How much can we survive on an IPv6 network?

Experience on the IPv6 only connectivity with NAT64/DNS64 at WIDE camp 2011 autumn

Hiroaki Hazeyama
NAIST
8916-5 Takayama
Ikoma, Nara, Japan
hiroa-ha@is.naist.jp

Ukito Ueno
Keio University
5322 Endo
Fujisawa, Kanagawa, Japan
eden@sfc.wide.ad.jp

Hirotaka Sato
Keio University
5322 Endo
Fujisawa, Kanagawa, Japan
hirotaka_sato@wide.ad.jp

Yuudai Yamagishi
Keio University
5322 Endo
Fujisawa, Kanagawa, Japan
yummy@sfc.wide.ad.jp

Takehiro Yokoishi
Keio University
5322 Endo
Fujisawa, Kanagawa, Japan
dokan@sfc.wide.ad.jp

Hisatake Ishibashi
The University of Tokyo
7-3-1 Hongo
Bunkyo, Tokyo, Japan
take@hongo.wide.ad.jp

ABSTRACT

This paper reports users' experiences on the WIDE Project conference network (camp-net) held in Sep. 6th to Sep. 9th in Matsushiro Royal hotel, and tries to describe the problems on IPv4 / IPv6 transition techniques. In the camp-net, the IPv6 only connectivity was achieved by DHCP6, NAT64 and DNS64, and was served as main connectivity for participants on the conference. Also IPv4 connectivity through SA46T or 4RD were served as optional connectivity. We explain the summary of our experiments on the camp-net with results of questionnaire and analysis of reported troubles.

Categories and Subject Descriptors

C.2.3 [**Network Operations**]: [Network management, Network monitoring, Public networks]

General Terms

Experimentation

Keywords

IPv6, NAT64, DNS64, DHCP6, SA46T, 4RD, Availability, Questionnaire

1. INTRODUCTION

Through experience of the world IPv6 day, the transition from IPv4 networks to IPv6 networks has reality. In Japan, several carriers and ISPs have started the IPv6 Internet services to home users. At the current situation, the majority of transition techniques are composed by dual stack techniques, however, the non-dual stack approaches must be considered, evaluated and documented along with the exhaustion of IPv4 global addresses.

In this paper, we report users' experiences and problems on IPv4 / IPv6 transition techniques in the WIDE Project conference network (camp-net), which was conducted in Sep. 6th to Sep. 9th at Matsushiro Royal hotel (Nagano prefecture). On the camp-net, we tested an IPv6 only connectivity environment by DHCP6 [1], stateful NAT64 [2] and DNS64 [3], as the main connectivity for participants on the conference. The camp-net also served two IPv4 connectivity environments through SA46T [4] or 4RD [5] as optional connectivity. In the following sections, we explain the summary of our experiments on the camp-net.

In Section 2, we refer the past experiments of the IPv6 only connectivity on conferences, and we explain the settings of the camp-net in Section 3. Section 4 presents the results of questionnaire about the availability of the camp-net and describes the reported problems on the NOC team. After discussing open issues and our recommendation on the IPv4 / IPv6 transition in Section 5, we conclude this paper with our future work.

2. RELATED WORK

The report by Arkko et.al in [6] well describes the current problems of the IPv6 only network with NAT64 and DNS64 through experiments on IETF meetings. Problems figured in the IETF's experiments about the IPv6 only networking with NAT64 and DNS64 were as follows;

Some pains due to the fallback routine

In the section 4 of [6], Arkko et.al reported some pain due to the fallback routine, many of which were broken by switching off the IPv4 property. They categorized the reasons of pain as follows; i) bugs, ii) lack of IPv6 support, iii) protocol, format, and content problems, iv) firewall issues.

Also, Arkko et.al mentioned the MTU (Maximum Transfer Unit) size would be potentially cause of pain.

Operating Systems

In the experiences of Arkko et.al, they met several problems on Linux, Mac OS X, Windows 7, Android.

Instant Messaging and VoIP

According to [6], many of instant messaging and VoIP clients,

AWFIT '11 Bangkok, Thailand

which do not use HTTP or XMPP, did not work well or stopped working.

Gaming
Except of web-based games, almost of all games did not work. Arkko et.al suspected the main reason would be the use of an IPv4-literal in the application itself.

Music Services
Arkko et.al reported that most of the web-based music services appear to work fine, presumably because they employ TCP and HTTP as a transport, however, some music service which uses IPv4 address, would need a proxy configuration.

Appliances
Arkko et.al mentioned that appliances such as webcams or firewalls may not support IPv6 yet. Also, Arkko et.al pointed that fragments will become problems.

IPv4 Address Literals
In [6], the access to web sites were tested by wget, then, 2.1 % of samples of URLs were failed. The failure of web sites, which were accessed from the IPv6-only network via a NAT64 device, were mainly caused the IPv4 address literals.

Actually, we did not know the Arkko's experiences until we started writing this report. We met problems as well as Arkko did, also we got differences of the Arkko's experiences and new tips on the IPv6 only networking with NAT64, DNS64 and DHCP6. Here, we described our experience in following sections.

3. THE CAMP 1109 NETWORK

In this section, we describe the overview of the camp 1109 network (camp-net) and the purposes of these experiments. We also figure the summary of technical aspects on the camp-net.

3.1 Overview

Four official experiments were conducted by the NOC team; **i)** the capability and availability test of DHCP6, **ii)** the capability and availability test of NAT64 / DNS64 as of a last resort technique to IPv4 networks from an IPv6 network, **iii)** the capability and availability test of SA64T as a last resort technique for IPv4 users / applications in an IPv6 network, **iv)** WPA2 Enterprise EAP-TLS capability tests for participants. Also, one additional experiment, which tested the capability and availability of 4RD, was conducted by an experiment team composed of IIJ, NTT-EAST, Internet MultiFeed and Keio university.

3.2 External Links

As shown in Figure 1, the camp-net had two IPv6 external links, one was satellite link between a portable satellite station at Matsushiro Royal Hotel and a Keio SFC campus satellite station, the other was a FTTH line served by NTT East, .

The settings of the satellite link were as follows; the channel was 1.5 GHz, the up-link bandwidth on the Matsushiro potable station was 512.0 kbps, the down-link bandwidth on the Matsushiro potable station was 1536.0 kbps. On the satellite line, we build a VLAN between the gateway router on Keio SFC campus and the camp-net core router on the Matsushiro. The satellite link was very stable during all camp days.

On the FTTH, we tested two types of IPv6 access services served by NTT East through Native method [7], Internet MultiFeed as a virtual network enabler and IIJ as an IPv6 ISP. From 2:00 PM of Sep. 5th to 8:00 PM of Sep. 6th (JST), we used a Flet's Hikari Next with IPv6 option. From 8:00 PM of Sep. 6th (JST), we changed the external line service to a Flet's Hikari Next with IPv6 option and a Hikari phone option, for the 4RD experiment. The difference by Hikari phone option was that *i)* an additional home gateway was added, *ii)* the IPv6 address delegation method was changed from RA with /64 prefix length to DHCP6 with /48 prefix length, as drawn in Figure 1(b).

We got the connectivity to IPv6 Internet from IIJ mio's FiberAccess/NF for IPv6 native service. On the external setting by 8:00 PM Sep. 6th, the IPv6 address to the camp-net L2TP gateway was assigned by RA, the prefix length was /64 (Fig. 1(a)). On the other hand, the external setting from 8:00 PM Sep. 6th, the IPv6 address for the WAN interface of IIJ' SEIL home router was served by DHCP6 with /48 prefix length for prefix delegation on 4RD (Fig. 1(b)).

For the IPv6 routing by WIDE Project's IPv6 address block, we achieved an L2TP tunnel between the L2TP gateway on the Matsushiro and that on Keio SFC campus over the FTTH line. The L2TP gateways were composed of Linux Debian squeeze (kernel 2.6.32) servers with our original L2TP for IPv6 implementation (v6tun). On our lab. test with two physical servers, v6tun got higher throughput than ut-vpn [8]; 719 Mbps for TCP and 738 Mbps for UDP by v6tun, on the other hand, 428 Mbps for TCP and 410 Mbps for UDP by ut-vpn [8].

3.3 NAT64 and DNS64

We served the IPv6 connectivity by ISC DHCP6 implementation [9]. Although we experienced the world IPv6 day, many networks have not IPv6 capability, yet. Thus, we have to prepare 6to4 translation techniques for the camp-net's IPv6 only connectivity experiment. We explored the best NAT64 [2, 10] and DNS64 [3] solution which satisfied our requirements.

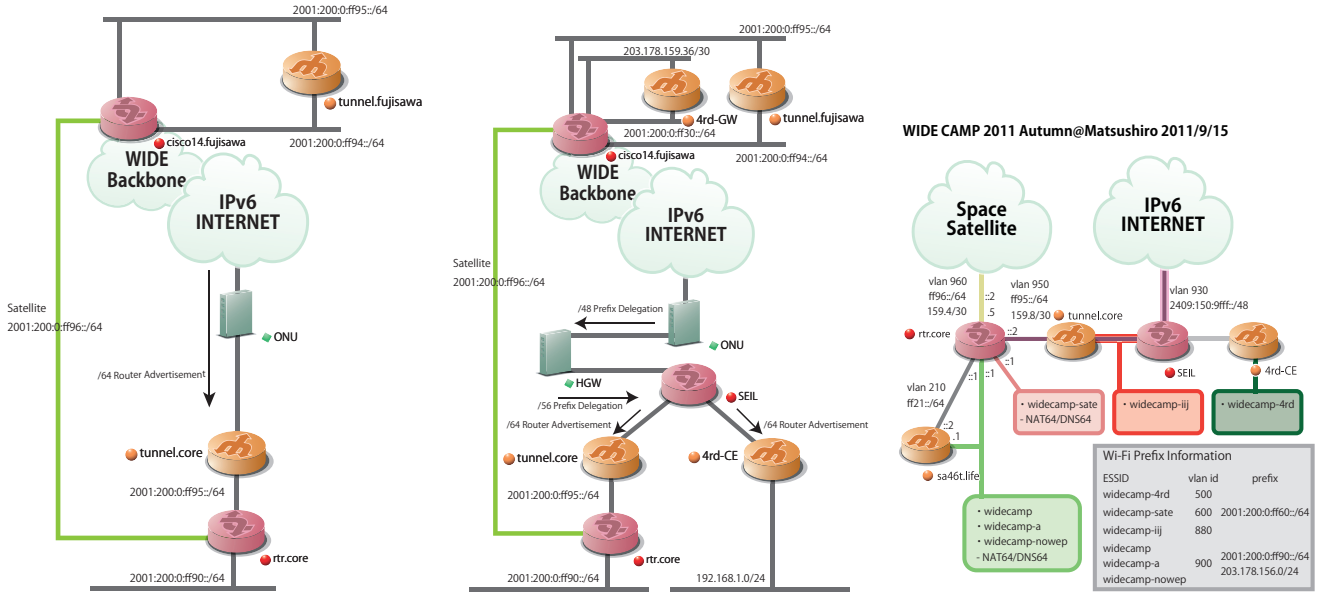
Our requirements as follows; **Requirement 1) the implementations SHOULD be open source software**, because we can debug them when some trouble occurs. **Requirement 2) the DNS64 implementation SHOULD work well**, because we cannot use a buggy implementation as a service. **Requirement 3) the NAT64 implementation SHOULD work well and MUST NOT collapse payloads**, because we cannot use a buggy implementation as well as the DNS64 implementation And **Requirement 4) the NAT64 implementation SHOULD NOT require other NAT cascades such as NAT44**, because we want to avoid troubles caused by the cascading of NATs or NAPTs. We tested three DNS64 implementations and three NAT64 implementations in the pre hot stage days.

Evaluated DNS64 implementations were ISC bind 9.8 p4 [11], NLnet labs' unbound [12], and Viagénie's ecdysis [13]. As the result of our examination, only bind worked well, therefore, we had no choice except for using bind as the DNS64 implementation in the camp-net.

We also evaluated three NAT64 implementations, linuxnat64 [14], tayga [15] and ecdysis [13]. linuxnat64 and ecdysis are stateful NAT64 [2] implementations, on the other hand, tayga is a stateless NAT64 [10] implementation. We chose linuxnat64 as NAT64 in the camp-net because we did not have enough number of IPv4 global addresses to run tayga's stateless NAT64, and because the ecdysis implementation, that we tested, collapsed TCP payloads. Only linuxnat64 worked well and satisfied our requirements.

3.4 IPv4 over IPv6 Encapsulation Implementations

Besides of the 6to4 translation, we had to explore the 464 encapsulation techniques to rescue such applications or OSes which does not have IPv6 capability yet. We selected an SA46T [4, 16–18] im-



(a) The backbone topology before 8:00 PM Sep. 6th

(b) The backbone topology after 8:00 PM Sep. 6th

(c) The topology around user access networks

Figure 1: The camp-net backbone topology

plementation developed by a cooperation R&D program Keio univ. and Fujitsu as a 464 encapsulation technology on the camp-net, because one of developers was included in the NOC team and because the SA46T implementation had been well evaluated though demonstration experiments between JGN-X of Japan and ThaiSARN of Thailand [19].

The camp-net had an additional experiment on 464 encapsulation technologies, 4RD [5]. This 4RD experiment was proposed at Sep. 1st by an experimenter team which was composed of Keio univ., NTT-EAST, Internet MultiFeed and IIJ. The experimenter team wanted to test the capability of the 4RD implementation of IIJ's SEIL and the availability of the 4RD service through NTT-EAST, Internet MultiFeed and IIJ. The NOC team prepared a vyatta 4RD implementation as a 4RD gateway in the Keio SFC campus. Because of an additional experiment, the NOC team set the start time of the 4RD experiment from Sep. 7th after when the initial experiments of the IPv6 capability test and the SA46T capability test had been finished.

3.5 WiFi Access and Address Allocation

The topology and settings around the user access is figured in Figure 1(c). Along with Figure 1(c), Table 1 shows the variations among ESSID, WiFi channels and Accounting methods, IPv4 and IPv6 connectivity, address allocation methods, and translation / encapsulation methods. We prepared each ESSID for each experiment's purpose. Basically, we served WiFi connections through WPA2 EAP-TLS for the capability test of WPA2 EAP-TLS and the verification of the update on personal certificate files at June 2011. The WPA2 EAP-TLS capability experiment was a regular experiment from the camp held in March 2008. We also prepared an ESSID **widecamp-nowep**, which was a hidden ESSID with no WEP, to resolve the WPA2 EAP-TLS incapability or participants who forgot to install his / her personal certificate file into his / her devices a priori. The accounting on **widecamp-nowep** was achieved by the radius authentication mentioned in [20].

Allocating IP addresses and informing name resolver address automatically, we used ISC DHCP implementation [9] of DHCP4 and DHCP6 except for the widecamp-4rd network. On the widecamp-4rd network, the SEIL home router behaved as the DHCP4 server.

3.6 Physical and Cloud Resources

For quick setup on the Matsushiro Royal hotel at Sep. 5th, we prepared most servers on a cloud environment. We constructed a cloud environment over six CISCO UCS servers on StarBED [21] and a NFS sever on Keio SFC campus by WIDE Cloud Controller (WCC) [22], with qemu-kvm 0.14.1, Linux Kernel 3.0.4 and libvirt 0.9.4. The six USC servers and the NFS server were connected through a VLAN over the WIDE backbone between StarBED and Keio SFC campus. We do not explain the detail of WCC and the cloud environment due to the limited space and out of scope in this paper.

3.7 Other Settings

As other settings and experiments, we tested our handmade operational tools as NOC operation experiments. We do not explain the detail of them due to the limited space.

4. EXPERIMENTS

In this section, we describe results of our camp-net experiments. Mentioned above, we had three main experiments, the WPA2 EAP-TLS capability test, the IPv6 capability test with NAT64 / DNS64, and the capability test of SA46T, which were conducted by the NOC team. Also, an additional experiment, the capability test of 4RD was handled by an experiment team which was composed of Keio univ., IIJ, Internet MultiFeed and NTT-EAST.

4.1 Overview and Time line

Table 1: Variations of IP address, address allocation methods, translation methods, and WiFi settings

ESSID	Accounting	Channel	Address version	Address scope	DNS	Address allocation	Trans. / Encap.
widecamp	WPA2 EAP-TLS	11b/g/n	v6	global	DNS64	DHCP6 (automatic)	NAT64
			v4	global	DNS64	DHCP4 (registration)	SA46T
widecamp-a	WPA2 EAP-TLS	11a	v6	global	DNS64	DHCP6 (automatic)	NAT64
			v4	global	DNS64	DHCP4 (registration)	SA46T
widecamp-sat	WPA2 EAP-TLS	11b/g/n	v6	global	DNS64	DHCP6 (automatic)	NAT64
			v4	N/A	N/A	N/A	N/A
widecamp-nowep (hidden)	MAC addr. Auth.	11b/g/n	v6	global	DNS64	DHCP6 (automatic)	NAT64
			v4	global	DNS64	DHCP4 (registration)	SA46T
widecamp-iij	WPA2 EAP-TLS	11b/g/n	v6	global	N/A	RA from SEIL (automatic)	N/A
			v4	N/A	N/A	N/A	4RD
widecamp-4rd	WPA2 EAP-TLS	11b/g/n	v6	global	N/A	RA from SEIL (automatic)	N/A
			v4	private	Proxy resolver	DHCP4 from SEIL (automatic)	4RD

Table 2 shows the time line of experiments on the camp-net. The experiments of the WPA2 EAP-TLS capability and the IPv6 capability test started at 10:00 AM of Sep. 6th. Initially, we hid the **widecamp-nowep** and the MAC address registration web page for the IPv4 connectivity through SA46T, for the aim to encourage participants to join the experiments. When a participant requested the IPv4 connectivity without WPA2 EAP-TLS at the NOC help desk due to some troubles, the NOC team served the IPv4 connectivity and help the participant setting up the WPA2 EAP-TLS and the IPv6 connectivity. Nowadays, mobile routers or mobile WiFi stations have become popular, therefore, a participant could easily escape to the IPv4 connectivity by his / her mobile router. We restricted the rogue APs at the conference floors, and the NOC fox hunting team controlled the usages of rogue APs, and led participants, who set rogue APs, to use his / her mobile router in his / her guest room or to come to the NOC help desk.

Until 1:30 PM of Sep. 7th, we hid the MAC address registration web page for IPv4 connectivity through SA46T. Also, we announced and started the 4RD experiment from 3:15 PM of Sep. 7th. Thus, almost of all participants lived in the IPv6 only connectivity at the conference floors through a whole day and night, at least.

4.2 Questionnaire

Here, we present the availability of the camp-net IPv6 only environment and encapsulated IPv4 connectivity (SA46T and 4RD) by questionnaire to participants. The number of participants was 153. By 1:30 PM Sep. 17th, 110 participants replied the questionnaire. The reply rate was about 71.9 %. Figure 2 shows the result of each question about the camp-net experiments, on the other hand, Figure 3 represents the answer for the questions about the 4RD experiment.

Figure 2(a) draws the population of used connectivity which participants replied. 30 participants (19.6%) surely lived in the IPv6 only connectivity with NAT64 / DNS64 during the all camp days. 7 participants, who used the v6 connectivity and the v4 connectivity through SA46T, might be such persons who failed the initial bootstrap of WPA2 EAP-TLS and / or the settings of IPv6, and escaped to the IPv4 connectivity through widecamp-nowep served in the 1st day (Sep. 6th). 33 participants, who replied that he / she used the IPv4 connectivity served by 4RD but did not use the IPv4 connectivity through SA46T, would such person that needed the IPv4 connectivity but would not want to register his / her MAC address to be registered. 34 participants, who used both SA46T and 4RD IPv4 connectivity, would join the comparison test between SA46T and 4RD.

According to Figure 2(b) and Figure 2(c), 90 participants (58.8%) were satisfied in the IPv6 only connectivity. Also, participants, who used IPv4 connectivity served by SA46T (Fig. 2(d)) or 4RD (Fig. 3(a)), replied main reasons of using IPv4 connectivity as follows;

Reason 1) Because I forgot to install my personal certificate file into my laptop PC(s) to connect WPA2 EAP-TLS, so I had to fetch my certificate file from my IPv4 only mail server whose name was not registered in DNS record.

Reason 2) My OS (Windows XP or Mac OS X 10.5.8) did not have IPv6 capability and / or I did not know how to setup it.

Reason 3) The Lenovo ThinkPad' wireless setting did not work well on the IPv6 only connectivity.

Reason 4) I used the IPv4 connectivity to use skype or windows live messenger due to my business.

Reason 5) I used the IPv4 connectivity to access the IPSec VPN or PPTP VPN server of my company which did not have IPv6 capability.

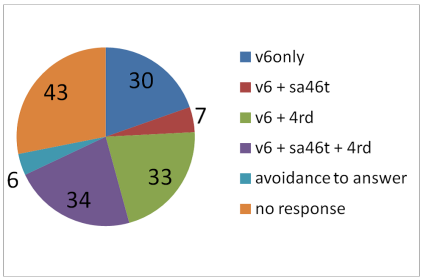
Reason 6) I tried to set up WPA2 EAP-TLS on my Android device, which required IPv4 connectivity for name resolution.

Reason 7) I could not browse some web sites on the IPv6 only connectivity due to the ServFAIL errors in AAAA.

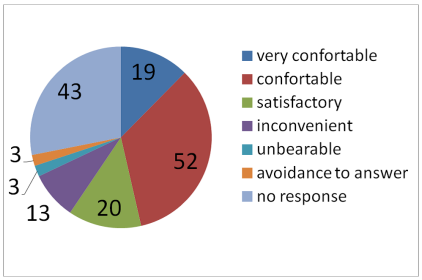
Reason 8) I could not wait the slow response of DNS64.

Reason 9) My VMware fusion's NAT did not work well in the IPv6 only connectivity.

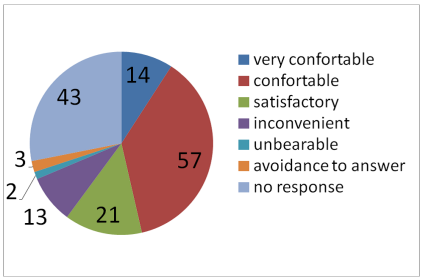
Reason 10) I used the IPv4 connectivity to join the comparison test between SA46T and 4RD, or to debug them.



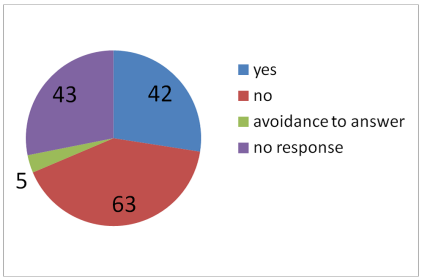
(a) Population of the connectivity which participants used



(b) Q1: We served an IPv6 only network as the main connectivity for user access in this camp, how was it?



(c) Q2: How was the quality of the network during the CAMP?



(d) Q3: Did you use the IPv4 connectivity by registering MAC address?

Figure 2: The results of questionnaire about main experiments

Figure 3(b), Figure 3(c), Figure 3(d), Figure 3(e) and Figure 3(f) show the availability of each application in the 4RD environment. Most participants were satisfied with the 4RD environment, however, some participants reported inconvenience of applications in the 4RD environment. The details of reported troubles and inconvenience of applications in section 4.3.

4.3 Reported Troubles

4.3.1 Troubles on WPA2 EAP-TLS

Unfortunately, the most reported troubles in Sep. 6th and 7th were failures on WPA2 EAP-TLS, which were out of assumptions on the NOC team because the WPA2 EAP-TLS experiment was a regular experiment from March 2008. Many participants forgot to install their certificate files into their laptop machines, and their certificate files were stored on the IPv4 only mail server over their companies' IPv4 only VPN. Participants, who came to the NOC help desk, were allocated the IPv4 connectivity by DHCP4 through widecamp-nowep or a wired connection. However, most participants felt shame to call for the NOC' help. Such participants fetched their personal certificate files through the IPv4 connectivity in guest rooms served by Matsushiro Royal Hotel or through their mobile routers.

We also had other troubles on WPA2 EAP-TLS due to the misconfirmation of the radius server or lack of TIPS, however, we do not explain them here due to the limitation of pages.

4.3.2 Troubles on the IPv6 capability

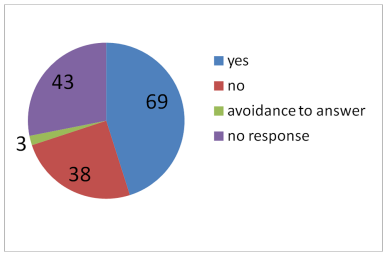
Troubles related with the IPv6 capability were as follows;

- **Pains due to long fallback routine**
  Almost of all participants, who could connect the IPv6 only connectivity environment, reported the too long fallback time to wait the finish of fallback routine without pain. Those claims were derived from Windows users and Mac OS X users because these OSes check the IPv4 connectivity on the initial connection setup sequence if their IPv4 property are enabled. The NOC team recommended them to "**turn off the IPv4 property**", and help setting the disable of IPv4 properties. Several participants surprised turning off the IPv4 property. However, when the IPv4 property was set off in a participant OSes, he / she got a comfortable initial set up sequence to the IPv6 connectivity.

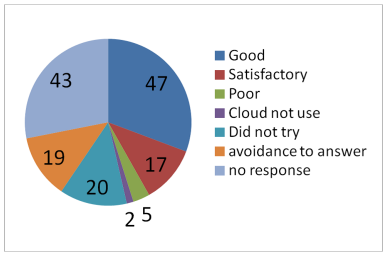
- **Pains due to lack of DHCP6 capability**
  Old version OSes, such as Windows XP or Mac OS X 10.6 (Snow Leopard) and older versions, did not have DHCP6 functions, especially the function to set DNS resolver announced by DHCP6. The NOC team announced the problem on DNS resolver on old version OSes, and let older OS users set up the DNS server entry by manual. On the other hand, almost of all Window 7 users and Mac OS X 10.7 (Lion) users did not claim about setting of DNS resolvers.

  As an exception, the think pad WiFi access control cloud not appropriately set up the IPv6 only connectivity and DHCP6 even when a user used Windows 7.

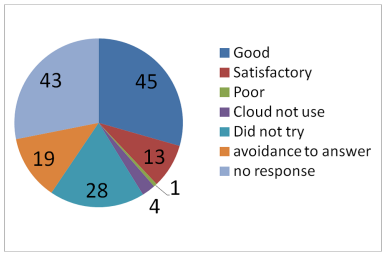
- **Pains due to the OS's incapability on IPv6 only setting**
  Windows XP or Android machines did not work well when the IPv4 properties were tuned off. Windows XP users had to



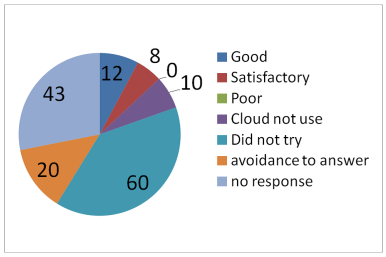
(a) Q4: SSID name: widecamp-4rd. Did you use it?



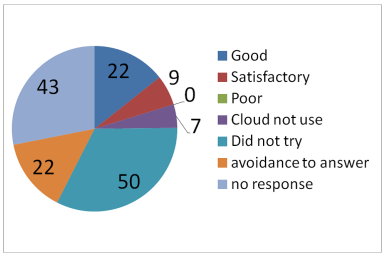
(b) Q5: How did you feel communications on 4rd? (Web)



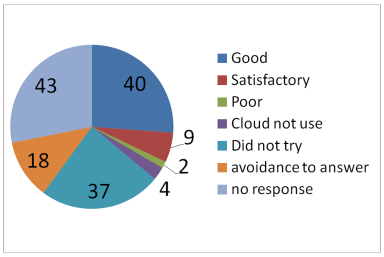
(c) Q6: How did you feel communications on 4rd? (Mail)



(d) Q7: How did you feel communications on 4rd? (VPN)



(e) Q8: How did you feel communications on 4rd? (Messenger)



(f) Q9: How did you feel communications on 4rd? (SSH)

Figure 3: The results of questionnaire about 4RD

set up a local proxy to DNS (nameproxy.exe) which requires the IPv4 DNS resolver as 127.0.0.1 in the IPv4 property.

Android machines might use the IPv4 DNS resolver. When the IPv4 properties were enabled, Android devices worked well in IPv6 communications.

- **Pains due to the device's incapability for IPv6**
  Several hardware devices did not have IPv6 capability.

  A Mac Book Air user met disappear of the DNS64 setting. We fixed it by setting through a command line, "**sudo networksetup -setdnsservers "AirPort" 2001:200:0:ff80::5**". Apple's USB Ethernet adapter or several hard ware devices did not have IPv6 capability. And, several participants with many platforms reported that they had to re-install device drivers.

4.3.3 *Troubles on Applications*

Reported troubles on specific applications were as follows;

- **Pains due to IPv6 incapability on applications**
  Instant Messaging and VoIP applications cloud not be available as well as Arkko's internet draft [6]. Several applications on Windows, such as CVSNT, virus signature updates of NOD32, might used only IPv4 socket functions, therefore, they did not work. In Mac OS X, several applications, which might not used COCOA framework, cloud not work well in the IPv6 only connectivity. On the other hand, Mac OS's applications based on COCOA framework worked well. Most HTTP / XMPP based applications or communications were available, expect for such HTTP / XMPP applications that might use IPv4 address literals.

- **Failures due to MTU mismatch problems**
  During the setup on Sep. 5th, the NOC team met MTU problem on the WIDE Cloud. The WIDE Cloud backbone MTU size was set 9000 for rapid live migration, however, MTU 9000 setting on KVM hyper-visors collapsed various communications in the set up day (Sep. 5th). Therefore, we set the MTU size of KVM hyper-visors to 1500.

  According to answers of questionnaire and reported troubles, various UDP based communications did not work well by MTU mismatch problems, not only from IPv6 to IPv4 with NAT64 / DNS64 on both L2TP pseudo layer 2 line over the FTTH line, but also on the satellite line and the 464 encapsulation through SA46T.

- **Failures due to incapability of protocol translation between IPv4 and IPv6**
  IPSec-based applications, such as OpenVPN or Apple Mobile Me IPSec and PKI based communications, did not work on the 6to4 connections. Also, some FTP clients did not work well on the v6 only connectivity with NAT64 / DNS64 and the 4RD IPv4 connectivity.

4.3.4 *Troubles on Name Resolution*

- **Failures due to IPv4 address literals**
  As well as Arkko's internet draft [6], many participants claimed they could not access to their IPv4 servers by IPv4 address literals through HTTP, SSH, VNC, IPSec, PPTP, IMAP, SMTP, POPFile, and so on. Some of them were fixed by changing name literals on the settings of their applications and / or by registering their IPv4 servers in DNS records. However, most of participants were not the administrators of their IPv4

Table 2: Time line of experiments

Date	Events
2:00 PM, Sep. 5th	started the setup
4:00 PM, Sep. 5th	finished the setup of the IPv6 L2TP over the FTTH external line
4:50 PM, Sep. 5th	finished the initial setup of the satellite link
3:00 AM, Sep. 6th	removed the DHCP helper due to the bad check sum problem
9:00 AM, Sep. 6th	finished the test of the satellite link
10:00 AM, Sep. 6th	started the WPA2 EAP-TLS capability test and the IPv6 capability test
8:00 PM, Sep. 6th	changed the FTTH setting
9:00 PM, Sep. 6th	finished the change of FTTH setting
10:00 PM, Sep. 6th	finished setting up the 4RD experiment and tested preliminarily
1:30 PM, Sep. 7th	opened the MAC address registration web page for the IPv4 connectivity through SA46T
3:15 PM, Sep. 7th	announced the 4RD experiment
4:15 PM, Sep. 7th	fixed the mis-configuration of firewall on the Mac address registration web server
5:47 PM, Sep. 7th	fixed the mis-configuration of the radius server
10:00 PM, Sep. 7th	almost of all participants connected to the camp-net with WPA2 EAP-TLS or through widecamp-nowep
1:42 PM, Sep. 8th	enabled DNSSEC on the DNS64 server
4:30 PM, Sep. 8th	set up the performance test environment for SA46T and 4RD
5:30 PM, Sep. 8th	fixed the mis-configuration on ns.wide and the lame delegation
6:00 PM, Sep. 8th	moved DNS64 server from the WIDE Cloud to a standalone physical server at Matsushiro side due to the performance problem
8:00 PM, Sep. 8th	started the comparison test between SA46T and 4RD
10:00 PM Sep. 8th	start performance tuning on the camp-net backbone
11:00 PM Sep. 8th	finished performance tuning on the camp-net backbone
11:00 AM Sep. 9th	stopped the camp-net experiments and struck the camp-net
2:30 PM Sep. 9th	withdrew the camp from Matsushiro, completely

servers or DNS servers, they escaped to the IPv4 connectivity served from the afternoon of Sep. 7th. On the VNC, PPTP, IPSec and other IPSec / UDP based communications, many participants claimed both on IPv4 only servers and on IPv6 capable servers even when they changed the access manners by name literals. Those access failures might be affected by MTU mismatch problems against UDP based communications.

- **Failures due to lack of reverse lookup entries on AAAA records**
  In the hot stage days, the NOC team detected several commercial web pages could not be accessed due to failure of reverse lookup. Therefore, we registered all reverse lookup AAAA records on the `camp.wide.ad.jp` domains.

- **Failures due to the lame delegation**
  As mentioned above, some commercial web sites required the reverse lookup in AAAA records as well as in A records. Several participants claimed some commercial web pages cloud not be seen by failure of reverse lookup, although we registered all reverse lookup entries in AAAA about the `camp.wide.ad.jp` domain. We investigated the causes of the failure of reverse lookup, the cause was the lame delegation on the upper authoritative server of the DNS64 server (`ns.wide.ad.jp`) brought by a mis-configuration of bind. After the lame delegation was solved by an operator of `ns.wide.ad.jp`, problems on reverse lookup were fixed.

- **Pains due to the overload of DNS64**
  After enabling DNSSEC, the DNS64 server, which was placed on the WIDE Cloud node of the Matsushiro side, was overwhelmed by handling many queries, key verifications, and log outputs into the NFS server on Keio SFC campus. Therefore, we moved DNS64 server from the KVM environment to a physical server on the Matsushiro side, then, the overload on the DNS64 server was solved.

- **Failures due to wrong AAAA replies**
  Some web pages, especially the search result pages of travel reservation sites, could not access from the IPv6 network through NAT64 / DNS64 translation. The reasons why connections to such web pages failed were derived from wrong DNS replies mentioned in RFC 4074 [23]. We observed "Return Name Error" mentioned in Section 4.2 of RFC 4074 [23], "Return Other Erroneous Codes" in Section 4.3 of RFC 4074 [23], and "Return a Broken Response" in Section 4.4 of RFC 4074 [23]. We could not solve these problems in the camp days because these problems were derived from wrong behaviors of DNS resolvers on the web sites.

5. DISCUSSION

5.1 Recommendation for IPv6 transition

According to our experience on the camp 1109 autumn experiments, the NOC team's recommendations for IPv6 transition are as follows;

- **You SHOULD implement or enable the IPv6 capability into your site soon, if possible,** because NAT or NAPT environments might cause various problems such as MTU mismatch, low throughput, incapability on translation, and so on.

- **You SHOULD update or purchase OSes on your computers to the latest version,** because Window 7 users and Mac OS X 10.7 (Lion) users did not meet critical troubles, and because older OS users met various troubles.

- **You WOULD be better to register reverse AAAA lookup entries,** because several commercial web sites require the reverse lookup.

- **You SHOULD check whether your web appliances return wrong DNS replies or not,** because some web appliances might return wrong DNS replies and wrong DNS replies can be solved by only administrators on web sites.

- **You SHOULD take care of MTU size on multiple overlaid underlay networks** because PMTUD might not work in some times.

5.2 Open Issues

5.2.1 PMTUD, MTU mismatch problems

On the camp-net experiments, PMTUD, MTU mismatch problems occurred in several points. These problems were derived from the failure of Path MTU Discovery. In the operational problem to avoid the overload of routers or DDoS attacks, many networks turn

off PMTUD functions on routers. However, many applications or implementations of tunneling / encapsulation protocols assume that the PMTUD would work.

One possible solution is that fragmentation is enabled on a router / encapsulation implementation even when DF bit is set. Also, lack of trouble shooting tools for multiple overlaid underlay networks makes it difficult to detect the point of MTU mismatch. Such trouble shooting tools should be developed.

5.2.2 Wrong DNS replies mentioned in RFC 4074

Mentioned in Section 4.3.4, wrong DNS replies pointed in RFC 4074 [23] are one of open issues on the IPv6 transitions. Ideally, all DNS resolvers are implemented along with RFCs and replaced as soon as possible. However, such solution will spend money and human resources.

One of possible solutions is change the fallback routine of DNS64 resolvers as follows;

A DNS64 resolver resolves the A record even when a DNS reply contained NXDOMAIN or ServFail.

A DNS64 resolver caches all possible A records a priori. When a DNS reply was NOERROR, the DNS64 resolver queries the AAAA record. If the AAAA record exists, then the DNS64 resolver returns the AAAA record to a client, and if not, the DNS64 resolver returns the cached A record to the client.

5.2.3 IPv4 / IPv6 translation capability on several protocols

Several protocols, such as IPSec or FTP, do not have capability on IPv4 / IPv6 translation. However, such problems are easily solved by enabling the IPv6 capability on servers.

6. CONCLUSION AND FUTURE WORK

In this paper, we reported our experiences on the IPv6 only connectivity with NAT64 / DNS64 and 464 encapsulation techniques. The only v6 connectivity of the camp-net was much more available than we and participants thought before the camp days. However, various problems, which have been already mentioned by various researchers, surely happened.

Due to the lack of trouble shooting methods and measurement methods, we cloud not analyze details of troubles or causes. As future work, we create the IPv6 only connectivity environments on several WIDE NOCs, and try to evaluate and analyze problems on IPv4 / IPv6 transition technologies.

7. ACKNOWLEDGMENTS

We have to say thank you for all participants in the WIDE Project camp 1109 Autumn, and the secretariats by e-side, inc.. We also thank NICT Japan for supporting StarBED[3] and JGN-X to achieve a part of the camp-net.

8. REFERENCES

[1] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315 (Proposed Standard), July 2003. Updated by RFCs 4361, 5494, 6221.

[2] M. Bagnulo, P. Matthews, and I. van Beijnum. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. RFC 6146 (Proposed Standard), April 2011.

[3] M. Bagnulo, A. Sullivan, P. Matthews, and I. van Beijnum. DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers. RFC 6147 (Proposed Standard), April 2011.

[4] N. Matsuhira. Stateless Automatic IPv4 over IPv6 Tunneling: Specification, Jul. 2011. individual draft `draft-matsuhira-sa46t-spec-03.txt`.

[5] Ed. R. Despres, S. Matsushima, T. Murakami, and O. Troan. IPv4 Residual Deployment across IPv6-Service networks (4rd) ISP-NAT's made optional, Mar. 2011. individual draft `draft-despres-intarea-4rd-01.txt`.

[6] J. Arkko and A. Keranen. Experiences from an IPv6-Only Network, Apr. 2011. individual draft `draft-arkko-ipv6-only-experience-03.txt`.

[7] A. Yasuda. Capacity Building for IPv6 by IPv6 Promotion Council Japan. Presentation in APRICOT / APNIC Meeting Febrary 2011 `http://meetings.apnic.net/__data/assets/pdf_file/0003/30981/Ayumu-Yasuda-apricot.pdf`, Feb. 2011.

[8] University of Tsukuba and SoftEther Corporation. UT-VPN. `http://utvpn.tsukuba.ac.jp/`.

[9] Internet Systems Consortium. DHCP. `http://www.isc.org/software/dhcp`.

[10] X. Li, C. Bao, and F. Baker. IP/ICMP Translation Algorithm. RFC 6145 (Proposed Standard), April 2011.

[11] Internet Systems Consortium. BIND. `http://www.isc.org/software/bind`.

[12] NLnet Labs. Unbound. `http://unbound.net/`.

[13] Viagénie. Ecdysis: open-source implementation of a NAT64 gateway. `http://ecdysis.viagenie.ca/index.html`.

[14] Geeknet, Inc. Linux NAT64 implementation. `http://linuxnat64.sourceforge.net/`.

[15] Nathan Lutchansky. TAYGA Simple, no-fuss NAT64 for Linux. `http://www.litech.org/tayga/`.

[16] N. Matsuhira. Motivation for developing Stateless Automatic IPv4 over IPv6 Tunneling (SA46T), Jul. 2011. individual draft `draft-matsuhira-sa46t-motivation-00.txt`.

[17] N. Matsuhira. Applicability of Stateless automatic IPv4 over IPv6 Tunneling (SA46T), Jul. 2011. individual draft `draft-matsuhira-sa46t-applicability-02.txt`.

[18] N. Matsuhira. Stateless Automatic IPv4 over IPv6 Tunneling: Global SA46T Address Format, Jul. 2011. individual draft `draft-matsuhira-sa46t-gaddr-03.txt`.

[19] C. Charnsripiny, P. Tantatsanawong, and T. Sribuddee. Research Network Infrastructure to Support Future Internet Technology in Thailand, Aug. 2011. Presentation in APAN 32nd meeting `http://www.apan.net/meetings/India2011/Session/Slides/fit/3-2.pdf`.

[20] M. Oe, H. Hazeyama, S. Yamamoto, and S. Shirahata. An implementation and verification of ieee 802.11 wireless network management system. *Electronics and Communications in Japan (Part I: Communications)*, 88(12):20–28, June 2005.

[21] StarBED Project.

[22] WIDE Cloud Working Group. WIDE Cloud Controller. `http://wcc.wide.ad.jp/`.

[23] Y. Morishita and T. Jinmei. Common Misbehavior Against DNS Queries for IPv6 Addresses. RFC 4074 (Informational), May 2005.