CIRA's experience in deploying IPv6

Canadian Internet Registration Authority (CIRA)
Jacques Latour
Director, Information Technology

Singapore, June 20, 2011

IPv6

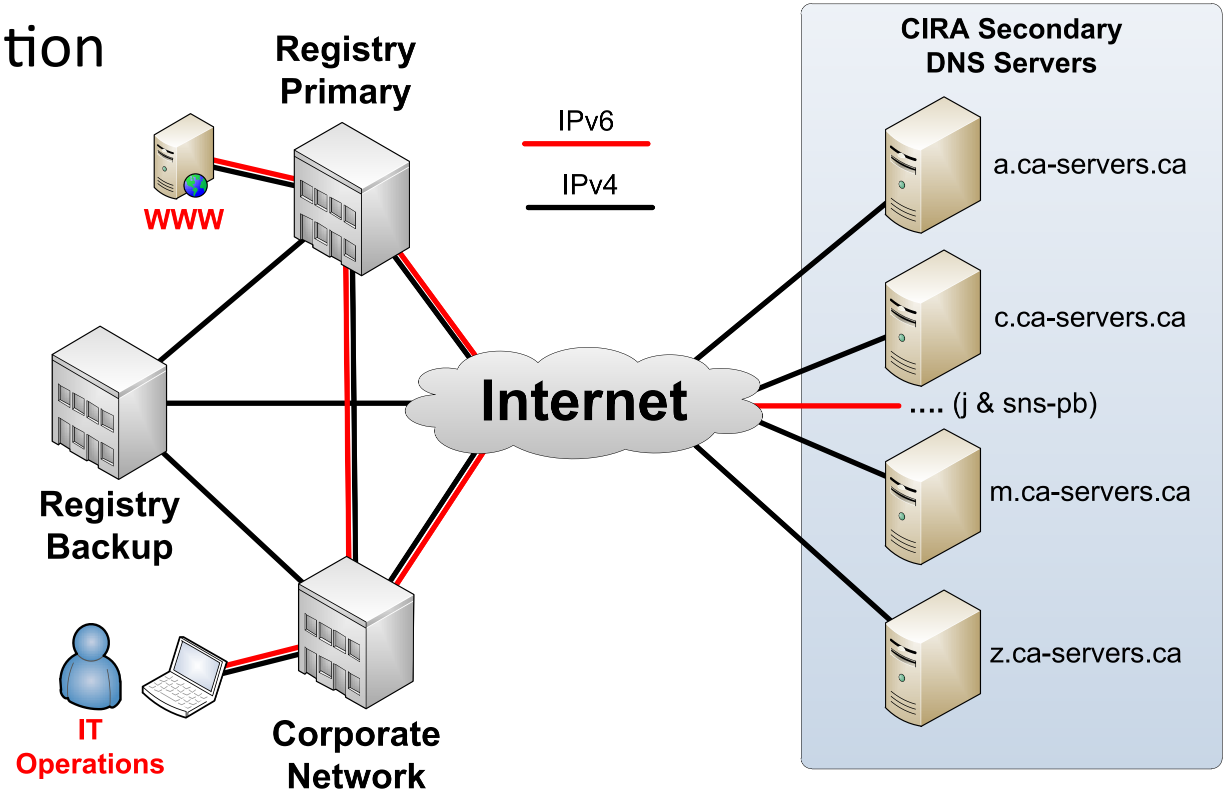
- New protocol (~15 year old)
- Not an extension of IPv4
- Not backward compatible
- New learning curve
- IPv6 **coexists** with IPv4
  - Not a transition
  - Not a migration
  - It's a journey!

IPv6 Adoption Strategy

- IPv6 Discovery & 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
- Assess IPv6 registrar accreditation tests

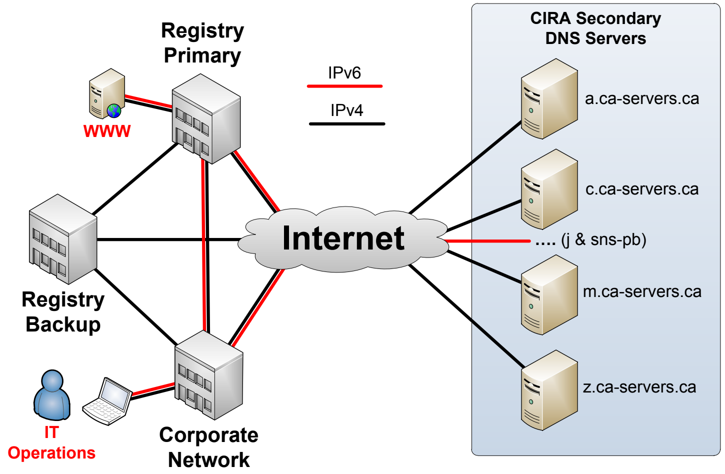
Objectives

- Not everything needs to be IPv6 on day 1
  - World IPv6 Day, June 8, 2011
    - Internet Perimeter & DMZ (www.cira.ca)
    - IT Organization
    - Permanent
    - Presence
    - Support



Critical Path

- Training [√] ongoing
- Develop an IPv6 security policy [√] – v1.0
- Order IPv6 Transit [√] – New circuits…
- IPv6 inside Corporate & DMZ [√]
- IPv6 on web servers [√]
- IPv6 for IT Operations [√]



IPv6 Internet Transit

- Architecture guideline:
  - Internet transit providers must support IPv4 & IPv6
- **We need to push Canadian ISPs for IPv6 enabled transits**
  - For the enterprise
  - If not, cancel/discontinue IPv4 only Internet transit
  - Order new IPv4/IPv6 Internet transits

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
  - Some of our Internet transits do not support IPv6
  - Need to test our custom/in house application for IPv6 compliance
  - Overall, we're in good shape to **coexist** with IPv6

Architecture Guidelines

"Rules of engagement"

- **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 disabled and not permitted
- **Native IPv6 Transit**
  - – IPv6 transit must support IPv6 natively without the use of tunnelling

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**
  - The interface identifier (64 bit) part must be randomly/ manually generated (Manual, RFC-3041)
  - MAC addresses of internal device must be kept confidential
  - Internet accessible Global Addresses must not use EUI-64 (MAC + FFFE)

Architecture Guidelines

- **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, ...) are assigned to number the links.
- **IPv6 Address Allocation**
  - DHCPv6 will be used where possible
  - We tested MacOSX Lion "Developer Preview" for DHCPv6 OK!!!
- **IPv6 Address Lifecycle (Life/Timeout)**
  - Need to assess impact on logging, correlation, & applications of having temporary IP addresses (Windows 7, MacOSX)

More Guidelines

"Can't remember all those IPv6 addresses"

- **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, BGPv4
  - Native IPv6 Routing, OSPFv3
  - Router redundancy, HSRPv6
  - OSPFv3 & BGPv4 secure routing adjacencies using filtering, passwords and hashes.
- **NetFlow data collection**
  - Use NetFlow 9 for IPv6 flow exports

Security Guidelines

"because we don't NAT IPv6"

- **Firewall**
  - Need excellent 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.

Based on best practise & RFC Recommendations

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 available at www.cira.ca/knowledge-centre/ipv6

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.

Learning curve…

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**

15 years of legacy?

Testing & Lab

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

Conclusion

- Dual Stack
- Limited deployment
- Planning
- Technical team trained to support IPv6
- Security policy
- Lab testing
- Pilot project
- Production implementation
- Success on June 8th – Try www.cira.ca on IPv6

ccNSO Tech Day Lunch

Sponsored by CIRA

At Café Swiss Swissotel