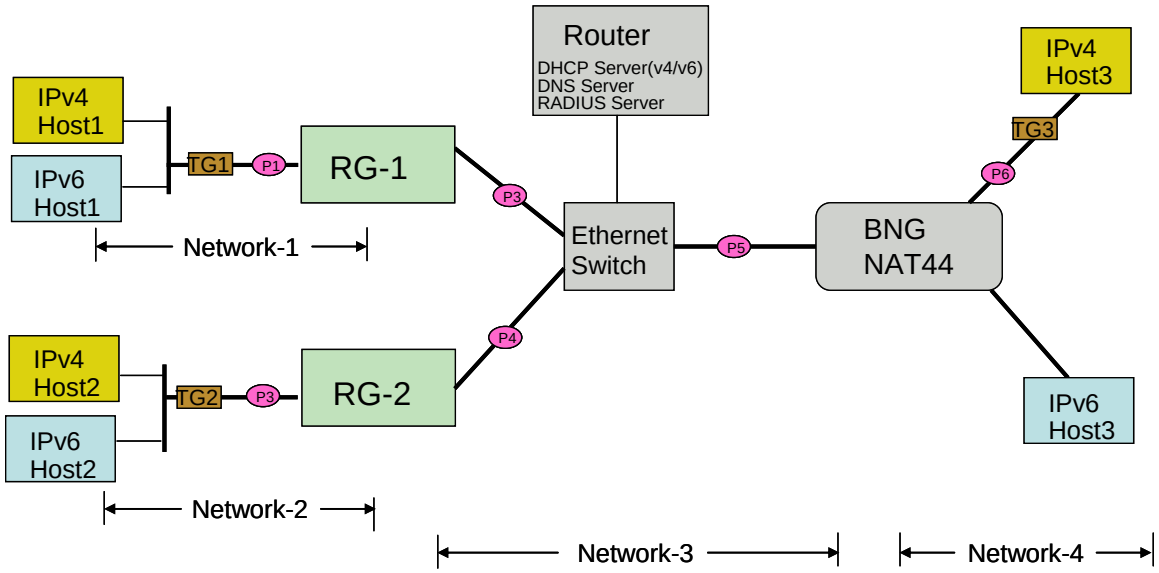

Figure 5 Dual-stack BNG and CG-NAT44 Test Topology

Table 4 Device and Functions Used in Dual-Stack BNG with CGN Test

Devices/Functions	Descriptions
RG1, RG2	These are Residential Gateways running in router mode (i.e., with NAT44 function). At least two units are required in order to allow testing of customer-to-customer traffic.
BNG	The BNG must support both IPv4 and IPv6
Ethernet Switch	This is a layer-2 Ethernet switch that connects all devices used in the test together.
Router	This is an IPv4-IPv6 dual-stack router that provides DHCP/DHCPv6 server function, DNS server function and RADIUS server function. Note alternatively, one or more of these server functions can be realized by other devices including traffic generators.
IPv4-Host1, IPv4-Host2, IPv4-Host3	These are IPv4 hosts which are used to test IPv4 communication among the hosts and traffic generators.
IPv6-Host1, IPv6-Host2,	These are IPv6 hosts which are used to test IPv4

IPv6-Host3	communication among the hosts and traffic generators.
TG1/TG2/TG3	These are insertion points where traffic generator may be connected in-wire. If connected, traffic generators provide IPv4 traffic source and destination and communicate with IPv4 hosts, respectively.
Probe points (p1 to p6)	The probe points may be inserted in different points of the test network in order to verify and monitor the IPv4 packets.
Network-1, Network-2 Network-3, Network-4	All these networks support both IPv4 and IPv6 simultaneously, i.e., dual-stack.

7.5 Test Cases

This section lists all test cases for dual-stack BNG with CGN NAT44. Note that the test cases are organized according to requirements defined in Section 7/TR-242.

7.5.1 Dual-Stack model with shared service provider IPv4 address Function

7.5.1	Dual-Stack model with shared service provider IPv4 address function
Test objective	The aim of this test is to check IPv6 forwarding function as defined in TR-187 [5], TR-177 [4], and TR-124 [3] in a dual-stack environment with CG-NAT44 function enabled.
Requirement	TR-242:R-65
Requirement description	R-65: When implementing CGN on the BNG, the BNG MUST support the CGN requirements specified in Section 9/TR-242.
Device under test	BNG as referred in Figure 5
Test configuration	**Test Setup** - Figure 5. **Preconditions:** 1) RG-1 and RG-2 are configured in router mode 2) Traffic generator is ready to simulate/analyze the IPv4 packets **Test Conditions:** 1) IPv4 and IPv6 stack are configured on RG-1 and RG-2 2) IPv6 address pool is configured on the DHCPv6 server. 3) The IPv4 address pool of Network-3 is configured on the DHCPv4 server. 4) The NAT44 function and the IPv4 public address pool of Network-4 are configured on the NAT44 device (It is recommended that the address pool

	contains only one IPv4 public address). 5) The IPv4 public address of Network-4 is configured, and HTTP and FTP services are enabled on IPv4-Host3 6) IPv6 address is configured, and HTTP and FTP services are enabled on IPv6-Host3
Test procedure	1) Establish IPv4 and IPv6 IP connection from RG-1 and RG-2 respectively. 2) IPv4-Host1 and IPv4-Host2 try to access HTTP or FTP service on IPv4-Host3 in the Internet respectively. 3) IPv6-Host1 and IPv6-Host2 try to access HTTP or FTP service on IPv6-Host3 4) Check the NAT address mapping table for correct translation on the NAT44 device via EMF or by analyzing the packets via the probes p5 and p6.
Expected result	1) At step 1, the IPv4 and IPv6 connection are established successfully. RG-1 and RG-2 are assigned at least one IPv6 address each by DHCPv6 server RG-1 and RG-2 successfully obtain IPv4 private addresses of the Network-3 from the DHCPv4 server: RG-1's IPv4 address: a1.b1.c1.d1 RG-2's IPv4 address: a2.b2.c2.d2, and a1.b1.c1.d1 ≠ a2.b2.c2.d2, and within the range of address pool of Network-3. 2) At step 2, IPv4-Host1 and IPv4-Host2 successfully access the HTTP service on IPv4-Host3 in the internet. 3) At step 3, IPv6-Host1 and IPv6-Host2 successfully access the HTTP or FTP service on IPv6-Host3 4) At step 4, the NAT44 device successfully translates the IPv4 private addresses and ports of Network-3 into the IPv4 public addresses and ports of Network-4, specifically, the two different IPv4 private addresses of Network-3 are mapped to the same IPv4 public address of Network-4: For RG-1: a1.b1.c1.d1: x1 <----> A1.B1.C1.D1: X1 For RG-2: a2.b2.c2.d2: x2 <----> A2.B2.C2.D2: X2 and A1.B1.C1.D1 = A2.B2.C2.D2 and X1 ≠ X2 Note: 1) an.bn.cn.dn:xn indicates the IPv4 private address and port of the Network-3.

	2) An.Bn.Cn.Dn:Xn indicates the IPv4 public address and port of Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8 Test Cases for CGN (NAT44)

8.1 Device Under Test

- Two RGs. Note: In this test, only router-mode RG (with NAT44 function) is used.
- A CG-NAT44 device.

8.2 Required Test Equipment

For NAT44 interoperability test, the required test equipment is follows:

- Six IPv4 hosts supporting the IPv4 stack, including handling of ICMP, DHCP, HTTP and DNS requests over IPv4.
  Note: all IPv4 hosts could be simulated using a Traffic Generator platform that is connected to the RG nodes and the NAT44 node, respectively.

- One Ethernet Switch
- One IPv4 router capable of providing server function of DHCP, DNS, RADIUS.
- Traffic generator capable of generating IPv4 packets.
- Protocol analyzer capable of interpreting IPv4 packets.

8.3 Test Setup

This section describes the requirements of RG and CGN (NAT44) including their interfaces, configuration, etc. for the test cases. Note the CGN functions and requirements are according to those in Chapter 9/TR-242 [6]. Note also the CGN function is only applicable to IPv4 networking in a broadband network but there are different scenarios as follows:

1) A CGN function may be deployed together with 6rd mechanism.
2) A CGN function may be deployed together with DS-Lite mechanism.
3) A CGN function may be deployed in a dual-stack broadband network.
4) A CGN function may be deployed in an IPv4-only broadband network.
5) A CGN function may be standalone or co-located with a BNG, a 6rd-BR, a DS-Lite AFTR.

For CG-NAT44 interoperability test, all network segments (Network-1, etc. in Figure 6) support IPv4 only.

Two simulated home networks (Network-1 and Network-2 in Figure 6) are needed, so that customer-to-customer communication can be tested. The Network-4 in Figure 6 serves as the source and destination for test traffic.

The CG-NAT44 device is either a stand-alone platform or co-located with a BNG or router.

This test also requires some network service functions, such as DHCP server function, RADIUS server function, and DNS server function.

8.4 Test Topology

Figure 6 is the topology for all CG-NAT44 test cases; note that depending on each individual test case, network equipments are connected and configured as needed. The connectivity as illustrated between the devices in the figure is at IP layer.

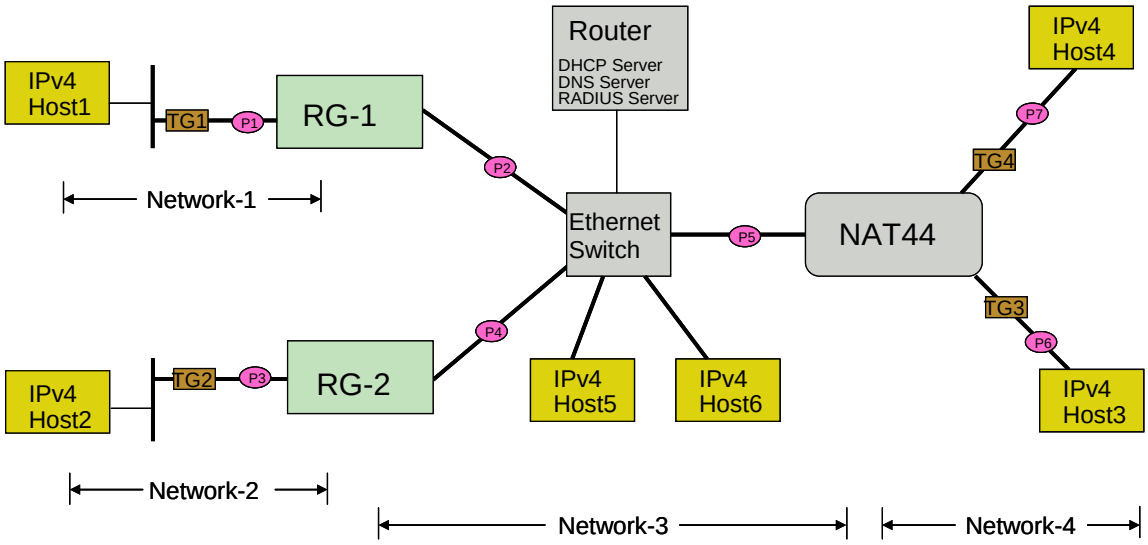

Figure 6 Device and Functions Used in CG-NAT44 Test

Table 5 Device and Functions Used in CG-NAT44 Test

Devices/Functions	Descriptions
RG1, RG2	These are Residential Gateways running in router mode (i.e., with NAT44 function). At least two units are required in order to allow testing of customer-to-customer traffic.
NAT44	A device that performs CG-NAT44 function. Note the function may be located on a BNG or on a separate platform.
Ethernet Switch	This is a layer-2 Ethernet switch that connects all devices used in the test together.
Router	This is an IPv4 router that provides DHCP server function, DNS server function and RADIUS server function. Note alternatively, one or more of these server functions can be realized by other devices including

	traffic generators.
IPv4-Host1, IPv4-Host2, IPv4-Host3, IPv4-Host 4, IPv4-Host5, IPv4-Host 6	These are IPv4 hosts which are used to test IPv4 communication among the hosts and traffic generators.
TG1/TG2/TG3/TG4	These are insertion points where traffic generator may be connected in-wire. If connected, traffic generators provide IPv4 traffic source and destination and communicate with IPv4 hosts, respectively.
Probe points (p1 to p7)	The probe points may be inserted in different points of the test network in order to verify and monitor the IPv4 packets.
Network-1, Network-2 Network-3, Network-4	All these networks are IPv4-only.

8.5 Test Cases

This section lists all test cases for CG-NAT44. Note that the test cases are organized according to requirements defined in Section 9/TR-242.

8.5.1 CG-NAT44 Network Address Port Translation Function

8.5.1	CG-NAT44 Network Address Port Translation Function
Test objective	The aim of this test is to check NAPT function for CG-NAT44
Requirement	TR-242:R-73
Requirement description	R-73: The CG-NAT44 device MUST implement NAT44, based on NAPT as defined in RFC2663 [13].
Device under test	The CG-NAT44 device in Figure 6.
Test configuration	**Test Setup** - Figure 6. **Preconditions:** 1) RG-1 and RG-2 are configured in router mode 2) Traffic generator is ready to simulate/analyze the IPv4 packets **Test Conditions:** 1) The DHCP and NAT44 functions are configured on RG-1 and RG-2 2) The IPv4 private address pool for Network-1 and Network-2 are configured on the DHCP server respectively.

	3) The NAT44 function and the IPv4 public address pool for Network-3 are configured on the NAT44 device (It is recommended that the address pool contains only one IPv4 public address). 4) The IPv4 public address is configured, and HTTP and FTP services are enabled on IPv4-Host3
Test procedure	1) RG-1 and RG-2 start the IP connection respectively. 2) IPv4-Host1 and IPv4-Host2 try to access the HTTP service on IPv4-Host3 in the Internet respectively. 3) Check the NAT address mapping table for correct translation on the NAT44 device via EMF or by analyzing the packets via the probes p5 and p6.
Expected result	1) At step 1, the IP connection is established successfully. 2) At step 2, IPv4-Host1 and IPv4-Host2 successfully access the HTTP service on IPv4-Host3. 3) At step 3, the IPv4 private addresses of Network-1 and Network-2 are successfully assigned to IPv4-Host1 and IPv4-Host2: IPv4-Host1's IPv4 address: a1 '. b1'. c1 '. d1' IPv4-Host2's IPv4 address: a2 '. b2'. c2 '. d2' RG-1 and RG-2 successfully obtain IPv4 private addresses of Network-3 from the DHCP server: RG-1's IPv4 address: a1.b1.c1.d1 RG-2's IPv4 address: a2.b2.c2.d2 and a1.b1.c1.d1 ≠ a2.b2.c2.d2, and within the range of address pool of Network-3. The NAT44 device successfully translates the IPv4 private addresses and ports of Network-3 into the IPv4 public addresses and ports of Network-4, specifically, the two different RG's IPv4 private addresses of Network-3 are mapped to the same IPv4 public addresses of Network-4: For RG-1: a1.b1.c1.d1: x1 <----> A1.B1.C1.D1: X1 For RG-2: a2.b2.c2.d2: x2 <----> A2.B2.C2.D2: X2 and A1.B1.C1.D1 = A2.B2.C2.D2 and X1 ≠ X2 Note: 1) an.bn.cn.dn:xn indicates the IPv4 private address and port of Network-3. 2) An.Bn.Cn.Dn:Xn indicates the IPv4 public address and port of

	Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.2 CG-NAT44 Full cone NAT mode of address translation

8.5.2	CG-NAT44 Full cone NAT mode of address translation
Test objective	The aim of this test is to check 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). And any external host can access the internal host by using this address mapping.
Requirement	TR-242:R-77, R-78
Requirement description	R-77: The CG-NAT44 device MUST have an "Endpoint-Independent Mapping" behavior as specified as REQ-1 in RFC4787 [18]. R-78: The CG-NAT44 device MUST have an "Endpoint-Independent Filtering" behavior as specified as REQ-8 in RFC4787.
Device under test	The CG-NAT44 device in Figure 6.
Test configuration	**Test Setup** - Figure 6. **Preconditions:** 1) RG-1 and RG-2 are configured in router mode 2) Traffic generator is ready to simulate/analyze the IPv4 packets **Test Conditions:** 1) The IPv4 private address pool of Network-3 is configured on the DHCP server 2) IPv4-Host5 and IPv4-Host6 are configured with the IPv4 private addresses of Network-1 and Network-2 respectively, and enabled with the HTTP and FTP services. 3) IPv4-Host3 and IPv4-Host4 are configured with the IPv4 public addresses of Network4, and enabled with the HTTP and FTP services. 4) The NAT mode is set to full-cone and the IPv4 public address pool of Network-4 is configured on the NAT44 device.
Test procedure	1) IPv4-Host5 tries to access the HTTP service on IPv4-Host3 in the internet and create the corresponding NAT address mapping table. 2) Check the NAT address mapping table on the NAT44 device via EMF or by analyzing the packets via the probes p5 and p6.

	3) IPv4-Host3 and IPv4-Host4 try to access the HTTP service on IPv4-Host5 in Network-3 respectively. 4) IPv4-Host5 tries to access the HTTP service on IPv4-Host4 in Network4 to create the NAT address mapping table. 5) Check the NAT address mapping table on the NAT44 device via EMF or by analyzing the packet via the probes p5 and p7. 6) IPv4-Host3 and IPv4-Host4 try to access the HTTP service on IPv4-Host6 in Network-3 respectively.
Expected result	1) At step 1, IPv4-Host5 successfully accesses the HTTP service on IPv4-Host3 in Network-4. 2) At step 2, the NAT44 device successfully completes the address translation for IPv4-Host5, the newly created NAT address mapping entry is: a1.b1.c1.d1: x1 <----> A1.B1.C1.D1: X1. 3) At step 3, IPv4-Host3 and IPv4-Host4 successfully access HTTP service on IPv4-Host5 in Network-3. 4) At step 4, IPv4-Host5 successfully access HTTP service on IPv4-Host4 in Network-4. 5) At step 5, the NAT44 device successfully translates the private address and port of Network-3 into the public address and port of Network-4. No new entry is created this time. It is the same NAT address mapping in Step2: a1.b1.c1.d1: x1 <----> A1.B1.C1.D1: X1 6) IPv4-Host3 and IPv4-Host4 can't access HTTP service on IPv4-Host6 in Network-3. Note: 1) an.bn.cn.dn:xn indicates the IPv4 private address and port of Network-3 2) An.Bn.Cn.Dn:Xn indicates the IPv4 public address and port of Network-4
Pass/Fail	Pass: The expected result was observed Fail: The Result was different from the expected result

8.5.3 CG-NAT44 High Availability

8.5.3	CG-NAT44 High Availability
Test objective	The aim of this test is to check high availability requirement of CG-NAT44
Requirement	TR-242:R-90
Requirement description	R-90: The CG-NAT44 network architecture MUST avoid single points of failure.

Device under test	The CG-NAT44 device in Figure 6. Note that the device must include hot-standby element. Note also that the implementation to support that requirement varies.
Test configuration	**Test Setup** - Figure 6. **Preconditions**: 1) RG-1 and RG-2 are configured in router mode 2) The NAT44 device has implemented hot-standby mechanism, which is proprietary since there is no standard so far in the industry, and so the details are not shown in Figure 6. 3) Traffic generator is ready to simulate/analyze the IPv4 packets **Test Conditions**: 1) Make sure that the hot-standby function is activated on the NAT44 device. 2) The DHCP and NAT44 functions are configured on RG-1 and RG-2 3) The IPv4 private address pool for Network-3 is configured on the DHCP server. 4) The NAT44 function and the IPv4 public address pool for Network-4 are configured on the NAT44 device. 5) The IPv4 public address is configured, and HTTP and FTP services are enabled on IPv4-Host3 and IPv4-Host4 respectively.
Test procedure	1) RG-1 and RG-2 start the IP connection respectively. 2) IPv4-Host1 and IPv4-Host2 try to access the HTTP service on IPv4-Host3 and IPv4-Host4 in the Internet respectively. 3) Check the NAT address mapping table on the NAT44 device. Identify the hardware component (e.g., a hardware module) or the software function (e.g., a process) that is the major element E that directly contributes to the storage and management of the NAT address mapping table. There is also E' that is the hot-standby of E. 4) While applications on both IPv4-Host1 and IPv4-Host2 going on normally, disable the E. Due to the proprietary nature of the hot-standby implementation, this action varies. Examples: 1) if E and E' are on separate hardware module, pull out the hardware module where E locates, 2) if E and E' are on separate chassis, power down the chassis where E locates. 5) After 1 minute, resume and enable the operation of E.
Expected result	1) When E is disabled (see the step 4 in the test procedure above), the applications on both IPv4-Host1 and IPv4-Host2 continue without any impact. The NAT44 mapping table that maintained by E' is the same as that maintained by E prior to its disabling.

	2) When E is resumed functioning (see the step 5 in the test procedure above), the IP connectivity on both IPv4-Host1 and IPv4-Host2 is maintained.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.4 PCP Server Function Support on CG-NAT44

8.5.4	PCP server function support on CG-NAT44
Test objective	The aim of this test is to check PCP server function support on CG-NAT44 with interoperability.
Requirement	TR-242:R-97
Requirement description	R-97: The device implementing CGN function MUST support Port Control Protocol (PCP) Server behavior as specified in RFC6887 [27].
Device under test	The CG-NAT44 device in Figure 6 Note-1: CG-NAT44 has PCP server function. Note-2: IPv4-Host1 and IPv4-Host2 have PCP client function and allow manual configuration for PCP client.
Test configuration	**Test Setup** - Figure 6 **Preconditions:** 1) RG-1 and RG-2 are configured in router mode 2) The NAT44 device has implemented PCP server function. 3) IPv4-Host1 and IPv4-Host2 have implemented PCP client function. 4) Traffic generator is ready to simulate/analyze the IPv4 packets **Test Conditions:** 1) Make sure that PCP server function is activated on the NAT44 device. 2) Make sure that PCP client function is activated on IPv4-Host1 and IPv4-Host2 respectively. 3) The DHCP and NAT44 function are configured on RG-1 and RG-2 4) The IPv4 private address pool for Network-3 is configured on the DHCP server. 5) The NAT44 function and the IPv4 public address pool for Network-4 are configured on the NAT44 device. 6) PCP Server address is configured on RG-1 and RG-2.
Test procedure	1) RG-1 and RG-2 start the IP connection respectively.

	1a) IPv4-Host1's IPv4 address: a1 '. b1'. c1 '. d1' 1b) IPv4-Host2's IPv4 address: a2 '. b2'. c2 '. d2' 2) Establish IP connectivity between IPv4-Host1 and IPv4-Host5, between IPv4-Host2 and IPv4-Host5, respectively. 2a) Note the NAT44 mapping on RG-1 for IPv4-Host1: a1'.b1'.c1'.d1':x1'/a1".b1".c1".d1":x1" 2b) Note the NAT44 mapping on RG-2 for IPv4-Host2: a2'.b2'.c2'.d2':x2'/a2".b2".c2".d2":x2" 2c) Note that there must be no mapping table entry on NAT44 device for IPv4-Host1 and IPv4-Host2 this time. 3) Note the availability of IPv4 address A1.B1.C1.D1, port X1 on the subnet with IPv4-Host3. Note the availability of IPv4 address A2.B2.C2.D2, port X2 on the subnet with IPv4-Host4. 4) Configure on IPv4-Host1 such that the PCP client will communicate with the PCP server on NAT44 to create a mapping: external A1.B1.C1.D1:X1 and internal a1".b1".c1".d1":x1". 5) Configure on IPv4-Host2 such that the PCP client will communicate with the PCP server on NAT44 to create a mapping: external A2.B2.C2.D2:X2 and internal a2".b2".c2".d2":x2". 6) Configure TG3 sending IPv4 traffic with destination address A1.B1.C1.D1 and destination port X1. 7) Configure TG4 sending IPv4 traffic with destination address A2.B2.C2.D2 and destination port X2
Expected result	1) At the end of step 4, there is an entry in the mapping table on NAT44 device created by PCP: external A1.B1.C1.D1:X1 and internal a1".b1".c1".d1":x1" 2) At the end of step 5, there is an entry in the mapping table of NAT44 device created by PCP: external A2.B2.C2.D2:X2 and internal a2".b2".c2".d2":x2". 3) At step 6, IPv4-Host1 receives all IPv4 traffic sent by TG3. 4) At step 7, IPv4-Host2 receives all IPv4 traffic sent by TG4. Note: 1) an'.bn'.cn'.dn':xn' indicates the IPv4 private address and port in Network-1 or Network-2. 2) an".bn".cn".dn":xn" indicates the IPv4 private address and port in Network-3.

	3) An.Bn.Cn.Dn:Xn indicates the IPv4 public address and port of Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.5 Paired IP Address Pooling Behavior of CG-NAT44

8.5.5	Paired IP address pooling behavior of CG-NAT44
Test objective	The aim of this test is to check that CG-NAT44 device uses the same external address mapping for all sessions associated with the same internal IP address. If there are not enough external ports available to match the ports of internal IP address, the CG-NAT44 should allocate a new external address with enough ports available to match that internal address.
Requirement	TR-242: R-79
Requirement description	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 CG-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.
Device under test	The CG-NAT44 device in Figure 6
Test configuration	**Test Setup** - Figure 6 **Pre-conditions:** 1) RG-1 is configured in bridge mode (Note: for this test, there must not be a NAT function on the RG). 2) Traffic generator TG1 and TG4 are ready to simulate/analyze the IPv4 packets. **Test Conditions:** 1) The IPv4 private address pool for Network-3 is configured on the DHCP server 2) The NAT44 function is configured on the NAT44 device. 3) The IPv4 public address pool of Network-4 is configured on the NAT44 device, only two public IPv4 addresses: A1.B1.C1.D1 and A2.B2.C2.D2 are included in the pool, and each address has been configured to have 1024 ports, the port range starts from 64512 to 65535.

Test procedure	1) The traffic generator TG1 sends 2048 traffic streams: Stream 1~1024: the source IPv4 addresses of all 1024 streams are a1.b1.c1.d1 of Network-1, the source ports of each stream is different from each other. Stream 1025~2048: the source IPv4 addresses of all 1024 streams are a2.b2.c2.d2 of Network-1, the source ports of each stream is different from each other. And the destination IPv4 addresses of all 2048 streams are A3.B3.C3.D3 of Network-4. Check the received traffic on TG4. 2) Check the NAT address mapping table on the NAT44 device via EMF or analyzing the packets received on TG4. 3) Based on the NAT address mapping table information obtained in step 2, modify the traffic sent by TG1 to stop sending 256 traffic streams with their internal address mapped to the external address A1.B1.C1.D1 and another 256 traffic streams mapped to the external address A2.B2.C2.D2, wait for NAT entries to be aged. 4) Send 512 additional traffic streams on TG1, in which the source IPv4 address is a3.b3.c3.d3 of Network-1 and different from that of existing traffic streams, the source ports of each stream is different from each other, and the destination IPv4 address is A3.B3.C3.D3 of Network-4. Check the received traffic on TG4. 5) Check the NAT address mapping table on the NAT44 device via EMF or analyzing the packets received on TG4. 6) Based on the NAT address mapping table information obtained in step 5, modify the traffic sent by TG1 to stop sending 256 traffic streams with their internal address (exclude the a3.b3.c3.d3 address) mapped to the external address A1.B1.C1.D1, wait for NAT entries to be aged. Check the received traffic on TG4.
Expected result	1) At step 1, TG4 successfully receives the traffic from TG1 without any packet loss. 2) At step 2, the NAT44 device successfully completes the address translation. The number of newly created NAT entries is 2048, 1024 of which are created by the internal address a1.b1.c1.d1 which mapped to the external address A1.B1.C1.D1, the other 1024 of which are created by the internal address a2.b2.c2.d2 mapped to A2.B2.C2.D2, and each internal IPv4 address only maps to one external IPv4 address. 3) At step 3, on the NAT44 device, 1536 NAT entries should remain, 768 of which are mapped to the external address A1.B1.C1.D1, and the other 768 of which are mapped to the external address A2.B2.C2.D2. 4) At step 4, TG4 successfully receives the traffic created by the source IPv4 addresses a1.b1.c1.d1 and a2.b2.c2.d2 from TG1, but for the 512

	additional streams created by the source IPv4 address a3.b3.c3.d3, only 256 streams should be received and other 256 streams should be discarded. 5) At step 5, 1792 NAT entries exist on the NAT44 device, 1536 of which created in step 3 should be unchanged. Only 256 newly entries should correspond to the internal IPv4 source address of a3.b3.c3.d3 which mapped to the external address A1.B1.C1.D1. (the result of the address mapping is implementation dependent, it could be mapped to the external address either A1.B1.C1.D1 or A2.B2.C2.D2, here we suppose it is A1.B1.C1.D1). 6) At step 6, 1792 NAT entries exist on the NAT44 device, but the content should be changed: 6.1) There are 512 NAT entries exist with the internal address a1.b1.c1.d1 mapped to the external address A1.B1.C1.D1, since the 256 old NAT entries which corresponding to the internal address a1.b1.c1.d1 have been aged. 6.2) 256 newly NAT entries should be created by the internal IPv4 source address a3.b3.c3.d3, therefore there are 512 NAT entries for the internal address a3.b3.c3.d3, which be mapped to the external address A1.B1.C1.D1. 6.3) 768 old NAT entries for the internal address a2.b2.c2.d2 should be unchanged which mapped to the external address A2.B2.C2.D2. TG4 successfully receives all traffic with the source IPv4 addresses a1.b1.c1.d1, a2.b2.c2.d2 and a3.b3.c3.d3 from TG1 without any packet loss. Note: 1) an.bn.cn.dn indicates the IPv4 private address in Network-1 2) An.Bn.Cn.Dn indicates the IPv4 public address in Network-4
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.6 TCP port in Bulk Port Allocation mode

8.5.6	**TCP port allocation in Bulk Port Allocation mode of CG-NAT44**
Test objective	The purpose of this test is to check that CG-NAT44 device pre-allocate a block of TCP ports for a subscriber, the pre-allocated ports are used for all TCP connections initiated from this subscriber. However, a new block of ports should be pre-allocated for other TCP connections initiated from another new subscriber.

Requirement	TR-242:R-87
Requirement's description	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.
Device under test	The NAT44 device in Figure 6
Test configuration	**Test Setup:** Figure 6 **Preconditions:** 1) RG-1 is configured in bridge mode 2) Traffic generator TG1 and TG4 are ready to simulate/analyze the IPv4 TCP packets **Test Conditions:** 1) The IPv4 private address pool for Network-3 is configured on the DHCP server 2) The NAT44 function is configured. Enable Bulk Port Allocation function and specify that the port size for allocation is 64 on the NAT44 device. 3) The IPv4 public address pool of Network-4 is configured on the NAT44 device, only one public IPv4 address A1.B1.C1.D1 is included in the pool of Network-4.
Test procedure	1) TG1 starts the IP connection. 2) TG1 sends one traffic stream, in which the source IPv4 address is a1.b1.c1.d1 of Network-1, the source TCP port number is arbitrary, the destination IPv4 address is A2.B2.C2.D2 of Network-4, and the destination TCP port is 8080. (In the following steps, the destination IPv4 address and TCP port of all traffic streams sent by TG1 will be the same as this traffic stream.) Check the received traffic on TG4. 3) Check the NAT address mapping table and the number of ports that are assigned to the internal address a1.b1.c1.d1 on the NAT44 device via EMF. 4) TG1 sends 31 additional traffic streams. The source TCP ports of all these streams are different from each other, and the source IPv4 addresses of all these streams are a1.b1.c1.d1. Check the received traffic on TG4. 5) Repeat step 3, check the NAT address mapping table and the number of the ports assigned on the NAT44 device via EMF. 6) TG1 sends 32 additional traffic streams again. The source TCP ports of all

	streams are different from each other, and the source IPv4 addresses are a2.b2.c2.d2. Check the received traffic on TG4. 7) Repeat step 3, check the NAT address mapping table and the number of the ports that are assigned to the a2.b2.c2.d2 on the NAT44 device via EMF. 8) TG1 sends 64 additional traffic streams. The source TCP ports of all these streams are different from each other and different from the TCP ports of streams sent by step 6, and the source IPv4 addresses of all these streams are a2.b2.c2.d2. Check the received traffic on TG4. 9) Repeat step 7, check the NAT address mapping table on the NAT44 device via EMF.
Expected result	1) At step 1, TG1 establishes IP connection successfully. 2) At step 2, TG4 receives the traffic stream from TG1 successfully without any packet loss. 3) At step 3, only one NAT entry should be created for the internal address a1.b1.c1.d1, and the NAT44 device allocates 64 external ports and one external IPv4 address A1.B1.C1.D1 to a1.b1.c1.d1. 4) At step 4, TG4 receives the 32 traffic streams from TG1 successfully without any packet loss. 5) At step 5, the NAT entry and the number of ports that are assigned to a1.b1.c1.d1 should not be changed on the NAT44 device. 6) At step 6, TG4 receives the 64 traffic streams from TG1 successfully without any packet loss. 7) At step 7, a new NAT entry should be created for the internal address a2.b2.c2.d2, and the NAT44 device allocates the external IPv4 address A1.B1.C1.D1 and another 64 external ports for a2.b2.c2.d2. 8) At step 8, TG4 only receives the 96 traffic streams from TG1, and the other 32 traffic streams should be dropped. 9) At step 8, among received traffic streams, 32 are mapped from private IPv4 address a1.b1.c1.d1, and 64 are from private IPv4 address a2.b2.c2.d2." 10) At step 9, the NAT entry and the number of ports should not be changed on the NAT44 device. **Note:** 1) an.bn.cn.dn indicates the IPv4 private address in Network-1 2) An.Bn.Cn.Dn indicates the IPv4 public address in Network-4
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.7 UDP port in Bulk Port Allocation mode

8.5.7	Pre-allocation of UDP ports with bulk port allocation scheme of CG-NAT44
Test objective	The purpose of this test is to check that CG-NAT44 device pre-allocate a block of UDP ports for a subscriber, the pre-allocated ports are used for all UDP connections initiated from this subscriber. However, a new block of ports should be pre-allocated for other UDP connections initiated from another new subscriber.
Requirement	TR-242: R-86
Requirement's description	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.
Device under test	The CG-NAT44 device as referred in Figure 6
Test configuration	**Test Setup -** Figure 6 **Pre-conditions:** 1) RG-1 is configured in bridge mode. 2) Traffic generator TG1 and TG4 are ready to simulate/analyze the IPv4 UDP packets **Test Conditions:** 1) The IPv4 private address pool for Network-3 is configured on the DHCP server 2) The NAT44 function is configured on the NAT44 device. 3) The IPv4 public address pool of Network-4 is configured on the NAT44 device, one public IPv4 address A1.B1.C1.D1 is included in the pool 4) The NAT44 function is configured. Enable Bulk Port Allocation function and specify that the port size for allocation is 64 on the NAT44 device..
Test procedure	1) TG1 starts the IP connection. 2) TG1 sends one traffic stream, in which the source IPv4 address is a1.b1.c1.d1 of Network-1, the source UDP port is arbitrary, the destination IPv4 address is A2.B2.C2.D2 of Network-4, and the destination UDP port is 80. (In the following steps, the destination IPv4 address and UDP port number of all traffic streams sent by TG1 will be the same as this traffic stream.) Check the received traffic on TG4. 3) Check the NAT address mapping table and the number of ports that are assigned to the internal address a1.b1.c1.d1 on the NAT44 device via

	EMF. 4) TG1 sends 31 additional traffic streams. The source UDP port numbers of all streams are different from each other, and the source IPv4 addresses of all these streams are a1.b1.c1.d1. Check the traffic received on TG4. 5) Repeat step 3, check the NAT address mapping table and the number of the ports assigned on the NAT44 device via EMF. 6) TG1 sends 32 additional traffic streams again. The source IPv4 addresses are a2.b2.c2.d2， and the source UDP port of all streams are different from each other. Check the received traffic on TG4. 7) Repeat step 3, check the NAT address mapping table and the number of ports that are assigned to the internal address a2.b2.c2.d2 on the NAT44 device via EMF. 8) TG1 sends 64 additional traffic streams. The source UDP ports of all these streams are different from each other and different from the UDP ports of streams sent by step 6, and the source IPv4 addresses of all these streams are a2.b2.c2.d2. Check the received traffic on TG4. 9) Repeat step 7, check the NAT address mapping table on the NAT44 device via EMF.
Expected result	1) At step 1, TG1 establishes IP connection successfully. 2) At step 2, TG4 receives the traffic stream from TG1 successfully without any packet loss. 3) At step 3, only one NAT entry should be created for the internal address a1.b1.c1.d1 and the NAT44 device allocates 64 external ports and one external IPv4 address A1.B1.C1.D1 to a1.b1.c1.d1. 4) At step 4, TG4 receives 32 traffic streams from TG1 successfully without any packet loss. 5) At step 5, the NAT entry and the number of ports that are assigned to a1.b1.c1.d1 should not be changed on the NAT44 device. 6) At step 6, TG4 receives the 64 traffic streams from TG1 successfully without any packet loss. 7) At step 7, a new NAT entry should be created for the internal address a2.b2.c2.d2, and the NAT44 device allocates the external IPv4 address A1.B1.C1.D1 and another 64 external ports for a2.b2.c2.d2. 8) At step 8, TG4 only receives the 96 traffic streams from TG1, and the other 32 traffic streams should be dropped. 9) At step 9, The NAT entry and the number of ports should not be changed on the NAT44 device. **Note:** 1) an.bn.cn.dn indicates the IPv4 private address in Network-1

	2) An.Bn.Cn.Dn indicates the IPv4 public address in Network-4
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.8 PCP - Learning Public IP address of the CGN

8.5.8	PCP server function support on CGN: Learning Public IP address assigned by the CGN
Test objective	The purpose of this test is to retrieve the external IP address assigned by the CGN. Note the CGN may be configured with a pool of public IP addresses. Only the (shared) address assigned by the CGN to the requesting host will be returned.
Requirement	TR-242:R-97
Requirement description	R-97: The device implementing CGN function MUST support Port Control Protocol (PCP) Server behavior as specified in RFC6887 [27].
Device under test	The CG-NAT44 device in Figure 6. Note-1: CGN device embeds a PCP server function. The PCP Server is being enabled. Note-2: IPv4-Host1 embeds a PCP client function and allows manual configuration for the PCP client.
Test configuration	**Test Setup** - Figure 6. **Preconditions:** 1) RG-1 is configured in bridge mode 2) The CGN device has implemented PCP server function. 3) IPv4-Host1 has implemented PCP client function. 4) Traffic generators and probes are ready to simulate and analyze exchanged IPv4 packets **Test Conditions:** 1) Make sure that PCP server function is activated on the CGN device. 2) Make sure that PCP client function is activated on IPv4-Host1. 3) The IPv4 private address pool for Network-3 is configured on the DHCP server. 4) The NAT44 function and the IPv4 public address pool for Network-4 are configured on the CGN device. 5) PCP Server address is configured on RG-1.

Test procedure	1) IPv4-Host1 starts the IP connection. IPv4-Host1's IP address is a1'.b1'.c1'.d1' 2) Establish IP connectivity between IPv4-Host1 and IPv4-Host3. 3) Check the NAT address mapping table on the CGN device via EMF or by analyzing the packets via probe p6. 4) Note the IPv4 source address received by IPv4-Host3. 5) Process a PCP MAP Request from IPv4-Host1 to PCP Server by requesting a short-lived mapping to the Discard service (TCP/9 or UDP/9). The request lifetime is set to 30 seconds. 6) Record the value returned by the PCP server in the PCP MAP Response
Expected result	1) At the end of step 5 of the test procedure (see above) there are two entries in the mapping table on the CGN device: 1a) external A1.B1.C1.D1:X1 and internal a1".b1".c1".d1":x1" 1b) external A1.B1.C1.D1:9and internal a1".b1".c1".d1":9 2) At step 6, the source IP address of the PCP MAP Response from the CGN is the same as that of data packets sent by IPv4-Host3, both received by IPv4-Host1, i.e., A1.B1.C1.D1. Note: 1) an'.bn'.cn'.dn':xn' indicates the IPv4 private address and port in Network-1 or Network-2. 2) an".bn".cn".dn":xn" indicates the IPv4 private address and port in Network-3. 3) An.Bn.Cn.Dn:Xn indicates the IPv4 public address and port of Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.9 PCP - Request an Already Used Port

8.5.9	PCP server function support on CGN : Requesting an already used port
Test objective	The purpose if this test case is to assess the behavior of the PCP Server when a port already in use is required by a PCP client. Two cases will be checked: (1) No PREFER_FAILURE option is included in the request and, (2) PREFER FAILURE is included in the request.
Requirement	TR-242:R-97
Requirement description	R-97: The device implementing CGN function MUST support Port Control Protocol (PCP) Server behavior as specified in RFC6887 [27].

Device under test	The CG-NAT44 device in Figure 6. Note-1: CGN device has PCP server function. The PCP Server is being enabled. Note-2: IPv4-Host1 and IPv4-Host2 have PCP client function and allow manual configuration for PCP client.
Test configuration	**Test Setup -** Figure 6 **Preconditions:** 1) RG-1 and RG-2 are configured in bridge mode 2) The CGN device has implemented PCP server function. 3) IPv4-Host1 and IPv4-Host2 have implemented PCP client function. 4) Traffic generators and probes are ready to simulate and analyze the IPv4 packets **Test Conditions:** 1) Make sure that PCP server function is activated on the CGN device. 2) Make sure that PCP client function is activated on IPv4-Host1 and IPv4-Host2 respectively. 3) The IPv4 private address pool for Network-3 is configured on the DHCP server. 4) The NAT44 function is configured on the CGN device and only one IPv4 public address for Network-4 is set. 5) PCP Server address is configured on RG-1 and RG-2.
Test procedure	The following steps are repeated for each configuration: (1) PREFER_FAILURE option is included in the PCP Request, (2) PREFER_FAILURE is included in the PCP Request. 1) IPv4-Host1 and IPv4-Host2 start the IP connection respectively. IPv4-Host1's IP address is a1'.b1'.c1'.d1' IPv4-Host2's IP address is a2'.b2'.c2'.d2' 2) Make sure that port X1 for address A1.B1.C1.D1 is available on the CGN device. 3) Configure on IPv4-Host1 such that the PCP client will communicate with the PCP server on the CGN device to create a mapping: external A1.B1.C1.D1:X1 and internal a1'.b1'.c1'd1':x1'. 4) Configure on IPv4-Host2 such that the PCP client will communicate with the PCP server on the CGN device to create a mapping: external A1.B1.C1.D1:X1 and internal a2'.b2'.c2'.d2':x2'. 5) Note the value of the assigned port returned by the PCP server in the PCP

	MAP Response.
Expected result	(a) PREFER FAILURE option is not included in the request 1) At the end of step 5 of the test procedure (see above) there are two entries in the mapping table on the CGN device created by PCP: 1a) external A1.B1.C1.D1:X1 and internal a1'.b1'.c1'.d1':x1'. 1b) external A1.B1.C1.D1:X2 and internal a2'.b2'.c2'.d2':x2'. 2) The value of the assigned port returned by the PCP server in the PCP MAP Response is equal to X2. 3) IPv4-Host1 receives all IPv4 traffic sent by TG3 on A1.B1.C1.D1:X1 4) IPv4-Host2 receives all IPv4 traffic sent by TG4 on A1.B1.C1.D1:X2 (b) PREFER_FAILURE option is included in the request 1) At the end of step 5 of the test procedure (see above) there is only one entry in the mapping table on the CGN device created by PCP: external A1.B1.C1.D1:X1 and internal a1'.b1'.c1'.d1':x1' 2) The PC Server returns an error "CANNOT_PROVIDE_EXTERNAL" 3) IPv4-Host1 receives all IPv4 traffic sent by TG3 on A1.B1.C1.D1:X1 Note: 1) an'.bn'.cn'.dn':xn' indicates the IPv4 private address and port in Network-1 or Network-2. 2) An.Bn.Cn.Dn: Xn indicates the IPv4 public address and port of Network-4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.10 The function of NAT ALG for TCP protocol for CG-NAT44

8.5.10	The function of NAT ALG for TCP protocol for CG-NAT44
Test objective	The purpose of this test case is to test that CG-NAT44 device implements the TCP ALG function such that FTP TCP-based application can operate across CG-NAT44 device.
Requirement	TR-242:R-75
Requirement description	R-75. The CG-NAT44 device MUST support TCP, UDP, ICMP, DCCP requirements as defined in RFC4787 [18], RFC5382 [19], RFC5508 [20], and RFC5597 [21], respectively.
Device under	The CG-NAT44 device in Figure 6

test	
Test configuration	**Test Setup:** Figure 6 **Preconditions:** 1) RG-1 is configured in bridge mode 2) The traffic generator TG1 and TG3 are ready to simulate/analyze the IPv4 TCP packets **Test Conditions:** 1) The IPv4 private address pool for Network-1 and the IPv4 address for Network-3 are configured on the DHCP server. 2) The IPv4 address and FTP server function are configured on IPv4-Host4. 3) The NAT44 function and IPv4 public address pool for Network-4 are configured on the NAT44 device.
Test procedure	1) IPv4-Host1 starts the IP connection. 2) Enable FTP ALG function on NAT44 device, and IPv4-Host1 starts a FTP connection to IPv4-Host4 which is functioning as a FTP server, check the result of the FTP connection on IPv4-Host1. 3) Disable FTP ALG function on NAT44 device, and repeat the step 2, check the result of FTP connection on IPv4-Host1.
Expected result	1) At step 1, IPv4-Host1 establishes IP connection successfully. 2) At step 2, IPv4-Host1 establishes a FTP connection to IPv4-Host4 successfully. IPv4-Host1 can transfer file to/from IPv4-Host4. 3) At step 3, IPv4-Host1 can't establish a FTP connection to IPv4-Host4.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.11 The function of NAT ALG for ICMP protocol for CG-NAT44

8.5.11	The function of NAT ALG for ICMP protocol for CG-NAT44
Test objective	The purpose of this test case is to test that CG-NAT44 device implements the ICMP ALG function so that the function of ICMP Echo message and TRACEROUTE message can traverse CG-NAT44 device.
Requirement	TR-242:R-75
Requirement description	R-75. The CG-NAT44 device MUST support TCP, UDP, ICMP, DCCP requirements as defined in RFC4787 [18], RFC5382 [19], RFC5508 [20], and RFC5597 [21], respectively.
Device under	The CG-NAT44 device in Figure 6

test	
Test configuration	**Test Setup**: Figure 6 **Preconditions:** 1) RG-1 is configured in bridge mode 2) The traffic generator TG1 and TG4 are ready to simulate/analyze the IPv4 ICMP packets **Test Conditions:** 1) The IPv4 private address pool for Network-3 is configured on the DHCP server 2) The IPv4 address of IPv4-Host1 and IPv4-Host4 are configured. 3) The NAT44 function and IPv4 public address pool of Network-4 are configured on the NAT44 device.
Test procedure	1) IPv4-Host1 starts the IP connection. 2) IPv4-Host1 sends ICMP Echoes to IPv4-Host4 in public Network-4. Check the result of ICMP Echo operation on IPv4-Host1. 3) IPv4-Host1 sends ICMP Traceroute to IPv4-Host4 in public Network-4. Check the result of ICMP Traceroute operation on IPv4-Host1
Expected result	1) At step 1, IPv4-Host1 and IPv4-Host2 establish the IP connection successfully. 2) At step 2, the ICMP Echo operation is successful with no ICMP Echo/Reply message is dropped. 3) At step 3, the ICMP Traceroute operation is successful with no ICMP Traceroute message dropped.
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

8.5.12 Pre-allocation of external ICMP identifiers for individual subscribers

8.5.12	Pre-allocation of external ICMP identifiers for individual subscribers
Test objective	The purpose of this test is to check that CG-NAT44 device pre-allocate a block of ICMP identifiers for a subscriber, the pre-allocated identifiers are used for all ICMP connections initiated from this subscriber. However, a new block of identifiers should be pre-allocated for other ICMP connections initiated from another new subscriber.
Requirement	TR-242:R-88
Requirement	TR-242:

description	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.
Device under test	The CG-NAT44 device in Figure 6.
Test configuration	**Test Setup** - Figure 6. **Preconditions:** 1) RG-1 is configured in bridge mode 2) Traffic generator TG1 and TG4 are ready to simulate/analyze the IPv4 ICMP packets **Test Conditions:** 1) The IPv4 private address pool for Network-3 is configured on the DHCP server 2) The NAT44 function is configured. Enable Bulk Port Allocation function and specify that the port size for allocation is 64 on the NAT44 device. 3) The IPv4 public address pool of Network-4 is configured on the NAT44 device, only one public IPv4 address A1.B1.C1.D1 is included in the pool of Network-4.
Test procedure	1) TG1 starts the IP connection. 2) TG1 sends one traffic stream, in which the source IPv4 address is a1.b1.c1.d1 of Network-1, the Identifier is x1, the destination IPv4 address is A2.B2.C2.D2 of Network-4. In the following steps, the destination IPv4 address of all traffic streams sent by TG1 will be the same as this traffic stream. Check the received traffic on TG4. 3) Check the NAT address mapping table and the number of identifiers that are assigned to the internal address as a1.b1.c1.d1 on the NAT44 device via EMF. 4) TG1 sends 31 additional traffic streams. The ICMP Query Identifiers of all streams are different from each other, and all the source IPv4 addresses are a1.b1.c1.d1. Check the received traffic on TG4. 5) Repeat step 3, check the NAT address mapping table entry and the number of the assigned identifiers on the NAT44 device. 6) TG1 sends 32 additional traffic streams again. The ICMP Query Identifiers of all streams are different from each other, and the source IPv4 addresses are a2.b2.c2.d2. Check the received traffic on TG4.

	7) Repeat step 3, check the NAT address mapping table entry and the number of the assigned identifiers on the NAT44 device. 8) TG1 sends 64 additional traffic streams. The ICMP Query Identifier of all these streams are different from each other and different from the Identifier of streams sent by step 6, and the source IPv4 addresses of all these streams are a2.b2.c2.d2. Check the received traffic on TG4. 9) Repeat step 7, check the NAT address mapping table on the NAT44 device via EMF.
Expected result	1) At step 1, TG1 establishes IP connection successfully. 2) At step 2, TG4 receives the traffic stream from TG1 successfully without any packet loss. 3) At step 3, only one NAT entry should be created for the internal address a1.b1.c1.d1, and the NAT44 device allocates 64 external ICMP identifiers and the external IPv4 address A1.B1.C1.D1 for a1.b1.c1.d1. 4) At step 4, TG4 successfully receives the 32 traffic streams from TG1 without any packet loss. 5) At step 5, the NAT entry and the number of identifiers that are assigned to a1.b1.c1.d1 should not be changed on the NAT44 device. 6) At step 6, TG4 successfully receives the 64 traffic streams from TG1 without any packet loss. 7) At step 7, a new NAT entry should be created for the internal address as a2.b2.c2.d2, and the NAT44 device allocates another 64 external identifiers and the external IPv4 address A1.B1.C1.D1 for a2.b2.c2.d2. 8) At step 8, TG4 only receives the 96 traffic streams from TG1, and the other 32 traffic streams with the source address a2.b2.c2.d2 should have been dropped 9) At step 9, the NAT entry and the number of identifiers should not be changed on the NAT44 device. Note: 1) an.bn.cn.dn indicates the IPv4 private address in Network-1 2) An.Bn.Cn.Dn indicates the IPv4 public address in Network-4
Pass/Fail	Pass: All the expected result were observed Fail: At least one of the result was different from the expected result

End of Broadband Forum Technical Report TR-296

