IPv6: A Guide for Governments

www.afrinic.net

www.afrinic.net
African Network Information Centre (AFRINIC)
11th Floor, Raffles Tower, Cybercity Ebene, Mauritius
t: +230 403 5100 | f: +230 466 6758

Table of Contents

Introduction

An Internet Protocol (IP) address is a numeric identifier, like a phone number. Every device connected to the Internet, such as a computer, router or mobile phone, must have a unique IP address so it can communicate with other devices. IP addresses provide every device on the Internet with its own unique identifier to which data packets can be sent. There are two versions of the Internet protocol in use today – IPv4 and IPv6.

IPv4

IPv4 has been in use since the Internet was created. An IPv4 address is a 32-bit long number, represented in a dotted decimal format such as 198.51.100.56.

There are 2^{32} (around 4.3 billion) unique IPv4 addresses and in the early days of the Internet, this seemed like a huge amount. But the Internet grew faster than anyone could have predicted and engineers soon realised that the limited supply of IPv4 address space would not be enough to meet future demand for emerging users and connected devices. In anticipation of this, the Internet Engineering Task Force (IETF) developed, tested and standardised IPv6 in the late 1990s.

IPv6

The main difference between the IPv6 and IPv4 protocols is that IPv6 uses addresses that are 128-bits long (96-bits more than IPv4). An IPv6 address is written in hexadecimal notation, such as 2001:db8:74a3:0042:1000:4e2e:0370:7328.

There are 2^{128} or around 340 trillion trillion trillion unique IPv6 addresses, enough to cater for the predicted increase in devices connecting to the Internet well into the future. First introduced in 1999, the massive pool of IPv6 addresses is expected to allow for expected Internet growth and allow the entire global population to access and enjoy the benefits of the future Internet.

How are IPv4 and IPv6 addresses distributed?

The global pool of IP address space is administered by the Internet Assigned Numbers Authority (IANA), which operates according to the rules that are defined by the five Regional Internet Registries (RIRs)' regional communities (see below). Each RIR uses regionally based, bottom-up, open and inclusive

policy development processes to develop regional and global policies for the distribution and management of Internet number resources.

The IANA delegates the responsibility for large blocks of IP address space to the RIRs according to the global policies defined by all of the regional communities. Each RIR then allocates smaller blocks of address space to their members within their defined service regions according to the regional policies developed by each RIR community.

There are five RIRs in the world, each covering a specific region:

- AFRINIC for Africa and Indian Ocean
- APNIC for Asia Pacific
- ARIN for Canada, many Caribbean and North Atlantic islands, and the United States;
- LACNIC for Latin America and the Caribbean
- RIPE NCC for Europe, the Middle East and parts of Central Asia

Map of the RIR regions

IPv4 Depletion

In February 2011, when IANA allocated two blocks of IPv4 address space to APNIC, the global IPv4 pool depleted to the low level threshold the community had foreseen. This triggered a previously agreed upon global policy, which stated that the 5 remaining blocks of IPv4 address space in the pool would be distributed equally between the five RIRs when the amount of space left in the pool reached a certain level. Each RIR then received one /8 each, which is around 16.8 million IPv4 addresses, irrespective of the amount of unused IPv4 space they already had in their pool at that time..

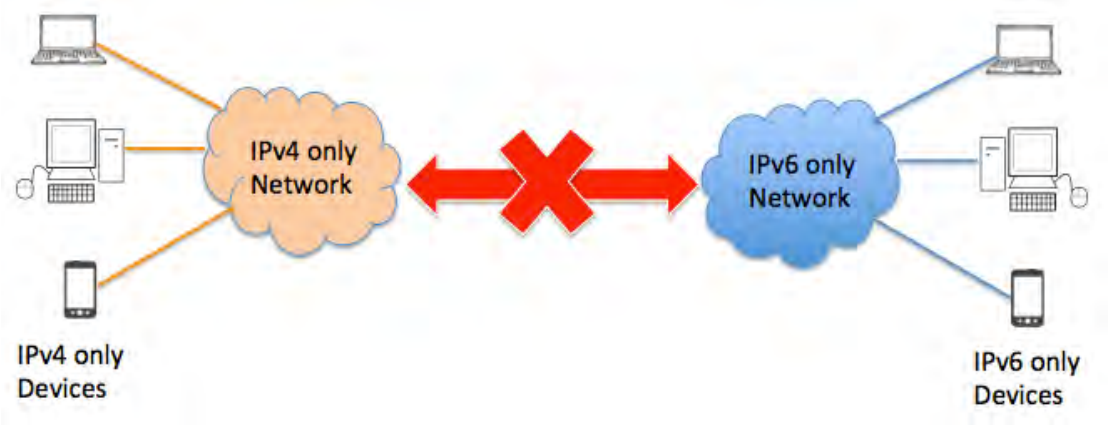
As of 2014, two of the five RIRs, APNIC and the RIPE NCC, were already allocating IPv4 address space from the last /8 they received from the IANA. Both ARIN and LACNIC are expected to exhaust their supplies and start allocating from the last /8 they received from IANA before the end of 2014. IPv4 address space that is being allocated from the last /8 is distributed according to special regional policies developed by each RIR community.

Organisations in the APNIC and RIPE NCC service regions are already unable to obtain large amounts of IPv4 address space to cover their actual needs and can obtain a one-time small allocation to ensure network continuity while deploying IPv6 networks. Existing and emerging networks in these regions face scalaibilty issues unless they deploy IPv6 in order to ensure long-term network growth and global connectivity.

An overview of global IP address consumption can be found online at: http://stats.research.icann.org/rir/

IPv6 Deployment: What's the Hurry?

By design, computers using **IPv4 and IPv6 cannot communicate directly with each other**. Devices connecting to the Internet with only an IPv4 address cannot communicate with devices that are connecting with only an IPv6 address.



On a global scale, it would be impossible to adapt the Internet overnight so that all networks and devices are upgraded to use IPv6. So in order to ensure that the network continues to run seamlessly and all devices around the world can continue to communicate with each other, IPv6 must be deployed in parallel with IPv4. This means that IPv4 and IPv6 will coexist and be operated in parallel for the time it takes to fully deploy IPv6 on a global scale.

To facilitate this period of coexistence and to ensure that the Internet remains reachable to all during the shift towards an IPv6 Internet, the technical community has developed a number of mechanisms to bridge the gap. The

most commonly used transition techniques/mechanisms are detailed on the following pages.

Although AFRINIC currently has a supply of IPv4 address space that is predicted to last for the next few years, the reallity is that the growth of Internet usage throughout Africa and the amount of IPv4 address space being allocated to members throughout the region is increasing rapidly. As consumption rates cannot be predicted, AFRINIC's available pool of IPv4 may be exhausted earlier than predicted.

In anticipation to the exhaustion of AFRINIC's IPv4 pool, the AFRINIC community proposed, developed and accepted AFPUB-2010-v4-005: "The IPv4 Soft Landing Policy". The AFRINIC Board of Directors ratified this policy in 2011. This proposal describes how AFRINIC allocates and manages IPv4 resources during the IPv4 "Exhaustion Phase" which will begin when AFRINIC starts to allocate IP addresses from the last /8 of IPv4 address space it received from IANA in 2011. It ensures that members can still receive a limited amount of IPv4 addresses to be used during the transition period. You can read more about this policy at:
http://www.afrinic.net/en/library/policies/697-ipv4-soft-landing-policy

Governments, operators, service providers and content providers therefore need to prioritise IPv6 deployment as a matter of urgency. **The future of the Internet is over IPv6 and unless Africa also transitions, the region risks becoming isolated from the global Internet.** As the rest of the world moves to IPv6, Africa also has to make sure its networks, services and content are IPv6-ready to ensure the region remains globally connected.

IPv6 Deployment in Africa

Unlike the other RIRs, AFRINIC, for the time being, has enough IPv4 address space left in its unallocated pool to enable African network operators to build clean networks without needing to resort to workarounds, such as NAT (Network Address Translation) or Carrier Grade NAT (CGN). CGN is a common transition technique that allows a single IPv4 address to be shared among several customers.

The global IPv4 address pool is already depleted (see page x). In those regions where operators can only obtain small IPv4 allocations because their RIR has exhausted its supply of IPv4, many now have to invest in IPv6 networks if they have not already done so.

It is extremely important that African network operators also start their transitioning process as soon as possible to ensure they can continue communicating with IPv4 and IPv6 networks in other regions. This will

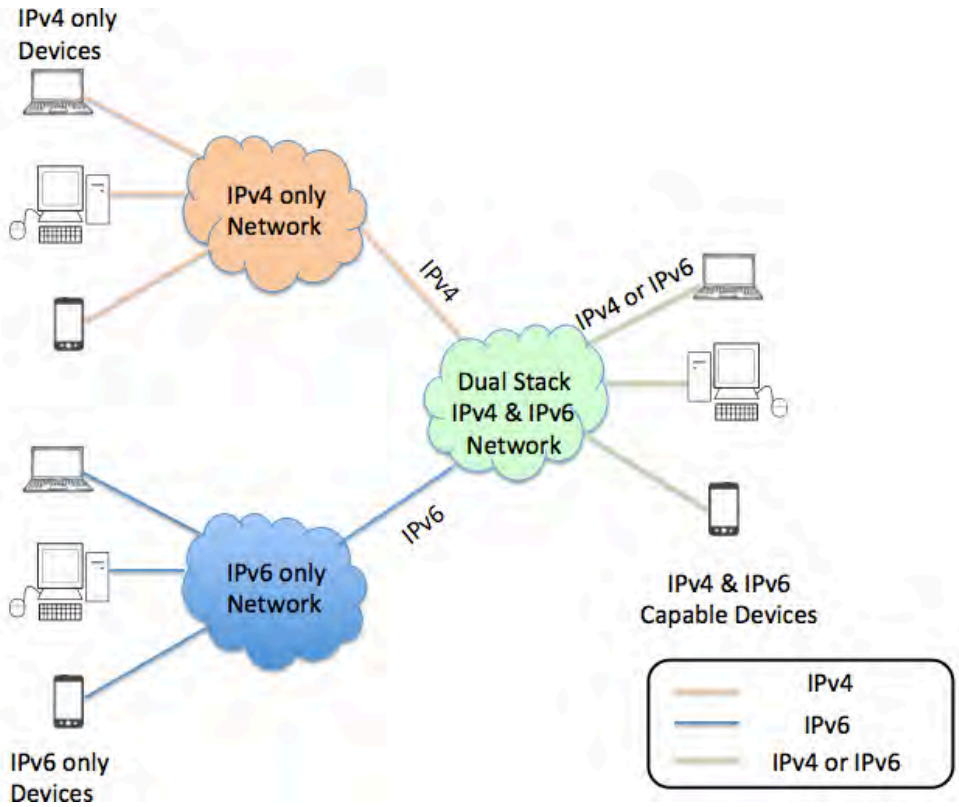
guarantee that all Internet users will be able to freely access the global Internet from Africa.

Transition mechanisms

IPv6 transition mechanisms are technologies that facilitate the coexistence and communication between IPv4 and IPv6 on the same Internet infrastructure. They enable IPv4 networks to interoperate with IPv6 networks and vice versa. It is important to note that there is no "one size fits all" scenario for the gradual deployment IPv6 and networks may choose to deploy one or several techniques based on the nature of services they provide or the equipment the network runs on. Three of the most commonly used types of transition mechanisms are described in this section**: Dual-Stacking, Tunnelling and Address Translation.**

Dual-Stacking

Dual stacking is a transition technology in which IPv4 and IPv6 operate side-by-side. In a dual-stacked network, both IPv4 and IPv6 are fully deployed across the infrastructure so that configuration and routing protocols handle both IPv4 and IPv6 addressing. It allows connected devices to simultaneously reach IPv4 and IPv6 content so it offers a very flexible coexistence strategy. However, connected devices and interfaces need both an IPv6 *and* an IPv4 address.



Organisations operating dual-stacked networks can exchange traffic with:

- IPv4-only networks
- IPv6-only networks
- Other dual-stacked networks

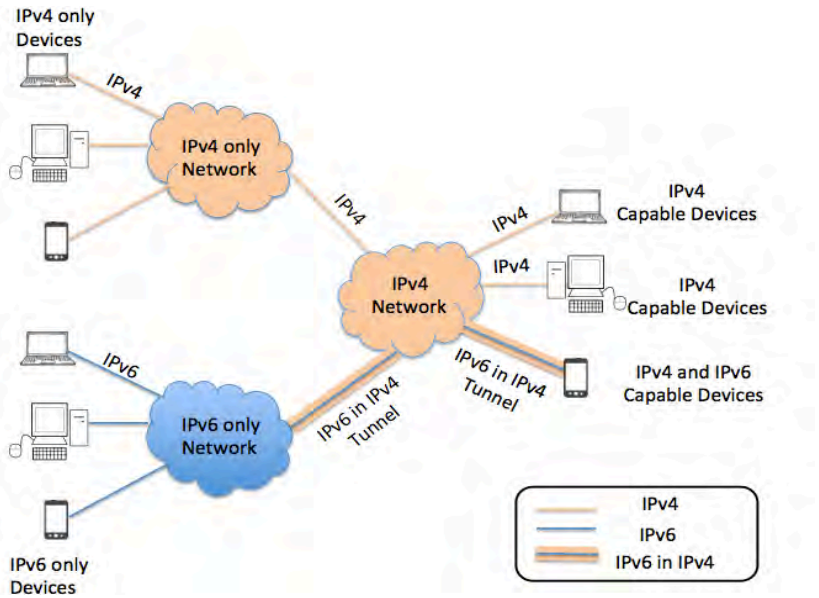
Tunnelling

Tunnelling methods involve using an overlay network that 'tunnels' one Internet Protocol over the other, encapsulating IPv6 packets within IPv4 packets and IPv4 packets within IPv6 packets. This allows packets to be sent over a network that does not support the encapsulated IP version.

Tunnelling enables a network operator to offer a dual-stack gateway interface to their IPv4 only devices prior to completing their full IPv6 infrastructure deployment.

There are two types of tunnels: manual (static) and automatic (dynamic). Manually configured IPv6 tunnelling requires configuration at both ends of the tunnel whereas automatic tunnels are created dynamically based on the packet destination address and routing.

A number of different tunnelling methods are available and can be selected based on the nature of the service or organisation. It is best practice to **dual-stack where you can; tunnel where you must**.



Tunnels can be used to move IPv6 traffic across the IPv4 Internet.

6in4 tunnels

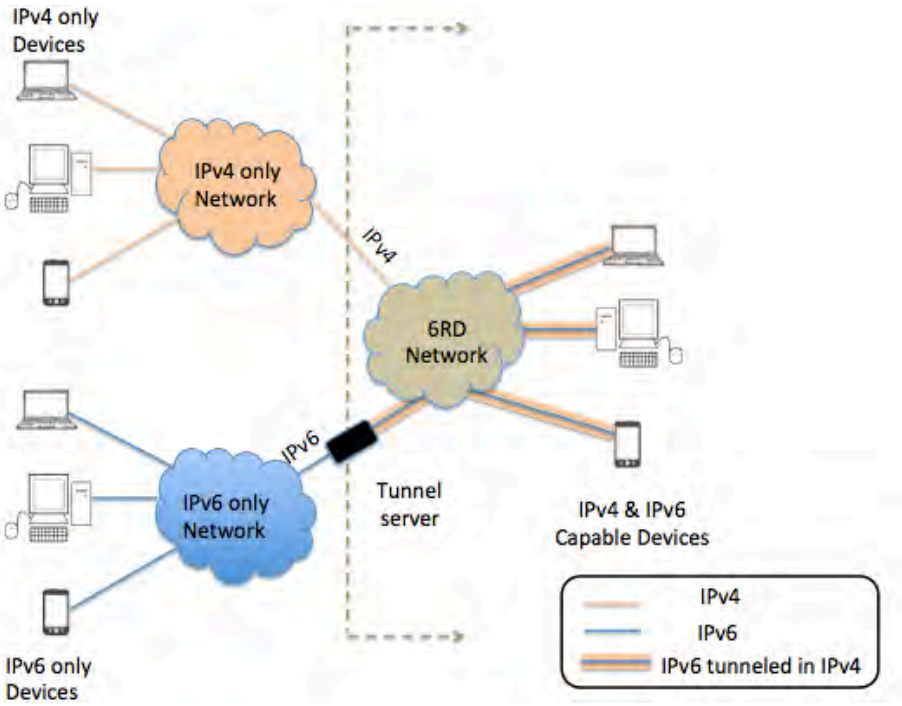
6in4 is an example of a manual tunnel that connects a device to a *tunnel broker*. A tunnel broker is essentially a service provider that offers IPv6 connectivity to another service provider's customers.

The 6in4 tunnelling mechanism often does not work for home or SME users, who commonly make use of NAT in their own network to connect multiple computers. The small routers used for this often lack support to forward this type of tunnelled traffic.

While manual configuration often provides greater stability and protects against certain security threats, it requires some technical knowledge to set up and maintain these tunnels. Also the use of a third party tunnel service could lead to less optimal traffic flows and more complex troubleshooting procedures should any technical problems arise.

IPv6 Rapid Deployment (6RD)

6RD is an example of an automatic tunnelling technique that allows IPv6 sites to communicate with each other over an IPv4 network without the need for any manual configuration. This technology is best applied to large-scale access networks, such as DSL and cable, in which manual configuration would be impossible.



In 6RD the tunnelled traffic remains within the network.

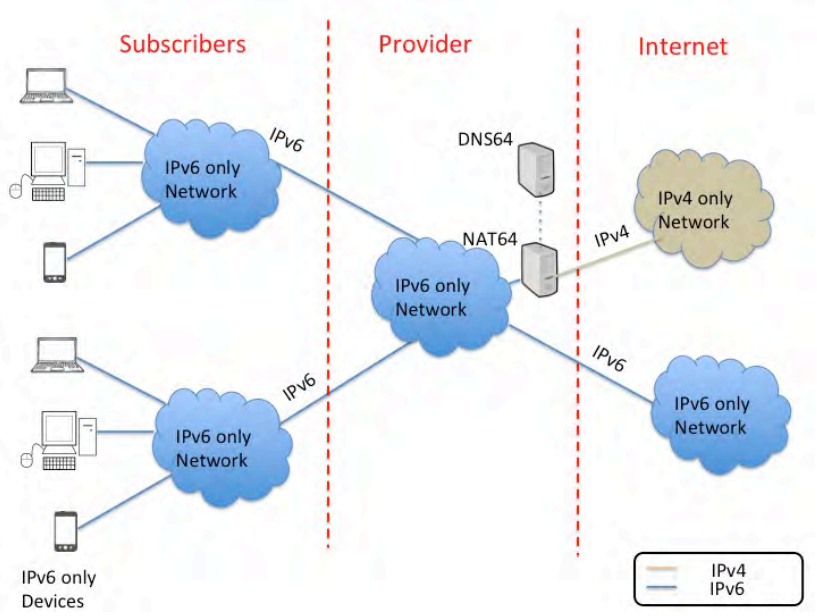
In this technique, the IPv4 and the IPv6 addresses, as well as the configuration parameters, are automatically supplied by the access provider and the IPv6 tunnelled traffic remains in the provider's network. This can simplify troubleshooting and reduce issues that arise from dependencies between different providers.

Security Concerns when tunnelling

The problem with IPv6 tunnelling mechanisms is that most networks have invisible IPv6 traffic running over them because it is disguised as IPv4 traffic. This exposes networks to IPv6-based attacks. Network operators need firewalls capable of handling IPv6 traffic as well as intrusion protection and detection systems in order to have visibility into encapsulated IPv6 packets.
Further, in cases where tunnelled traffic is routed via third party networks, there is an increased risk of interception of data traffic and so-called man-in-the-middle attacks.

Address Translation

Translation mechanisms map an IPv4 address onto an IPv6 address and vice versa. IPv6 translation technologies differ from IPv6 tunnelling technologies in that translation technologies enable IPv4-only devices to communicate with IPv6-only devices in cases where the use of tunnels is not possible or imposes too much overhead on the network. This situation is quite commonly found in GSM-based networks and mobile devices.



However, IPv4/IPv6 translation and IPv4-only translation can be quite

complex. Some translators, such as Network Address Translation - Port Translation (NAT-PT) , work at the network layer and convert all packets from one version to the other version. Other translators are Application Layer Gateways (ALGs) that only convert packets belonging to certain applications. Using dual-stack and tunnelling techniques is preferable to using any of the translation mechanisms.

Drawbacks of transitioning techniques

Apart from Dual-Stacking all the transition technologies described in this document impose certain limitations in the form of reducing network capacity or speed by introducing additional processing and overhead. Or, in case of translation or address sharing, the need for Application Layer Gateways (ALG) could restrict further innovation and the deployment of new protocols and services throughout the Internet. These technologies should only be deployed when there are no alternatives available and used only temporary for as long as the need exists. **Whenever possible the use of Dual-Stack is recommended.**

More Information about IPv6 Deployment

AFRINIC's IPv6 Programme
Since 2005, AFRINIC has been leading the effort to promote and support IPv6 deployment throughout Africa through outreach, education, statistics, and information dissemination.
http://www.afrinic.net/en/services/ipv6-programme

IPv6 Training
AFRINIC offers free IPv6 Training Courses and facilitates IPv6 Forum Certified IPv6 courses throughout the region and governments are encouraged to send technical staff to take part in these courses. AFRINIC also runs an IPv6 test bed to enable engineers to test IPv6 networks in a live environment.
http://learn.afrinic.net/index.php/en/

The AFRINIC Government Working Group
The AFRINIC Government Working Group (AfGWG) ensures that African governments are highly involved in Internet governance and policy matters and can interact with the Internet technical community particularly when it comes to the management of Internet number resources:
http://www.afrinic.net/en/community/ig

Useful Links

Global IPv4 depletion:
http://www.nro.net/news/ipv4-free-pool-depleted

AFRINIC PDP:
http://www.afrinic.net/en/community/policy-development

AFRINIC: IPv4 soft landing policy:
http://www.afrinic.net/en/library/policies/697-ipv4-soft-landing-policy

AFRINIC: free IPv4 pool:
http://www.afrinic.net/en/statistics/ipv4-exhaustion

AFRINIC: How to become a member:
http://www.afrinic.net/en/services/rs/membership-eligibility

IETF
http://www.ietf.org/

Global Policy Proposal for Remaining IPv4 Address Space:
http://www.icann.org/en/resources/policy/global-addressing/proposal-ipv4-report-29nov07-en.htm

APNIC: IPv4 soft landing policy:
http://www.apnic.net/policy/proposals/prop-056

The RIPE NCC: IPv4 Address Allocation and Assignment Policies:
https://www.ripe.net/ripe/docs/ripe-592

www.afrinic.net
African Network Information Centre (AFRINIC)
11th Floor, Raffles Tower, Cybercity Ebene, Mauritius
t: +230 403 5100 | f: +230 466 6758