riverbed

WHITE PAPER

Key Steps in the Transition to IPv6

Ashton, Metzler & Associates

Leverage Technology & Talent for Success

Content

Introduction

The Internet is rapidly running out of globally unique, routable IPv4 addresses. The free pool of addresses held by the Internet Assigned Numbers Authority (IANA) was depleted in February 2011. While each Regional Internet Registry (RIR) still has a free pool of addresses previously assigned to it by IANA, these pools are expected to be exhausted some time between 2011 and 2013. As these RIR pools become depleted, public IPv4 addresses will become at best a scarce resource, and at worst a non-existent resource. This is a challenge that must be addressed by enterprise IT organizations as well as ISPs and web properties such as Yahoo and Google.

The problem of IP address scarcity is exacerbated by the fact that the population of Internet-connected devices is projected to grow from 6 billion today to 15 billion in 2015[1]. This population explosion is the result of increases in the number of users, as well as rapid increases in the number of Internet-connected devices per user, including computers, TVs, smart phones, tablets, game consoles, smart appliances, and smart grid utility meters.

As IPv4 addresses become scarce, Internet Service Providers (ISPs) can buy some time by supporting wider use of Network Address Translation (NAT) both in CPE devices and in the ISP's access networks. However, a more strategic solution is to begin to support IPv6. Unlike IPv4 that allocates 32 bits for an IP address, IPv6 allocates 128 bits for an IP address. As a result, IPv4 provides 4.3×10^{10} (4.3 billion) IP addresses, which is slightly less than one IP address for each person currently on the earth. In contrast, IPv6 provides 3.4×10^{38} IP addresses, which is roughly 5.6×10^{29} addresses for each person currently on the earth.

So, while there is no doubt that IPv6 provides more than enough IP addresses for any conceivable situation, transition to IPv6 is complicated by the fact that IPv6 is not backwards compatible with IPv4. One of the implications of this fact is that as the number of Internet-connected devices continues to grow, it is inevitable that user devices will emerge that support IPv6 only, rather than support both IPv4 and IPv6 in a dual stack configuration. However, the majority of Internet services and content will be based on IPv4 for the foreseeable future. Consequently, the dual protocol Internet will need to provide some sort of gateway functionality that will allow interoperability between single stack end systems that support only IPv4 or only IPv6. Without this functionality, IPv6-only user devices will not have access to the full content of the Internet.

The remainder of this white paper provides a brief overview of some the technologies that are available to enterprise IT organizations, ISPs and web properties as they make the transition to IPv6. This white paper is intended to serve as a framework for organizations that are planning their migration to IPv6. The goal of this white paper is to ensure that the Internet's transition to IPv6 will have a minimal impact on normal business communications. It concludes with a discussion of how Riverbed's Stingray Traffic Manager supports the transition to IPv6.

Internet Movement to IPv6

ISPs seeking to significantly expand their customer bases will need to adopt a strategy that is not based on their ability to obtain additional globally unique IPv4 addresses. A wide range of mechanisms is available to support the conservation of IPv4 addresses and the eventual transition to IPv6. These mechanisms are primarily based on the familiar technologies of address translation, tunneling, and encapsulation and include:

- **Shared IPv4 Addresses:** With this approach, the ISP shares a globally routable IPv4 address among several hundred or even thousands of its subscribers using network address translation (NAT). Each subscriber's private IPv4 address is only used within the ISP network and ISP NAT functionality is used to provide access to IPv4 resources on the Internet. This form of NAT, allowing multiple subscriber to share a single public IPv4 address, is sometimes referred to as NAT44. NAT44 does not preclude the subscriber from also using IPv4 NAT within his Intranet.

- **Address Family Translation (AFT):** Address Family Translation (AFT) involves the translation of an address from one IP address family to another. NAT 46 refers to the bidirectional translation between an IPv4 address and an IPv6 address when the initiator is on the IPv4 side, while NAT64 refers to this type of translation when the initiator is on the IPv6 side. NAT46 can be deployed in conjunction with Shared IPv4 addresses to allow subscribers to access both IPv4 and IPv6 resources. NAT46 is not likely to be needed until a significant amount of Internet content is based solely on IPv6. NAT64 will be needed earlier in the transition process since it is likely to be used by providers of wireless services to 4G mobile devices that support only IPv6 protocol stacks.

[1] http://www.intel.com/technology/advanced_comm/322202.pdf

- **IPv6 Rapid Deployment (6rd):** IPv6 rapid deployment (6rd) allows an ISP to support IPv6 service delivery over an IPv4 access network. This is possible only if the subscriber's CPE supports stateless IPv6 in IPv4 encapsulation and the ISP provides 6rd gateway functionality to terminate the tunnel at the edge of the IPv6 Internet. Within the provider network, 6rd could coexist with both NAT44 and NAT64.
- **Dual Stack:** As the ISP begins to support IPv6 routing, each existing subscriber can be issued a routable IPv6 address block in addition to the existing routable IPv4 address block or shared IPv4 address. The subscriber's end systems would then select the appropriate stack with which to connect to another computer on the Intranet or Internet. Where the dual stack is based on a shared IPv4 address, NAT44 would be required as noted earlier. Dual stacks are recommended by the IETF as the best general approach to a transition to IPv6.
- **Dual-Stack Lite (DS-Lite):** At some point in the future, the service provider network will be based on routing only IPv6 traffic. When this occurs a DS-Lite CPE can be used to tunnel IPv4 traffic through the IPv6 network to a DS-Lite gateway that terminates the tunnel and converts a subscriber's private IPv4 address to a public IPv4 address via NAT44.
- **IPv6-only:** In this scenario, the ISP no longer supports Internet access via IPv4. The CPE and ISP access network will support only IPv6 and subscriber communications with IPv4 resources could possibly be provided via ISP NAT64.

Each ISP will select the transition and coexistence technologies that is best suited to their specific network and subscriber base. The result will be several distinct categories of Internet users based on type of support provided for IPv4 address conservation or IPv6:

- **Public IPv4-only**: This status quo group of users can only access IPv4 services.
- **Shared Public IPv4-only:** This group's connections to the Internet go through a NAT44 function operated by the ISP. This user can only access IPv4 servers.
- **Dedicated or Shared Public IP plus ISP NAT46:** These users can access all IPv4 and IPv6 servers.
- **Shared IPv4 and IPv6:** A group of dual stack users who have a shared IPv4 and a routable IPv6 address providing access to all IPv4 services through a NAT44 device and native access to all IPv6 services.
- **Public IPv4 and IPv6:** This group of users has dual stack devices and can access both IPv4 and IPv6 services without any restrictions.
- **IPv6-only:** This class of user has only an IPv6 address and can access only IPv6 services.
- **IPv6-only plus ISP NAT64:** These users can access all IPv4 and IPv6 servers.

Impact on the Enterprise

There are a number of possible reasons for enterprises to consider supporting IPv6 in the enterprise network, including government regulations and mandates, support for new IPv6 applications, and enhanced security. However, for most organizations the transition to IPv6 will be driven initially by the need to provide a full set of services for partners and new Internet users that are accessing the Internet with devices restricted to IPv6-only Internet access. This type of Internet newcomer may become quite numerous, especially as smartphones transition to 4G technologies, such as LTE. Enterprises can deliver web services to IPv6-only clients by providing a NAT64 AFT function in routers, load balancing devices, or other types of reverse proxies. These alternatives are discussed in greater detail in the next section of this paper.

As more IPv6 content and services begin to appear on the Internet, the enterprise will need to give its employees access to this IPv6 content. If the ISP does not provide NAT46 services, it may be sufficient initially to use dual-stack application proxies for email and web access in conjunction with IPv6 access. These proxies can act as application-specific gateways between an IPv4 intranet user and an IPv6 service or content on the Internet. In addition, some future IaaS or SaaS cloud computing services may be accessible only over the Internet via IPv6. In this case, application proxies may need to be supplemented by a NAT46 function provided by either the Enterprise or the ISP. When more content is based on IPv6, an enterprise transition to dual stack end systems could be considered.

In general, IPv4 address exhaustion will not affect the operations within the enterprise Intranet. Internal users can continue to access internal applications using IPv4 for years after the Internet transitions to IPv6. An exception might be where an enterprise uses a small block of public IPv4 addresses in their Intranet and then finds that it needs a large number of additional addresses to accommodate new employees. This problem could be solved by either a transition to IPv6 or a transition to a private IPv4 address and the use of NAT. This latter approach might not be the best choice in those instances in which the enterprise wants to leverage certain applications, such as Microsoft Windows 2008 Clustering, that run on IPv6 by default. On an IPv4 network, this class of application would typically tunnel the IPv6 through IPv4. Unfortunately, this approach reduces the ability of network management tools to monitor and control this type of traffic.

Establishing Enterprise Web Presence on the IPv6 Internet

The first step in establishing a web presence on the IPv6 Internet is to acquire a block of routable IPv6 addresses to be used in the Internet data center. Typically, this would be provider allocated (PA) address space obtained from an ISP. If the web service is multi-homed involving multiple ISPs, as would often be the case for Cloud Balancing or Cloud Bursting among disparate IPv6 data centers, it would be necessary to acquire provider independent (PI) address space from a Regional Internet Registry.

The second step is to configure IPv6 routing on routers and possibly other Layer 3 devices in the Internet data center. Most routers and Layer 3 switches have incorporated support for IPv6 for a number of years. The third step in the process is to enable IPv6 on the front end of all web servers. There are multiple ways of adding IPv6 client connectivity to a web server farm, including:

- **Enabling native IPv6 on existing web servers:** Many modern web server platforms have supported IPv6 for some time. The result is dual stack web servers capable of delivering the same content to both IPv4 and IPv6 clients.
- **Adding a set of dedicated IPv6 web servers:** This involves deploying additional servers and replicating at least some of the web content from IPv4 web servers to the IPv6 web servers.
- **Deploying NAT64 AFT in the Internet Data Center:** This allows IPv6 clients to gain access to content on IPv4 web servers. When stateful NAT64 is used in conjunction with DNS64, no changes are required in either the IPv6 client or the IPv4 server. DNS64 is a DNS server that synthesizes the AAAA records from A records. When asked for a domain's AAAA records and only A records exist, DNS64 synthesizes a IPv6 address with a first part that points to a NAT64 device and a second part that embeds the IPv4 address from the A record. NAT64 functionality can be implemented in routers, load balancing devices, or other types of reverse proxy servers. It is expected that router vendors will add the NAT64 function to their enterprise product lines in 2011 or 2012. Some multi-function Application Delivery Controllers (ADCs) that include load balancing functionality already support NAT64 functionality.

There are a number of advantages of deploying NAT64 in the ADC or load balancing device, including:

- AFT is applied exactly where it is needed in the data center, as the IPv6 traffic enters the web server farm
- No additional web servers are required and no re-configuration of existing IPv4 web servers is required
- There is no reconfiguration or performance impact on load balanced IP v4 applications
- Data center routers do not need to be upgraded and there is no concern that NAT64 processing will affect router throughput for native IPv4 traffic entering the data center

The State of IPv6 Migration

The need to migrate to IPv6 has been discussed for such a long period of time that until recently many organizations ceased to pay any attention to the topic. That situation has changed dramatically in the last year. For example, 455 of the attendees at the Fall 2011 Interop conference were surveyed about their IT organization's plans to migrate to IPv6. Twenty percent of the survey respondents indicated that their IT organization has an IPv6 migration plan in place and over half of these organizations have already begun to implement their migration plan and the rest of the organizations expect to within a year.

Another example of the growing interest in IPv6 is that on June 8, 2011 many of the top websites and ISPs around the world, including Google, Facebook, Yahoo!, Akamai and Limelight Networks joined together with more than 1000 other participating websites in World IPv6 Day[2]. This was a highly successful, global-scale trial of the use of IPv6. The event helped to demonstrate that major websites around the world are well positioned for the move to a global IPv6-enabled Internet. However, the interest

[2] http://www.worldipv6day.org/

that these websites have in IPv6 is not constrained to a one-day event. According to the IPv6 Forum[3] there are more than 1300 worldwide web sites that are IPv6 enabled and there are 118 ISPs that currently provide IPv6 connectivity. Two of the ISP that provide IPv6 connectivity are described below.

- **Verizon**
  According to Verizon[4], they currently offer their enterprise and government customers IPv6 dedicated Internet services on a global basis, including support for Dual Stack, native and tunneled IPv6. They also intend this year to roll out IPv6 capabilities across their global Private IP network services and are offering a suite of professional consulting services to help businesses and government agencies create an IPv6 adoption plan within their specific operations.

  In addition, the new Verizon Wireless 4G LTE network has IPv6 built-in with the requirement that all LTE devices must be IPv6 capable. The Verizon websites are becoming IPv6-enabled, and Verizon has stated their commitment to continue to test IPv6 with their FiOS service to make this transition as seamless as possible for all of our customers.

- **AT&T**
  According to AT&T[5], based on connectivity to the North American Task Force's Moonv6 next-generation Internet network, AT&T's customers can currently access the broader IPv6 Internet using either tunneling technologies or an overlay network for native IPv6 protocol support. AT&T also states that they have established IPv6 peerings with other IP backbone providers, such as Global Crossing and that this allows agencies to seamlessly exchange IPv6 traffic across the two networks. Agencies who want dual homing can enjoy diverse routing for their IPv6 traffic to maintain continuity of operations.

  AT&T has announced their intention to offer a range of services and technologies in order to support the federal government's IPv6 mandate. The services they have announced include a managed IPv6 Internet connectivity service that provides connectivity to the IPv6 Internet and a remote access service to the IPv6 Internet for small locations and individual remote users. The technologies they have announced include the Tunnel Setup Protocol (TSP) and the support of multiple access methods, including PPP, MLPPP, Frame Relay and ATM.

  AT&T also offers a range of professional services designed to facilitate IPv6 migration. This includes IPv6 planning, architecture and migration, implementation, and optimization.

The Riverbed Solution for Web Presence on the IPv6 Internet

Riverbed Stingray Traffic Manager is a virtual appliance software product that incorporates a number of functions including Global Server Load Balancing (GSLB), Application Delivery Controller local load balancing, HTTP Caching, and other traffic optimization and application optimization capabilities. Traffic Manager v5.0 has supported NAT64 AFT functionality since its introduction in 2008.

As shown in Figure 1, a cluster of Stingray Traffic Manager vADCs can be used to front end a web server farm. The cluster provides fault tolerant processing of virtual IP addresses, which can be either IPv4 or IPv6 addresses. The traffic received via these virtual addresses is load balanced across the farm of web servers, based on a variety of local or global parameters. If the web servers support only IPv4, the Traffic Managers can use NAT64 to translate IPv6 addresses to IPv4 addresses. If the web server pool is comprised of a mixture of IPv4 and IPv6 servers, the Traffic Managers can use a mixture of native IPv4, native IPv6, NAT 64, and NAT46 to establish client connections to the web servers.

[3] http://www.ipv6forum.com/ipv6_enabled/approval_list.php

[4] http://www.verizonbusiness.com/about/news/pr-25703-en-Verizon+Expands+Support+for+Next+Generation+Internet+Protocol+Across+Dedicated+Internet+Services.xml

[5] http://att.de/gov/solution/network_services/data_nw/ipv6/

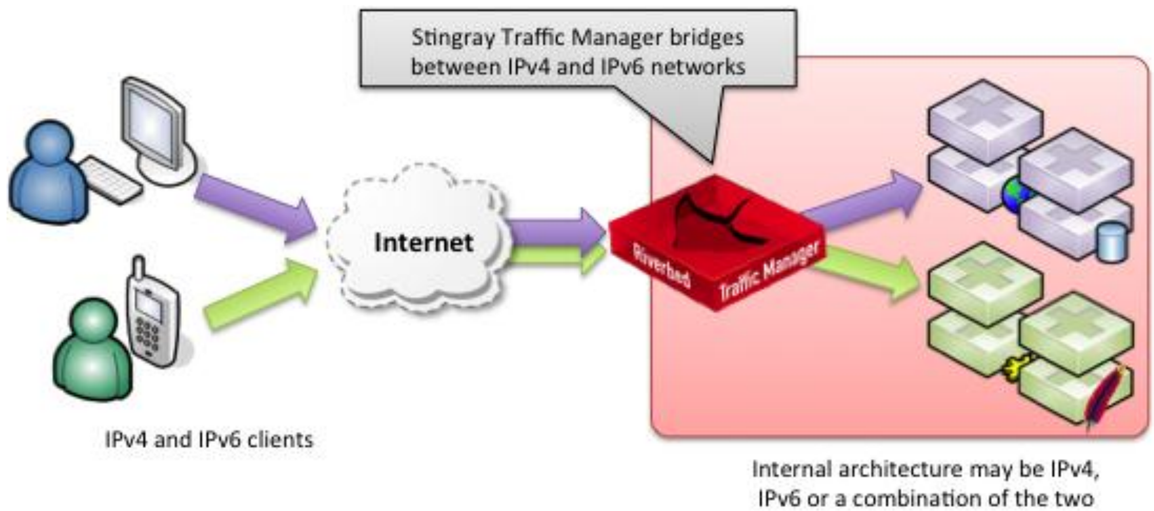

Figure 1: Stingray Traffic Manager Clustered ADC Solution

Conclusion

The transition of the Internet from IPv4 to IPv6 will pose significant challenges for ISPs, other service providers on the Internet, enterprises and consumers. As a result, most organizations have preferred to postpone implementation of IPv6 transition programs until those programs are absolutely necessary in order to maintain normal business operations. Given that the last pools of IPv4 addresses are expected to be depleted by 2012, the time to commit resources to finalizing IPv6 transition plans and to begin early implementation is at hand. Fortunately, many technologies have emerged over the last few years that make it fairly easy for ISPs to make the transition to IPv6. These technologies include NAT44, AFT, NAT46, NAT64, IPv6 Rapid Deployment, dual-stack and dual-stack lite.

IT organizations that want to begin the transition to IPv6 can start by establishing a web presence on the IPv6 Internet by acquiring a block of routable IPv6 addresses to be used in the Internet facing data center. They would need to configure IPv6 routing on its routers and possibly on other Layer 3 devices in their Internet facing data centers. The organization would also have to enable IPv6 on the front end of all web servers. Another key step that any IT organization that envisions transitioning to IPv6 needs to take is to only acquire networking equipment that supports the functionality that will enable that transition.

riverbed

Riverbed Technology, Inc.
199 Fremont Street
San Francisco, CA 94105
Tel: (415) 247-8800
www.riverbed.com

Riverbed Technology Ltd.
One Thames Valley
Wokingham Road, Level 2
Bracknell, RG42 1NG
United Kingdom
Tel: +44 1344 401900

Riverbed Technology Pte. Ltd.
391A Orchard Road #22-06/10
Ngee Ann City Tower A
Singapore 238873
Tel: +65 6508-7400

Riverbed Technology K.K.
Shiba-Koen Plaza Building 9F
3-6-9, Shiba, Minato-ku
Tokyo, Japan 105-0014
Tel: +81 3 5419 1990