# *IPV6 MIGRATION AND ADOPTION IN INDIA*

**By Shweta Satao**

## Abstract

One of the major reasons for the IPv6 transition is because the allocation of IPv4 address space is running out of control and is gradually being exhausted. Though the Regional Internet Registries of all the continents are still allocating IPv4 addresses.

Annually hundreds of millions of new smart phones that require internet connectivity are being sold. These demands for mobile phone have made the demand for internet connectivity to be increasing exponentially. We are in the age of smart mobile devices, social networking, and cloud computing and other new internet developments that are linked to the internet. There is need for Service Providers to ensure there is good, smooth and reliable internet connectivity via IP addresses. These makes IP addresses critical resources that sustain the business growth of service providers and also sustains an exponential economic growth generated through the internet. As hundreds of millions of mobile users are connected to the internet, there is need for a network that is ready for an internet that have both IPv4 and IPv6 addresses “IPv4 and IPv6 networks are not directly interoperable but the technologies used in the transition mechanisms allow hosts on either network to be involved in networking with opposing networks”. The transition mechanisms include: - Dual Stack Techniques - IPv6 over IPv4 tunneling techniques: 6to4 tunnel, Tunnel broker, Manually Configured Tunnel, ISATAP tunnels, IPv6 over IPv4 GRE tunnel. - IPv6 over MPLS (6PE) technique - NAT PT technique - NAT 64 technique.

## Introduction

Devices on the Internet are assigned a unique ip address for their identification.

An Internet Protocol address (IP address) is a numerical identification of a device connected in the computer network. An IP address has two main parts: Host Part and Network part.

Internet Protocol version 4 is the fourth version of the Internet Protocol. IPv4 uses a 32-bit number, using which total 232 addresses can be possible. Internet protocol Version 6 uses a 128-bit address, theoretically allowing 2128 addresses

With the rapid growth of the Internet, There were more requirements of IP address spaces than the IPv4 address space had available.

The total number of possible IPv6 addresses is more than 7.9×1028 times as many as IPv4,

IPv6 provides other technical benefits in addition to a larger addressing space such as Device mobility, security. It permits hierarchical address allocation methods that facilitate combination of two or more networks into a larger network across the Internet,. IPv6 addresses are represented as eight groups, separated by colons, of hex digits each.

IPv6 transition mechanisms are needed to enable IPv6 hosts to reach IPv4 services facilitates the transitioning from the Internet Protocol version 4 (IPv4) infrastructure addressing and routing system of Internet Protocol Version 6 (IPv6).

**Operating system support**

Microsoft Windows has supported IPv6 since Windows 2000, Windows Vista and later have improved IPv6 support. Some peer-to-peer file transfer protocol makes use of IPv6 to avoid NAT issues common for IPv4 private networks.

**Stateless IP/ICMP Translation**

Stateless IP/ICMP Translation (SIIT) translates between the packet header formats in IPv6 and IPv4.The SIIT method defines a class of IPv6 addresses called IPv4-translated addresses.They have the prefix ::ffff:0:0:0/96 and may be written as ::ffff:0:a.b.c.d, in which the IPv4 formatted address a.b.c.d refers to an IPv6-enabled node. The prefix was chosen to yield a zero-valued checksum to avoid changes to the transport protocol header checksum. The algorithm can be used in a solution that allows IPv6 hosts that do not have a permanently assigned IPv4 address to communicate with IPv4-only hosts. Address assignment and routing details are not addressed by the specification. SIIT can be viewed as a special case of stateless network address translation.

The specification is a product of the NGTRANS IETF working group, and was initially drafted in February 2000 by E. Nordmark of Sun Microsystems.[5] It was revised in 2011,[6] and in 2016 its current revision was published.

### Tunnel broker

A tunnel broker provides IPv6 connectivity by encapsulating IPv6 traffic in IPv4 Internet transit links, typically using 6in4. This establishes IPv6 tunnels within the IPv4 Internet. The tunnels may be managed with the Tunnel Setup Protocol (TSP) or AYIYA.

### 6rd

6rd is a mechanism to facilitate rapid deployment of the IPv6 service across IPv4 infrastructures of Internet service providers (ISPs). It uses stateless address mappings between IPv4 and IPv6 addresses, and transmits IPv6 packets across automatic tunnels that follow the same optimized routes between customer nodes as IPv4 packets.

It was used for an early large deployment of an IPv6 service with native addresses during 2007 . The standard-track specification of the protocol is in RFC 5969

Transport Relay Translation

RFC 3142 defines the Transport Relay Translation (TRT) method. TRT employs DNS translation between AAAA and A records known as DNS-ALG as defined in RFC 2694.

### NAT64 and DNS64

NAT64 is a mechanism to allow IPv6 hosts to communicate with IPv4 servers. The NAT64 server is the endpoint for at least one IPv4 address and an IPv6 network segment of 32-bits, e.g., 64:ff9b::/96 (RFC 6052, RFC 6146). The IPv6 client embeds the IPv4 address with which it wishes to communicate using these bits, and sends its packets to the resulting address. The NAT64 server then creates a NAT-mapping between the IPv6 and the IPv4 address, allowing them to communicate.

### DNS64

DNS64 describes a DNS server that when asked for a domain's AAAA records, but only finds A records, synthesizes the AAAA records from the A records. The first part of the synthesized IPv6 address points to an IPv6/IPv4 translator and the second part embeds the IPv4 address from the

A record. The translator in question is usually a NAT64 server. The standard-track specification of DNS64 is in RFC 6147. There are two noticeable issues with this transition mechanism:

- It only works for cases where DNS is used to find the remote host address, if IPv4 literals are used the DNS64 server will never be involved.
- Because the DNS64 server needs to return records not specified by the domain owner, DNSSEC validation against the root will fail in cases where the DNS server doing the translation is not the domain owner's server.

**ISATAP**

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network.

Unlike 6over4 (an older similar protocol using IPv4 multicast), ISATAP uses IPv4 as a virtual nonbroadcast multiple-access network (NBMA) data link layer, so that it does not require the underlying IPv4 network infrastructure to support multicast.

**464XLAT**

464XLAT allows clients on IPv6-only networks to access IPv4-only Internet services, such as Skype.

The client uses a SIIT translator (see above) to convert IPv4 packets (e.g. Skype client software) into IPv6 to send (over an IPv6-only network) to a NAT64 translator (see above) which translates them back into IPv4 to send (over an IPv4-capable network) to an IPv4-only server (e.g. Skype server). The SIIT translator (CLAT: customer-side translator) may be implemented on the client itself (as special software) or an intermediate IPv4-capable LAN (but if it had IPv4 Internet connectivity, 464XLAT would not be needed), and the NAT64 translator (PLAT: provider-side translator) must be able to reach both the server and the client (through the CLAT).

The use of NAT64 limits connections to a client-server model using UDP, TCP, and ICMP.

Dual-Stack Lite (DS-Lite)

"DS-Lite" redirects here. For the video game system, see Nintendo DS Lite.

### DS-Lite

Dual-Stack Lite technology does not involve allocating an IPv4 address to customer-premises equipment (CPE) for providing Internet access. It is described in RFC 6333. The CPE distributes private IPv4 addresses for the LAN clients, according to the networking requirement in the local area network. The CPE encapsulates IPv4 packets within IPv6 packets. The CPE uses its global IPv6 connection to deliver the packet to the ISP's Carrier-grade NAT (CGN), which has a global IPv4 address. The original IPv4 packet is recovered and NAT is performed upon the IPv4 packet and is routed to the public IPv4 Internet. The CGN uniquely identifies traffic flows by recording the CPE public IPv6 address, the private IPv4 address, and TCP or UDP port number as a session.

Lightweight 4over6 (RFC 7596) extends DS-Lite by moving the NAT functionality from the ISP side to the CPE, eliminating the need to implement carrier-grade NAT. This is accomplished by allocating a port range for a shared IPv4 address to each CPE. Moving the NAT functionality to the CPE allows the ISP to reduce the amount of state tracked for each subscriber, which improves the scalability of the translation infrastructure.

### 4rd

IPv4 Residual Deployment (4rd) is a mechanism specified in RFC 7600 to facilitate residual deployment of the IPv4 service across IPv6 networks. Like 6rd, it uses stateless address mappings between IPv6 and IPv4. It supports an extension of IPv4 addressing based on transport-layer ports. This is a stateless variant of the A+P model.

### MAP

Mapping of Address and Port (MAP) is a Cisco IPv6 transition proposal which combines A+P port address translation with tunneling of the IPv4 packets over an ISP provider's internal IPv6 network.[24] As of July 2015, MAP-T and MAP-E are proposed standards.

### NAT-PT

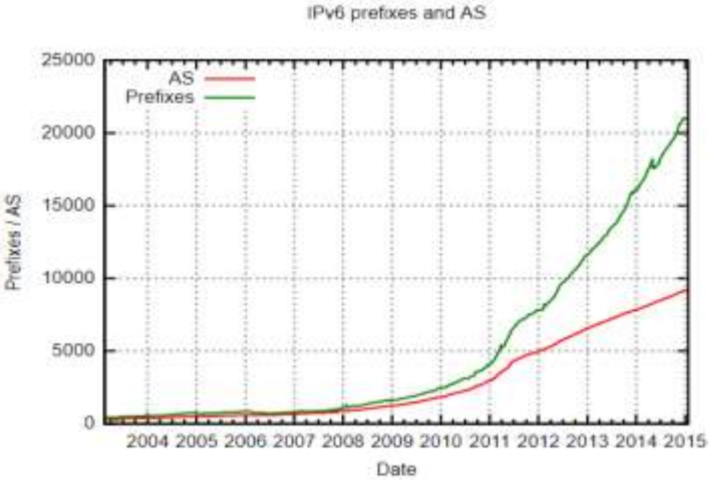
Network Address Translation/Protocol Translation (NAT-PT) is defined in RFC 2766, but due to numerous problems, it has been obsoleted by RFC 4966 and deprecated to historic status. It is typically used in conjunction with a DNS application-level gateway (DNS-ALG) implementation.

### NAPT-PT

While almost identical to NAT-PT, Network Address Port Translation + Protocol Translation, which is also described in RFC 2766, adds translation of the ports as well as the address. This is done primarily to avoid two hosts on one side of the mechanism from using the same exposed port on the other side of the mechanism, which could cause application instability and/or security flaws. This mechanism has been deprecated by RFC 4966.

### IPv6 Deployment in India

According to Google's statistics, India has reached an IPv6 adoption rate of around 33% at the end of December 2018.



## Conclusion and future scope

Having explained the IPv6 technology and its social implications to you, we hope you will consider migrating to IPv6. You have been given you all the information needed to help you make the right business decision concerning the deployment and implementation of an IPv6 network. This information is for the general public. You are the internet stakeholders. It doesn't matter whether you are an internet service provider, a network operator, a vendor, a regulator, a governmental organization or an end-user. IPv6 technology is for you. It is the future of the internet. Make the right decision now by investing in the future now. Think IPv6!

## References

1. *"IPv6 adoption". Retrieved 2014-01-21.*
2. *"IPv6 – Google".*
3. *"IPv6 transit". Sixxs.net. Retrieved 2012-01-20.*

## Bio

Shweta Satao is working as an Assistant Professor at Bharat College of Arts & Commerce. The author can be reached at shwetasatao@gmail.com