On Campus IPv6 Beta Site: Requirements, Solutions, and Product Defect Evaluation

Ying-Dar Lin[1], Ren-Hung Hwang[2], Raghavendra Kulkarni[1], Chinyang Henry Tseng[3], Chun-Hung Hsu[4]
[1]Department of Computer Science, National Chiao Tung University, Taiwan
[2]Department of Information Science and Computer Engineering, National Chung Cheng University, Taiwan
[3]Department of Information Science and Computer Engineering, National Taipei University, Taiwan
[4]Network Benchmarking Lab, National Chiao Tung University, Taiwan
ydlin@cs.nctu.edu.tw, rhhwang@cs.ccu.edu.tw, raghu196@gmail.com, tsengcyt@gm.ntpu.edu.tw, chhsu@nbl.org.tw

Abstract

Due to IPv4 address exhaustion, IPv6 deployment has been in progress and the transition from IPv4 to IPv6 has become more imminent. In this article, we report an on-campus IPv6 beta site coexisting with IPv4 networks and designed with requirements from its stakeholders. We conducted a wide range of test cases, from essential functionality tests to advanced stability tests which require complex interoperability tests and cannot be performed in laboratory testing. After one year of operation, tens of defects were observed and seven representative defects in dual-stack tunneling, IPv6 routing table, RIPng, and OSPFv3, are reported. Most defects are reproducible, and some could be fixed by proper configuration while others are caused by flaws in system design, memory management, or protocol implementation. We suggest careful configuration, overloading prevention, limited resource sharing, and robust error handling as the lessons to vendors and administrators of IPv6 devices.

Keywords: IPv6, Beta site, Dual-stack tunneling, OSPFv3, RIPng.

1 Introduction

1.1 IPv4 Exhaustion and IPv6 Deployment

After a successful experience with constructing an IPv4 beta site [1], we advanced to build an on-campus IPv6 beta site, where IPv6 can coexist with IPv4 by utilizing IPv4/IPv6 dual stack and tunneling transition techniques. The need of deploying IPv6 becomes imminent as the Number Resource Organization (NRO) announced full depletion of the free pool of IPv4 addresses on 3 February 2011, commonly known as the IPv4 address exhaustion problem. The period before this date was referred as the first phase of IPv4 exhaustion. On that date, based on a global policy [2], the Internet Assigned Numbers Authority (IANA) entered the IPv4 address exhaustion phase and allocated the remaining five "/8 addresses" equally between the five Regional Internet Registries (RIRs), where a "/8" address block consists of 16,777,216 addresses. This phase was referred as the second phase of IP exhaustion. Right after IANA's exhaustion, the RIR of the Asia Pacific region, APNIC, announced it had reached the final /8 IPv4 address block and entered the third phase of IPv4 exhaustion [3]. It is now only a matter of time before other RIRs will announce the exhaustion of their IPv4 address pools.

During the third phase of IPv4 exhaustion, each RIR assigns IPv4 addresses based on its "last /8 address policy," which is aimed to provide IPv4 address space for new Local Internet Registries (LIRs) and for those deploying IPv6. That is, the new allocation of the IPv4 address is expected to be used as a means of essential connectivity to IPv6 networks. This explains the imperative demand of IPv6 deployment coexisting with IPv4 networks and the emergent requirement of IPv6 beta site for testing IPv6 enabled devices and applications.

Although we have faced the IPv4 exhaustion problem, the deployment of IPv6 is not as fast as expected, especially for Internet content providers. Therefore, on June 8, 2011, the Internet Society and several large content providers, such as Google, Yahoo, YouTube, and Facebook, organized an event, called World IPv6 Day, to test and promote the IPv6 deployment. The event was successful; the IPv6 traffic was increased from 0.024% to 0.041%. However, most of the participants did not maintain the IPv6 availability of their web sites after that event. Therefore, the Internet Society carried out another event, called World IPv6 Launch Day, on June 6, 2012 with an aim to encourage participants to bring permanent IPv6 deployment of their services. According to reports from Cisco [4] and Ars Technica [5], about 27% of global Web pages can be reached via IPv6 after the World IPv6 Launch Day.

Another issue of deployment of IPv6 is the transition from IPv4 to IPv6. Although several transition mechanisms have been proposed and tested to connect IPv6 only networks to the IPv4 network, such as 6to4 [6] and NAT64 [7], the dual-stack [8] approach remains the most recommended transition mechanism.

1.2 Stability Test in IPv6 Beta Site

Beta testing is the last stage of testing computer products prior to commercial release. It is normally

*Corresponding author: Ren-Hung Hwang; E-mail: rhhwang@cs.ccu.edu.tw
DOI: 10.6138/JIT.2015.16.7.20130221

performed at beta test sites outside the manufacturer for real-world exposure. As a contrast to laboratory testing, or called alpha testing, which lacks for diversity of real-world network scenarios, beta testing can complement it with field testing in real networks. However, it is recommended to have a product undergo alpha testing before it is deployed into beta testing which should be used to isolate problems that cannot be found in alpha testing. It is inefficient to use beta testing to find problems that could be found using alpha testing.

Since no previous work had reported on building an IPv6 beta site, we were dedicated to constructing an on-campus IPv6 beta site in a real IPv4/IPv6 dual stack network for advanced IPv6 stability testing. Stability testing requires real user-generated network traffic running on different networking devices to perform interoperability tests. Through the stability test provided by our beta site, vendors can check if their IPv6 devices perform correctly and effectively when communicating with other vendors' devices. The stability test also provides vendors with a way to resolve potential defects of their products before commercial release.

The design of IPv6 beta site considers requirements from its three stakeholders, namely, vendors, users, and administrators. With a variety of test zones and debugging capability, the beta site allows vendors to test a wide range of IPv6 network devices over a sufficiently long period of time (over 720 hours, i.e., one month). With dual-stack topology and IPTV multicasting programs, users enjoy seamless and high quality IPv6 services. We chose IPTV multicast because it would generate high volume of IPv6 traffic to a large scale of user groups. With redundant network topology design and automated network management, administrators are able to ensure the service quality of the beta site.

Defects observed in the beta site are collected, analyzed, and reported in this article. To cover a wide range of test cases, the IPv6 beta site is constructed to cover many important IPv6 features including IPv6 transition mechanisms, IPv6 routing protocols, and IPv6 multicasting service. The beta site was tested for a year, and seven representative defects are reported in this article. In order to understand the real causes and solutions for these defects, we first classified them into four categories and then analyzed them from four different aspects, including impact level, work around solution, time of occurrence, and cause of the defect. After analyzing these defects, we found three defects that were severe or catastrophic. Most of the defects are reproducible and can be resolved by proper configuration of network devices. Furthermore, most of the defects are caused by flaws in memory management or protocol implementation.

1.3 Related Work

Transition from IPv4 to IPv6 has been in progress for several years since the forecast of IPv4 address exhaustion. However, since the process is an evolution, not a revolution, the transition is expected to take a long time while new transition mechanisms come up. Noticeably, IPv4 and IPv6 will coexist during the transition period and thus coexistence strategies have also been studied [9-10]. In the literature, transition mechanisms are classified into three categories, namely, dual-stack, tunneling, and translation. Furthermore, combining dual-stack and tunneling, referred to as "dual-stack with tunneling", is commonly adopted at an early transition stage as it facilitates IPv4 and IPv6 enabled applications operating on the same host while allowing IPv6 applications to pass through *IPv4-only* networks.

Development and deployment of an IPv6 network at the University of Venezuela was reported in [11]. Both dual-stack and tunneling mechanisms were adopted for connecting to the Internet and Internet2. The study also showed competitive TCP and UDP throughput over IPv4 and IPv6. However, it did not discuss any transition problems encountered. A much larger scale deployment of IPv6 over multiple universities was conducted in the China Next Generation Internet (CNGI) project [12]. In this project, CNGI-CERNET2, an IPv6-only network connecting more than 2000 campus networks, was built. It provides a "Solution for Delegated IPv6 Prefixes" (SAVI) framework to ensure legitimate IP addresses and also develops a cross-domain charging system for mobile users *roaming* from one campus site to another. SAVI is the suite of protocols for *auto-generation* of IPv6 addresses. An IPv6 conformance and interoperability test was studied in [13]. It introduced the *IPv6 Ready Logo* testing program and how worldwide IPv6 programs built IPv6 testing sites and testing tools to certify the credibility of conformance and interoperability tests. Currently, IPv6 Ready Logo is the most commonly adopted conformance and interoperability testing program worldwide. It consists of two testing programs: IPv6 Core Protocols testing and CE Router testing. These two testing programs cover following protocols: IPv6 core protocols (RFC 1981 [14], RFC 2460 [15], RFC 4443 [16], RFC 4291 [17], RFC 4861 [18], RFC 4862 [19]), CE Router (RFC 6204 [20]), IPsec (RFC 2404 [21], RFC 2410 [22], RFC 2451 [23], RFC 3566 [24], RFC 3602 [25], RFC 3686 [26], RFC 4301 [27], RFC 4303 [28], RFC 4305 [29], RFC 4312 [30]), IKEv2 (RFC 4306 [31], RFC 4307 [32], RFC 4718 [33]), DHCPv6 (RFC 3315 [34], RFC 3646 [35], RFC 3736 [36]), SNMP-MIBs (RFC 3416 [37], RFC 3418 [38], RFC 2578 [39], RFC 2579 [40], RFC 2580 [41]), MIPv6 (RFC 3775 [42], RFC 3776 [43]), NEMO (RFC 3961 [44], RFC 3775 [42]), and SIP (RFC

3261 [45], RFC 3264 [46], RFC 4566 [47], RFC 2617 [48], RFC 3665 [49]). In United States, National Institute of Standards and Technology (NIST) also announced the specification for the USGv6 testing program in 2009. Both testing programs specify *conformance* and *interoperability* features for routers and hosts based on RFCs published by the IETF. Chunghwa Telecom Laboratory, Taiwan (CHT-TL), and InterOperability Laboratory of University of New Hampshire, USA (UNH-IOL), are two laboratories that provide *both* IPv6 Ready Logo and USGv6 certification tests. Notably, these testing programs are conducted in laboratories while our work emphasizes on beta testing with real-world traffic.

The remainder of this work is organized as follows. Requirements from the vendors, users and network administrators are addressed in Section 2. Solutions for satisfying these requirements are then described in Section 3. Next, seven representative defects along with evaluation analysis are presented in Section 4. The final section concludes our work.

2 Requirements

The requirements from the main stakeholders of IPv6 beta site are described as follows.

2.1 Vendors

Vendors are the major experimentalists of the beta site as they need a customizable and accessible test bed for their IPv6 devices under test (DUTs). DUTs include a wide range of IPv6 enabled networking devices, such as layer 3 switches, routers, security appliances, and residential gateways. Vendors require a customizable test bed so that they can obtain any traffic with different characteristics and test any devices according to their needs. Vendors also require an accessible test bed so that they can remotely access their DUTs whilst being provided with sufficient facilities to assist them in fixing reported defects.

2.2 Users

The IPv6 beta site was built on the campus of National Chiao Tung University (NCTU) which consists of wired and wireless networks. Over 1,000 students had subscribed to the beta site. The beta site was built with coexistence of IPv4 and IPv6 networks and applications. Generally, most of the users are not familiar with an IPv6 address configuration, thus the first requirement from users is a seamless migration between IPv6 and IPv4 addresses. To provide incentive for using the IPv6 beta site, killer applications, such as IPTV and VoIP, are provided as free services to users. However, these services are bandwidth-intensive and time-sensitive. Therefore, the second requirement from users is to provide high quality services that are not available from the IPv4 network.

2.3 Administrators

The administrators of the beta site are responsible to provide reliable services including maintaining DUT stability, monitoring testing features, troubleshooting network events, and balancing network requirements between vendors and users. High network *availability*, however, is the first priority of network administration. Therefore, the first requirement from the administrator is a speedy *recovery* from network failures to minimize the network downtime. Secondly, the administrator also needs an *automatic* network management system, such as automatic failure notification, to assist the network management and maintenance work.

3 Solutions

Table 1 summarizes requirements of stakeholders discussed in the previous section and our solutions to these requirements. We illustrate each solution in detail in this section.

Table 1 Summary of Stakeholders, Requirements, and Solutions

Stakeholders	Requirements	Solutions
Vendors	Customizable beta test accommodating variety of DUTs	Variety of testing zones
Vendors	Accessible with debugging information	Remote access tool and debug information collection strategy
Users	Seamless IPv4/ IPv6 migration	Dual-stack with tunneling
Users	High quality service	IPTV Multicasting
Administrators	Speedy failure recovery	Redundant network topology
Administrators	Ease of network management and maintenance	Automated network management system

3.1 Solutions to Vendors -- Variety of Testing Zones

Many defects of networking devices could only be observed under real traffic patterns. Therefore, it is very important for the IPv6 beta site to be able to provide a testing environment with real user-generated traffic. Figure 1 shows the topology of the IPv6 beta site which consists of a variety of testing zones. First, zone 4 and zone 6 are dual-stack *backbone* networks designed for IPv6 stability

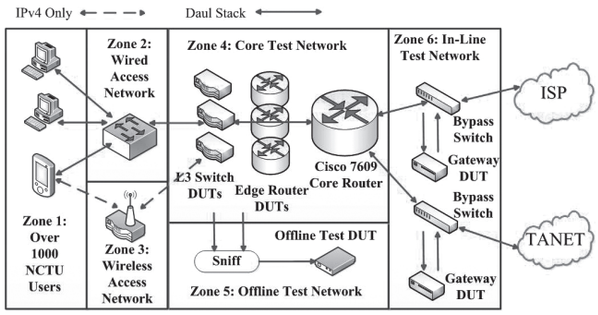

Figure 1 IPv6 Beta Site Testing Zones

tests. Most of DUTs, such as dual-stack Layer 3 (L3) switches, edge routers, and gateways, are put in these two zones. Zone 2 is the *access* network to beta site *users* which consists of more than 1000 NCTU students that form zone 1. Packets generated from devices in zone 1 will be forwarded by DUTS in zone 2, zone 4, and zone 6 to the Internet, either through an ISP or the Taiwan Academic Network (TANET). Since users in zone 1 can consume any IPv6 and IPv4 services simultaneously at any IPv6 enabled devices, the stability testing environment in zone 4 and zone 6 is close to real commercialized networks. In addition, an IPv4-only *wireless access* network is placed in zone 3. It also could be replaced with a dual-stack wireless network depending on the testing scenario. The IPv6 beta site had been running for over a year so that new IPv6 features of DUTs could be tested for a longer time which provided more opportunities to observe defects of DUTs. Table 2 gives the detailed information of devices deployed in the beta site testing zones (Note that vendor and model name are anonymized.

Besides real-time inline tests, zone 5 in the beta site also supports *offline* tests for IPv6, such as IPv6 functional and conformance tests. The real user-generated traffic passing through zone 4 is captured into PCAP files. The packet sniffers replay the captured traffic in the PCAP files into the DUTs for customized offline tests [50]. Since zone 5 is separated from the core network, it can perform risky tests, such as stress tests, without influencing the normal operations of the core network.

3.2 Solutions to Vendors -- Collecting Debug Information

When a defect was discovered in the beta site, the task of collecting adequate debugging information to *reproduce* the same defect is very critical for defect fixing. It helps vendors verify whether the reported defect is a real defect and perform root cause analysis, i.e., find the real cause of the problem and derive a solution to resolve the defect rather than simply trial by error. Since defects may occur at any time under any unexpected and unknown testing scenarios, the following approaches are adopted to collect adequate debugging information.

First, traffic is *mirrored* and *saved*. Once a defect occurs, the captured traffic can assist engineers investigating the defect by replaying the traffic to reproduce the defect. Since the replay depends on the *stateful* behaviors of the DUT, the replayer also needs to be stateful [50]. Noticeably, the captured traffic has been anonymized to protect user privacy. Second, we provide automatic notifications to instantly inform vendors and administrators of detected defects. Third, after receiving a defect notice, we give vendors two hours to debug. During this debugging period, vendors can remotely turn on additional debug features and collect desirable debug information, such as system logs and memory dumps, on their DUTs. The collected information could be used for reproducing the defect. Similarly, administrators of the beta site also have two hours to troubleshoot the defect and inform users in case of network service disruption. Thus, the *two-hour-debug-time* policy is a win-win strategy for both vendors and administrators. It is especially important for vendors to turn on the *debug mode* of their DUTs to collect adequate debugging information.

3.3 Solutions to Users -- Dual-Stack Topology

Most of the users on the beta site are not familiar with IPv6 configurations and expect plug-and-play services just like IPv4. In addition, users expect to run their IPv4 and IPv6 applications at the same time without any service switching interruptions. To meet this requirement, a dual-stack topology is deployed to provide coexistent services of IPv4 and IPv6 which are transparent to users. This dual-stack extends from zone 1 to zone 6, all the way to the ISP. Most of the users' devices run operating systems that already support dual stacks, e.g., Linux and Windows 7. For these devices, *stateless* IPv6 address *auto-configuration* is adopted to automatically configure devices' IPv6 addresses. On the other hand, based on NCTU's policy, the IPv4 address of a device is manually configured with the public IPv4 address, just like other computers on-campus. Thus, IPv6 is provided to users transparently.

Figure 2 illustrates IPv6 dual–stack with *tunneling* deployment at the IPv6 beta site. The dual-stack Layer 3 switch, which is one of the DUTs, forwards traffic from the dormitory access network to the dual-stack edge router, which is also a DUT. This dual-stack edge router supports automatic configuration of the IPv6 address. It connects to the Internet through a dual-stack core router which is a Cisco 7609 router. The dual-stack L3 switch also connects to an IPv4-only edge router for testing the *IPv6-over-IPv4* tunneling function of DUTs.

Table 2 Detailed Information of Devices Deployed in the Beta Site Testing Zones

Device type	Vendor	Model	Description	Specification	Zone
DUT	A	A-3472	Layer 2 Ethernet Switch	20 10/100/1000BASE-T 4 Combo 10/100/1000BASE-T/SFP 3 Open Slots for 10-Gigabit Uplink Modules	2
DUT	A	A-3450	Layer 2 Ethernet Switch	44 10/100/1000BASE-T 4 Combo 10/100/1000BASE-T/SFP 2 Open Slots for 10-Gigabit Uplink Modules	2
DUT	A	A-3650	Layer 3 Ethernet Switch	44 10/100/1000BASE-T 4 Combo 10/100/1000BASE-T/SFP 2 Open Slots for 10-Gigabit Uplink Modules	2
DUT	A	A-3627	Layer 3 Ethernet Switch	24 10/100/1000BASE-T 4 Combo 10/100/1000BASE-T/SFP 3 Open Slots for 10-Gigabit Uplink Modules	2 and 4
DUT	A	A-3200-10	Layer 2 Ethernet Switch	8 10/100/1000BASE-T Gigabit Ports 2 Combo 10/100/1000BASE-T/SFP Ports	2
DUT	A	A-3200-16	Layer 2 Ethernet Switch	14 10/100/1000BASE-T Gigabit Ports 2 Combo 10/100/1000BASE-T/SFP Ports	2
DUT	A	A-3528	Layer 2 Ethernet Switch with PoE	24 10/100/1000BASE-T Gigabit Ports 2 10/100/1000BASE-T Gigabit Ports 2 Combo 10/100/1000BASE-T/SFP Ports	2
DUT	A	A-3528P	Layer 2 Ethernet Switch	24 10/100/1000BASE-T Gigabit Ports 2 10/100/1000BASE-T Gigabit Ports 2 Combo 10/100/1000BASE-T/SFP Ports	2
DUT	A	A-3552	Layer 2 Ethernet Switch	48 10/100/1000BASE-T Gigabit Ports 2 10/100/1000BASE-T Gigabit Ports 2 Combo 10/100/1000BASE-T/SFP Ports	2
DUT	A	A-8006	Layer 3 Ethernet Switch	Chassis Switch with 8 slots	4
DUT	A	A-6604	Layer 3 Ethernet Switch	Chassis Switch with 6 slots	4
DUT	B	B-4526	Layer 3 Ethernet Switch	20 10/100/1000BASE-T 4 Combo 10/100/1000BASE-T/SFP 1 Open Slots for 10-Gigabit Uplink Modules	4
In-service	C	C-7609	Layer 3 Ethernet Switch	Chassis Switch with 9 slots Core router of BetaSite, aggregate and forward traffic from each building in campus	4
In-service	D	D-ibypass	Bypass Switch	10/100/1000 bypass switch with Heartbeat Intelligent bypass switch to check forwarding function of DUT by heartbeat packets	6
In-service	D	D-ibypass	Bypass Switch	Gigabit Fiber bypass switch with Heartbeat and SFP Monitor Ports	6
In-service	D	D-5204	Intelligent TAP	24 10/100/1000BASE-T Gigabit Ports 4 Combo 1000BASE-T/SFP Ports 4 10G XFP slots Intelligent regeneration TAP to aggregate and regenerate traffic to different DUTs with different filter policy	5

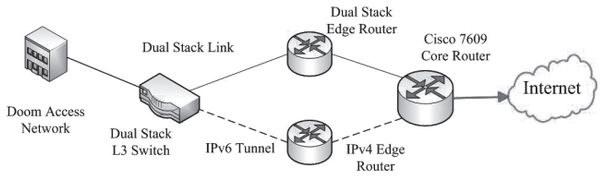

Figure 2 Dual-Stack with Tunneling Topology at the IPv6 Beta Site

3.4 Solutions to Users -- IPTV Multicasting

An IPv6 network needs a heavy application for generating a large amount of traffic to demonstrate its network capability. In our beta site, the IPTV service with high quality TV programs is provided via *IPv6 multicasting*. Each TV program is delivered with the resolution of 1,920 × 1,080 in an interlaced format (1,080 i). To subscribe the IPTV service, users just need to install the open source Video LAN Client (VLC) software. The IPTV service was quite successful and popular during the test period, thus becoming the major IPv6 traffic in the beta site.

Figure 3 illustrates the IPTV multicast service and its deployment requirements, including IPv6 Multicast Listener Discovery (MLD) snooping at Layer 3 switches and Protocol Independent Multicast (PIM) v6 at IPv6 routers. By multicasting, network devices only distribute the IPTV video stream to the multicast group members. To do this, the network devices, including L3 switches and routers, need to build a multicast topology to connect the IPTV users to the video source. Firstly, the IPv6 MLD snooping enabled switches discover the IPTV users who listen to the IPTV multicast service. In other words, switches will know which *ports* to forward the traffic of a particular multicast group. Secondly, participating IPv6 routers form a *multicast tree* via the PIMv6 protocol. Delivering IPTV multicasting service using the layer 3 multicast function is more efficient than using the application layer approach. Furthermore, IPv6 multicasting function of DUTs can be tested under real user-generated traffic pattern in the beta site.

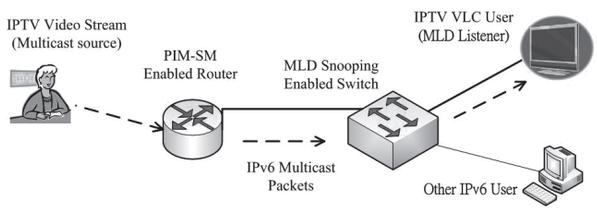

Figure 3 IPTV Multicast Service in the IPv6 Beta Site

3.5 Solutions to Administrators -- Redundant Network Topology Design

For beta site administrators, it is a critical task to maintain network stability and reliability of the beta site with massive deployment of DUTs. Since DUTs are not as reliable as commercial products, our solution is to provide *redundant* network topology design. All DUTs must follow one of the two redundant design strategies to prevent network disconnections caused by a single DUT failure.

The first type of redundant design is to deploy a *backup* device of the DUT beta testing. The backup device has exactly the same function capability as the DUT under testing. Figure 4 demonstrates this type of redundant design exercised in the core testing network, i.e., zone 4 in Figure 1. Specifically, the core network consists of two major types of devices: layer 3 switches and routers. As shown in Figure 4, a duplicate switch or router is deployed *in parallel* to a DUT under testing. For layer 3 switches, Virtual Router Redundancy Protocol (VRRP) is adopted which converts the pair of layer 3 switches as a *virtual router*. Both switches are kept active at all times. During normal operation, all traffic is directed to the master DUT. However, when the *master* DUT fails, all traffic will be redirected to the *backup* DUT automatically. Thus fault tolerance can be achieved. For edge router DUTs, not only a backup router is deployed, but also the configuration of the backup router is properly configured. For example, IPv6 subnet addresses and prefix lengths of all interfaces are set as that of the master router. User devices will connect to the backup DUT automatically when the master router fails.

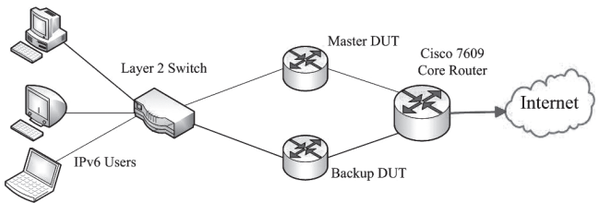

Figure 4 Redundancy Design of the Testing Network

Zone 6 in Figure 1 illustrates the second type of redundant deployment where a *bypass switch* is designed to test a gateway DUT which directly connects to the Internet. During normal operation, the bypass switch forwards the traffic to the gateway DUT. The bypass switch also sends "hear beat" messages to poll the presence of the DUT gateway periodically. If no reply messages are received from the gateway DUT after a period of time, the bypass switch assumes the gateway DUT failed and will forward all traffic to the Internet without passing through the gateway DUT.

3.6 Solutions to Administrators -- Automated Network Management

It is a big challenge for administrators of the beta site to manage a large number of DUTs and monitor abnormal events in real time. Our solutions include use of network management tools and assisting network

monitoring by volunteers from a student club of NCTU. The IPv6 beta site adopts two management systems, Cacti and PRTG, which periodically send SnmpWalk requests for reviewing network statistics of MIB objects, such as traffic volume and port status. Upon detecting suspicious events based on abnormal network statistics, these systems *automatically* notify administrators and trace the cause of the abnormal events. As a consequence, administrators can instantly troubleshoot the failed DUTs and collect debugging information for vendors. For example, if a DUT experiences extremely high CPU loading, which results in accidental DUT rebooting, Cacti will send *three* emails to administrators reporting SNMP request failures, host disconnections, and CPU usage alert diagram. With these emails, administrators can identify the failed DUT immediately.

To provide 24-7 all year round network management puts a high demand on human resources for administrators. The IPv6 beta site gets help from a NCTU student club, Network Benefit Association (NBA), to assist the network management and operation during off-office hours. Since *members* of the NCTU NBA are also *users* of the IPv6 beta site, they also provided user experiences and feedbacks of the beta site. In particular, network failures experienced by them are reported instantly.

4 Observed Defects

During one year of beta site testing, major IPv6 features have been tested along with IPv4 features, including IPv6 addressing, IPv6 static routing, IPv6 Access Control Lists (ACLv6), Routing Information Protocol next generation (RIPng), Open Shortest Path First version 3 (OSPFv3), Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) and 6to4 Tunnel, MLD Snooping, and Protocol Independent Multicast for IPv6 (PIMv6). Totally 17 models of DUTs, switches and routers, from 3 manufacturers have been tested. All models have passed IPv6 Ready Logo. On June 8, 2011, the World IPv6 Day, numerous IPv6 services were launched around the world. The IPv6 traffic has been ten times larger in beta site since that day, and more defects were observed. To evaluate these discovered defects, appropriate evaluation matrices are necessary.

4.1 Evaluation Matrices

We evaluated those observed defects from 4 aspects: impact level, work around solution, time of occurrence, and cause of the defect. Impact level measures the impact of service failure against the network operation. Six levels of impact severity were defined that included *catastrophic*, *severe*, *normal*, *minor*, *configuration*, and *informative*. The work around matrix explains the type of work around solution, include *configuration*, *reboot*, and *unsolvable*. Time of occurrence matrix explains when the defects occurred, either (1) at *boot* time, (2) *reproducible* under certain conditions, (3) at *heavy-load*, or (4) *unpredictable*. Finally, cause of the defect explains the rationale of causing the defect. It could be related to flaws in *system design*, *memory management*, or *protocol implementation*.

4.2 Defect Overview

Table 3 summarizes the seven representative defects along with the evaluation matrices and IPv6 features. Informative errors, such as incorrect warning messages, are ignored in the discussion. We further categorize defects according to their IPv6 features into 4 classes: dual-stack with tunneling, IPv6 routing table, RIPng, and OSPFv3. All 17 models of DUTs have passed IPv6 Ready Logo before entering beta testing here. Thus, the defects reported here were not observed during testing for IPv6 Ready Logo. Apparently IPv6 Ready Logo could not catch these defects because it only tests conformance and interoperability. All defects reported here are due to flaws in system design, memory management, or protocol implementation. Though it is possible to find these defects in some other types of alpha testing, it requires specific configurations for the underlying beta site environment which is difficult to mimic in alpha testing.

Most of the reported defects happened only *once* or *twice* either because the similar configuration was not tried

Table 3 Defect Observation and Evaluation

Defect	Impact	Work around	Occurrence	Cause
Tunneling_1	Catastrophic	Unsolvable	Boot	System
Tunneling_2	Minor	Configuration	Reproducible	Implementation
Routing_Table_1	Catastrophic	Configuration	Heavy-load	Memory
RIPng_1	Normal	Reboot	Unpredictable	Memory
OSPFv3_1	Configuration	Configuration	Reproducible	Implementation
OSPFv3_2	Configuration	Configuration	Reproducible	Implementation
OSPFv3_3	Severe	Reboot	Heavy-load	Memory

again to avoid the same event, or because the manufacturers have fixed the defect after debugging. One exception is OSPFv3_3 which has happened over 10 times, where *heavy load* often incurs reboot easily.

4.3 Dual Stack with Tunneling Defects

Since the beta site adopts dual stack approach, both IPv4 and IPv6 features are configured at DUT routers, especially IPv6-over-IPv4 tunnels, such as 6to4 and ISATAP. When new IPv6 features are added to DUT routers, new IPv6 configurations may *interfere* with existing IPv4 operations. In the IPv6 beta site, such defects are observed frequently. When firmware of a DUT is upgraded to add new IPv6 features, these kinds of defects usually occur right after the DUT reboots.

Defect 1: This defect occurs when a DUT is rebooted with the new IPv6-enabled firmware, OSPFv2 neighbor state of an interface of the DUT is reset back to the Init state during the ISATAP tunnel initiation process. Since the neighbor state is *reset*, both OSPFv2 and ISATAP adjacencies cannot be *setup* and the routing entry to the neighboring peer cannot be *added* into the routing table. The impact level of this defect is classified as catastrophic as ISATAP tunnel is an important IPv6 feature. The root cause of this defect is that the ISATAP tunnel *process* took too much time which caused the OSPFv2 neighbor status *timeout*. Due to the timeout event, the neighbor state of OSPFv2 was set back to Init state. Although the OSPFv2 neighbor state could go to Full state by *disabling* the ISATAP tunneling, system *re-design* is required to fix the defect. Thus, the work around level is classified as *unsolvable*.

Defect 2: While performing 6to4 and ISATAP tunneling test, we found that some DUTs do not check *illegal IPv6 prefixes* while configuring an IPv6 address for tunnel interfaces. As a consequence, arbitrary IPv6 prefixes can be configured to 6to4 or ISATAP tunnels. The cause of this defect is thus the lack of a tunnel address prefix checking function. To work around the defect, IPv6 address prefixes configured to each interface of the DUT need to be checked *manually*.

4.4 IPv6 Routing Table Defects

IPv6 routing usually involves core routing services and much memory. If systems do not dynamically allocate sufficient memory for IPv6 routing, DUT would encounter severe system or functional defects due to memory *contention* or *exhaustion*.

Defect 1: We found that the IPv6 address cannot be configured on an interface of a DUT if the number of routing entries of its routing table is too large (over 12,000). By root cause analysis, the defect is due to the fact that IPv6 addressing and routing services share the *same* block of memory and the DUT does not allocate sufficient memory to these services. That is, the cause of this defect is due to improper memory management. The defect can be *temporarily* worked around by reducing the size of the DUT's IPv6 routing table *configuration*, while the *redesign* of the memory management of these services shall be done by the vendor. The impact level of this defect is severe.

4.5 RIPng Defects

RIPng is an essential IPv6 routing service. From our testing experience, implementation flaws of RIPng process could be observed only after a *long* period of testing time.

Defect 1: We found that, while testing RIPng and ICMPv6, RIPng daemon cannot be *disabled* after the test had been running for 30 days. The defect was fixed after the DUT was rebooted. By analyzing the cause of the defect, we found that RIPng and ICMPv6 share the *same* memory block and *memory leak* may occur to cause partial memory of RIPng being *locked*. Due to this memory leak, RIPng could not be disabled. The impact level of this defect is classified as normal as there is no essential need to disable RIPng during normal operation.

4.6 OSPFv3 Defects

A DUT usually supports many complicated OSPFv3 features, which could *conflict* with other routing services. Due to the complexity of OSPFv3 configuration, some observed defects are not DUT defects but *configuration mistakes*.

Defect 1: We found that if the Maximum Transmission Unit (MTU) is not the same for a pair of OSPFv3 *neighbors*, OSPFv3 neighbor state of a DUT would be stuck at the ExStart state and thus could not go to the Full state, i.e., running at normal state with full functionality. By analyzing the root cause of this defect, we concluded that if a DUT does not support *OSPF-MTU-mismatch-ignoring* feature, the same MTU must be configured on *adjacent* OSPFv3 neighbors.

Defect 2: Another defect observed was that the default route *disappeared* after the OSPFv3 process of a DUT started. In general, the default route is either manually *configured* or *exchanged* via routing protocols. For example, "default-information originate" must be manually configured on a Cisco router in order to exchange the default route to other routers in the same domain. If the default route is neither manually configured nor propagated from other routers, rebooting the DUT will cause the default route to disappear. Therefore, the root cause of this defect is also classified as a *configuration mistake*. The work around solution for this defect is to properly configure the OSPFv3 default route.

Defect 3: A catastrophic defect was observed when an interface encounters a large volume of IPv6 unicast traffic toward a specific IPv6 destination address, OSPFv3 and DHCPv6 services became *unstable* and eventually *terminated*. The impact level of the defect is catastrophic because of failed essential IPv6 services. By analyzing the defect, we deduced that the real cause was that, due to the heavy traffic, the IPv6 unicast process occupied *most* of the *interface memory*, which was also used by the OSPFv3 and DHCPv6 processes. Thus, the OSPFv3 and DHCPv6 processes ran out the memory, and then terminated. Although the defect can be fixed by rebooting the device or OSPFv3 and DHCPv6 processes, a new *memory management* design and implementation must be done by the vendor.

5 Conclusions

We applied dual stack and tunneling mechanisms to construct our IPv6 beta site coexisting with IPv4 to satisfy different requirements from its stakeholders: vendors, users, and administrators. We provided various test zones and debug information collection for vendors' testing purpose while providing users with high quality and seamless IPv6 services, especially the IPTV service. Besides, automated network management and topology redundancy offered administrators useful tools for operating the beta site reliably. With satisfaction from the stakeholders, the beta site has obtained a large amount of real-user-generated traffic to test vendors' IPv6 networking devices. The test cases not only included fundamental functionality and conformance tests, but also advanced stability tests. After one year of beta site operation, we observed seven representative defects, which are caused by flaws in system design, implementation logic, or memory management. We have provided detailed analysis of these defects and evaluated them from different aspects, including impact level, work around solutions, time of occurrence, and root cause. We believe that our experiences in building the IPv6 beta site, as well as the observed defects, are beneficial for future IPv6 deployment. In the future, we expect that our IPv6 beta site shall have more users and vendors involved and support more IPv6 features, such as VRRPv3, IPv6 replay, and GRE (Generic Routing Encapsulation) tunneling.

Finally, we summarize below lessons learned during the one-year beta testing period. These could be useful tips for administrators and manufacturers (or vendors).

(1) Vendors should perform alpha testing *before* undergoing more expensive beta testing.
(2) Many networking devices in operations today already have IPv6 implementations which might pass IPv6 Ready Logo or USGv6. But most of them are not yet turned on. Once turned on, they might not have conformance or interoperability issues. But there could be many stability issues to clean up, due to the flaws in system design, memory management, and protocol implementation.
(3) Administrators should avoid conflict or mismatch in configuring *different* functions, while vendors could provide utilities to check any conflict or mismatch and suggest administrators to modify the configurations when needed.
(4) *Overloading* is often the source of instability. Administrators should put a device of the right size to meet their traffic, while vendors could embed a throttling mechanism to protect the device from instability due to overloading.
(5) *Resource sharing* is another source of instability. Vendors should avoid sharing resources such as memory pools among too many functions or among big and small functions, because one exhaustive function would drain all resources and fail the other functions.
(6) *Error handling* in the functions probably is the last resort of vendors to survive through instability. Vendors should embed robust error handling to *all* function calls. For administrators, redundancy and external monitoring mechanisms are the last resort of protection.

References

[1] Y. D. Lin, I. W. Chen, P. C. Lin, C. S. Chen and C. H. Hsu, On-Campus Beta Site: Architecture Designs, Operational Experience, and Top Product Defects, *IEEE Communications Magazine*, Vol. 48, No. 12, pp. 83-91, December, 2010.

[2] IANA, *Global Policy for the Allocation of the Remaining IPv4 Address Space*, 2009, http://www.icann.org/en/general/allocation-remaining-ipv4-space.htm

[3] APNIC, *APNIC IPv4 Address Pool Reaches Final / 8*, 2011, from http://www.apnic.net/publications/news/2011/final-8

[4] A. Fiocco, *World IPv6 Launch: Impact on the Web*, 2012, http://blogs.cisco.com/news/ipv6webimpact/

[5] I. van Beijnum, *World IPv6 Launch Gets 27 Percent of Pageviews on IPv6*, 2012, http://arstechnica.com/information-technology/2012/06/world-ipv6-launch-gets-27-percent-of-page-views-on-ipv6/

[6] B. Carpenter, *Advisory Guidelines for 6to4 Deployment*, IETF RFC 6343, August, 2011.

[7] J. Arkko and A. Keranen, *Experiences from an IPv6-Only Network*, IETF RFC 6586, April, 2012.

[8] E. Nordmark and R. Gilligan, *Basic Transition Mechanisms for IPv6 Hosts and Routers*, IETF RFC 4213, October, 2005.

[9] D. Waddington and F. Chang, Realizing the Transition to IPv6, *IEEE Communications Magazine*, Vol. 40, No. 6, pp. 138-147, June, 2002.

[10] M. Tatipamula, P. Grossetete and H. Esaki, IPv6 Integration and Coexistence Strategies for Next-Generation Networks, *IEEE Communications Magazine*, Vol. 42, No. 1, pp. 88-96, January, 2004.

[11] E. Gamess and N. Morales, Implementing IPv6 at Central University of Venezuela, *The 4th International IFIP/ACM Latin American Conference on Networking*, San Jose, Costa Rica, 2007, pp. 43-51.

[12] J. Wu, J. H. Wang and J. Yang, CNGI-CERNET2: an IPv6 deployment in China, *ACM SIGCOMM Computer Communication Review*, Vol. 41, No. 2, pp. 48-52, April, 2011.

[13] A. Vallejo, J. Ruiz, J. Abella, A. Zaballos and J. M. Selga, State of the Art of IPv6 Conformance and Interoperability Testing, *IEEE Communications Magazine*, Vol. 45, No. 10, pp. 140-146, October, 2007.

[14] J. McCann, S. Deering and J. Mogul, *Path MTU Discovery for IP Version 6*, IETF RFC 1981, August, 1996.

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

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

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

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

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

[20] H. Singh, W. Beebee, C. Donley, B. Stark and O. Troan, *Basic Requirements for IPv6 Customer Edge Routers*, IETF RFC 6204, April, 2011.

[21] C. Madson and R. Glenn, *The Use of HMAC-SHA-1-96 within ESP and AH*, IETF RFC 2404, November, 1998.

[22] R. Glenn and S. Kent, *The NULL Encryption Algorithm and Its Use with IPsec*, IETF RFC 2410, November, 1998.

[23] R. Pereira and R. Adams, *The ESP CBC-Mode Cipher Algorithms*, IETF RFC 2451, November, 1998.

[24] S. Frankel and H. Herbert, *The AES-XCBC-MAC-96 Algorithm and Its Use with IPsec*, IETF RFC 3566, September, 2003.

[25] S. Frankel, R. Glenn and S. Kelly, *The AES-CBC Cipher Algorithm and Its Use with IPsec*, IETF RFC 3602, September, 2003.

[26] R. Housley, *Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)*, IETF RFC 3686, January, 2004.

[27] S. Kent and K. Seo, *Security Architecture for the Internet Protocol*, IETF RFC 4301, December, 2005.

[28] S. Kent, *IP Encapsulating Security Payload (ESP)*, IETF RFC 4303, December, 2005.

[29] D. Eastlake, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*, IETF RFC 4305, December, 2005.

[30] A. Kato, S. Moriai and M. Kanda, *The Camellia Cipher Algorithm and Its Use with IPsec*, IETF RFC 4312, December, 2005.

[31] C. Kaufman (Ed.), *Internet Key Exchange (IKEv2) Protocol*, IETF RFC 4306, December, 2005.

[32] J. Schiller, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*, IETF RFC 4307, December, 2005.

[33] P. Eronen and P. Hoffman, *IKEv2 Clarifications and Implementation Guidelines*, IETF RFC 4718, October, 2006.

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

[35] R. Droms (Ed.), *DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, IETF RFC 3646, December, 2003.

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

[37] R. Presuhn (Ed.), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*, IETF RFC 3416, December, 2002.

[38] R. Presuhn (Ed.), *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*, IETF RFC 3418, December, 2002.

[39] K. McCloghrie, D. Perkins and J. Schoenwaelder (Ed.), *Structure of Management Information Version 2 (SMIv2)*, IETF RFC 2578, April, 1999.

[40] K. McCloghrie, D. Perkins and J. Schoenwaelder (Ed.), *Textual Conventions for SMIv2*, IETF RFC 2579, April, 1999.

[41] K. McCloghrie, D. Perkins and J. Schoenwaelder (Ed.), *Conformance Statements for SMIv2*, IETF RFC 2580, April, 1999.

[42] D. Johnson, C. Perkins and J. Arkko, *Mobility Support in IPv6*, IETF RFC 3775, June, 2004.
[43] J. Arkko, V. Devarapalli and F. Dupont, *Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents*, IETF RFC 3776, June, 2004.
[44] K. Raeburn, *Encryption and Checksum Specifications for Kerberos 5*, IETF RFC 3961, February, 2005.
[45] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, *SIP: Session Initiation Protocol*, IETF RFC 3261, June, 2002.
[46] J. Rosenberg and H. Schulzrinne, *An Offer/Answer Model with Session Description Protocol (SDP)*, IETF RFC 3264, June, 2002.
[47] M. Handley, V. Jacobson and C. Perkins, *SDP: Session Description Protocol*, IETF RFC 4566, July, 2006.
[48] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart, *HTTP Authentication: Basic and Digest Access Authentication*, IETF RFC 2617, June, 1999.
[49] A. Johnston, S. Donovan, R. Sparks, C. Cunningham and K. Summers, *Session Initiation Protocol (SIP) Basic Call Flow Examples*, IETF RFC 3665, December, 2003.
[50] Y. D. Lin, P. C. Lin, T. H. Cheng, I. W. Chen and Y. C. Lai, Low-Storage Capture and Loss-Recovery Selective Replay of Real Flows, *IEEE Communications Magazine*, Vol. 50, No. 4, pp. 114-121, April, 2012.

Biographies

Ying-Dar Lin is a distinguished professor at National Chiao Tung University, Taiwan. He received his PhD from UCLA in 1993. He directs Network Benchmarking Lab which is an approved test lab of the Open Networking Foundation (ONF). He is an IEEE Fellow, IEEE Distinguished Lecturer and ONF Research Associate.

Ren-Hung Hwang received his PhD from University of Massachusetts. He is a distinguished professor of the department of Computer Science and Information Engineering and the Dean of the Engineering College at National Chung Cheng University, Taiwan. His research interests include wireless networks, Internet of Things, and cloud computing. He is a senior member of the IEEE.

Raghavendra Kulkarni is a Senior Application Engineer at Unex Technology Corporation. He defines software design methodology to complement V2X specification and addresses customer queries related to V2X Protocol Stack: ETSI ITS G5 (EU), IEEE 1609.x (US). He is a graduate of Department of Computer Science, National Chiao Tung University, Taiwan.

Chinyang Henry Tseng received the PhD degree in computer science from University of California in 2006. He is currently an Assistant Professor at National Taipei University and worked as senior software engineer at Cisco Systems Inc., and senior research scientist at Telcordia.

Chun-Hung Hsu is Executive Director at Network Benchmarking Lab, which is an approved test lab of Open Networking Foundation (ONF). He received his MS degree from NYUST. His current job focuses on designing test methodologies to test OpenFlow appliances and developing SDN application to operate SDN-enabled Wi-Fi system.