

Toward an IPv6 world in mobile networks

IPv4 has served the internet well, but the world has to shift to IPv6 – and soon. Mobile networks need to be among the first to make the change. Fortunately, there are good mechanisms available to ease this transition.

✦ ARI KERÄNEN, JARI ARKKO, SURESH KRISHNAN AND FREDRIK GARNEIJ

The internet has outgrown the limits of its current IPv4 address space. IPv6 solves the address space problem, but migrating to the new version still requires some effort and a set of transition mechanisms. This article presents mechanisms for providing IPv6 connectivity, and outlines their benefits, applicability and the challenges faced during different phases of the transition, particularly by mobile networks. Measurements relating to IPv6 network use, as well as IPv6 user trials are also presented.

Background

The IPv4 address space – with roughly 4 billion globally unique addresses – has turned out to be inadequate for the billions of devices that are part of the global internet today, and the tens of billions of devices that are expected to exist in the near future.

IANA, the main authority responsible for assigning IP addresses, recently allocated the last IPv4 address blocks to the Regional Internet Registries (RIRs), which in turn will assign these blocks within their geographical regions through ISPs. In mid-April 2011, the first RIR to run out of major address blocks was APNIC. The other RIRs will follow suit within a few years.

The problem of a shortage of IPv4 addresses was identified back in the late 1980s. Solutions were developed for both sharing IPv4 addresses and for increasing the size of the address space. Network address translation (NAT) has since become a common mechanism for sharing a small number of globally unique addresses among a large number of hosts. NAT works by providing private (usually RFC1918¹) addresses to hosts and translating them into public IPv4 address/port pairs on demand when the hosts send packets to the internet. NAT provides effective statistical multiplexing, but constantly

connected hosts reduce this effectiveness, as do many web applications that demand multiple ports. NAT also introduces further complications (**Box B**). Nevertheless, many mobile networks employ NAT today, and more will do so in the future.

While NAT was devised as a short-term solution, the IETF defined the next version of IP, IPv6, as the long-term solution for the address shortage. IPv6 has numerous improvements over IPv4, but one key feature is the fact that the new address space is orders of magnitude larger.

Now facing an enormous increase in the number of connected devices, mobile networks are among the first that need the IPv6 address space.

IPv6 migration models

Migration to IPv6 is essential if the internet is to continue to grow, but it will not happen overnight; rather it will take place over a number of years and in several phases. Different networks may end up utilizing different migration mechanisms, depending on their specific needs and constraints.

Dual-stack

Network equipment and dual-stack hosts have network stack support and IP addresses from both IPv4 and IPv6. When services are available over IPv6, hosts use native IPv6 connectivity, but for services available only over IPv4, that version is used instead. If the network equipment supports IPv6, dual-stack can be utilized simply by configuring the network nodes appropriately. Existing mobile network nodes, such as the Ericsson GPRS and

BOX A Terms and abbreviations

ALG	application-level gateway	IPv4	IP version 4
APNIC	Asia Pacific Network Information Centre	IPv6	IP version 6
DHCP	Dynamic Host Configuration Protocol	ISP	internet service provider
DNS	Domain Name System	MSP	Multiservice Proxy
DNS64	DNS translation for NAT64	MTU	maximum transmission unit
EPC	Evolved Packet Core	NAT	network address translation
GPRS	general packet radio service	NAT44	NAT between IPv4 and IPv4 networks
GTP	GPRS Tunneling Protocol	NAT64	NAT between IPv6 and IPv4 networks
IANA	Internet Assigned Numbers Authority	PDP	Packet Data Protocol
IETF	Internet Engineering Task Force	RIR	Regional Internet Registry
IKE	Internet Key Exchange	UE	user equipment
IMS	IP Multimedia Subsystem	XMPP	Extensible Messaging and Presence Protocol
IP	Internet Protocol		

EPC core nodes, have such support. Dual-stack and native IPv6 connectivity do not introduce additional encapsulation, processing or new network nodes, so dual-stack networks are robust and reliable. As such, dual-stack is the recommended transition model for the majority of the networks.

Most mobile networks may need to employ the dual-stack model together with a NAT on the IPv4 side, because they may not have enough public IPv4 addresses for all their users. This is particularly true for the growing set of constantly connected applications. Fortunately, with dual-stack, an increasing amount of traffic can be moved to IPv6. A large proportion of all internet traffic is directed to a few large content providers, such as Akamai and Google². When these networks enable IPv6, dual-stack networks can move much of this traffic to IPv6 and reduce the load on the IPv4 NAT device. Most of these large content providers – along with Ericsson – are participating in World IPv6 Day on June 8, 2011³. On that day, IPv6 will be enabled by default for 24 hours on numerous networks and sites that previously supported only IPv4. The aim is to identify any remaining issues with widespread IPv6 usage in these networks. Most of the potential problems associated with using IPv6 are, after all, of a practical nature, such as: ensuring that the necessary components have IPv6 turned on; that configurations are correct; and that any implementation bugs have been removed.

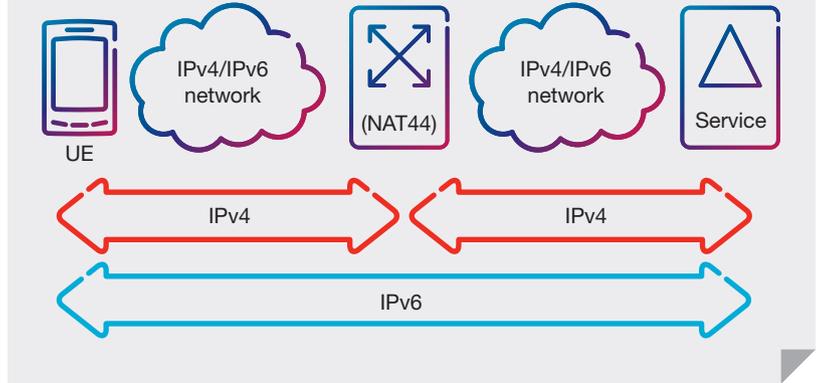
The native dual-stack model is shown in **Figure 1**. Here the entire network – from the UE to the servers running the services – supports both IPv4 and IPv6. Services can be accessed using either protocol, depending on which one is supported by the particular service. If NAT44 is used, the IPv4 connections go through address translation at the edge of the two networks, but for IPv6 connections there is no need for any address translation.

In 3GPP-based mobile networks, UEs can request IPv4 or IPv6 Packet Data Protocol (PDP) contexts. IPv6 user-traffic support was added to the Ericsson GPRS product family in 2002-2003, enabling native IPv6 connectivity in mobile networks. The main driver was IMS, which initially supported only IPv6.

BOX B
Among other issues, NAT may:

- ❖ prevent unsolicited incoming connections to hosts inside the network behind the NAT. While this was fine when hosts were merely clients for services provided over the internet, this complicates the new content-creation models where hosts also provide services to the internet;
- ❖ require that hosts send keep-alive messages so that NAT bindings remain active. This can cause excessive (and unnecessary) traffic on expensive and spectrum-bound radio interfaces, and reduce battery life on mobile devices;
- ❖ require the use of ALGs to enable certain classes of application to work through the NAT; and
- ❖ cause complications related to debugging and network management.

FIGURE 1 Native dual-stack model



Dual-stack UE connectivity requires both IPv4 and IPv6 PDP contexts, however, having separate PDP contexts consumes resources. Release 8 of the 3GPP standards included the introduction of a dual-stack connection capability – making it possible to use both IPv4 and IPv6 – over a single bearer. This capability is now being introduced into Ericsson products.

The dual-stack mechanism is useful when actual destinations advertise IPv6 addresses. How many websites are IPv6-enabled? The top three of the 1 million

most popular websites⁴ – google.com, facebook.com and youtube.com – provide IPv6 addresses, at least for parts of their sites. However, the likelihood of finding an IPv6 address falls dramatically beyond these three. The top 100 sites include 24 that are IPv6-enabled, but for the top 1 million sites the rate is only 3.2 percent. The probability of finding an IPv6-enabled site, as a function of the most popular sites examined, is shown in **Figure 2**. After falling below 2 percent around 50,000 sites, the probability starts to increase slowly as many ❖❖❖

FIGURE 2 IPv6 address record probability by Alexa Rating

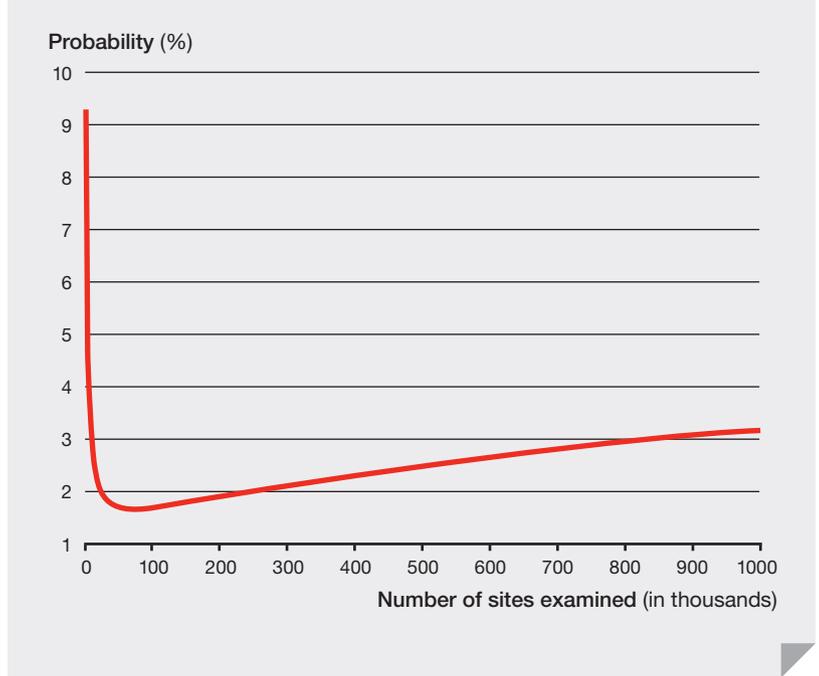
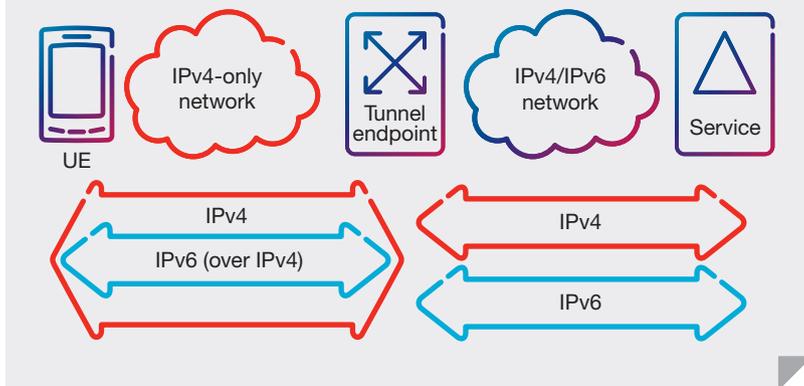


FIGURE 3 Tunneling IPv6 over IPv4



BOX C Figure 3

shows an example of tunneling IPv6 over IPv4. The UE is in an IPv4-only network, and when IPv6 services are used, the IPv6 packets are sent over IPv4 to the tunnel endpoint. The tunnel endpoint removes the encapsulating IPv4 header and sends the IPv6 packets forward. In the reverse direction, incoming IPv6 packets that are addressed to the UE are encapsulated by the network tunnel endpoint in IPv4 before forwarding them on to the UE.

Tunneling

Tunneling mechanisms can provide IPv6 access over IPv4 networks (the most common form of access today) and IPv4 access over IPv6 networks, which is set to become more popular as IPv6 becomes more widespread. Tunneling mechanisms work by encapsulating the payload IP version into the transport IP version in order to travel across a network that does not recognize the payload IP version.

The IP packets used by the endpoints are encapsulated in IP packets using the version supported by the network, then decapsulated before the other endpoint uses them. The tunnel endpoints that perform encapsulation and decapsulation can be either network elements or the endpoints themselves. Commonly, one tunnel endpoint is a dual-stack host, the network access of which supports only one IP version while the other endpoint is a dual-stack network element with both IPv4 and IPv6 access. Regardless of the mechanism used, a host using tunneling for IPv6 (or IPv4) connectivity appears as a dual-stack host for local applications and for other hosts.

Tunneling mechanisms have some drawbacks such as a smaller maximum transmission unit (MTU, the biggest packet size that can be used without fragmentation) due to the additional IP headers and reliance on the tunnel endpoints to provide the encapsulation service. However, many of these problems can be mitigated with proper network design.

Mobile networks employ GTP to allow terminals to move around while retaining connectivity. Because these tunnels effectively separate the IP networks, an operator can enable IPv6 for subscribers without requiring that every router in its own or its roaming partners' networks supports IPv6.

IPv6-only networks with IPv6/IPv4 NAT

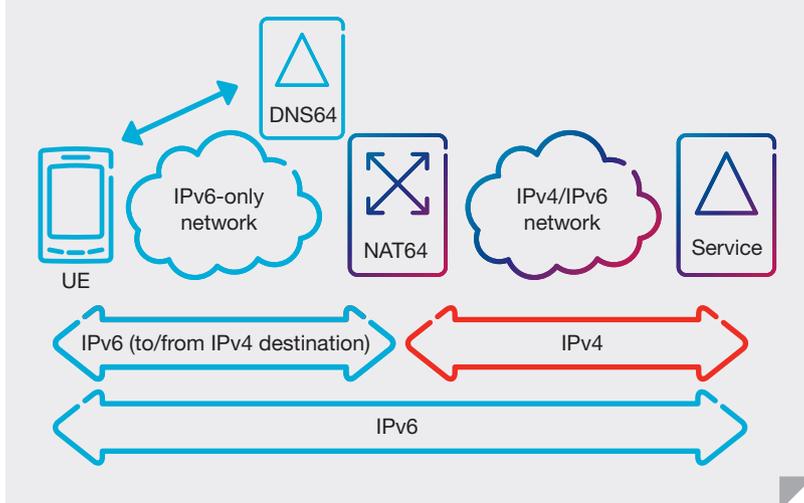
When all devices in a network support IPv6, sometimes the simplest network configuration is to employ only IPv6. NAT64, along with DNS64, can provide access to IPv4 services from IPv6-only networks⁶. This is important in the final phases of transition, because for quite some time certain content will be available only in the IPv4 internet. NAT64

of the sites positioned below the first 50,000 are in fact hosted by Google.

Delay and failure rates for downloading websites over IPv4 and IPv6 were measured. For most of the 6,884 top-ranked sites accessible using both IPv4 and IPv6, the delay penalty for IPv6 was insignificant. For 90 percent of the sites tested, IPv6 was either faster or up to 2.6ms slower than IPv4 in delivering the first two packets of the TCP handshake. On the other hand, 5 percent of sites had an average additional delay of more than 37ms, possibly due to packet loss or bad IPv6 routing. TCP connections over IPv6 failed more often than their IPv4 counterparts: whereas roughly 1 percent of sites were inaccessible with IPv4, around 2 percent failed with IPv6.

Some content providers have been reluctant to enable IPv6. The reasons for this include delays for applications attempting to connect over broken IPv6 links before falling back to IPv4, and unreliable IPv6 connectivity. Bad IPv6 routing has been behind many of the problems. Among the causes are broken 6to4 tunneling protocol⁵ connectivity, experimental IPv6 setups that are untested and unmonitored, and configuration problems with firewalls. The situation is improving as more users and operators put IPv6 to use and fix the problems that emerge. Technical measures, such as deprioritizing 6to4, have also proven helpful. World IPv6 Day will help to uncover further problems and, more importantly, resolve them.

FIGURE 4 Address translation with NAT64 and DNS64



works by translating IPv6 packets into IPv4 packets, and vice versa. Every IPv4 address has a special representation in the IPv6 address space, and a DNS64 service automatically synthesizes IPv6 addresses for hosts that only have an IPv4 address.

In the address translation process outlined in **Figure 4**, UE first performs a DNS query to DNS64 for the address of the server providing the service. If the server has an IPv6 address in the domain name system records, the DNS64 returns this record unchanged and the UE uses IPv6 to connect to the server directly. Otherwise, the DNS64 returns a synthesized address, and packets using that address are automatically routed to the NAT64. The NAT64 will perform address translation and forward packets to the right IPv4 destination. Return traffic is translated back to IPv6 and forwarded to the UE. In mobile networks, the Ericsson MSP 5.3 can be configured to provide a carrier-grade NAT64 translation service.

There are many reasons for using only IPv6: cost reductions, ease of management, simplified network planning and, of course, the availability of IP addresses for the network. An IPv6-only network does, however, place demands on the devices and applications using it, and even claimed IPv6 compatibility may not always be sufficient for smooth operation. To gather practical experience of IPv6-only networking, a small number of volunteers used an IPv6-only network at two sites.

Based on their experiences, office and home users can already rely entirely on an IPv6-only network. In terms of web browsers and e-mail clients, the volunteers observed no difference when comparing the IPv6-only experience with that offered by a dual-stack network. Software updates, operating system services, many chat systems and streaming media all worked well.

On the other hand, switching off IPv4 creates challenges for some applications that still do not have IPv6 support and consequently require additional tunneling mechanisms to work in IPv6-only networks. When IPv4 and DHCP are not available, manual configuration of DNS servers is required for some operating systems. The test networks used

address translation to connect to the IPv4-only parts of the internet. In this kind of environment, protocols that use plain IPv4 addresses (also known as IPv4 literals) in their payloads can cause problems because those addresses are not translated by the NAT64 unless ALGs are used.

The number of IPv4 literals can be measured from internet content. Of the 10,000 most popular websites, there were no problems with the top 100 in terms of their home pages and the resources required to render them, such as images and JavaScript files. Beyond the most popular sites, the probability of finding an IPv4 literal increases to roughly 2 percent. The actual effect of these literals depends on how the site uses these resources; some may not be visible or usable in any network. Some sites were fixed after the owners were notified of such problems. The practical effect of this problem with web-based content is negligible: the volunteers ran into it only a couple of times over the course of a year.

With instant messaging (IM), games, applications, and peripheral devices such as webcams, experiences vary. Some IM applications, particularly those using Extensible Messaging and Presence Protocol (XMPP) or web interfaces, work without problems, while others, such as Skype, do not currently support IPv6 at all. Games that run on a web browser work flawlessly, but there have been only a few stand-alone game applications that have a functioning network mode without IPv4 connectivity. Many peripherals also still support only IPv4. On the other hand, applications such as the widely used BitTorrent clients Vuze and µTorrent, as well as the video-streaming service Netflix, have already added IPv6 support. Switching such bandwidth-intensive applications to run over IPv6 can provide major relief on the NAT of the IPv4 side of networks. The situation is improving for applications that did not previously work with IPv6: a recent release of the massively multiplayer online role-playing game World of Warcraft supports IPv6, and support is on the roadmap for Skype to do the same. Experiments have also shown that IPv6-only networking is easy to arrange on mobile devices; as long as the device itself supports IPv6,

the applications tend to work without any problems.

Conclusions

The number of internet-connected devices has exceeded the capabilities of IPv4 and adoption of IPv6 is needed to deal with the growth – especially in mobile networks, where the number of new users is increasing fastest. The dual-stack mechanism, whereby IPv4 and IPv6 operate side-by-side, is the recommended model for IPv6 migration. If dual-stack is not possible, tunneling mechanisms can be used to provide both IP versions to users. While the number of hosts accessible with IPv6 has historically been low and the connectivity unreliable, initiatives such as World IPv6 Day are improving the situation. IPv4 will no longer be needed in local networks during the final phase of the migration, but NAT64 can be used to connect to the IPv4 internet. While a lot of work remains to be done on IPv6 support for various applications and devices, it is already possible to live and work with an IPv6-only network. ❖

Ari Keränen



is a research scientist at Ericsson Research Packet Technologies in Finland. Ari received his M.Sc. in telecommunications from Helsinki University of Technology in 2008.

He first joined Ericsson R&D in 2005 to do an internship. Then, after working as a researcher at the university, he returned to Ericsson as a researcher in 2007. His research areas, and the topics of his academic publications and IETF standardization contributions, have included delay-tolerant networks, host identity protocol and peer-to-peer networks. His current focus areas are IPv6 and the Internet of Things.

Suresh Krishnan



is a researcher at Ericsson Research Packet Technologies in Montreal, Canada. He has been

working with IPv6 since 1998, and has authored several RFCs related to this area. His main areas of interest include IPv6, IP mobility and the smart grid.

Fredrik Garneij



works with IPv6 at Ericsson Mobile Packet Core products and participates in 3GPP/IETF standardization. He studied automation

engineering at Chalmers University of Technology in Gothenburg, Sweden. He has extensive experience in early deployment of upcoming key internet technologies and is a champion for IP and end-to-end. In 2001 he deployed the first commercial IPv6 network in Europe, while working with Telia. In 2000, he engineered a SIP-based solution that made all Telia employees accessible via their e-mail/SIP addresses. He has participated in several EC projects related to IPv6 and has served as an expert in project audits. His passion and hands-on ability have led to several firsts, including IPv6@Mona Lisa and IPv6 on Android over 3G.

Jari Arkko



is a research scientist at Ericsson Research Packet Technologies in Finland. His main interests include internet architecture,

IPv6, the Internet of Things and social media. He also serves as one of the area directors at the IETF. He has authored 28 RFCs and managed several standards efforts relating to IPv6, mobile IPv6, EAP, secure neighbor discovery, and MOBIKE. He also builds and operates some of this technology for his own networking needs, including running an IPv6-only home automation network.

References

1. Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G.J. and Lear, E. Address Allocation for Private Internets, BCP 5, RFC 1918, February 1996.
2. Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide and Farnam Jahanian, Internet Inter-Domain Traffic, Proceedings of ACM SIGCOMM 2010, New Delhi. August, 2010.
3. Internet Society, World IPv6 Day, <http://isoc.org/wp/worldip6day/>
4. Alexa the Web Information Company, Top 1,000,000 Sites, <http://s3.amazonaws.com/alexa-static/top-1m.csv.zip>
5. B. Carpenter and K. Moore, Connection of IPv6 Domains via IPv4 Clouds, RFC 3056, February 2001.
6. Bagnulo, M., Matthews, P., and van Beijnum, I., Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, RFC 6146, April 2011.