國立交通大學

網路工程研究所

碩 士 論 文

校園 IPv6 實驗網：架構、運作與經驗

On Campus IPv6 Beta Site: Architecture, Operations and Lessons

研 究 生：柯瑞固

指導教授：林盈達 教授

中 華 民 國一 百 年七 月

校園 IPv6 實驗網：架構、運作與經驗

On Campus IPv6 Beta Site: Architecture, Operations and Lessons

研究生：柯瑞固　　Student：Kulkarni Raghavendra Manohar

指導教授：林盈達　　Advisor：Dr. Ying-Dar Lin

國立交通大學

網路工程研究所

碩士論文

A Thesis

Submitted to Institute of Network Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

July 2011

Hsinchu, Taiwan

中華民國一百年七月

校園 IPv6 實驗網：架構、運作與經驗

學生：柯瑞固　　指導教授：林盈達

國立交通大學網路工程研究所碩士班

摘　　要

Betasite 測試是一種用來驗證新網路產品效能與品質的測試架構。從目前網際網路發展的趨勢來看，從 IPv4 轉換到 IPv6 是必然的趨勢。因此，在 IPv6 網路產品能夠正式被商業化之前，這些產品有需要透過一種測試環境並以真實的網路流量來驗證其品質。本篇論文的目的想要深入研究實作 IPv6 測試環境時會遇到的困難並利用此測試環境來找出各種網路產品的缺陷。我們在國立交通大學的校園網路中設計了一個針對 IPv6 架構的 Betasite，利用校園中的網路流量來幫助廠商測試各種網路產品，幫助使用者可以輕易地存取 IPv6 網路，並且也幫助校園網路管理者可以擷取與分析 IPv6 流量的特性。對於廠商而言，我們建立了一個由數個 test zone 所組成的測試環境，來測試各種類型的網路產品。對於使用者而言，我們在校園網路拓樸中佈設了一個雙堆疊(dual stack)機制。而對於校園網路管理者而言，我們建立了一個快速網路修復機制。在我們的 IPv6 Betasite 測試平台中，待測物(DUT)的路由(routing)與通道建立(tunneling)功能都已經經過為期一年的測試。在這個測試當中，我們辨識出五個 OS-level，四個 function level，兩個 kernel level 和一個 conformance level 的缺陷。大部分所觀察到的網路產品缺陷是由於協定實作和裝置設定上的問題。

關鍵字: *實驗網，雙堆疊，真實的 IPv6 測試平台，評估，穩定性，功能性，一致性*

On Campus IPv6 Beta Site: Architecture, Operations and Lessons

Student: Kulkarni Raghavendra Manohar Advisor: Dr. Ying-Dar Lin

Institute of Network Engineering

National Chiao Tung University

Abstract

Betasite testing represents a typical clinical trial, the results of which are used to validate new network devices. In view of the present Internet situation, transitioning from IPv4 towards IPv6 is inevitable. Hence, before IPv6 network devices can be transformed into commercial products, testing them under the environment of real network flow becomes essential. The purpose of carrying out this work was to understand the intricacies in IPv6 implementation with a view to spot the weak points. We design and deploy an IPv6 Betasite on the campus of National Chiao Tung University, Hsinchu, Taiwan, for vendors to test different kinds of network devices; for users to easily transfer to IPv6 network and for network administrators to capture and analyze IPv6 traffic. For vendors, we establish environments such as an array of test zones for testing different types of network devices. For ease of operation to the users, we employ the dual stack mechanism in our campus network topology. For network administrators we establish mechanisms of speedy network recovery. In our IPv6 Betasite testbed, addressing, routing, tunneling and administrator supporting test cases were designed and tested for the duration of one year. In these tests, we identified 5 OS-level, 4 function level, 2 kernel level and one conformance level defects. Most of the defects were due to protocol implementation issues and few of them due to configuration issues.

Keywords: Betasite, dual stack, real IPv6 testbed, evaluation, stability, functionality, conformance

Contents

List of Figures

List of Tables

Chapter 1: Introduction

Betasite testing represents a typical clinical trial, the results of which are used to validate new network devices. In view of the present internet situation, transitioning towards IPv6 is inevitable. Hence, before IPv6 network devices can be transformed into commercial products, testing them under the environment of real network flow becomes essential.

Table 1: Comparison between Beta site test and Lab test

Parameter	Betasite test	Lab test
Traffic	Real and complex	Fake and monotonous
Applications	Complex and keep updating	Old and monotonous
Replay technique	Real traffic environment	Lab test methodology
IPv6 real environment	Yes	Not sure
Reduce CFD	Yes	No
Programs made by users	Yes	No
Tested under many NICs	Yes	No

From Table 1 it can be observed that Betasite test is more efficient than lab test as the traffic on which the device is being tested is real and complex in nature. Moreover, it has been proved that product quality improves through betasite testing [1].

The design of our campus IPv6 Betasite can be viewed from three perspectives: that of vendors, that of betasite users and that of network administrators. Vendors demand diverse test environments for testing broad range of network products. Users demand ease of operation and maintaining end-to-end connectivity, while network administrators desire convenience of testing and network recovery.

For easy transfer to IPv6 [2] network, there are three transition mechanisms: dual stacks, tunneling and translation [3], which can be deployed in several ways [4] depending on the need. Dual stack mechanism [5] facilitates IPv4 and IPv6-enabled applications to operate on the same node. Tunneling at different points [6, 7] is required to pass through a network that does not have native IPv6 support in which IPv6 packet is encapsulated within an IPv4 packet and sent onto the IPv4 network. If IPv4-based clients need to access IPv6-based servers, and vice versa, then translation mechanisms [8] are employed.

With respect to this, there are several studies that deploy IPv6 in campus networks to address different issues such as to solve the problem of IPv4 address exhaustion [9, 10], to enable the introduction of IPv6-only devices into the network [11] and for research and education [12]. There are many participants involved in the development [13-14] and validation of IPv6 products [15]. Several studies propose formal languages for IPv6 testing [16, 17] while some works review IPv6 conformance and interoperability testing initiatives [18, 19]. However, none of them perform stability testing of IPv6 supported network products. The novelty of our work is emphasized by the fact that no previous work attempts to test IPv6 supported network products under the environment of real network flow. Neither there are studies that design test cases to evaluate stability of network products.

In our IPv6 Betasite testbed, we perform stability testing of network products considering 'duration' as a critical factor. In order to obtain a real flow certificate, a network product must show full compliance to certain criteria: (a) Major criterion – product functions work stably over 4 weeks (over 720 hours) in field test and in replay test in an environment consisting of more than one thousand users. (b) Minor criterion – products pass the tests on primary functionality and performance. If a product acquires a realflow certificate, it indicates that the stability of the product is good under the environment of real network flow. Moreover, the product works normally and steadily at user side without unstable situations, such as crashing, lowering speed, re-booting, frequently disconnecting. Currently the certification service is provided for Security Appliance (ex. UTM, Anti-Virus, IPS), SOHO Router, IAD, Gateway, and DSL Router.

In this work, we design an On Campus IPv6 Betasite for vendors to test different types of network devices; for users to provide seamless access to IPv6 applications and services; for network administrators to capture and analyze IPv6 traffic. For vendors, we setup environments such as array of test zones for testing different types of network devices. For ease of operation to the user, we employ dual stack mechanism in our campus network topology. For network administrators we setup mechanisms of speedy network recovery. Furthermore, we identify some common IPv6 defects of network products deployed in our testbed.

The rest of this work is organized as follows: Chapter 2 gives adequate background that facilitates understanding of IPv6 betasite functioning and discusses the needs of vendors, betasite users and network administrators. Chapter 3 describes our methodology for satisfying these needs. Chapter 4 discusses some of the common IPv6 defects found in network products deployed in our testbed. Finally, Chapter 5 concludes this work and discusses the future works.

Chapter 2: Background for IPv6 Betasite

2.1 IPv6 features in Betasite

- **Addressing in IPv6 Betasite**

In our IPv6 Betasite, we have employed the automatic stateless addressing scheme [20] for address configuration. Most of the betasite users have end systems with native IPv6 support. They obtain an IPv6 address by the following procedure: The betasite core router (as shown in figure 1) helps nodes in the autoconfiguration process by sending RAs (Router Advertisements). A RA is an ICMPv6 message periodically sent by the core router or on request of a node. When a node is powered on, it first derives its link-local address from its MAC address. With this address, the node can communicate within the link since link-local addresses are not routed. Then, the node tries to discover local routers by sending an ICMPv6 message called Router Solicitation (RS). Betasite core router on the link will answer with a RA. RA will include Prefix options, which the node will use to configure itself with additional IPv6 addresses derived from the advertised prefixes. In the meanwhile, when a host name to an IPv6 address needs to be resolved, host can make a DNS query using IPv4 and receive quad A resource records.

- **Routing in IPv6 Betasite**

In our IPv6 Betasite, we have employed dynamic routing protocols RIP, OSPF, BGP for routing IPv4 traffic while RIPng, OSPFv3 [21, 22] for routing IPv6 traffic. As IPv6 is already initialized on the system, IPv6 routing table is generated automatically. IPv6 routing tables essentially represent the routes which are as follows: (a) Host routes: that identify a specific IPv6 node and contain 128-bit prefixes (b) Network routes which are directly attached: that identify the adjacent links and contain 64-bit prefixes (c) Remote network routes: that identify the remote links and they have varying prefixes (d) Default route: this is used when a host route cannot be determined. It uses the network prefix ::/0. When an IPv6 packet arrives at a network interface, the host adopts one of the following methods in order to determine how to forward the packet to its destination: (a) checking the destination cache which should match with the address in the packet header.

In such cases, host forwards the packet directly to the address and the routing process ends. (b) If the destination address in the packet header and the destination cache do not match, then the host uses local routing table to determine the forwarding mechanism using next-hop address and next-hop interface which work in tandem.

- **Multicasting in IPv6 Betasite**

In our IPv6 Betasite, we employ the Protocol Independent Multicast Sparse Mode (PIM-SM) multicast routing protocol [23] for routing multicast streams between VLANs, and subnets. It is responsible for constructing distribution trees and forwarding multicast packets and facilitates the exchange of information between routers. A detailed description on how multicast packets are transmitted in IPv6 betasite is given in next chapter.

- **Roles of IPv6 Betasite key players**

In our IPv6 Betasite, there are three key players whose concerns need to be addressed in a systematic manner. The key players are: (1) Vendor (2) Betasite user (3) Network administrator.

(1) Vendor

The role of a vendor is of an experimentalist who requires an appropriate and customized testing ground for testing various IPv6 supported network devices.

(2) Betasite user

In our campus, totally there are three services provided for easy access to internet: The first one is a regular network and the second one is NCTU wireless. The third one is Betasite network, provided by Network Benchmarking Lab in association with Computer Center, which has about 1000 users. In this project, it is proposed to adopt all the students who have subscribed to Betasite network as users.

(3) Network administrator

The roles of a network administrator in this project are multi-faceted, beginning with the testing of a device to balancing the requirements of user and vendor.

The roles which are most crucial for this project are as follows: (a) check DUT for stability issues such as: crash, reboot, lowering speed and others (b) check DUT supported features (c) check DUT incompatibility issues (d) maintain balance between user and vendor.

2.2 Concerns in Building an IPv6 Betasite

From the point of view of Vendor, the possible concerns are as follows:

- **Array of test zones**

Due to the growing number of IPv6 supported network devices such as: L3 switches, core routers, security appliances, residential gateways and so on, the Betasite must provide wide range of environments to test these devices.

- **Debugging**

The facility that Betasite extends through IPv6 in a few instances may not fulfill the demands of the vendor. In some cases, vendor may design new features and would want to test them. Betasite must provide such facility which would assist in fixing the defects.

From the point of view of Betasite User, the possible concerns are as follows:

- **Easy migration to IPv6**

Noticing the number of devices that have become web-enabled (smart phones and other electronic equipment such as televisions, cameras and even cars), it becomes unbearable to provide internet access to them using IPv4. If those devices should continue to function in the same way, IPv6 is the ideal solution. However, expecting users to configure their IPv6 address, like the way they do for IPv4 is impractical, since IPv6 has 128-bit addressing scheme. Hence for user convenience, Betasite must provide mechanisms for easy transfer to IPv6.

- **Access to IPv6 enabled services**

As we move to IPv6, there is an increasing demand for bandwidth-intensive applications such as online video, IP-based telephony services from the users. Betasite must provide support for IPv6 enabled applications and services.

From the point of view of Network administrator, the possible concerns are as follows:

- **Speedy network recovery**

Minimizing network downtime is a critical task. It is obvious that a network topology consisting of many network components may incur failures such as link failure, node failure and others. Hence, it is necessary to ensure that there are fewer network failures and more productivity. In addition to providing adequate hardware support for IPv6, Betasite must provide mechanisms for speedy network recovery thereby maintaining connectivity.

- **Status reporting and maintenance team**

Delivery of desired service with appropriate feedback mechanism from customers would assist network administrators in understanding user necessities and technical hitches. Betasite must have a maintenance team for its continued growth and success.

2.3 Protocol procedure formats

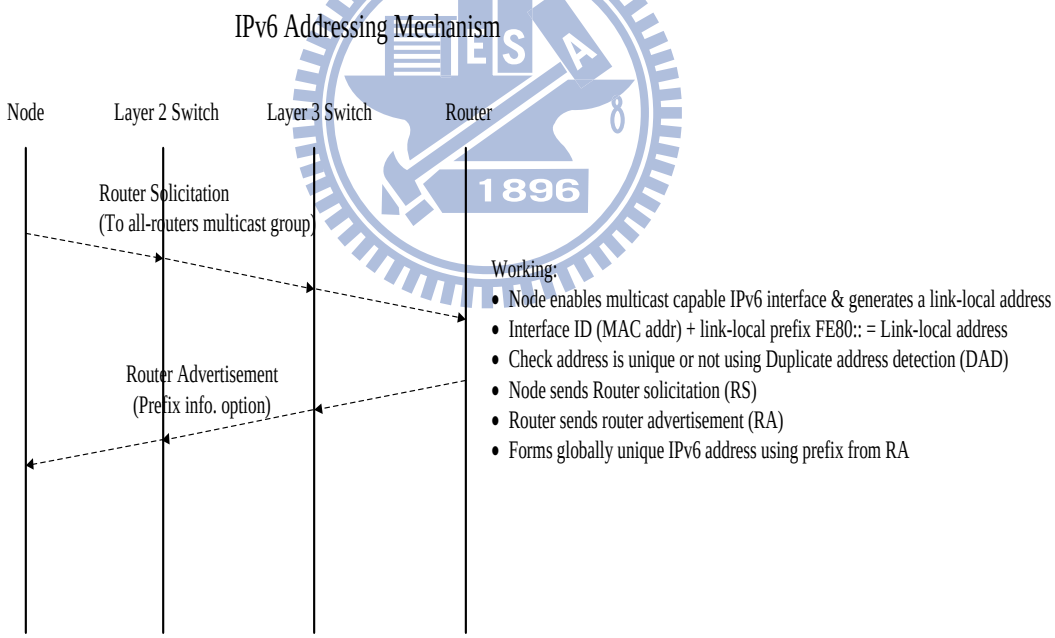


Figure 1: Protocol procedure format (Addressing)

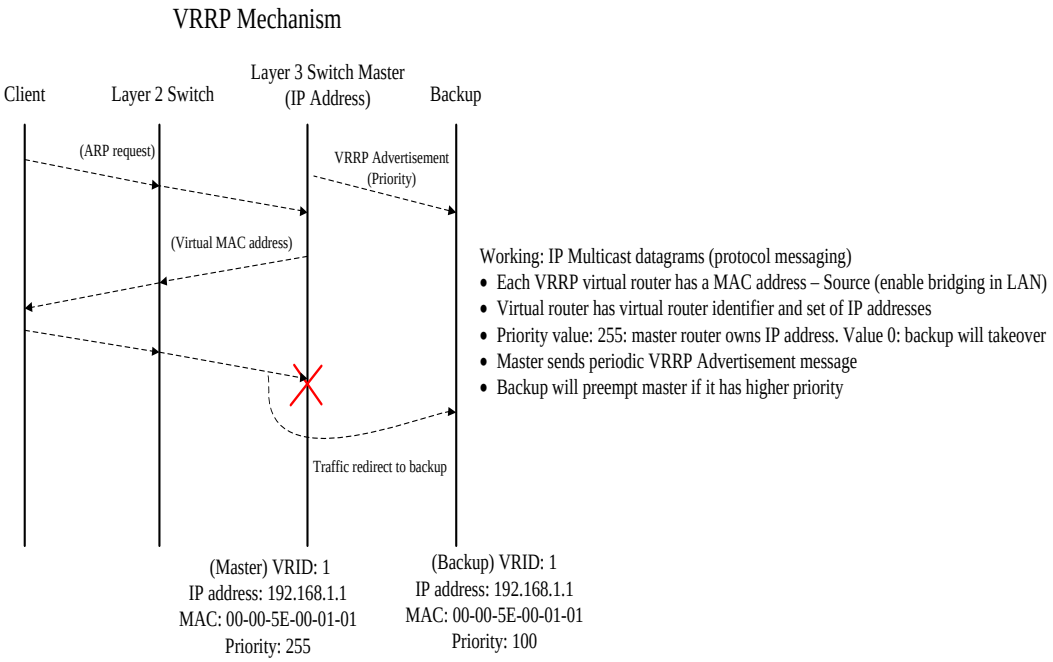


Figure 2: Protocol procedure format (Network recovery)

Chapter 3: IPv6 Betasite Architecture Designs

In this chapter, we address the concerns of Vendors, Betasite users and network administrators as discussed in chapter 2.

3.1 To satisfy concerns from Vendors

- **Solutions to the first concern: Array of test zones**

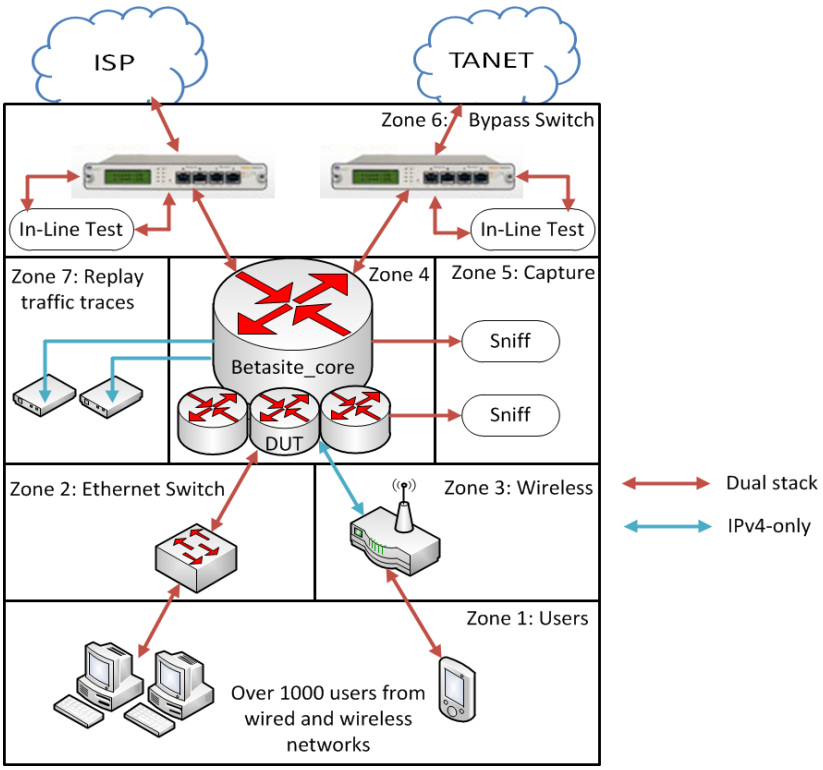


Figure 3: Structure of IPv6 Betasite

Figure 3 shows the IPv6 Betasite network topology, which provides seven test zones. To ensure adequate hardware support for IPv6, 24 stackable and 2 chassis based switches have been deployed. We have about 20 prefixes with 64-bit prefix length.

All prefixes are in the range of 2001:f18:113:/48. Each zone provides a unique test environment for testing network devices depending upon their capability and requirements. There are more than 1000 IPv6 users in the dormitory network which comes to zone 2, zone 3 and links to the Ethernet switch and wireless access points. Then it passes through the Core Router in zone

4 to access ISP and TANET. IPv6 users in zone 1 generate diverse and complex traffic as they use different operating systems and access wide range of applications and services.

This traffic is captured in zone 5 and replayed in zone 7 for troubleshooting and debugging DUT defects. Packet sniffing is performed in zone 5 to serve two purposes. One reason is to capture and store IPv6 traffic and another reason is to test devices in offline mode. We use a high performance interface card (DAG card) to capture and store the mirrored packets from Betasite core router. Unlike regular network interface cards, the DAG cards are optimized for sustained performance under extreme load conditions. We make use of a content filter to test devices in sniff mode. In our IPv6 Betasite, we test wide variety of IPv6 supported network devices such as core routers, layer 3 switches in zone 4, IPS/IDS, residential gateways in zone 6 and SOHO routers in zone 7. Apart from that we also provide customized environments for testing network devices that are not in current Betasite architecture.

- **Solutions to the second concern: Debugging**

We provide customized environment in Betasite depending upon the needs of the vendor to debug the newly created functions. Moreover, we also provide traffic to the vendor in case he is performing a private debug operation. The ultimate purpose of providing this traffic is to enable the vendor to carry out the relevant DUT debugging operation. To exercise our control in this operation, the traffic provided is anonymized thereby preventing the misuse of this facility by the vendor.

3.2 To satisfy concerns from Betasite users

- **Solutions to the third concern: Easy migration to IPv6**

Figure 4 shows part of our campus network topology which includes more than 1000 users located in the dormitories. Majority of the users employ those systems which have built-in IPv6 support. For them, access to IPv6 is provided by employing routers that have dual stack support. The preferred mechanism for interoperation with legacy nodes is to use dual-stack and thus IPv4 to communicate to IPv4 nodes and IPv6 to communicate to IPv6 nodes. Users get IPv6 address through stateless address autoconfiguration mechanism configured in layer 3 switches. Routing for the dual stack model is set up using RIP, OSPF, BGP protocols for IPv4 and RIPng, OSPFv3 protocols for IPv6.

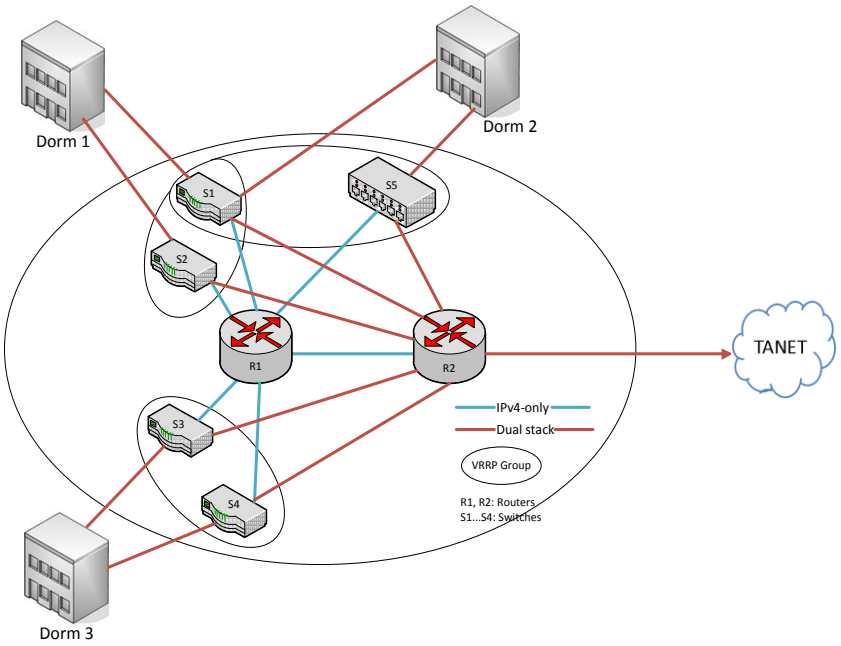


Figure 4: NCTU Campus network topology

- **Solutions to the forth concern: Access to IPv6 enabled services**

Betasite allows the users to gain seamless access to several IPv6 applications such as: Web, P2P, FTP, SSH, Telnet and others. One of the special services that we provide to IPv6 Betasite users which is exclusively because of IPv6 is Internet Protocol Television service, called IPTV. The process of how a user gets access to IPTV service is described below.

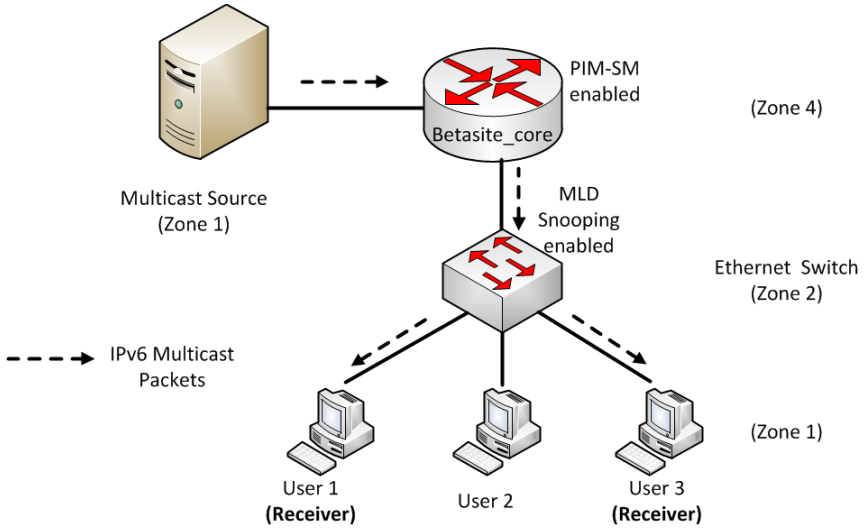


Figure 5: IPv6 Multicast packet transmission in IPv6 Betasite

Figure 5 shows multicast packet transmission in IPv6 Betasite. After installing VLC media player on the source as well as clients, streaming of video can be started to a source specific multicast group using VLC. PC running Ubuntu is used as a Multicast Source while Protocol Independent Multicast (PIM) routing is enabled on the betasite core router that enables the IPv6 hosts to join a network wide multicast group. With MLD snooping enabled on layer 2 switches, we control the distribution of multicast traffic only on those ports that are actively listening. To receive a particular multicast data stream, hosts join IPv6 multicast groups by sending an unsolicited MLD report to Betasite core router. In response to a snooped MLD report, the switch creates an entry in its Layer 2 forwarding table for the VLAN on which the report was received. When other hosts that are interested in this multicast traffic send MLD reports, the switch snoops their reports and adds them to the existing Layer 2 forwarding table entry.

Betasite core router is responsible for replicating the source content and forwarding it to multiple recipients. It uses the PIM protocol to build distribution trees for multicast routing in the network and Reverse Path Forwarding (RPF) techniques to ensure content is forwarded to the appropriate downstream paths without routing loops.

3.3 To satisfy concerns from Network Administrators

- **Solutions to the fifth concern: Speedy Network recovery**

As shown in figure 2, there are two layer 3 switches for each dormitory. For continuous connectivity, automatic network recovery and auto redirect traffic, every layer-3 switch is connected to both R1 and R2. Network recovery is achieved by using the Neighbor Unreachability Detection mechanism provided by Neighbor Discovery (ND) protocol. This is done by sending unicast Neighbor Solicitation messages to the neighbor host. By this process, it will take a host about 38 seconds to learn that a router is unreachable before it will switch to another default router. While testing devices in zone 6, a bypass switch modified for IPv6 usage is used for network recovery. It contains an editable heartbeat packet in which we fill IPv6 values to test the DUT status. The bypass switch periodically sends heartbeat packets to check whether the DUT can forward the heartbeat packets back to it, and this period is determined by a configurable timer. When the number of lost heartbeat packets exceeds a threshold decided by a configurable counter, the bypass mode is turned on thereby recovering the network.

- **Solutions to the sixth concern: Status reporting and maintenance team**

The success of application of Betasite is monitored by the following feedback mechanism. It involves instantaneous report of the status of the on-going operations through a student club, known as Network Benefit Association, who are the actual beneficiaries of this plan. Further, there is a separate maintenance team which handles the technical aspects associated with the execution of this plan.

Chapter 4: Test case design and Observations

Since IPv6 beta site has been designed taking into account the concerns of user, network administrator and vendor, we design test cases in order to verify the correctness of their implementation by the DUT. From the user's perspective, addressing, routing and tunneling are the most commonly used services. Our test cases focus on these three aspects. Furthermore, for network administrator ICMPv6, Ping6, DHCPv6, SSH are most critical services. We design test cases for their support.

4.1 Terminology

Following terminology applies for the defects found. Level: indicates the root cause. Can be categorized into -

- OS level: function error in DUT
- Kernel level: hanging, reboot, memory leak, CPU usage too high in DUT
- Function level: DUT does not provide the assured feature
- Conformance level: DUT does not conform to RFC
- Hardware limitation: function is not supported by DUT
- Deterministic problem: occurs repeatedly, can be reproduced

4.2 Topology

Test Environment for DUT:

Figure 6 shows sample DUT that were being tested in our IPv6 Betasite testbed over a period of 1 year. 6to4, ISATAP tunneling mechanisms were setup on DUT1 and DUT 2 while Static route, OSPFv3 and RIPng routing protocols were setup on DUT2 to evaluate their functionality and conformance. If DUT1 fails, traffic is redirected to betasite core router so that continuous connectivity is maintained. Since DUT 1 and DUT 2 use the same firmware version, they would fail at the same time. If DUT 3 fails, DUT 4 will take over in 38 seconds by the neighbor unreachability mechanism. Hence, we provide double backup mechanism for speedy network recovery and auto redirect traffic. The test cases and defects found are explained in the next section.

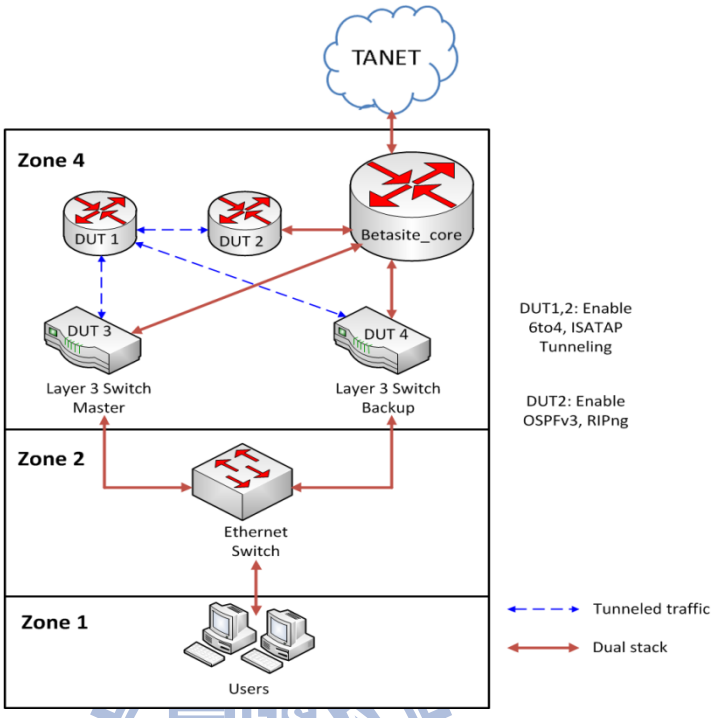


Figure 6: DUT testing methodology in IPv6 Beta site

- **Client statistics:**

Based on the pcap file captured at the beta site core router, we employ a heuristic approach and determine that 80% of the beta site users are IPv6 users.

4.3 User related test cases

- **Topic: IPv6 addressing**

Though we provide stateless address auto configuration for the users, network administrators still need to perform manual configuration on routers. The following test case describes this aspect, wherein we try to add new IPv6 address to the DUT. We found that IPv6 address of newly created DUT interface could not be configured, due to lack of adequate hardware support.

Table 2: Addressing related test cases

Test case 1:	**Test case 2:**
Objective: Test IPv6 address configuration for functionality Procedure: 1. Connect cable to eth 1,3,5,7 and 9. 2. Add new IPv6 address to DUT Configuration: 1. show ip int vlan80 (to check configuration of interface) 2. Interface vlan80 (enter vlan80) 3. IPv6 address 2001:f18:113:2421::6604/64 (add IPv6 address) Result: Cannot configure IPv6 address of newly created DUT interfaces Defect: Hardware Limitation (deterministic problem)	Objective: Test IPv6 address configuration for functionality Procedure: 1. Create VLAN interface 2. Assign IPv6 address to the interface Configuration: 1. Interface vlan450 2. IPv6 address 2001:f18:113:2495::FF Result: One IPv6 address of DUT loses its communication ability Defect: OS level (non-deterministic problem)

- **Topic: IPv6 routing**

Functionality, conformance and stability testing of commonly used IPv6 routing protocols such as static route, ripng and ospfv3 has been performed. We report the problems encountered during their operation and fixed solutions in few cases. Stability testing of RIPng protocol for a duration of 30 days resulted in non-deterministic problem wherein IPv6 routes learnt from RIPng protocol were not erased from the routing table. Similarly, functionality testing of static route and OSPFv3 protocols resulted in not being able to write the default IPv6 route into the routing table. Moreover, web GUI configuration of IPv6 router advertisement function disables ospf and vrrp state. However, CLI configuration worked fine.

Table 3: Routing related test cases

Test case 3:	**Test case 4:**
Objective: Test ICMPv6, RIPng routing protocol for stability Procedure: 1. Enable RIPng function on DUT 2. Wait 30 days 3. Disable RIPng function Configuration: 1. router rip 2. no router rip Result: DUT cannot get ICMPv6 response from its own IP interface Defect: Kernel level (non-deterministic problem)	Objective: Test OSPFv3 routing protocol for functionality Procedure: 1. enable ospfv3 function on DUT 2. display database summary Configuration: 1. Configure terminal 2. router ipv6 ospf 3. show ipv6 ospf database Result: OSPFv3 status cannot become 'FULL' after DUT reboot

	After reboot, ospf state is always exchange/loading Solution: clear ipv6 ospf Defect: Functional level (deterministic problem)
Test case 5: Objective: Test RIPng routing protocol for functionality Procedure: 1. enable ripng function on DUT Configuration: 1. configure terminal 2. ipv6 router rip Result: DUT will prompt '% invalid interface' when rip is enabled Solution: 1. no ipv6 router rip 2. ipv6 router rip Defect: Functional level (deterministic problem)	**Test case 6:** Objective: Test static route, OSPFv3 routing protocols for functionality Procedure: 1. Enable OSPFv3 function 2. Create ipv6 route 3. Delete ipv6 route 4. Disable OSPFv3 function Configuration: 1. Create IPv6 default route ::/0 2001:f18:113:fe80::ff 2. Show ipv6 route (default route not shown in routing table) 3. Ping ipv6 address (no route to host) 4. No router ipv6 ospf (disable OSPFv3) Result: Creation of IPv6 default route gets merged with OSPFv3 routes Defect: Kernel level (non-deterministic problem)
Test case 7: Objective: Test RIPng routing protocol for conformance Procedure: 1. Enable RIPng function 2. Check routing table Configuration: 1. router rip 2. show ipv6 rip database Result: absence of timer and flag field in routing table Defect: Conformance level (deterministic problem)	**Test case 8:** Objective: Test IPv6 RA function Procedure: 1. Enable IPv6 RA function Configuration: 1. Use web gui to configure IPv6 RA 2. Configure lifetime, interval, reachable time Result: disabling of ospf state and absence of vrrp configuration Defect: OS level (deterministic problem)

- **Topic: IPv6 tunneling**

Functionality tests of 6to4 and ISATAP tunneling schemes is performed. We found a peculiar problem with respect to their addressing, wherein the DUT does not check the address format of either scheme while forming an IPv6 address. Addresses which are not in the prescribed range can still be created.

Table 4: Tunneling related test cases

Test case 9: Objective: Test 6to4 tunneling protocol for functionality Procedure: 1. Enable 6to4 tunneling function on DUT 2. Configure IP address in abnormal range Configuration: 1. interface tunnel1 2. tunnel source 140.113.252.61 3. tunnel mode ipv6ip 6to4 4. ipv6 address 2002:8c71fc3d:1::1/64 Result: DUT does not check the address format of 6to4 tunnel IPv6 address Defect: Function level (deterministic problem)	**Test case 10:** Objective: Test ISATAP tunneling protocol for functionality Procedure: 1. Enable ISATAP tunneling function on DUT 2. Configure IP address in abnormal range Configuration: 1. interface tunnel1 2. tunnel source 140.113.252.61 3. tunnel mode ipv6ip ISATAP 4. ipv6 address 2002::5efe:8c71fc3d Result: DUT does not check the address format of ISATAP tunnel IPv6 address Defect: Function level (deterministic problem)

4.4 Network administrator related test cases

There are certain quintessential services that a network administrator needs to check to ensure smooth operation of the network such as: Pingv6, DHCPv6 and SSH. Functionality test of SSH function resulted in the conclusion all of a sudden DUT closes the established ssh session. While from stability test of Ping6 and DHCPv6 functions, we observe that they fail after duration of 10 days.

Table 5: Administrator supporting test cases

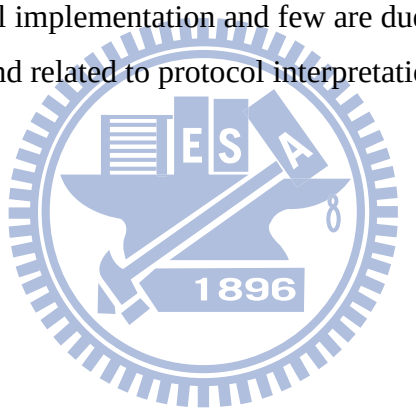
Test case 11: Objective: Test Ping6 for functionality Procedure: 1. Execute ping6 function Configuration: 1. Ping :: Result: If destination address is unspecified IPv6 address, DUT replies ‘Ping6 task is busy’ Defect: OS level (deterministic problem)	**Test case 12:** Objective: Test SSH for functionality Procedure: 1. Execute SSH function Configuration: 1. Establish ssh connection with DUT 2. show ip ssh Result: DUT closed SSH session unexpectedly Defect: OS level (non-deterministic problem)
Test case 13: Objective: Test Ping6, DHCPv6 functions for stability Procedure: 1. Execute ping6, DHCPv6 function Configuration: 1. ping 2001:e10:5c00:2::101:150 2. show ipv6 dhcp Result: Ping6, DHCPv6 functions fail after booting for 10 days	

DUT can not ping its IPv6 address Defect: OS level (non-deterministic problem)

Table 6: Defects Summary

Feature	Protocol interpretation issue	Protocol implementation issue	Configuration issue
Addressing	-	Case 1, 2	
Routing	-	Case 3 to 10	Case 4
Tunneling	-	Case 11, 12, 13	

In our IPv6 Betasite, we have tested the above IPv6 related functions provided by vendor 'A' for a router that was under test for duration of 1 year. The purpose of carrying out this work is to understand the intricacies in implementation with a view to spot the weak points and provide remedies on a test site. Table 6 shows a summary of the defects that we have identified. Most of the failures are due to protocol implementation and few are due to configuration issues. So far, no specific failed cases were found related to protocol interpretation issue.



Chapter 5: Conclusion and Future works

In this work, we have proposed a Betasite architecture for testing IPv6 supported network devices. Moreover, we have designed test cases for functionality, conformance and stability testing of IPv6 features in network products. Most common IPv6 implementation problems were found in protocol implementation and configuration issues. In the future, we plan to recruit more users to diversify the network traffic in Betasite. We also plan to add more IPv6 supported testing environments and features such as: VRRPv3 (in zone 4), IPv6 supported replayer (in zone 7) and GRE tunneling (Generic Routing Encapsulation) in our IPv6 Betasite.

References

[1] Ying-Dar Lin; Chen, I-Wei; Po-Ching Lin; Chang-Sheng Chen; Chun-Hung Hsu; , "On campus beta site: architecture designs, operational experience, and top product defects," Communications Magazine, IEEE , vol.48, no.12, pp.83-91, December 2010

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

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

[4] Tatipamula, M.; Grossetete, P.; Esaki, H.; , "IPv6 integration and coexistence strategies for next-generation networks," Communications Magazine, IEEE , vol.42, no.1, pp. 88- 96, Jan 2004

[5] E. Nordmark, et al. “Basic Transition Mechanisms for IPv6 Hosts and Routers.” RFC 4213, 2005

[6] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[7] F. Templin, et al. “Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)”. RFC4214, 2005.

[8] Tsirtsis, G. and P. Srisuresh. "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.

[9] Eric Gamess and Neudith Morales. 2007. Implementing IPv6 at Central University of Venezuela. In*Proceedings of the 4th international IFIP/ACM Latin American conference on Networking* (LANC '07). ACM, New York, NY, USA, 43-51.

[10] Jianping Wu, Jessie Hui Wang, and Jiahai Yang. 2011. CNGI-CERNET2: an IPv6 deployment in China. SIGCOMM Comput. Commun. Rev. 41, 2 (April 2011), 48-52.

[11] Chown, T.; , "IPv6 Campus Transition Experiences," Applications and the Internet Workshops, 2005. Saint Workshops 2005. The 2005 Symposium on , vol., no., pp. 46- 49, 31-04 Jan. 2005

[12] Homer Carlisle and Bliss Bailey. 2008. Enabling IPv6 within a campus network. In Proceedings of the 46th Annual Southeast Regional Conference on XX (ACM-SE 46). ACM, New York, NY, USA, 454-457.

[13] Esaki, H.; Kato, A.; Murai, J.; , "R&D activities and testbed operation in WIDE project," Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on , vol., no., pp. 172- 177, 27-31 Jan. 2003

[14] Chown, T.; , "IPv6 initiatives within the European National Research and Education Networks (NRENs)," Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on , vol., no., pp. 149- 152, 27-31 Jan. 2003

[15] (2009) IPv6 Ready Logo Program website. [Online] Available: http://www.ipv6ready.org

[16] J. Tian, L. Zhongcheng, “The next generation Internet protocol and its test”, IEEE International Conference on Communications (ICC’01), Volume: 1, June 2001, pp. 210-215.

[17] Z. Yujun, L. Zhongcheng, “A new formal test suite specification language for IPv6 conformance testing”, Proceedings of International Conference on Communication Technology (ICCT ‘03), Volume: 1, April 2003, pp. 174-7.

[18] Ruiz, J.; Vallejo, A.; Abella, J.; , "IPv6 conformance and interoperability testing," Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on , vol., no., pp. 83- 88, 27-30 June 2005

[19] Vallejo, A.; Ruiz, J.; Abella, J.; Zaballos, A.; Selga, J.M.; , "State of the Art of IPv6 Conformance and Interoperability Testing," Communications Magazine, IEEE , vol.45, no.10, pp.140-146, October 2007

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

[21] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

[22] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

[23] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.