第 XXXII 部

大規模な仮設ネットワークテストベッドの設計・構築とその運用

第 32 部
大規模な仮設ネットワークテストベッドの設計・構築とその運用

第 1 章　2010 年春合宿ネットワークに関する報告

1.1 2010 年春合宿ネットワーク

本節では、2010 年 3 月 9 日から 12 日まで静岡県浜松市浜名湖ロイヤルホテルにて開催された WIDE プロジェクト春合宿におけるネットワーク運用、及びそのネットワーク上で実施された実証実験の内容とその結果を報告する。

1.1.1 対外接続用回線

本合宿で構築したネットワークでは、合宿地から WIDE バックボーン及びインターネットへの接続用回線として、フレッツ光、Ku-band 衛星回線の 2 種類の対外接続用回線を使用した。表 1.1 に本ネットワークで使用した対外接続用回線を示す。

本合宿では、浜名湖ロイヤルホテルに敷設された光回線を用いた OCN への接続を主系統とし、帯域が十分ではない Ku-band 衛星回線を予備系統として用いた。また、合宿地において WIDE Project のアドレスを用いて運用するため、合宿地と WIDE 藤沢 NOC それぞれに Cisco 2800 を設置し、L2TPv3 によるトンネルを用いて WIDE バックボーンとの L3 の対外接続を構築した。

1.1.2 ネットワークの内部構成

合宿地に構築したネットワークでは、合宿参加者が接続するユーザセグメント、DNS や WEB など合宿地に設置するサーバ群を収容するサーバセグメント、ルータやスイッチなどのインターフェースに付けるためのマネージメントセグメント、その他に後述の実験を行うためのセグメントを構築した。図 1.1、図 1.2 に本合宿のネットワークトポロジを示す。

前回合宿以前までのアンケート結果や参加人数から、合宿参加者に対して、/24 のネットワークを無線 LAN を主とした接続で提供した。有線 LAN については、各部屋に設置した L3 スイッチにてユーザセグメントを提供した。また後述する実験に関しては、実験用参加者を収容するセグメントを別 SSID でユーザセグメントとは分けて提供した。

本合宿では、合宿地ネットワークを WIDE のアドレスで運用するために L2TPv3 を用いた。前述の通り、合宿地と WIDE 藤沢 NOC それぞれに Cisco 2800 を設置し、この 2 台で L2TPv3 によるトンネルを構築し、この仮想 L2 線を用いて L3 の対外接続を構築した。今までの合宿では、L3 の対外接続に L3 トンネルを用いることによって MTU サイズが減少し、DFbit を用いるサービスに障害が発生することがあった。しかし、本合宿ではこの L2TPv3 による L2 トンネルを用いることによって、この障害を回避することができた。

1.1.3 合宿ネットワーク運用によって得られた知見

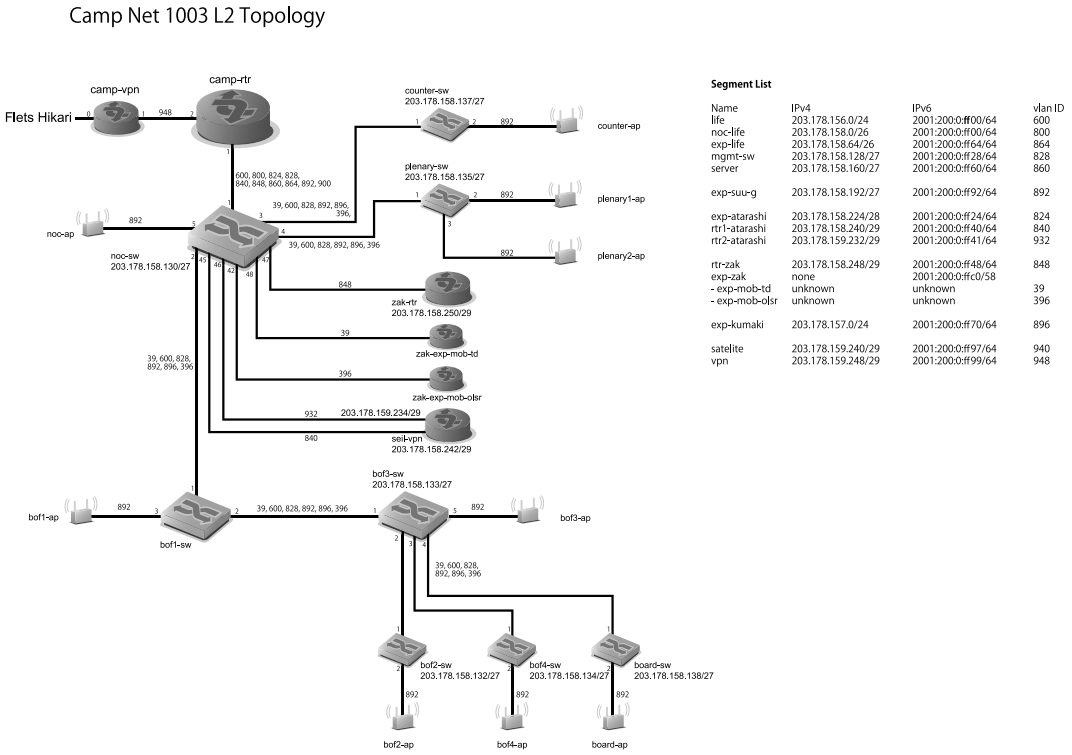
本合宿における合宿ネットワークの運用によって得られた知見について述べる。

1.1.3.1 機材構成

本合宿では、全ての部屋に L3 スイッチを 1 台以上設置したが、移動や配送のことを考慮すると、最小構成を目指すことにも価値がある。特に本合宿では、無線アクセスポイント（AP）の運用に Cisco Wireless LAN Controller（WLC）を用いた。WLC では、AP に直接接続するネットワークは 1 つのセグメントでよく、別のセグメントを別 SSID で運用する際は WLC に vlan で入れるのみでかまわない。そのため、本来

表 1.1.　本合宿で使用した対外接続用回線

回線名	回線数	通信速度
フレッツ光プレミアム	1	100 Mbps
Ku-band 衛星回線	1	Uplink: 512 Kbps, Downlink: 1536 Kbps



Segment List

Name	IPv4	IPv6	vlan ID
life	203.178.156.0/24	2001:200:0:ff00/64	600
noc-life	203.178.158.0/26	2001:200:0:ff00/64	800
exp-life	203.178.158.64/26	2001:200:0:ff64/64	864
mgmt-sw	203.178.158.128/27	2001:200:0:ff28/64	828
server	203.178.158.160/27	2001:200:0:ff60/64	860
exp-suu-g	203.178.158.192/27	2001:200:0:ff92/64	892
exp-atarashi	203.178.158.224/28	2001:200:0:ff24/64	824
rtr1-atarashi	203.178.158.240/29	2001:200:0:ff40/64	840
rtr2-atarashi	203.178.159.232/29	2001:200:0:ff41/64	932
rtr-zak	203.178.158.248/29	2001:200:0:ff48/64	848
exp-zak	none	2001:200:0:ffc0/58	
- exp-mob-td	unknown	unknown	39
- exp-mob-olsr	unknown	unknown	396
exp-kumaki	203.178.157.0/24	2001:200:0:ff70/64	896
satelite	203.178.159.240/29	2001:200:0:ff97/64	940
vpn	203.178.159.248/29	2001:200:0:ff99/64	948

図 1.1.　WIDE 春合宿ネットワークトポロジ（Layer 2）

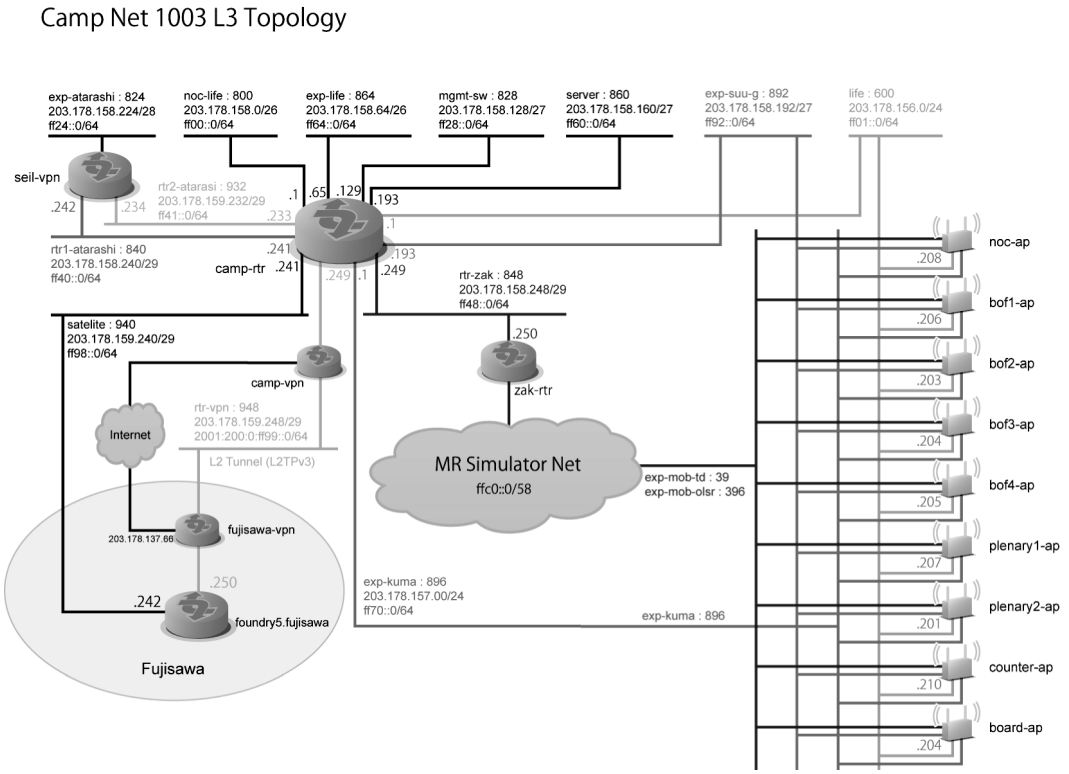


図 1.2.　WIDE 春合宿ネットワークトポロジ（Layer 3）

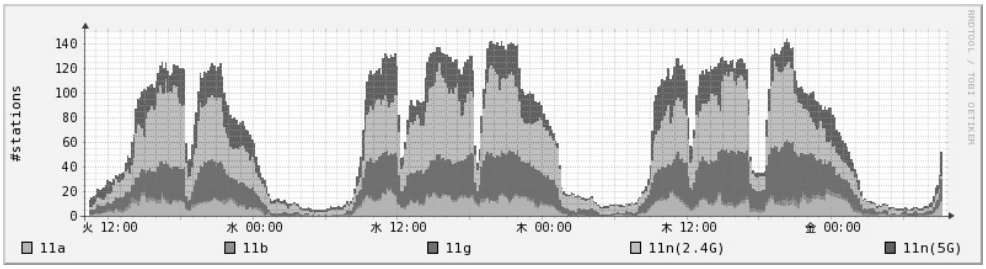


図 1.3. IEEE 802.11a/b/g/n (2.4 GHz)/n (5 GHz) ごとの接続数

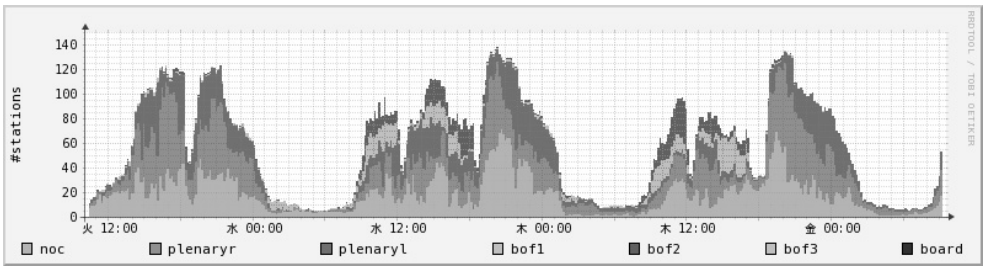


図 1.4. 部屋ごとの接続数

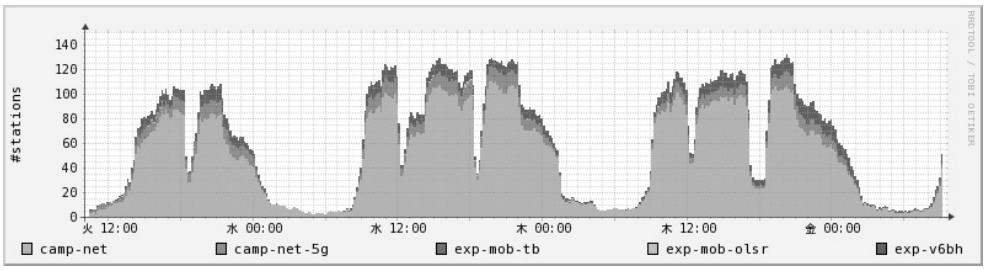


図 1.5. SSID ごとの接続数

であれば全ての部屋に vlan を解釈できるスイッチを設置する必要は無く、ネットワークをよりコンパクトに設計することができたはずである。

1.2 合宿ネットワークを利用した実験

本合宿では以下の実験が行われた。

1. 無線ネットワークの運用
2. モバイルシミュレータを用いた、仮想ネットワーク構築
3. 有線リンク上でのパケット計測による無線ホストの検出と特徴抽出
4. IPv4/IPv6 デュアルスタック環境にて現実に発生する事象の洗い出しと考察
5. WIDE 合宿におけるネットワークカメラを利用した研究参加支援システム

1.2.1 無線ネットワークの運用

本実験は、WIDE 合宿という 100 人規模の会場に無線ネットワークを構築した際の現在の様々なハードウェア・ソフトウェアにおける対応状況・問題を知り、設営・運用に関するノウハウを獲得することを目的として行った。

1.2.1.1 無線 LAN の運用状況

今回の合宿における無線 LAN の利用状況を以下に示す。図 1.3 は無線 LAN のプロトコルごとの接続数、図 1.4 は提供した各部屋ごとの接続数、図 1.5 は SSID ごとの接続数のそれぞれグラフである。

1.2.1.2 今回の実験で得られた知見

Cisco の Wireless LAN Controller を用いて無線 LAN を運用する際に、以下の手順を踏むことにより IPv6 を正しく運用することができた。

1. WLAN の設定項目内にある “IPv6 Enable” にチェックを入れる
2. WLAN の設定ページ内にある注意書きに従

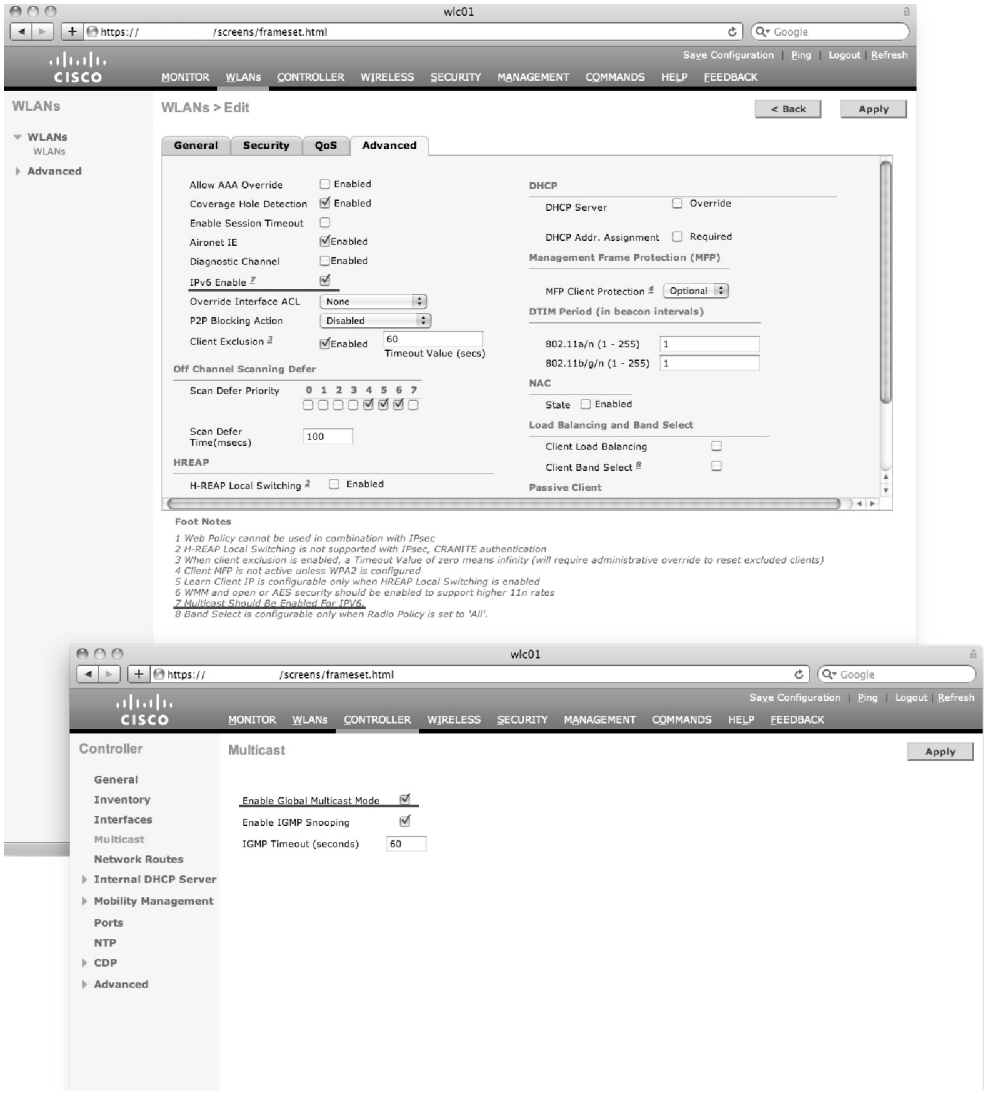


図 1.6.　WLC における IPv6 利用の設定

い、Controller の “Enable Global Multicast Mode” にチェックを入れる

1.2.2 モバイルシミュレータを用いた、仮想ネットワーク構築

1.2.2.1 実験内容

本実験では、ネットワークシミュレータ ns-3 上に実装されたソケット・システムコールエミュレーション機能を利用して動作する Zebra[1]を用い、移動環境下でトポロジを動的に組替えるネットワークを、ユーザへはブラックボックスとして提供した。提供した環境を通じ、仮想環境の性能評価・実験環境としての課題発見を試みる。

1　http://www.zebra.org

1.2.2.2 目的と意義

ネットワークプロトコルの研究において、その研究成果の評価を行うテストベッド構築の手法として、実ノードを設置してそこにソフトウェア実装物を配備し、実験をする手法、また KVM、Xen、Linux VServer などの仮想化手法を用い、ノードを仮想的に設置したものにソフトウェア実装物を配備する方法などがある（e.g., Planetlab[143]）。しかしながら、これらの手法は大量数ノードの実験のための制御が困難であったり、また無線デバイスなどを用いた移動を伴う実験の実施が困難である、といった点が問題点として挙げられる。

一方、ネットワークシミュレータを用いた実験・評

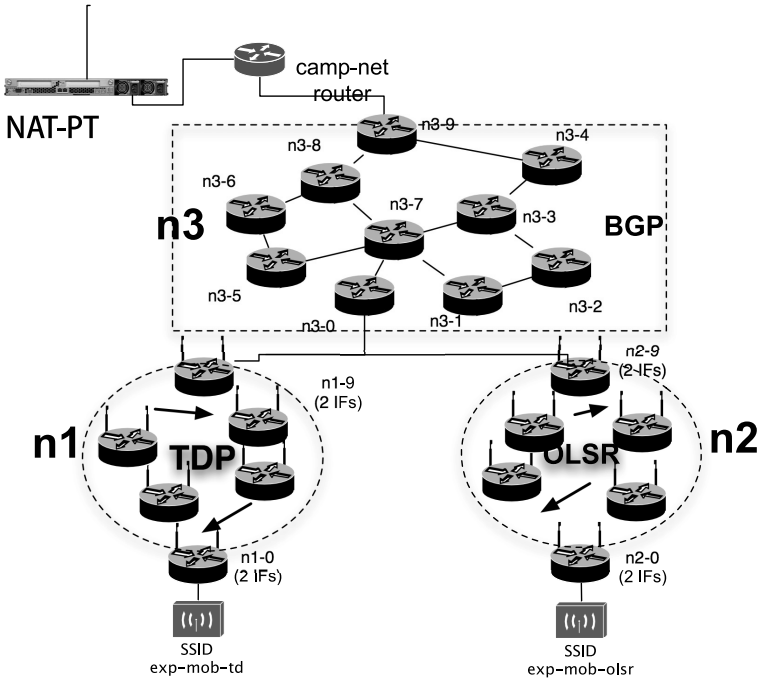


図 1.7. ns-3 により構築された実験ネットワーク

価は、その抽象化されたモデルにより、研究によって提案されたプロトコルの挙動を定量的に評価する事など、目的となる評価を実施するための実験環境としては熟成されたものである。しかしながら、シミュレータの実装で利用されているネットワークスタックや、経路制御などのプロトコルは、実ネットワークで運用され、実績のあるものではなく、そのシミュレータのために実装した、実績の少ないものである。この事により、一度シミュレータを実ネットワークに接続をすると、相互接続性が取れない事が問題となっている。この問題は、ネットワークシミュレーションによる実験結果の信頼性を下げる一因となっており、深刻である。

本実験では、前述の 2 つの問題を解決するために、ネットワークシミュレータ ns-3[2]のソケット・システムコールエミュレーションを利用した、Linux/BSD などで利用可能な経路制御ソフトウェア Zebra を実行できる環境を提供し、そのシミュレータにより構築されたネットワークを、WIDE 合宿参加者へ提供し、仮想的にモバイルネットワーク環境に参加している状態をつくりだす。

実アプリケーション Zebra を利用した仮想ネットワークの性能評価。シミュレーション環境で転送可能なトラフィック容量、フロー数、仮想ノード数等を、ユーザに接続性を提供しながら計測する。

2 http://www.nsnam.org/

1.2.2.3 実験の詳細

図 1.7 は本実験で構築したネットワークを示している。合宿ネットワーク内のルータ（図中 camp-net router）を上流ルータとし、その配下に ns-3 の内部で動作させる Zebra bgpd によりトポロジ構築を行う BGP 網（図中 n3）を配置し、更にその配下に Tree Discovery（TDP）[174] と Optimized Link State Routing（OLSR）[35] との別々の経路制御プロトコルを動作させる 2 つのネットワークを配置する（図中 n1 と n2）。この TDP と OLSR もそれぞれ Zebra の拡張として実装したプログラムを ns-3 の内部で動作させ、また ns-3 の仮想ノードは、Random WayPoint 移動モデルに従い、秒速 20 m で移動しながら経路情報の交換を行なう。その 2 つの移動ネットワークのうち 1 ノードは、無線アクセスポイントを接続し、合宿ネットワーク内で、ESSID exp-mob-td と exp-mob-olsr という 2 つの Wi-Fi 接続口を提供する事で、合宿参加者がこの ns-3 により構築された移動ネットワークのノードとともに移動し、インターネット接続性を確保する。

実験ネットワークへの参加者は、IPv6 アドレスをホストに割り当てる事で実現した。ESSID の選択とともに、DNS サーバのアドレスを手動で設定させ、慶應 SFC 内に設置されたその DNS サーバにて動作

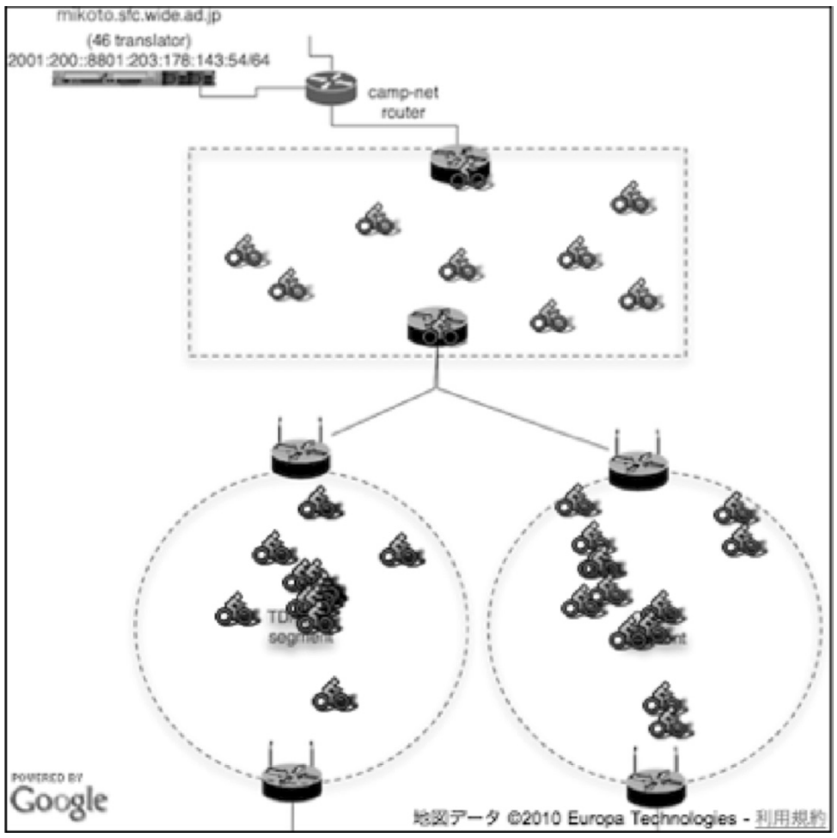


図 1.8.　実験ネットワークコントローラ

している faith[67] により、合宿地外部の IPv4 ノードとの通信も可能とさせた。

実験ネットワークの様子は、Google MAPS API を用いて実装した「実験ネットワークコントローラ（図 1.8）」により、移動ノードの論理的な位置を表示したり、BGP ピアの接続をクリック操作により切断させたりする事で、実験ネットワークの状態変動の可視化・制御を実現した。

1.2.2.4 実験結果

実験を通じ、Zebra の BGP、OLSR、TDP のエミュレーション部分の動作は、期待通り動作し、移動による頻繁なトポロジ変動を経路制御により迂回させる事は実現できた。しかし、4 日間の合宿を通して、実験参加者が最大同時利用ノード数で 6 ノード、延べ利用ノード数で 10 ノードと、大変少ない状態であった。IPv6 アドレスのみによる実験ネットワーク参加や、手動での設定変更が必要であった事、などが原因であったと考えられる。IPv4 アドレスの払出しによる実験参加者の誘導などは今後の課題として考えられる。

更に、実験ネットワークへ小さいサイズのバーストパケットが入力されると、ns-3 プロセスの処理停止により制御不能となるケースがあった。これは技術的な課題として今後解決に取り組んでいく予定である。

1.2.3 有線リンク上でのパケット計測による無線ホストの検出と特徴抽出[3]

The number of wireless devices and the traffic volume generated by these devices become significant today, and many devices begin supporting 802.11n protocol for higher-speed wireless access. However, the diversification in link types of end-hosts may degrade system performance. For example, hosts using 802.11 protocols had better not be relay nodes in a P2P live streaming system because 802.11 is a half-duplex protocol and usually less stable compared to modern wired links. Hence, understanding traffic characteristics

3　The achievement of this work has been published in Ref. [7].

of various link types is essential for improving or building network architectures. Moreover, estimation of the link type of a remote host possibly achieves better performance (e.g., higher throughput) in some network systems. Baiamonte et al.[11] have proposed an algorithm to detect wireless hosts from passive measurement by using the entropy of packet interarrival time (PIT). Wei et al.[188] have also proposed an algorithm to classify access network types. However, these algorithms pay no attention to new link types such as 802.11n, 3G, and WiMAX even though each of them has different characteristics and possibly degrades the performance of network systems.

Our goal is to analyze and model the characteristics of various link types which can be criteria for system design, and then to provide an algorithm to identify the link type of a remote host. During the biannual symposium of the WIDE project on 9–12 March 2010, we had measured wireless traffic in relatively large-scale network. In this report, we analyze PIT, its entropy of 802.11 hosts, and fairness between 802.11a/g and 802.11n in coexisting these wireless networks with the measured packet trace. The contributions of this report are to show that 802.11n has different characteristics from 802.11a/g in PIT and its entropy, and to confirm fairness between 802.11a/g and 802.11n hosts in time-domain.

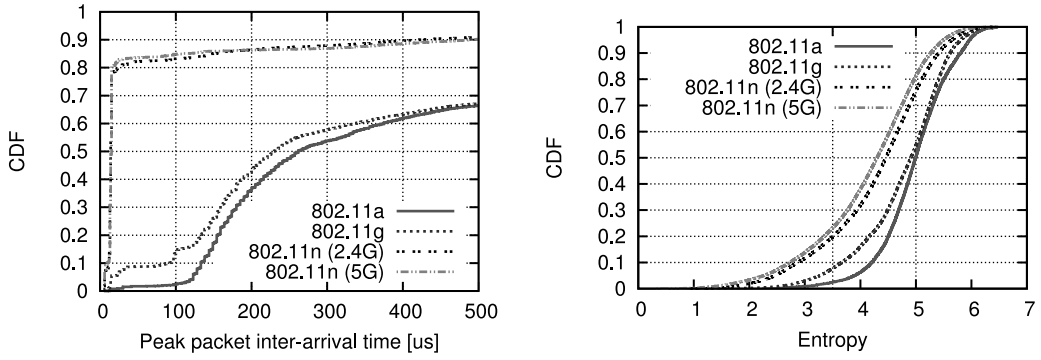
1.2.3.1 Traffic Characteristics

The entropy of PIT has been commonly used to characterize the traffic of bottleneck links[11, 188]. A probability mass function (PMF) of PIT is defined as $P(\tau_i) = m_i/m$, where m is the total number of sampled PIT and m_i is the number of samples whose PIT is in the range $[\tau_i, \tau_{i+1})$. N.B., $\tau_i = bi$, where the time bin b is a constant value. We then define the entropy of PIT from the PMF in the equation: $H := -\sum_i P(\tau_i) \log_2 P(\tau_i)$. The entropy in this context represents uncertainty of PIT; for example, PIT of hosts connecting with *shared* links might be fluctuated due to collisions and the entropy would be larger while those connecting with *non-shared* (i.e., exclusive) and stable links can certainly send packets without collisions nor loss. In this report, we use the same parameters as those used in Ref. [11], that is, the time bin b is 100 µs, a maximum threshold of PIT is set to 10 ms, a time window for calculation of entropy is 20 s, and a minimum threshold of the number of samples in a time window is 200.

We also define two fairness indexes, throughput and transfer duration fairness indexes, to evaluate fairness between 802.11a/g and 802.11n hosts in coexisting these networks. The throughput fairness index of the protocol p ($p \in \{$802.11a/g, 802.11n$\}$) with the channel c is defined as $F_s^{p,c}(\Delta) := \frac{s_c^p(\Delta)}{s_c^{802.11a/g}(\Delta) + s_c^{802.11n}(\Delta)}$, where $s_c^p(\Delta)$ is average throughput among hosts using the protocol p with the channel c during the duration Δ. In the same way, the transfer duration fairness index is also defined as $F_d^{p,c}(\Delta) := \frac{d_c^p(\Delta)}{d_c^{802.11a/g}(\Delta) + d_c^{802.11n}(\Delta)}$, where $d_c^p(\Delta)$ is average transfer duration among hosts using the protocol p with the channel c during the duration Δ.

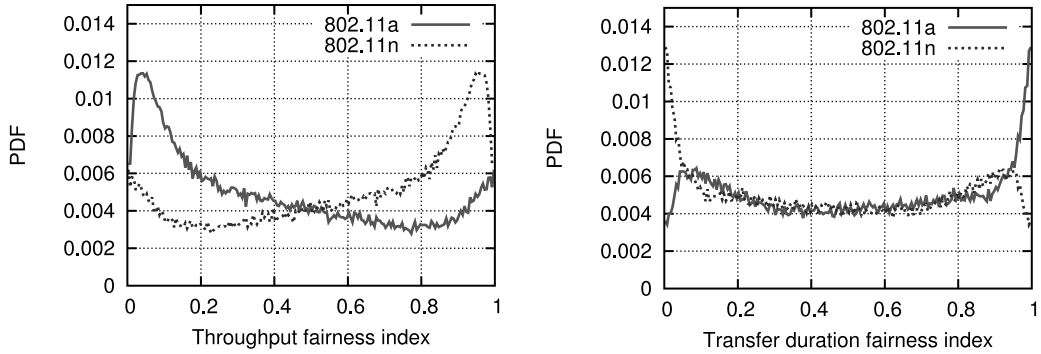
1.2.3.2 Measurement and Results

The measurement was conducted in the biannual symposium of the WIDE project on 9–12 March 2010; the wireless network of the symposium consisted of nine wireless access points (APs: Cisco Aironet 1250) with one controller (Cisco Wireless Controller 5508), and 215 (client) stations. All the APs were operated in lightweight mode, and consequently, all the data frames through APs were encapsulated by the CAPWAP protocol (RFC 5415) and went through the controller. We had captured these encapsulated data frames at a monitored interface between the controller and APs by tcpdump (total: 122 million frames). After the measurement, we extracted 802.11 frames from the encapsulated traffic trace. We had also measured the information of associated stations from APs every ten seconds by SNMP. The maximum number of stations simultaneously connected to APs was 148. The number of measured associations of 802.11a, 802.11g,



(a) Peak PIT　　(b) Entropy

Fig. 1.9. CDF of peak PIT and entropy of PIT by protocols



(a) Throughput ($F_s^{p,c}$)　　(b) Transfer duration ($F_d^{p,c}$)

Fig. 1.10. PDF of fairness indexes by protocols ($c = 36$)

802.11n (2.4 GHz) and 802.11n (5 GHz) are 105, 129, 129 and 116, respectively; N.B., we double-counted the hosts that support both 2.4 GHz and 5 GHz etc.

We show the cumulative distribution function (CDF) of peak PIT by protocols in Figure 1.9(a). The peak PIT is the peak value in the PMF P with the time bin $b = 1$. We confirmed that the peak PIT of 802.11a/g mostly distributed above 120 µs, and that of 802.11n concentrated around 10 µs, meaning that the block ACK mechanism in 802.11n affected PIT significantly. We then show the CDF of the entropy of PIT by protocols in Figure 1.9(b). The entropy of 802.11n has smaller values than that of 802.11a/g. The result points out that the identification algorithm in Ref. [11] makes inaccurate annotations to more than 20% hosts though it is appropriate for 802.11a/g because it judges a host with $H \leq 3.5$ as "wired". Thus, the simple entropy-based algorithm has a difficulty in identifying 802.11n hosts.

We also evaluate fairness between 802.11a/g and 802.11n hosts in coexisting these networks. 802.11a and 802.11n share the 5 GHz band, and 802.11g and 802.11n also share the 2.4 GHz band, implying the potential conflicts (i.e., fairness issue). In this evaluation, we focus on the channel 36 in 5 GHz band. Figures 1.10(a) and (b) show the probability distribution functions (PDF) of throughput and transfer duration fairness indexes for each second by protocols, respectively. Here, throughput is calculated from the accumulated frame length, and transfer duration is estimated from the transmission rate and frame length although control frames such as ACK were not captured. From Figure 1.10(a), the PDFs of the throughput fairness index are biased by protocols, and the index of 802.11n distributes to larger

values; i.e., $\int_0^{0.5} y\,dx \ll \int_{0.5}^1 y\,dx$, where x is the throughput fairness index of 802.11n and y is the PDF of x. This means 802.11n has an advantage in throughput. On the other hand, from Figure 1.10(b), the PDFs of the transfer duration fairness index are flat and similar to each other; i.e., $\int_0^{0.5} y\,dx \simeq \int_{0.5}^1 y\,dx$, where x is the transfer duration fairness index of 802.11n and y is the PDF of x. Note that the PDFs have large jumps around at 0 and 1. We can ignore these jumps because they come from errors in transfer duration estimation due to different ACK mechanisms between 802.11a/g and 802.11n. Hence, the transfer duration is approximately fair between 802.11a and 802.11n. This finding enables us to fairly compare 802.11a/g and 802.11n in coexisting these network.

1.2.3.3 Conclusion

We had measured and analyzed traffic from hosts using 802.11 protocols in coexisting 802.11a/g and 802.11n wireless networks. We showed that the entropy of PIT of 802.11n was different from that of 802.11a/g. However, the entropy-based link type estimation algorithm has difficulty in distinguishing 802.11n hosts from wired hosts. We also showed 802.11a/g and 802.11n were fair in terms of transfer duration though 802.11n gained in terms of throughput.

We will investigate further characteristics of wireless network traffic to identify link types of remote hosts and to find criteria for system design as well as cross-layer characteristics (i.e., TCP).

1.2.4 IPv4/IPv6 デュアルスタック環境にて現実に発生する事象の洗い出しと考察

1.2.4.1 概要

近年、IPv4 アドレスの枯渇が迫り IPv6 の利用・移行が実サービス上でも意識されるようになり、一般ユーザ向けのアクセスサービスにおいても IPv6 で構成されたサービスが始まった。2010 年 3 月現在、アクセスサービスの一つであるフレッツサービスの一部でも IPv6 を用いたサービスを提供しているが、IPv6 クローズド網を想定した仕様となっている。このサービスとインターネットを同時に利用する場合、到達性のない IPv6 アドレスが意図せず追加で付与され、問題が発生することが確認されている。本問題は WIDE メーリングリスト上でも一時期話題となった。

そこで本実験では上記問題が発生する疑似環境を再現し、問題を体験した上での意識の強化および影響度の確認として具体的な現象とユーザ環境についての洗い出しを行った。

1.2.4.2 背景と目的

元来、アクセスサービスを利用する接続ノードにはグローバル IPv4 アドレスのみ付与される。これに加えてノードが IPv4/IPv6 デュアルスタックに対応しインターネットへの到達性がない IPv6 アドレスが付与された場合、問題が発生する。具体的にはデュアルスタック環境のノードから IPv4/IPv6 両方のアドレスが割り当てられた通信先へ接続しようと試み、最初に選んだ通信プロトコルで接続できずタイムアウトが発生した場合もう一方の通信プロトコルに切り替えて再接続する、いわゆるフォールバックが発生する。同時に、デュアルスタックに対応した OS、ソフトウェアの実装では、IPv6 を IPv4 よりも優先するものが多く、IPv6 での接続性がない場合にはタイムアウトするまでフォールバックせず、IPv4 での接続ができない。さらに、一部のソフトウェアではフォールバックしない実装となっている。

一般ユーザは、本事象が発生し対象としたサービスへ数十秒以上の遅延もしくはタイムアウトが一度でも発生すると障害が発生していると考え、以降そのサービスを利用しない可能性があり、今後の IPv4・IPv6 併用使用期間では大きな問題となる。本実験では、現状の各 OS やクライアントソフトウェアでの動作状況の検証・調査を行い、事象の体験を通した問題意識の共有および一般ユーザの影響度を量ることを目的とする。

1.2.4.3 実験

本実験を実施するにあたり、実際に問題が発生しているネットワークを合宿地に引き利用することがベストである。しかし、camp-net への影響が大きいためユーザの実験参加の選択性（他実験への参加）を考慮し、疑似環境を準備した。

- DHCP で IPv4 アドレスを配布、RA で IPv6 アドレスを配布し、デュアルスタック環境を提供
- 実験環境と camp-net 本体との接続点にルータを設置
- IPv4 では camp-net へ接続する経路を、IPv6 では到達性が無いよう、静的経路を設定

IPv4 ではインターネットへ接続可能であるが IPv6 ではクローズド網となる条件を満たした環境を再現した。また、上記ルータは PC にて構築し、DHCP ルータ、RA 配布元等のサービスおよび計測を兼ね、DHCP pool 利用者数、IPv6 アドレス利用者数を計測した。実験結果は、WIDE メンバ向けコミュニティシステムである “CSAW” へコミュニティを設置し、実験参加者が環境と事象を記載する形とし、収集した。

1.2.4.4 結果と課題

本実験への参加者は、会期を通して最高 30 名程度であった。1 参加者あたり 1 度は本現象を体感し問題意識を十分に共有できた。参加者の普段の接続環境と事象、実施している対策について議論し、今後の問題の波及について熟考できたことは成果であり実験は成功といえる。しかし、その中でも実験を意識した集中的に参加する時間が限られていたことを考えると、収集データの不足を否めないことは反省点といえる。

実験および議論の結果として、次のことを確認した。

- 大多数の OS、クライアントソフトウェアにおいて、IPv6 およびデュアルスタックが実装済みであり、IPv6 を優先しフォールバックする。一部のクライアントソフトウェアではフォールバックしない実装であり、IPv6 でタイムアウトし接続不可能であった
- 本問題のため、認識のあるユーザは IPv6 機能を停止する傾向にあり、システム管理者の間ではデュアルスタックでのサービス提供およびサーバ構築は非推奨の風潮がある
- 特定のネットワークに限らず、IPv6 のみの障害発生、ユーザが気付かぬ間に RA を投げ IPv6 での通信を阻害する現象が発生するなど、IPv6 接続性は不安定であることが多く、本実験と同様の環境が自然にでき問題が発生する

考察の結果、デュアルスタックを利用可能な環境は増えているが同時に不満なく利用できる環境は限られることを浮き彫りにした。システム管理者・ユーザともに IPv6 の利用は、問題が発生し接続に難を感じることが多く、積極的ではない状況である。この先々を考えると、サーバ運営者・コンテンツ開発者等は IPv6 対応に対し「問題発生は確実」と認識し、IPv4 アドレス枯渇後も NAT 等を利用し IPv4 延命策にて対応、IPv6 対応への意識・行動がより遅れる。さらに、コンテンツが増えないためユーザの IPv6 利用も進まず、IPv4 アドレス枯渇後に一気にパニックとなるのではないかと考えられる。IPv6 へのスムーズな利用を目指し、今後も対策を検討していきたい。

1.2.5 WIDE 合宿におけるネットワークカメラを利用した研究参加支援システム

1.2.5.1 実験の概要

さまざまなライフステージにおいて、仕事や研究への関わりかたは様々である。社会的には、仕事や研究には一定期間継続して従事することが期待されるが、個人をとりまく環境によっては継続が難しいこともある。例えば、育児や介護、あるいは病気や怪我などで仕事や研究に従事する時間が限られたり、通勤・通学が難しくなったりすることもある。これまでは、仕事や研究の継続には会社や大学にいなければならなかったため、環境が変化すると継続を断念せざるを得ないことが多かった。

しかし近年の画像や音声の電子化技術や伝送技術の発展によって、場所に縛られずに様々な情報を得たり、コミュニケーションを取ったりすることができるようになってきた。これらの技術を活用すれば、実際にその場所にいなくても仕事や研究を継続していける可能性がある。一方で、仕事や研究と育児や介護の両立においてはどちらにどの程度重心を置くかは人により、また場面により異なる。このため、遠隔からの仕事・研究への参加と同時に、遠隔での子どもや高齢者の見守りはケースに応じて使い分ける必要がある。しかし、これらの技術はシーズとしては揃いつつあるものの、システムとしては完成しておらず、実際に活用するには、ネットワーク、アプリケーションの環境を整えるほかに、それぞれの技術に対する専門知識が必要となる。

本実験では、育児中の研究者が子ども同伴で WIDE 研究会合宿に参加する場合に、特に夜の会議への参加を支援するシステムを設計し、実際の研究会にお

いて構築し実証実験を行った。会議場にいながら寝室の子どもの監視を行う「仮想子ども見守りシステム」を設計し、WIDE 研究会合宿において実際に構築、運用を行った。

1.2.5.2 実験の背景

WIDE 研究会合宿は、3 泊 4 日で朝 9 時から夜 22 時頃まで議論を行うという形態である。朝 9 時から 19 時頃までは保育園の一時預かりおよびベビーシッターを依頼することで、通常の勤務体系と同じ状況を確保するため、会議参加には特に問題はない。しかし 19 時以降は寝る準備と寝かしつけ、また寝た後は様子を見ていなければならず、これまでは 19 時以降に会議に参加することは困難であった。

まず、子どもと保護者の夜 19 時から 22 時までのだいたいのスケジュールを表 1.2 に整理する。子どもの状況に応じ、21 時前後の就寝前と就寝後とでは必要となる対応が違うため、それぞれに対して異なる要求事項が生じることになる。

子どもが就寝前に遊んでいる時間は、現状では保護者が部屋などで相手をしており会議には参加できない。しかし入眠直前でなければ部屋で過ごす必要はなく、子供も多少は動きたがる時間である。一方で会議は行われており、できれば参加したいができない時間になる。しかし子どもが会議場に入っておとなしく聞くことは不可能なため、会議場の外で会議の様子を知ることができるシステムが必要である。

子どもが就寝した後は、保護者は部屋で様子を見なければならず、やはり会議やその後の懇親会に参加することはできない。ときどき目覚めて泣くこともあるため目を離せないが、よく眠っていれば特に手がかからないため、会議にも参加したい時間帯となる。懇親会の場合は、会議の様子を知ることだけではなく直接その場に参加しなければ意味がないため、会議場から子どもの様子を知ることができるシステムが必要となる。

表 1.2. 19 時から 22 時までのスケジュール

時間	保護者	子ども
19 時	夕食	夕食/入浴
20 時	会議	遊ぶ/就寝準備
21 時	会議	就寝
22 時	懇親会	就寝

1.2.5.3 システム構成

2010 年 WIDE 春合宿では構築した仮想子ども見守りシステムは、寝室で眠っている子どもの様子を中継して会議場から仮想的に子どもを見守るシステムである。基本的には静かに寝ている子どもを中継するため、ずっと画面を監視するのではなく、泣くなどのイベントを検知して通知する仕組みを同時に構築する。保護者はイベント通知を受け取ったら画像を確認して、様子を確認する。具体的には、中継についてはパナソニックコミュニケーションズ株式会社製のネットワークカメラを利用して実現する。搭載されたカメラとマイクにより、会議場の画像と音声を取得できる。また、配信システムも装備されており、中継も実現できる。見守る保護者は無線 LAN 機能を有するスマートフォンなどの携帯端末から画像を見る。

また、音声検知と通知システムについては別システムが必要であるため、マイクとリレーを使って作成するほか、カメラの機能である動作検知機能を利用する。通知については、ネットワークカメラに装備されている、アクションによってメールや画像の保存を行う機能を利用する。

仮想子ども見守りシステムを構築するためには、研究会会場と同じネットワークを寝室にも用意する必要がある。必要となるのは、実験参加者の部屋に対してローカルなネットワークサービスを提供すること、および外部接続を利用して研究会会場のネットワークシステムに VPN を構築することである。カメラを外部ネットワークサービスに接続することも可能であるが、画像が外部に公開されることになり望ましくない。そこで、VPN の構築が必要となる。

外部ネットワークサービスについては、株式会社インターネットイニシアティブの iijmobile サービス/タイプ DS（固定グローバル IP アドレス割当）およびデータ通信カードを利用する。データ通信カードは、同じく株式会社インターネットイニシアティブ製の SEIL というルータに接続し、ローカルに接続した 3 室のネットワークから研究会のネットワークに VPN を構築する。

1.2.5.4 実証実験

2010 年 WIDE 春研究会合宿において、本システムを稼働させ実証実験を行った。仮想見守りシステムが稼働したことで、懇親会の時間に議論に参加す

ることができ、また、子どもが寝返ったり泣いたりした場合にはメールで通知され、カメラを見て寝返りなのか泣いているのかを確認してから寝室に様子を見に行くことができた。仮想会議参加システムについては、会議場の近くで子どもを見ながら発表や議論を聞くことができた。

1.2.5.5 アンケート

今回はシステムとしては 2009 年に行った実験と同じであるため、前回の課題であった、実験者以外の参加者へのメリットを探るため、アンケートを行った。その結果、同様のシステムが身近にあれば、子どもやペットなど見守りたい対象は多くあるという意見が得られ、今後応用を考えていく上で参考となった。

1.2.5.6 まとめと今後の課題

実証実験を通じて、本システムの稼働が研究活動の継続に有益であり、これまでできなかった議論に参加できたという結果を得た。

また、アンケート結果により、見守りシステムの社会的需要を知ることができ、子どもの見守り以外にも応用があることがわかった。

実験参加者の子どもの成長につれて、子どもができることも増え、システムへの要求も変わってきている。今後は要求を整理しなおすと共に、システムの再設計を行う予定である。

1.3 まとめ

本合宿では、光回線を利用した対外接続と L2TPv3 を利用した L2 トンネルを利用して、合宿ネットワークを提供した。また、そのネットワークを利用し 5 件の実験が実施された。

合宿ネットワークは L2TPv3 を利用することにより、参加者に安定したネットワーク接続を提供することができた。また、各実験においては、100 人規模の会場を利用し、合宿参加者に被験者になってもらうことにより、よりよい結果を得る環境を提供することができた。

第 2 章　WIDE Project 2010 秋合宿報告書

2.1 CAMP-PC

2.1.1 合宿運営における取り組み

2010 年秋の WIDE 合宿は「Unveiling WIDE Potential」をテーマとして、合宿運営や参加者、議論の国際化とより活発な議論の機会の醸成を中核としてプログラム運営に取り組んだ。

WIDE プロジェクトがよりグローバルな研究活動をおこない、技術の向上・普及に貢献するためには、日本人研究者が海外に出向くだけでなく、海外の研究者を日本での研究会をはじめ様々な場面で受け入れる準備が必要となる。

今回の合宿運営のロジスティックスでは、海外からの研究者が WIDE プロジェクトに参加する際の障壁をなるべく小さくするよう取り組んだ。「PayPal」の導入によって参加費支払いのオンライン化によって参加申し込みと決済プロセスをスムーズにおこなえるようにし、「英語サポート PC」は海外からの参加者にトラブルやリクエストが生じた場合に、円滑にコミュニケーションできるよう、PC メンバーから担当者を指名し会場内に設置した。

また、プレナリセッションにおける研究発表等では、英語による発表資料の作成と口頭発表を積極的に推奨した。プレナリセッションでは、日本語、あるいは英語の口頭発表の内容を英語のテキストとしてプロジェクタで逐次表示する「リアルタイムログ」を実施した。これにより、会場内の参加者が少なくとも日・英の言語のいずれかで発表内容を参照できる環境を整えた。

プログラム構成における新しい取り組みとして、ボードメンバーが屋台を出店する「ボード屋台村」を実施した。これまでの合宿で実施してきた「屋台村」とは異なり、ボードメンバーからの情報発信をコミュニケーションのトリガとして位置づけ、会場内での議論を活発化させる機会として活用した。また、海外からの合宿参加者とコミュニケーションをとる機会として「Evening Session」を導入したほか、研究発表にもゲスト参加者に登壇を促した。

その一方で、秋に実施する WIDE 合宿では、初めて

参加するメンバーの人数が多いことから、合宿プログラムとして新規参加者を対象とした「新人サポート」を実施した。新人サポートでは、新規参加者によるBoF セッションのログ作成やプレナリセッションにおけるサマリ発表を実施し、合宿期間中に参加者同士でのコミュニケーションを促進できるよう工夫した。

2.1.2 まとめと今後の課題

今回の WIDE 合宿では、プログラム構成や運営アプローチに合宿の国際化に重きを置いた。海外からの研究者や新規参加者を合宿プログラムに巻き込んで、参加者全体で活発に議論をする場を提供する当初の目標について一定の成果が上げられたと考える。

その一方で、タイムテーブルの時間配分における不備や Evening Session の時間帯設定などで、プログラムとしてバランスが悪くなった点は、今後のプログラム構成において十分な注意と改善が必要である。また、海外からの研究者とのコミュニケーションの機会が増えた一方で、議論の質がトレードオフとなる問題点は、今回の合宿では解決することが出来ず、今後も工夫が必要な点である。

新しく取り入れたプログラムや運営の取り組みは、実践方法が十分に確立されているとは言いがたく、取り組みの継続と経験の蓄積によって効果が高まると期待出来る。また、従来より指摘されている、合宿 WEB ページの構築やアナウンスのタイミングについて、十分な改善は実現できなかった。PC メンバーが数回にわたって合宿 PC を継続できるような体制を作ることで、問題解決や内容改善に向けてより効率的に取り組めると考えられる。

2.2 CAMP-NET and Experiments

2.2.1 camp-net と実験

camp-net は、WIDE 合宿参加者の合宿期間中の利便のため、また参加者を被験者とした大規模実験のテストベッドたるため、構築・運営されるネットワークである。WIDE 2010 年秋合宿では以下の 4 つの実験が行われた。

- WiFi access control by Diameter and EAP
- SA46T
- LISP による合宿ネットワーク提供
- P2P Overlay を用いた Any Source Multicast の実現

本節では camp-net の構成と実験について述べる。

2.2.2 camp-net の構成

WIDE 2010 年秋合宿の camp-net では、対外線として NTT 東日本の提供する Flet's 光ネクストによる地上線（100 Mbps）と衛星回線（下り 1.5 Mbps 上り 0.5 Mbps）の 2 回線を利用した。合宿地で WIDE インターネット配下のネットワーク（IPv4: 203.178.156.0/22、IPv6: 2001:200:0:ff00::/56）を提供するために、camp-net と WIDE バックボーンを接続する必要がある。地上線は後述する LISP 実験により、KDDI 大手町ビルまでトンネルを構築し、WIDE バックボーンへと接続した。衛星回線は WIDE 藤沢 NOC の地球局にて対地し、WIDE バックボーンと L2 で接続した。

図 2.1 に camp-net の構成を示す。

合宿参加者用のネットワークとして、表 2.1 に示す 5 種類のネットワークを提供した。合宿参加者へは無線 LAN（IEEE802.11a/b/g/n）にてネットワークへのアクセスを提供し、接続する SSID によりユーザが “SA46T” および “WiFi access control by Diameter and EAP” の 2 実験への参加を選択できるよう配慮を行った。

“-sa46t” を含む SSID を利用することで合宿参加者は “SA46T” 実験に参加することができた。同実験では、ネットワークの内部（SA46T 装置と合宿地上流ルータ間）を IPv6 のみで構成し、SA46T 装置により IPv4 パケットをカプセル化・トンネルすることで、ユーザに対しては IPv4/IPv6 のデュアルスタック環境を提供した。また、プレナリルーム、BoF 部屋 1、2 と BoF 部屋 3、4 であえてネットワークを分割することで、合宿参加者間の通信に関しても SA46T が利用されるよう構成した。

“-diameter” を含む SSID を利用することで合宿参加者は “WiFi access control by Diameter and EAP” 実験に参加することができた。同実験では moCA WG の提供する WIDE 証明書を利用し、WPA2-EAP による認証を行った。“-diameter” を含まない SSID では WPA-PSK による認証を行い、ゲスト参加者など WIDE 証明書の準備できなかったユーザーや、WPA2-EAP による無線認証の利用できないクライアントが主に利用した。

SSID “narrow” は実験に参加しないユーザ向け、および “-sa46t”、“-diameter” を含む SSID でトラブルが発生した場合のバックアップ用として、“sa46t”、“diameter” の実験と関連せず動作するネットワーク

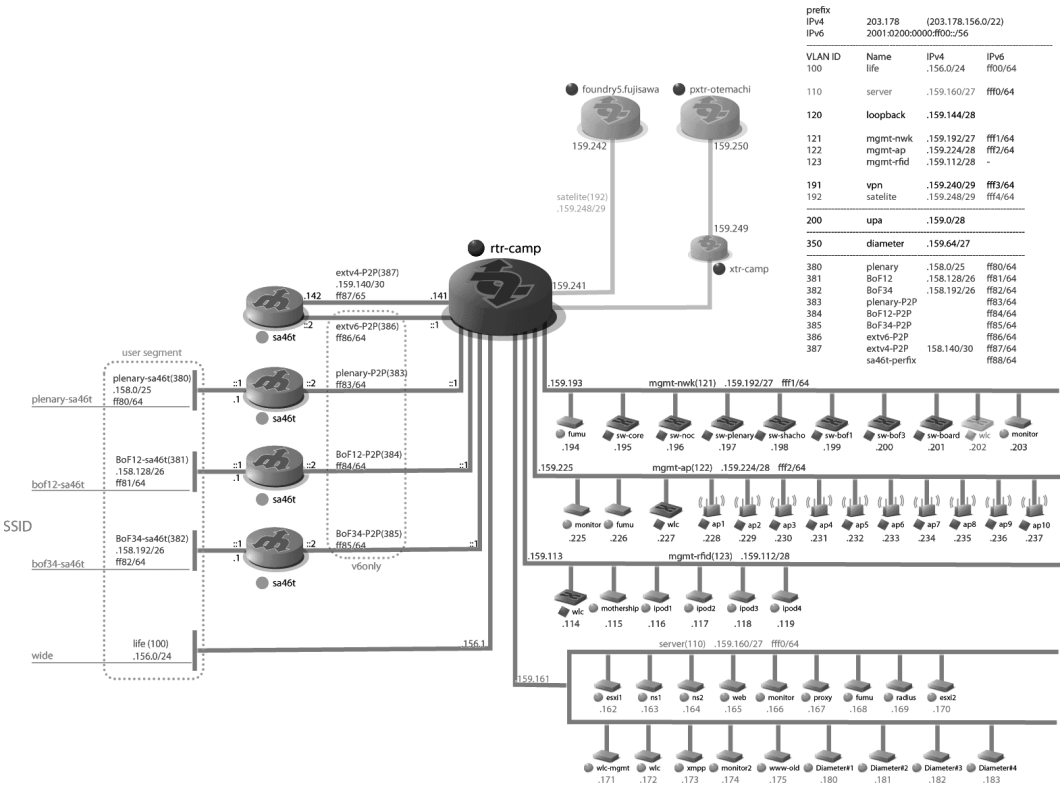


図 2.1.　camp-net L3 トポロジ図

表 2.1.　合宿参加者に提供したネットワーク

ネットワーク名	提供範囲	SSID	無線認証方式
plenary	プレナリルーム	plenary-sa46t-diameter	WPA2-EAP
		plenary-sa46t	WPA-PSK
bof12-sa46t	BoF 部屋 1、2	bof12-sa46t-diameter	WPA2-EAP
		bof12-sa46t	WPA-PSK
bof34-sa46t	BoF 部屋 3、4	bof34-sa46t-diameter	WPA2-EAP
		bof34-sa46t	WPA-PSK
narrow	全部屋	narrow	WPA-PSK
board	Board 部屋	board	WPA-PSK

として構成した。

SSID “board” は Board 部屋専用のネットワークである。Board 部屋以外の場所で提供しないことを除いて、構成は SSID “narrow” と同等である。

2.2.2.1 camp-net の運用

WIDE 2010 年秋合宿では、2010 年 09 月 08 日から 09 月 11 日に掛けて camp-net の運用を行い、合宿参加者にネットワーク接続性を提供した。図 2.2 に無線 LAN コントローラーから集計した、camp-net の利用統計を示す。延べクライアント数は 301 台であり、“-sa46t” を含む SSID に接続したクライアント数が 275 台、“-diameter” を含む SSID に接続したクライアント数が 192 台であり、合宿参加者がこれら実験に活発に参画した様子がうかがえる。

無線方式についてみると 2.4 GHz 帯（IEEE 802.11b/g/n）を利用したクライアントが 236 台（うち 183 台が IEEE802.11n を利用）、5 GHz 帯（IEEE802.11a/n）を利用したクライアントが 161 台（うち 159 台が IEEE802.11n を利用）となっており、WIDE 合宿参加者の持つデバイスのなかで IEEE802.11n の普及が進んでいることも明らかとなった。

WIDE 2010 年秋合宿の camp-net 運用の中では、

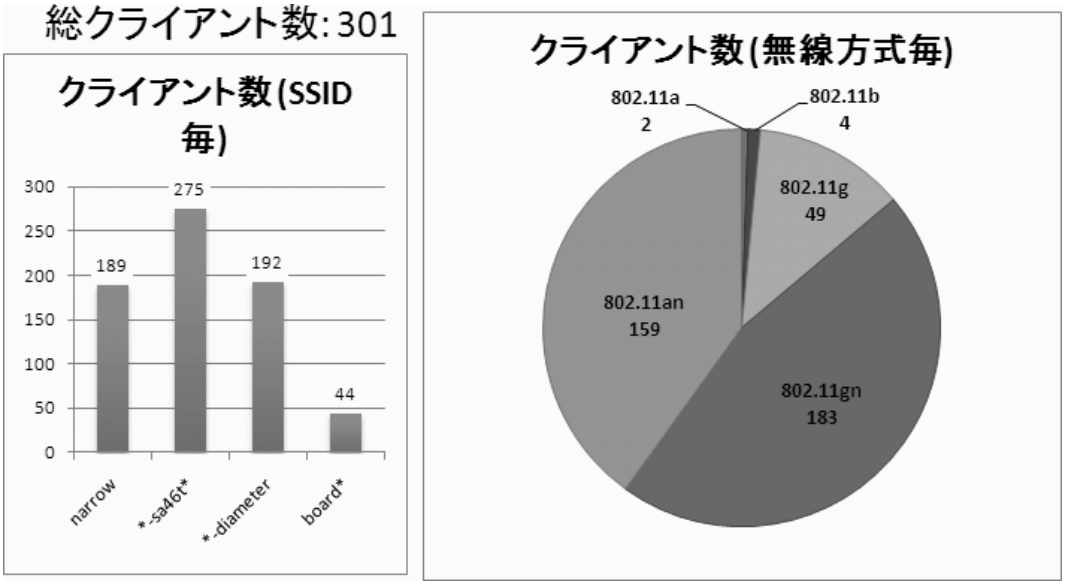


図 2.2. camp-net WiFi 利用統計

トラブルもいくつか発生した。トラブルとその発生原因、今後に役立てられるべき知見について記す。

1. 09 月 08 日 16:40–20:40 に掛けて、衛星回線が切断され完全に利用できなくなった。これは当該時間帯に衛星回線の地球局がおかれた藤沢地方を台風 9 号が通過した、天候不順によるものである。幸い衛星回線の位置づけは Backup であり、地上線にトラブルがなかったことからユーザへの影響は発生しなかった。

2. 09 月 08 日 16:40–18:30 に掛けて、“plenary” ネットワークに接続したクライアントがIPv4 アドレスを取得できない問題が発生した。プレナリルームでは実験参加用の “plenary”、実験非参加用の “narrow” という 2 種類のネットワークが提供されており、ユーザが接続するネットワークを選択できる形式であった。当該時間帯のプログラムがすべてプレナリルームで行われたことに加え、ユーザが “plenary” ネットワークに集中したため “plenary” ネットワークの DHCP pool から IPv4 アドレスがすべて払い出されたことにより問題が発生した。18:30 からの夕食時間中、合宿参加者のネットワーク利用が少なくなったタイミングを計り、ネットワークのリナンバリングと “plenary” ネットワークの DHCP pool へアドレスを追加し、この問題を解決した。

合宿参加人数が 200 名程度であったことから、“plenary” ネットワークは /24 の IPv4 アドレスセグメントとして設計されていた。実験の要求から、合宿地ネットワークを単一のセグメントとして構成できず、全体で /22 ある IPv4 アドレスを細かく分割して利用せざるを得なかったこと、また実験に不具合が生じた場合の備えとして実験参加用のネットワークと非実験参加用のネットワークを設けたことで、大きなアドレスブロックの確保が困難だったこと、その 2 点が本問題の発生した原因である。今後、同様に実験の要求からネットワークを分割する場合、NAPT 装置などの利用により必要なアドレス空間を確保する必要が考えられるだろう。

また、WiFi の利用統計からもわかるように、camp-net を利用したクライアント数は 300 台を超えており、想定を超えて単一の参加者が複数台のデバイスを camp-net に接続していることが判明した。この傾向は今後の合宿でも同様であると考えられ、単純に合宿参加人数から必要アドレスブロックを計算するべきでないという教訓も生まれた。

3. 09 月 09 日–09 月 11 日に掛けて、“plenary” ネットワークにて、クライアントが接続後 30 分程度経過すると IPv4 にて通信できなくなる問題が発生した。

問題が発生していた期間中、合宿 PC が原因の特定に取り組んだが原因わからず不明であり、根本的解決には至らなかった。次善の対策として、問題発生時には “narrow” ネットワークを利用するようユーザに促すことで対応した。

現象としては、DHCP pool には払い出し可能な

IPv4 アドレスがあるにもかかわらず、クライアントが接続後 30 分程度で DHCP から取得したアドレスを更新できなくなり、また DHCP からアドレスの再取得もできないため通信できなくなるため発生する問題であることが判明している。DHCP のパケットの追跡から、無線 AP-無線 AP コントローラの間でパケットが失われることまで判明したが、発生条件やそのような挙動のおこる原因についてはついぞ究明がかなわなかった。

ただ、“plenary” ネットワークと L2 的に同じ構成で、実験の有無のみ異なる “narrow” ネットワークにて、本問題が発生しなかったことから、実験との関連が疑われる。一方で、合宿ネットワークとほぼ同じ構成で望んだ HotStage 中には発生しなかった問題であり、2. の問題解決のため “plenary” ネットワークのアドレスをリナンバリングした後から発生していることから、クライアント数の増加と実験の影響との複合的な要因からなる問題だった可能性がある。

行われる実験の性質によって、原因特定の困難な性質の問題が発生することは今後も十分考えられる。実験参加用のネットワークと非実験参加用のネットワークを分割するネットワークデザインを行うことが今後も推奨される。それにより非実験参加用ネットワークを、実験に起因することが疑われる問題が発生した際のラストリゾートとして、また問題の切り分けのための比較対象として利用できるだろう。

2.2.3 WiFi access control by Diameter and EAP

AAA WG has implemented Diameter-related protocols such as Diameter Base Protocol, Diameter EAP Application, and EAP-TLS for access control to WiFi. We would like to validate the stability of our implementations by having WIDE members use our system.

2.2.3.1 What is Diameter?

Diameter[29] is a back-end protocol that carries Authentication, Authorization, Accounting (AAA) information between the AAA client and the AAA server. In Diameter protocol, requests and answers are represented by AVPs (Attribute Value Pairs). The basic functions are capability negotiation and accounting, and extensible by adding new commands or AVPs. There are several Diameter applications, such as Network Access Server application[30], EAP application[48], SIP application[62], etc.

EAP application is a one of Diameter applications for user authentication and authorization, used for network access control. EAP[1] is a Extensible Authentication Protocol, that supports multiple authentication methods such as EAP-TLS[164], EAP-TTLSv0[61], EAP-GPSK[34], etc.

Diameter potocol has several advantages over RADIUS protocol.

- multi-realm support
- message transport reliability (TCP/SCTP)
- message security (TLS)
- failover support
- extensibility, new applications/commands
- server initiated message
- introduction of agents. proxy agent, relay agent, redirect agent, translation agent

2.2.3.2 freeDiameter and DiamEAP

freeDiameter is an open-source of Diameter Base Protocol developed by sebastien@nict. freeDiameter is in comformance with RFC 3588 and 3588-bis and other Diameter applications can be implemented as extensions.

`http://www.freediameter.net/`

DiamEAP is an open-source of Diameter EAP application developed by souheil@tera. DiamEAP includes codes of EAP-TLS and EAP-MD5 and other EAP methods can be implemented as plug-ins.

`http://diameap.yagami.freediameter.net/`

2.2.3.3 WIDE camp experiments

We've installed two Diameter servers that authenticate users and two gateways that translate the authentication protocol from RADIUS into Diameter, and vice versa. If a user selects one

of our AP, the user's PC requests authentication by IEEE802.1X to the AP. The AP translates the request from IEEE802.1X into RADIUS and sends the request to the gateway we installed. The gateway translates the request from RADIUS into Diameter and sends the request to the Diameter server we installed. Then, the user is authenticated by the Diameter server and the user is allowed to access the WiFi AP.

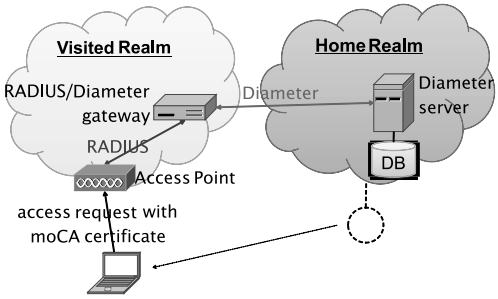


Fig. 2.3. Basic System Structure of Diameter and EAP Experiment

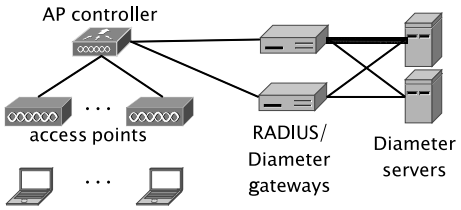


Fig. 2.4. Logical topology of Diameter and EAP Experiment

Fig. 2.3 shows the basic system structure of the Experiment and Fig. 2.4 shows the logical topology of Diameter and EAP Experiment.

We've measured following items.

- Basic performance (authentication time)
  - # of clients
  - local server@camp vs. remote server@teralab.
  - changing session lifetime (1 hour ? 10 min)
- failover transparency
  - intentional failure of a gateway or a server
- statistics

As a result of this experiment, we expect to enhance the quality of our implementations. We also plan to submit some papers to workshops and journals.

Fig. 2.5 shows authentications per hour in WIDE camp period. The system work well in the period.

2.2.4 LISP による合宿 NW 提供実験

WIDE 合宿として初めて、LISP（Locator/ID Separation Protocol）を利用した合宿ネットワークの提供実験を行った。例年の WIDE 合宿は、一般インターネット回線上で GRE や L2TP などのトンネル技術を用いて、合宿地と WIDE インターネットを

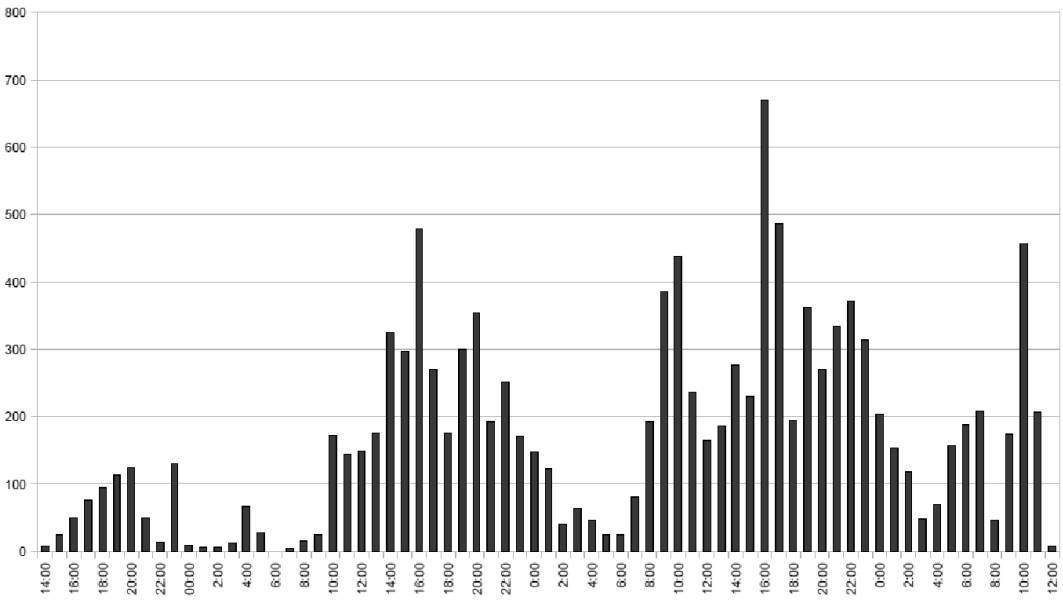


Fig. 2.5. Result of Experiment: Authentication per hour

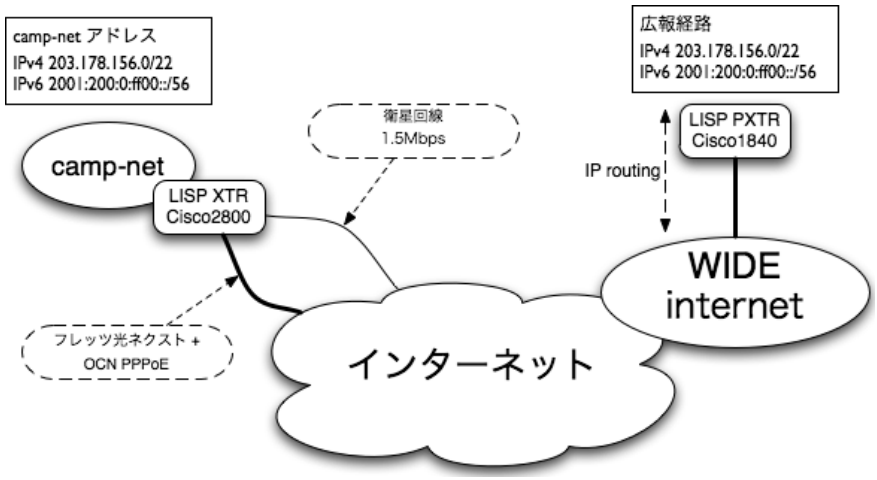


図 2.6.　合宿 NW の全体構成

結んでいる。トンネルによる仮想回線上で ip routing を行い、合宿地のインターネット接続は提供される。今回は通常の ip routing は用いずに LISP を利用することで合宿ネットワークのようなバックボーンから切り離された飛び地のネットワークを提供できるのか試みた。

2.2.4.1 LISP を利用した合宿 NW の構成

合宿ネットワークは例年通り、NTT のフレッツ回線と衛星回線が準備された。衛星回線は WIDE 藤沢 NOC へ接続され、専用線として利用出来るので、トンネルなどは必要ない。フレッツ回線は ISP に接続されるので、合宿ネットワーク内で WIDE インターネットの IP アドレスを使用するために例年は WIDE バックボーンへトンネルによる仮想回線接続が行われる。

今回の合宿では、外部接続ルータを LISP XTR とした。H/W は Cisco2800、S/W は IOS15.1XB2 である。さらに LISP PXTR を WIDE KDDI 大手町 NOC に設置した。H/W は Cisco1841 で S/W は XTR と同様である。WIDE バックボーンとの IP routing 接続は PXTR が代理で行う（図 2.6）。

IPv4 のトラフィックフローは、合宿ネットワークから見てダウンロード方向は一旦 PXTR に IP パケットが届き LISP カプセル化により XTR に送られる。アップロード方向はフレッツ回線の接続 ISP ネットワークをそのまま利用する。このとき NAT のようなアドレス書き換えは行われず、合宿ネットワーク内の IPv4 アドレスがそのまま使われる。

IPv6 のトラフィックフローは、ダウンロード方向は IPv4 と同様である。アップロード方向は処理が異なり、LISP カプセル化により PXTR へパケットが送られる。これはフレッツ回線の ISP にて IPv6 接続性が提供されていないためである。このように IPv4 回線を利用して IPv6 パケット転送を行う機能を LISP は有している。

衛星回線は当初はバックアップ回線として設定され、使用しなかった。

2.2.4.2 利用実験結果

3 日半の合宿ネットワークのトラフィック量は、XTR のフレッツ回線側で計測すると以下のようになる（図 2.7）。これは過去の合宿や他のイベントと比べて、参加者 200 人程度のイベントネットワークとして一般的な結果と考えられる。

合宿期間中は LISP 提供機器の CPU 負荷は 5 分間平均で常に 2%以下となるなど処理能力上の問題は発生しなかった。また過去の合宿ネットワークにて発現した、トンネル使用時の IP MTU サイズに纏わる通信不具合などは起こらなかった。

今回の結果より、WIDE 合宿ネットワークのように、遠隔地へ IP アドレスを持ち込み短期間使用するネットワークにおいて LISP を使用することは有用であった。さらに、通常 IP アドレス持ち込みでは、接続サービスを受ける ISP との調整に長い時間を要し、IP パンチボールを引き起こすなどの運用上の問題も発生させる。そのような問題も LISP の使用で回避することが可能である。また IPv4 のインターネット接続性しか準備できない場合に IPv6 サービスを提供できる点でも使用できる。

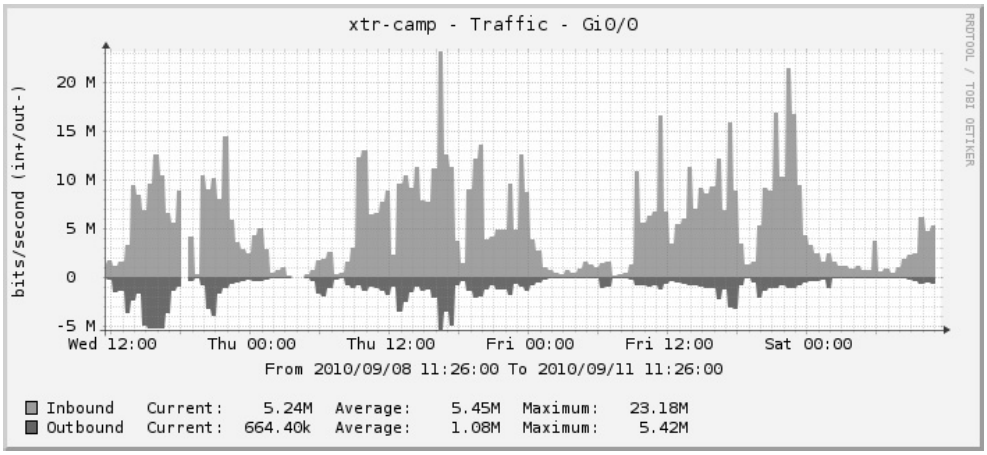


図 2.7. フレッツ回線のトラフィック量

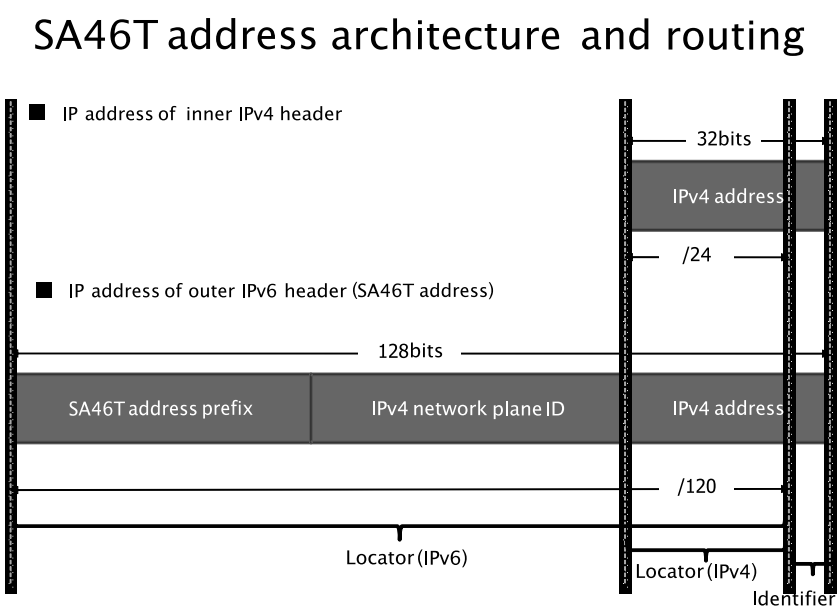


図 2.8. SA46T address architecture and routing

2.2.5 SA46T

2.2.5.1 概要

sa46t（Stateless Automatic IPv4 over IPv6 Tunneling）は、バックボーンネットワークの IPv6 only 化を可能とする技術で、現在、IETF（The Internet Engineering Task Force）にて提案・議論されている。2010 年 9 月に開催された WIDE 秋合宿に於いて、sa46t の実証実験を行った。この実験について報告する。

2.2.5.2 sa46t 技術について

sa46t は IPv4 over IPv6 自動トンネリングの技術である。技術を要約すると、(1) IPv4 アドレスのロケーターとアイデンティファイアーの境界を維持して IPv6 アドレス（sa46t アドレス）を自動で生成し、それぞれロケータ部の経路を広告すること、(2) IPv4 アドレスの上位に IPv4 network plane ID という領域を設けることによりひとつの IPv6 バックボーンネットワーク上に複数の IPv4 ネットワークを多重化できること、である。図 2.8 は、IPv4 アドレスと sa46t アドレス（IPv6）の関係を説明するものである。従来のトンネル技術はひとつのインタフェースとひとつのインタフェースを接続する、つまり点と点を線で結ぶ技術と言えるが、sa46t はサブネットとサブネットを IPv6 で接続する技術と言える。別の見方をすると、sa46t は IPv4 ネットワークの面を

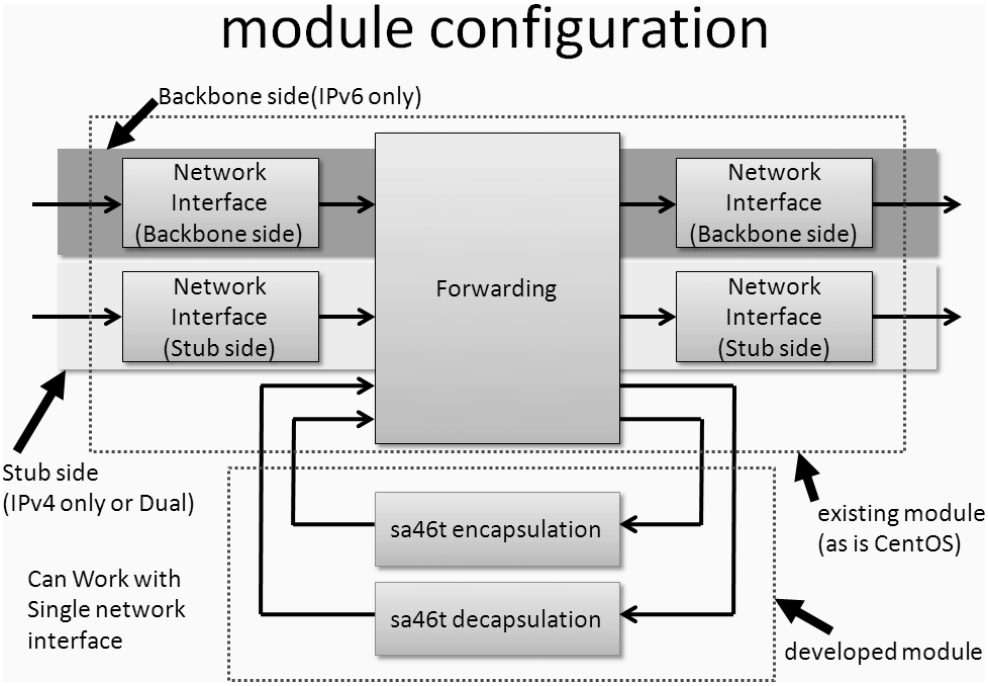


図 2.9.　SA46T module configuration

作成し、その面に加わるサブネットを指定する、つまり面を構成していく技術であるとも言える。主な特徴を 3 つだけ記載すると、(1) ロケーターとアイデンティファイアーのマッピングを IPv4 から IPv6 で行っただけなので、既存のルーティングプロトコルをそのまま使えること、(2) N 箇所をフルメッシュでつなぐためには N 個の設定のみすればよいこと（既存技術では $N(N-1)$ 個の設定が必要）、(3) トンネル終点の冗長化が可能であること、である。

2.2.5.3 sa46t 標準化提案の状況

sa46t の最初の Internet-Draft[113, 114] は、2010 年 2 月 1 日に発行され、3 月に開催された IETF Anaheim 会議に於いて v6ops WG にて提案 [115] が行われた。2010 年 7 月 3 日に改版された Internet-Draft[113, 118] 及び適用に関する新規の Internet-Draft[117] が発行され、第 78 回 IETF Maastricht 会議に於いて、softwire WG にて提案 [116] が行われた。そして、9 月の WIDE 合宿に於いて sa46t の実験が行われた。

2.2.5.4 sa46t の実装

sa46t の実装開発の目的は (1) 実装可能であることの実証、(2) 正しく動作し想定する以外の問題が発生しないかを実際に動作させて確認する方式の実証である。実装モジュールのアーキテクチャを図 2.9 に示す。sa46t のカプセル化／デカプセル化処理を行うか否かは、ルーティングテーブルの設定で起動される構造になっている。なお、この構造は、収容する複数の stub network の IPv4 アドレスがユニークでなければならないという制約があるが、今回の実証目的を達成するには十分である。もし、IPv4 network plane を用いる構成で、IPv4 アドレスの再利用に対応する構成とするなら、ネットワークインタフェース毎の Inner Header を処理するルーティングテーブル（Dual Stack）と Outer Header を処理するルーティングテーブルを分離したアーキテクチャを採用すればよい。また、今回採用したアーキテクチャは一個の Ethernet Interface でも動作する。この場合は、IPv6 Packet のフォワーディングは行わず、IPv4 パケットのみ処理するような構成が可能となる。実装は、CentOS をベースにカーネル空間で動作するソフトウェアとして開発された。実装規模は C 言語で約 300 step である。本ソフトウェアを、ネットブックに分類される PC である、Fujitsu FMV-BIBLO LOOX M/G30 （Atom N450 1.66 GHz、1 GByte memory、Fast Ethernet）に USB Fast Ethernet Dongle を接続した構成にインストールした。この

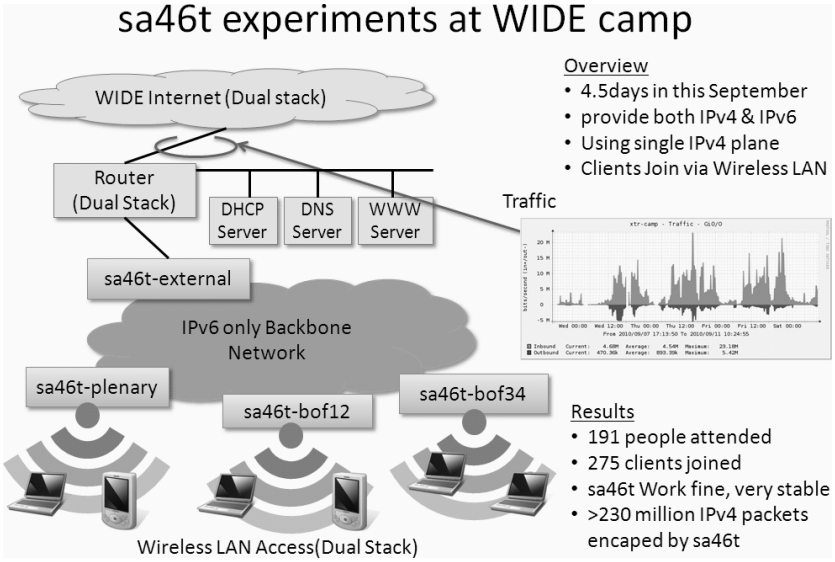


図 2.10. sa46t experiments at WIDE camp

ハードウェアで 90 Mbps を超える性能を確認した。約 3000 ステップと小さい規模であり、性能がさほど高くないハードウェアでも高い性能を出せることを実証した。

2.2.5.5 WIDE 合宿での実験

本実装を用い、9 月 8 日から 9 月 11 日に開催された WIDE 合宿の場で実験を行った。図 2.10 は、sa46t の実験のみを簡略化して表した図である。4 台の sa46t を用い、4 日間半の間、連続動作させた。今回の実験では、1 個の plane のみ使用した。実験への参加は、*-sa46t-* という SSID の無線 LAN に接続することにより行われ、IPv4 の場合 DHCP で、IPv6 の場合 RA の配布によりアドレス割り当てがなされる。実験結果は、191 名が実験に参加、接続された総クライアント数は 275 台で、約 2.3 億個の IPv4 パケットが sa46t によるカプセル化／デカプセル化が成された。sa46t はきちんと機能し、細かいトラブルもあったが、非常に安定して動作した。

2.2.5.6 sa46t-as

WIDE 合宿に於ける sa46t 実験の良好な結果を得たためか、IPv4 アドレス共有の機能を sa46t の仕組みを拡張すれば容易に対応可能であるとの着想を得て、新たに、sa46t-as（as は IPv4 Address Sharing の略）の Internet-Draft[119] を執筆し提出した。

2.2.5.7 79th IETF Beijing 会議でのプレゼン

WIDE 合宿での実験結果を IETF 会議で報告すべく準備を行ったが、softwire WG 開催の前日に突然スライド枚数の削減要請が議長より出され、急遽対応した [120]。このため、短い時間ではあったものの、WIDE 合宿で実験がうまくいった旨の報告を行なった。

2.2.5.8 まとめ

sa46t の方式の有効性の確認を、実装し、そして WIDE 合宿の場で実際に動作させて実証した。標準化提案を行っている技術の実装を作成し実験室レベルの小規模な環境で動作確認を行うことは難しくない。しかし、数百人規模の人に実際に利用して貰えるような環境を新たにゼロから用意することは、非常に難しいと言えるだろう。しかし、WIDE 合宿の場であれば、それが可能であり、上記に記載した通り、200 名弱が 300 台弱の端末を用いて 4 日間に渡って実利用を行った。端末の種類も WIDE ならではで、多種多様であった。このような場は WIDE 合宿以外には無いだろうし、WIDE 合宿が如何に貴重な場であるかを改めて認識した。この成果を標準化活動に活かしていきたい。最後に、本実験を強力にサポートして頂けた Camp Net 長をはじめとする Camp Net の皆様、実験で連携を頂けた実験参加者の皆様、Camp PC 長をはじめとする Camp PC の皆様、そして合宿に参加された WIDE メンバの方々に感謝致します。

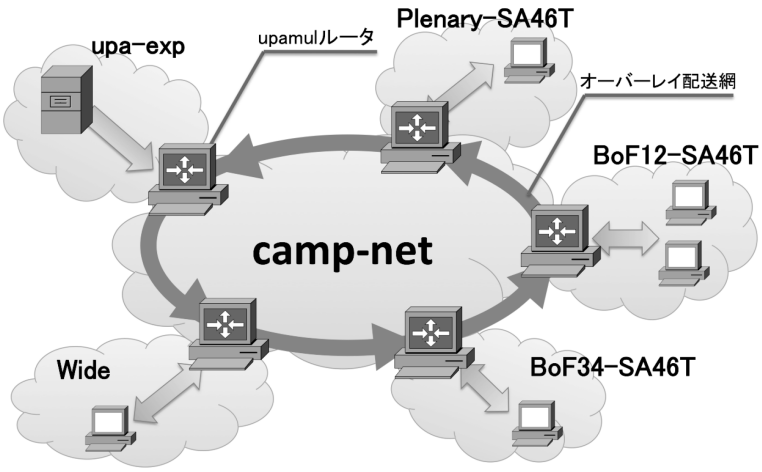


図 2.11.　実験トポロジーの概要

2.2.6 P2P Overlay を用いた Any Source Multicast の実現

本実験では、世界規模でのユーザによる自由な Any Source Mutlicast の実現を目的とするアーキテクチャである Universal P2P Architecture for feasible IP Multicast（upamul）の合宿ネットワークにおける運用を行った。多数のユーザを収容する実ネットワークで運用することにより、現在のプロトコルや実装の問題の洗い出しを行った。

2.2.6.1 手法概要

本手法は、ユーザを収容するエッジネットワークに IP マルチキャストを用い、エッジネットワーク間の配送網をオーバーレイネットワークで構築することによって、ユーザによる自由な 1 対多型の通信を実現する。現行の大抵のホストは既に IP マルチキャストを使用可能であるため、それらのホストは特に変更することなく upamul の構築するマルチキャスト網に参加することができる。さらに、upamul が利用する IP マルチキャストは IP 層の機能であるため、アプリケーションは透過的にこのマルチキャスト網を利用することができる。

また、配送網をオーバーレイネットワークで構築することによって、バックボーンの構成に影響されることなく配送網を広域に構築することができる。さらに、配送網となるオーバーレイネットワークをリングトポロジーで構築することにより、ソース毎のトポロジーを計算する必要を無くし、Any Source Multicast を実現する。また、このリング状のオーバーレイの配送網はマルチキャストグループアドレス毎に構築される。これによって、グループアドレス毎のトラフィックを必要な upamul ルータのみで構築される配送網内に限定し、余剰なトラフィックを削減する。

2.2.6.2 実験環境

本合宿において構築されるネットワークのうち、ユーザを収容する全てのセグメントに実装した upamul ルータを設置することで、合宿参加者に対して Any Source Multicast できる環境を提供した。実験に絞って簡略化したトポロジーを図 2.11 に示す。また、ユーザを収容するセグメント以外に、専用に用意されたセグメントに upamul ルータとビデオストリームの送信ノードを設置し、合宿期間中ビデオストリームを流し続けた。計測項目としては、各 upamul ルータにおいてマルチキャストグループアドレス毎に、帯域、パケット数を、upamul ルータ毎にコントロールパケットのパケット数、グループ数を計測した。

2.2.6.3 実験結果

実験の結果、配送用のオーバーレイネットワークのトポロジーを維持するためのプロトコルに問題を発見した。upamul はマルチキャストグループアドレス毎にオーバーレイでリングトポロジーの配送網（Group Channel）を構築する。その際、全ての upamul ルータは Group Channel 毎に自ルータの 2 ホップ先までの upamul ルータのアドレスを記憶する。また、全ての upamul ルータは自ルータのネクストホップに対して定期的に生存確認を行っており、ネクストホッ

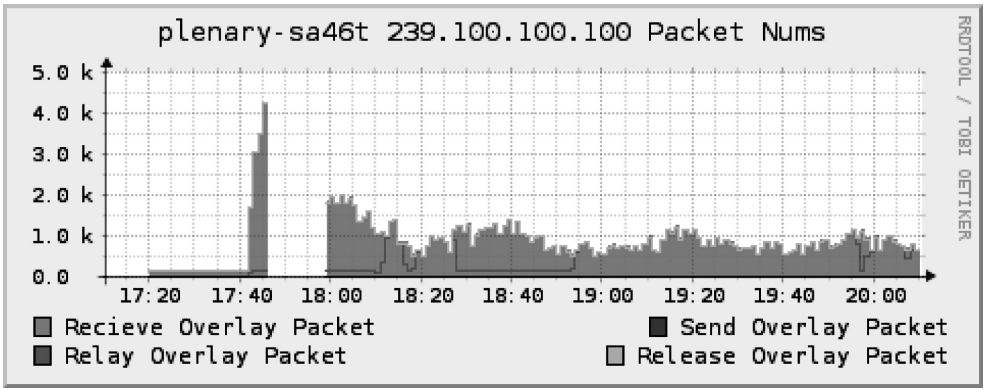


図 2.12. 送受信したパケット数

プのルータが離脱した際には 2 ホップ先のルータをネクストホップに変更することでリングトポロジーを修復する。しかし、このアルゴリズムではルータ離脱の誤検知によって問題が起こることが分かった。

配送網がオーバーレイであるため、実際にネクストホップの upamul ルータが離脱していなくても、生存確認用のパケットが途中で消失することによって、ルータがネクストホップが離脱したと誤検知することがあった。upamul ルータが A、B、C の順番で並んでいるとする。A と B の間で生存確認パケットが消失した際、A は B が離脱したと認識し、ネクストホップを C に変更する。C は、自身の前ホップが A になったと認識し、B からの生存確認に応答しなくなる。すると、B は C が離脱したと誤検知する。このように、1 箇所の誤検知によって、連鎖的に復旧処理が発生してしまうことが分かった。

また、Group Channel の前ホップから受信したパケットよりも、ネクストホップへと送信したパケットの方が少なくなる現象が確認された。これを表すグラフを図 2.12 に示す。Group Channel の前ホップから受信したパケット数（Recieve Overlay Packet）と、カプセル化を解いてサブネットへと送信したパケット数（Release Overlay Packet）が同じパケット数が同じであることから、カプセル化を解いてサブネットへ送信した後、カプセル化されたパケットを Group Channel のネクストホップへとフォワードする際にパケットロスが起きていることが分かった。

2.2.6.4 今後の課題

今後の課題として、まず実験から分かった復旧プロトコルの修正と実装を行う必要がある。さらに、カプセル化されたパケットのフォワーディング部分で起きるパケットロスの原因解明と修正をする必要がある。また、upamul は IP マルチキャストを用いて 1 対多型の通信を行うため、upamul の配送網を利用するアプリケーションは、必然的に IP マルチキャストに対応したアプリケーションに限られる。しかし、現在のインターネットでは IP マルチキャストを利用可能なネットワークは少なく、それに伴い IP マルチキャストを利用するアプリケーションも普及してはいない。そのため、このアーキテクチャをデプロイしていくにあたって、IP マルチキャストを利用するアプリケーションも同時に開発していく必要がある。

2.3 総括

今回の WIDE 合宿では、プログラム面では国際化への取り組みが注力され、Evening Session など新たなプログラムを提供する試みも行われた。新しい取り組みの常として、課題や改善すべき点も散見されたが、それらは今後の取り組みの継続と経験の蓄積により改善可能と信ずる所である。そのために何より、合宿 PC のメンバーが数回の WIDE 合宿で継続して合宿 PC として取り組める体勢づくりが求められる。

ネットワークと実験の面では、2010 年秋の WIDE 合宿 camp-net では合宿参加者に期間中のネットワークを提供すると共に、参加者を被験者として “WiFi access control by Diameter and EAP”、“SA46T”、“LISP による合宿ネットワーク提供”、“P2P Overlay を用いた Any Source Multicast の実現” という 4 つの実験が行われた。各実験について、期待される成果が得られる、あるいは 200 人規模のイベントネットワークで運用されたからこそわかる問題点が明らかになるなど、有意義な camp-net と実験であったと言える。