This section summarizes the most relevant questions on what is meant by IPv4 exhaustion IPv6 adoption for all Internet stakeholders: Internet Service Providers (ISPs), network operators, vendors, regulators, governmental organizations and end users.

IP is the acronym for (Internet Protocol). This protocol was designed in the 1970s to connect computers from different networks. At the beginning, the protocol was for military use, later computers from universities, users and enterprises followed.

Today all devices directly connected to the Internet are identified using Internet Protocol (IP) addresses, unique numbers that are used to route data between different points on the network.

Internet Protocol version 4 (IPv4) is a system of addresses used to identify devices on a network. IPv4 addresses are 32-bit numbers. This means that there are just over four billion unique possible addresses. Over time, and with the rapid growth of the Internet, it became clear that more addresses would be required to ensure ongoing growth and scalability of the Internet.

Internet Protocol version 6 (IPv6) the Internet's next generation protocol. The Internet Engineering Task Force (IETF) developed IPv6 as the long-term solution to forecast IPv4 depletion. IPv6 addresses have 128 bit addresses versus 32 bits in IPv4 addresses. This means that there are over 340 trillion trillion trillion unique possible addresses. IPv4 addresses and IPv6 addresses however are not compatible with each other.

It means that the central pool of available IPv4 addresses managed by the Internet Assigned Numbers Authority (IANA) is empty. As of February 2011, most of the four billion IPv4 addresses available have been allocated for use or reserved for a specific technical purpose.

Phoca PDF

The five RIRs (AFRINIC, APNIC, ARIN, LACNIC and the RIPE NCC) continue to allocate IPv4 address space to their members in accordance with their community-based regional policies until their pools of available IPv4 addresses are depleted.

Yes. The Internet will continue to work and the IPv4 addresses already in use will continue to function.

Yes. This is referred to as (Dual stack), all of the new operative systems and devices that currently support IPv6 allow the simultaneous use of both protocols. This way, the communication with IPv4 only networks as well as IPv6 only networks is possible.

Temporarily, to alleviate the lack of addresses, some networks use Network Address Translation (NAT) mechanisms. These mechanisms share a limited small number of IPv4 addresses among an entire larger network to access to Internet.

Deploying NAT has several negative consequences and may end up breaking applications, services as well as security concerns. Network Address Translator (NAT) is NOT a long-term solution to the IPv4 depletion.

Carrier Grade NAT (CGN) and Large Scale NAT (LSN) are often presented as "IPv6 Transition Technologies". In reality CGN, LSN, or any other mechanisms that provide IPv4-to-IPv4 connectivity on Network Address Translator (NAT) platforms are NOT transition mechanisms to IPv6.

- **Government Organizations:** Coordinate with industry to support and promote awareness and educational activities. Adopt regulatory and economic incentives to encourage IPv6 adoption. Require IPv6 compatibility in procurement procedures. Officially adopt IPv6 within your government agencies.

- **Broadband Access Providers**: Your customers want access to the entire Internet, and this means IPv4 and IPv6 websites. Offering full access requires running IPv4/IPv6 transition services and is a significant engineering project. Multiple transition technologies are available, and each provider needs to make their own architectural decisions.
- **Internet Service Providers:** Implement a plan that will allow your customers to connect to the Internet via IPv6 and IPv6/IPv4, not just IPv4. Businesses are beginning to ask for IPv6 over their existing Internet connections and for their co-located servers. Communicate with your peers and vendors about IPv6, and confirm their timelines for production IPv6 services.
- **Internet Content Providers**: Content must be reachable to future Internet customers. Plan on serving content via IPv6 in addition to IPv4 as soon as possible.
- **Enterprise Customers**: Email, web, and application servers must be reachable via IPv6 in addition to IPv4. Open a dialogue with your ISP about providing IPv6 services. Each organization must decide on timelines, and investment level will vary.

Momentum for IPv6 deployment is increasing globally, while IPv4 addresses are becoming scarce. In February 2011 IANA officially announced the exhaustion of its IPv4 addresses pool. This represented that there were no more space IPv4 available for the Regional Internet Registries.

IPv6 transition mechanisms are technologies that facilitate the transitioning of the Internet from its IPv4 infrastructure to the successor addressing and routing system of Internet Protocol Version 6 (IPv6). Listed below is a description of the different transition mechanisms options available to ensure IPv4 and IPv6 interoperability. These mechanisms are categorized in the following three broad classes:

1. Dual-stack
2. Tunnels (includes configured and automatic tunnels)
3. Translation mechanisms

The term "dual-stack" refers to TCP/IP capable devices providing support for both IPv4 and IPv6. It is important to understand that having a device being able to communicate over both IPv4 or IPv6 does not necessarily means that all applications operating within this device are capable of utilizing both IPv4 and IPv6. The term "Dual-stack routing" refers to a network that is dual IP, that is to say all routers must be able to route both IPv4 and IPv6.

Requiring all new devices be both IPv4 and IPv6 capable permits these devices to have the

Phoca PDF

ability to use either IP protocol version, depending on the services available, the network availability, service, and the administrative policy. A transition scenario called for "dual-stack everywhere" provides the most flexible operational environment. Dual-stacked hosts running on a dual-stack network allow applications to migrate one at a time from IPv4 transport to IPv6 transport. Legacy applications and devices that are not yet upgraded to support access to the IPv6 stack can coexist with upgraded IPv6 applications on the same network system.

The term "tunnelling" refers to a means to encapsulate one version of IP in another so the packets can be sent over a backbone that does not support the encapsulated IP version. For example, when two isolated IPv6 networks need to communicate over an IPv4 network, dual-stack routers at the network edges can be used to set up a tunnel that encapsulates the IPv6 packets within IPv4, allowing the IPv6 systems to communicate without having to upgrade the IPv4 network infrastructure that exists between the networks.

1. **Configured Tunnels**: The term "configured tunnels" is used when network administrators manually configure the tunnel within the endpoint routers at each end of the tunnel. Any changes to the network like renumbering must be must manually reflected on the tunnel endpoint. Tunnels result in additional IP header overhead since they encapsulate IPv6 packets within IPv4 (or vice versa).
2. **Automatic Tunnels**: The term "automatic tunnels" is used when a device directly create their own tunnels to dual-stacked routers for shipping IP packets within IP. The IPv6 Tunnel Broker (RFC 3053), 6to4 (RFC 3056), Teredo (Tunnelling IPv6 over UDP through NATs- RFC 4380) and ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) ship IPv6 packets within IPv4 and can be referenced as IPv6-over-IPv4 mechanisms while DSTM (Dual-stack Transition Mechanism) ships IPv4 packets within IPv6 and can be reference as IPv4-over-IPv6 mechanism.

   The IPv6 tunnel broker mechanism uses dual-stacked servers sitting between IPv6 and IPv4 networks to assist in the set up of a configured tunnel to a host. 6to4, Teredo and ISATAP allow end host systems to create their own automatic tunnels to dual-stacked routers for shipping IPv6 packets within IPv4. While ISATAP is mainly for IPv6-over-IPv4 tunnelling within a domain, all of the other IPv6-over-IPv4 mechanisms are designed to tunnel IPv6 packets out of an IPv4-only administrative domain. Like configured tunnels, automatic tunnelling has double IP header overhead, since tunnels encapsulate IPv6 packets within IPv4 (or vice versa).

   DSTM technique provides a unique solution to the IPv4-IPv6 transition problem. This mechanism is designed to rapidly reduce the reliance on IPv4 routing and is intended for IPv6-only networks in which hosts still occasionally need to exchange information directly with other IPv4 hosts or applications. Network administration is simplified and the need of IPv4 global addresses is reduced. DSTM can be integrated with an IPv6 Tunnel Broker for tighter security integration. DSTM routers can be coupled with IPv4 Firewalls and Intrusion Detection systems to secure IPv4 tunnel endpoints from IPv4-based attacks.

Phoca PDF

Special consideration must be given to the security risk associated with automatic tunnelling as it allows user-nodes to establish tunnels that may bypass a site's security checkpoints such as firewalls and intrusion detection systems. In general, a full dual-stack along with IPv6-capable firewalls, guards, intrusion detection, and end-host security may provide a more secure and interoperable IPv6 transition solution than tunnelling However, for network infrastructures that contain IPv4-only or IPv6-only routing coupled with dual-stack end-nodes, automatic tunnelling provides a flexible transition strategy. Again the risks associated with all potential solutions must be carefully considered.

The term "translators" refers to devices capable of translating traffic from IPv4 to IPv6 or vice and versa. This mechanism is intended to eliminate the need for dual-stack network operation by translating traffic from IPv4-only devices to operate within an IPv6 infrastructure. This option is recommended only as a last resort because translation interferes with objective of end-to-end transparency in network communications. Use of protocol translators cause problems with NAT and highly constrain the use of IP-addressing.

AFRINIC IPv6 webinars | Episode 4 (English) | 09/07/2012

IPv6 webinars archive

- AFRINIC IPv6 webinars | Episode 5 (French) | 15/10/2012
- AFRINIC IPv6 webinars | Episode 4 (English) | 09/07/2012
- AFRINIC IPv6 webinars | Episode 3 (French) | 04/06/2012
- AFRINIC IPv6 webinars | Episode 2 (English) | 30/04/2012
- AFRINIC IPv6 webinars | Episode 1 (English) | 04/04/2012

AFRINIC has an extensive training program provides free training to over 600 network engineers per year on Internet Number Resources Management (INRM) and IPv6 Planning and Deployment.

Our training courses are always growing to support the technologies related to Internet resources, including DNSSEC & RPKI.

Our IPv6 course are IPv6 Forum (Gold) Certified and are fully hands-on, making use of our extensive IPv6 testbed access which gives participants hands-on experience on real equipment to configure, test and troubleshoot IPv6.

Attendance at our workshops is free of charge with priority given to our members. For more details, please visit our dedicated training portal at http://learn.afrinic.net

- IPv6 Address Allocation and Assignment Policy
- Global Policy for IPv6 Allocation from IANA to RIR
- Policy to Change the IPv6 HD Ratio from 0.8 to 0.94
- IPv6 Provider Independent (PI) Assignment for End-Sites

AF6TF

This community driven initiative is dedicated to encourage IPv6 deployment in the African region and to serve as a regional consolidated platform for knowledge and best practice exchange. AFRINIC has volunteered to run all secretariat work for the Task Force, along with providing the hosting platform for the task force's services.

Read more

Webinars

AFRINIC, France Telecom and Internet Society have partnered together in an effort to ignite African IPv6 initiatives and activities. These Webinars aim at assisting African operators with their adoption plans through sharing best experiences and practices region wide. Each month an IPv6 related topic (technical or non-technical) will be chosen for discussion and through out the month the topic will be discussed on the mailing list to get a better understanding of the community's needs and points of view. The webinar will address these topics through a number of regional experts.

Phoca PDF

The webinar will be 90 minutes long, divided into two segments of 45 minutes each:

- Expert presentation and experiences
- Open discussion

Tinga Tinga

Ting'aTing'a is the swahili word for Tunnel. It also doubles for the word tractor or bulldozer that pushes progress forward through building such tunnels, bringing useful and necessary recourses to regions that were considered before hard to reach.

Read more

The Number Resource Organization (NRO) is a coordinating body for the five Regional Internet Registries (RIRs) that manage the distribution of Internet number resources including IP addresses and Autonomous System Numbers. Each RIR consists of the Internet community in its region.

2010

- IPv6 Global Survey: Results of the Global IPv6 Deployment Monitoring Survey.

2011

- IPv6 Global Survey: Results of the Global IPv6 Deployment Monitoring Survey.
- IPv6 around the world: NRO Documentation for Internet Governance Forum (IGF) Kenya

2012

- IPv6 Global survey - Results of the Global IPv6 Deployment Monitoring Survey.
- IPv6 around the world - NRO Documentation for Internet Governance Forum (IGF), Azerbaijan.
- IPv4: Where are we now NRO Documentation for Internet Governance Forum (IGF),

Azerbaijan.

Media & Publications

- IPv4 exhaustion press conference - Press release (PDF)
- Internet address space: economic considerations in the transition from IPv4 to IPv6 - Organisation for Economic Cooperation and Development)
- Analysis of the future exhaustion of the IPv4 Central pool in relation to IANA and its impact on the AfriNIC region (Archive)
- Studies by Geff Huston (APNIC) on IPv4 exhaustion
- The choice; IPv4 exhaustion or IPv6 adoption - Jordi Palet Martinez (PDF)

RFCs

Protocols

- RFC 2460 Internet Protocol, version 6 (specification)
- RFC 2461 Neighbour Discovery for IPv6 version 6 (IPv6)
- RFC 2462 IPv6 stateless address auto-configuration
- RFC 4193 Unique local IPv6 unicast addresses
- RFC 4213 Basic translation mechanisms for IPv6 hosts and routers
- RFC 1887 An architecture for IPv6 unicast address allocation
- RFC 4291 IP version 6 addressing architecture
- RFC 3596 DNS extensions to support IP version 6

Transition & Interoperability

- RFC 4038 Application aspects of IPv6 transition
- RFC 4213 Basic transition mechanisms for IPv6 hosts and routers
- RFC 4380 Teredo: Tunnelling IPv6 over UDP through Network Address translations (NATs)
- RFC 4891 Using IP-sec to Secure IPv6-in-IPv4 Tunnels
- RFC 3053 IPv6 Tunnel Broker
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3064 An Any-cast Prefix for 6to4 Relay Routers
- RFC 3068 Security Considerations for 6to4
- RFC 3942 An IPv6-to-IPv4 Transport

Deployment

- RFC 3750 Unmanaged networks IPv6 transition scenarios
- RFC 4029 Scenarios and analysis for introducing IPv6 into ISP networks
- RFC 4057 IPv6 enterprise network scenarios
- RFC 4192 Procedures for renumbering an IPv6 network without a Flag Day
- RFC 4779 ISP IPv6 Deployment Scenarios in Broadband Access Networks
- RFC 4852 IPv6 Enterprise Network Analysis - IP Layer 3 Focus

Phoca PDF

Relay Translator

- RFC 3338 Dual Stack Hosts Using Bump-in-the-API (BIA)
- RFC 2765 Stateless IP/ICMP Translation Algorithm (SIIT)