ETSI TS 103 443-6 V1.1.1 (2016-08)

TECHNICAL SPECIFICATION

Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition Technology Engineering and Operational Aspects; Part 6: 6RD

Reference

DTS/CABLE-00018-6

Keywords

cable, HFC, IPv6

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Integrated broadband cable telecommunication networks (CABLE).

The present document is part 6 of a multi-part deliverable. Full details of the entire series can be found in part 1 [20].

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Considering the depletion of IPv4 addresses, transition to IPv6 is required in order to enable continued growth of the customer base connected to cable networks and ensure service continuity for existing and new customers. High-quality connectivity to all kinds of IP-based services and networks is essential in today's business and private life.

The present document accommodates an urgent need in the industry to implement and integrate the IPv6 transition technologies as specified by ETSI TS 101 569-1 [1] into their cable networks. The choice of the technology implemented depends on factors such as the business needs, current deployed architectures and plans for cost effectively transition from IPv4 to IPv6.

Current global IPv4 address space was projected to be depleted around the middle of 2012; depletion for the operator was estimated around end 2012. As part of the resulting roll-out of IPv6 in the operator's network, specific measures had to be taken to allow a smooth transition and coexistence between IPv4 and IPv6. ETSI developed requirements to address transition from IPv4 to IPv6 specifying six transition technologies as given by ETSI TS 101 569-1 [1] that were at the time considered to be the most appropriate to assist cable operators to transition there cable networks to IPv6.

Since then the industry has acquired more experience with the technology options settling in the main for DS-Lite across the cable network market and NAT64 IPv6 transition technologies across the mobile market.

The objective of the present document is to define the operational and engineering requirements to enable engineers to implement a seamless transition of the cable networks to IPv6 with the application of the 6RD transition technology.

The present document is the final part of a companion of ETSI standards developed in 4 phases to provide the cable sector in particular cable operators engineering and operational staff a standardized approach when integrating one of the five IPv6 transition technologies, NAT64, DS-Lite, 464XLAT, 6RD and MAP-E.

The first phase assessed the different IPv6 transition technology options being defined by industry with recommendation for the most appropriate with consideration of current network architectures, ensuring adequate scale and a cost effective transition approach from IPv4 to IPv6 as the IPv4 addresses deplete. The objective being to examine the pros and cons of the IPv6 transition technologies and recommend the most cost effective solution that would enable the cable operators to minimize the cost of upgrades to their existing network plant whilst maintain continuity of services to their present and new added customers. The details of the study are given by ETSI TR 101 569 [i.2].

In the second phase an ETSI technical specification was developed to specify technical requirements for six transition technologies that industry were considering for use by Cable Operators depending on the current state of their deployed cable network architecture, service model requirements and their IPv6 transition strategy as the IPv4 addresses depleted. These six IPv6 transition technologies are specified by ETSI TS 101 569-1 [1], covering NAT64, DSLite, 6RD, NAT44, 464XLAT and MAP-E.

In the third phase ETSI developed a series of conformance test specifications to enable the compliance verification of the five IPv6 transition technologies, NAT64, DS-Lite, 464XLAT, 6RD and MAP-E that were specified during phase 2 standardization. The conformance tests are developed against the requirements given by the ETSI TS 101 569-1 [1]. The series of conformance tests developed for each of the four transition technologies, are as given by ETSI TS 103 238 parts 1 [2] and to 3 [4] respectively for NAT64; ETSI TS 103 239 parts 1 [5] to 3 [7] respectively for MAP-E; ETSI TS 103 241 parts 1 [8] to 3 [10] respectively for DS-Lite; ETSI TS 103 242 parts 1 [11] to 3 [13] respectively for XLAT and ETSI TS 103 243 parts 1 [14] to 3 [16] respectively for 6RD.

Phase 4 is the present project phase for development of technical specifications covering the operational and engineering requirements with the present document being Part 6 of a multi-part series covering the IPv6 transition technology 6RD.

DOCSIS® is a registered Trade Mark of Cable Television Laboratories, Inc., and is used in the present document with permission.

1 Scope

The present document presents the engineering and operational requirements for the application of the IPv6 transition technology 6RD as defined by ETSI TS 101 569-1 [1] (IPv6 Transition Requirements) implemented within an integrated broadband cable network end to end across its network domains.

The present document is Part 6 of a multi-part series and presents the operational aspects of the IPv6 transition technology 6RD across the cable network domains.

Only those elements of the network that have to be engineered to operate the IPv6 transition technology 6RD are presented. Descriptions and interface details of network elements that do not change are already addressed by the relevant equipment cable standards and therefore this information is not included in the present document.

The conformity of the 6RD implementation is relevant when assessing its implementation and operational requirements across the cable network to ensure the implementation is correctly engineered to conform to the requirements of the base standard ETSI TS 101 569-1 [1]. These conformance tests are not specified in the present document as they are already specified by ETSI TS 103 243 parts 1 [14] to 3 [16].

The operational aspects for the IPv6 transition technology 6RD are considered when engineered end to end across the cable network domains;

- CPE Home Networking Domain
- Access Network Domain
- Core Network Domain
- Data Centre Domain
- DMZ Service Domain
- Transit and Peering Domain
- Management and Monitoring Domain
- Security Domain

The present document specifies the requirements to be considered when the defined IPv6 transition technology 6RD is engineered across the cable network domains.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 101 569-1: "Integrated Broadband Cable Telecommunication Networks (CABLE); Cable Network Transition to IPv6 Part 1: IPv6 Transition Requirements".

[2] ETSI TS 103 238-1: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for NAT64 technology; Part 1: Protocol Implementation Conformance Statement (PICS) proforma".

[3] ETSI TS 103 238-2: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for NAT64 technology; Part 2: Test Suite Structure and Test Purposes (TSS&TP)".

[4] ETSI TS 103 238-3: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for NAT64 technology; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

[5] ETSI TS 103 239-1: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for MAP-E technology; Part 1: Protocol Implementation Conformance Statement (PICS) proforma".

[6] ETSI TS 103 239-2: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for MAP-E technology; Part 2: Test Suite Structure and Test Purposes (TSS&TP)".

[7] ETSI TS 103 239-3: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for MAP-E technology; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

[8] ETSI TS 103 241-1: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for DS-Lite technology; Part 1: Protocol Implementation Conformance Statement (PICS) proforma".

[9] ETSI TS 103 241-2: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for DS-Lite technology; Part 2: Test Suite Structure and Test Purposes (TSS&TP)".

[10] ETSI TS 103 241-3: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for DS-Lite technology; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

[11] ETSI TS 103 242-1: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for 464XLAT technology; Part 1: Protocol Implementation Conformance Statement (PICS) proforma".

[12] ETSI TS 103 242-2: "Integrated broadband cable telecommunication networks (CABLE) Testing; Conformance test specifications for 464XLAT technology; Part 2: Test Suite Structure and Test Purposes (TSS&TP)".

[13] ETSI TS 103 242-3: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for 464XLAT technology; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

[14] ETSI TS 103 243-1: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for 6rd technology; Part 1: Protocol Implementation Conformance Statement (PICS) proforma".

[15] ETSI TS 103 243-2: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for 6rd technology; Part 2: Test Suite Structure and Test Purposes (TSS&TP)".

[16] ETSI TS 103 243-3: "Integrated broadband cable telecommunication networks (CABLE); Testing; Conformance test specifications for 6rd technology; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

[17] IETF RFC 5969: "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification".

[18] IETF RFC 4459 (April 2006): "MTU and Fragmentation Issues with In-the-Network Tunneling".

[19] IETF RFC 2983 (October 2000): "Differentiated Services and Tunnels".

[20]	ETSI TS 103 443-1: "Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition Technology Engineering and Operational Aspects; Part 1: General".
[21]	IETF RFC 4787: "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP".
[22]	IETF RFC 5382: "NAT Behavioral Requirements for TCP".
[23]	IETF RFC 5508: "NAT Behavioral Requirements for ICMP".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] CableLabs.

NOTE: Available at http://www.cablelabs.com/specs/.

[i.2] ETSI TR 101 569: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; Cable Network Transition to IPv6".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

4in6: encapsulation of IPv4 packets within IPv6 packet format

NAT44: network address translation from an IPv4 address to another IPv4 address

P Router: label switching router acting as a transit router in the core network of an MPLS network

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

6PE	IPv6 Provider Edge
6RD	IPv6 Rapid Deployment
6VPE	IPv6 VPN Provider Edge
AAA	Authentication, Authorization and Accounting
ALG	Application Layer Gateway
AMPS	Amplifiers
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuit
B4	Basic Bridging BroadBand element
BFD	Bidirectional Forwarding Detection
BGP	Boarder Gateway Protocol
BNG	Broadband Network Gateway
BR	Boarder Routers

CDP	Cisco Discovery Protocol
CE	Customer Edge
CEF	Cisco Express Forwarding
CMTS	Cable Modem Termination System
CoPP	Control Plane Policing
CPE	Customer Premises Equipment
CPU	Central Processing Unit
DAD	Duplicate Address Detection
dCEF	distributed Cisco Express Forwarding
DCU	Destination Class Usage
DHCP	Dynamic Host Configuration
DMZ	Demilitarised Zone
DNS	Domain Name System
DOCSIS 3.0	Data over Cable System Interface Specification version 3.0
DR	Data Retention
DSCP	Differentiated Services Code Point
DS-Lite	Dual Stack-Lite
ECMP	Equal-Cost-Multi-Path
ESM	Enterprise Subscriber Management
FTP	File Transfer Protocol
GRT	Global Routing Table
GW	Gateway
GW	GateWay
HA	High Availability
HFC	Hybrid Fibre Coax
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
ID	IDentifier
IGP	Interior Gateway Protocol
IMIX	Internet Mix
IP	Internet Protocol
IPFIX	IP Flow Information Export
IPv4	IP version 4
IPv6	IP version 6
IRB	Integrated Routing and Bridging
ISIS	Intermediate System to Intermediate System
ISP	Internet Service Provider
ISSU	In-Service Software Upgrade
IXPE	Internet Exchange Provider Edge
L2	Layer 2
LAN	Local Area Network
LDP	Label Distribution Protocol
LI	Lawful Intercept
LLDP	Link Layer Discovery Protocol
LSN	Large Scale NAT
MAP-E	Mapping of Address and Port - Encapsulation mode
MFIB	Multicast Forwarding Information Base
MLD/L2	Multicast Listener Discovery / Layer 2
MLD/L2	Multicast Listener Discovery/ Layer 2
MP BGP	MultiProtocol Boarder Gateway Protocol
MP	MultiProtocol
MPLS	MultiProtocol Label Switching
MSS	Maximum Segment Size
MSTP	Multiple Spanning Tree Protocol
MT	Multi-Topology
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAT44	Network Address Translation IPv4 to IPv4
NAT64	Network Address Translation IPv6 to IPv4
NCC	Network Coordination Center
ND	Neighbour Discovery
NDP	Neighbour Discovery Protocol

NFv9	Netflow Version 9
NPU	Network Processing Unit
NSF/GR	Non-Stop Forwarding Graceful Restart
NTP	Network Time Protocol
NUD	Neighbour Unreachability Detection
OAM	Operation, Administration and Maintenance
PCP	Port Control Protocol
PE	Provider Edge
PIM	Protocol Independent Multicasting
PPTP	Point-to-Point Tunneling Protocol
PPTP	Point-to-Point Tunnelling Protocol
PS-BGP	Pretty Secure Boarder Gateway Protocol
QoS	Quality of Service
QPPB	QoS Policy Propagation via Boarder Gateway Protocol
RADIUS	Remote Authentication Dial-In User Service
RDT	Reliable Data Transfer
RG	Residential Gateway
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIPE	Réseaux Internet Protocol Européens
RIR	Regional Internet Registry
RSTP	Rapid Spanning Tree Protocol
RTCP	Real-Time Transmission Control Protocol
RTP	Real-Time Protocol
RTSP	Real-Time Streaming Protocol
SCU	Source Class Usage
SEND	Secure Neighbour Discovery
SIP	Session Initiated Protocol
SNMP	Simple Network Management Protocol
SSH	Secure SHell
SSO	Stateful SwitchOver
SVI	Switched Virtual Interface
SYSLOG	Syslog Protocol
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual LAN
VPLS	Virtual Protocol Local Area Network Service
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
XLAT	transLATor
XML	eXtensible Markup Language

4 General Considerations

4.1 Background

The present document is part of a series of ETSI technical specifications specifying requirements to engineer and operate the 6RD transition technology end to end across a cable operator's network. Its implementation would ensure the network provider can continue to provide business continuity throughout the depletion of publicly routable IPv4 addresses and the subsequent rollout and migration to IPv6 in the operator's network.

To aid this transition some sectors of industry are currently evaluating 6RD as their chosen technology to mitigate the gap and lack of integration and compatibility between IPv4 and IPv6.

4.2 General Overview

An objective of deploying the IPv6 transition technology is to provide a seamless experience to users accessing IPv6 network services through IPv4 only networks and to enable current and new content to be delivered seamlessly to IPv6 users by encapsulating the IPv6 to IPv4 (6RD).

It should be noted that Cable broadband access networks may vary in build and design with characteristics that may be vendor equipment specific. Consequently there may be aspects to the engineering and operation of the IPv6 transition technology 6RD that are dependent on the network build and vendor specific equipment deployed.

The present document does not offer information that may be vendor and network build specific since such information may be confidential to the network operator and/or based on proprietary data.

The present document assumes the reader is familiar with the cable network architecture requirements since the description of the various elements within a cable network across its domains are already defined by ETSI standards and standards developed by CableLabs [i.1]. The present document details only the changes to the network aspects when operating the transition technology 6RD.

The present document uses network encapsulation of IPv6 to IPv4 (6RD) technology to provide a seamless Internet experience to users accessing IPv6 Internet services from an IPv6 client through a IPv4 only cable network enabling service providers to transparently deliver and enable new and existing services to IPv6 internet users with little or no change in their existing network infrastructure.

The network elements required to implement the IPv6 transition technology 6RD across the cable network domains is as illustrated by figure 1.

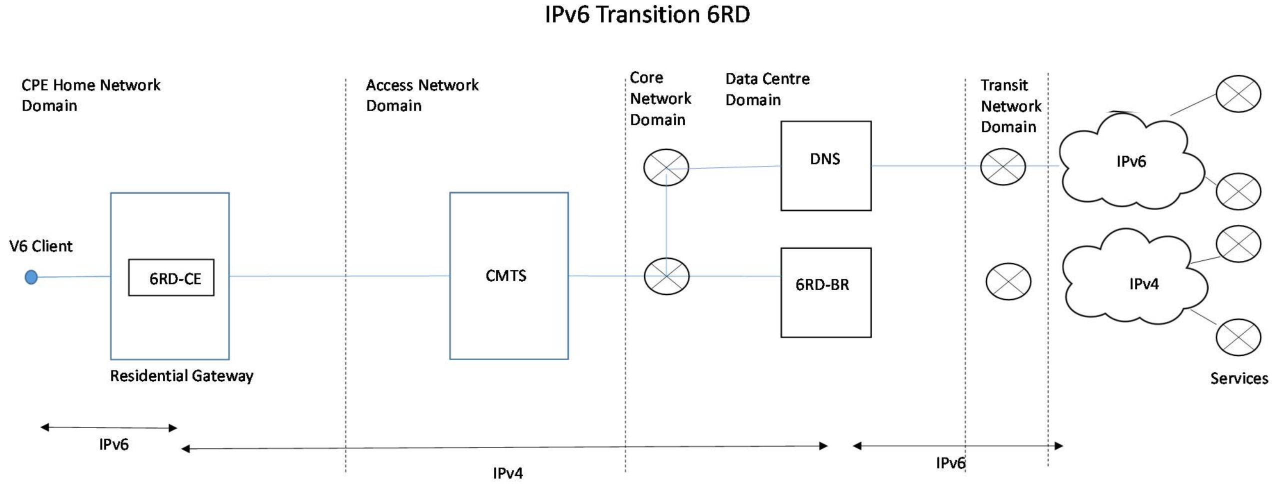

Figure 1: Illustration of network elements to support IPv6 transition technology 6RD across Cable Network Domains

The specific aspects are given in the subsequent clauses for each network domain.

When engineering IPv6 transition technology IPv6 needs to be implemented on all of the network elements.

The engineered network elements to enable 6RD in each cable network domain is integrated with existing network elements and shall be validated by network integration testing. The conformance of the implementation for 6RD would need to be verified before operation as given by ETSI TS 103 243 parts 1 [14] to 3 [16].

4.3 Vendor Considerations

6RD was the easiest delivery of IPv6 transition technologies introduced to the industry, it was the earliest primary technology to be exposed to the market. Many off-the-shelf vendors and network vendors supported the concept from an early stage. Many vendor supported, and still do today, 6RD as a mechanism within their product line and is one of the most supported transition technologies in the retail world.

5 Gap Analysis

5.1 Consideration

The engineering and operational requirements applying ETSI TS 101 569-1 [1] need to be specified with the following design objective to define the logical and physical parameters to allow for customers to access the public IP Internet across an IPv6 network using 6RD.

5.2 Overview

6RD is defined in IETF RFC 5969 [17] and it is one of the incremental methods for deploying IPv6. IPv6 native traffic is tunnelled over IPv4 access network. The IPv4 tunnel end points are the RG/CPE and the Border Router. These two elements perform encapsulation/decapsulation of IPv6-in-IPv4 traffic. BR is placed at IPv6 edge and is addressed via IPv4 (anycast) address for load balancing and resiliency.

6RD is considered stateless which means that no flow states are created in order to forward traffic. In addition, name resolution (DNS) works natively over the IPv6-in-IPv4 tunnel.

From the subscriber management prospective (ESM), there is no IPv6 awareness needed at the BNG (for example DHCPv6, IPv6 ND, etc.).

IPv4 traffic is flowing natively between the RG/CPE and the IPv4 network behind the BNG. NAT44 is implemented on the Border Router for IPv4 continuity.

In contrast, IPv6 traffic originating at the subscriber host is encapsulated into IPv4 traffic at the RG/CPE and is carried over IPv4 network to the BR which decapsulates IPv6 traffic and forwards it natively onto the IPv6 network that is directly attached to the BR.

In the opposite direction, the BR encapsulates IPv6 traffic coming from the native IPv6 network into IPv4 tunnel. The tunnel destination is the RG/ CPE which decapsulates IPv4 traffic and forwards native IPv6 traffic to the host.

6RD requires no NAT per say on the CPE or the LSN border router as the LSN in this case acts solely to decapsulate the IPv4 packets exposing the IPv6 packet payload. LSN is therefore used lightly as the term for the 6RD border router where the IPv4 and the IPv6 network abstract to one another. It does, however, require that the border router, the LSN, is carrier grade in function and scaling.

6RD, as a technology, is mainly based on a cable operators network topology that cannot be made IPv6 ready. Its base function is to allow IPv6 to be transported over IPv4 seamlessly and as IPv6 has no NAT, it is solely a methodology of wrap-and-tag with an IPv4 embedded address. Much like MPLS, it acts as a forwarding transit, and does not need any particular intelligence relative to the protocol, it just send on, from the edge, to the LSN, a wrapped packet with no intrinsic understanding of what the packet contains, only that it is IPv6. Certain 6RD implementations have allowed L2 to be forwarded, but in a vast majority of cases the IPv6 gateway has a basic function to wrap the IPv6 packet into IPv4.

The simplest 6RD deployment, which uses 32 bits of IPv6 address space to map the entire IPv4 address space, consumes more address space than typical with IPv6 natively supported in all ISP routers. This can be mitigated by omitting redundant parts of the IPv4 address space, and in some cases by deploying multiple 6RD domains.

The default allocation of IPv6 space by a Regional Internet Registry (RIR) is a 32-bit prefix. Since it takes 32 bits to map an IPv4 address with 6RD, this implies that an ISP would only be able to allocate 64-bit IPv6 prefixes to its customers if it were to use entire IPv4 addresses. 6RD, however, allows any redundant part of an IPv4 address to be discarded: For example, if the IPv4 addresses an ISP issues to its customers all share the same first eighteen bits, a 6RD prefix only need include the remaining fourteen bits. Without this flexibility, some internet providers originally assigned 64-bit IPv6 prefixes to its customers but was able to assign them shorter prefixes once it obtained a larger allocation of IPv6 space (a 26-bit prefix) from the RIPE NCC.

6 Domain Functionality

6.1 End to End Network Domains

In order to operate the IPv6 transition technology is has to be engineered and verified end to end across the cable broadband network addressing each of the domains as illustrated in figure 2.

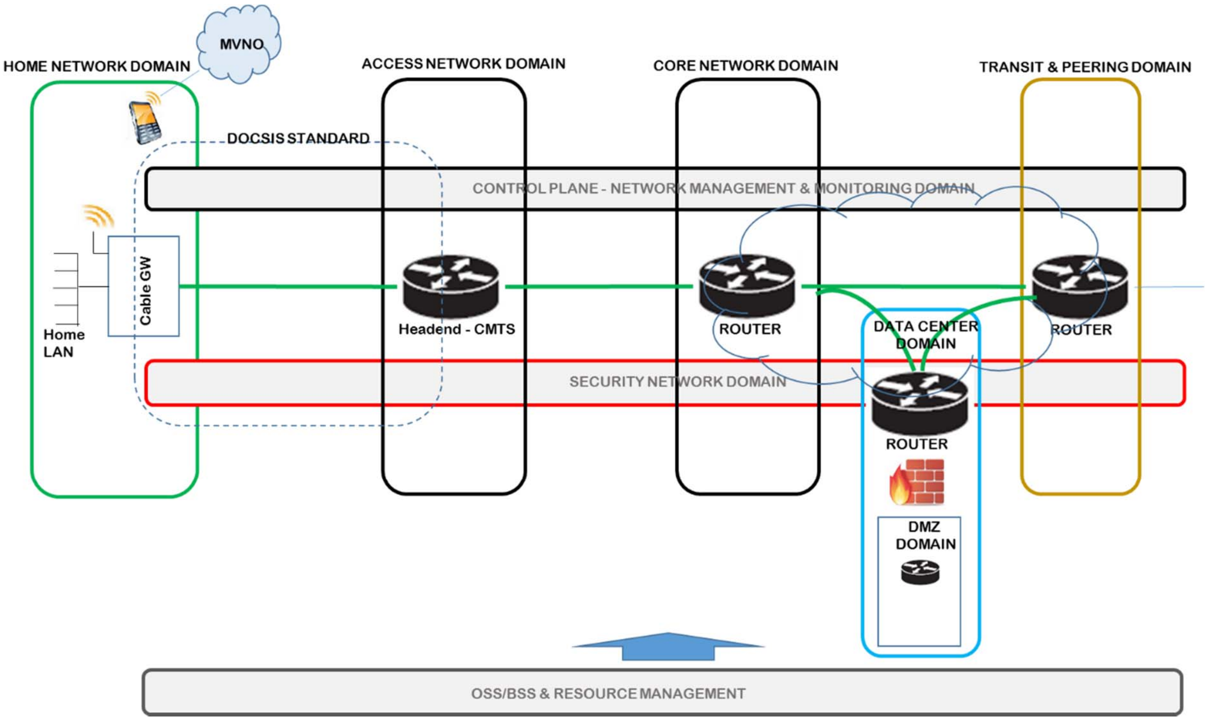

Figure 2: Illustration of the Cable Broadband Network Domains

6.2 CPE Home Network Domain

6RD enables a customer's device that is V6 to be supported across the Cable network when communicating to a V6 service across an IPv4 cable network.

A device that is V4 only can communicate natively with a V4 service without the use of the 6RD-CE and 6RD-BR resources.

Functionality to be engineered in the cable network:

- The cable residential gateway device shall implement the 6RD-CE functionality as defined by IETF RFC 5969 [17].
- IPv4 packet size is 1 500 bytes. When the 20 bytes (IPv4 header) is added for the 6RD encapsulation, the packet size increases to 1 520 which exceeds the DOCSIS 3.0 IP MTU size of 1 500.
- A solution would be to reduce the data field from 1 440 bytes to 1 420 bytes using MSS clamping as detailed within IETF RFC 4459 [18].
- However, as not all service providers will be able to increase their MTU, the 6RD-CE elements will be required to fragment the IPv4 packet before transmission which is reassembled at the 6RD-BR.
- To reduce the impact on CPU processing it is recommended to implement MSS clamping.
- The DOCSIS management between the Cable Modem and CMTS would be IPv4.

Operation:

A V6 packet received by the RG is encapsulated to an IPv4 packet as detailed by IETF RFC 5969 [17] and forwarded to the 6RD-BR.

See also CPE requirements in clause 8.3.

6.3 Access Network Domain

Functionality to be engineered in the cable network:

- The cable headend CMTS shall be capable of IPv6 connectivity for customer traffic.
- The DOCSIS management between the Cable Modem and CMTS would be IPv4.

NOTE: There are no additional requirements on the HFC distribution network i.e. AMPS, taps, etc.

6.4 Core Network Domain

Functionality required:

- The core network routers shall support IPv4 routing and forwarding capabilities.
- 6RD-BR shall be implemented as specified by IETF RFC 5969 [17].

Operation:

A v4 client communicating with v4 service has direct native end to end connectivity and does not utilize the 6RD resources, however a v6 client communicating with a v6 service will utilize the functions of the 6RD-CE and 6RD-BR, forwarding the V4 packets to the 6RD-BR which de-encapsulates the packet and forwards to the v6 server.

The communication between the 6RD-BR and V6 server for the session will be using v6 packets, whereas the communication between the 6RD-CE and 6RD-BR will be using v4 packets so this enables the V6 client to communicate to a V6 service with the 6RD-BR maintaining the state of the session.

See also the LSN requirements in clause 8.2.

6.5 Data Centre Domain

Functionality to be engineered in the cable network:

There are no changes to be engineered when considering 6RD as the network elements remain supporting IPv4 thus there are no additions engineered within the cable network elements.

6.6 DMZ Service Domain

Functionality to be engineered in the cable network:

There are no changes to be engineered when considering 6RD as the network elements remain supporting IPv4 thus there are no additions engineered within the cable network elements.

6.7 Transit and Peering Service Domain

Functionality to be engineered in the cable network:

There are no changes to be engineered when considering the transit and peering domain since the transmit and peering links are dual stack and support both IPv6 and IPv4 packets simultaneously and therefore no specific additional requirements are needed to be defined for this domain.

6.8 Management and Monitoring Domain

Functionality to be engineered in the cable network:

- DOCSIS management between the CMTS and Cable Modem is using IPv4 addresses.
- There is the additional functionality to monitor and manage the 6RD-CE within the RG and monitor and manage the 6RD-BR in order to provide sufficient capacity to scale with the traffic throughput.

6.9 Security Domain

Functionality to be engineered in the cable network:

- The continuity of the security of the end to end service shall be maintained when operating 6RD, however the operational implications from 6RD shall be minimized as specified in IETF RFC 5969 [17] section 12.
- The logging of IPv6 addresses is required for LI and DR purposes.

7 Technical Considerations

7.1 Hardware

There is no change in hardware requirements at the edge, only software dependent forwarding, although the 6RD relays, LSNs, are required but this is usually a software upgrade with no extra hardware needed due to the simplicity of the technology.

7.2 MTU and fragmentation

The maximum DOCSIS MTU size is 1 518 bytes long and the MTU of the 6rd traffic needs to be modified so that the MTU of the DOCSIS transport is not exceeded. The 6rd tunnel MTU has to be reduced to 1 480 bytes. If a packet is received on the LAN interface which exceeds this, it has to be dropped and an ICMP 'fragmentation needed' message sent to the source device.

Fragmentation has to be placed on the ingress interface (virtual or physical) pre decapsulation on upstream and post-encapsulation on downstream on IPv4. All fragmentation on 6RD on the BR and CPE has to be on IPv4 to prevent IPv6 fragmentation requirements and overlay code. IPv6 inherently does not have fragmentation built into it and thus can cause major performance issues on an BR forwarding plane.

Reassembly has to only be used when the BR receives noted IPv4 fragmented packets incoming upstream from the CPE.

Operational considerations:

1) The CE constructs a payload of any size and content to be sent to the BR (e.g. a zero-length null payload, a padded payload designed to test a certain MTU, a NUD message, etc.). The exact format of the message payload is not important as the BR will not be processing it directly.

2) The desired payload is encapsulated with the inner IPv6 and outer IPv4 headers as follows:

    - The IPv6 destination address is set to an address from the CE's 6RD delegated prefix that is assigned to a virtual interface on the CE.
    - The IPv6 source address is set to an address from the CE's 6RD delegated prefix as well, including the same as used for the IPv6 destination address.
    - The IPv4 header is then added as it normally would be for any packet destined for the BR. That is, the IPv4 destination address is that of the BR, and the source address is the CE IPv4 address.

3) The CE sends the constructed packet out the interface on which BR reachability is being monitored. On successful receipt at the BR, the BR shall decapsulate and forward the packet normally. That is, the IPv4 header is decapsulated normally, revealing the IPv6 destination as the CE, which in turn results in the packet being forwarded to that CE via the 6RD mechanism (i.e. the IPv4 destination is that of the CE that originated the packet, and the IPv4 source is that of the BR).

4) Arrival of the constructed IPv6 packet at the CE's IPv6 address completes one round trip to and from the BR, without causing the BR to process the message outside of its normal data forwarding path. The CE then processes the IPv6 packet accordingly (updating keepalive timers, metrics, etc.).

7.3 Reliability

As explained in clause 6.2, when the 20 bytes (IPv4 header) is added for the 6RD encapsulation, the packet size increases to 1 520 which exceeds the DOCSIS 3.0 IP MTU size of 1 500. MTU size of 1 520 is a major issue for the transit network with unmanaged devices.

For operators, the decision to use Cold Standby mode or Hot Standby mode depends on the trade-off between capital cost and operational cost. Cold Standby mode does not require a Backup Standby BR to synchronize session states. This simplifies the operational model. When the Primary BR goes down, any BR with extra capacity could potentially take over. Hot Standby mode provides a smoother failover experience to users; the cost for the operators is more careful failover planning though.

7.4 Quality of Service

The QoS policies defined by the cable operator for their network shall be engineered to operate properly with the new 6RD environment.

A 6RD tunnel can be viewed as a particular case of uniform conceptual tunnel model, as described in IETF RFC 2983 [19]. This uniform model views an IP tunnel only as a necessary mechanism to forward traffic to its destination: the tunnel has no significant impact on traffic conditioning. In this model, any packet has exactly one DSCP field that is used for traffic conditioning at any point, and it is the field in the outermost IP header. In the 6RD model, this is the Traffic Class field in the IPv6 header. Implementations of this model copy the DSCP value to the outer IP header at encapsulation and copy the outer header's DSCP value to the inner IP header at de-capsulation.

Operators should use this model by provisioning the network such that the BR copies the DSCP value in the IPv4 header to the Traffic Class field in the IPv6 header, after the encapsulation for the downstream traffic. Similarly, the B4 copies the DSCP value in the IPv4 header to the Traffic Class field to the IPv6 header, after the encapsulation for the upstream traffic. Traffic identification and classification can be done by examining the outer IPv6 header in the IPv6 access network.

8 LSN and CPE Requirements

8.1 General

The requirements of the 6RD implementation are based on enabling seamless 6RD connections without degradation in service, access, functionality or speed.

Two network components are involved in the end-to-end 6RD approach; the LSN and the CPE. Requirement considerations for both are listed below.

8.2 LSN

The LSN device placed in the edge of the network (IXPE) as the IPv4 gateway to perform de-capsulation on the egress from a 4in6 packet to a pure IPv4 packet. Requirement considerations for LSN are:

- Hardware Topology
- Logical Topology

- Software/Hardware Features
- Scalability
- Resilience and Redundancy
- IP Allocation & DHCP specific features(v4 and v6)
- Forwarding/Convergence Performance
- Monitoring, Management, Reporting & Access
- DR Specifics

8.3 CPE

The CPE is a device in customer's home to encapsulate the traffic on egress from a pure IPv4 packet to a 4in6 packet. Requirement considerations for 6RD CPE are:

- Hardware Topology
- Logical Topology
- Software/Hardware Features
- Scalability
- Stability
- IP Allocation/DHCP (v4 and v6)
- Forwarding performance

9 6RD Feature Requirements

The 6RD features are as summarized in table 1 detailing for each function the requirement as required or optional with a brief description of each of the named functions.

Table 1: Summary of 6RD Features Requirements

Functional Name	Requirement	Description
NAT44 - IETF RFC 4787 [21] (UDP)	Required	Compliance with NAT behaviour according to IETF RFC 4787 [21] for UDP.
NAT44 - IETF RFC 5382 [22] (TCP)	Required	Compliance with NAT behaviour according to IETF RFC 5382 [22] for TCP.
NAT44 - IETF RFC 5508 [23] (ICMP)	Required	Compliance with NAT behaviour according to IETF RFC 5508 [23] for ICMP.
Redundancy	Required	All critical components shall be redundant in such a manner that they can fail-over without impact to customer or management traffic greater than 1 ms.
Anycast	Required	Anycast BR gateway addresses are a requirement to allow simplicity of deployment for a single prefix across multiple BR's.
BR Address withdrawal	Required	The BR should have at least four points of BR GW address withdrawal occurrence. The list includes: - loss of IPv6 route out, - loss of all BGP/IGP sessions, - loss of forwarding, - loss of NPU capacity Any of the failures should be detectable based on configurable timers with 15 seconds being the default setting.

Functional Name	Requirement	Description
Fragmentation	Required	Fragmentation should be done on the IPv4 packet. Fragmentation should be placed on the ASIC running in the line card.
NAT - Network Address and Port Mapping - Endpoint Independent Mapping	Required	For two flows for a common inside source IPv4 address and port, the external address/port translation is independent of the destination IPv4 address and port and when the flows exist simultaneously in the NAT state table they will use the same translation.
NAT - Translation Filtering - Endpoint Independent Filtering	Required	A flow initiated externally can use the existing External/Inside IPv4 address/port mapping and it is independent of the source IPv4 address/port of the senders.
NAT - Paired IP Address Assignment	Required	Translation to External IPv4 address is done in a paired fashion. A given Inside address is always translated to the same External IPv4 address.
NAT - Hair-pinning	Required	Different internal addresses on the same internal interface shall be able reach each other using external address/port translations.
NAT - 1:1 IP Mapping	Required	Ability to configure a one to one type of mapping for particular inside-VRFs: every public IP will be mapped to one and only one private IP (multiple ports are allowed).
NAT44 - Outside-Service-App mapping for inside-VRF	Required	Ability in the inside-vrf to provide the explicit outside serviceapp to be paired.
NAT - Port Limit configuration	Required	A maximum amount of ports can be configured for every IPv6 source B4 address.
NAT - Per-Protocol Timeout configuration	Required	Timeout of mappings is critical and removing a NAT mapping at the appropriate time maximizes the shared port resource.
NAT - Dynamic Port Range start configuration	Required	The start port for dynamic port ranges should be configurable to allow for a range of ports for static port mappings.
NAT - Software Load Balancing	Required	NAT Inside to Outside hashing performed on the Source private IPv4 address. NAT44 Outside to Inside hashing performed on the Destination IPv4 (lower-order 2 bits) address assigned from the pool prefix.
Port Allocation	Required	In order to reduce the volume of data generated by the NAT device (logging creation and deletion data), bulk port allocation can be enabled. When bulk port allocation is enabled and when a subscriber creates the first session, a number of contiguous outside ports are pre-allocated. A bulk allocation message is logged indicating this allocation.
Deterministic NAT	Optional	Algorithmically maps a customer's private IPv4 address to a set of public IPv4 address ports, allowing a significant reduction in logging.
FTP ALG (Active and Passive)	Required	FTP clients are supported with inside (private) address and servers with outside (public) addresses. Passive FTP is provided by the basic NAT function. Active FTP is used with the ALG.
RTSP ALG	Required	Remote control protocol for streamers (which use RTP/RTCP or RDT). Our implementation considers the server is located "outside" and clients are "inside". RTSP is used in many streamers like QuickTime or RealNetworks. Both "SETUP" and "SETUP response" are analysed. Based on this information, the translation entry will be created in the table.
SIP ALG	Required	
PPTP ALG	Required	
Use of Application SVI's, connecting multiple routing entities (inside/private VRF, outside/public VRF)	Required	NAT should be possible from any routing context (VRF, GRT) to any routing context (VRF, GRT).
Stateful ICMP	Required	Stateful ICMP mappings between inside and outside ICMP identifiers should be supported.

Functional Name	Requirement	Description
Thresholds	Required	Configurable thresholds using watermarks should be supported to monitor the resources on the BR.
Chassis NAT Clustering	Optional	Clustering of BR's to allow for inter-chassis resiliency.
PCP	Required	Support for PCP to allocate static port bindings.
Logging via Netflow V9/IPFIX	Required	Netflow v9 support for logging of the translation records. Logging of the translation records can be mandated by for Lawful Intercept. The Netflow uses binary format and hence requires software to parse and present the translation records.
Logging via Syslog	Required	Syslog support for logging of the translation records as an alternative to Netflow. Syslog uses ASCII format and hence can be read by users. However, the log data volume is higher in Syslog than Netflow.
Destination based Logging	Required	Destination Based Logging will generate one record per session, including the destination port and address. NFv9 templates including destination IP address and destination port will be used.
Base Logging Fields	Required	BR logs the following information when a translation entry is created: - Inside instance ID - Outside instance ID - Inside IPv4 Address - Inside Port - Outside IPv4 Address - Outside Port - Protocol - Start Time - Stop Time
Radius Logging	Required	Logging using Radius accounting messages.
XML l	Optional	Logging using XML files.
Static port forwarding (up to 6 K static forward entries per npu)	Required	Static port forwarding configures a fixed, private (internal) IPv6 address and port that are associated with a particular subscriber while the BR allocates a free public IP address and port. Therefore, the inside IPv6 address and port are associated to a free outside IP address and port.
Static port forwarding 1:1 active/standby	Required	Static Port Forwarding mapping will be kept constant with two npu cards in Active/Standby mode.
64 BR instances per npu Card	Required	
20 M+ Translations (per npu)	Required	
Minimum Gbps throughput per npu (Inside-to-outside VRF + Outside-to-inside VRF) with IMIX traffic	Required	
1 M+ connections per second setup rate	Required	
1 M users	Required	
Latency	Required	Latency is between 390 and 580 micro seconds (μs).
6 npu Cards per chassis	Required	
IRB support	Required	Integrated Routing and Bridging (L3 interface for Bridge Domain).
Broadband Network Gateway (BNG) support	Optional	32 k BNG sessions and up to 256 k NAT users at the same time.

10 Network node Requirements

10.1 BR Network node Hardware Feature and Topology

BR is an implementation of an IPv4/IPv6 transition protocol based on 6RD, and is the CORE node that all CPE/CEs running 6RD and creating softwares for the technology connect to. It is the termination for the IPv4 tunnel for native IPv6 traffic and it is the IPv4 NAT device egressing traffic towards the destination on IPv4.

This clause concerns itself solely with the 6RD specific required functionality to allow the technology to function completely and fully. The subsequent clauses specify engineering requirements that allows 6RD technology to be deployed on the BR to be non-service deprecating comparative to a native private IPv4 delivery to any given customer within a Carrier Topology.

10.2 Network node specific requirements

10.2.1 General considerations

In 6RD architecture, only the routers (Border Relay) need a public IPv4 address, so even if subscribers were assigned private IPv4 addresses from the ISP, this would not hinder the connectivity of 6RD tunnels. Users can build 6RD tunnels with Border Relays using private IPv4 addresses, so the scale will not be bounded by the number of public IPv4 addresses owned by the ISP.

The implementation of 6RD can be divided into two parts, configuration of the Customer Edge (CE) and then to build the Border Relay (BR). Setting up the environment for a network would be specific to the network topology and its capabilities.

10.2.2 Integrated topology requirements

List of features required for both IPv4 and IPv6/L2 and L3 for an integrated topology solution:

- MP BGP (as well 6PE and 6VPE)
- BGP Community/32 bit AS
- MPLS LDP (potentially only v4 native at present but the requirement for v6 native MPLS may become an absolute)
- ECMP
- QoS (v4/v6) - classification, priority queuing, etc.
- QPPB/SCU/DCU
- SNMP (transport over v4 and v6) v1/v2/v3
- ACLs/Prefix Listing (both v4/v6)
- TACACS/RADIUS (v4/v6)
- Syslog (event reporting for v4 & v6 as well as transporting over both protocols)
- CoPP (v4/v6)
- Netflowv9 (potentially previous versions will be required depending on the state of the NA4 implementation of Netflow)
- XML (v4 & v6 reporting and transport)
- Mac Accounting

- 802.1q
- Ether-channel
- Ether OAM
- NSF/GR (v4/v6)
- Policy Based Routing (v4/v6)
- ISIS (Potentially MT for ISIS as well if the MPLS IPv6 LDP allows for dual stacking) (v4/v6)
- Static Routing (v4/v6)
- OSPFv2/v3
- CDP/LLDP (v4/v6)
- VRRP/HSRP (v4/v6)
- VLAN Mapping/Double Tagging
- L3 Multicasting/MFIB (v4/v6)
- IPv6 Forwarding
- IPv4 Forwarding
- Ethernet technologies
- Hardware forwarding functionality, instead of software, across all priority flows (v4/v6)
- Virtual Interfaces (v4/v6)
- AAA (v4/v6)
- BFD (v4/v6)
- MLD/L2 Multicast
- Full NDP (ICMPv6, DAD, NUD, etc.)
- PIM/IGMPv2/v3
- CEF/dCEF
- Anycast
- Route Reflection (v4/v6)
- Standard v4 VPN
- ISSU/SSO
- NTP (v4/v6)
- SEND
- IP-Sec
- DNS (v4/v6 server & client)
- DHCP relay (v4/v6)
- MSTP/RSTP
- L2/L3 Load Balancing (v4/v6)

- VPLS (v4/v6)
- L2 Bridging
- NAT64
- 6RD
- NAT Cache Writing
- SSH/Telnet (v4/v6)
- Authentication across most protocols such as SNMPv3/BGP/LDP/ISIS/, etc.
- PS-BGP

10.2.3 Hairpin topology requirements

List of features required for both IPv4 and IPv6/L2 and L3 for a "hairpin topology" solution:

- SNMP (transport over v4 and v6) v1/v2/v3
- ACLs/Prefix Listing (both v4/v6)
- TACACS/RADIUS (v4/v6)
- Syslog (event reporting for v4 & v6 as well as transporting over both protocols)
- CoPP (v4/v6)
- Netflowv9 (potentially previous versions will be required depending on the state of the NA4 implementation of Netflow)
- XML (v4 & v6 reporting and transport)
- 802.1q
- Ether-channel
- Ether OAM
- Static Routing (v4/v6)
- CDP/LLDP (v4/v6)
- VRRP/HSRP (v4/v6)
- IPv6 Forwarding
- IPv4 Forwarding
- Ethernet technologies
- Hardware forwarding functionality, instead of software, across all priority flows (v4/v6)
- Virtual Interfaces (v4/v6)
- Full NDP (ICMPv6, DAD, NUD, etc.)
- CEF/dCEF
- Anycast
- ISSU
- NTP (v4/v6)

- SEND
- BFD
- IP-Sec
- DNS (v4/v6 server & client)
- MSTP/RSTP
- L2/L3 Load Balancing (v4/v6)
- NAT64
- 6RD
- NAT Cache Writing
- SSH/Telnet (v4/v6)
- Authentication across most protocols such as SNMPv3/BGP/LDP/ISIS/, etc.
- PS-BGP
- ECMP

10.3 Scalability

The scalability requirements are dependent on the cable network build and delivery requirements. The values given are examples and would need to be scaled dependent on the network traffic.

Example to illustrate the scalability considerations for a network build should take account of:

1) Minimum number flows per NPU.

2) Number of customer IP sources per NPU.

3) Throughput e.g. 20 Gb/s throughput, 10 Gb/s in, 10 Gb/s out.

4) Load balancing on ingress ports across the chassis.

5) Number of BRs per network region e.g. 2 BR's per network region.

6) Number of global BRs for failover of traffic e.g. 2.

7) Number of secondary bindings per second NPU e.g. 500 k.

8) Initial bindings per second per NPU e.g. 500 k.

9) Scalability configurable for ports per IP and sessions per IP.

10) Minimum throughput per chassis e.g. 120 Gb/s.

11) Minimum number of slots and maximum number of port slots to support the correct sizing of the backplane e.g. 4 slots, maximum 10 port slots, to support a 120 Gb/s backplane.

12) Matching blades using both a NAT NPU and a port card in a single blade.

Engineer monitoring abilities to validate the capacity on the node and scale up the node accordingly.

10.4 Performance

The BR performance should be based on lowest acceptable benchmarks and the actual delivery of throughput, convergence, failover and latency for all aspects and features within the chassis interoperable on the network.

All performance requirements should be based on peak capacity and average throughput and are factors for the platform placement in capacity. Capacity is also based on expected growth of subscribers and increase of throughput per subscriber.

Throughput interfaces

All interfaces shall be engineered to work at line rate e.g. 10 gbps. The interface shall be compatible with the regional network P/PE router connectivity.

Node latency

The required node latency may be engineered to 100 microseconds.

Flow throughput

The flow throughput is defined by three main performance figures:

- CPE initialization
  This is the initialization of the port allocation per subscriber (i.e. when a CPE comes up for the first time) with a single external IP per CPE.

- Primary flow initialization
  Primary flow initialization is if the CPE has already been granted a port allocation but the flow is a "new" flow in the NAT cache, which further defined would be a flow that has no entry except a source IPv6 address already in the cache, so the whole flow needs to be allocated and set into the NAT cache. For example it may be engineered for 800 k flows per 40 Gb/s chassis throughput capacity

- Secondary flow initialization
  engineer the flows per chassis throughput, for example, required performance of 1 million flows per 40 Gb/s chassis throughput capacity.

Convergence

Convergence of routing and link failure should be configured e.g. to be within 10 ms performance.

History

Document history		
V1.1.1	August 2016	Publication