

Nokia Siemens Networks Moving to IPv6 An urgent priority

Nokia Siemens
Networks



White Paper



Contents

- 2 Executive summary
- 3 IPv6 – meeting demand long into the future
- 4 Multiple benefits with IPv6
- 5 Technical maturity
- 8 Migration technologies
- 10 Transition scenarios
- 12 Access-specific transition scenarios
- 14 The Nokia Siemens Networks approach to IPv6
- 15 Conclusion: Moving to IPv6 is becoming critically urgent

Executive summary

A growing need for IPv6

It is likely that 5 billion people will be connected by 2015, but such figures raise serious questions about the number of Internet Protocol (IP) addresses available to connect everyone. And that is without considering the probability of the widespread connection of machines to the networks of the future.

Service providers (SPs) are already finding IP version 4 (IPv4) addresses increasingly difficult to obtain, and predictions suggest that the unallocated address pool could run dry as soon as 2011.

The growing popularity of smartphones will make the issue even more pressing, because many applications occupy an IP address once the smartphone is switched on, rather than using a dynamically assigned IP address only when browsing the web.

Furthermore, we are seeing continuous growth in always-on, IP-based multimedia services that need permanent connections between the terminal and a central gateway. Next-generation mobile networks (3GPP Long Term Evolution / System Architecture Evolution, (LTE/SAE)) rely on permanent packet connections, as do smartphones on 3G networks. The increasing penetration of wireline Voice over IP (VoIP) is fostering the use of permanent IP addresses in fixed networks too.

Today the vast majority of Internet services are still based on IPv4 and SPs are using work-around solutions to address the resulting limitations. However, the pool of available IPv4 addresses is dwindling. The shift to IPv6 should solve the problem,

releasing a mind-boggling 340 trillion trillion trillion possible addresses.

IPv6: Plentiful, secure addresses

IPv6 enables direct communication between equivalent devices using a globally routed IPv6 address. This will allow SPs to offer services cost-effectively for devices that are connected to the Internet all the time. This supports the growth in Machine-to-Machine (M2M) communications. Protecting these autonomous devices against attacks will be crucial.

An adequately sized address pool will simplify network operations. Rigorous address management can be maintained for efficiency and not for operability, as is sometimes the case.

Developing a tangible IPv4-to-IPv6 transition plan now is a wise move for SPs, as is the factoring of IPv6 into their service development strategies.

To secure their future growth, SPs need to be ready to offer connectivity services to enterprises that are using IPv6.

Some large enterprises have already adopted IPv6 and enjoy improved reliability, efficiency and flexibility.

IPv6 will enable new always-on convenience for consumers, such as maintaining a phone call or data session across while moving between fixed and mobile networks without having to 'hang up'.

IPv6 – meeting demand long into the future

IPv4 has been extremely popular and has encouraged the take up of the Internet and other IP networks in all areas of modern networking. However, rapid growth is quickly exhausting the remaining pool of IP addresses.

IPv4 addresses are specified in a 32-bit field. This provides 4 billion theoretical addresses, and the IPv4 address space is expected to run out in 2011.

IPv6 was developed in the late 1990s by the Internet Engineering Task Force (IETF) to address the problem by providing many orders of magnitude more addresses. The IPv6 address is

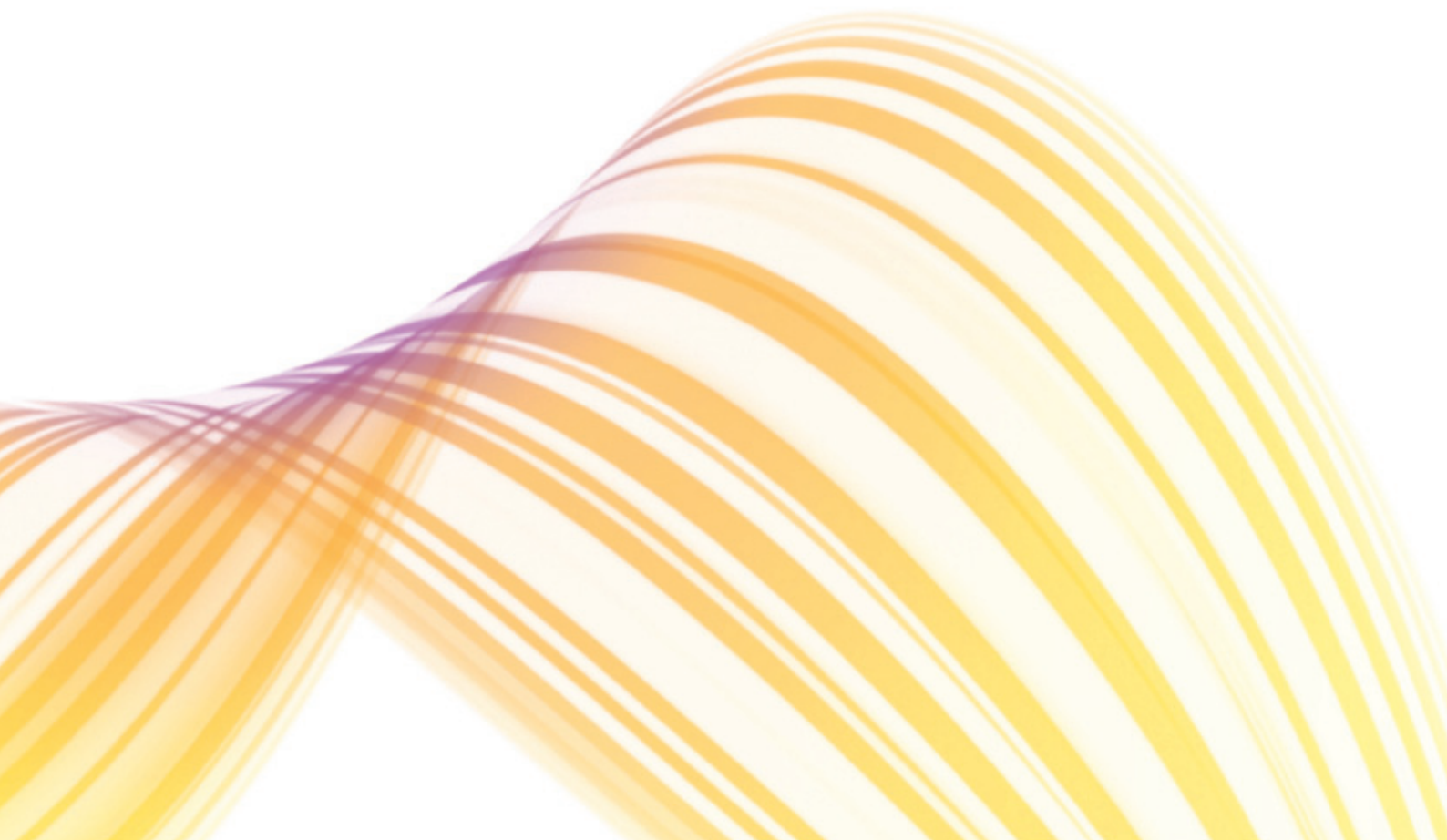
128 bits long and provides 3.40×10^{38} theoretical addresses.

The exhaustion of the IPv4 address space is imminent. Soon the IANA (Internet Assigned Numbers Authority) will no longer be able to allocate /8 address blocks to Regional Internet Registries (RIRs). Shortly thereafter the RIRs' own address pools will run dry and they will not be able to allocate new addresses. In practice this means that SPs will not be able to get new addresses for new customers, services and applications.

The adoption of IPv6 so far has been slow. Today, the vast majority of

Internet services are still based on IPv4. Network Address Translation (NAT) has been widely implemented to work around address space limitations, and SPs have learned to manage small and fragmented address blocks.

NAT has slowed IPv4 address pool depletion, but it cannot prevent it. Forward-looking SPs should be thinking about IPv6 now. Although IPv4 and IPv6 are similar in most respects there are some differences. Gaining operational experience in IPv6 is vital, and those SPs doing it first will be in a better competitive position.



Multiple benefits with IPv6

IPv6 is designed to replicate the winning formula of IPv4. The main benefit of IPv6 over IPv4 is clearly the increased address space. As well as the ability to connect more nodes, more address space also provides indirect benefits such as simplified network planning. In addition, IPv6 delivers improvements including easier end-host address configuration and better integration with IPsec.

Assuring the continued growth of the Internet

The issue of IPv4 address space seriously limits the growth potential of the Internet, other IP networks and SPs. Although there may be a secondary market in IPv4 addresses after the main pool is exhausted, it will clearly not be enough to secure continued growth on the same scale. In addition, the cost of addresses may exceed the possible profit they generate.

Address space is not an issue for IPv6.

Simplified networking

IPv6 allows SPs to plan their networks unrestrained by the artificial limitations of inadequate address space.

In IPv4 the address space is split into small fragmented blocks. IPv6 provides large blocks of continuous address space. This allows simpler address management.

The ability to use globally unique IP addresses will mean ultimately make NAT unnecessary and this will lead to cost savings by simplifying the network and its operation.

One of the tangible benefits of IPv6 compared to IPv4 with NAT is battery consumption in mobile devices. NAT devices maintain ongoing connections by looking at the traffic that goes through them. If a connection has not passed any traffic within a specified time, NAT determines that the connection has ended. Thus, applications must send “keep-alive” messages to maintain a connection. This may not be a problem for devices connected to the power grid. But mobile devices operating on battery power are not able to conserve power by going dormant.

In addition to battery consumption, NAT makes application development more difficult by adding considerable complexity.

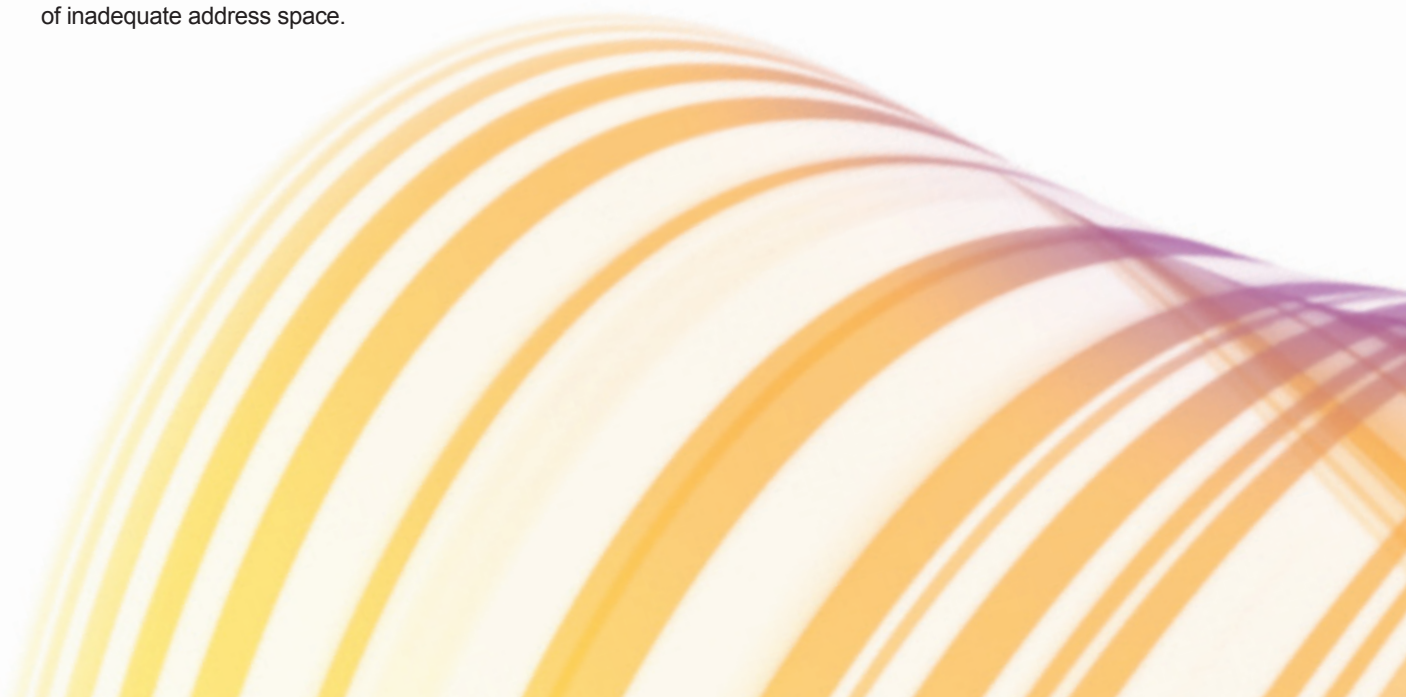
Enabling more advanced services

The restriction in IPv4 address space has shaped IP services and applications. It has also limited the creation of new services.

The almost unlimited address space of IPv6 enables new services that need many addresses, such as efficient VoIP and IP sensor networks.

Beyond simplifying operations and reducing costs, embracing IPv6 will allow SPs to address new opportunities, such as M2M communications, where cars, sensors and other devices can be connected permanently to the Internet and contacted from anywhere around the world.

Industrial automation is also turning towards IP and Ethernet for improved performance at lower cost.



Technical maturity

IPv6 is an evolving standard

IPv6 as a technology was first defined in standards more than ten years ago, and the specifications have since gone through several revisions.

Management and configuration technologies

Technologies traditionally considered vital for IP end-host configuration and management are the Point-to-Point Protocol (PPP) and Dynamic Host Configuration Protocol (DHCP).

PPP has been enhanced to support IPv6 parameter configuration and IPv6 packet transport.

IPv6 has a new version of DHCP – DHCPv6 – which can be used in the same way as IPv4 DHCP to completely configure the IPv6 end device with an IP address and other parameters.

Alternatively, it can be combined with address auto-configuration, which is built into IPv6.

State-of-the-art network management protocols such as Simple Network Management Protocol (SNMP) for node management all support IPv6.

Routing

All modern routing protocols provide extensions for IPv6 support or an IPv6-capable version of the protocol has been specified:

- **Routing Information Protocol (RIP)** – A new version called RIP next-generation (RIPng) has been specified, which has IPv6 support.
- **Open Shortest Path First (OSPF)** – OSPFv3 is needed for IPv6. When a common IPv4/IPv6 network exists, OSPFv2 must also run on the router for IPv4.
- **Intermediate System-to-Intermediate System (IS-IS)** - IS-IS specifies a new Type, Length, Value (TLV) for IPv6.
- **Border Gateway Protocol (BGP)** – A new Address Family Identifier (AFI) has been specified for IPv6.

MPLS and IPv6

Multiprotocol Label Switching (MPLS) is the leading technology for packet-based backbone networks in fixed, mobile and converged environments for the following reasons:

- Support for traffic engineering (MPLS-TE)

- Support for network restoration through MPLS 1:1 protection and Fast ReRoute
- Enabling Virtual Private Network (VPN) services
- Enabling pseudo-wire emulation services

Most of today's IP backbone network implementations are based on MPLS technology because it offers a clear separation between the control plane and forwarding plane. This allows different types of payload to be transported over the same infrastructure, including Ethernet frames, IP packets, ATM (Asynchronous Transfer Mode) and cells. MPLS is seen as the main enabling technology for TDM-to-packet conversion (TDM = Time Division Multiplex).

Consequently, many SPs are migrating their IP backbone towards an IPv4 MPLS backbone and the expected return on investment for those transformations is yet to be realized. This may mean that SPs will be reluctant to adopt IPv6 for their newly built and stabilized IPv4 MPLS infrastructure.

A further hindrance to IPv6 adoption is the incomplete standardization of MPLS signaling protocols for IPv6. Also, today's MPLS networks are in most cases based on a pool of private IPv4 addresses, which are not affected by IPv4 address depletion. It is therefore understandable that there may be a lack of urgency among SPs to migrate their MPLS backbone networks towards IPv6 on the control plane.

Against this backdrop, the most common way to implement IPv6 over MPLS networks will be the connection of IPv4 and IPv6 networks over an IPv4 MPLS backbone by upgrading the Provider Edge (PE) routers. This requires both IPv6 and IPv4 versions of RIP and OSPF, and enabling IS-IS IPv6 support in the PE routers because direct interworking between IPv6 and

IPv4 is not possible and a dual stack is needed to support both versions. Therefore, SPs will need to check whether their current PE implementation will support dual stacks of IPv4 and IPv6 and deliver the desired performance.

However, a benefit of this approach is that it supports VPNs based on IPv4

and IPv6 over the same infrastructure. IPv6 also provides similar Quality of Service (QoS) mechanisms in MPLS networks as IPv4.

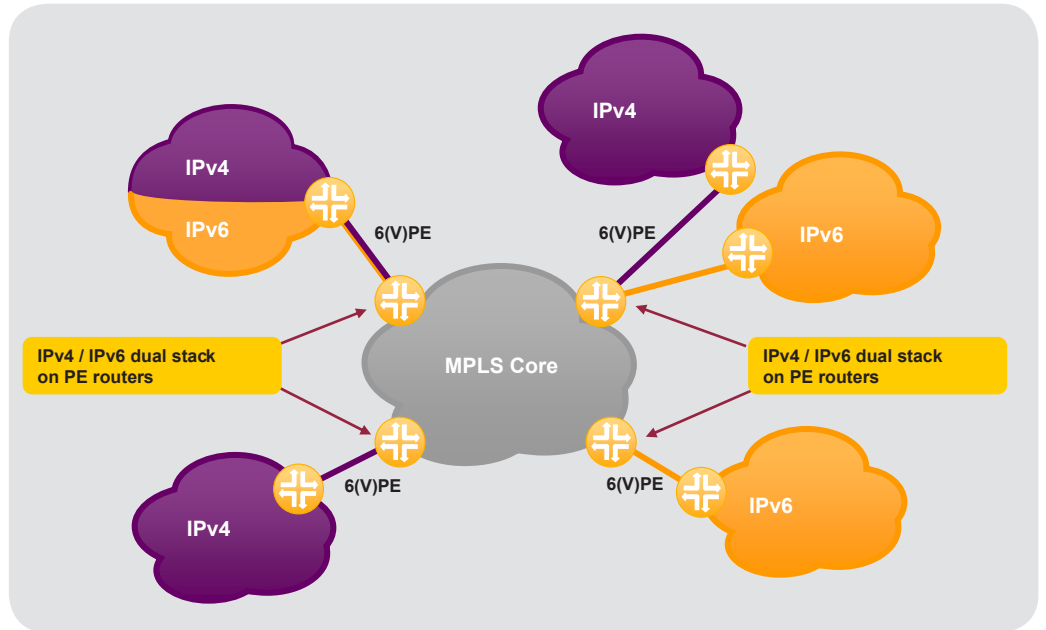


Figure 1: IPv6 transition options

Other transport technologies (DWDM, NG-SDH and MWR)

As long as IPv6 packets are forwarded using pure layer-1 technologies, such as Packet over SONET/SDH (Synchronous Optical Network / Synchronous Digital Hierarchy), no special requirements need to be met for the transport of IPv6.

In the case of other technologies, such as Next-Generation SDH (also called Next-Generation Metro), DWDM (Dense Wavelength Division Multiplexing) systems with integrated L2 switches and transponders with Ethernet interfaces, or so-called Pure Packet or Hybrid Microwave Radio System with IP/Ethernet user equipment would need to support all the necessary VLAN and QoS operations.

For example, to enable equipment to forward IPv6 packets encapsulated in Ethernet frames requires support of the Ethertype used in IPv6. IPv6 uses the 0x86DD Ethertype while IPv4 uses 0x0800.

For access nodes such as the Digital Subscriber Line Access Multiplexer (DSLAM), IPv6 support requires not only the forwarding of IPv6 frames but also the support of features for identifying the individual subscriber.

IPv6 and security

In contrast to IPv4, IPv6 is designed to cope with typical security threats. Every IPv6 implementation must therefore support the IPsec framework. IPsec provides encryption and integrity protection for all IP traffic and, assuming NAT-free operation, may be applied between any pair of communicating hosts in an IPv6 network.

While the IPsec framework provides automatic negotiation of session keys between peers, it does not support the distribution of long-term keys. For this reason, it is unlikely that IPsec will be used for most host-to-host communication in an early IPv6 Internet. Furthermore, IPsec may not be widely used in private networks because it restricts network security mechanisms such as firewall filtering and network intrusion detection.

IPv6 also introduces new mechanisms (like auto-configuration, router renumbering or specific multicast groups) that may be open to abuse by attackers, making it vital to configure and use them with care.

IP networks will also be more vulnerable during the transition from IPv4 to IPv6:

- Not all IPv6 software will be “field proven”, so bugs must be expected.
- Lack of experience with IPv6 security may lead to inadequate configuration.
- IPv4 to IPv6 transition mechanisms like dual stack, tunneling and translation increase vulnerability.
- Security products may initially provide only a limited feature set for IPv6.
- Hosts may be IPv6-enabled without the host-based security features being upgraded.

After the transition phase, IPv6 networks will provide the same level of security as IPv4 networks. However, IPv6 is unlikely to make IP networks much more secure because all large-scale threats are independent of the IP version.

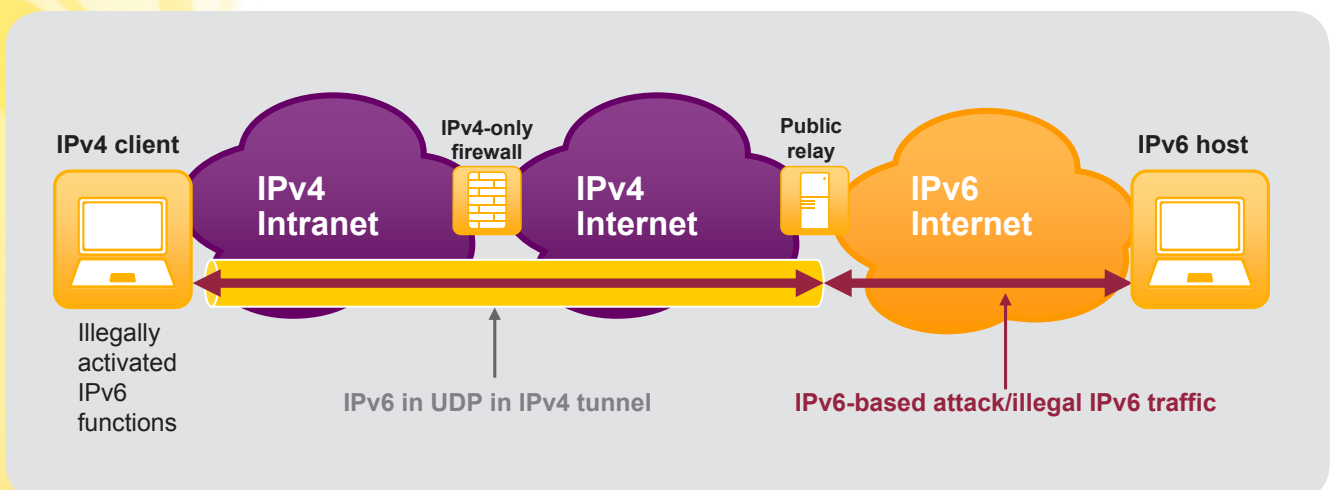


Figure 2: IPv6 threat scenario

Migration technologies

IPv6 nodes cannot communicate directly with IPv4 nodes and vice versa. In addition, in some instances it will be costly to enable IPv6 in a network with legacy equipment or equipment that cannot be upgraded easily.

Various techniques are available to help communications between IPv4 and IPv6 nodes or allow IPv6 traffic to flow over an IPv4 network or vice versa. These technologies can be classified into two basic categories:

- Technologies that avoid translation of user traffic
 - Dual stack enables both IPv4 and IPv6 on the same network devices
 - Tunneling encapsulates one version of IP in another in configured or automatic tunnels
- Translation technologies that enable communication between an IPv6-only device and an IPv4-only device

Dual stack

The dual-stack approach is based on the implementation of both IPv4 and IPv6 protocol stacks on all network devices and end-user equipment.

Any node in the network must be configured with both IPv4 and IPv6 addresses, enabling applications to communicate over an IPv4 or an IPv6 network. They may obtain these addresses via DHCP or, in the case of IPv6, via the auto-configuration feature. This solution requires that every device in the network is capable of supporting both versions of IP.

The dual-stack approach is the preferred method to deploy IPv6 support in networks where IPv4 address availability is not an urgent problem.

Note that dual-stack devices still require IPv4 addresses, so this

approach does not solve the IPv4 address exhaustion problem. It is possible to reduce the number of public IPv4 addresses needed using NAT, but this is contrary to the long-term aim of a complete move to IPv6. SPs may start to deploy IPv6-only services once they no longer need to support legacy device access.

However, dual stack is considered to be a good way to start implementing IPv6 while also supporting IPv4 services. To better support IPv6 in dual-stacked services and applications, the Domain Name System may need to be optimized to ensure that the IPv6 reply is always faster than the IPv4 answer.

Tunneling

Tunneling encapsulates one version of IP within another, enabling packets to be sent over a network that does not support the encapsulated version.

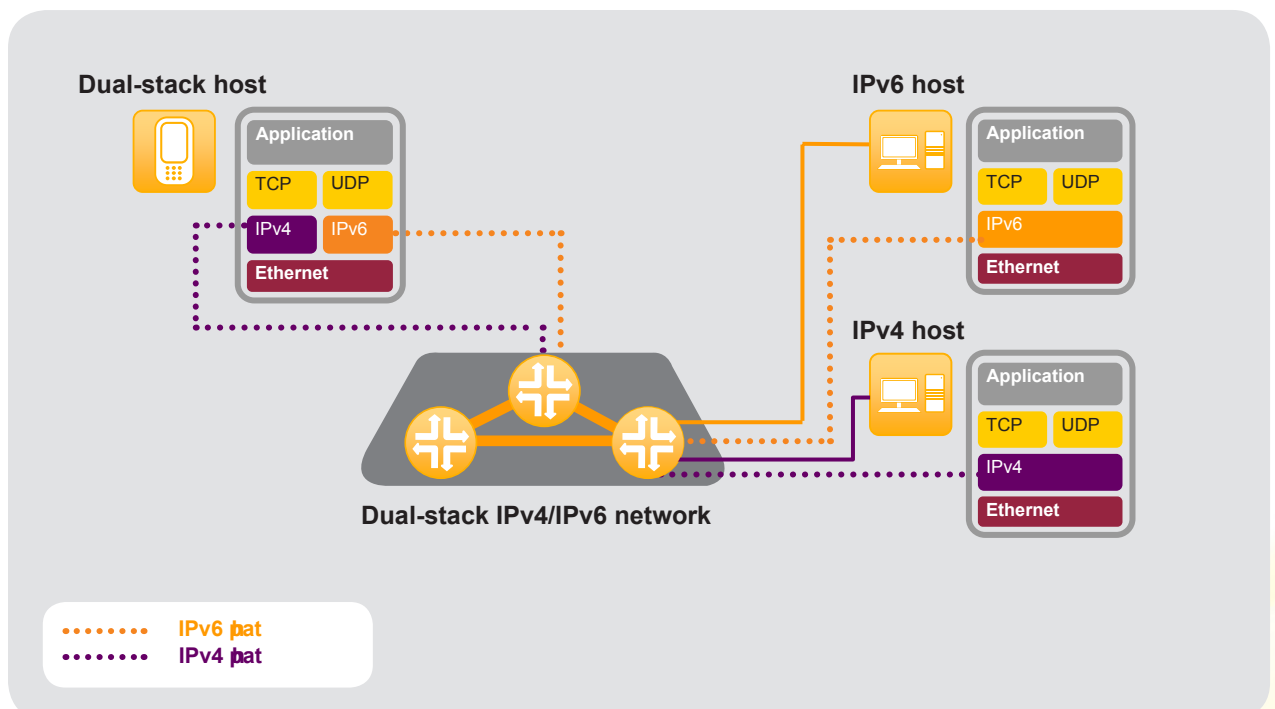


Figure 3: Transition to IPv6, dual-stack migration

Several different tunneling technologies support IPv6 over IPv4 and vice versa. Tunnels can be configured manually with statically configured end points, or automatically created dynamically with end points deleted on request.

In an IPv6 deployment, tunneling of IPv6 packets through an IPv4 network entails encapsulating each IPv6 packet with an IPv4 header.

Generally, automatic tunneling is used where the end-user device tunnels the traffic itself or in small-scale test environments. Configured tunneling is more common in the network infrastructure.

In addition to general purpose tunneling mechanisms, different domain-specific mechanisms can be used to help the transition to IPv6. A good example is the 3GPP mobile network system. Since user traffic is already tunneled over the network, the user service can adopt a different IP address family that is then used by the network itself. This enables IPv6 to be offered to the end user regardless of

the IP version in the network infrastructure. This tunneling concept for mobile networks is described in more detail in section “Mobile broadband access”, page 12.

Translation

Translation techniques support the flow of traffic from IPv4 to IPv6 protocols via a gateway. Different methods perform the translation at the network, transport or application layer.

Unlike tunneling, translation refers to a technique of exchanging one version of IP to another by completely replacing the header of each packet. This may also involve translating information inside the IP packet itself.

This method does not depend on dual-stack technology. It enables nodes or applications that speak only one version of IP to communicate with another node or application that speaks the other.

Translation is recommended where IPv6-only nodes must communicate with IPv4-only nodes if there is no

realistic option for deploying private IPv4 and regular IPv4 NAT. Currently, only NAT-PT (NAT - Protocol Translation) has been specified fully. But the specification has serious drawbacks and is no longer recommended for general use (RFC 4966). Several possible alternatives are currently being reviewed by the IETF.

Furthermore, using NAT to translate between IPv6 and IPv4 is more complex than regular IPv4 NAT. For example, information about the relationship between the IPv4 and IPv6 addresses must always be retained. The technique should therefore be used only when there is no alternative.

It is important for SPs to be able to provide connectivity between users with IPv6 addresses and IPv4-only applications. This is currently under specification by various IETF working groups, such as NAT64 and DNS 64, which will provide this functionality. Nokia Siemens Networks is contributing to this specification and plans to implement it in its products where it is appropriate.

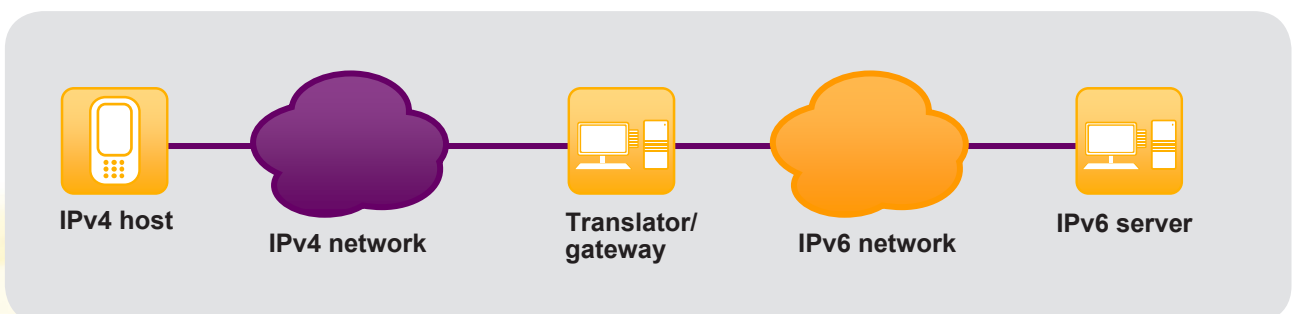


Figure 4: Transition to IPv6, translation

Transition scenarios

The most effective way to make the transition from IPv4 to IPv6 depends on the available budget, resources and time constraints, as well as the current set-up of end-user devices, network devices, operating systems and the service core applications running on servers.

Typical transition scenarios can be explained by referring to a network with client, IP access, IP core, and server building blocks. In some cases, a

combination of approaches is necessary.

Core transition

Transitioning the IP core network elements to IPv6 requires IPv6-capable routing protocols (IGP, Interior Gateway Protocol) in each element and the enabling of IPv6 routing. Configured tunnels are established between dual-stack edge routers to provide IPv4 routes and distribute IPv4

traffic and services across the IPv6 core.

This technique should have no impact on the client side, the IP Access and Aggregation network or the server side. An added advantage is that most core routers already support IPv6. This is a good way for operations staff to become familiar with IPv6 without affecting residential and business customers.

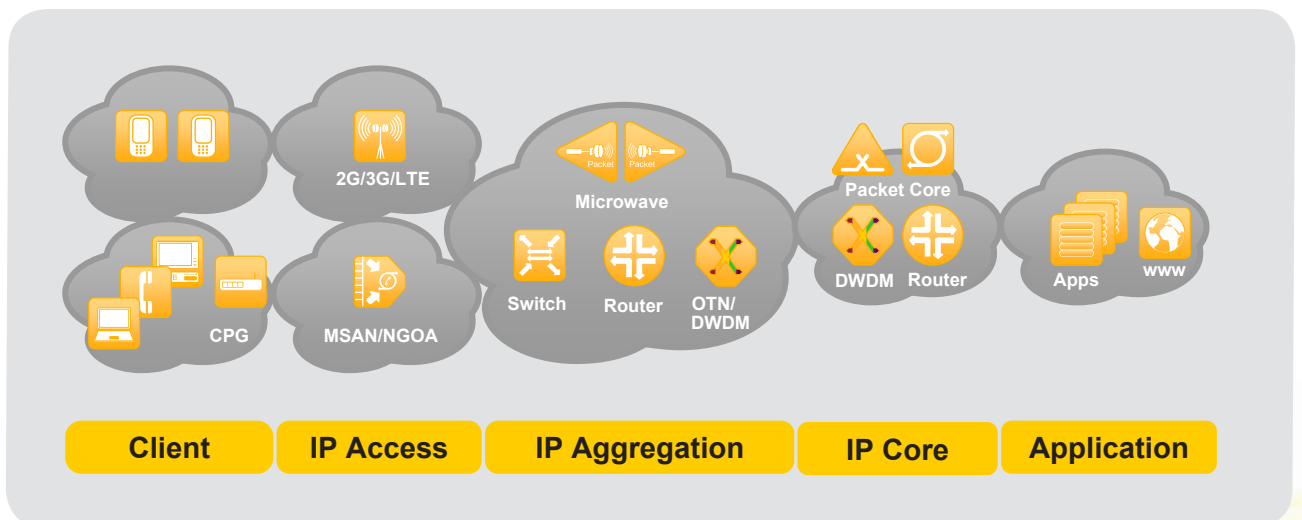


Figure 5: Transition to IPv6

Client transition

This scenario involves upgrading the clients to dual-stack implementations and also applies to IPv6-only clients. The nodes in the IP Access and Aggregation network must also support both protocols. Dual-stack routers are needed at the boundary between the IP Access and Aggregation network and IP Core, where they serve as translation gateways.

This approach is needed only while the clients need the dual stack to access IPv4-based services, and becomes redundant once the services have migrated to IPv6. It should be considered if a Service Provider needs more time to upgrade the core network infrastructure to support IPv6 while operating the IPv4 network in parallel.

Nokia Siemens Networks believes that this client transition approach is highly beneficial because it helps SPs to solve the IPv4 address depletion problem and to maintain growth.

Server transition

This strategy requires the Service Provider to upgrade its Service Core Application servers to dual stack and to adopt Service Core Applications that support the dual stack technique. This enables clients to use IPv4 services as normal, but also serves IPv6 clients. Dual-stack routers again serve as translation gateways.

This is another temporary solution for clients that need to access IPv4-based services. It can help staff to ensure the smooth operation of IPv6-based services and the Core Application Servers prior to deploying them for end users.

Client and server transition

Dual-stack implementations in the clients and the Service Core Application servers are the key to this approach. The nodes in the IP access and aggregation network must also support both protocols. Dual-stack routers are needed at the boundaries

between the IP access and aggregation network and IP core, and between the IP core and the server side. In this case, they serve as tunnel end-points to enable clients across the IP core to access the Service Core Application servers.

This approach serves both IPv4 and IPv6 clients. IPv6 services can be provided depending on the availability of IPv6-capable devices on the client side, as well as the deployment of IPv6-based Service Core Applications.

The concept can also apply if the Core uses MPLS. In this case, PE routers must support both IPv4 and IPv6, whereas the Provider (P) routers remain on IPv4. The IPv6 packets are transported from PE router to PE router over an MPLS tunnel according to the signaled Label Switched Path. The P core router still uses IPv4 in the control plane.

VPNs based on IPv6 use the existing IPv4 MPLS infrastructure and features for MPLS.

VPN customers can use IPv6 VPN services in the same way as IPv4 VPN services.

Access-specific transition scenarios

Different transition scenarios suit different access technologies. Common to all scenarios is the dual-stack implementation in user equipment and edge equipment, such as BNG (Broadband Network Gateway) and packet core (Serving GPRS Support Node SGSN, Gateway GPRS Support Node GGSN, Mobility Management Entity MME, System Architecture Evolution Gateway SAE-GW). Fixed and mobile accesses can share the same MPLS backbone which needs either dual stack or 6PE/6VPE. Network address translation devices such as NAT64 can then be implemented either centrally or distributed to ensure services are available to pure IPv6 users.

Mobile broadband access

Modern mobile broadband networks based on 3GPP specifications have been standardized from the beginning with IPv6 transition in mind. Regardless of the IP version used by the underlying network, 3GPP systems support IPv4 and IPv6.

As shown in Figure 6, the SP network is IPv4 and most end users use IPv4 for their services. In addition to IPv4, a mobile device can open an IPv6 connection, called a Packet Data Protocol context (PDP context), giving them dual-stack capabilities. Alternatively the mobile might use only IPv6 PDP contexts if it doesn't need to connect to the IPv4 network.

The incremental change for the SP is very small. A Service Provider only has to enable the IPv6 software feature in the SGSN and in GGSN, enable the IPv6 subscription for the user and provide IPv6 connectivity for the GGSN. IPv6 connectivity can be provided natively via the SP's IPv6 core or via IPv6-in-IPv4 tunneling. Mobile terminals must also be IPv6-capable.

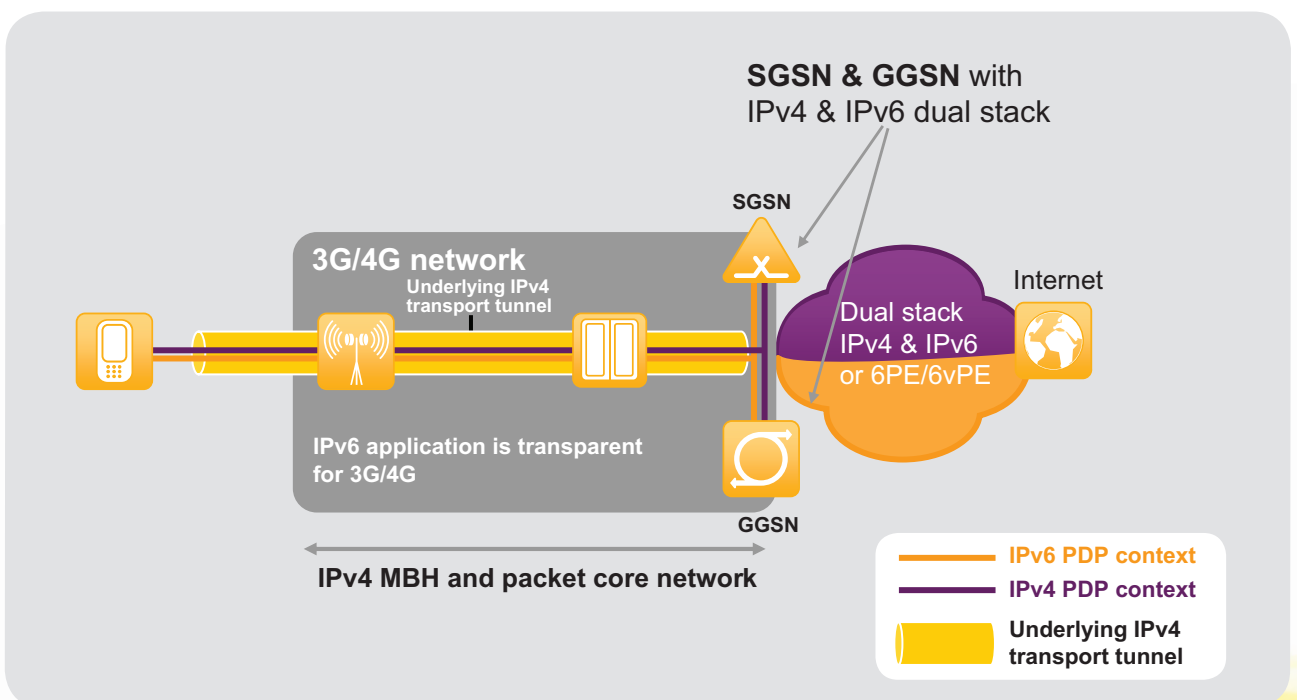


Figure 6: Transition scenarios, mobile broadband access

Fixed broadband access

There are several possible transition strategies for fixed broadband networks. PPP- or DHCP-based Ethernet access are the most important, although tunneling IPv6 over IPv4 can be used in pilot deployments.

PPP access

In a PPP-based access network, end-user traffic is encapsulated in PPP frames between the end-user equipment and the BNG.

PPP supports both IPv4 and IPv6, while IPv6 can be added to the same network infrastructure as IPv4.

Although adding IPv6 with PPP access is relatively easy it does require support for IPv6 in both the end-user equipment and the BNG terminating the PPP connection. This may mean either software or hardware upgrades at both ends.

Ethernet access

The Broadband Forum (formerly the DSL Forum) WT-177 recommends the

following best-practice allocation of residential user IP addresses.

A single subscriber / access line should have a single global IPv6 prefix that is used for all its services.

In a DHCP IP over Ethernet (IPoE)-based access network, the end-user device gets its IPv6 address via DHCPv6. The DHCPv6 server assigns 128-bit addresses according to the address assignment policies determined by the server administrator and specific information about the client.

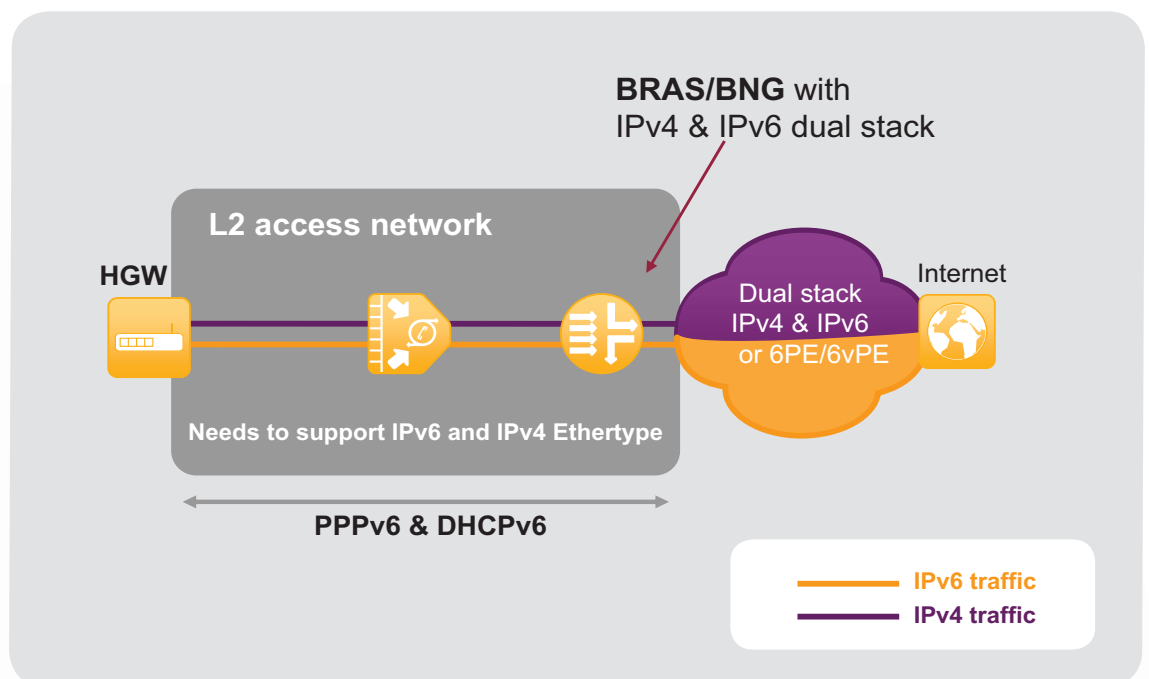


Figure 7: Transition scenarios, fixed broadband access

The Nokia Siemens Networks approach to IPv6

Nokia Siemens Networks has been a leader in driving the Internet beyond IPv4. Nokia Siemens Networks has been actively pushing the development of IPv6 technologies and standards within the IETF. Nokia Siemens Networks has also been supporting IPv6 in technologies such as GSM, WCDMA and LTE through the 3GPP, the WiMAX Forum, and other organizations.

Nokia Siemens Networks' unique end-to-end IP knowledge allows it to help SP's make the transition to IPv6, whether they're using Nokia Siemens Networks products or not.

Nokia Siemens Networks delivers world-class service solutions and consulting to help every SP achieve a smooth transition to IPv6.

Proven solutions

The Nokia Siemens Networks mobile broadband solution provides dual IPv6/IPv4 PDP context and connects the mobile network gateway to the SP's IPv6 network and the IPv6 Internet.

The GGSN can be connected to the IPv6 network natively or by tunneling. In addition, the Nokia Siemens Networks IPv6 mobile broadband

solution supports the advanced features needed for a successful launch of IPv6.

The Nokia Siemens Networks IP Multimedia Subsystem (IMS) offers IPv6 capability that enables a future-proof IMS deployment.

All of the Nokia Siemens Networks transport and access equipment follows the company's strategy to provide IPv6, including DWDM, NG-Metro, microwave radio and finally IP and Ethernet products.

Proven services

As the pressure to make the move to IPv6 grows, Nokia Siemens Networks Global Service IPv6 Consulting can help. From defining technical and business objectives to optimizing the profitability of the SP's service portfolio, consultants can support SPs throughout the process.

Nokia Siemens Networks specialists have extensive experience that enables them to recommend industry best practices and discuss the latest solutions and technologies that apply to a specific network environment. Migration Services analyzes the SP's current network and develops a

migration concept to transform the infrastructure and services to the new IPv6 architecture with minimal impact on end-user services and operations.

Nokia Siemens Networks can integrate IPv6 into the SP's multi-vendor environment across all network layers. This minimizes the risk associated with complex projects, speeds time to market and makes the whole process more cost-effective.

Nokia Siemens Networks also integrates "best-of-breed" third-party IP/Ethernet equipment to complement its own portfolio of products.

Software customization is also undertaken to meet the needs of the IPv6 environment and different migration projects.

Some Nokia Siemens Networks partners offer tools to automate network operational methods and procedures to simplify the provisioning of large-scale IPv6 networks and reduce the risk of IP transformation.

Conclusion: Moving to IPv6 is becoming critically urgent

The transition from IPv4 to IPv6 should be top of the agenda for SPs, since the IPv4 address pool will run dry in 2011.

However, IPv6 offers far more benefits than just solving the current address problem. It will allow SPs to offer services for a new breed of mobile and fixed devices, which are connected to the Internet all the time. The emerging space of M2M communications such as Smart Grid is a good example.

IPv6 is a mature technology that has already been adopted by various networks. Migration scenarios and related technologies are well understood.

Early experience will offer SPs an advantage in terms of moving up the learning curve. It will also be a prerequisite for companies looking to

be first to market with innovative, IPv6-based services.

As an IPv6 pioneer with comprehensive service and network understanding, Nokia Siemens Networks is the right partner to help SPs achieve the transition to IPv6.



Nokia Siemens Networks

P.O. Box 1

FI-02022 NOKIA SIEMENS NETWORKS

Finland

Visiting address:

Karaportti 3, ESPOO, Finland

Switchboard +358 71 400 4000 (Finland)

Switchboard +49 89 5159 01 (Germany)

Order No. C401-00678-WP-201101-1-EN

Copyright © 2010 Nokia Siemens Networks.

All rights reserved.

Nokia is a registered trademark of Nokia Corporation,

Siemens is a registered trademark of Siemens AG.

The wave logo is a trademark of Nokia Siemens

Networks Oy. Other company and product names

mentioned in this document may be trademarks of

their respective owners, and they are mentioned for

identification purposes only.

This publication is issued to provide information only

and is not to form part of any order or contract.

The products and services described herein are

subject to availability and change without notice.

