IPv6 CE Router Interoperability Whitepaper

March 2011

InterOperability Laboratory
University of New Hampshire

121 Technology Drive, Suite 2
Durham NH, 03824
Phone: +1-603-862-3941
Web: www.iol.unh.edu

University of New Hampshire
InterOperability Laboratory

Table of Contents

Overview

The University of New Hampshire InterOperability Laboratory (UNH-IOL) hosted an interoperability test event focusing on Customer Edge (CE) router IPv6 device capability. This event brought users and suppliers together in order to gain perspective on the current status of interoperability and the Internet Engineering Task Force (IETF) Basic Requirements for IPv6 Customer Edge Routers draft. The testing documented in this paper took place during the week of February 14th through 18th 2011.

An IPv6 CE router is a customer edge router intended for use in a home or small office environment. The router connects the end-user network to a service provider network and forwards packets not explicitly addressed to it. Implementing IPv6 on CE routers is necessary in order to sustain growth and usability of the Internet. Core networking equipment has supported IPv6 for some time and the next logical step is moving to the edge for IPv6 support.

While IPv6 is the solution for keeping current customers connected and adding new customers to the network as the supply of remaining allocated IPv4 addresses reach exhaustion, it is not widely deployed in broadband networks at this time. During the test event, cable suppliers found solutions to interoperability challenges that may be experienced in the transition thereby cost-effectively speeding broadband deployments.

In the wake of the Number Resource Organization's (NRO) central IPv4 address pool depletion announcement, the UNH-IOL remains focused on helping member companies identify potential interoperability issues by developing new IPv6 test plans, enabling members to speed go-to-market time for IPv6 products and devices, and sharing extensive knowledge of IPv6 with the industry.

Going forward, the UNH-IOL will continue to host IPv6 CE router IPv6 Interoperability Test Events to provide users and developers fast feedback in their implementations.

Participants

The following companies have agreed to be mentioned in this whitepaper.

Test Methodologies

The tests executed during this event were performed in order to verify that a IPv6 CE router implements IPv6 routing; that is, that the IPv6 CE router properly looks up IPv6 addresses in the Routing table and sends them to the correct interface as well as acts like a proper IPv6 node. Tests were also designed to verify the WAN side configuration, specifically that a node supports protocols necessary to access multiple network access architectures. LAN side configuration testing was limited due to time constraints.

The following common topology was used for all test cases.

Common Topology
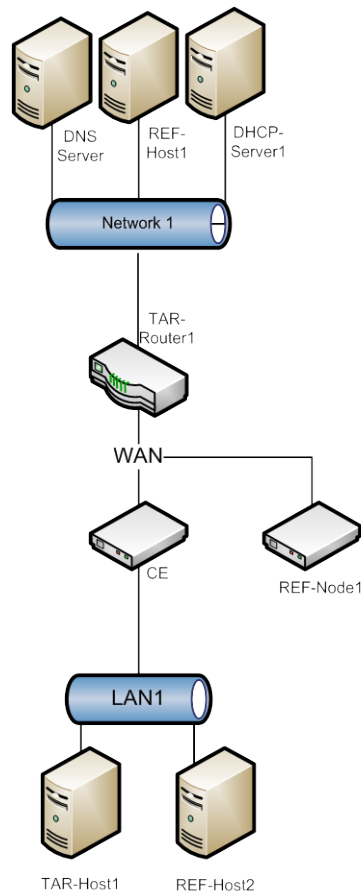
- o The WAN interface was either a DOCSIS or an Ethernet network for all CE devices.
- o The LAN and Network 1 were Ethernet networks.
- o Cisco Network Registrar (CNR) acted as both the DHCP-Server1 and DNS-Server.
- o REF-Host1 was a Linux Operating System.

- o TAR-Host1 and REF-Host2 was a mix of popular Operating Systems including Microsoft Windows 7, Microsoft Vista, Linux and Apple Mac OS X.

Observable Results

IETF Draft: Basic Requirements for IPv6 Customer Edge Routers

Detailed test cases were developed from the MUST requirements in the IETF Basic Requirements for IPv6 Customer Edge Routers draft including General Requirements, WAN Side Configuration, Address Assignment Requirements and LAN Side Configuration. Throughout the testing no issues were discovered with the IETF draft.

Test Plan Evolution

This initial event was critical for proving the theoretical test plan into real deployment test scenarios. The original test methodologies assumed full access to IPv6 CE router configurations. This however was not practical, and thus the test procedures were updated to accommodate for zero configuration testing. This was achieved by removing all need for user input and used alternative protocols to assure the purpose of the test. For example, using DHCPv6 prefix delegation rather than manually configuring an IPv6 address on the LAN interface. In cases where there were no alternatives to satisfy the test procedure, possible problems were included to omit the test.

Other changes to the test plan included updating the common test topology by removing a second LAN interface on the IPv6 CE router as well as adding a test case for testing link MTU.

Router Discovery and ICMPv6

Router Discovery on the IPv6 CE router LAN interface was verified. This testing included the processing of Router Solicitation messages and the transmission of Router Advertisements. All of the TAR-Host1 devices were able to discover the CE router and properly add the router to their default router list as per IETF RFC 4861.

ICMPv6 was also successful during the testing, verifying that an IPv6 CE router implemented the IPv6 node requirements. This testing observed that the IPv6 CE router properly assigned an IPv6 global address and delegated prefixes for the LAN interface allowing ICMPv6 Echo Request and Reply communication between the TAR-Host1 and IPv6 CE router.

Duplicate Address Detection (DAD)

Duplicate Address Detection was tested on both the LAN and WAN interfaces of the IPv6 CE router. DAD is the process of discovering if an address is unique on a local network. This was tested on both link-local and global addresses as per processes defined in IETF RFC 4862.

During the test event, IPv6 ND DAD failures were observed where two different CE's with different Ethernet MAC addresses generated the same IPv6 link-local address. It

was also observed that not all IPv6 CE routers supported link-local DAD on their LAN interfaces.   Duplicate Address Detection must be implemented in IPv6 networks to support Stateless Address Autoconfiguration.

DHCPv6 Address Acquisition

DHCPv6 was tested for addressing acquisition as a client on the WAN interface. The DHCPv6 client testing was successful and demonstrated that IPv6 CE routers were capable of supporting DHCPv6 on WAN interfaces.

It is merely a note that neither DHCPv6 Confirm messages nor DHCPv6 Release messages were observed on the DOCSIS WAN network. Transmission of DHCPv6 Confirm message is not expected on a DOCSIS WAN network, the test specification was updated to allow this. Restarting the DHCPv6 process when the DOCSIS interface was disabled and then enabled confirmed the lack of the DHCPv6 Confirm messages. Also, it is important to note that DHCPv6 Release messages are required when a device has ceased using the IPv6 address and thus be sent to remove DHCPv6 information. The DHCPv6 Release message issue was raised and thus being added to the appropriate DOCSIS standards.

It was also observed that during the event a few DHCPv6 implementations did not keep the same DUID between reboots.   This feature is a requirement of the CE router draft. The reasoning behind this requirement is because service provider routers (TAR-Router1), make decisions and keep cached information based on the DUID. If the DUID changes between reboots a service provider router will cache multiple entries of information for the same device leading to the router overflowing.

DHCPv6 Prefix Delegation (DHCPv6 PD)

The testing observed a couple of areas that IPv6 CE routers will need to address with respect to implementing DHCPv6 Prefix Delegation (DHCPv6 PD). Each of these observations will be detailed below.

The first issue discovered during DHCPv6 PD testing was that IPv6 CE routers did not properly transmit DHCPv6 Renew or Rebind messages containing the IA_PD option on their WAN interface. During this test, the DHCP-Sever1 returns the addresses to the prefix delegation pool, which in turn causes TAR-Router1, as a snooping DHCPv6 Relay Agent, to stop forwarding IPv6 packets addressed to the prefix delegation pool. According to RFC 3633, Section 12.1 "The requesting router includes IA_PD options in any Renew, or Rebind messages sent by the requesting router. The IA_PD option includes all of the prefixes the requesting router currently has associated with that IA_PD." Therefore, the IPv6 CE router should transmit DHCPv6 Renew message with IA_PD after T1 seconds. TAR-Router1 would continue to forward IPv6 packets correctly and the DHCP-Server would not return the addresses to the prefix delegation pool.

A second issue was discovered with the IA_PD option containing prefix lengths smaller then 64, for example /60 and /56. During the test, the DHCP-Server transmitted a DHCPv6 Reply message with an IA_PD prefix length of 60.   The IPv6 CE router transmitted a Router Advertisement with a Prefix Information Option that contained the prefix with a prefix length of 60. However, the TAR-Host1 was unable to acquire a global address, due to the Router Advertisement Prefix Information Option being invalid for an Ethernet network. According to RFC 3633, Section 12.1 "When a requesting router subnets a delegated prefix, it must assign additional bits to the prefix to generate unique, longer prefixes. For example, if the requesting router… were delegated 3FFE:FFFF:0::/48, it might generate 3FFE:FFFF:0:1::/64 and 3FFE:FFFF:0:2::/64 for assignment to the two links in the subscriber network." Therefore, the IPv6 CE router should take the IA_PD option with a prefix length of 60 and transmit Router Advertisements with a longer unique prefix then the prefix contained in the IA_PD option. TAR-Host1 will then obtain a global address from the IPv6 CE router thru Router Advertisements. This behavior was experienced on all but one of the IPv6 CE router devices at the event.

A third issue was found with respect to forwarding loops when one IPv6 CE router properly supported Prefix Delegation with a prefix length other than 64. During this test, the IPv6 CE router received a DHCP Reply with the IA_PD containing a valid prefix with a length of 60. The IPv6 CE router then properly transmits a Router Advertisement with a unique prefix from the delegated prefix pool. This enables TAR-Host1 to acquire a global address using the unique prefix. The test continues when TAR-Host1 transmits IPv6 traffic using an IPv6 prefix not assigned by the IPv6 CE router however with in the IA_PD prefix pool. This causes the IPv6 CE router to forward the packets to TAR-Router1 while the TAR-Router1 will then forward the packet back to the IPv6 CE router causing the forwarding loop. This process continued until the hop limit of the packets was met.

According to draft-ietf-v6ops-ipv6-cpe-router-09 Section 4.2 "If the delegated prefix(es) are aggregate route(s) of multiple, more-specific routes, the IPv6 CE router MUST discard packets that match the aggregate route(s), but not any of the more-specific routes. In other words, the nexthop for the aggregate route(s) should be the null destination. This is necessary to prevent forwarding loops when some addresses covered by the aggregate are not reachable [RFC4632]." Therefore the IPv6 CE router should not transmit the IPv6 traffic to an unassigned prefix to TAR-Router1. The IPv6 CE router should also send an ICMPv6 Destination Unreachable to TAR-Host1.

The fourth issue uncovered was that the IPv6 CE routers did not properly handle the distribution of prefix lifetimes. When the IPv6 CE router receives a DHCPv6 Reply message with an IA_PD option containing proper valid lifetime, the IPv6 CE routers were observed using default valid lifetime in Router Advertisements on the LAN network. According to RFC 3633 Section 12.1 "If the requesting router assigns a delegated prefix to a link to which the router is attached, and begins to send router advertisements for the prefix on the link, the requesting router MUST set the valid lifetime in those advertisements to be no later than the valid lifetime specified in the

IA_PD Prefix option. A requesting router MAY use the preferred lifetime specified in the IA_PD Prefix option." Therefore, the IPv6 CE router must use the valid lifetime contained in IA_PD Prefix option in the Router Advertisement Prefix Information Option on the LAN networks.

The last issue discovered during the testing was IPv6 CE router lack of support for DHCP Reconfigure. According to draft-ietf-v6ops-ipv6-cpe-router-09, "WAA-4: The IPv6 CE router MUST be able to support the following DHCPv6 options: IA_NA, Reconfigure Accept [RFC3315], DNS_SERVERS [RFC3646]." Therefore the IPv6 CE routers should have included the Reconfigure Accept in DHCPv6 Request or Solicit messages.

Domain Name Server (DNS)

Another observation arose regarding DNS proxy and recursion; all the devices were able to receive DNS information successfully on the WAN interface, however not all of the devices properly implemented DNS proxy or were observed to forward the DNS information along to the LAN interface. This is critical for TAR-Host1 in order to receive DNS information. One area for the IETF to investigate regarding the advanced requirements for IPv6 Customer Edge router bis document would be to require the method that DNS is distributed on the LAN interfaces.

Conclusion

As IPv4 addressing runs out, it is vital that IPv6 be implemented in edge equipment in order for operators to have the ability to use IPv6 in deployments. The participants in the IPv6 CE Interoperability Test Event demonstrated that IPv6 is being implemented in IPv6 CE routers. This inaugural IPv6 event tested fundamental IPv6 CE router functionality derived from the IETF CE Router draft document, which gives both the operators, and equipment manufactures a common set of requirements for IPv6 CE routers. During the event no issues with the draft document were uncovered.

As part of the IPv6 event we successfully demonstrated IPv6 addressing. The IPv6 CE router did not show any issues around addressing and accessing WAN interfaces through IPv6. This allows operators with current IPv6 CE router implementations to have IPv6 connectivity as well as have the ability to manage the devices. This is an important and necessary step in the use of IPv6 in operational networks.

This early event showed that more testing and development are needed in IPv6 implementations on IPv6 CE routers, however the backbone protocols were there. The main focus area that requires further testing is the DHCPv6 Prefix Delegation protocol. The ability to propagate relevant information to end-user devices is an important function of the IPv6 CE router.

Moving forward, the UNH-IOL is working in conjunction with the IPv6 Forum in order to create an IPv6 Ready Logo program that will help both the user and equipment manufactures understand what features they need to support to aide in the worldwide deployment of IPv6. After the basic requirements are complete new areas such as transition mechanisms and routing protocols will need to be covered in future testing. This type of testing will ensure that IPv6 deployment be a seamless transition.

About the UNH-IOL

Founded in 1988, the UNH-IOL provides independent, broad-based interoperability and standards conformance testing for data, telecommunications and storage networking products and technologies. Combining extensive staff experience, standards bodies' participation and a 32,000+ square foot facility, the UNH-IOL helps companies efficiently and cost effectively deliver products to the market. For more information, visit http://www.iol.unh.edu./.

The UNH-IOL hosts multi-vendor group tests (often called "plugfests") as often as four times a month. These group test events compliment over 20 year-round standards-based testing programs that are managed and operated by the UNH-IOL. Each of the testing groups, called "consortiums", represents a collaboration of industry forums, service providers, test equipment vendors and otherwise competing companies who benefit each other by:

- Distributing the cost of testing
- Lowering R&D and QA expenses
- Reducing product time to market
- Obtaining trusted vendor-neutral verification

The laboratory maintains a strong reputation for independent, vendor-neutral testing with a focus on quality assurance. The confidential test reports the UNH-IOL provides to its members are recognized throughout the data communications industry as evidence of interoperability and conformance to technical standards.

Terminology

CE LAN: CE Router LAN Interface
CE WAN: CE Router WAN Interface
DAD: Duplicate Address Detection
DHCP: Dynamic Host Configuration Protocol
ICMP: Internet Control Message Protocol. ICMP Echo Requests and Replies facilitate troubleshooting at Layer 3 for both IPv4 and IPv6. IPv6 has built extra features into ICMP.
IETF: Internet Engineering Task Force
LAN: Local Area Network
NS: Neighbor Solicitation
NA: Neighbor Advertisement
NCE: Neighbor Cache Entry
NUT: Node Under Test
PD: Prefix Delegation
RA: Router Advertisement
RS: Router Solicitation
WAN: Wide Area Network

References

The following documents are referenced during the test event:

[RFC 2460]   R. Hinden, S. Deering, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998.

[RFC 3315]   R. Droms, J. Bound, B. Volz, T.Lemon, C. Perkins, M.Carney, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315, July 2003.

[RFC 3633]   O. Troan, R.Droms, IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, RFC 3633, December 2003.

[RFC 3484]   R. Draves, Default Address Selection for Internet Protocol version 6 (IPv6), RFC 3484, February 2003.

[RFC 3646]   R.Droms, DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3646, December 2003.

[RFC 3736]   R.Droms, Stateless Dynamic Host Configuration Protocol (DHCP) Server for IPv6, RFC 3736, April 2004.

[RFC 4191]   R. Draves, D. Thaler, Default Router Preferences and More-Specific Routes, RFC 4191, November 2005.

[RFC 4291]   R. Hinden, S. Deering, IP Version 6 Addressing Architecture, RFC 4291, February 2006.

[RFC 4294]   J. Loughney, Ed. IPv6 Node Requirements, RFC 4294, April 2006.

[RFC 4443]   A. Conta S. Deering, M. Gupta, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 4443, March 2006.

[RFC 4861]   T. Narten, E. Nordmark, and W. Simpson, H. Soliman, Neighbor Discovery for IP Version 6 (IPv6), RFC 4861, September 2007.

[RFC 4862]   S. Thomson, T. Narten, T. Jinmei, IPv6 Stateless Address Autoconfiguration, RFC 4862, September 2007.

[RFC 5942]   H. Singh, W. Beebee, E. Nordmark, RFC 5942, July 2010.

[ipv6-cpe-router]   Singh, H., W. Beebee, C. Donley, B. Stark, O. Troan. "Basic
Requirements for IPv6 Customer Edge Routers", draft-ietf-v6ops-
ipv6-cpe-router-09. December 2010.

Contributors

Timothy Carlin, UNH-IOL
Erica Johnson, UNH-IOL
Lincoln Lavoie, UNH-IOL
Thomas Peterson, UNH-IOL
Timothy Winters, UNH-IOL