IPv6-ready Ethernet Switches for Industrial Networking

Ray Hsu, Supervisor, Product Marketing

support@moxa.com

Overview

Experts foresee that the depletion of unallocated IPv4 addresses will become a major problem in the next two to three years, unless an alternative solution is found.

As of September 2007, nearly 80% of the world's IPv4 address capacity was exhausted, leaving only 20% for future Internet users. In recent years, the demand for IPv4 addresses has steadily accelerated due to rapid population growth, broadband deployment, and global demand for unique addresses for communication applications such as Voice over IP (VoIP), mobile phones, and connecting sensors over the Internet.

Experts foresee that the depletion of unallocated IPv4 addresses will become a major problem within the next two to three years, unless an alternative solution is found. According to Geoff Huston, **the Internet Assigned Number Authority (IANA)** will exhaust all available IPv4 addresses in the IANA pool by 2010 and the **Regional Internet Registries (RIRs)** will run out of large unallocated contiguous blocks of IPv4 addresses in 2011 (Chart 1 and 2)[1] if current allocation rates prevail.

[1]OECD Report: "Internet Address Space", Seoul, South Korea, 15–17 June, 2008.

Released on March 3, 2009

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778
Web: www.moxa.com
Email: info@moxa.com

MOXA®

This document was produced by the Moxa Technical Writing Center (TWC). Please send your comments or suggestions about this or other Moxa documents to twc@moxa.com.

IPv4 Consumption Model (IANA Pool)

Chart 1: IPv4 address exhaustion by IANA
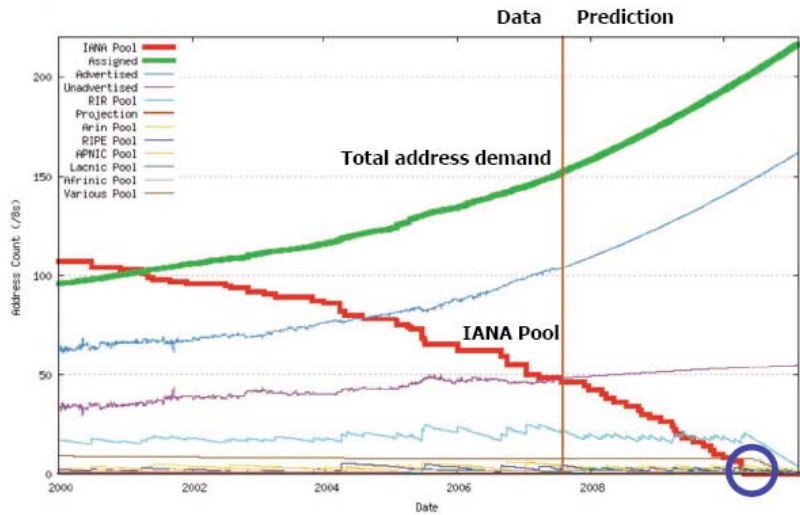
IPv4 Consumption Model (RIR Pool)

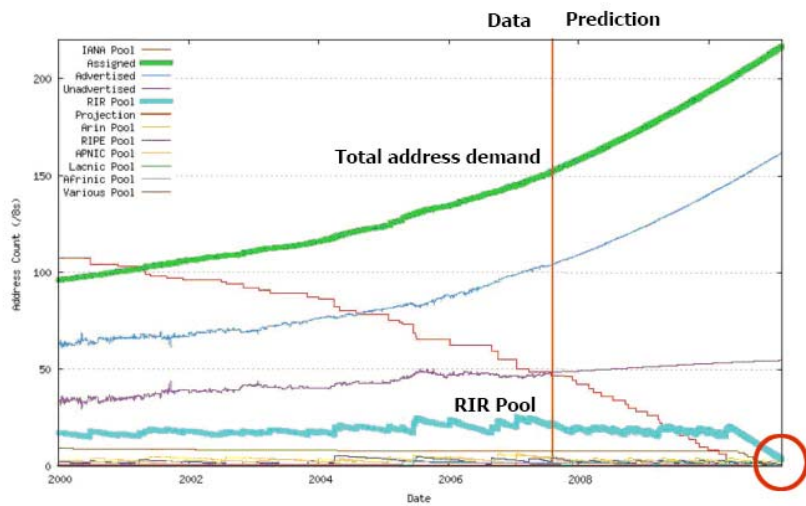Chart 2: IPv4 address exhaustion by RIR

As a result, the coming exhaustion of IPv4 addresses has been the driving force in creating and adopting several new technologies including Classless Inter-Domain Routing (CIDR) addressing, Network Address Translation (NAT) and a new version of the Internet Protocol, IPv6. The transition of the Internet to IPv6 is generally seen as the only practical and readily available long-term solution to IPv4 address exhaustion.

What is IPv6 and Why Now?

The Internet Protocol Version 6 (IPv6) is the next generation protocol designed by the Internet Engineering Task Force (IETF) to replace Internet Protocol Version 4 (IPv4). Most of today's Internet and enterprise networks use IPv4, which is now more than twenty years old as it was first introduced in the 1980s.

When IPv4 was originally developed, the sheer vastness of today's Internet was beyond imagination. Although this protocol is still the standard for the Internet, its limitations have been surfacing for some time. The primary constraint is that IPv4 address space only allows up to four billion nodes on the network, and the number of free addresses is rapidly depleting due to the Internet's continuous expansion. In contrast, IPv6 allows for 340 undecillion (340×10^{36}) addresses, large enough to accommodate expansion of the Internet to include every electronic device in the world—now and in the future.

Features of IPv6

Even though NAT has given IPv4 a slightly longer life span, it only delays the world's inevitable transition to IPv6. IT professionals will most likely encounter fierce debates over this issue in the coming years. Is this transition realistic and necessary? And what are the supporting arguments?

Let's examine the advantages of using IPv6 over IPv4. These benefits include:

- **Large Address Capacity**

  IPv6's extremely large address capacity enables global connectivity to many more electronic devices such as IPTV, mobile phones, laptops, in-vehicle computers, cameras, building sensors, medical devices, and more.

- **Enhanced Security**

  Authentication and encryption are mandatory in IPv6 and provided through IPsec. The protocol defines authentication and encryption extension headers separately so that higher layer applications can use either or both of these functions when required.

- **Address Auto-Configuration**

  A highly valuable feature of IPv6 is its ability to automatically configure itself without the use of a stateful configuration protocol, such as Dynamic Host Configuration Protocol for IPv6 (DHCPv6). By default, an IPv6 host can configure a link-local address for each interface. By using router discovery, a host can also determine the addresses of routers, additional addresses, and other configuration parameters.

- **Multicast**

  The ability to send a single packet to multiple destinations is a basic specification in IPv6, unlike IPv4 where it is optional.

- **Better Support for QoS**

  New fields in the IPv6 header define how traffic is identified and handled. Traffic identification, by using a Flow Label field in the IPv6 header, allows routers to identify and provide special handling for packets that belong to a flow. A flow is a series of packets between a source and destination. Because the traffic is identified in the IPv6 header, support for QoS can be easily achieved even when the packet payload is encrypted with IPsec.

- **Support for Mobile Devices**
  IPv6 is designed to account for mobile networks, the ubiquitous networks of the future that provide on-line connectivity, anytime and anywhere. IPv6 is considered to be the backbone of the future information society.

The Transition from IPv4 to IPv6

Due to the time required for massive infrastructure deployment, IETF has been working on specific provisions to allow a smooth transition from IPv4 to IPv6, as well as hardware and software interoperability solutions so new IPv6 devices can access IPv4 hosts. A technique was developed in IPv6 to allow administrators to embed IPv4 addresses within IPv6 addresses. Special solutions are defined to handle interoperability, including:

- **"Dual Stack" Networking**
  This approach requires hosts, routers and some other network devices to implement both IPv4 and IPv6 protocols. This enables networks to support both IPv4 and IPv6 services and applications during the transition period. The dual-stack approach is a fundamental mechanism for introducing IPv6 in existing IPv4 architectures and will remain heavily used in the near future.

- **IPv4/IPv6 Translation**
  When an IPv6 host needs to communicate with an IPv4 host, the IP address has to be translated. IPv4/IPv6 translation technology involves address mapping between IPv4 and IPv6, and the methods used to translate protocols.

- **IPv4 Tunneling of IPv6**
  Tunneling enables the interconnection of different IP networks. For instance, separate IPv6 networks can be interconnected through a native IPv4 service by means of a tunnel. IPv6 packets are encapsulated by a border router before transportation across an IPv4 network and decapsulated at the border of the receiving IPv6 network.
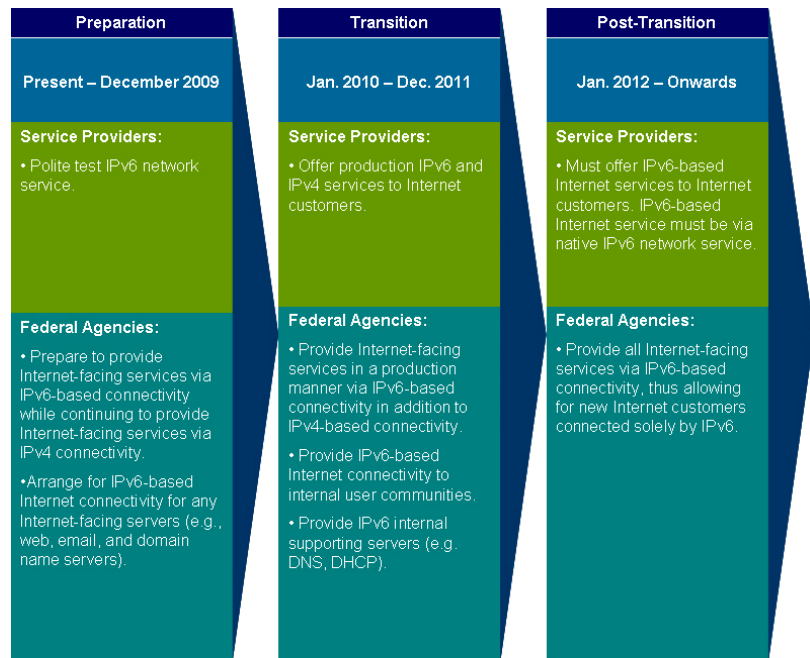
Currently, there are no universal rules in place for the IPv4 to IPv6 transition process so each country must determine how to implement the migration. For instance, IPv6 can be enforced by government guidelines to provide sufficient IP addresses to sustain the economic growth. Another method is the large scale deployment of new IP architecture (such as mobile or home networking) to provide benchmark applications and innovative services.

Worldwide Deployment Status

The United States Office of Management and Budget (OMB) has stated that by June 30, 2008, all network backbones for US federal agencies must adopt IPv6 and be able to interface with this infrastructure.

It should be recognized that by the end of 2011, there will already be new clients and servers on the Internet with IPv6 addresses. Even if the rest of the world hasn't made the full migration to IPv6 by that point, IPv4 computers and devices will still need to access IPv6 servers and provide services to IPv6 customers.

In many cases, public procurement mandates play an important role in encouraging vendors to develop IPv6 solutions, which then speeds up deployment in the private sector. The United States Office of Management and Budget (OMB) has stated that by June 30, 2008, all network backbones for US federal agencies must adopt IPv6 and be able to interface with this infrastructure[2]. According to OMB, agencies should focus on establishing secure, shared IPv6-enabled network services during their regular technology upgrade cycles.

Preparation	Transition	Post-Transition
Present – December 2009	Jan. 2010 – Dec. 2011	Jan. 2012 – Onwards
Service Providers: • Polite test IPv6 network service.	**Service Providers:** • Offer production IPv6 and IPv4 services to Internet customers.	**Service Providers:** • Must offer IPv6-based Internet services to Internet customers. IPv6-based Internet service must be via native IPv6 network service.
Federal Agencies: • Prepare to provide Internet-facing services via IPv6-based connectivity while continuing to provide Internet-facing services via IPv4 connectivity. •Arrange for IPv6-based Internet connectivity for any Internet-facing servers (e.g., web, email, and domain name servers).	**Federal Agencies:** • Provide Internet-facing services in a production manner via IPv6-based connectivity in addition to IPv4-based connectivity. • Provide IPv6-based Internet connectivity to internal user communities. • Provide IPv6 internal supporting servers (e.g. DNS, DHCP).	**Federal Agencies:** • Provide all Internet-facing services via IPv6-based connectivity, thus allowing for new Internet customers connected solely by IPv6.

Chart 3: IPv6 Transition Phases and Timeline in US Federal Agencies

To date, the OMB has not allocated any special funding for federal agencies to implement the transition to IPv6 even though the estimated expenditure by federal agencies was about US$56.5 million in 2007, according to Shawn McCarthy, Director of Research for government vendor programs for IDC's Government Insights. A report by RTI International for the National Institute of Standards and Technology (NIST) released in October 2005 estimates that federal agencies will incur nearly $1.5 billion over the next five years, and $4.6 billion over the coming two decades in the process of transitioning to IPv6[3].

[2] OMB Memorandum for the Chief Information Officers, M-05-22, August 2, 2005

[3] Kaushik Das, "US Government using IPv6", http://www.ipv6.com/articles/general/US_Government_IPv6.htm

In addition, there has already been significant progress by international governments in attempting to take the advantages of early deployment of IPv6. For example:

- The Next Generation Internet Project (CNGI) in **China** is a five-year plan with the objective of taking leadership in Internet and information technology. The core technology of CNGI is IPv6. China showcased CNGI and its IPv6 network infrastructure at the 2008 Olympics in Beijing this summer, networking everything from security cameras and taxis to the professional cameras covering Olympic events using IPv6.

- In **Europe**, the mobile industry is a strong supporter of the transition to IPv6. The European Telecommunications Standards Institute (ETSI) and the IPv6 Forum have established a cooperation agreement. In addition to the agreement with ETSI, the IPv6 Forum has also partnered with UMTS Forum, GSM Association, and the 3GPP Group.

- In the **Asia-Pacific Region**, the Japanese Ministry of Internet Affairs and Communications released the Guideline for e-Government IPv6 Systems in April 2007 to help central ministries and agencies plan for IPv6 adoption and promote IPv6 for e-Government systems. NTT Communications has already launched the world's largest tier one IPv6 backbone—the NTT Communications North American IPv6 Gateway Services. The Korean Ministry of Information and Communication has set targets to convert Internet equipment in public institutions to IPv6 by 2010. The Australian Government Information Management Office (AGIMO) has also released its strategy for a three-stage transition to IPv6 for Australian Government agencies to last from January 2008 to December 2015.

IPv6 Ready Logo Program

The IPv6 forum is a worldwide consortium to provide technical guidance for IPv6 deployment. It launched the IPv6 Ready Logo Program to increase user confidence by certifying products that pass conformance and interoperability testing. A globally recognized program would avoid confusion and facilitate the global migration to IPv6.

The IPv6 Logo Program consists of three phases[4]

- **Phase 1:**

  In this stage, the Logo will indicate that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations. Its objective is to verify minimum IPv6 support. The logo background color is silver. The Phase 1 Logo has been available since September 1, 2003.

- **Phase 2:**

  The Phase 2 Logo expands the "core IPv6 protocols" test coverage to approximately 450 tests and adds new extended test categories. The Logo background color is Gold. The Phase 2 Logo has been available since February 16, 2005.

- **Phase 3:**

  The requirements are the same as Phase 2, except that the extended text category of IPsec will be mandatory.

The approval lists of IPv6 compliant network equipment and devices are available on www.ipv6ready.org.

---

[4] IPv6 Ready Logo Program, http://www.ipv6ready.org/frames.html

The First IPv6-ready Industrial Ethernet Switches

Moxa has recently released the world's first IPv6-ready industrial managed Ethernet switches. The EDS-400/500/700/800 series managed Ethernet switches are certified by the IPv6 Ready Logo Program, making them fully compliant with IPv6 mandatory core protocols and compatible with other IPv6 equipment.

Gradually, both public and private sector companies will migrate to IPv6-compatible switches, routers and operating systems in PCs and servers. However, the few IPv6 compliant routers and switches available in the market today are mainly developed for office use. But industrial environments often involve unknown, hazardous factors that can interfere with the continuous operation of Ethernet devices. In fact, some of these factors may even cause serious disasters or the loss of life and property. As a result, industrial-grade products are highly recommended for building a reliable and ruggedized communication network.

Moxa recently released the world's first IPv6-ready industrial managed Ethernet switches. The EDS-400/500/700 series managed Ethernet switches are certified by the IPv6 Ready Logo Program, making them fully compliant with IPv6 mandatory core protocols and compatible with other IPv6 equipment. By adopting the next-generation internet protocol for industrial Ethernet networks, Moxa's managed Ethernet switches offer automatic IP address configuration and built-in QoS.

Moxa's industrial Ethernet switches have been tested and certified for secure and reliable operation in hazardous locations in accordance with stringent and internationally recognized standards. For example, these industrial Ethernet switches are UL/cUL Class I, Division 2, Group ABCD certified to operate in hazardous locations where flammable gases or vapors may be present. Moreover, DNV approval ensures that Moxa's industrial Ethernet switches are safe for marine environments and guarantee their ability to withstand a wide temperature range, humidity, vibration, EMC and other harmful factors.

In addition, Moxa's IPv6-ready industrial managed Ethernet switches support Turbo Ring technology that provides system administrators a convenient way to set up a stable Ethernet network. If any segment of the network is disconnected, communication will be back online in just few milliseconds.

Robust Ethernet Switches for Mission-Critical Networking

The criteria for network availability in industrial domains are substantially different from those for office environments. For applications where human life or property may be at risk—such as industrial automation and control, risk detection and prevention, or transportation network management—network equipment and devices deployed must be compliant with strict industrial standards and robust enough to withstand harsh environmental conditions.

From the management perspective, the key challenge to operating mission-critical networks is ensuring reliable, secure, and easy-to-maintain communication.

From the management perspective, the key challenge to operating mission-critical networks is ensuring reliable, secure, and easy-to-maintain communication. In order to operate effectively, the deployed networks should support services such as location determination of authorized and unauthorized entities, audio/video transmission, emergency calling and alerts, and remote monitoring and control in a secure and dependable manner.

There are several criteria to consider when system integrators and solution providers select industrial-grade Ethernet switches for mission-critical applications and construct a reliable and robust communication network.

- **Network Redundancy**
  "Redundancy" is one of the most important aspects of industrial automation networks used for applications such as power utilities, transportation, and surveillance. A basic redundancy requirement for control systems is that each part of the communication network should be equipped with a backup power supply for smooth operation even during a power outage. In addition to power redundancy, media

redundancy is also a basic requirement for industrial applications. With this function, the communication network can form a backup path when part of the network fails.

- **Safety and Reliability**
  System integrators and developers for mission-critical applications tend to look at either the MTBF (mean time before failure) or warranty period of a product to evaluate reliability. However, since the MTBF for general purpose products is not readily available, it is more common to use the warranty period as the barometer. Whereas general purpose devices tend to be warranted for only 1 or 2 years, the warranty period for products used in industrial applications should be at least 3 to 5 years to ensure system reliability and reduce the probability that devices will need to be changed frequently.

- **Ruggedness**
  Industrial Ethernet components are designed to operate in harsh environments and withstand extreme conditions. The specifications of industrial Ethernet switches (wide operating temperature, immunity to electromagnetic interference, anti-shock, anti-vibration, etc.) often exceed those of the connected devices (PLCs, HMIs, etc.) and can be much stronger compared to those of office-grade equipment.

- **Installation Flexibility**
  A rugged and user-friendly DIN-Rail mounting or panel mounting option is proven to better withstand strong industrial vibration, freefall, and shock than most commercial devices for industrial applications. These easy and secure installation options greatly ensure network stability.

- **Wide Operating Temperature**

  For some industrial applications, especially applications located in factories or outdoors, network devices must be able to operate under extreme temperatures from -40 to 85°C. For these types of applications, it is critical to look for products with optimal heat dissipation or fan-free solutions.

Summary

With a large number of appliances already functionally IPv6 network-ready, the transition to IPv6 is inevitable. Fortunately, IPv6 offers new features, advantages, and services for the Internet community. Even organizations and enterprises that have enough IPv4 address space and continue to operate their IPv4 networks will need to implement IPv6 on their networks eventually. Any organization that runs its business, manages its facilities, and communicates via Internet will need to take steps to ensure that those services are visible over both IPv4 and IPv6 networks. Over time, they too will migrate to IPv6-compatible switches, routers, and operating systems in computers and servers.

Moxa's IPv6-ready industrial Ethernet switches adopt a dual stack transition structure that supports both IPv4 and IPv6 simultaneously, so users don't need to worry about upgrading their networking infrastructure in the coming years. By automatically allocating IP addresses, Moxa's IPv6-ready industrial Ethernet switches ensure secure and reliable communication over industrial networks to safeguard your mission-critical applications.