TEC
TELECOMMUNICATION ENGINEERING CENTRE

NEWSLETTER
टी ई सी संचारिका

VOL 10 AUGUST 2006 ISSUE 3

IPv6

IN THIS ISSUE

IPv6

What is IPv6?

IPv6 (Internet Protocol Version 6) is a new version of IP protocol designed by the IETF. In 1990, IETF started work on a new version of IP, one which would never run out of addresses, would solve a variety of other problems, and be more flexible and efficient as well. Its major goals were

- Supports billions of hosts, even with inefficient address space allocation.
- Reduce the size of the routing tables.
- Simplify the protocol, to allow routers to process packets faster
- Provide better security (authentication and privacy) than current IP
- Pay more attention to type of service, particularly for real time
- Aid multicasting by allowing scopes to be specified
- Make it possible for host to roam without changing its address
- Allow the protocol to evolve in the future
- Permit the old and new protocols to coexist for years

The main feature of IPv6 is the larger address space, which is 128 bits long. The larger address space avoids the potential exhaustion of the address spaceas in IPv4. 128 bits might seem an overkill to achieve that goal. However, since addresses are plentiful, it is reasonable to allocate addresses in large blocks, which makes administration easier and avoids fragmentation of the address space, which in turn leads to smaller routing tables. A technical reason for selecting 128-bit address is that since most future network products will be based on 64 bit processors, it is more efficient to manipulate 128-bit addresses. Another advantage of the larger address space is that it makes scanning certain IP blocks for vulnerabilities significantly more difficult than in IPv4, which makes more resistant to malicious traffic. The drawback of the large address size is that it is less efficient in bandwidth usage, and this may hurt regions where bandwidth is limited.

Why IPv6?

Currently IPv4 serves what could be called the computer market. The computer market has been the driver of the growth of the Internet and growing at an exponential rate. Peer-to-Peer communications, file exchange applications etc. can not work across NAT (Network Address Translation) and requires direct routable IP addresses which IPv6 has plenty of.

Home networking is one of the emerging applications which will require unique identification of all home gadgets like lighting equipment, heating and cooling equipment, motors, and other types of equipment. These gadgets can be controlled from any place in the world using IPv6 unique address.

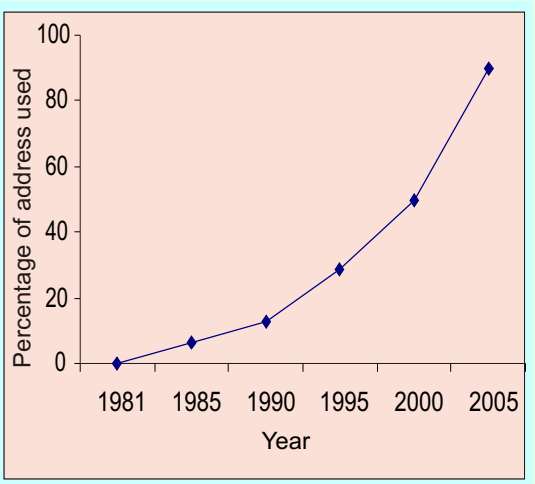
There are a number of reasons why IPv6 is appropriate for the next generation of the Internet Protocol. It solves the Internet scaling problem, provides a flexible transition mechanism for the current Internet, and was designed to meet the needs of new markets such as nomadic/mobile personal devices, networked entertainment, and device control. It does this in a evolutionary way which reduces the risk of architectural problems.

Ease of transition is a key point in the design of IPv6. IPv6 is designed to interoperate with IPv4. Specific mechanisms (embedded IPv4 addresses, pseudo- checksum rules etc.) were built into IPv6 to support transition and compatibility with IPv4. It was designed to permit a gradual and piecemeal deployment with a minimum of dependencies.

(contd… on page 4)

IPv4 Address Allocation History

- 1981 - Ipv4 Published
- 1985 - 1/16 of total space
- 1990 - 1/8 of total space
- 1995 - 1/3 of total space
- 2000 - 1/2 of total space
- 2003 - 2/3 of total space
- This despite increasingly intense conservation efforts
  PPP/DHCP address sharing
  NAT (Network Address Translation)
  CIDR (Classless Inter Domain Routing)
- Theoretical limit of 32 bit space : 4 billion devices
  Practical limit of 32-bit space : 250 million devices
  (RFC 3194)



Source : Internet

Changes from IPv4 to IPv6

- **Expanded Routing and Addressing Capabilities :** IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy.
- The scalability of multicast routing is improved by adding a "scope" field to multicast addresses.
- A new type of address called a "anycast address" is defined, to identify sets of nodes where Packets sent to an anycast address or list of addresses are delivered to the nearest interface identified by that address. Anycast is a communication between a single sender and a list of addresses.
- **Header Format Simplification :** Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to keep the bandwidth cost of the IPv6 header as low as possible despite the increased size of the addresses. Even though the IPv6 addresses are four time longer than the IPv4 addresses, the IPv6 header is only twice the size of the IPv4 header.
- **Improved Support for Options :** Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
- **Quality-of-Service Capabilities :** A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real- time" service.
- **Authentication and Privacy Capabilities:** IPv6 includes the definition of extensions which provide support for authentication, data integrity, and confidentiality. This is included as a basic element of IPv6 and will be included in all implementations.

IPv6 supports large hierarchical addresses which will allow the Internet to continue to grow and provide new routing capabilities not built into IPv4. It has anycast addresses which can be used for policy route selection and has scoped multicast addresses which provide improved scalability over IPv4 multicast. It also has address mechanisms which provide the ability for "plug and play" installation.

The address structure of IPv6 was also designed to support carrying the addresses of other internet protocol suites. Space was allocated in the addressing plan for IPX (Internetwork Packet Exchange) and NSAP (Network Service Access Point) addresses. This was done to facilitate migration of these internet protocols to IPv6. IPv6 provides a platform for new Internet functionality. This includes support for real-time flows, provider selection, host mobility, end-to- end security, auto-configuration, and auto-reconfiguration.

Migration to IPv6

Migration to IPv6 by a Service Provider is not a single step exercise. However, for a user it may be single step process. Some aspects about migration to IPv6 are as below:

- Migration to IPv6 involves cost.
- Both IPv4 and IPv6 networks will coexist during the period of migration.
- The migration from IPv4 to IPv6 shall have to be implemented in phases.
- Migration to IPv6 over a span of time shall be more expensive than implementing the migration as part of a normal life cycle update.
- Hardware and software suppliers are developing IPv6 enabled products and some of the IPv6 enabled products are available.
- Government has taken initiative for introduction and migration towards IPv6.

Migration Techniques and the issues

A country's infrastructure employing the IP technology equipments usually involves networks of Service Providers, R & D organisations, academic and other Institutions, e-governance Networks owned and operated by various state Governments and other networks owned and operated by various Government departments.

A migration strategy involves the transition of all these networks. It is important to note that IPv6 deployment requires it to coexist with IPv4 for considerable period of time. Different options are available for managing this complex and prolonged transition from IPv4 to IPv6.

The transition is not only related to the ISP's network but it requires migration strategies for other Service Providers also. There are numerous components in other service providers (GPRS, CDMA2000 1.x) which use IPv4 protocol and shall require to be migrated on IPv6.

Transition requirements

The transition strategy involves the requirement of upgrading the various components of the infrastructure. The components of the infrastructure, which are required to be migrated are as follows:

- Networks and Protocols
- Applications
- Customer Access Equipment

The transition strategy for various components to be migrated is required to be tested first in the test bed. The various options need to be tested for operational ease and efficiency in a Service Provider's environment before implementing it in the operational networks so that there is minimum disruption in the commercial services being provided by Service Provider. This prior testing could also enable

the Service Providers to optimise the cost of migration.

Transition mechanisms for the Network and Protocols

The network infrastructure consists of many devices like routers, switches, RAS (Remote Access Server)/other access gateways, DNS (Domain Name Server), IXPs (Internet Exchange Points), etc. running various protocols. It is the most complex part of migration both technically and cost wise. Such migration can not be achieved in one go. There will be many phases in between the present IPv4 only and final IPv6 only networks.

Transition requirements have been included in IETF RFC 1752 and consist of the following:

- Incremental upgrade
- Incremental deployment
- Easy addressing i.e. existing addressing should continue.
- Low start-up costs

IETF further defines two basic mechanisms in IETF RFC 2893 for total compatibility between IPv4 and IPv6 routers/ hosts as:

- Tunnelling
- Dual stacking

Tunnelling

Tunnels allow transmission of packets through IPv6 ignorant Routers and Switches by encapsulating IPv6 packets inside of IPv4 packets or MPLS frames.

Dual Stack

Dual Stack is a dual IP layer approach where only IP layer is duplicated and not the whole stack. The dual stack nodes have both IPv4 and IPv6 addresses and corresponding routing tables. Applications can talk to both the stacks; choice of the IP version is based on name lookup and application preference. It is logically equivalent of two different networks.

Protocols

Many Protocols running in various components are also required to be upgraded so that complete migration can be achieved. For example the network component running routing protocol like OSPFv2 and BGPv4 required to be updated to OSPFv3 and BGPv4+. Similarly many other protocols are required to be updated. Many of them have been already standardised and tested but few other are required to be standardised and tested.

Applications

In general the IPv4 applications need modification when ported to IPv6 because the TCP/IP Network architecture was not properly layered. Applications can use domain address or IP address to identify Hosts or Routers. Many applications perform a proper independence of layers and use domain names above socket interface. But the application where no such layer independence has been implemented and which uses IP addresses as parameters are required to be upgraded.

There are various applications being used by the Service Providers like Billing, AAA, LDAP, NMS/OSS, firewall and other security components, subscriber service selection gateways, etc. These applications may require a upgrade to support IPv6. Application transition may require an upgrade of the Operating System also though rigorous testing shall be required for the new versions. The IETF RFC 4038 - Application Aspects of IPv6 Transition deals with the transition requirements.

Customer Equipment

CPE (Customer Premise Equipment) for xDSL and other access, set top box, PC, etc. are to be modified for hardware and software. Though technically it is possible but the cost involvement and customers desire to switch over to IPv6 shall be major area of concern.

IMPORTANT ACTIVITIES OF TEC DURING APRIL 2006 TO JULY 2006

Preparation of GRs/IRs

Following GRs/IRs and Technical documents were issued:

- Mediation Equipment and CDMA 2000 network Sub system for Lawful Interception
- Composite Optical Test Instrument (Power Meter & Light Source)
- Location based Services / System (LBSS) for CDMA 2000 network
- Drive Test Tool for CDMA 2000 Network
- Post Processing Tool for CDMA 2000 Network

Revised GRs/IRs

- Tools For Installation & Operating the OFC & For Assembly of the Optical Fibre Splice Closures
- Uninterrupted Power Supply (UPS)
- Optical Fibre Splice Protection Sleeves
- Billing and Customer Care System for Cellular Mobile System
- Buttinski Telephone Handset
- Cell Broadcast Service

Tests and Field trials

- Firewal System of BSNL GSM (East Zone)
- Billing & Customer care System (B&CCS) of BSNL and MTNL
- LBIS (Location Based Information System) of Phase IV of BSNL GSM (South Zone)
- Line Interception Equipment of ILD Gateway, TCIL

Other Activities

- **Manufacturer Forum conducted for**

- GSM Base Station Panel & Omni Antennas for 890-960 MHz and 1710-1880 MHz
- Personalized Ring Back Tone (PRBT) System For PSTN
- Telephone Revenue Billing and Accounting

- A meeting of TEC FG-NGN (TEC Focus Group on NGN) was held on 13-07-2006, in which representatives of DoT, BSNL, MTNL and CDOT participated.
- A meeting was held on 14-07-2006 with Service Providers to discuss the DCC procedures involving Licensed Private Service Providers, for preparation of Telecom Standards.

Approvals issued by TEC during the period April 2006 to July 2006

Interface Approvals	39
Service Test Certificate	111
Total	150

Approvals issued by TEC upto 31.07.2006

Type Approvals	7018
Interface Approvals	4301
Service Test Certificates	1988
Grand Total	**13307**

टी ई सी संचारिका
अगस्त 2006
भाग 10
अंक 3

दूरसंचार इंजीनियरी केन्द्र
खुर्शीदलाल भवन
जनपथ
नई दिल्ली-110001

Editor : I. S. Sastry, DDG (S) Phone : 23329540 Fax : 23723387 Email : ddgsw@bol.net.in

CSN 37

Prabhat Publicity, New Delhi