

# IPv6 TRANSITION IN FIXED AND MOBILE ENVIRONMENTS

PLANNING A STRATEGY AND  
NAVIGATING THE ISSUES

TECHNOLOGY WHITE PAPER

IPv6 migration has become an important topic for most network operators as the projected increase of Internet Protocol (IP) – enabled applications, services and consumer devices – is expected to exhaust the available public IPv4 address space in the coming years.

Although IPv6 has been around for some time, very few operators have been adopting IPv6 in the residential wireless/wireline environment to date. As a result, service providers require the tools to continue to grow the Internet adoption while introducing IPv6. This white paper discusses different strategies to adopt IPv6 while continuing to support IPv4 services in residential broadband environments.

# TABLE OF CONTENTS

1. The Internet today / 1
  - 1.1 IPv4 address exhaust / 1
  - 1.2 IPv6 transition: A multi-dimensional problem / 1
  
2. Implications of IPv6 support in carrier environments / 4
  - 2.1 IPv6 in combination with PPPoX in Telco environments / 4
  - 2.2 IPv6 in combination with IPoE in Telco environments / 6
  - 2.3 IPv6 and DOCSIS 3.0 in cable environments / 7
  - 2.4 IPv6 in mobile environments based on R7 or R8 3GPP / 8
  
3. IPv6 transition scenarios / 9
  - 3.1 Scenario 1: IPv6 single stack / 9
  - 3.2 IPv4/IPv6 dual-stack deployment options / 12
  
4. Carrier grade network address translation / 16
  
5. Summary / 18
  
6. References / 19
  
7. Abbreviations / 20

# 1. THE INTERNET TODAY

## 1.1 IPv4 address exhaust

The IANA Public IPv4 address space was exhausted in January 2011. The highest levels of the Internet addressing authorities have been assigned the latest available public IPv4 address blocks. A number of factors, including the amount of unused Public IPv4 address space available and the amount of addresses required to sustain network service growth, will decide how soon this affects individual cases. Depending on these factors, service providers will eventually feel the impact on their service offerings.

Although IPv6 has been around for some time, very few service providers have actually introduced IPv6 in residential broadband networks. Studies indicate that less than 1% of the top 1000 websites support IPv6, and certain applications on the end devices do not support IPv6 connectivity at all.

This situation poses multiple issues to carriers such as:

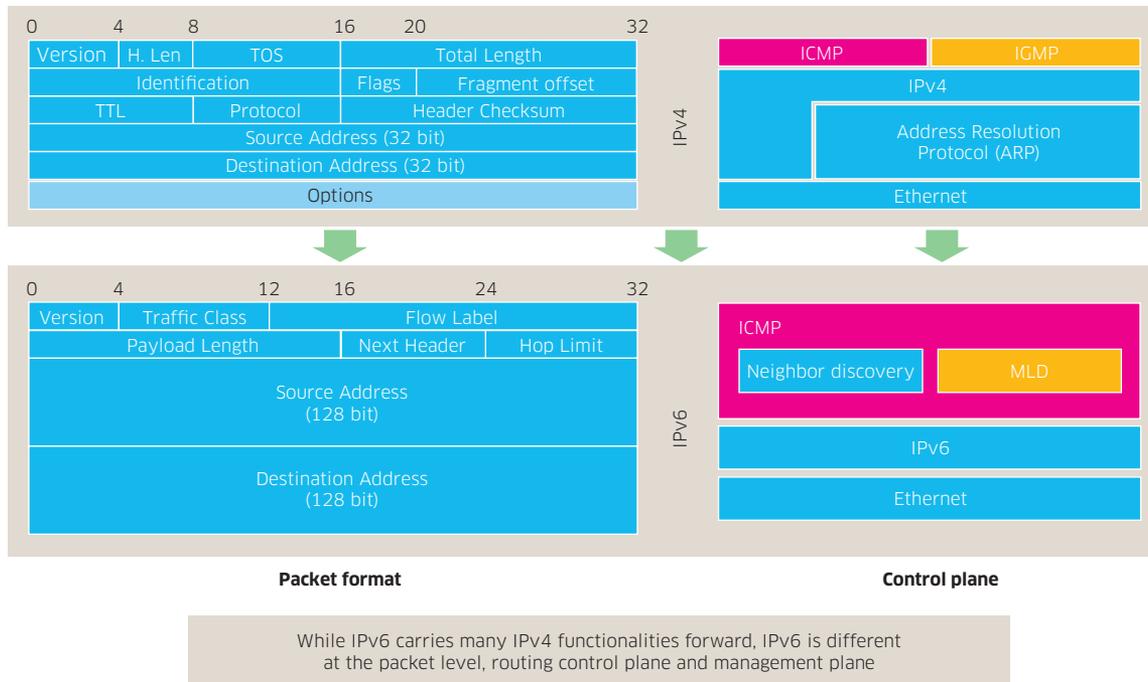
- How to continue growing the network when there are no new Public IPv4 addresses available
- How to connect legacy devices that only support IPv4
- How to continue offering service to websites on the Internet that are IPv4 only
- How to support legacy applications that do not support IPv6 connectivity

This white paper contains a detailed discussion of these issues and questions, and examines the design considerations for the different solutions available for both wireline and wireless environments.

## 1.2 IPv6 transition: A multi-dimensional problem

While the IETF started work on IPv6 in 1990, there has been limited IPv6 adoption to date in residential environments. Although government institutions have been pushing service providers to adopt IPv6, so far there have not been strong business drivers for service providers to introduce IPv6. There were no new applications that required IPv6 while the cost of introducing IPv6 was perceived as high. All of this has resulted in service providers placing very little focus on introducing IPv6 in the residential broadband networks to date. However, with the Public IPv4 address exhaustion and the very rapid adoption of smartphones and M2M devices, the introduction of IPv6 is becoming urgent in order to sustain Internet growth and provide customers with proper service.

**Figure 1. IPv4 versus IPv6: Fundamental differences in packet format and control plane**

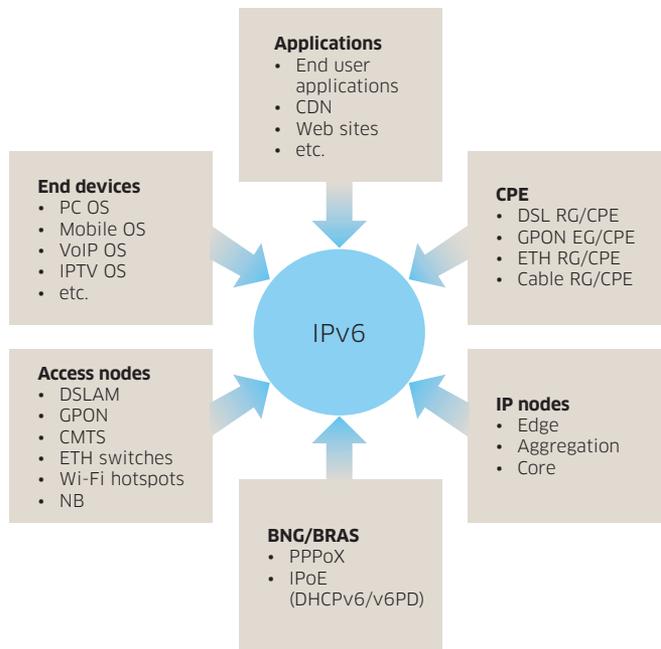


At the heart of the problem lies the fact that IPv6 is technically incompatible with IPv4 (see Figure 1) and has introduced several new concepts that change the present operation of broadband networks such as:

- IPv6 addressing – unicast: Link local addresses (LLA), global unicast address (GUA) and unique local address (ULA), multicast addressing, deprecation of broadcast addressing
- IPv6 header changes: Next Header, etc.
- SLAAC: Stateless address auto-configuration for IPv6 addresses without consuming a DHCP server
- Default router support using Route Advertisements (RA)
- DHCP PD: DHCP prefix delegation to assign prefixes to home networks
- Neighbor discovery (ND), Multicast Listener Discovery (MLD), etc. supported through ICMP

Although there have been many valid reasons for these changes, these concepts have ramifications on how IPv6 can be offered to residential subscribers.

Figure 2. Introducing IPv6 is a multi-dimensional problem



Moreover, IPv6 poses multi-dimensional issues (Figure 2) with requirements over which service providers have no or little control. IPv6 has also implications on multiple elements, as follows:

- End-user devices (hardware and operating systems)
  - PC: MAC OS, Linux, Windows Vista/7 have solid IPv6 support while Windows XP operates only in dual-stack mode and earlier Windows versions have no IPv6 support!
  - IPv6 support on mobile handsets are emerging (iPhone, Android, Symbian, etc.)
  - VoIP Operating Systems have little IPv6 support to date
  - IPTV OSs and Set-top boxes have little IPv6 support to date
  - CPE/RG: Support for IPv6 is emerging on xDSL/GPON/ETH/cable residential GW
- Access nodes
  - DSL/GPON/ETH: Most vendors start supporting certain architectures for IPv6
  - CMTS: Most vendors support IPv6
- Aggregation/Edge/Core network elements
  - Most of devices deployed have supported IPv6 for many years
- Fixed (BNG/BRAS), MGW (GGSN/PGW) Edge node
  - BNG/BRAS: Emerging support for IPv6 in PPPoX, IPoE (DHCPv6/DHCPv6 PD), LNS
  - GGSN/PGW: Widespread support for R8 and R7 3GPP IPv6 architectures
- Applications
  - End-user applications: Proper OS support, API(s) for IPv6 network connectivity
  - Websites: Support for IPv6 addressing/connectivity
  - Content Delivery Networks: Support for IPv6 addressing/connectivity

The implications on some of these elements depend on the network design that is chosen for introducing IPv6. The following chapter highlights the implications of certain scenarios in Telco, cable and mobile environments, with focus on unicast IPv6 connectivity.

# 2. IMPLICATIONS OF IPV6 SUPPORT IN CARRIER ENVIRONMENTS

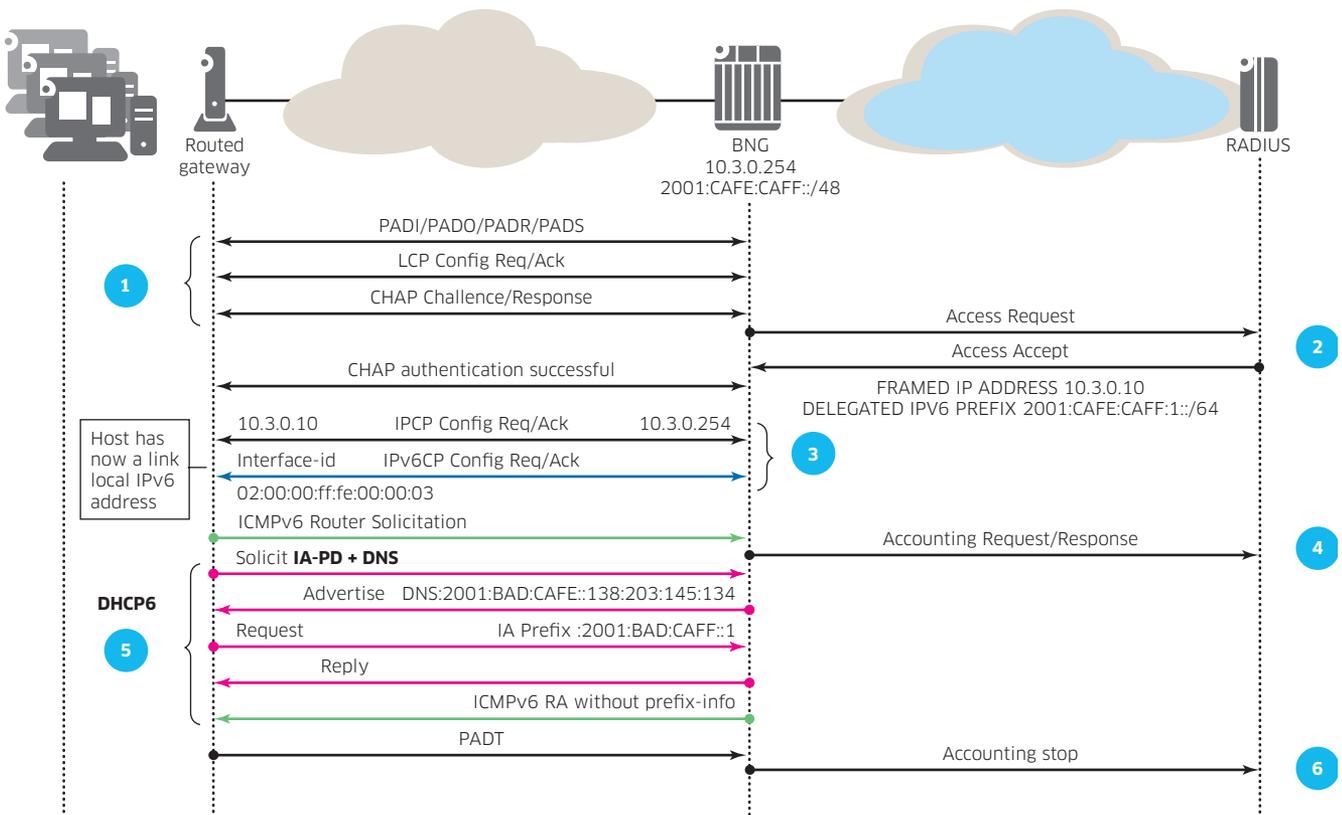
## 2.1 IPv6 in combination with PPPoX in Telco environments

IPv6 support in Telco environments using Point-to-Point Protocol over Ethernet (PPPoX) and/or ATM is defined in TR-187 of the Broadband Forum. The introduction of IPv6 using PPPoX/L2TP has no implications on the access and aggregation network elements. PPP session authentication for IPv6 is identical to IPv4, using PAP/CHAP or option 82. IPv4 and IPv6 authentication can be done in a single authentication phase to optimize RADIUS transactions. Since PPPoX IPv6CP is only defining the Link Local Address, global IPv6 addresses are typically assigned using DHCP or SLAAC. To support an IPv6 routed Residential Gateway (RG) using the PTA/LNS model, the following mechanisms are required between the RG and the BNG/BRAS to ensure IPv6 connectivity:

- PPPoX IPv6CP for Link-Local Address (LLA) assignment.
- DHCPv6 Prefix Delegation (IA-PD) is used to obtain a prefix for LAN address assignment.
- Stateless DHCPv6 is used to obtain additional configuration parameters.
- When the numbered RG model is deployed, stateful DHCPv6 (IA-NA) is used to obtain an RG management IPv6 address; in case of an unnumbered RG model, this is not required.
- Route advertisements are required to assign the default GW assignment.

Figure 3 shows a flow diagram of how to establish IPv6 connectivity using a routed RG PPP model.

Figure 3. Telco IPv6 PPPoE-based access – routed home: DHCPv6 Prefix Delegation (PD)



Another option to provide IPv6 connectivity with PPPoX is by using the Bridged Residential Gateway (also called the “host model”). The following mechanisms are required between the end-device (PC typically) and the BNG/BRAS to ensure IPv6 connectivity in this model:

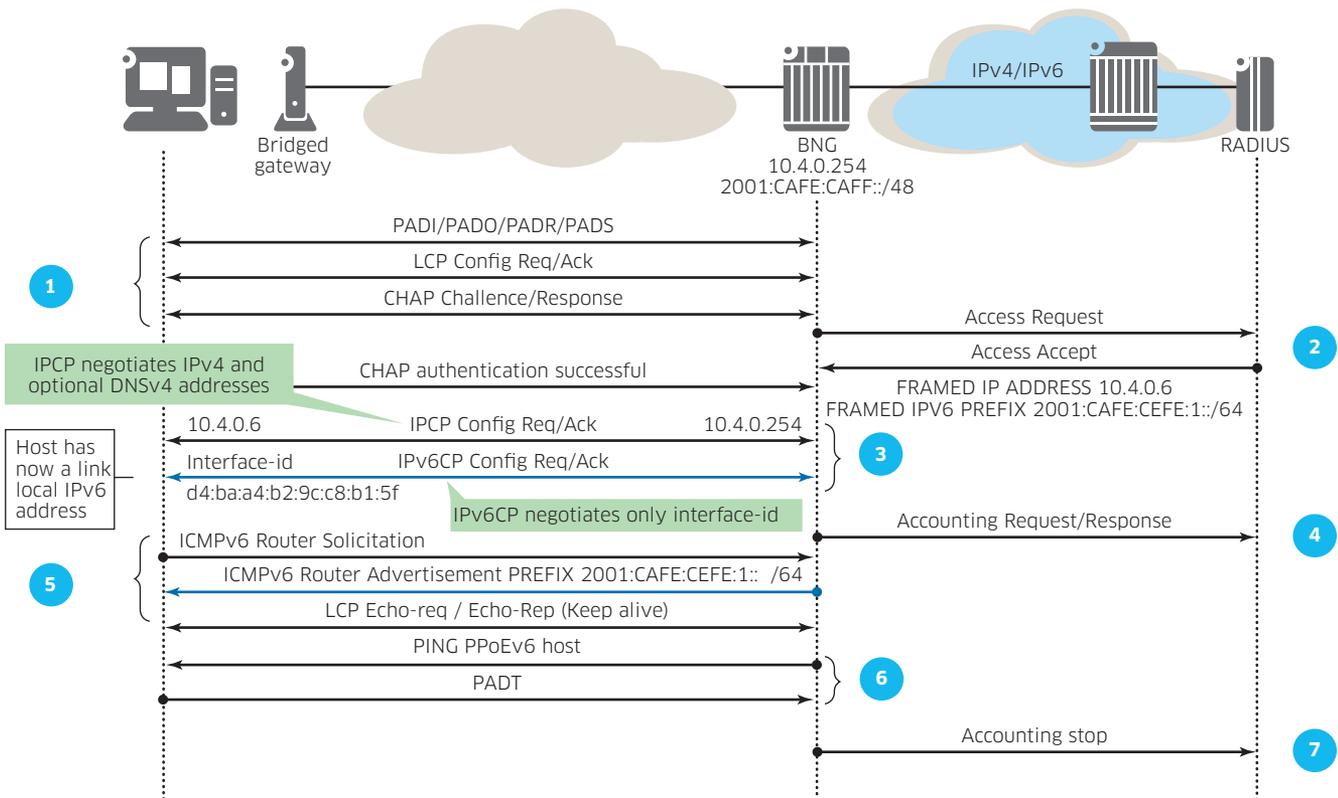
- PPPoX IPv6CP for LLA assignment
- SLAAC used for the host to obtain a Global-Unicast IPv6 address
- Stateless DHCP can be used to obtain additional configuration parameters
- Route advertisements are required to assign the default GW assignment

Figure 4 shows a typical flow diagram of how IPv6 connectivity is established using PPPoX in a bridged RG environment.

PPPoX for IPv6 imposes no different requirements on N:1 VLAN or 1:1 VLAN architectures compared to IPv4.

To support IPv6 in a Telco environment, using PPPoX only impacts the BNG/BRAS, CPE and/or RG, depending on whether bridged or routed RG are deployed. If RADIUS is used for authentication, accounting and CoA (Change of Authorization), some new attributes also need to be supported in the AAA environment.

Figure 4. Telco IPv6 PPPoE-based access – bridged home: Stateless Address AutoConfiguration (SLAAC)



## 2.2 IPv6 in combination with IpoE in Telco environments

Broadband Forum specification TR-177 defines support for IPv6 in Telco environments based on IpoE (IP over Ethernet). The implications for introducing IPv6 IpoE mainly depend on the VLAN model used (1:1 or N:1), and the operational model of the home gateway (bridged or routed).

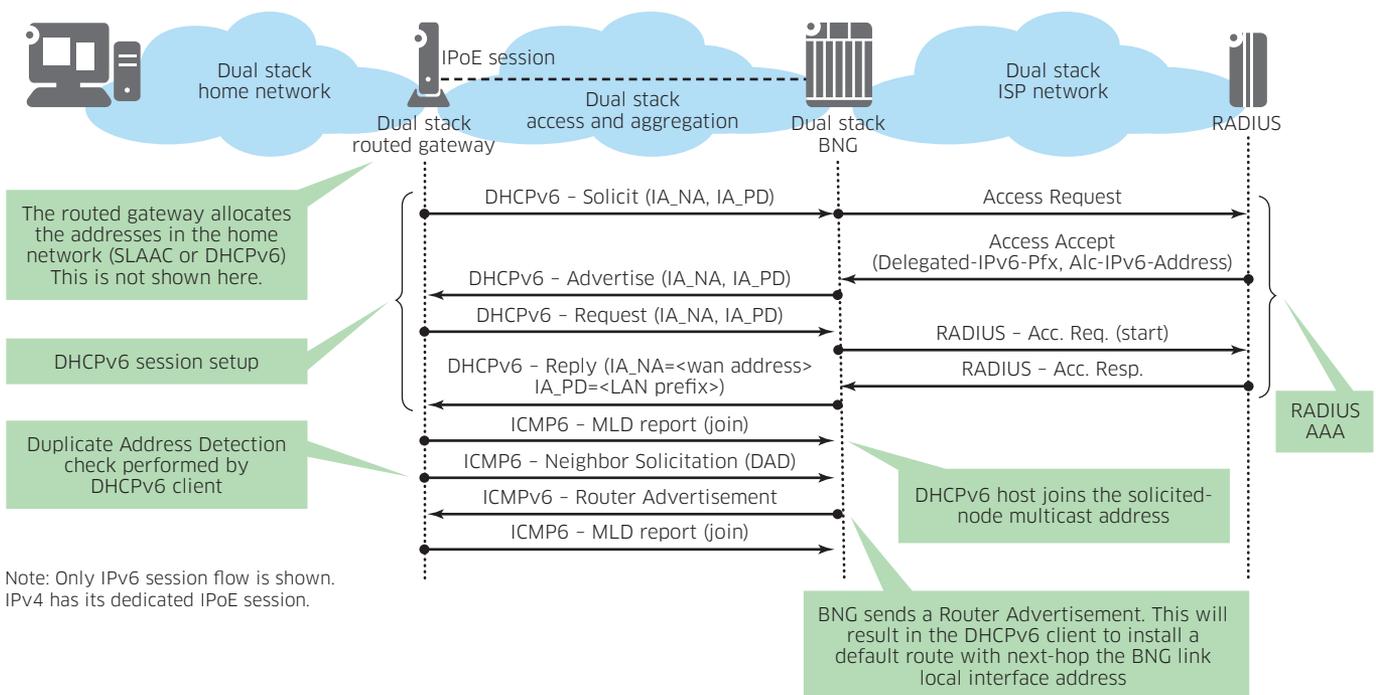
In a 1:1 VLAN model, the home identity can be derived from the VLAN ID. As such, it is possible to deploy IPv6 without any changes to the access/aggregation network if the existing devices support the basic IPv6 forwarding mechanism. When an N:1 VLAN model is deployed, the Access Node has to support at a minimum a Lightweight DHCP Relay Agent (LDRA), as defined in IETF draft-ietf-dhc-dhcpv6-ldra-03, to ensure that the BNG/BRAS can determine from which subscriber the DHCP request was received. It is further advised that anti-spoofing on the access node be supported.

To support IPv6 for the Routed Residential Gateway model using the DHCPv6, the following mechanisms are required between the RG and the BNG/BRAS to ensure IPv6 connectivity:

- DHCPv6 prefix delegation (IA-PD): A unique per-subscriber IPv6 prefix is delegated to the RG for use within the home network
- DHCPv6 WAN address assignment to the RG if a numbered RG model is used
- A default route is installed on the receipt of a valid Router Advertisement from the BNG with a next-hop of the BNG link-local address

Figure 5 depicts a typical flow diagram of the IPv6 connectivity setup using a routed RG IpoE model.

Figure 5. IPv6 for IpoE using xDSL/FTTx Access - Routed Home: DHCPv6 Prefix Delegation (PD)



The impact of IPv6 support for IPoE in a Bridged Residential Gateway model depends on whether DHCP or SLAAC is used to the end device. When deploying DHCP, the main difference from the Routed RG IPoE model comes from the fact that there is no DHCP PD address required and only an IA address is assigned to the host. Care must be taken to ensure communication between IPv6 devices in the home remains local and is not sent via the BNG.

Stateless address auto-configuration (SLAAC) poses a whole new set of issues. In an N:1 VLAN model, the BNG cannot determine from which subscriber a Router Solicitation (RS) message is originating and hence the BNG is unable to decide which Prefix to send back in the Route Advertisement (RA) messages. To overcome this issue, the Access Node should add a Line Identification option in the RS messages, in the same way as it is done for DHCPv6. The BNG needs to ensure that the RA, as a response to an RS, is sent such that the Access Node can forward the RA to the proper subscriber.

Furthermore, due to the split-horizon forwarding behavior of an access network, it must be ensured that Duplicate Address Detection (DAD) is still functioning properly, since DAD messages are not sent to neighboring subscribers. The BNG must assist in ensuring DAD is still functioning properly by supporting a DAD proxy function. Since these issues are still being discussed in IETF, they may arise in most current implementations of Access Nodes and BNG(s).

### **2.3 IPv6 and DOCSIS 3.0 in cable environments**

In a cable environment, IPv6 connectivity is defined in DOCSIS 3.0. The main elements involved in the IPv6 connectivity establishment are the CPE/RG, the Cable Modem Termination System (CMTS) and the DHCP server. The CMTS acts as the Edge Router and as a DHCP relay with a central DHCP server.

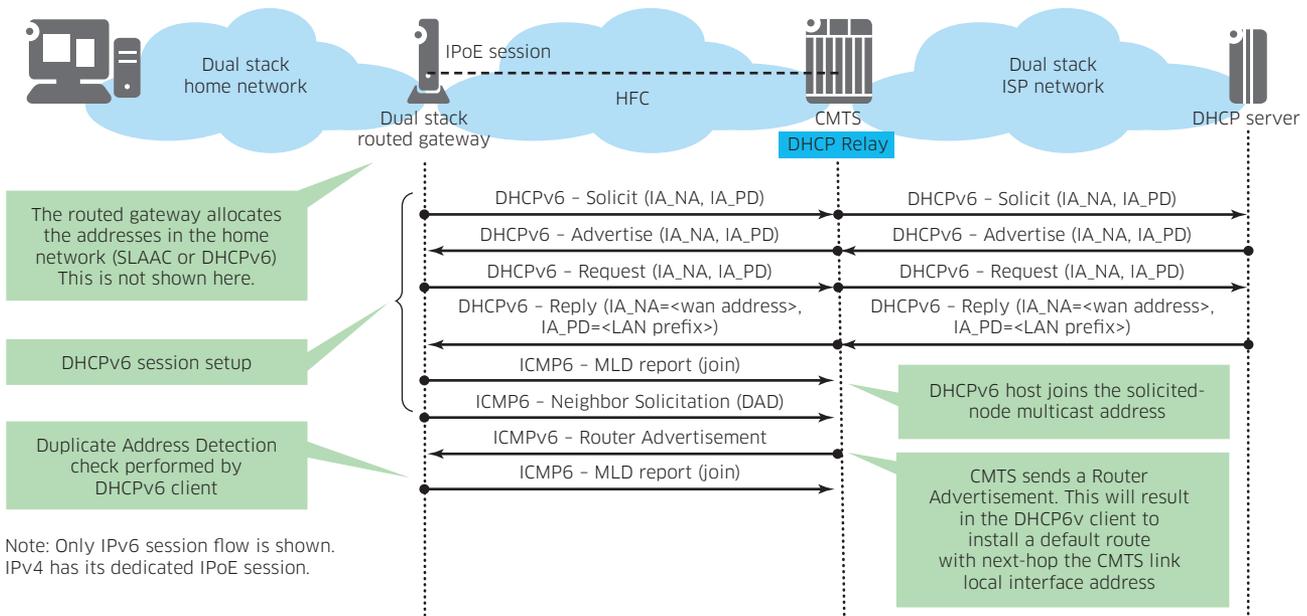
To provide IPv6 connectivity in the cable network, the following mechanisms are required between the RG, the CMTS and the DHCP server to ensure IPv6 connectivity:

- DHCPv6 prefix delegation (IA-PD): a unique per-subscriber IPv6 prefix is delegated to the RG for use within the home network
- DHCPv6 WAN address assignment to the RG if a numbered RG model is used based on SLAAC or DHCPv6
- A default route is installed on the receipt of a valid Router Advertisement from the CMTS with a next-hop of the CMTS link-local address

The implications of introducing IPv6 connectivity in a cable environment are mainly focused around the Residential Gateway, CMTS and the DHCP server. DOCSIS specifies a bridged IPv6 solution in the home, which uses SLAAC and/or DHCP for IPv6 address assignment.

Figure 6 shows a typical flow diagram of how IPv6 connectivity is established using a routed RG IPoE model.

Figure 6. IPv6 for IPoE using CMTS access - routed home: DHCPv6 Prefix Delegation (PD)



## 2.4 IPv6 in mobile environments based on R7 or R8 3GPP

IPv6 connectivity in a mobile environment is defined in 3GPP R7/R8/etc. The main elements involved in the IPv6 connectivity establishment are the User Equipment (UE) and the GGSN/PGW. To provide IPv6 connectivity in a Mobile network, the following mechanisms are required between the UE and the Gateway GPRS Support Node (GGSN)/PDN Gateway (PGW):

- SLAAC router solicitation (RS)/router advertisement (RA) using /64 addresses are used to provide IPv6 connectivity
- DNS information is supplied in the protocol configuration options of the Create PDP Response
- A default route is installed on the receipt of a valid Router Advertisement from the GGSN/PGW with a next-hop of the GGSN/PGW link-local address

Figure 7. IPv6 in mobile environment

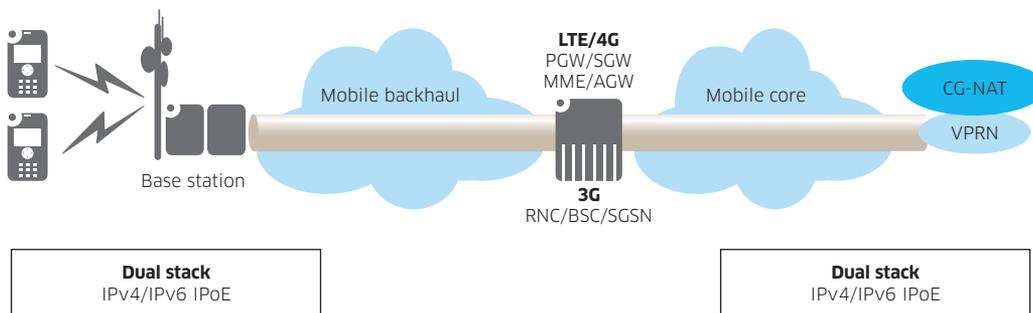


Figure 7 shows a flow diagram of how IPv6 connectivity is established in a mobile environment. From R8 onwards, 3GPP has defined a mechanism using PDP type (IPv4IPv6) to assign both an IPv4 address and an IPv6 address using a single PDP/Bearer Context. With this mechanism, no additional PDP Context has to be created. However, prior to R8 a PDP Context was required per PDN type (IPv4 and IPv6), which results in reduced scalability of the GGSN.

## 3. IPV6 TRANSITION SCENARIOS

There are different choices to be made to deal with the IPv4 exhaustion and IPv6 introduction. However, for best results, it is important to understand the various implications of providing native IPv6 connectivity in residential broadband environments for Telcos, cable and mobile service providers.

There are three main scenarios for dealing with the issues:

- **Scenario 1:** Provide IPv6 single stack to end customer and provide NAT64 when connectivity is required from a IPv6 host to a IPv4 host/website
- **Scenario 2:** Provide dual-stack IPv4 and IPv6 to end customers. There are multiple options when choosing this strategy.
  - Scenario 2A: Leverage the IPv4 installed base and provide IPv6 connectivity, using tunneling IPv6oIPv4 using 6RD [18]. IPv4 connectivity is provided natively.
  - Scenario 2B: Provide native IPv4 and IPv6 connectivity without any tunneling.
  - Scenario 2C: Provide both native IPv6 connectivity and IPv4 connectivity using DS-Lite by tunneling IPv4oIPv6.
- **Scenario 3:** Avoid introducing IPv6 and keep IPv4 single stack by using Carrier-grade Network Address Translation or CG-NAT (NAT444). Although this might be seen to be the least costly option, there are implications that NAT has on end customer services. The implications are explained in chapter 4.

The following sub-sections provide more details on these scenarios and the implications of their introductions. Note that the IT/DHCP/RADIUS systems need to support the IPv6 allocation/management on top of providing IPv6 connectivity.

### 3.1 Scenario 1: IPv6 single stack

In this scenario, only native IPv6 connectivity is provided to the end customer (using one of the mechanisms described in section 2). End-to-end IPv6 connectivity is provided natively between end-hosts/websites. To provide communication from IPv6 to an IPv4 host/website, a NAT64/DNS64 service needs to be deployed in the network.

Figure 8 and Figure 9 show scenarios for establishing basic connectivity in an IPv6 single stack deployment in a wireline, respectively mobile environment.

Figure 8. Scenario 1: IPv6-only operation in wireline deployments

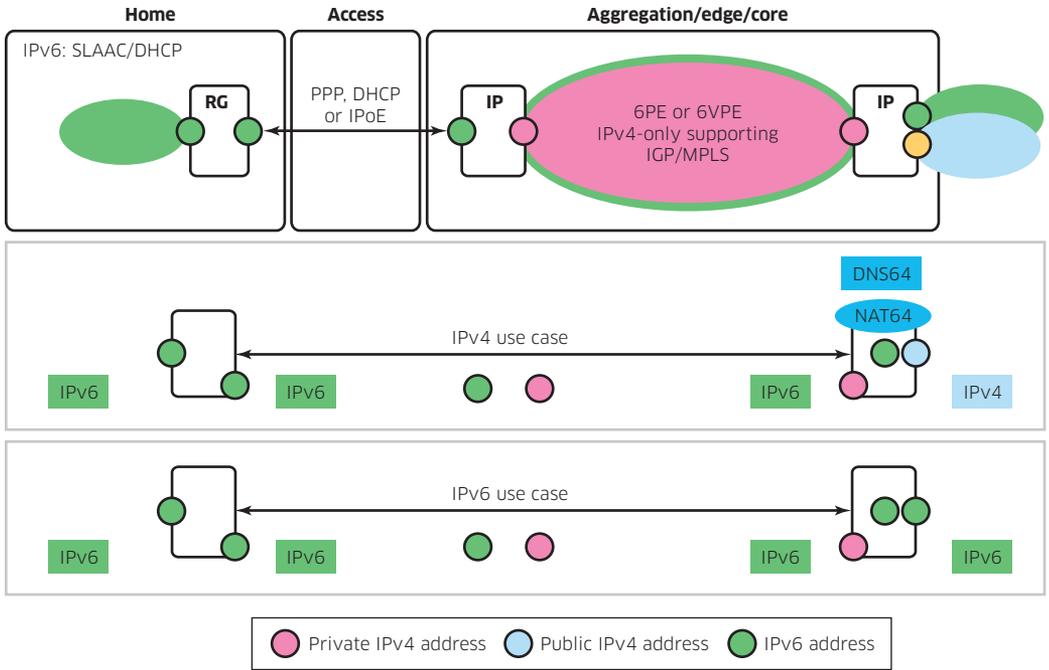
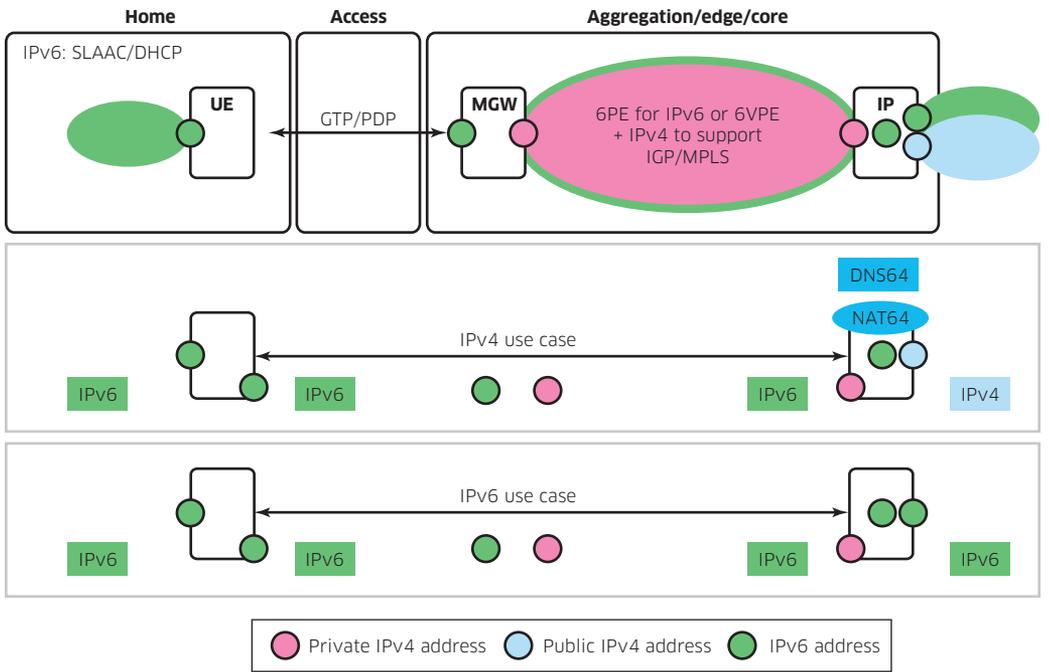


Figure 9. Scenario 1: IPv6-only operation in mobile deployments

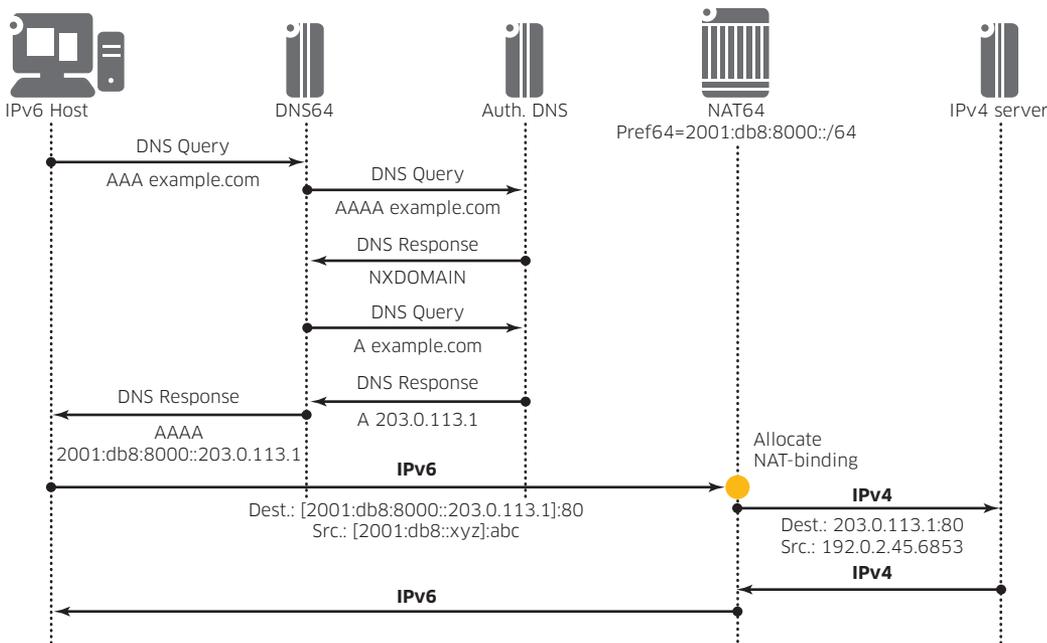


The operation of DNS64/NAT64 is as follows:

- 1) An IPv6 host requests connectivity using DNS to a host/web-site.
- 2) The DNS query is sent to the DNS64 server and resolves the request via the Auth. DNS server.
- 3) When an A record is returned, the DNS64 synthesizes this into a AAAA record and provides a IPv6 address to the end device using a well-known IPv6 prefix that embeds the IPv4 address.
- 4) When the IPv6 end-host gets this DNS response, it sent the IPv6 packet to the destination IPv6 address received in the DNS response.
- 5) Since this well-known prefix is allocated/advertized by the NAT64 element, the packet arrives in the NAT64 device.
- 6) The NAT64 device translates the IPv6 packet into an IPv4 packet and NAT(s) the packet such that a public IPv4 source IP address is assigned. The NAT64 device forwards the native IPv4 packet to the end system (host/web-site)

More details are described in draft-ietf-behave-v6v4-xlate-stateful and Figure 10 shows the call flow of the communication of DNS64/NAT64.

Figure 10. NAT64/DNS64 operation



Although this scenario looks simple, some consideration needs to be taken into account:

- The network needs to be upgraded to support native IPv6 in the RG/CPE and access, aggregation, edge, core and peering routers.
- There is no need to provide an IPv4 address to the end devices, which can improve scalability.
- A NAT64 and DNS64 service needs to be embedded into the network.
- Windows XP, which represents the majority of OS deployments on PC(s) to date, does not natively operate in this model since it uses DNSv4 to get IPv6 AAAA records. Due to the fact that there is no IPv4 connectivity, this causes a big issue.
- Since end devices are mainly using SLAAC and since supplying DNS in SLAAC (RFC5006) was an afterthought, some OSs might not support DNS using IPv6. In mobile environments, this is not an issue since DNS is provided using PCO in the Create-PDP-Context-response message.
- Recent studies have shown that not all applications are designed to date to operate in an IPv6-only environment. (See draft-arkko-ipv6-only-experience-02 for more details.)
- When subscribers are using static IP addressing for communication without using DNS, they need to be supplied with the synthetic prefix for the NAT64 device.

Since mobile UE OS have more and more IPv6 support and since some mobile operators have more control on the OS used in their environment, we believe that adopting this model in a mobile environment is acceptable under these circumstances. For fixed operators, the non-native support of Windows XP is a major hurdle for adopting this model in the short term.

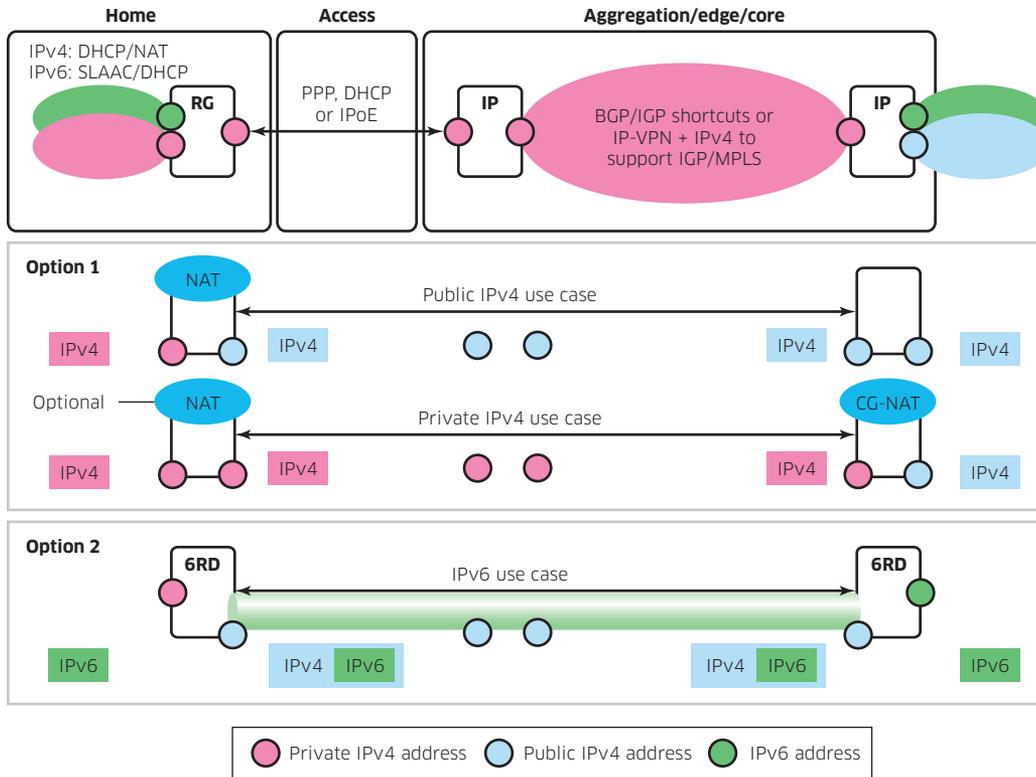
The cost for this model includes CAPEX/OPEX to exchange/upgrade RG/UE, CAPEX/OPEX of the DNS64/NAT64 GW, CAPEX/OPEX of introducing IPv6 in access, aggregation, edge and core, as well as OPEX on the OSS.

## **3.2 IPv4/IPv6 dual-stack deployment options**

### **3.2.1 Scenario 2A: Tunneling IPv6 over IPv4 using 6RD**

In this scenario, the end devices are supplied with dual-stack addressing. Both an IPv4 and an IPv6 address are provided to the customer LAN. IPv4 connectivity in this model is provided as usual, i.e., using private or public IPv4 addressing. IPv6 connectivity is provided using 6to4 tunneling (RFC 3056), where the standard 6to4 prefix 2002::/16 is changed by an IPv6 prefix that belongs to the ISP-assigned address space. The IPv6 prefix allocated to the end customer is derived from the IPv4 address assigned to the CPE/RG. The v4suffix-length, v6prefix-length, 6RD Border Relay IPv4 (Anycast) Address and 6RD SP Prefix are provided to the CPE using DHCP. To deploy 6RD, a 6RD CE (CPE/RG) needs to be deployed in conjunction with a 6RD Border Relay (BR) which provides 6to4 tunneling. More details can be found in RFC 5969.

Figure 11. Scenario 2A: Dual stack and 6RD (wireline)



The following implications should be considered when selecting this model:

- The RG/CPE needs to be upgraded to support 6RD, and a 6RD BR function needs to be added into the network
- There is no need to upgrade the Access/Aggregation/BNG/BRAS
- IPv6 traffic is always tunneled between 6RD CE and 6RD GW; if native IPv6 support is required, a second upgrade is required using one of the other scenarios described in this white paper
- Proper support for MTU size issues that might be introduced due to the 6to4 tunneling
- Mobile UE OS have not been adopting this strategy due to the tunneling implications, which means that this scenario is not applicable in a mobile environment
- Differentiating per subscriber services for both IPv4 and IPv6 are cumbersome to implement

This scenario is positioned in wireline deployments for rapid IPv6 introduction to support Internet access in cases where the access network is incapable of supporting IPv6. Native IPv6 is not supported in this scenario, thus potentially requiring a second upgrade. The costs are determined by CAPEX/OPEX to change/upgrade RG to support 6RD, CAPEX/OPEX of the 6RD BR and OPEX on the OSS.

### 3.2.2 Scenario 2B: Dual stack throughout the network

This scenario is supporting both native IPv4 and native IPv6 to the end customer. IPv4 is supported using the current mode of operation with optional deployment of CG-NAT, depending on the available Public IPv4 address space. IPv6 is provided using one of the methods described in chapter 2. Figure 12 and Figure 13 show more details on IPv4 and IPv6 connectivity.

Figure 12. Scenario 2B: Dual stack throughput in wireline deployments

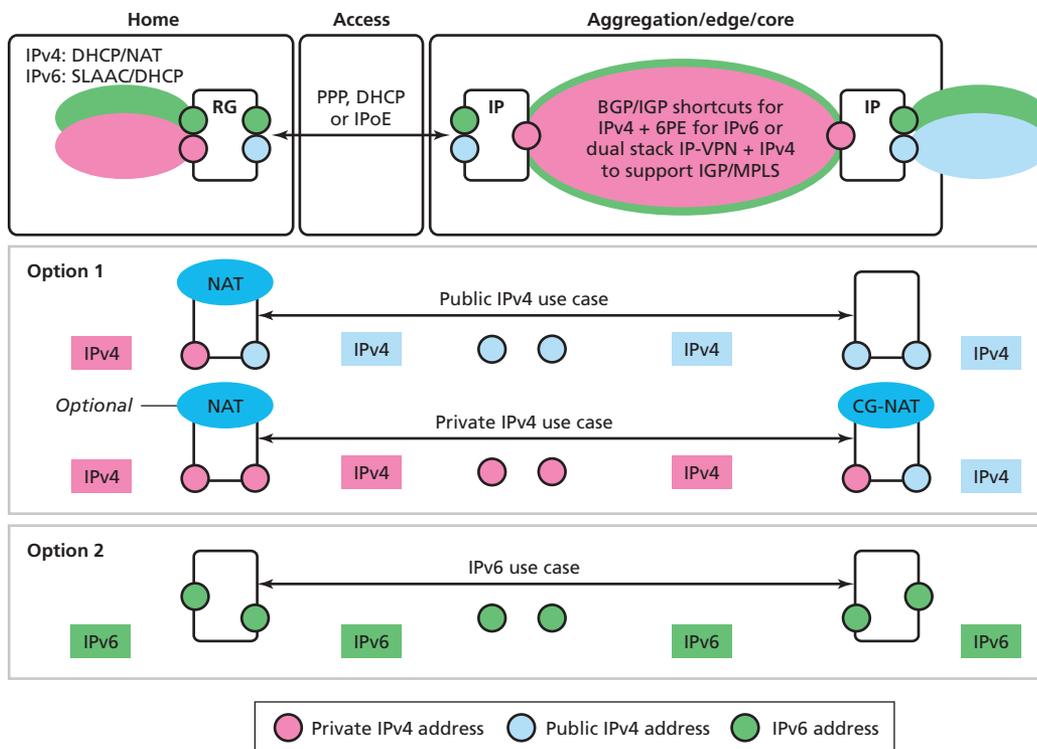
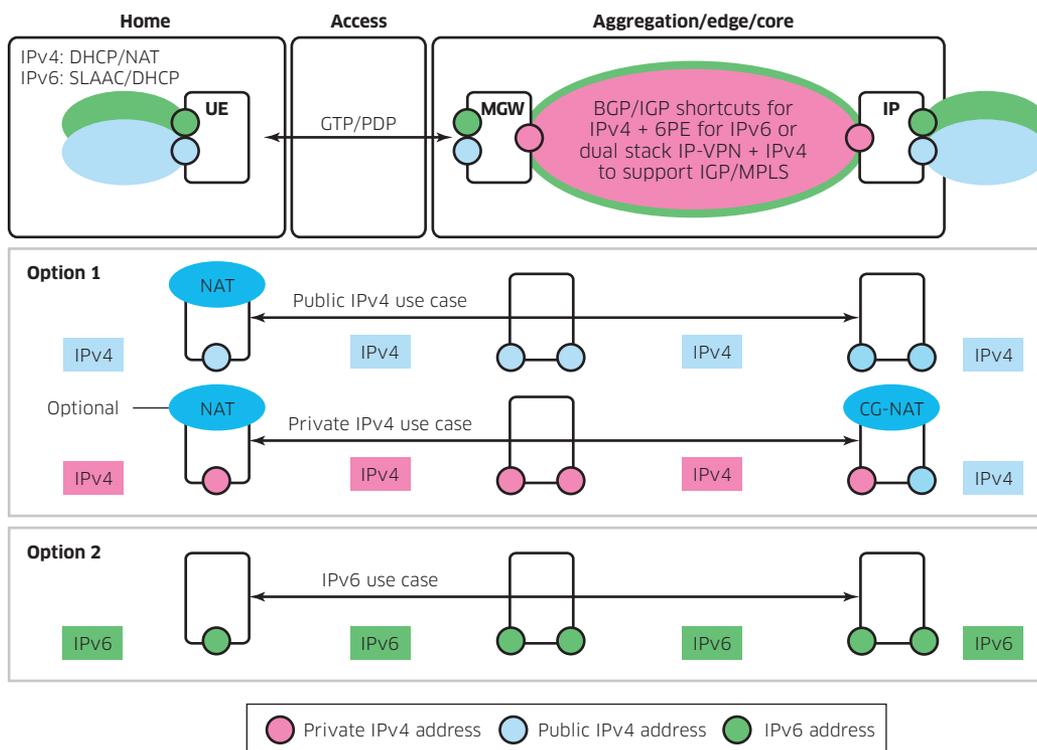


Figure 13. Scenario 2B: Dual stack throughput in mobile deployments



The following implications should be considered when selecting this model:

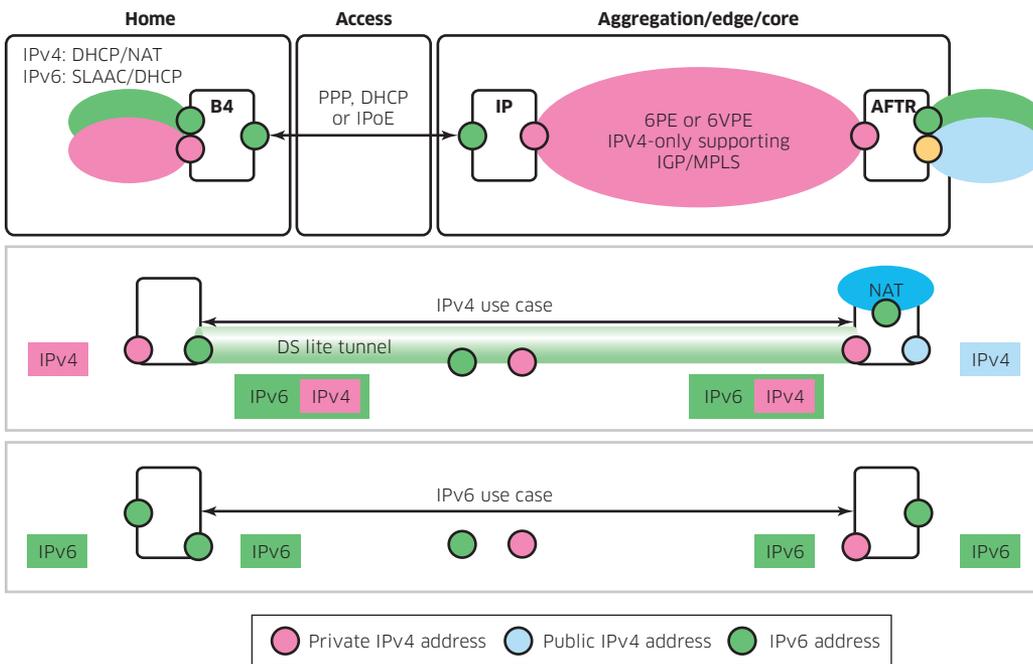
- The RG/CPE, Access, Aggregation, BNG/BRAS and/or GGSN/PGW need to be upgraded to support native IPv6.
- To support both IPv4 and IPv6 in fixed networks and mobile environments (prior to R8), there can be implications on the scalability on the CMTS, BRAS/BNG and GGSN/PGW. Additional elements need to be deployed potentially to scale the network properly.
- IPv4 and IPv6 services (like Internet, Voice, IPTV, etc.) can be deployed independently leveraging IPv4 or IPv6 without tunneling.
- CG-NAT is optional if depending on the available public IPv4 addresses are available.
- Ability to offer differentiated services for both IPv4 and IPv6 is straightforward.

Scenario 2B is positioned in wireline and wireless network deployments. Service providers can leverage synergies between fixed and mobile if they supply both services. The cost is determined by the CAPEX/OPEX to change/upgrade the RG/UE, the CAPEX/OPEX of the CGNAT, and the CAPEX/OPEX of introducing IPv6 in Access, Aggregation, Edge and Core and OPEX on the OSS.

### 3.2.3 Scenario 2C: Partial dual-stack deployment in combination with IPv6-only

Scenario 2C provides native IPv6 connectivity while IPv4 connectivity is provided using IPv4inIPv6 tunneling. In this model, the B4 element (Basic Broadband Bridging) is introduced in the CPE/RG, which provides IPv4inIPv6 tunneling capabilities.

Figure 14. Wireline Scenario 2C: Partial dual stack in combination with IPv6-only



An Address Family Transition Router (AFTR) is introduced in the aggregation network to encapsulate/de-encapsulate IPv4 traffic in/from IPv6, and provides CG-NAT using the IPv6 source prefix as the subscriber key. The CPE/RG is supplied using DHCPv6 with the AFTR GW address and uses a predefined private IPv4 prefix. More details are described in draft-ietf-softwire-dual-stack-lite-06. Figure 14 shows more details on the IPv4/IPv6 connectivity using this transition scenario.

The following implications should be considered when selecting this model:

- The RG/CPE, Access, Aggregation, BNG/BRAS and/or GGSN/PGW need to be upgraded or changed to support native IPv6.
- The RG/CPE need to be upgraded to support the B4 capability and an AFTR element needs to be introduced in the network.
- Since IPv4 services are tunneled, upgrading Voice/Video/Multicast services to IPv6 should be considered. In essence, there is a trade off between the implications of the tunneling versus the cost of upgrading services to IPv6.
- Mobile UE Operating Systems have not been adopting this strategy due to the tunneling implications, which means that this scenario is not applicable in a mobile environment.
- Differentiating per subscriber services for both IPv4 and IPv6 are cumbersome to implement.

Scenario 2C is mainly positioned in wireline deployments that need to transition quickly to a native IPv6-only environment in access and aggregation. Implementation costs includes CAPEX/OPEX to exchange/upgrade RG/UE to support B4/IPv6, CAPEX/OPEX of the AFTR, CAPEX/OPEX of introducing IPv6 in Access, Aggregation, Edge and Core and OPEX on the OSS.

## 4. CARRIER GRADE NETWORK ADDRESS TRANSLATION

Besides approaches to providing IPv6 and IPv4 connectivity, there are other considerations such as CG-NAT and its various implications that determine the IPv6 transition strategy. The following considerations need to be taken into account for CG-NAT:

- Network connectivity must be initiated from the inside towards the outside, unless static port-forwarding rules are configured on the CG-NAT device. Note that Universal Plug and Play (UPnP) and NAT Port Mapping Protocol (NAT-PMP) will no longer work with CG-NAT, and potentially a portal needs to be deployed to enable customers to use pinholes in the CG-NAT service. The IETF is attempting to address this issue in the Port Control Protocol (PCP) Working Group for which implementations are starting to appear.
- The private IP address space has a limited size which must be factored in when making network design decisions. DS-Lite is addressing this issue by performing NAT on the basis of the source IPv6 address. L2-aware NAT is a similar solution that performs NAT on the basis of PPP, VLAN-id and MAC addresses and described in draft-miles-behave-l2nat.

- Application Level Gateways (ALGs) must be supported to allow certain applications (FTP/RTSP/SIP/etc.) to operate across CG-NAT. In parallel, Session Traversal Utilities for NAT (STUN), Interactive Connectivity Establishment (ICE) and Traversal Using Relays around NAT (TURN) can optionally be deployed to assist certain application and minimize ALG requirements.
- To track the allocations of hosts to Public IP addresses and ports, it is best to let the CG-NAT allocate port blocks to reduce logging and storage of the logging files. As a percentage of customers are off-line at any time, 1:1 CG-NAT can be deployed to relax data retention requirements and avoid port overloading issues.
- When N:1 CG-NAT strategy is selected using port block allocations, the solution should ensure that sufficient ports are allocated to a given host. Dividing the available ports by a factor of 10 increases the available Public addressing space by a factor of 10 and prevents additional logging and multiple port block allocations. A typical Internet user consumes close to 100 ports, whereas heavy users consume around 500 ports and more at peak times.
- Lawful Intercept (LI) should be integrated in the CG-NAT device to ensure public IP communication is presented to the LI mediation device.
- When CG-NAT is deployed in other devices than the subscriber Edge (e.g., GGSN/PGW, BNG/BRAS or DHCP Server), IP addresses are allocated independently from NAT Public IP/port mappings. This can result in allocating the same inside IP address to a different host, while the NAT mapping has not timed out. Either an implicit timeout mechanism or an explicit mechanism should be installed to take this into account.
- Subscriber Deep Packet Inspection (DPI) enforcement should be deployed in front of the NAT function unless the subscriber DPI enforcement can operate with IP address/port block allocations provided by the CG-NAT device. In case DS-Lite/6RD is used, deploying DPI in front of the NAT might be problematic since DS-Lite/6RD is tunneling the IPv4/IPv6 packet in IPv6/IPv4. When using NAT64/NAT444, the DPI system should be upgraded to support IPv6 signatures and heuristics.
- Certain Internet services, which operate based on IP only information, will no longer be able to identify a host based on IP address and need to be enhanced with the port information allocated to a certain host.
- Take into account the throughput, NAT binding translation rates, and binding scalability support of the deployed CG-NAT device.
- Select a solution that can be deployed in both a centralized or distributed manner, since NAT requirements might change over time.

Many service providers that have offered public IP services have to face these challenges while minimizing the impact to their customers. Hence, providing native IPv6 will be important to satisfy a customer base as it avoids the various issues that are related to the use of CG-NAT.

## 5. SUMMARY

The impending exhaustion of public IPv4 addresses has a non-trivial impact on the network infrastructure and services of all network providers. As a result, the network providers must prepare themselves appropriately ahead of time by taking into account the following:

- Determine the most appropriate IPv6 introduction strategy. This encompasses aspects such as:
  - How various legacy IPv4 services would interwork and/or migrate to IPv6 operation
  - The differences and ramifications of IPv6 operation, as compared to IPv4 operation, on the network, control plane and OSS level (noting that some of the largest impacts can be on OSS and IT systems)
  - IPv6 readiness of existing network and OSS infrastructure and potential hardware and software upgrades required to enable IPv6 operation
  - Cost options and timing of introducing dual-stack operation in client devices, access, aggregation, edge and core
  - IPv6 readiness as a planning parameter for future network expansions and upgrades
  - Educating operational workforce as well as customers about IPv6 and the steps being taken to prepare for its introduction
- Determine the most suitable IPv4 continuity strategy to assure the continued operation of IPv4-based legacy services, devices and applications until they can be migrated over to IPv6, including:
  - The potential impact of introducing network-based CG-NAT functionality on existing services and processes, for example, think about satisfying lawful intercept requirements, support for server-initiated IP communication, usage auditing and troubleshooting
  - The implications of IPv4 address overloading on the existing addressing plan, noting that a NATed operation could impact network-wide address numbering and summarization)
  - Required operational procedures to migrate from transparent IPv4 to a NATed operation
  - Performance, scalability, interoperability and management requirements

As there are many options in deploying IPv6 and dealing with IPv4 exhaustion, Alcatel-Lucent is committed to help network service providers make the right choices for their networks. Alcatel-Lucent solutions focus on technical, business and service challenges to solve this multi-dimensional transition issue in the most cost-effective way.

Alcatel-Lucent products have been validated in various deployments and through independent validation of these strategies by ISOCORE, which shows details on how well our solution supports and scales in IPv6 transition scenarios. For more details, contact Alcatel-Lucent sales support.

## 6. REFERENCES

REFERENCE	DOCUMENT NAME
RFC 1918 [1]	RFC 1918 Address Allocation for Private Internets
RFC4787 [2]	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
RFC5382 [3]	NAT Behavioral Requirements for TCP
RFC5508 [4]	NAT Behavioral Requirements for ICMP
RFC 3489 - RFC 5389 [5]	Session Traversal Utilities for NAT (STUN)
RFC 5766 [6]	Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
RFC 5245 [7]	Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
draft-cheshire-nat-pmp-03.txt [8]	NAT Port Mapping Protocol (NAT-PMP)
draft-ietf-tsvwg-port-randomization-09 [9]	Transport Protocol Port Randomization Recommendations
draft-ietf-softwire-dual-stack-lite-06 [10]	Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
RFC4213 [11]	Basic Transition Mechanisms for IPv6 Hosts and Routers
draft-ietf-softwire-ds-lite-tunnel-option-07 [12]	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite
draft-ietf-dhc-dhcpv6-ldra-03 [13]	Lightweight DHCPv6 Relay Agent
WT146 [14]	Internet Protocol (IP) Sessions
TR177 [15]	IPv6 in the context of TR-101
TR187 [16]	IPv6 for PPP broadband access
RFC 3056 [17]	6to4 tunneling
RFC 5969 [18]	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)
draft-ietf-softwire-dual-stack-lite-06 [19]	Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
draft-ietf-behave-v6v4-xlate-stateful-12 [20]	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
RFC 4862 [21]	IPv6 Stateless Address Auto-configuration
RFC 3315 [22]	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3633 [23]	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC 5072 [24]	IP Version 6 over PPP
RFC 2516 [25]	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 3162 [26]	RADIUS and IPv6
RFC4818 [27]	RADIUS Delegated-IPv6-Prefix Attribute
draft-ietf-radext-ipv6-access-02 [28]	RADIUS attributes for IPv6 Access Networks
RFC3363 [29]	Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)
RFC 4294 [30]	IPv6 Node Requirements
RFC 3736 [31]	Stateless Dynamic Host Configuration Protocol (DHCP)
draft-miles-behave-l2nat-00 [32]	Layer 2-Aware NAT

## 7. ABBREVIATIONS

6PE	IPv6 Provider Edge over MPLS	LNS	L2TP Network Server
6RD	IPv6 rapid deployment	LSN	Large Scale Network address translation
6RD CE	CPE/RG supporting 6RD	LSP	Label Switched Path
6RD BR	6RD Border Relay	LSR	Label Switch Router
6VPE	IPv6 provider Edge over MPLS VPN	MME	Mobility Management Entity
AFTR	DS-Lite Address Family Transition Router element	MPLS	Multi-Protocol Label Switching
AGW	Application Gateway	NAT	Network address translation
ALG	Application level gateway	NAT64	Network address translation between IPv6 and Ipv4
B4	DS-Lite Basic Bridging Broadband element	NAT-PMP	NAT Port mapping protocol
BNG	Broadband Network Gateway	OPEX	Operational expenses
BGP	Border Gateway Protocol	OS	Operating system
BRAS	Broadband Remote Access Server	OSS	Operation support system
CAPEX	Capital expenses	PCP	Port configuration protocol
CE	Customer Edge router	PDP	Packet Data protocol
CG-NAT	Carrier Grade Network address translation	PE	Provider Edge router
CPE	Customer Premises Equipment	PGW	PDN Gateway
DHCP	Dynamic Host configuration protocol	PGW	Packet Gateway (LTE)
DNS	Domain Name system	PTA	PPP Termination and Aggregation
DPI	Deep Packet inspection	RD	Route Distinguisher
DS	Dual Stack	RG	Residential Gateway
DS-Lite	Dial Stack Lite protocol	RP	Rendezvous Point
EBGP	Exterior Border Gateway Protocol	RPF	Reverse Path Forwarding
GGSN	Gateway GPRS Support Node	RR	Route Reflector
GRE	Generic Routing Encapsulation	SGW	Serving Gateway
GUA	Global unicast address (IPv6)	SLAAC	Stateless address auto-configuration
IA-NA	Association - Non-temporary Address	STUN	Simple Traversal of User Datagram Protocol
IA-PD	Identity Association - Prefix Delegation	TURN	Traversal Using Relays around NAT
ICE	Interactive Connectivity Establishment	UE	User equipment
IPv6CP	IPv6 Control Protocol	ULA	Unique Local address (IPv6)
LDP	Label Distribution Protocol	UPnP	Universal plug and Play protocol
LI	Lawful intercept	VPN	Virtual Private Network
LLA	Link local address (IPv6)	VPRN	Virtual Private Routed Network