

第XX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20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 2001年秋合宿ネットワーク

この章では、2001年9月に行われた2001年度WIDEプロジェクト秋合宿におけるネットワーク構成および、そのネットワーク上で行われた実験結果について報告する。

1.1 ネットワーク構成

ここでは、2001年度秋合宿ネットワークの全体構成を説明する。図1.1に合宿ネットワーク全体のトポロジを示す。トポロジ図において、四角はルータもしくはホストを示す。線、破線、二点鎖線等は、イーサネット、ATM回線、衛星回線等を示す。上側1/3は慶應大学湘南藤沢キャンパス(以下SFC)側のネットワークであり、下側2/3が合宿地側のネットワークである。

WIDEインターネットバックボーンとは、camp-entryと書かれたルータを介して接続されている。SFCと現地との間は、ATM-fujisawa/ATM-shirakaba間のATM回線(1.5Mbps)とSAT-fujisawa/SAT-shirakaba間の衛星回線(768Kbps双方向)で接続された。なお、DialupRouter2台を接続しているINSは非常用であり、何らかの要因でATM、衛星回線ともに使用不能となった場合に最低限の接続性を得るためのバックアップである。

合宿地側のネットワークは、後述する「優先制御ポリシデリゲートによるトラフィック優先制御実験」の一貫として準備されたALTQを用いた優先制御用ルータを介して、会議が行われている各会場のネットワークを提供した。また、Wireless(IEEE802.11bを使用)ネットワークについては、「無線は最後まで無線」というポリシーの基、衛星回線を使用した外部接続性を提供した。なお、合宿地側中央部にあるhatchanと呼ばれるホストは、各セグメントにDHCP、DNSサービスを提供するとともに、合宿地内のWebサーバとしての機能を持つものである。全セグメントを

一括して管理することにより、管理工数の削減および、各実験で不具合が生じ、他のセグメントへの到達性が失われた場合でも、Webによる障害告知が可能になること等を考慮して設計されている。

1.2 合宿ネットワークを利用した実験項目

2001年度秋合宿では、以下の8つの実験が行われた。

- 優先制御ポリシデリゲートによるトラフィック優先制御
- IPv6/IPv4トランスレータ「TTB」によるUDPトランスレーション実験
- IPv6上のSIPプロトコルによるVoIP通信実験
- MobileIPv6実験
- Honeypotを用いたDeception Network実験
- XCAST実験
- 分散プローブによるセキュリティおよびトラフィック監視実験
- Passive and Active Measurement of WWW Server

これらの実験について、以下に報告する。

1.3 優先制御ポリシデリゲートによるトラフィック優先制御

実験者 小島 元、海崎 良
所属 慶應義塾大学

1.3.1 実験の目的

現状のインターネットでは、フローによる識別が直ちに通信しているホストの識別に結びつかない問題がある。それは、例えばNATなどの中間ノードがフローの識別に使用するIPアドレスなどの情報を書き換えてしまうケースがあるためである。

本実験ではNATやIPv4-v6トランスレータによるトラフィック情報の隠蔽化の影響をうけないトラフィック優先制御機構の構築を目的とした。

1.3.2 実験の概要

ボトルネックとなる回線が明らかな場合、通常その回線に直接面するルータにおいてトラフィック優

WIDE Project CAMP Autumn 2001
Topology Map

update:2001.9.8

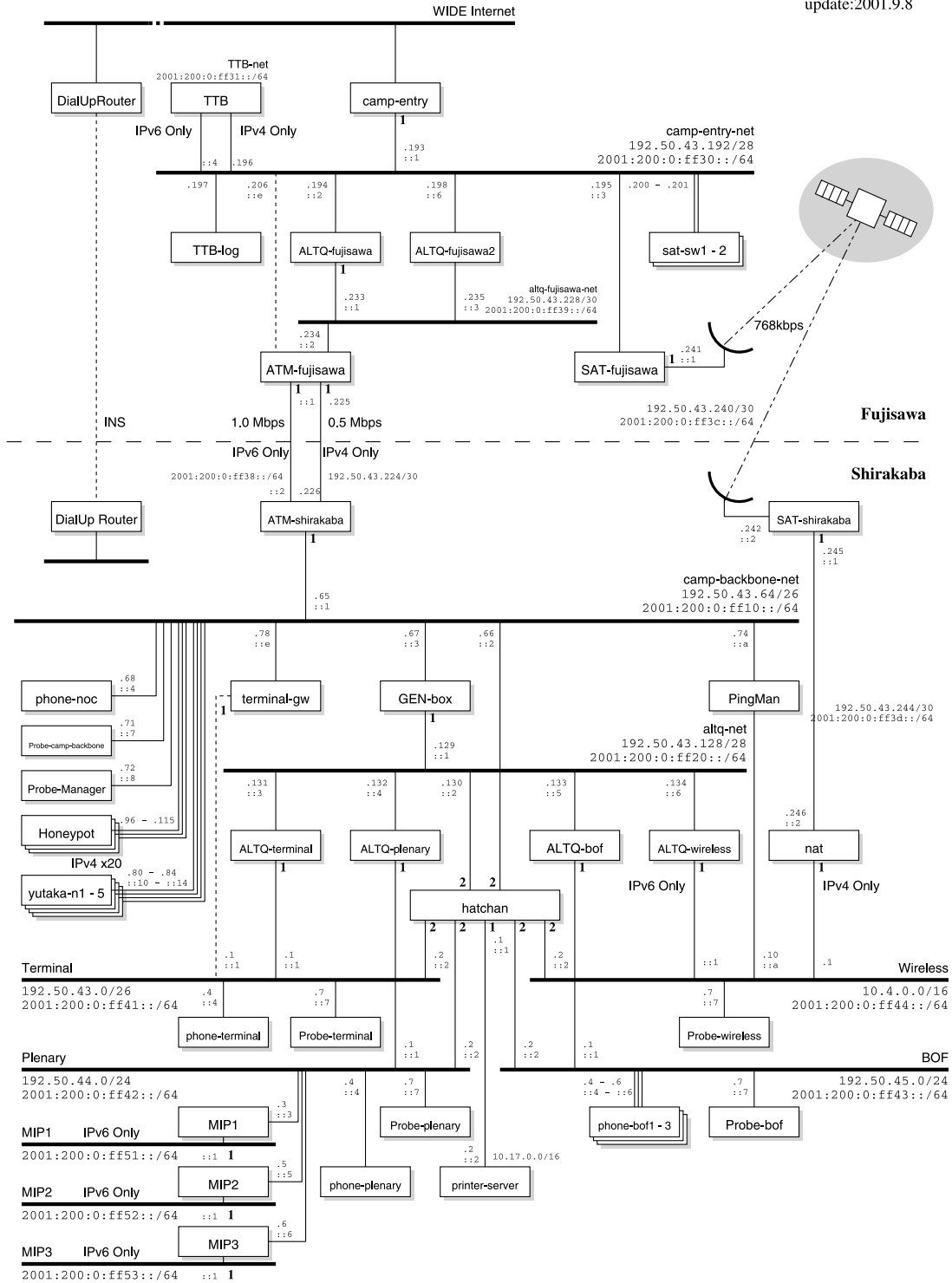


図 1.1. 2001 年度秋合宿ネットワークトポロジ

W I D E P R O J E C T 2 0 0 1 a u t u m n r e p o r t

先制御を行う。しかしトラフィック情報を隠蔽化する機構を含むネットワークでは有効に機能しない。よって本実験ではボトルネックに面するルータではなく、下位ルータである NAT や IPv4-v6 トランスレータでトラフィックの識別した。また各ノード毎の重み付けによるトラフィック優先制御を行った。結果、情報が隠蔽化された環境において公平なトラフィック優先制御が可能となった。

図 1.2 に概念を示す。

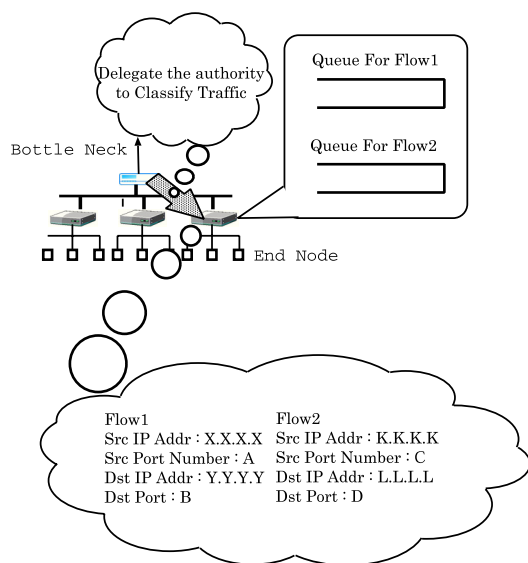


図 1.2. 優先制御ポリシーのデリゲート

1.3.3 実験の環境

合宿ネットワークではボトルネックとなる 1.5 Mbps の対外線を 4 個のセグメントで共有した。ボトルネック回線以外は 802.11b および 100Base-TX で構成されており、最大 300 個のエンドノードが存在した。セグメントは部屋ごとに分かれており、各セグメントに属するエンドノードの個数が時間により大きく変動する環境である。

1.3.4 結果と考察

本実験ではトラフィックの情報を隠蔽化してしまう機構が存在するネットワークでのトラフィック制御機構の構築に成功した。よって NAT や IPv4-v6 トランスレータの存在するネットワークにおいて、それらを意識すること無くトラフィック優先制御を行うことが可能となった。

解決方法としてエンドノードの優先度別に、ボト

ルネック上の帯域資源を割り振る方法を取った。下位ノードから優先度の合計を上位ノードに伝搬し、上位ノードがその優先度から各下位ノードの帯域資源の割り振りを決定する。各下位ノードはエンドノードの優先度を保持する。下位ノードは各エンドノードの優先度、エンドノードのトラフィック量、および割り当てられて帯域幅から、エンドノード毎の帯域制御を行う。

本機構は複数ルータによる分散トラフィック優先制御を行う仕組みとなった。また、本機構は優先度が動的にかわる環境にも対応できる。従って本研究では動的に帯域制御を行う、中間ノードによる分散トラフィック制御を行う機構の作成に成功した。

今後の課題としてエンドノード別の優先づけ、適応型トラフィックである TCP のフローコントロールをいかにしておこなうか、が挙げられる。

1.4 IPv6/IPv4 トランスレータ「TTB」による UDP トランスレーション実験（及び MIP6 との連携実験）

実験者 秋定 征世

所属 横河電機株式会社

1.4.1 実験の目的

IPv6/IPv4 トランスレータ「TTB」プロトタイプは、従来の IPv6/IPv4 TCP トランスレート機能に加えて新機能として、IPv6/IPv4 UDP トランスレート機能と MIP6 のコレスポンデントノード機能を搭載した。本実験では UDP トランスレート機能が実験環境ネットワークにおいて有効であることを確認し、またモバイルノードからの通信をトランスレートできることを確認することで、トランスレータと MIP6 が共存できることを実証する。

1.4.2 実験の概要

トランスレータ/DNS サーバ搭載 TTB(1) を IPv6 ネットワーク上のクライアントから到達できる位置に配置する。IPv6 クライアントが IPv4 サーバと通信するとき、TTB に名前を問い合わせることで IPv4 サーバのアドレスを基に生成された IPv6 アドレスを得ることができる。こうして得られた IPv6 アドレスへの通信を TTB が IPv4 サーバへの通信として変換する。また、TTB はホームアドレスオプションを処理することができるので (2)、外部リ

リンク上のモバイルノードからの通信をホームリンクからの通信として処理する。

1 本実験で使う TTB はトランスレータと DNS サーバの機能を持っている。

2 Binding Cache は持っていないので、Routing header を利用した経路の最適化はできない。

TTB トランスレータ、TTB DNS サーバの説明

● TTB トランスレータ

TRT 方式のトランスレーション機能を持ち、宛先にダミープレフィックスを持った IPv6 パケットを IPv4 パケットに変換し、IPv6 ノードから IPv4 ノードへの通信を可能にしている。

● TTB DNS サーバ

DNS プロキシ機能を持ち、DNS クライアントからの AAAA レコードの問い合わせに対し、外部 DNS サーバへ問い合わせ、A レコードが返って来た場合、TTB トランスレータにアサインされたダミープレフィックスを IPv4 アドレスに付加して DNS クライアントに返す。また、問い合わせに行った DNS サーバから AAAA レコードが返って来た場合は、そのまま DNS クライアントに AAAA レコードを返すこともできる。

1.4.3 実験環境

本実験では TTB を SFC 側のキャンブネットワークの出口に配置し、また、TTB と同じセグメントに配置したログサーバで TTB のログ収集を行う。

1.4.4 結果

宿泊期間中、連続稼働運転を行った。その結果 TTB トランスレータの使用状況と転送データ量は表 1.1 となった。またプロトコル別の使用状況と転送データ量は TCP、UDP においてそれぞれ図 1.3、図 1.4 となった。TCP においてはプロトコルの特性から、リクエスト数は HTTP が一番多く、データ転送量は HTTP に次いで SSH、FTP が多い結果となっている。逆に UDP においては全く使われることがなかった。

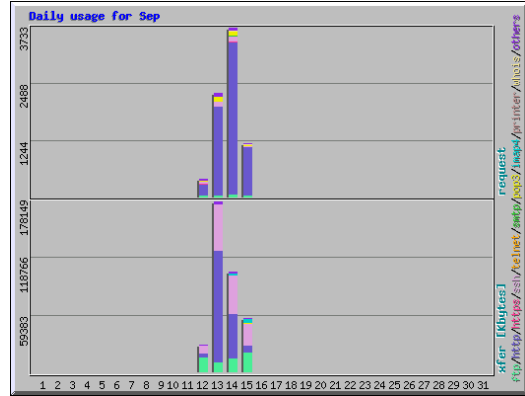


図 1.3. TCP におけるトランスレータ使用状況

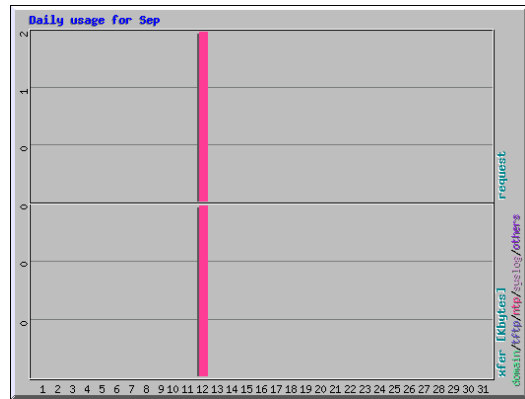


図 1.4. UDP におけるトランスレータ使用状況

表 1.1. トランスレータ使用状況

—	TCP	UDP
リクエスト数	7,527	2
データ転送量 (Kbytes)	364,662	0

表 1.2. TTB リクエストリスト

No.	Host	Request 数
1	2001:200:0:ff44:260:1dff:fe1:8e1e	1058
2	2001:200:0:ff44:260:1dff:fe6:1e64	921
3	2001:200:0:ff44:240:96ff:fe5a:758b	822
4	2001:200:0:ff51::277	735
5	2001:200:0:ff44:202:2dff:fe1b:31c	721
6	2001:200:0:ff44:202:2dff:fe0f:f845	663
7	2001:200:0:ff42:200:39ff:fe18:352b	581
8	2001:200:0:ff44:260:1dff:fe21:c959	446
9	2001:200:0:ff42:240:26ff:fe61:2b3b	416
10	2001:200:0:ff44:260:1dff:fe1c:5dc7	209

また、IPv6 クライアントのソースアドレスの統計は表 1.2 のようになった。使用率が 4 番目に多かつ

た「2001:200:0:ff51::/64」は「MobileIPv6 の評価」実験におけるホームリンクであり、MIP6 とともに十分に連携できた結果となった。

1.4.5 まとめ

今回の実験結果により、IPv6 UDP クライアントも十分に無いこともあり、UDP トランスレート機能は時期尚早であることが分かった。一方、コレスポンデントノードとしてのトランスレータは十分にMIP6 と連携できることが確認できた。

1.5 IPv6 上の SIP プロトコルによる VoIP 通信実験

実験者 富永 聡

所属 ヤマハ株式会社

1.5.1 実験の目的

ヤマハ(株)では、家庭・小規模企業用 ISDN ルータにおいてローカルな VoIP 機能である MGCP プロトコルによる機器間アナログ通話機能をサポートし、IPv6 上で動作するファームウェアをユーザーに対して配布中である。この拡張として、SIP プロトコルによる VoIP 通信を試験的に実装中であり、IPv6 上での動作をサポートする予定である。

今回の合宿では、レジストラを使用しないピア・ツー・ピアでの SIP による VoIP 網を IPv6 上で構築する。実験ネットワーク上で実際に利用することで、意見収集、動作の安定化をめざす。

1.5.2 実験の概要

合宿内の主要箇所(各 BoF 部屋、NOC 部屋、Terminal 部屋、Plenary 部屋)に VoIP アダプタとなる ISDN ルータ及び電話機を配置する。また、合宿会場外としてヤマハ社内にも端末を配置し、合宿ネットワーク外とも通話できる構成とする。この配置を含めたネットワーク図を図 1.5 に示す。

このように配置された VoIP 電話をトラブル時の BoF 部屋と NOC 部屋間の連絡等、合宿内線電話の代わりとして利用して頂く。

1.5.3 実験の環境

VoIP アダプタとなる ISDN ルータには、ヤマハの RT60w を使用した。RT60w は ISDN インターフェースと無線 LAN インターフェースを有してい

るが、今回の実験では利用していない。各 RT60w には固定 IPv6 アドレスが割り当てられており、各々に他の RT60w の IPv6 アドレスとそれに対応させる電話番号の組み合わせを登録する。この RT60w に繋がった電話機から、呼び出したい相手の IPv6 アドレスに対応させた電話番号をダイヤルすることで IPv6 上の SIP プロトコルにより呼び出し、受話器を取った相手と通話ができる。

なお、音声 Codec としては無圧縮 8 bit μ -law、8 kHz サンプリングの G.711 を使用しており、音声接続中は IP ヘッダを含めて約 80 kbit/s の帯域が必要となる。

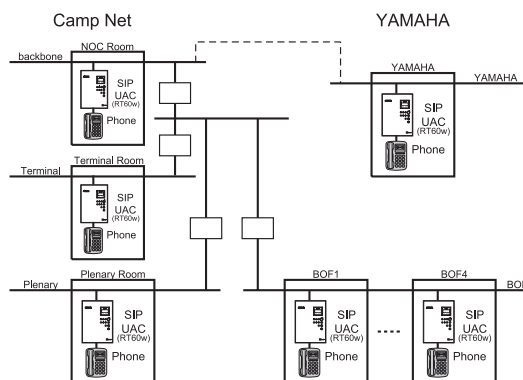


図 1.5. 各 VoIP 端末と合宿ネットワークの関係

1.5.4 結果とまとめ

合宿ネットワーク内では常に良好な音質による通話を確認できた。ヤマハ社内との通話では、音声無圧縮による帯域の問題により音声の途切れが発生し、トラフィックの多い時間帯においては会話が成り立たないという状況も発生した。

今回の実験の反省としては、

- 音声品質の指標であるパケットロス、ジッタ等のパラメータを自動的に収集する仕組みを欠いていたため、客観的な音質評価ができなかったこと
- 電話が個対個が主となる音声コミュニケーションであるため、実験としてアピールするものが少なかったこと

が挙げられる。

SIP は MGCP のようなサーバ/クライアント型のプロトコルと異なり、ピア・ツー・ピアでの接続が可能である。そのため、特定のサーバが立ち上がっていないと通話できない、という状況が発生しない反

面、端末の管理や情報収集が難しいという問題があり、実験でどのように情報を収集するかという手法について検討が必要である。

今回の合宿での成果を元に、ヤマハの ISDN ルータ上で SIP プロトコル (IPv6/IPv4 デュアルスタック) による VoIP 電話を実現する β 版ファームウェアを以下の URL において公開している。

<http://www.rtrpro.yamaha.co.jp>

1.6 MobileIPv6 の評価

実験者 狩野 秀一

所属 NEC ネットワークス

1.6.1 実験の目的

MobileIPv6 を実環境に近い状況で使用し、課題や最適設定を探る。

1.6.2 実験の概要

合宿ネットワークに MobileIP の HA を接続し、別途用意する小型ルータによって分離されたネットワークセグメント間を NotePC を持ち歩いて移動し、MobileIP によってこの移動を追尾する。このとき、RA の設定、HA の負荷状況などに応じて、通信がどのような振る舞いをするか測定・評価する。

1.6.3 実験内容と結果

ホームエージェント (HA) および通信ノード (CN) として、FreeBSD 4.3 release に 2001/5/7 版 KAME と 2001/9/11 版 necmip6 をインストールしたものをを用いた。

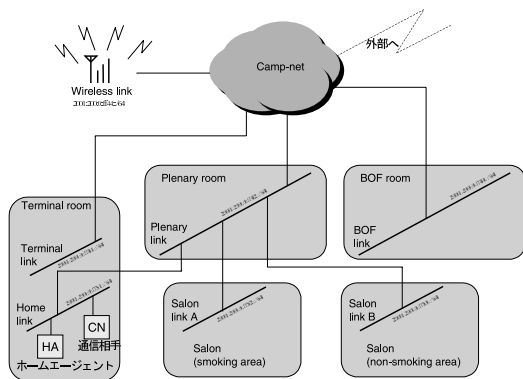


図 1.6. MobileIPv6 ネットワーク構成図

まず、予め準備した装置が正常に動作することが確認できた。また、我々の用意したネットワーク

のみでなく、研究会会場の他の様々なネットワークに接続した移動ノード (MN) を、他のリンクに移動させることが問題なく行えることを確認できた。研究会用に作成した IPsec ポリシー管理スクリプト等も問題なく動作した。

当初の実験の目的は、研究会参加者が各自持ち込んだ PC に MN になってもらい、necmip6 のスケーラビリティを検証することだったが、実際には MN となって参加してくれる人がほとんどいなかったため、この目的は達成できなかった。それでも、普段開発者でもなかなか利用できない実環境での Mobile IPv6 が利用できたという点で、スケーラビリティとは異なる視点でのいくつかの検証/検討を行うことができ、得るもの多かった。

1. 異種メディア間での移動

実験のために利用した NEC Mobile IPv6 実装は、当初より無線 ↔ 有線での移動は想定していたために、ある程度の機能は実装しており、おおむね安定していた。しかし、比較の実環境に近い研究会ネットワークで利用したところ、移動検知の機能が不十分であることが判明し、それを修正することができた。

また、利用するメディアの選択や、リンクの選択 (ホームリンクと外部リンクの両方に接続されているときどちらを選択するか) を何らかのポリシーでユーザーが明示的に指定できるとよりよいだろう、ということが分かった。

さらに、リンク層の種類ごとに別々に存在する移動検知の情報を、汎用性を持ってネットワーク層に通知するインターフェースが必要であることも分かった。

2. Windows2000 での動作検証

かねてより Windows2000 用の Mobile IPv6 実装がある (<http://www.landmarc.net/>) ことは知っていたが、実際にこれを動かしたことがなかった。この実験の場で試用し、NEC Mobile IPv6 実装とのある程度のインターオペラビリティを確認することができた。もっとも、Windows2000 の DNS resolver が IPv6 対応になっていないために常用することはできなかった。

3. TTB との接続確認

TTB は横河電機のソフトウェア製品であるが、実験で持ち込んでいたものは新機能を搭載し

Home Address オプションを解釈できるようになっている (Binding Update オプションは解釈できない)。これを經由して、MN から IPv4 (インターネット) への接続が問題なく動作することが確認できた。

同時に、Home Address オプションは解釈できて Binding Update オプションを解釈できないノードとの通信も確認できた。

4. CN 宛での Binding Update

MN が、HA からトンネルされて来るパケットすべてについて、送信元の CN に Binding Update を返すことについて議論をした (たとえば、通信相手にない経路上のルータからの ICMP6 エラーなど、ICMP6 エラーに対しては Binding Update の送信が不要な場合が多い)。

1.6.4 まとめ

この合宿では、運用ネットワークを用い、我々が開発している Mobile IPv6 実装の実験を行った。当初目的としていたスケーラビリティの検証はできなかったが、実環境で利用することにより、さまざまな検証、問題点の発見、検討を行うことができ、得るものが多かった。

1.7 Honeypot を用いた Deception Network の研究

実験者 宮本 大輔

所属 奈良先端科学技術大学院大学

1.7.1 実験の目的

Deception Network は、クラッカーの個々の不正アクセスを無力化する環境である。本実験ではこの環境を Honeypot を用いることによって実現する。しかし、Honeypot はその効果が不明な点、運用が難しい点が問題である。

本実験では Honeypot の有効性の検証や運用に必要な知識を蓄積することを目的とする。

1.7.2 実験の概要

本実験では、ネットワーク型 Honeypot とホスト型 Honeypot を配置し、クラッカーからの攻撃を監視する。

- ネットワーク型 Honeypot

ネットワーク型 Honeypot は、クラッカーのス

キャン行為に対し、偽の情報を返す環境である。通常、クラッカーはスキャンによってホストの脆弱性を調査し、そのホストを攻略するための戦略を策定する。しかし、ネットワーク型 Honeypot が設置されていた場合、クラッカーはスキャン結果が正しい情報であるか、あるいは偽りの情報であるかを判別できなくなると考えられる。これによって、そのホストを攻略する為に必要なとなる時間が飛躍的に増大し、セキュリティが高まることを期待できる。

- ホスト型 Honeypot

ホスト型 Honeypot は未知のクラック手法を、より簡単に解明するための環境である。ホスト型 Honeypot を踏み台として利用したクラッカーの攻撃手法 (攻撃プログラムやその利用法等) を取得することより、未知の攻撃手法の発見やその対策に役立てることができる。図 1.7 に、ホスト型 Honeypot がクラッカーの監視を行う箇所を白抜き文字で示す。実験で用いたホストは、ファイルに対するシステムコールの発行、仮想ターミナルデバイスへのデータ入出力を監視し、クラッカーの行動を記録する。

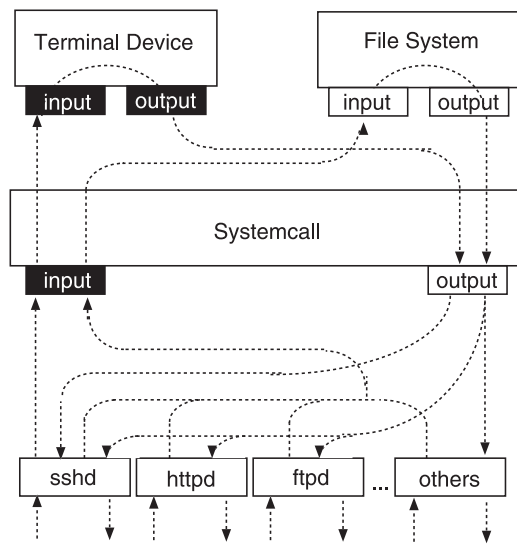


図 1.7. ホスト型 Honeypot が監視を行う箇所

1.7.3 実験環境の構築

ネットワーク型 Honeypot は、様々な脆弱性が指摘されている Microsoft Windows 98 上で Internet Information Server 4.0 が HTTP サービスを行っているように偽装する。クラッカーがネットワーク

型 Honeypot に対しスキャンを行うと、Application Banner や OS Fingerprint が偽造され、あたかも Windows98 上に IIS4.0 が動作しているかのように見える。また、攻撃の監視は IDS として広く使われている Snort により行った。

ホスト型 Honeypot は、既知のセキュリティホールを全て修正した Linux を用いる。このため、本ホストがクラッカーに侵入された場合、侵入者は未知の手法によるクラック行為を行ったと仮定できる。これにより分析しなければならないデータ量を削減できるようになり、より効率よく新たなセキュリティホールを見つけだし、その対策を行うことが可能となる。

1.7.4 結果と考察

合宿期間中に実験を行ったが、ネットワーク型 Honeypot に対するスキャン行為、ホスト型 Honeypot に対するクラック行為は極めて少く、Honeypot の有効性を検証するには至らなかった。

この原因として、クラッカーに不正アクセスを行わせるだけの魅力を Honeypot が持たなかったことや、運用が短期間であったことが挙げられる。この問題の解決には、クラッカーの動機や目的を工学的に分析する技術や、不正アクセスを誘致する技術が必要であると考えられる。

1.8 BoF & WineTime by XCAST

実験者 今井 祐二

所属 株式会社富士通研究所

1.8.1 実験の目的

合宿の BoF の XCAST による遠隔プレゼンテーションと、WineTime での無線ラップトップ同士の映像交換を行い、XCAST 多地点コミュニケーションの有用性を実証する。

1.8.2 実験の概要

以下の 2 つのシチュエーションで XCAST による多地点ストリーム配信実験を行った。

- XCAST BoF において Korea Telcom Freetel、奈良先端大、合宿会場の 3 地点を相互にストリーム配信し、合宿地の外からそれぞれの研究内容の遠隔プレゼンテーションを行った。
- WineTime 会場内で、無線 LAN で接続された

複数のラップトップ間で相互にストリーム配信を行い、インフォーマルな場での使用可能性を検証した。

1.8.3 実験内容と結果

遠隔プレゼンテーション

会場、奈良先端科学技術大学院大学 (以下奈良先端大)、Korea Telecom Freetel に MDO6 多地点ビデオ会議システムをインストールした FreeBSD 4.2 セットを用意した。会場内では画像を CCD カメラで、音声を発表者の持つマイクロフォンより採取した。会場外からの音声は PC 用スピーカを用いて会場内に流した。

プレゼンテーション資料のネットワークでの中継は行わなかった。あらかじめ発表者が Web ページに掲載し URL を交換しあった。会場では援助者が代理でプロジェクトに投影した。また、会議のコーディネーションはグループ管理機構を使わず、3 地点の IPv6 アドレス、資料の URL 等を事前およびその場でメールを用いて交換してた。

Korea Telecom Freetel とは事前リハーサルなどが充分できず、当日にアドレスの指定などを試行錯誤し、ようやく画像の交換には成功した。しかし、音声の交換にトラブルが発生した。ミーティングの進行と並行して行われていたこともあり、先方の端末のオーディオカード等のトラブルなのか、6Bone や合宿ネットのトラブルかの調査が充分できないまま、プレゼンテーションをキャンセルする結果となった。

一方、奈良先端大は、発表者が定期的に MDO6 ミーティングに参加しシステムも常に使用されている状態であったため、上記の準備で良好な通信環境を得ることができた。プレゼンテーションは予定どおり行い、合宿地との間でディスカッションを行うことができた。

WineTime での無線 LAN による運用

ブレナリルールの 3 台の無線ラップトップ、1 台の有線ラップトップを用いて WineTime のブレナリルームを巡回した。

無線 LAN は同一セグメントであるため 4 台の間は Ethernet Frame としては、すべて Unicast でパケットが飛び交う形になり、無線トラフィックの圧迫が心配された。アプリケーションのパ

ケット損失率表示を目視確認しながら使用した。使用帯域上限値を vic 128 Kbps、rat 13.2 Kbps をそれぞれのデフォルトで運用したが、特に重大なパケット損失、画質/音質の劣化は見られなかった。

無線 LAN による移動性を活用して、プレナリルームの各所のグループの間を巡回したり、動きを加えた映像を撮影するなどし、それを離れた地点から実時間で視聴することができた。使い方として非常に面白いものになった。半面、音声によるコミュニケーションはほとんど取れず、期待していたグループ間での対話などは行われなかった。

1.8.4 まとめ

今回の実験で得られた知見を以下にまとめる。

- 遠隔プレゼンテーションは事前の準備が充分で無かったため韓国からの参加に失敗した。XCAST ビデオ会議システムとしての成熟度が充分でなく、オーディオデバイスの問題なのか、ネットワークの問題なのかの切り分けできないことも混乱に拍車をかけた。
- グループ管理機構の欠如でアドレスの交換作業に手間がかかり、これも会議の参加が遅れる要因になった。
- 無線 LAN による可搬カメラ型の中継は娯楽性が高く、応用として非常に興味深い。今後、研究課題として取り組む価値がある。

1.9 分散プロープによるセキュリティおよびトラフィック監視実験

実験者 土井 一夫

所属 株式会社サイバー・ソリューションズ

1.9.1 実験の目的

大規模であれ小規模であれ、ネットワークというものを計画し構築し運用する上において、それを適切に監視し管理を行うことが必要である。だが、その規模が大きくなればなるほど、管理のためのコストはマシン・ネットワークへの負荷、管理者の負担という形で著しく増大する。

また、ネットワーク環境の非対称性によって、ある一箇所だけからすべての監視が行えないこともあり得る。たとえば NAT/NAPT ルータによるアドレス・ポート変換を利用するネットワークセグメント

は、外から直接監視することが非常に困難である。

これらの問題を最終的に解決するために、我々はネットワーク上各所に情報収集プロープを分散配置する方式を提案した。この方式のメリットは、個々のプロープへの負担を軽減しつつよりネットワークそのものに密着した、きめ細かな情報収集が行えるということである。たとえば全てのパケットを監視しインシデント検知を行うといった類のことが可能になるということである。また、ネットワーク障害時にデータ取得が行えなくなる危険性も少なくなるはずである。

また、分散方式をとった場合に新たに問題となる情報の統合提供の面にも配慮し、最終的には一箇所のマネージャにその集約公開の機能を持たせることにした。またその際のプロープからマネージャへの通知のためにインシデント情報の SNMP 通信モジュールを開発し用いた。

1.9.2 実験の概要

ブロードキャストセグメント単位でプロープを配置し、近隣のネットワーク・インシデント情報を収集させた。収集した情報は SNMP トラップとして別に用意されたマネージャに通知し、マネージャ上では複数のプロープからの情報の統合と公開を行った。

プロープ上ではインシデント情報と併せ、通常のトラフィック情報収集やネットワークポロジの観測を行った。その結果もマネージャ上で公開した。

マネージャで公開された情報は合宿地のどこからでも Web を使いアクセスできるようにした。

1.9.3 実験の環境

各マシンの配置は図 1.8 の通り。

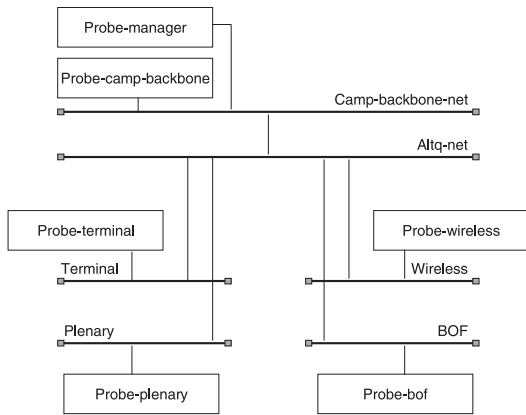


図 1.8. マシン配置図

各プローブはそれぞれ一つブロードキャストセグメントを監視し、ネットワーク・インシデント情報を収集した。セグメントの監視にはインテリジェントスイッチのミラーポート、リピータハブを使用した。

各プローブからマネージャへのインシデント情報通知は SNMP トラップ通信、トラフィック情報はマネージャ・プローブ間での SNMP リクエスト通信により行われた。

データの公開には Web と Java を用いた。

1.9.4 結果と考察

各プローブのインシデント情報収集、マネージャへの通知、マネージャでの可視化提供に成功した。プローブの存在するセグメントを通過した攻撃がネットワーク地図上に可視化されている。(図 1.9)

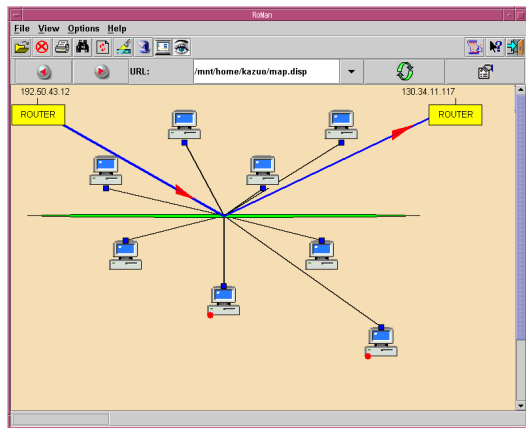


図 1.9. インシデント情報可視化

また、複数のプローブ上で収集されたトポロジ情報を統合した地図の公開にも成功した。(図 1.10)

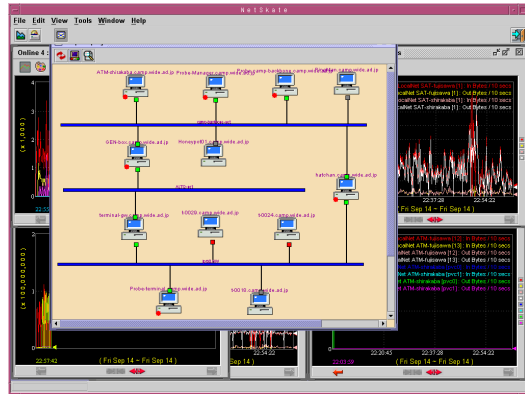


図 1.10. 複数のトポロジ情報の統合

そのネットワーク地図・情報をベースにし、ネットワーク内要所のトラフィック情報の収集・可視化も問題なく行えた。(図 1.11)

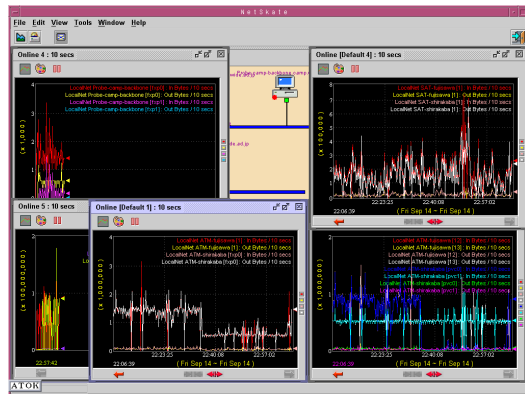


図 1.11. 地図ベーストラフィック情報可視化

今後の課題としては

- (1) 収集するインシデント情報の高度化
 - (2) インシデント情報公開マネージャの高度化
 - (3) IPv6 情報の収集対応
 - (4) SNMP 通信の IPv6 対応
- が挙げられる。

1.10 Passive and Active Measurement of WWW Server

実験者 中村 豊、西村 敦隆

所属 奈良先端科学技術大学院大学

1.10.1 実験の目的

パケットモニタリングを用いた WWW サーバの観測および、ネットワーク遅延を考慮したベンチマークシステムの検証実験。

1.10.2 実験の概要

甲子園で用いているツール (ENMA) の紹介を行い、さらに現在開発中のベンチマークシステムの検証実験を行う。ベンチマークシステムは従来の問題点の一つであるネットワーク遅延を考慮したものである。具体的には dummynet を用いてサーバ・クライアントの各々の対毎に異なる遅延時間を挿入することでより現実に近いベンチマークシステムとなる。このベンチマークの出力を ENMA を用いてリアルタイムに出力する。

1.10.3 実験ネットワークの構成図

今回の宿舎における実験ネットワークを図 1.12 に示す。dummynet を用いて、コネクション毎の遅延を設定し、ENMA を用いて観測する構成となっている。

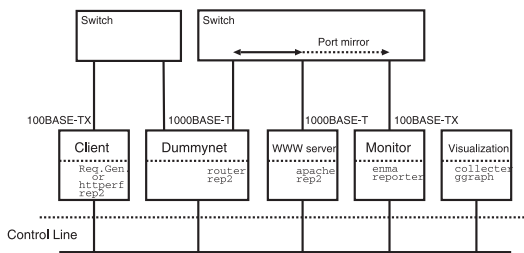


図 1.12. 実験ネットワーク構成図

1.10.4 2000 年夏の甲子園の結果

参考として、2000 年の夏の甲子園における ENMA の結果を示す。

図 1.13 の左はコネクションを処理した割合で、右は同時に処理しているコネクション数である。同時コネクション数はサーバに留まっているコネクションのキューであると考えられることができる。

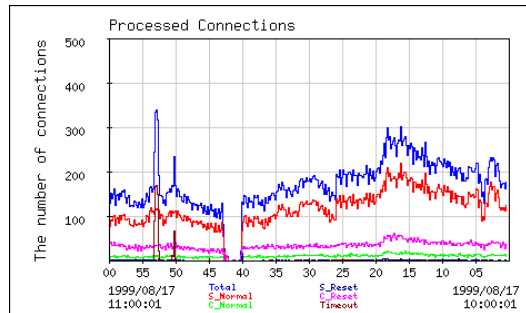
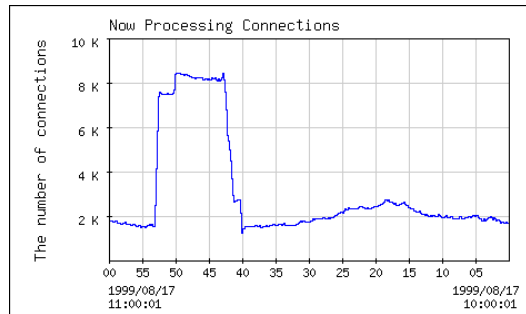


図 1.13. サーバシステム再起動時

図 1.14 に飽和時のグラフを示す。飽和時には、完全に処理が停止するわけではなく、ごく一部のコネクションのみが処理されることがわかる。右図で同時コネクションが 10 分程度で減少しているのは、ENMA のタイムアウトの設定が 10 分であるためである。

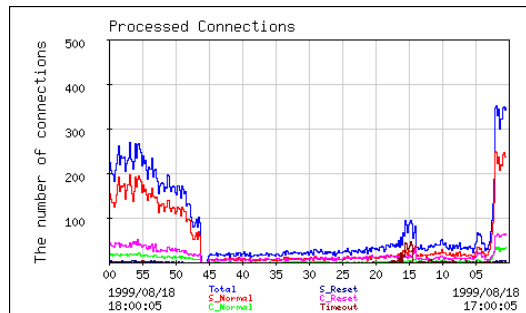
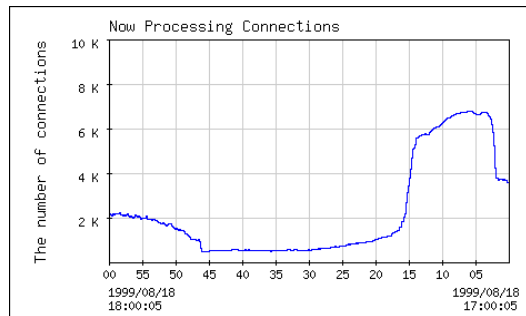


図 1.14. サーバシステム飽和時

第 2 章 2002 年春合宿ネットワーク

この章では、2002 年 3 月に行われた WIDE プロジェクト春合宿におけるネットワーク構成およびそのネットワーク上で行われた実験結果を報告する。

2.1 ネットワーク構成

この節では、2002 年春合宿のネットワークの全体構成を説明する。

図 2.1 は、2002 年春合宿のネットワークトポロジを示している。この図において、点線より上側は WIDE 藤沢 NOC (Fujisawa) に置かれた機器、下側は合宿地 (Hamanako) に設置された機器を示している。WIDE 藤沢 NOC と合宿地は、ATM 回線 (1.5 Mbps) および 衛星回線 (合宿地からは 0.5 Mbps、合宿地へは 1.5 Mbps) で接続した。図中の DialUpRouter、router-camp につながる点線は、通常時は利用しない非常用の回線として用意した。合宿中、これらの回線を利用するような障害は発生しなかった。

ルータは衛星回線を接続するルータを除き、「MPLS/L3TE/Diffserv/ネットワーク制御」実験による MPLS ルータを用いた。経路制御は IPv4/IPv6 共に OSPF プロトコルを使用した。

ユーザへは、有線 (100Base-TX/10Base-T)、無線 (IEEE802.11b) による IPv4/IPv6 接続を提供し、IPv4 アドレス割り当ては DHCP を使用した。ユーザセグメントは、「iCARs」実験の要請により、有線は部屋ごと、無線は基地局ごとに異なる 13 セグメントで構成した。DNS、WWW 等のサービスは、ルータの障害時にも利用可能にするために、全ユーザセグメントにインターフェースをもつ「hatchan」で提供した。

2.2 合宿ネットワークを利用した実験項目

2002 年春合宿では、以下の実験が行われた。

- MPLS-TE/Diffserv/ネットワーク制御
- iCARs
- 小型 GR で遊んでみよう
- SOI-ASIA プロジェクト授業配信
- IETF ネットプレ実験

- XCAST 会議状況把握システム
- 遠隔ネットワーク監視とネットワーク分散管理実験
- IPv6 マルチキャスト接続実験

2.3 MPLS-TE/Diffserv/ネットワーク制御

- 実験者 小川晃通
 所属 慶應義塾大学
 実験者 森島直人、垣内正年
 所属 奈良先端科学技術大学院大学
 実験者 宇夫陽次朗、宇多仁、小柏伸夫、宮地利幸、清原智和
 所属 北陸先端科学技術大学院大学

2.3.1 実験の背景と目的

インターネットの安定と拡大とともに、広域ネットワークが提供するサービスにさまざまな付加価値が求められるようになった。特に、リアルタイム性を持つネットワークアプリケーションや帯域制御を必要とするサービスが登場するにつれ、End-to-End での通信特性を制御する必要性がでてきた。しかし、インターネットは分散した構成要素が独立して緩やかな協調分散をおこなう系として設計・運用されてきたため、現用のモデルでは包括的制御の実現は困難である。これに対し、転送層と制御層の分離モデルが提案されている。転送層は、パケット転送を実際に行うノードの集合から構成され、Diffserv(Differentiated Services) [19] や MPLS(MultiProtocol Label Switching) [128] がある。また、制御層は転送層に属するノードの集合を、管理ドメイン内でのポリシーに応じて包括的に制御するものである。

WIDE プロジェクトでは、上記のような背景のもと、『あやめプロジェクト』 [11] および『くまプロジェクト』 [102] がネットワーク制御に関する研究を行っている。

あやめプロジェクトは、第 3 層以下の技術に着目したネットワーク制御に関する議論を背景に、MPLS の研究と開発を行っている。また、研究開発用 MPLS 環境として、MPLS ルータ (LSR) および MPLS シグナリング機構である LDP(Label Distribution Protocol) [5]/ CR-LDP(Constraint Routing LDP) の設計および実装を行っている。くまプロジェクトは、多様なポリシーを多様な方法で実現するためのアーキテクチャ、コンポーネント間のインタフェース、さ

**WIDE Project CAMP Spring 2002
Topology Map**

update:2002.2.26

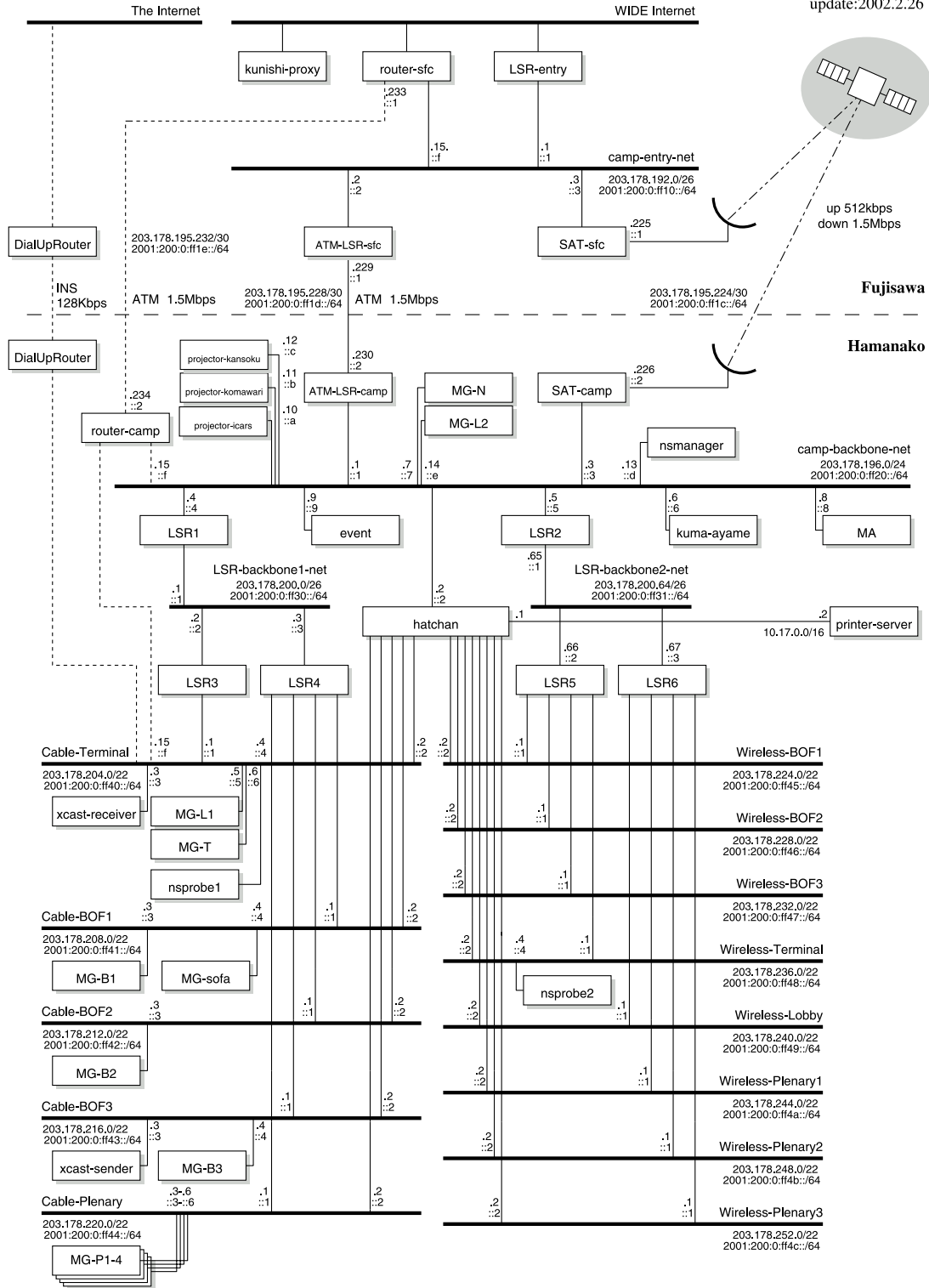


図 2.1. 2002 年春合宿ネットワークトポロジ

さまざまなポリシを調停する多目的フィルタなど、広域ネットワーク制御を実現するためのフレームワークの研究を行っている。

今回の合宿において、2 プロジェクトの共同プロジェクトである『くまあやめプロジェクト』は、合宿参加者からの動的な要求に対するネットワーク制御の実証実験を行った。このような粒度の細かな包括的制御は現用モデルでは扱いづらく、さまざまなモデルに対する考察と、技術的な検討が必要である。この実験では、合宿参加者へのサービスの提供とともに、上記のような考察や検討も目的としている。

2.3.2 実験の概要

本システムは、さまざまな技術が相互に関連して動作している。以下に利用している技術とその説明を示す。

制御層

制御層のシステムは、くまプロジェクトが設計・実装している KUMA である。KUMA のシステム構成概要を図 2.2 に示す。本システムは、制御パラメータトランスポート、細分化意思決定機構、細分化意思統合機構から構成されている。

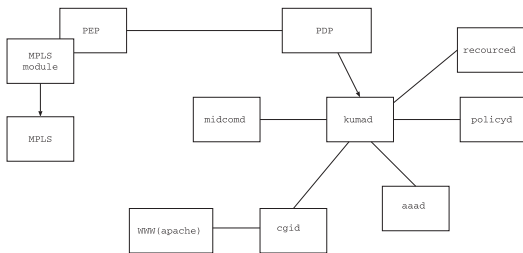


図 2.2. KUMA システム構成概要

- 制御パラメータトランスポート

制御パラメータトランスポートは、なんらかのシステムによって決定された制御パラメータを配布するための機構である。KUMA では、制御パラメータトランスポートのプロトコルとして、COPS(Common Open Policy Service)[21]を採用した。図 2.3 に本機構における COPS 設計を示す。

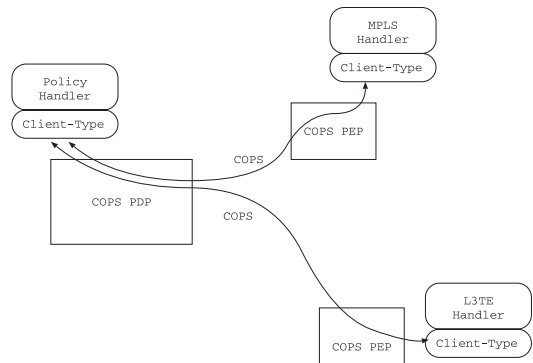


図 2.3. COPS による制御パラメータトランスポート

COPS は、意思決定や機器に固有のパラメータには関与しない。そのため、転送機構に依存しない汎用制御パラメータトランスポートとして利用することができる。

PDP(Policy Decision Point) は複数の PEP(Policy Enforcement Point) とのコネクションを維持する。ポリシ制御情報を送信する際には、必要な PEP を選択して送信する。

PEP は、転送機構に対応するモジュールを組み込み、それによって制御パラメータを変換・適用する。今回は、合宿用に AYAME MPLS に対応したモジュールを実装した。

- 細分化意思決定機構・統合機構

サービスは、その提供者によってさまざまなポリシが適用される。その組み合わせは無限であり、ひとつの意識決定機構によってそのすべてをサポートすることは不可能である。そのため、数多くのポリシを柔軟に組み合わせ、思い通りのサービスを提供するためのフレームワークが必要になる。また、サービス提供者独自の条件を追加する場合にも、出来るだけ少ないコストで実現できるような仕組みが必要である。

これを実現するため、KUMA ではポリシを細分化し、それぞれのポリシの適用とその結果導出される意思の統合を分離した。

前者は細分化意思決定機構として、ポリシごとに独立したデーモンとなる。また、課金管理システムのように、ほかのサービスとの共用も考慮されている。合宿でのサービスに対応するため、今回は以下のデーモンを実装・利用した。

CGId 合宿参加者からの要求発行インタフェースである CGI の接続管理

AAAAd 認証・課金管理

RESOURCEd 帯域などの資源管理

POLICYd その他一般的なポリシー判断

MIDCOMd NAT などの End-to-End 情報変換対応

後者は細分化意思統合機構として、それぞれの細分化意思決定機構によって導出された意思を統合し、系全体としての意思決定を行う。この機構は、KUMAd という単一のデーモンによって実装されている。

転送層

- MPLS/CR-LDP

合宿ネットワークからインターネットまで LSP(Label Switching Path) を確立し、要求に応じた通信品質を保証する。今回の実験においては、通信品質(経路指定、帯域指定)を満たした LSP の確立のためにトラフィックエンジニアリング技術が必要となるため、MPLS のシグナリングには CR-LDP を用いた。

また、今回は、Campnet 内のほとんどのルータを AYAME LSR で構築し、ユーザセグメント収容ルータからインターネットとの結節点(WNOC-SFC)までの MPLS ドメインを構築した。昨年度の WIDE 合宿においても MPLS を用いたネットワークを構築したが、その際には、各所に MPLS over IPv4 の技術を用いていた。

さらに、MPLS 網制御は IPv4 を用いて行いつつも、IPv6 トラフィックを LSP を用いて流すことに対応したことも今回の大きな特徴である。

- Diffserv

MPLS ドメイン内での通信品質(帯域)の保証のために、MPLS/Diffserv の技術を用いた。今回の実験トポロジにおいては、帯域におけるボトルネックが合宿地～慶應義塾大学間の回線(対外線と呼ぶ)のみであった。このため、エッジノードにおいて LSP 毎のポリシングとマーキングを、対外線収容ルータにおいてマークにもとづいた優先処理を行った。

今回の実験では、MPLS 網に対し Diffserv を行った。MPLS パケットに対するマーキングには、E-LSP の手法を用い、SHIM ヘッダ内の exp.

field に対しマーキングを行った。その上で、対外線収容ルータの優先処理ではプライオリティ・キューイングを用い、exp. field のマークに応じた優先処理を行った。

- 一般化パラメータフィルタ

通信品質を制御するとき、対象となる通信を識別し、その通信に対して適用する処理を決定しなければならない。通信の実体は、当事者間である意味を持った一連のデータの流れである。通信を制御するには、この一連のデータの流れ、フローを識別し、それに対応する操作の集合を決定することが必要となる。しかし、識別に利用するデータの適用順序や優先順位によって、結果が変わったり競合したりすることもある。くまプロジェクトでは、この問題を解決するため、競合条件を発生しうる場合を抽出し、その調停を容易にするためのパラメータフィルタ KUPF の設計と実装を行っている。今回の合宿では、優先処理を適用するフローの抽出に KUPF を利用した。

合宿参加者は、Web サーバ経由で要求を発行する。発行には、(src, dst)などのパラメータを Web ページのフォームに投入する。

投入された予約には、細分化意思決定機構により課金や資源などの状況やポリシーにしたがって意思決定される。複数の意思決定機構による意思は細分化意思統合機構によって統合され、系としての意思が導出される。要求が受理された場合、各構成ルータの制御パラメータを決定し、制御パラメータトランスポートによって対象となるルータまで送信される。制御パラメータを受信したルータでは、内容にしたがって機器の設定を行う。具体的には、CR-LDP をもちいて LSP を確立する。対象となるトラフィックは、一般化パラメータフィルタにより識別され、Diffserv を利用して優先制御される。

2.3.3 結果

今回の実験においては、安定的ネットワークの提供という今回の Campnet のポリシーに基づき、実験直前に発見された実装上の問題の解決などのために提供サービスを数段階に分け順に投入した。各サービスは、

- 初日: IPv4 トラフィックに限定した予約サービス
- 2 日目: IPv6 トラフィックの予約サービスを

開始

● 3 日目: LIN6 サポートを含む全サービスを開始の順に投入され、3 日目以降は、全サービスが問題なく稼働した。

合宿期間中、いくつかの軽微な障害は発生したものの、サービス全体としては大きな障害もなく概ね順調に動作し、問題なくサービス提供を行うことができた。

2.3.4 まとめ

本実験を通して、ユーザからの動的な要求に対するネットワーク制御に関して、さまざまな知見が得られた。これらは論文としてまとめられる予定である。

2.4 小型 GR で遊んでみよう

実験者 新 善文、鈴木 伸介、矢野 大機、鈴木 知見
所属 日立製作所

2.4.1 実験の目的

日立製作所は、ギガビットルータ GR2000 の外観・機能・コマンドラインインタフェース (CLI) を改良した GR2000 小型モデルを 2002 年 4 月に製品出荷する予定である。

本実験の目的は、WIDE Project の研究者に本装置を実際に触ってもらうことを通じて本装置の改良点を評価して頂き、その評価結果を製品開発へフィードバックすることである。

2.4.2 実験の概要

ネットワークから切り離れた GR2000 小型モデルを 1 台置き、WIDE Project 研究者に自由に触ってもらった。その過程で次の 2 点を評価した。

- 外観/機能
- CLI の使いやすさ

2.4.3 実験結果

- 外観/機能
外観面では、「従来モデルに比べ小さくなりがなばった」「ファンが静かでよい」という肯定的な意見を多く頂いた。一方で「エアフィルタを付けて欲しい」「ドライバ無しで装置を分解できるようにして欲しい」などといった改善要求を頂くことが出来た。

機能面では、「1U サイズで IPv4、IPv6 いずれも

ワイヤレス中継できるとは素晴らしい」という肯定的な評価を頂いた。「MPLS も動く面白い」「ファイアウォールとして動く面白い」などといった機能仕様面からの提案を頂くことができた。

● CLI の使いやすさ

運用系コマンドに関しては全般に Cisco-like で使いやすいとの評価を頂いた。しかしながら一部の Cisco コマンドが実装されていないために、直感的に打ちこんだコマンドが不在なために利用者の期待する結果を表示することができない場合があった。

構成定義系コマンドに関しては「Cisco-like ではないので違和感を感じる」「複雑な ISP オペレーションに堪えない」という否定的な評価を多く頂いた。

2.4.4 考察・結論

外観/機能に関しては、全般に良好な反応を頂くことが出来た。今回頂いた様々な改善提案は実際の製品開発に持っていくべく検討を進めている最中である。

運用系コマンドに関しては Cisco コマンド実装洩れによる使い勝手の悪さを指摘された。この点に関しては実装洩れを無くすことにより使い勝手を改善できる見通しである。

構成定義系コマンドに関してはまだまだ多くの改善が必要であることがわかった。Cisco-like にしていくことや運用現場のオペレーションからのフィードバックを通じて今後も使い勝手を改善して行く予定である。

以上の対策を通じて、今回頂いた意見を製品開発にフィードバックさせ、GR2000 小型モデルをさらに使いやすく高機能なルータへ進化させる。

2.5 SOI-ASIA プロジェクト授業配信

実験者 村井 純、大川 恵子、三川 莊子、
三島 和宏、白畑 真、工藤 紀篤

所属 慶應義塾大学

実験者 篠田 陽一

所属 北陸先端科学技術大学院大学

2.5.1 実験の概要

SOI-ASIA プロジェクトでは、2002 年 3 月 6 日にその授業配信の一環として、WIDE 合宿の会場から

表 2.1. グループ 2 のパートナー大学

大学	地域	国
ブラビジャヤ大学 サムラトランギ大学 ハサヌディン大学 Asian Institute of Technology	ジャワ島東部マラン スラウェシ島メナド スラウェシ島マカッサル 首都バンコク	インドネシア共和国 タイ王国

表 2.2. WIDE 合宿で行われた授業トピック

講師	タイトル
村井純 教授	SOI ASIA Project Key Note
篠田陽一 教授	MPLS : A Packet forwarding technology for next generation Internet



図 2.4. 授業の様子

アジアに向けて授業の配信を行った。これは、表 2.1 に示すインドネシア国内の 3 大学及びタイの 1 大学に向けた 5 つのシリーズ授業の一部であり、WIDE プロジェクト代表である慶應義塾大学の村井純教授と WIDE メンバーである北陸先端科学技術大学院大学の篠田陽一教授が講師となって授業を行った。トピックは、表 2.2 の通りである。

授業配信は、日本側からは WMT(Windows Media Technology) を利用し、500 kbps の WMT ストリームがアジア各地に配信された。また各サイトからの質問は、IRC・Polycom/NetMeeting によるのビデオカンファレンスシステム・E-mail を通して配信され、リアルタイムのコミュニケーションが行われた。授業の様子を図 2.4 に示す。

2.5.2 ネットワークの設定

図 2.5 に当日のネットワークポロジを示す。

WMT ストリームの映像・音声の品質を落とすことなくアジアに届けるため、SOI-ASIA プロジェクトでは WIDE 合宿ネットワークとは独立して、1.5 Mbps

の専用線を利用した。

合宿地でリアルタイムにエンコードされた WMT のストリームは、この専用線を通して WIDE バックボーンに抜け、SFC の WMT サーバへ Unicast 通信で送信される。受信した WMT サーバはそれをマルチキャストでアジアに配信する。また、Polycom/NetMeeting などのビデオ会議システムを利用

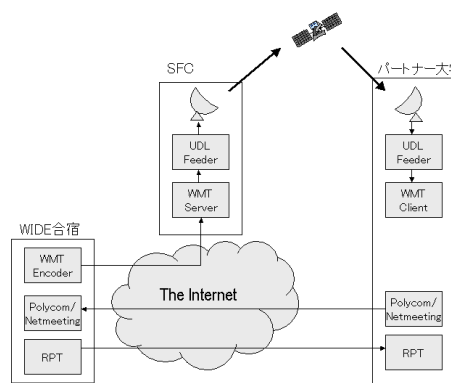


図 2.5. WIDE 合宿における SOI-ASIA ネットワークポロジ

してアジアの各パートナーと質疑応答のコミュニケーションを取り、RPT ソフトウェアを利用して授業マテリアルと送信するビデオとの同期を取った。

2.5.3 問題点

インドネシア 3 大学、タイの AIT に対しての初めての授業であった点、また WIDE 合宿というイベント会場での授業であったため、いくつかの問題点があった。

- AIT の学内 LAN スイッチにマルチキャストパケットが通らず、C-Band を利用してマルチキャストで授業を受けられなかったため、Ku-Band のネットワークを利用して、直接合宿地のエンコーダから Unicast でストリームを受信することで、授業を受講した。Ku-Band は SOI-ASIA プロジェクト以外のトラフィックが流れるため、十分な帯域が確保できず、映像・音声は鮮明ではなかった。
- ハサヌディン大学はスタッフにコンピュータ関係の知識者がいないため、準備が間に合わず授業を受けることができなかった。
- プラビジャヤ大学は、地上線を使った合宿地へのネットワーク帯域が充分でなかったため、音声・映像による質疑応答ができなかった。

なお、これらの問題は後日解決された。AIT ではスイッチのソフトウェアをアップデートすることで問題を解決し、ハサヌディン大学では、故障機器の交換および、現地への技術者の派遣によりこの問題を解決した。

2.5.4 今後の課題

すでに機器が設置してある教室を使った授業ではなく、WIDE 合宿のようなイベント会場からでも SOI の経験の蓄積を生かして、必要な機器リストの作成・機器の準備・ネットワーク帯域の確保・IP アドレスの割り当て・機器の配置決定を行うことで、授業の配信が可能であると分かった。

以上のことより、今後はマニュアルを整備し、各パートナーのオペレーションスタッフへ技術移転を行い、安定した授業配信を目指す。

2.6 IETF ネットプレ実験

実験者： 中村 修、石原 知洋

所属： 慶應義塾大学

実験者： 森島 直人

所属： 奈良先端科学技術大学院大学

実験者： 清原 智和

所属： 北陸先端科学技術大学院大学

2.6.1 実験内容

横浜 IETF に向けた無線と L2 機材のチェック

2.6.2 実験の目的

横浜 IETF で使用する無線 LAN 機器およびスイッチなどの機材の評価を行う。

2.6.3 実験の概要

switch に関しては WIDE 合宿で使用し、その期間での評価および運用実績の蓄積のみとする。無線 LAN に関しては、毎日 19:00 より 24:00 まで参加者のホスト (200 台弱) を 1 つのセグメントにまとめ、L2 ローミングの安定性/耐久性を評価する。

2.6.4 実験結果

図 2.6 に各基地局に接続しているホスト数の変化をしめす。また、図 2.7 に基地局ごとの無線デバイスでの受信バイト数をしめす。

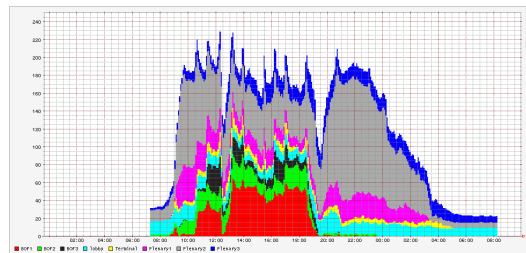


図 2.6. ホスト数の変化: 3/6

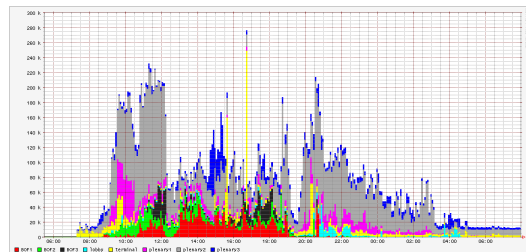


図 2.7. 受信バイト数の変化: 3/6

2.6.5 実験結果の考察

- 切り替え後のスループットが切り替え前と変化

がないことから、L2 ローミングでの問題が発生していないことが確認できる。

- 1つの基地局に接続されたホストの最大数は120程度であったが、最大時にも特に通信に問題が発生していなかった。

2.7 XCAST 会議状況把握システム

実験者： 今井 祐二

所属： 富士通研究所

2.7.1 実験の概要

XCAST による会議状況把握システムの試行実験を行った。XCAST の特徴である手軽にマルチキャスト利用が可能である点を活用し、会議の音声とプレゼンテーション映像を合宿会場で中継した。

2.7.2 実験の目的

中継の運用の手間が充分省力化できる、複数並行セッションを含む会議を小人数で中継可能かを評価する。

2.7.3 実験内容

国際会議などにおいて講演内容を効率的に伝達し、会議運営を円滑にするために、会議状況を会場内外に中継するシステムが有効であると考えられる。今回の実験では、会議状況の把握支援システムを XCAST を応用して試行した。XCAST を使えば手軽に同報グループを作成 / 運用可能であることを利用し、多数のセッションを中継の対象にすることができる。しかし、せっかく多数の並行セッションがあっても、画像の撮影やスイッチング、音声の調整などをオペレータを張り付けて行えば、複数の並行セッションを持つような国際会議においては、中継にかかる人的コストがかかりすぎてしまう。

本実験では、中継の省力化が可能な範囲で、会議状況の把握に必須の情報を選んで中継に用いた。また、安定して無人オペレーションでデータが取得できるように工夫を行った。

発表の中で内容把握に重要なのは会場スクリーンに表示されるプレゼンテーションの画像と発表者の音声である。プロジェクト画はスクリーンをカメラで撮影して取得する事が多い。この場合会議参加者の体や影、スクリーンの揺れなどの外因でプレゼンテーションの一部が欠けたり、画像が不安定になる恐れがある。今回は RGB fan out より画像を直

接ダウンスキャン&キャプチャして用いた。これにより、プロジェクトの明るさ、スクリーンへの投影環境に影響されず安定した画像を安定して取得できる事を狙った。音声は会場内に設置したオーディオアンプの AUX を無調整で使用した。

中継画像は、WG メンバの PC で受信する他、ロビー横に設置した PDP に表示し、会場内の参加者への提示を行った。



図 2.8. ロビー設置 PDP システム

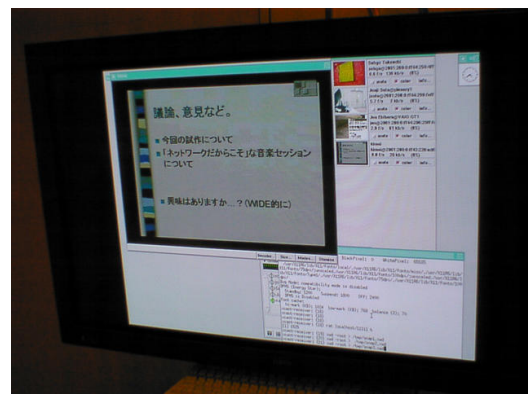


図 2.9. PDP 表示イメージ

2.7.4 結果とまとめ

中継実験の結果として以下の知見がえられた。

- プロジェクト画像の取得は無人で安定して行う

ことができた。カメラ撮影の場合の外因による不安定は取り除くことができ、内容の把握に十分な品質を無人操作で得ることができた。

- ビデオキャプチャカードの性能で画質が大きく劣化した。プレゼンテーションの内容を判読するには充分で、WG 参加者のラップトップへの表示には問題ないが、PDP などある程度大きな画面へ表示した際にははっきりと解像度が落ちていることがわかる。
- 運用上の問題として、中継機材の物理的な接続を切られてしまう場合が多々あった。送信対象とした BoF 部屋が非公開セッションにもたびたび使用され、中継のカットを確実にするためにケーブルが抜かれた。この場合、ラップトップへの中継で画像が来ていないことを確認しオペレータが部屋まで行っていた。画像が無い場合に、ケーブル抜けなのか、プレゼンテーションが行われていないかを判別する必要がある。

全体としておおむね、会議の進行状況把握に十分な品質の中継を安定して省力化して行う目処がたつたと考えられる。

2.8 遠隔ネットワーク監視とネットワーク分散管理 実験

実験者： 土井 一夫

所属： サイバー・ソリューションズ

2.8.1 実験の目的

大規模ネットワークの利用者に対し、特定の端末・管理者を必要としないネットワーク可視化ツールを広く提供し、ネットワーク管理の新しい形を提案する。

ネットワークを直接監視しその情報を MIB 化するプローブ (CpMonitor) をもって非 SNMP 機器や個々の機器によらない情報を新たに観測対象に含め、既存の SNMP 対応機器の観測と統合した上でさらに自由度が高く応用範囲の広いネットワーク観測というものを模索する。また、それらの IPv6 上での SNMP 通信への対応も行う。

2.8.2 実験の概要

合宿ネットワーク各所に CpMonitor を設置し、ネットワーク自体から情報収集を行う。収集された情報は MIB 化され、IPv6 および IPv4 上の SNMP によりアクセス可能な形で公開される。

公開される情報は以下の通り。

- (1) IPv6
 - (a) IP パケット数・量
 - (b) UDP データグラム数・量
 - (c) TCP セグメント数・量
 - (d) ICMP メッセージ数・量
 - (e) アプリケーション毎トラフィックのパケット数・量
- (2) IPv4
 - (a) IP パケット数・量
 - (b) UDP データグラム数・量
 - (c) TCP セグメント数・量
 - (d) ICMP メッセージ数・量
 - (e) アプリケーション毎トラフィックのパケット数・量

マネージャは SNMP によりその情報を収集・蓄積・公開する。収集の際は IPv6 を用いる。公開には Java プログラムを使用し、対応 Web ブラウザのある環境ならどこからでも参照できることとする。

また、標準管理プロトコル SNMP 採用の特質を生かし、ネットワーク観測チームの MRTG ページへの情報提供も行う。

2.8.3 実験の環境

各マシンの配置は図 2.10 の通り。

3 台のマシンを用意し、それぞれ図で示された以下の部位の観測を行った。なおそのうちの一台は公開用マネージャを兼任させた。

- (1) nsmanager(2001:200:0:ff20::d/203.178.196.13)
 - (a) SAT-camp と camp-backbone-net をつなぐ線
 - (b) ATM-LSR-camp LSR1 LSR2 と camp-backbone-net をつなぐ線
 - (c) LSR5 と Wireless-Terminal をつなぐ線
- (2) nsprobe1(2001:200:0:ff40::4/203.178.204.4)
 - (a) LSR3 と Cable-Terminal をつなぐ線
- (3) nsprobe2(2001:200:0:ff48::4/203.178.236.4)
 - (a) Wireless-Terminal の無線で見えている範囲全部

通信の観測のためにはインテリジェントスイッチのミラーポートを用いた。

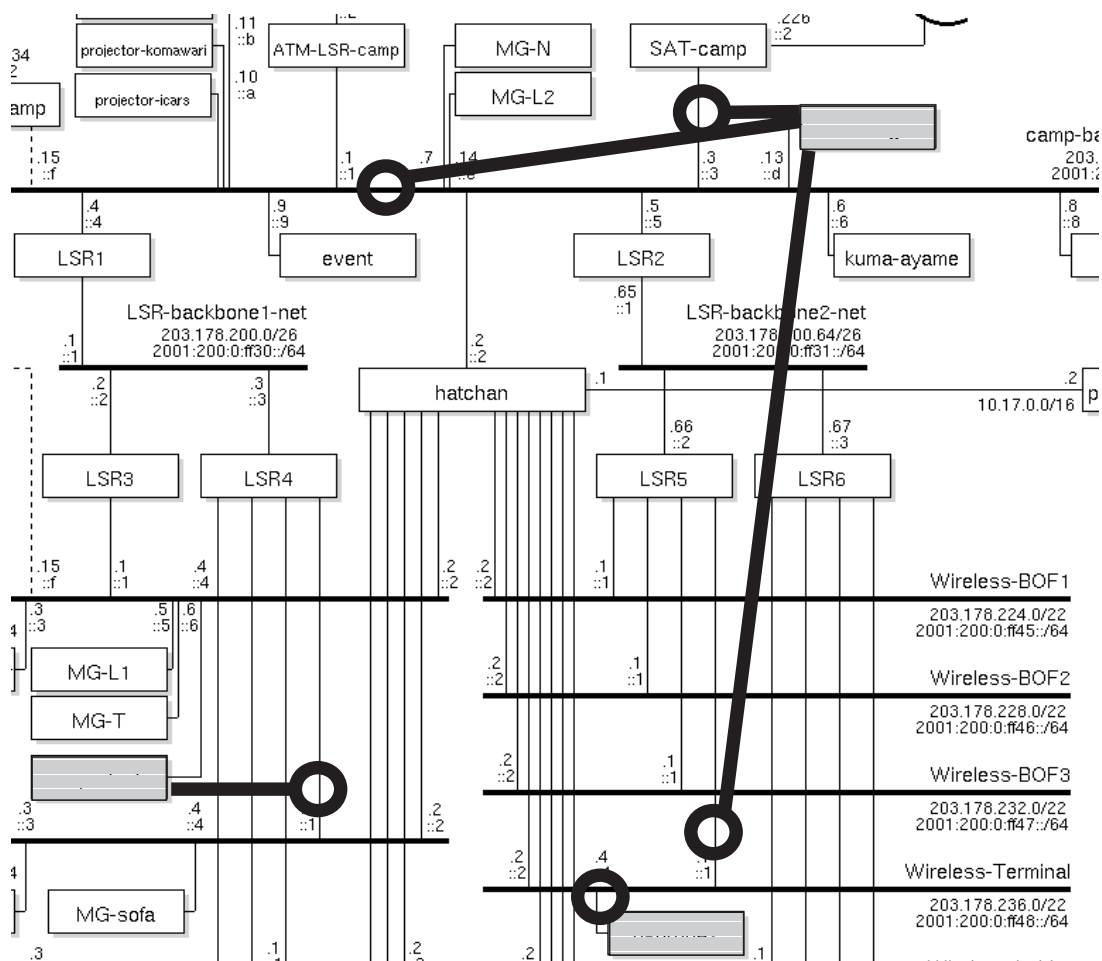


図 2.10. マシン配置図

2.8.4 結果と考察

CpMonitor による情報収集・公開は合宿期間中を通して問題なく安定して行われ、このシステムを使った観測が実用的であることを示した。特に IPv6 上のアプリケーション毎トラフィック情報はここでも公開していない情報であった。

マネージャによる IPv6 上の SNMP 情報収集も安定して行われた。収集された回数は以下の通りであった。毎分毎の収集であるので 1 日あたり 1440 回の収集が行われるはずであるが、実際には準備状況やネットワークの状況によって収集が行われない場合があった。ただその場合も回復次第収集が再開されており、3/6 はほぼ全日の収集が行われている。

- (1) nsmanager(2001:200:0:ff20::d/203.178.196.13)
 - 3/4 0 回
 - 3/5 510 回
 - 3/6 1418 回

- 3/7 619 回
- (2) nsprobe1(2001:200:0:ff40::4/203.178.204.4)
 - 3/4 105 回
 - 3/5 621 回
 - 3/6 1462 回
 - 3/7 676 回
- (3) nsprobe2(2001:200:0:ff48::4/203.178.236.4)
 - 3/4 65 回
 - 3/5 619 回
 - 3/6 1245 回
 - 3/7 566 回

公開に関しては利用した Java の制限などから IPv4 のみの公開となった。ユーザは合宿地のどこからでも GUI を操作し全てのデータをグラフで見ることができた。図 2.11 に公開時のスクリーンショットを示す。

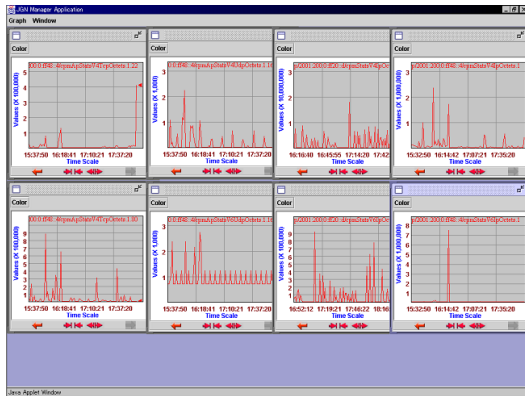


図 2.11. データ公開ユーザインタフェース

今後の課題としては

- (1) 公開部分の IPv6 化
- (2) 公開インタフェースの改良
- (3) 収集情報の高度化
- (4) 収集情報の解析が挙げられる。

2.9 IPv6 マルチキャスト接続実験

実験者: 高井 道久、大野 修
 所属: NEC
 実験者: 城子 紀夫
 所属: NEC 通信システム

2.9.1 実験の目的

IPv6 マルチキャストの実際の運用に近い環境の下での実用性の検証、ネットワークに負荷を掛けた場合における各通信機器の耐性の評価と、ネットワーク全体の安定化のためのノウハウを得ることを目的とする。

2.9.2 実験の概要

IPv6 マルチキャストのプロトコルとして PIM-SM を用いる。マルチキャストデータは DVTS(Digital Video Transport System) を使用し、3 箇所の BoF 部屋の会議の様子をロビーと Terminal Room の 2 箇所にリアルタイムにマルチキャスト配信することにより、ネットワークに負荷を掛けた場合の機器の耐性の評価を行う。また、QoS を適用し、3 本の DVTS データが流れる Fast Ether の総帯域を QoS によって 80 Mbps に設定し、1 本を EF クラス (40 Mbps)、残り 2 本を BE クラスに割り当てた場合の受信画像の品質を比較する。

2.9.3 実験環境

今回の実験環境を図 2.12 に示す。送信側として 3 箇所に DV カメラを配置し、それぞれをルータに入力し受信側 2 箇所へマルチキャストで送信を行う。受信側へは、一方は Fast Ether、他方は GbE を経由して、それぞれに 3 本分の DVTS データが流れるようにする。また、ネットワーク内のユニキャストルーティングプロトコルとして OSPFv3 を使用する。

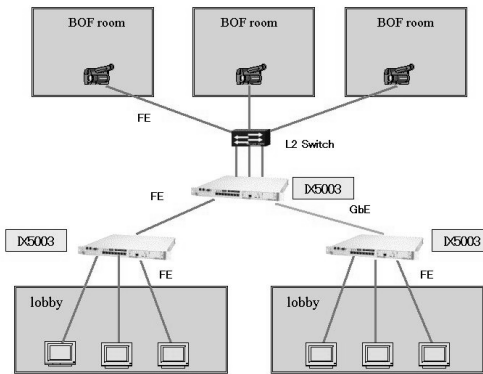


図 2.12. IPv6 マルチキャスト実験環境

2.9.4 実験結果

DVTS データ 3 本を用いた環境では、画像・音声 が乱れることはなく、安定して転送でき、ルータ・L2 スイッチの動作に関して特に問題は発生しなかった。BoF 部屋が満員のときに、会議の様子をマルチキャスト配信された DV 画像によって視聴する人も見られ、十分に実用に耐えうることが証明された。QoS に関しては、EF クラスに設定したデータは画像・音声とも乱れることなく転送でき、BE クラスに設定したデータはパケットロスにより映像、音声 が乱れていたため、QoS による優先制御が正しく動作していることが確認できた。

2.9.5 まとめ

3 本の DVTS データを流しても問題無く安定して転送できたという実験の結果から、Fast Ether のワイヤスピードに近いデータ量に対するルータと L2 スイッチの耐性が示された。また、社内放送や遠隔授業などの用途に対する IPv6 マルチキャストの実用性が証明された。QoS に関しては、回線の総帯域

を越えるデータ量が流れている環境において、リアルタイム性が重視されるデータもしくはその他の重要なデータの配信をマルチキャストを使用して行う場合、EF クラスを割り当てることによって輻輳による品質低下を避けることが可能であることが示された。

2.10 iCARs 合宿支援システム

実験者 羽田 久一
 所属 奈良先端科学技術大学院大学
 実験者 川喜田佑介、國司光宣、岡田耕司、
 若山史郎、成瀬大亮
 所属 慶應義塾大学

2.10.1 iCARs と合宿ネットワーク実験

iCARs(Internet Creates Augmented RealSpace)では、実空間ネットワークという考え方により、新しい社会を構築するプロジェクトである。iCARsでは現在のインターネットを構成している要素であるPCやルータのみならず、ありとあらゆるものを仮想的にネットワーク化することを目標としている。このような仮想的にネットワークに接続された物体は、その位置情報やIDなどを管理する必要がある。合宿での実験項目として、無線タグを用いた人間の位置情報把握をメインとして実験を行った。

2.10.2 実験概要

本実験は、ネットワークを利用した合宿参加者の追跡を可能とするシステムを用いて合宿中のユーザビリティを向上させるとともに、実空間ネットワークに関する実験を行うことを目標とした。特定の参加者を追跡するのみならず、複数の参加者の関連や、位置情報からの参加者の検索などについて、インターフェースを用意することにより、柔軟な検索を可能としている。参加者の追跡手法としては、RFIDを用いた部屋単位での人間の追跡とLIN6-MA(Mapping Agent)を利用したセグメント単位でのPCの位置追跡を行った。

システムは対象である参加者やPCの位置を把握するためのセンサノードとセンサノードで検知した情報を集積するバックエンドサーバの2つの部分から構成される。センサノードとしてはRFIDを用いたもの、LIN6MAを用いたものの2つを用意した。

これらを元に、人間やPCの位置情報をネットワー

ク上から閲覧、検索可能とする実験を行い、Webを通したインターフェースを用いることにより、実験参加者がそれぞれ他の参加者の居場所を追跡したり、ある場所に存在する参加者の集合を検索することを可能とした。

2.10.3 RF タグによる位置情報の取得

本実験では参加者の位置情報を追跡するためのシステムとしてRF Code社のspiderタグを利用した。spiderタグは電池を内蔵した無線タグであり、それぞれが固有のIDをもち、300MHz帯の電波として発信している。このタグを名札とともに、参加者全員に携帯してもらうことにより、ユーザの位置情報を特定することを試みた。

アンテナにもよるがひとつの受信機が認識できるタグの距離は10m程度となっており、今回の会場それぞれの部屋をカバーするのに十分な能力を持っている。そこで、今回はそれぞれの部屋について最低1つの受信機を配置し、参加者の位置情報を特定することとした。受信機の配置方法を図2.13に示す。



図 2.13. 受信機の配置方法 (プレナリルーム)

アンテナ、受信機とネットワークに接続するための計算機はそれぞれ一組で配置され、これをまとめてセンサノードと呼ぶ。受信機と計算機はRS-232Cポートで接続され、コマンドや情報の入出力を行う。計算機はNetBSD/hpcmipsの実装されたPDA端末(モバイルギアII R550)で構成されている。本実験で利用した典型的なセンサノードを図2.14に示す。



図 2.14. 典型的なセンサノード

2.10.4 LIN6 マッピングエージェントによる端末位置の取得

LIN6MA 内部では、LIN6ID とネットワークの prefix の対を管理している。これを、ユーザ毎に利用することによってユーザのマシンの大まかな位置情報とみなすことができる。

今回の合宿では、LIN6 MA を改変し、各ユーザが Mapping Update を MA に通知するタイミングで、Locator を nlx と呼ばれるデーモンに通知した。通知内容には、LIN6ID とネットワークの prefix が含まれる。nlx は、RF タグによる位置情報センサノードと同様に動作し、その名前は、Network Locator eXchanger から由来している。

2.10.5 位置情報サーバ

位置情報は通常、緯度経度高さのような数値的な情報として扱われることが多い。しかしながら、これらの数値は人間の一般的な位置の把握形態とは違う。そこで今回は位置情報としては、センサノードを配置した部屋単位、場所単位での情報提供を行った。

センサノードで収集された ID 情報は MySQL データベースを用いたサーバに格納される。MySQL データベース内には、それぞれの参加者に対応したエントリが存在し、それが各参加者のネットワーク上での存在として認識される情報の集合となっている。これをわれわれのモデルでは CSO(Cyber Space Object) と呼んでいる。センサノードはこの CSO への情報を供給する仕組みであり、Web を用いた UI は CSO からのデータを利用者に適した形に表現するための手法である。

2.10.6 実験項目

UI としてユーザに提供した実験項目は以下のとおりである。

1. 位置情報の検索

ある利用者の ID を指定し、それを検索する。ID の指定方法として、WIDE メンバーにユニークに割り振られている WIDE 番号を用いるほか、名前やメールアドレスを元に検索することもできる。

2. 位置からの情報検索

位置を指定することにより、その付近に存在している利用者のリストを提供する。これにより部屋ごとに存在している利用者を知ることができる。そのため、部屋の稼動状況や参加者の集まり具合を知ることができた。また、メンバーリストからどの BoF が行われているかを推測することも可能である。

3. 特定ノードの追跡

今回は利用者それぞれのタグのみならず、合宿の運営委員にはそれぞれ、役職に応じたタグを用意し、個人のタグだけではなく、追加として役職タグを携帯してもらっている。この役職タグは検索のみならず、専用のインターフェースを用いて、常時追跡することを可能とした。

2.10.7 まとめと課題

実空間に存在するさまざまな情報をネットワークを利用して透過的に扱うことを目的として実験を行った。実験項目として、ユーザに無線タグを携帯してもらい、会場内部に受信機を設置することにより、ユーザの位置情報を検出した。この位置情報をユーザそれぞれの属性として取り扱い、ネットワークを通じて閲覧、検索などの操作を行った。本実験により、ユーザの位置情報やある部屋といった単位での参加者の状況を把握することが可能となり、合宿の運営の支援や参加者どうしのコミュニケーションを支援することが出来た。しかしながら、センサノードによる認識が不十分であることや、直接的なコミュニケーションの支援システムが実装できていないため、さらなる改善が必要であると考えられる。