Department of Telecommunications,
Ministry of Communications and IT,
Government of India

India IPv6 Task Force Newsletter

September 2012
Issue 7

INSIDE THIS ISSUE

IPv6 Day: Switch to V6

(Left to Right) Shri R M Aggarwal DDG(NT), DOT HQ , Shri Lalit S Chowdhary System Engineering Director at Cisco Systems, Dr. Govind, Sr. Director, DeitY , Sh.Rajesh Chharia President at Internet Service Providers Association of India (ISPAI)

The Department of Telecommunication and Cisco jointly hosted the Switch to V6 conference on 7th August 2012, at the Cisco Campus, Cessna Business Park in Bangalore. After the recent launch of IPv6, the next big question for organizations was preparing for the successful transition to IPv6 while keeping the existing IPv4 investments intact.

The IPv6 conference was held with the primary objective of establishing a forum for organizations to learn as to how they can support future business continuity, growth, and global expansion through the IPv6 transition. Switching to V6 ‘Effortlessly Efficiently and Effectively’ was the theme for the day, and event was a huge success with participation of top dignitaries from government and private enterprise organizations.

The conference threw light on the role that IPv6 can play while providing unlimited address space and allow organizations to deliver large number of newer applications and services along with reliability, improved user experiences and increased security. It also spoke about how technology is changing the way we interact as global citizens and how we govern

Centre of Innovation Activities

3rd meeting of the committee on Centre of Innovation was held in Sanchar Bhawan on 30th August 2012 for firming up the model, structure, scope of work and details.
Meeting Highlights:

- TCOE , C-DOT , TEC have proposed their model options on Centre of Innovation.
- It was felt that Innovation Centre under a Government Organisation set up may not in bring in desired results. It could be implemented through an autonomous body having 'society' type Model in which rules of Scientific Organization could be applicable. Three layer structure was considered desirable.
- The Centre should have long term vision and take into consideration security aspects and should focus on innovations as a long term measure.
- It was suggested that framing of DPR should be initiated on the models that are close to above methodology

Building IPv6 Talent Pool

With IPv4 address having depleted in APNIC, moving to IPv6 is business critical for India. A critical aspect towards ensuring this seamless migration is to build skillsets to implement and manage the IPv6 networks. Building IPv6 skillsets is the first step for IPv6 transition, it is required not only to maintain business continuity but also to ensure a smooth transition to IPv6.

Trained human resource availability has been identified as a critical gap towards adoption of IPv6.It is well recognized that trained manpower on IPv6 will be a major contributor towards accelerating IPv6 rollout. It is important that the adoption of IPv6 be carefully planned, so that the technical impact and performance impact on the network are minimized and the transition happens in a seamless manner. With limited trained resources availability in the country, organizations are faced with the challenges of talent scarcity on IPv6.This in turn is not only contributing towards the delay in their adoption plans but is also a serious roadblock towards planning a seamless migration strategy towards ensuring minimal business impact.

"Building IPv6 skill set Is the first transition tool for IPv6 adoption "

DOT having mandated the organizations to build IPv6 service capability and IPv6 being identified as a major technology thrust area in the National Telecom Policy 2012 ,it is imperative for organizations to begin IPv6 adoption ,which would require trained manpower resources as the first step.

However currently there is no structured or standardized training program being offered in the country. A very small percentage of IPv6 talent pool comprises of self-trained personnel with basic theoretical understanding on IPv6.No expert level deep dive training with practical hands on is presently available in the country.

It is with this intent that DOT proposes to facilitate building up a talent pool on IPv6 in the country. DoT has formed a committee for development of standardized IPv6 Training Certified Courses in India. The training and certification will be target 3 level of the resource pool

1. Basic level
2. Professional Level
3. Expert Level

Committee is currently evaluating multiple options to meet India IPv6 training requirements.

Recent meetings and outcomes

Department of Telecommunications has held several meetings with key stakeholders across the IT eco-system for IPv6 adoption covering Service providers, Content providers, Government sector. The key highlights of the various meeting are as below:

"IPv6 security, test certification and education been identified as key focus area"

Name of the meeting	Key highlights
IPv6 Standing Committee Meeting	• Major Service providers are ready and to get the actual and effective migration to IPv6, Content & Application Providers are also progressing in the migration process. • NIC is evaluating IPv6 security aspects. Once the evaluation gets completed, all websites would be migrated and NIC plans to complete this in three months • TEC test bed is ready for the test as per the procedure of given RFC. TEC is working for IPv6 ready logo certification recognition • ERNET is working for the Test Bed under DIT • Registrar and Data Center Level workshops should be organized with facility of Remote Participation • TEC certification would facilitate achieving uniformity among the End User Equipments and develop related ecosystem • Common approach for IPv6 in Educational Institute
Meeting with Applications Service Providers and content providers	• Major Service providers such as MTNL, Airtel, Aircel have informed that their network is not yet ready for retail, BB and mobile because of delays in IPv6 ready equipment especially due to handset and GGSN/SGSN equipments. • All major service providers shared the concerns around enterprise customers for more IPv4 addresses demand. • BSNL is testing DSLAM and IPv6 compliant CPEs and commercial launch will be intimated in due course • CGN solution requires careful planning and TCO analysis

"Mobile packet core and handset equipment ipv6 readiness is next focus for IPv6 adoption in retail broadband networks"

Name of the meeting	Key highlights
Meeting with Contents Providers and Application Providers	• Google India said that on world IPv6 Launch day on 6th June 2012, no major problem was reported. Already major websites like Google, Yahoo, Facebook etc have migrated to dual stack. There are several tools with regard to IPv6 on the Ipv6 Google website. • Axis Bank said that the bank is yet to start IPv6 activity and it need to consult the Service Providers. Also the bank is yet to receive directive from RBI
Meeting with Equipment Vendor	• NSN India said that User and Radio equipment are IPv6 ready , Control and Transport equipment are progressing towards IPv6 readiness • Qualcomm India said that all designs are IPv6 ready and all majors OEM are their customer • Huawei India said that Network equipments including GGSN are required to be upgraded with software. New equipment will be ready by 2015 • Ericssion India, said that as far as end to end IPv6 services are concerned,the equipments including GGSN and Radio related equipments are IPv6 ready
Oversight Committee Meeting	• 6 out of 22 major service providers are fully ready and remaining are going to be ready in the next one or two quarters. • Main issues highlighted by States are shortage of trained technical resources. • Government organizations should incorporate the provision of funds for IPv6 implementation in their IT projects. • TEC Test Bed is ready, C-DOT's GPON and other IP equipments are expected to be tested in the coming month, Ready Logo accreditation is in process, Draft handset standards with IPv6 compliance requirement have been circulated. • All Government static websites will be on dual stack by October, 2012 and others including non static etc will be on dual stack by December, 2012 followed by IPv6 forum WWW certification accreditation. Security aspects are under assessment. • BSNL conducted 22 awareness workshops and three more are planned soon. • C-DOT is capable to handle the IPv6 LIMS and ISP's should have their existing LIMS infrastructure ready. • Centre of Innovation (COI) has been discussed and finalized by the committee and model and structure are under discussion. Participation from industry on various possible models and options for COI is encouraging. • Certified training modules are needed and this needs to be expedited.

IPv6 Security Best Practices

Rajat Arora , IPv6 Evangelist, SIXMATRIX GLOBAL SERVICES PVT.LTD.

Just like the early deployment of many technologies, security is often left to the final stages of implementation. Intent is to improve the security of early IPv6 deployments from day one. Organizations should begin now to build strategies for secure IPv6 transition.

When the IETF developed IPv4, the global expansion of the Internet and the current Internet security issues were not anticipated. In the 1980s, when IPv4 was developing, the "Internet" was constructed by a set of cooperative organizations and network security was only given minor consideration. As IPv4 was developed and the Internet explosion took place in the 1990s, Internet threats became prolific. If the current environment of Internet threats could have been predicted when IPv4 was being developed, the protocol would have had more security measures incorporated into its design. As IPv6 becomes more popular, it will continue to grow as a target of attacks, just as Microsoft software became more popular it became a larger target. Internet Explorer is a dominant web browser and experiences many attacks. As the Firefox web browser increased in popularity, so did the number of people working to find flaws in it. IPv6 will follow the same course as the number of deployments increases and it becomes a focus of new security research. The process of finding and correcting vulnerabilities will only make IPv6 stronger. The attacker community is gaining interest in ipv6 as it is an easy route for them with lack of IPv6 expertise in organizations. It is important for organizations to improve the security of early IPv6 deployments from day one.

"IPv6 makes some things better and most things are just different, but no more or less secure than IPv4"

The transition to IPv6 is inevitable, and therefore originations should understand the threats that exist in IPv6 networks and protect against them. Organizations will most likely face below security challenges throughout the deployment process, including:

- An attacker community that most likely has more experience and comfort with IPv6 than an organization in the early stages of deployment.
- Difficulty in detecting unknown or unauthorized IPv6 assets on existing IPv4 production networks.
- Added complexity while operating IPv4 and IPv6 in parallel.
- Lack of IPv6 maturity in security products when compared to IPv4 capabilities.
- Proliferation of transition-driven IPv6 (or IPv4) tunnels, which complicate defenses at network boundaries
- If organizations elect to deploy IPv6 without security, it is like running a backdoor protocol to the dual-stack systems that could potentially be exploited

Security vulnerabilities that exist for IPv4 also generally apply to IPv6 however there are additional vulnerabilities that exist for IPv6 but do not apply to IPv4. These fall in three major categories:

1. **IPv6 Basic Protocol Vulnerabilities** :
    - Reconnaissance and scanning worms: Brute-force discovery is more difficult.
    - Attacks against ICMPv6: ICMPv6 is a required component of IPv6.
    - Extension Header (EH) attacks: EHs need to be accurately parsed.
    - Autoconfiguration: NDP attacks are simple to perform.
    - Mobile IPv6 attacks: Devices that roam are susceptible to vulnerabilities.

2. **IPv6 Transition Mechanism Protocols Vulnerabilities** :
    - Attacks on transition mechanisms: Migration techniques are required by IPv6 for transition mechanisms like Dual-stack , Tunneling , NAT.

3. **IPv6 Operational Vulnerabilities**:
    - Operation vulnerabilities: Complex ipv6 filtering, Padding option, new extension header introduction.

In order to achieve security parity with IPv4 networks, the emerging IPv6 networks should be protected against all attacks for which IPv4 networks are currently protected; and should additionally be protected against new attacks that are specific to new features of IPv6 such as the Neighbor Discovery, Auto Configuration, ICMPv6 etc. Below are few best practices for reference:

"Organizations should have secure IPv6 deployment from day-1 and build IPv6 security policy"

- Encourage staff to increase their knowledge of IPv6 to a level comparable with their current understanding of IPv4
- Plan a phased IPv6 deployment utilizing appropriate transition mechanisms to support business needs; don't deploy more transition mechanisms than necessary
- Plan for a long transition period with dual IPv4/IPv6 co-existence
- Apply an appropriate mix of different types of IPv6 addressing (privacy addressing, unique local addressing, sparse allocation, etc) to limit access
- Use automated address management tools to avoid manual entry of IPv6 addresses, which is prone to error because of their length.
- Be aware of the way that attackers perform reconnaissance and use random node identifiers for servers and client computers.
- Use IPsec (Internet Protocol Security) to authenticate and provide confidentiality to assets that can be tied to a scalable trust model
- Ensure that IPv6 routers, packet filters, firewalls, and tunnel endpoints enforce multicast scope boundaries
- Use modern operating systems that are patched against vulnerabilities.
- Be cognizant of extension header threats and filter extension headers appropriately.
- Drop packets containing Routing Header Type 0 and unknown option headers
- Perform Unicast RPF filtering to prevent spoofed source addresses.
- Develop a granular ICMPv6 (Internet Control Protocol for IPv6) filtering policy
- Restrict who can send messages to multicast group addresses.
- Filter IPv6 bogon addresses at the perimeter.
- Filter IPv4 Protocol 41 and UDP 3544 at your perimeter if tunneling required.
- Include protection against RA, ND, and DHCP attacks
- Identify capabilities and weaknesses of network protection devices in an IPv6 environment
- Use authenticated DHCPv6 if applicable. Look toward using SEND to secure the LAN.
- Use Control Plane Policing for granular control over the router's processes.
- Use QoS policy to control misbehaving IPv6 applications and ICMPv6 flooding.
- Review neighbor cache for unauthorized systems.
- Leverage the OS's embedded IPv6-capable stateful firewall.
- Secure deployment of tunneling

This newsletter is being issued by 'Networks and Technologies' (NT) cell DoT, in coordination with "National IPv6 Task Force Work Group-9 Co-Lead SIXMATRIX"

For feedback and suggestions, please contact:

1. Shri N Ram,
   Director (NT)
   Department of Telecommunications,
   Government of India,
   M: +91 9868811933, Ph: +91 11 23372533,
   E-Mail: dirnt-dot@nic.in

2. Shri R.M.Agarwal
   Deputy Director General (NT)
   Department of Telecommunications,
   Government of India,
   M: +91-9868133440,Ph:+91-11-23372606
   E-mail: ddgnt-dot@nic.in, DOT Website: www.dot-gov.in