CYBERNET

World IPv6 Day Experience

By
Aftab A. Siddiqui
Cyber Internet Services (Pvt.) Ltd
IPv6 Task Force Pakistan

Introduction

- IPv6 is the new version of the Internet Layer Protocol (IP) in the TCP/IP suite.
- BUT, its not new….
- RFC 2460 (IPv6) was released in December 1998.
- It has been more than a decade now.

- So, NO MORE EXCUSES…..

IPv6 Adoption Strategy

- Cybernet Enabled IPv6 in 2008 for testing after SANOG VIII in Pakistan.
  - So we have to be ready by all means.

- Not everything needs to be IPv6 ready on day 1
  - World IPv6 Day, June 8, 2011

Objective

- IPv6 Research
- Perform an IPv6 Readiness Assessment
- Define IPv6 Objectives (can't do everything)
- Develop a Project Plan
- Develop a detailed IPv6 Architecture & Design
- Development, testing and pilot mode
- Implement in production

Critical Points

- Team Readiness:
  - Training [ ]
- Equipment Readiness [ ]
- Develop an IPv6 security policy [ ]
- IPv6 Transit [ ]
- IPv6 inside Corporate & DMZ [ ]
- IPv6 on web server [ ]
- IPv6 for IT Operations [ ]

Architecture & Design

- Need to define architecture guidelines & security policies for developing & implementing our IPv6 solution
- Address the results from our “Readiness Assessment” report
  - Some of our load balancers do not support IPv6
  - One of our Internet transits do not support IPv6
  - Need to test our custom/in house application for IPv6 compliance

Architecture Guidelines

- **Keep IPv4 as-is**
- **Dual Stack**
  - All systems participating in the IPv6 implementation must support a concurrent IPv4 and IPv6 stack
- **No IPv6 Tunnelling**
  - Usage of IPv6 tunnelling mechanisms such as ISATAP, Teredo, 6to4, 6rd are not permitted
- **Native IPv6 Transit**
  - IPv6 transit must support IPv6 natively without the use of tunnelling (avoid MTU problems)

Architecture Guidelines

- **One host, one IP**
  - All IPv6 hosts/interface will use one Global address
  - Unique Local Addresses (ULA) must not be used
- **No Network Address Translation (NAT)**
  - NAT66, NAT64 & NAT46 technologies not permitted
- **IPv6 Address Assignment – Privacy**
  - Internet accessible Global Addresses must not use EUI-64 (MAC + FFFE)
  - The interface identifier (64 bit) part must be randomly/manually generated (Manual, RFC-3041)

Architecture Guidelines

- **Question: IP Addressing Plan**
  - Based on most efficient algorithm (RFC 3531)
  - Leftmost bits (48, 49, 50,...) are assigned to segment the site
  - The rightmost bits (63, 62, 61, 60 ...) are assigned to number the links.
- **Question: IPv6 Address Allocation**
  - DHCPv6 will be used where possible
  - SLAAC enable for non DHCPv6 devices (Mac) with privacy
- **Question: IPv6 Address Lifecycle (Life/Timeout)**
  - Need to assess impact on logging, correlation, & applications of having temporary IP addresses (Windows 7)

Misc. Guidelines

- **DNS Address Mapping**
  - All static IPv6 address entry must have AAAA and PTR reverse mapping records
  - Naming convention required (interface level)
- **Routing**
  - Native IPv6 Peering, BGP
  - Native IPv6 Routing, IS-IS/OSPFv3
  - IS-IS/OSPFv3 & BGP secure routing adjacencies using filtering and passwords.
- **NetFlow data collection**
  - Use NetFlow 9 for IPv6 flow exports

Security Guidelines

- **Firewall**
  - Change & configuration management processes
  - “No NAT, check permit ANY/ANY, wide open Internet”
- **Network Perimeter**
  - IPv6 enabled firewalls
  - IPv6 deep packet inspection IDS/IPS
- **Desktop, Hosts & Device Hardening**
  - IPv6 host enabled firewalls
  - IPv6 HIPS (host based IPS)
- **Security Management**
  - SIEM alerts, regular review of logs for all IPv6 enabled devices.
  - Log & monitor all IPv6 traffic Corporate & DMZ

Security Policy

- **Default deny ANY/ANY of IPv6** addresses and services on perimeter devices such as firewalls, VPN appliances and routers.
  - Log all denied traffic
- **Block** 6to4, ISATAP (rfc5214) and TEREDO (rfc4380) and other **IPv6 to IPv4 tunneling protocols** on perimeter firewalls, routers and VPN devices as this can bypass security controls.
  - Block TEREDO server UDP port 3544
  - Ingress and egress filtering of IPv4 protocol 41, ISATAP and TEREDO use this IPv4 protocol field
- Filter internal-use IPv6 addresses at border routers and firewalls to prevent the all nodes multicast address (FF01:0:0:0:0:0:0:1, FF02:0:0:0:0:0:0:1) from being exposed to the Internet.
- Filter unneeded IPv6 services at the firewall just like IPv4.
- Filtering inbound and outbound RH0 & RH2 headers on perimeter firewalls routers and VPN appliances.

Security Policy

- **ICMPv6 messages to allow RFC4890.**
  - Echo request (Type 128) Echo Reply (Type 129)
  - Multicast Listener Messages to allow
    - Listener Query (Type 130) Listener Report (Type 131)
    - Listener Done (Type 132) Listener Report v2 (Type 143)
    - Destination Unreachable (Type 1) – All codes
    - Packet Too Big (Type 2 message)
    - Time Exceeded (Type 3) – Code 0 only
    - Parameter Problem (Type 4 message)
  - SEND Certificate Path Notification messages:
    - Certificate Path Solicitation (Type 148)
    - Certificate Path Advertisement (Type 149)
  - Multicast Router Discovery messages:
    - Multicast Router Advertisement (Type 151)
    - Multicast Router Solicitation (Type 152)
    - Multicast Router Termination (Type 153)

Security Policy

- **Deny** IPv6 **fragments** destined to an internetworking device.
- Drop all fragments **with less than 1280 octets** (except on the last one)
- Filter ingress packets with IPv6 multicast **(FF05::2 all routers, FF05::1:3 all DHCP)** as the destination address.
- Filter ingress packets with IPv6 multicast **(FF00::/8)** as the source.
- Use IPv6 hop limits to protect network devices to drop hop count greater than 255.
- Configure "**no ipv6 source-route**" and "**no ipv6 unreachable**" on external facing perimeter devices.
- Drop all **Bogon** addresses on perimeter firewalls, routers and VPN appliances.

Security Policy

- **The following addresses should be blocked as they should not appear on the Internet, based on rfc5156**
  - Unspecified address: ::
  - Loopback address: ::1
  - IPv4-compatible addresses: ::/96
  - IPv4-mapped addresses: ::FFFF:0.0.0.0/96 ::/8
  - Automatically tunneled packets using compatible addresses : ::0.0.0.0/96
  - Other compatible addresses:
    - 2002:E000::/20 2002:7F00::/24 2002:0000::/24
    - 2002:FF00::/24 2002:0A00::/24 2002:AC10::/28 2002:C0A8::/32
  - Deny false 6to4 packets:
    - 2002:E000::/20 2002:7F00::/24 2002:0000::/24
    - 2002:FF00::/24 2002:0A00::/24 2002:AC10:;/28 2002:C0A8::/32
  - Deny link-local addresses: FE80::/10
  - Deny site-local addresses: FEC0::/10
  - Deny unique-local packets: FC00::/10
  - Deny multicast packets (only as a source address): FF00::/8
  - Deny documentation address: 2001:DB8::/32
  - Deny 6Bone addresses: 3FFE::/16

June 8th World IPv6 Day

www.cyber.net.pk

Some Statistics: Google Analytics

- **Number of hits as per the protocol.**

	Protocol Status	Hits
1.	ipv4:yes	805
2.	dual:yes	804
3.	v6lit:yes	164
4.	ipv6:yes	126

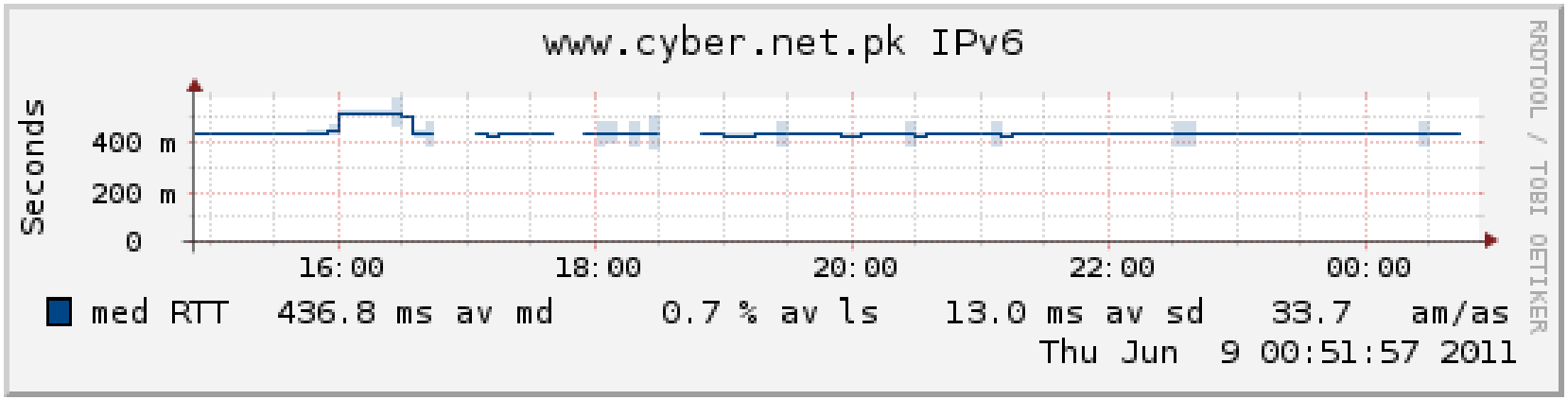
Some Statistics: Google Analytics

- **List of countries from where www.cyber.net.pk was accessed.**

	Country	Hits	Page/visit	Time on Site	% new visit
1.	Pakistan	3,161	1.28	00:01:06	51.66%
2.	United States	83	1.06	00:00:10	61.45%
3.	UNKNOWN	68	1.16	00:00:10	67.65%
4.	United Arab Emirates	57	1.16	00:00:49	68.42%
5.	China	45	1.33	00:00:45	48.89%
6.	United Kingdom	41	1.17	00:00:11	80.49%
7.	Canada	23	1.39	00:00:40	47.83%
8.	Netherlands	20	1.00	00:00:01	45.00%
9.	Spain	14	1.64	00:00:18	85.71%
10.	Saudi Arabia	13	1.08	00:01:03	53.85%

Some Statistics: Google Analytics

- Latency from ISOC Portal.
  - That was the biggest concern for us.



Test Running

- **Developing an IPv6 lab**
  - Test applications
    - Web, application logging
  - Test load balancers, routers, firewall
  - Log analysis
  - Security – IDS/IPS
  - Packet capture
  - Network connectivity, routing protocols
  - ICMPv6

Critical Points – Review

- Team Readiness:
  - Training [√] ongoing… ?
- Equipment Readiness [√]
- Develop an IPv6 security policy [√] – BAD
- IPv6 Transit [√] – Finally
- IPv6 inside Corporate & DMZ [√] – somehow
- IPv6 on web server [√] – partially
- IPv6 for IT Operations [√] – partially

IPv6 delegations in Pakistan

- As of 8th June 2011, there were 57 APNIC members in Pakistan.
- Every member is entitled to get an IPv6 allocation of /32.
- BUT Unfortunately…..
- According to APNIC routing database out of 58 only 24 Members have got their IPv6 address space.

IPv6 delegations in Pakistan

Member Name	Category	IPv6 Address Space
AMZ Technologies (Private) Limited	SMALL	2401:a200::/32
Connect Communication	MEDIUM	2401:ea00::/32
Cyber Internet Services Pakistan	MEDIUM	2001:4538::/32
Delta Networks	SMALL	2402:7c00::/32
Gerrys Information Technology (PVT) Ltd	MEDIUM	2406:ac00::/32
HEC	SMALL	2400:fc00::/32
IMZAK UK Limited	SMALL	2401:9e00::/32
Linkdotnet Telecom Limited	LARGE	2401::/32, 2404:148::/32
Micronet Broadband (Pvt) Ltd.	MEDIUM	2407:d000::/32
Multinet Broadband	MEDIUM	2401:8e00::/32
National Institutional Facilitation Technologies.	VERY SMALL	2001:df0:84::/48
Pakistan Software Export Board	SMALL	2405:c00::/32
Pakistan Telecom company limited	VERY LARGE	2404:7000::/32
Supernet, PDS Limited	MEDIUM	2001:fe8::/32
Telenor Pakistan (Pvt) Ltd	SMALL	2402:e000::/32
TRANSWORLD ASSOCIATES (PVT) LIMITED	MEDIUM	2404:d400::/32
WARID TELECOM	SMALL	2407:9c00::/32
Wi-Tribe Pakistan Limited	LARGE	2404:f400::/32
Worldcall Multimedia Limited (WML)	LARGE	2406:7000::/32

We are already late!

- A planned rollout in an average moderate network environment could take 2 years.
- If you are still looking for a business case than imagine Internet with NAT only.
- The sooner you start, the more time you have to test the network.
- Start conserving your IPv4 addresses for rainy days.

Conclusion

- Dual Stack
- Limited deployment
- Planning
- Technical team trained to support IPv6
- Security policy
- Lab testing
- Pilot project
- Production implementation
- June 8th – Not Bad

Bye Bye IPv4

- Re-phrasing from Gary Feldman @RIPE 55
  - bye bye, folks at SANOG XVIII
    be persuaded to upgrade it or your
    network will die
    IPv6 just makes me let out a sigh
    but I suppose we'd better give it a try
    I suppose we'd better give it a try

Any Questions…..

Thank you..

- Related Links
  - *IPv6 Task Force Pakistan www.**ipv6**tf.org.pk*
  - *Cyber Internet Services (Pvt) Ltd. www.cyber.net.pk*
  - Tunnel Broker www.he.net
  - APNIC IPv6 Program *www.**apnic**.net/community/**ipv6**-program*
  - IPv6 Forum www.ipv6forum.org

Contact:
aftabs@cyber.net.pk
aftab.siddiqui@gmail.com