ETSI TS 103 443-5 V1.1.1 (2016-08)

TECHNICAL SPECIFICATION

**Integrated broadband cable telecommunication networks (CABLE);
IPv6 Transition Technology Engineering and Operational Aspects;
Part 5: 464XLAT**

Reference
DTS/CABLE-00018-5

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

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 5 of a multi-part deliverable. Full details of the entire series can be found in part 1 [25].

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 464XPAT 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 part 1 [2] to 3 [4] respectively for NAT64; ETSI TS 103 239 part 1 [5] to 3 [7] respectively for MAP-E; ETSI TS 103 241 part 1 [8] to 3 [10] respectively for DS-Lite; ETSI TS 103 242 part 1 [11] to 3 [13] respectively for XLAT and ETSI TS 103 243 part 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 5 of a multi-part series covering the IPv6 transition technology 464XPAT.

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 464XPAT 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 5 of a multi-part series and presents the operational aspects of the IPv6 transition technology 464XPAT across the cable network domains.

Only those elements of the network that have to be engineered to operate the IPv6 transition technology 464XPAT 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 464XPAT 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 103 242 part 1 [11] to 3 [13].

The operational aspects for the IPv6 transition technology 464XPAT 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 464XPAT 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 4459 (April 2006): "MTU and Fragmentation Issues with In-the-Network Tunnelling".

[18] IETF RFC 6877 (April 2013): "464XLAT - Combination of Stateful and Stateless Translation".

[19] IETF RFC 6145 (April 2011): "IP/ICMP Translation Algorithm".

[20] IETF RFC 6791 (November 2012): "Stateless Source Address Mapping for ICMPv6 Packets".

[21] IETF RFC 6052: "IPv6 Addressing of IPv6/IPv4 Translators".

[22] IETF RFC 6146 (April 2011): "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers".

[23] IETF RFC 7269 (June 2014): "NAT64 Deployment Options and Experience".

[24] IETF RFC 6147: "DNS64: DNS Extension for Network Address Translation from IPv6 Clients toIPv4 Servers", April 2011.

[25] ETSI TS 103 443-1: "Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition Technology Engineering and Operational Aspects; Part 1: General".

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".

[i.3] ETSI TS 103 443-2: "Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition Technology Engineering and Operational Aspects; Part 2: NAT64".

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

Stateful Translation: process of converting IPv4 to IPv6 addresses and vice versa whereby the translating device maintains a mapping table with entries binding IPv6 addresses to IPv4 addresses

NOTE: In this case, an IPv4 address can be mapped to any IPv6 address (certain restrictions apply to the usable address space).

Stateless Translation: process of converting IPv4 to IPv6 addresses and vice versa by applying a well-defined mapping algorithm

NOTE: In this case, an IPv4 address is always mapped to the same IPv6 address (a specific IPv6 range is reserved for the algorithm to operate in).

3.2 Abbreviations

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

6PE	IPv6 Provider Edge
6RD	IPv6 Rapid Deployment
AAAA	Quad-A Resource Record
ALG	Application Layer Gateway
AMPS	Amplifiers
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuit
B4	Basic Bridging BroadBand element
BGP	Boarder Gateway Protocol
BNG	Broadband Network Gateway
CLAT	Customer-side transLATor
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CPU	Central Processing Unit
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
FTP	File Transfer Protocol GW Gateway
GRT	Global Routing Table
GW	GateWay
HA	High Availability
HFC	Hybrid Fibre Coax
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
IXPE	Internet Exchange Provider Edge
LAN	Local Area Network
LI	Lawful Intercept
LSN	Large Scale NAT
MAP-E	Mapping of Address and Port - Encapsulation mode
MPLS	MultiProtocol Label Switching
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAT44	Network Address Translation IPv4 to IPv4
NAT64	Network Address Translation IPv6 to IPv4
NFv9	Netflow Version 9
NPU	Network Processing Unit
PCP	Port Control Protocol
PE	Provider Edge
PLAT	Provider-side ransLATor
PMTU	Path Maximum Transport Unit
PPTP	Point-to-Point Tunnelling Protocol
PPTP	Point-to-Point Tunnelling Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RDT	Reliable Data Transfer

RFC	Request For Comments
RG	Residential Gateway
RTCP	Real-Time Transmission Control Protocol
RTP	Real-Time Protocol
RTSP	Real-Time Streaming Protocol
SEND	SEcure Neighbour Discovery
SIIT	Stateless IP/ICMP Translator
SIP	Session Initiated Protocol
SVI	Switched Virtual Interface
SYSLOG	Syslog Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VRF	Virtual Routing and Forwarding
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 464XPAT 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 464XPAT but it has been considered as a last resort technology. This technology allows customers to access services natively over IPv6 and through translation over IPv4.

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 legacy IPv4 only networks and to enable current and new content to be delivered seamlessly to IPv4 users by deploying network address translation IPv4 to IPv6 (464XLAT).

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 464XLAT 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 464XLAT.

The present document uses network address translation IPv4 to IPv6 (464XLAT) technology to provide a seamless Internet experience to users accessing IPv4 Internet services from an IPv6 only client through a 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 464XPAT across the cable network domains is as illustrated by figure 1.

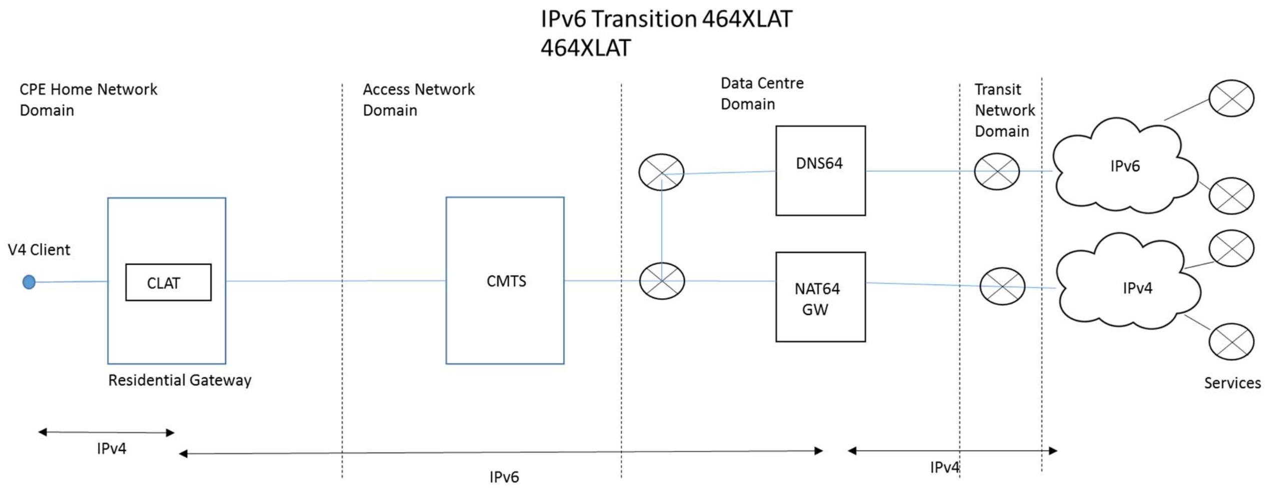

Figure 1: Illustration of network elements to support IPv6 transition technology 464XLAT

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 464XPAT 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 103 242 part 1 [11] to 3 [13].

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

5 Domain Functionality

5.1 End-to-End Network Domains

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

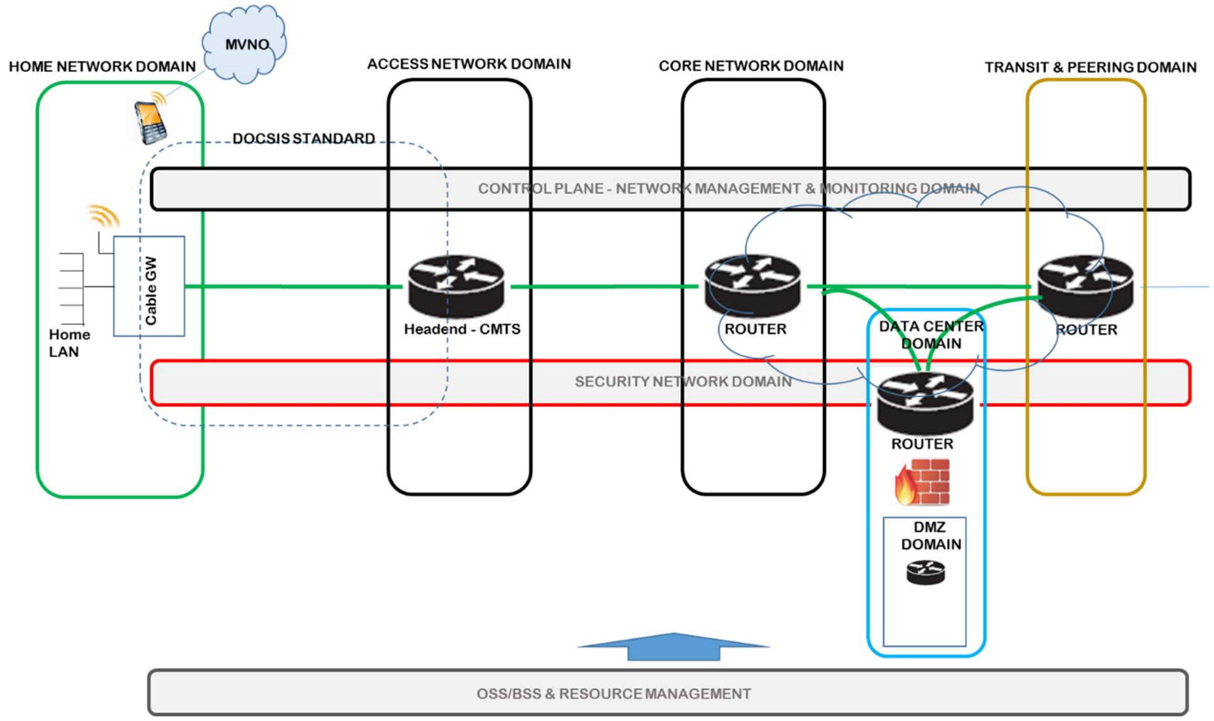

Figure 2: Illustration of the Cable Broadband Network Domains

5.2 CPE Home Network Domain

464XLAT enables a customer's device that is V4 to be supported across the Cable network when communicating to a V4 service.

A device that is V4 only cannot communicate with a V6 service using 464XLAT.

Functionality to be engineered in the cable network:

- The cable residential gateway device shall implement the CLAT functionality as defined by IETF RFC 6145 [19] and updated in IETF RFC 6791 [20].
- IPv4 packet size is 1 500 bytes. When the 20 (40 v6 - 20 v4) bytes is added for the IPv6 translation, 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 1 460 bytes to 1 440 bytes using MSS clamping as detailed within IETF RFC 4459 [17].
- However, as not all service providers will be able to increase their MTU, the CLAT elements will be required to fragment the IPv6 packet before transmission which is reassembled at the NAT64.
- To reduce the impact on CPU processing it is recommended to implement MSS clamping.
- The DOCSIS management between the Cable Modem and CMTS may be IPv4 or IPv6.

Operation:

A V4 packet received by the RG is translated to an IPv6 packet with the original V4 address embedded as detailed by IETF RFC 6052 [21].

The CLAT forwards the IPv6 packet to the NAT64 GW. Refer to clause 5.4 for details of the functionality of the NAT64.

5.3 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 may be IPv4 or IPv6.

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

5.4 Core Network Domain

Functionality to be engineered in the cable network:

- The core network routers shall support IPv6 routing and forwarding capabilities
- NAT64 gateway shall be implemented as specified by IETF RFC 6146 [22] for further information on its operation refer also to IETF RFC 7269 [23].

Operation:

A v6 client communicating with v6 service has direct end to end connectivity and does not utilize the XLAT or NAT64 resources, however a v4 client communicating with a v4 service will utilize the functions of the XLAT as given in clause 5.2, forwarding the V6 packets to the NAT64 GW which translates the address family from IPv6 to a shared IPv4 address which is then forwarded to the v4 server.

The communication between the NAT64 and V4 server for the session will be using v4 packets, whereas the communication between the CLAT and NAT64 gateway will be using v6 packets so this enables the V4 client to communicate to a V4 service with the NAT64 gateway maintaining the state of the session.

5.5 Data Centre Domain

Functionality to be engineered in the cable network:

- The DNS64 shall be implemented when operating IPv6 transition technology NAT64. The requirements for DNS64 shall be in accordance with IETF RFC 6147 [24].
- The DSN64 functionality replaces the exiting DNS caching server within the cable network.

Operation:

For an IPv6 request from the client to the DNS64 server if a valid IPv6 response is received by the DSN64 server then this is returned to the client. In this case the v6 client shall have a direct connectivity with the V6 service. The NAT64 server is not involved.

If it does not receive an IPv6 record then a synthetic AAAA record is created from the IPv4 record as specified by IETF RFC 6147 [24] to direct the IP packets to the NAT64 gateway. The NAT64 gateway then translates the address family as defined in clause 6.

The DHCP server is inherently IPv6 only. The DHCP server shall include the DNS64 IPv6 addresses in its reply options to the CPE.

5.6 DMZ Service Domain

Functionality required:

- There are no specific operational requirements for the DMZ however it is strongly recommended that all services within the DMZ are IPv6 capable either by dual stack configuration or the use of V6/V4 load balancing.

- V6/V4 load balancers allow V6 access to existing v4 services such as a web server avoiding the need to engineer v6 only content on these servers.

To minimize the impact on the NAT64 server from the requirement of network address translation for the network providers own services then all services within the DMZ shall be IPv6 capable.

5.7 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.

5.8 Management and Monitoring Domain

Functionality to be engineered in the cable network:

- DOCSIS management between the CMTS and Cable Modem may remain deployed either using IPv4 or IPv6 addresses.
- There is the additional functionality to monitor and manage the CLAT within the RG and monitor and manage the NAT64 gateway and DNS64 server in order to provide sufficient capacity to scale with the traffic throughput. Also the available V4 address pool shall need to be managed based on the number of customers and the address sharing ratio between the V6 and V4 ports e.g 16 customers sharing 1 IPv4 address.

5.9 Security Domain

Functionality to be engineered in the cable network:

- The cable modem packet classifiers shall be updated to support IPv6 filtering.
- The continuity of the security of the end to end service shall be maintained when operating NAT64, however the operational implications from NAT64 shall be minimized as specified in IETF RFC 7269 [23] section 9, IETF RFC 6147 [24] section 8 and IETF RFC 6146 [22] section 5 and for the CLAT as specified by IETF RFC 6877 [18] section 8.
- The logging of IPv4 addresses for LI and DR purposes shall additionally contain the IP port and the customers IPv6 address.

6 Topologies

This clause explains the potential XLAT domain topologies. At the time of writing, two topologies are possible, the integrated topology and the hairpin topology; however, depending on future hardware and software developments, additional topologies may be introduced.

Use of the integrated topology would provide the most flexibility, as in the hairpin topology the use of an IGP is required and will not allow to connect the BNG anywhere on the core to any PE without running BGP in the core.

To support the hairpin topology P-routers may need to be converted into PE-routers or extra PE-router devices may need to be deployed for one to distribute the BNG's as one wish to.

In the integrated topology the BNG would function as a full MPLS 6PE router.

In the hairpin topology the BNG functions as L3 router, hair-pinning connections through an external 6PE router. This topology would only be used when application of the integrated topology is not possible.

7 Technical Considerations

7.1 General

The XLAT mechanism is used to access the IPv4-only content in the operator's network and to use 464XLAT IPv4 traffic to enable IPv4-only applications to work on IPv6-only networks. The 464XLAT architecture is a combination of stateless translation on the customer-side translator (CLAT) and stateful translation on the provider-side translator (PLAT). The 464XLAT architecture is used to translate the packet information of a device using the combination of stateless (translates private IPv4 address to global IPv6 addresses, and vice versa) and stateful (translates IPv6 addresses to global IPv4 addresses, and vice versa) translation as defined by IETF RFC 6877 [18].

The 464XLAT architecture, provides IPv4 connectivity across an IPv6-only network by combining existing and well-known stateful protocol translation on PLAT in the core and stateless protocol on CLAT at the edge. The private

IPv4 host can reach global IPv4 hosts through both CLAT and PLAT translation. Conversely, the IPv6 host can directly reach other IPv6 hosts on the Internet without translation. This means that the customer premises equipment (CPE) can support CLAT and also operate as an IPv6 native router for native IPv6 traffic.

464XLAT provides limited IPv4 connectivity across an IPv6-only network by combining existing and well-known stateful protocol translation IETF RFC 6146 [22] in the core and stateless protocol translation IETF RFC 6145 [19] at the edge.

464XLAT combines IETF RFC 6145 [19] and IETF RFC 6146 [22] together to create a new transition technology which is found to be simpler to deploy and available both commercial and with open source products. It is very effective at providing basic IPv4 service to consumers over IPv6-only access networks, but has the limitation of the ALG. If correctly implemented it creates efficient use of very scarce IPv4 resources and an IPv6-only network that is simpler and therefore less expensive to operate. Combined with DNS64, a cable operator can provide sharing IPv4 address and IPv4/IPv6 translation at same time and can perform IPv6 traffic engineering without deep packet inspection. Where ISPs operate PLAT as PLAT providers, ISPs for IPv6 consumers can independently perform IPv6 traffic engineering on common backbone routers.

7.2 MTU and fragmentation

464XLAT is an address family translation technology and has less MTU issues than tunnelling technologies. But this does not imply that MSS clamping, IPv4 fragmentation and IPv6 fragmentation are not required in order to avoid ICMP blocking. Fragmentation resends and general PMTU control can have performance effects on customer services. Therefore, it is a requirement to optimize implementations such that they do not cause a large impact on current RTTs and node latency.

7.3 Reliability Considerations

To increase reliability and robustness or to distribute the load, network operators may decide to deploy multiple BNGs, to share load across a large network footprint. In the case of having multiple BNGs deployed, the IPv6 destination prefixes should be Anycast based if stateless and the client should hold a primary and secondary if stateful.

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 464XLAT environment.

QoS considerations are relative with PLAT deployments unlike XLAT. The QoS capabilities for 464XLAT are comparable to NAT64, see clause 9.5 of ETSI TS 103 443-2 [i.3].

A XLAT stream can be viewed as a particular case of uniform conceptual tunnel model. 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 PLAT 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.

Network operators should use this model by provisioning the network such that the BNG copies the DSCP value in the IPv4 header to the Traffic Class field in the IPv6 header or the other way around, after the translation for the downstream or upstream traffic. Similarly, the B4 copies the Traffic Class field value in the IPv6 header to the DSCP to the IPv4 header. Traffic identification and classification can be done by examining the outer IPv6 header in the IPv6 access network and IPv4 in the corresponding CORE network after the LSN.

8 Technical Requirements

8.1 General

The client uses a SIIT translator to convert IPv4 packets into IPv6 to send (over an IPv6-only network) to a NAT64 translator which translates them back into IPv4 to send (over an IPv4-capable network) to an IPv4-only server. The SIIT translator (CLAT) may be implemented on the client itself or an intermediate IPv4-capable LAN (but if it had IPv4 Internet connectivity, 464XLAT would not be needed), and the NAT64 translator (PLAT) shall be able to reach both the server and the client (through the CLAT). The use of NAT64 limits connections to a client-server model using UDP, TCP, and ICMP.

IPv6-only + 464XLAT topologies take NAT64 a step further PLAT and CLAT diversification in multiple forms. The positives of the technology allows the solving of IPv4 address depletion issue by not assigning IPv4 to clients and allowing IPv4-only applications to work on an IPv6-only network.

464XLAT is an IPv6 transition technology documented in IETF RFC 6877 [18], which enhances on previous technologies such as NAT64 and DNS64. The problem with just using NAT64 and DNS64 is that specific applications, could not function through NAT64 without a specific and complex ALG but by using 464XLAT you can provide native IPv6 connectivity where possible and allow these types of services and applications to function through your cable network.

8.2 High Level Requirements

8.2.1 General

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

Two network components are involved in the end-to-end XLAT approach; the BNG and the CPE. Requirement considerations for both are given in the following clauses.

8.2.2 BNG

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 BNG are:

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

While networks and devices migrate to IPv6, there are many applications and services that will continue to support only IPv4. This causes many interoperability challenges, especially with peer-to-peer communication services, even with the use of NAT64 and DNS64 technologies. With 464XLAT support, which builds on NAT64, cable operators can deploy a scalable technique that provides access to IPv4 services over IPv6-only networks without encapsulation. CLAT and PLAT are the client-side and provider-side, respectively, stateful translators that translates N:1 global IPv6 addresses to IPv4 addresses.

8.2.3 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 XLAT CPE are:

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

8.2.4 Scalability

The details of the scalability are structured below showing the requirements for delivery in any single case/footprint.

An XLAT solution can actually have lower scaling and performance capabilities than other transition technologies due to the address embedding and ALG requirement. So a minimum of 100 000 CPE addresses can be a difficult scale. Carrier grade solution can have latency issues, especially on primary flows and ALG functions, and this has a direct correlation to the processing requirement.

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 of flows per NPU e.g. 4-6 million.
2) Throughput: e.g. 60 Gb/s throughput on a single direction.
3) Load balancing on ingress ports across the chassis.
4) Number of LSNs per cluster e.g. two as a minimum.
5) Number global LSNs for failover of traffic e.g. Two global LSNs.
6) Number bindings per second NPU e.g. 500 k.
7) Number of initial bindings per second per NPU e.g. 500 k.
8) Scalability configurable for sessions per IP.
9) Minimum throughput per chassis e.g. 120 Gb/s.
10) 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.
11) Matching blades using both a NAT NPU and a port card in a single blade.

8.2.5 Performance

To increase reliability and robustness or to distribute the load, cable operators may decide to deploy multiple LSNs, to share load across a large footprint. In the case of having multiple LSN's deployed, the IPv6 destination prefixes shall be Anycast based if stateless and the client should hold a primary and secondary if stateful.

9 XLAT Feature requirements

The XLAT technology feature is summarized in table x detailing for each function the requirement as required or optional with a brief description of each of the named functions.

Table 1: Summary of 464XLAT Features Requirements

Functional Name	Requirement	Description
IETF RFC 6877 [18]	Required	464XLAT: Combination of Stateful and Stateless Translation.
IETF RFC 6052 [21]	Required	IPv6 Addressing of IPv4/IPv6 Translators.
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.
Shared Resource	Required	Single PLAT GW Prefix. The PLAT IPv6 prefix should be able to be shared amongst different NPU's in the PLAT. A hashing mechanism should be in place to hash all upstream packets based on the source IPv6 address.
Si-ID	Optional	Tunnel/customer identifier based on both IPv6 CLAT prefix public & IPv4 Client Private addresses embedded in the IPv6 source address.
PLAT Addressing & Virtual Interfaces	Required	PLAT shall be able to assign a single virtual interface with up to 8 PLAT GW prefixes for any given 464XLAT instance on the node.
Anycast	Required	Anycast PLAT gateway prefixes are a requirement to allow simplicity of deployment for a single prefix across multiple PLAT's.
PLAT Address withdrawal	Required	The PLAT should have at least five points of PLAT GW prefix withdrawal occurrence. The list includes: - loss of route out, - loss of all BGP/IGP sessions, - loss of forwarding, - loss of NPU capacity and certain errors in the NAT caching. Any of the failures should be detectable based on configurable timers with 15 seconds being the default setting.
NPU Load Balancing (hashing)	Required	464XLAT Inside to Outside hashing performed on the Source IPv6 (x bits) prefix of the CLAT device. 464XLAT Outside to Inside hashing performed on the Destination IPv4 (lower-order 2 bits) address assigned from the pool prefix.
MTU	Required	Due to a larger header size for IPv6 packets, the MTU shall be configurable. Expected value will be 1480 bytes.
MSS Clamping	Required	TCP MSS support is mandatory for the PLAT due to the removal of an end-to-end MTU sizing functionality. This will avoid the need for excessive fragmentation.
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.

Functional Name	Requirement	Description
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 IPv6 CLAT prefix 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).
NAT - 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 CLAT prefix.
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 IPv6 CLAT Prefix. 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.
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.
Thresholds	Required	Configurable thresholds using watermarks should be supported to monitor the resources on the PLAT.
QoS translation	Required	For QoS consistency, the Traffic Class of the inbound IPv6 packet should be copied into the DSCP field of the outbound IPv4 packet. The DSCP of the inbound IPv4 packet should be copied into the Traffic Class field of the outbound IPv6 packet.
Chassis NAT Clustering	Optional	Clustering of PLAT's to allow for inter-chassis resiliency.
PCP	Required	Support for PCP to allocate static port bindings.
per IPv4 user port limiting	Optional	The ability to assign port blocks per private IPv4 address.

Functional Name	Requirement	Description
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	PLAT logs the following information when a translation entry is created: - Inside instance ID - Outside instance ID - Inside IPv6 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 PLAT 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 PLAT instances per npu Card	Required	
20 M+ Translations (per npu)	Required	
Minimum 10 Gbps throughput per npu (Inside-to-outside VRF + Outside-to-inside VRF) with IMIX traffic	Required	
1M+ connections per second setup rate	Required	
Minimum 1M users (private IPv6 CLAT prefixes on the inside)	Required	
Latency	Required	Latency is between 390 and 580 micro seconds (µs).
Minimum 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.

Annex A (informative): Bibliography

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

History

Document history		
V1.1.1	August 2016	Publication