

第 XXXV 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 35 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

報告する。なお、本合宿で構築したネットワークで実施された実証実験の内容とその結果は、第 XVIII 部第 3 章にて詳述する。

第 1 章 2005 年春合宿ネットワーク

本章では、2005 年 3 月 22 日から 25 日まで静岡県浜名湖口イナ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について

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、合宿から WIDE バックボーンおよびインターネットへの接続用回線として、デジタル専用回線、DVB-RCS 衛星回線、VSAT 衛星回線、そして ADSL の 4 種類の

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
デジタル専用回線	2	Uplink/Downlink: 1.5 Mbps
DVB-RCS 衛星回線	1	Uplink: 最大 2 Mbps/Downlink: 最大 10 Mbps
VSAT 衛星回線	1	Uplink/Downlink: 768 Kbps
ADSL	1	—

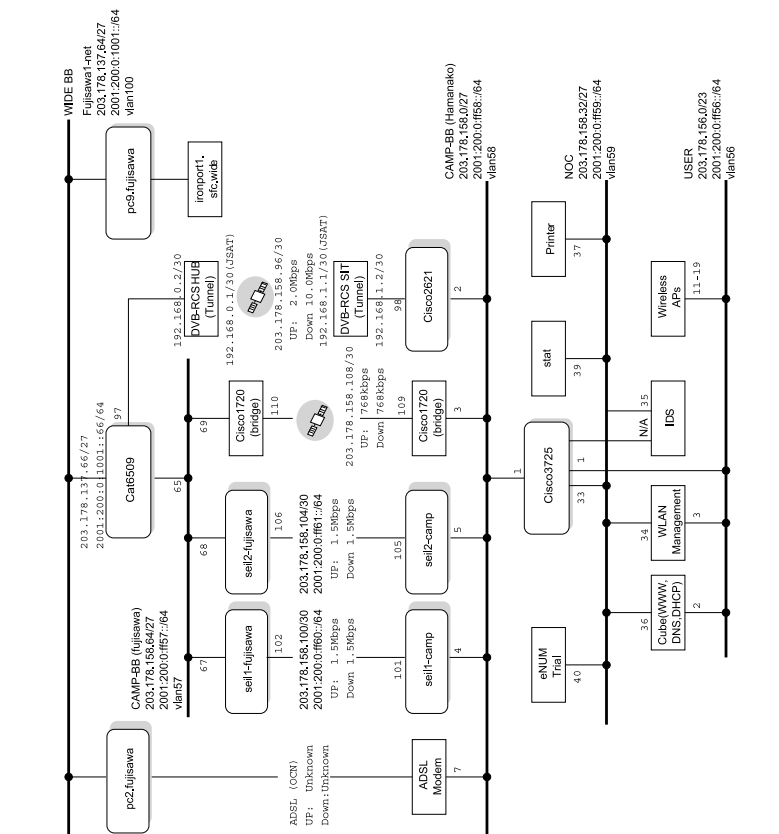


図 1.1. 2005 年春合宿ネットワークトポロジ

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、各通信回線で帯域や遅延などの特性が異なるため、安定した接続性を持つデジタル専用回線と DVB-RCS 衛星回線を主系統として、VSAT 衛星回線と ADSL を予備系統としてそれぞれ運用した。また、トラフィックの特性に応じて通信回線を選択する Policy-based Routing を行い、各回線の負荷分散を実現した。

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は、合宿参加者が接続するユーザセグメント、DNS や WEB などのサーバ群が接続する NOC セグメント、そして対外接続用回線を収容するルータ機器が接続するバックボーンセグメントによって構成した。

図 1.1 に本合宿のネットワークトポロジを示す。

合宿参加者の申し込み時にアンケートを実施し、ほとんどの参加者が有線による接続性を必要とせず、無線 LAN の使用を想定していることを確認した。このため、本ネットワークでは無線 LAN を主とした接続性を提供し、有線 LAN 機器の設置が必要最小限となるようネットワーク機器を配置した。また、ユーザセグメントには合宿参加者が全員接続可能な大きなアドレス空間を持たせ、無線 LAN、有線 LAN とともにユーザセグメントに収容した。

第 2 章 2005 年秋合宿ネットワーク

2005 年 WIDE プロジェクト秋合宿（以降、本合宿）が 2005 年 9 月 6 日（火）から 9 日（金）までの期間に長野県信州松代ロイヤルホテルにおいて開催された。本合宿のテーマは活発な実験による合宿の活性化であった。このテーマを実現すべく各 PC は努力し、結果的に下記の 5 つの実験が行われた。

- 802.11 クライアント位置検出試験および追跡訓練
- 中小規模ネットワーク向けマルチホーム技術実証実験
- 多数のノードを収容した大規模ネットワークを用いた、移動ネットワークの実証デモンストレーション

ション

- 研究会ネットワーク上でのサンプリング計測の運用
- 合宿アンケートや、所属 WG などの情報を利用した WIDE 内人間関係の可視化

本報告書では本合宿におけるネットワーク構成および、行われた実験の内容と結果を報告する。

2.1 合宿ネットワーク

本節では合宿ネットワークの構成を説明し、その運用について述べる。

2.1.1 合宿ネットワークの構成

本合宿での実験に必要な条件として実験者から挙げられていたのは下記のとおりであった。

- 対外接線が 2 接続以上あること。
- それぞれの対外接線から割り当てられる IPv6 ブレフィックスが異なること。
- IPv6、IPv4 それぞれのネットワークに関して、合宿参加者を収容するセグメント（以降、User-net）と対外接線との間に IPv4、Pv6 それぞれ別の Mobile Router（以降、MR）を接続すること。

以上の条件を満たすネットワークとして本合宿では図 2.1 で示される構成のネットワークを構築した。

対外接続

合宿ネットワークでは、物理的な対外接線として地上回線と衛星回線の 2 つを用意した。地上回線は NTT 東日本フレッツ ADSL モア（12M タイプ）を契約し、ISP 契約は OCN ADSL「フレッツ」（以降、OCN）IIJ4U（以降、IIJ）の 2 契約を用いた。この 2 つの ISP へ、1 つの ADSL 物理回線で PPPoE マルチセッション機能を用いてマルチホーム接続を行った。また、衛星回線は DVB-RCS を用いた。これらの回線の実効帯域は表 2.1 のとおりであった。表中の下りはインターネットから合宿地に向かう方向を表し、上りはその逆方向を表す。なお、OCN 接続と IIJ 接続は 1 つの同一物理回線を通しており、この物理回線が帯域ボトルネックとなっていたため、同時に使用可能な帯域は OCN、IIJ の 2 接続を合わせて 6 Mbps 程度であった。

OCN、IIJ の 2 つの地上回線では、合宿地で WIDE プロジェクト保有の IPv4 アドレスブロックを利用するために、合宿地の対外接続ルータ（noc-rt1、

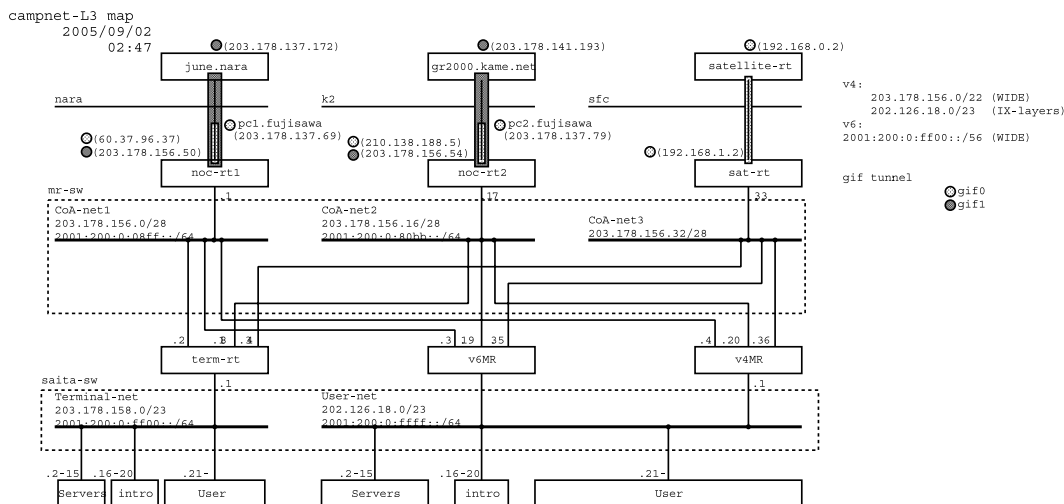


図 2.1. 2005 年秋合宿ネットワーク図

表 2.1. 対外回線実効帯域

回線	下り帯域	上り帯域
OCN	6.44 Mbps	856 Kbps
IJ	5.97 Mbps	903 Kbps
DVB-RCS	8 Mbps	1 Mbps

noc-rt2) と WIDE 藤沢 NOC に設置されたルータ (pc1.fujisawa、pc2.fujisawa) との間で IPv4 over IPv4 トンネルを設定した。更にそのトンネル上に、合宿地で WIDE プロジェクト保有の IPv6 プレフィックスを利用するために、合宿地の対外接続ルータ (noc-rt1、noc-rt2) と WIDE 奈良 NOC、WIDE K2 NOC に設置されたルータ (june.nara、gr2000.kame.net) との間に IPv6 over IPv4 トンネルを設定した。

衛星回線は、IPv4 接続のみとし、合宿地の衛星接続ルータ (sat-rt) と WIDE 藤沢 NOC に設置された衛星用ルータ (satellite-rt) との間で IPv4 over IPv4 トンネルを設定した。

気付ネットワーク

対外接続ルータと衛星接続ルータは、実験に用いられる IPv4/IPv6 それぞれの MR に対して 3 つのネットワークを提供した。MR はこの 3 つのネットワークで提供される気付アドレスを利用して切り替え・移動を行うため、この 3 つのネットワークを気付ネットワーク (以降、CoA-net1、CoA-net2、CoA-net3) と呼ぶ。ここで CoA-net1、CoA-net2、CoA-net3 に流れるトラフィックはそれぞれ noc-rt1、noc-rt2、sat-rt を介して必ず OCN 回線、IJ 回線、衛星回線

を経由するように設定を行った。

ユーザセグメント

合宿参加者が持ち込む PC とサーバは、実験用の各 MR から提供されるユーザセグメントに収容した。ユーザセグメントで用いられていた IPv4 アドレスは WIDE プロジェクト保有のものではなく、有限会社ナインレイヤーズから借用したものである。また前回合宿のアンケート結果で、ほとんどのユーザが有線接続は必要ないと回答していたことから、本合宿ではユーザセグメントは無線接続 (802.11a/b/g) のみの提供とした。

本合宿でのユーザセグメントからのトラフィックの各対外回線への振り分け方式は、IPv4 は各回線の帯域比率に応じてフロー単位で振り分け、IPv6 はすべてのトラフィックを振り分ける回線を定期的に切り替えということであった。

ターミナルスペース

本合宿では、モビリティの実験を行う関係上、合宿参加者とインターネットとの接続性が不安定となることが想定された。このため、どうしても安定した接続性が必要な参加者のためにターミナルスペースを設けることにした。ターミナルスペースのトラフィックは IPv4/IPv6 共に OCN 回線を経由するように設定を行った。また、出来るだけ多くの合宿参加者にユーザセグメントに接続し実験に参加してもらえるよう、ターミナルスペースはあえて無線接続では提供せず、有線接続のみとした。

2.1.2 合宿ネットワークの運用

合宿ネットワークの運用に関しては、初日に台風の影響で衛星の設営が遅れた他は特に大きなトラブルはなかった。あえてトラブルとしてあげるとすれば、一時的にある合宿参加者の Windows PC が IPv6 Router Advertisement をユーザセグメントに出し、他の参加者の IPv6 トラフィックを吸い込んでしまったことがあったが、即座に無線 LAN 実験チームのツールによって該当参加者の遮断を行ったため、大きなトラブルとはならなかった。また、個人所有の無線 LAN AP を持ち込んで一時的に使用していた参加者もいたようだったが、短時間しか電波を発生しておらず、こちらもトラブルとはならなかった。

対外回線の利用状況としては、初日は対外回線が ADSL のみであったために、一時的に ADSL の最大帯域まで利用してしまうことがあったが、衛星回線も利用できるようになった二日目以降は帯域には十分に余裕があった。

ターミナルスペースは、帯域計測とアンケートの結果を見る限り、あまり利用されなかったようである。

2.2 合宿において行われた実験

本節では本合宿において行われた 5 つの実験について述べる。

2.2.1 802.11 クライアント位置検出試験および追跡訓練

概要

本報告書は、2005 年 9 月に実施された WIDE 合宿において、802.11 クライアントの位置を検出するシステムの運用を行い、その運用を通して、運用技術や、検出精度、特性などを調査した。その結果、5 Ghz 帯 802.11a のクライアントについては、かなり高い検出精度であることがわかり、2.4 Ghz 帯 802.11g クライアントについては、誤差が大きくなる場合があることが判明した。また、検出に用いた AirMagnet 社の製品は、総じて使える形式となっていたものの、保管されたデータからの事後調査や、データのエクスポートについては、十分な機能を有していないことが明確になった。

目的

ワイヤレスネットワークにおける不正クライアント（偽 DHCP サーバや、ウイルス・ワームなどに

感染したクライアント）の存在は、安定運用に対する脅威となる。一方、種々の製品化が行われている 802.11 クライアントの位置検出システムは、安定運用とトラブル収束に向けて重要な技術であり、これらの脅威を最終的に除去する上で有効なツールである。そこで、2005 年 9 月に開催される WIDE 合宿において検出システムの運用を行い、その性能調査とノウハウの習得を試みた。

実験報告

本検出システム（AirMagnet 社製）は、センサ群と各センサからの情報を元に位置の特定や管理を行うサーバで構成されており、センサとサーバ間は、IP ネットワークによって接続しなければならない。したがって、会場ではセンサ用のネットワーク配線や電源配線を行い、インフラ用の無線基地局とは独立したネットワークにて運用をおこなった。また、本システムは、パッシブモニタリング手法を使用しており、検出にともなう無線ネットワーク性能の低下を招かないようになっている。

これらのセンサを各会場内に設置し、WIDE 合宿期間中継続したモニタリングと、検出精度や特性の調査をおこなった。また、センサの配置パターンを変更し、変更が精度や特性へ与える影響の調査を行った。

その結果、802.11b/802.11a においては、おおよそ正しい位置を特定することができたが、802.11g においては、かなり曖昧な位置を検出することが明確となった。これらの原因については、センサ位置の変更や設定内容も含めて検討をおこなったが、原因の特定には至っていない。

本システムの有効性については、高いという結論に至った。合宿期間中、不正な RA を送出する問題が 2 件発生し、無線ネットワーク側において、該当クライアントを遮断し、本検出システムにより、物理的な追跡を行った。その結果、おおよそ正しい位置を特定し、早急なクライアントへの対応が可能であった。従来、多数のユーザが集中している環境においては、問題あるクライアントの物理位置を特定することは困難であり、根本的対策を実施することはできなかった。しかし、本システムより、特定が可能となったことは、非常に有意義なことといえる。

また、本センサは、モニタリングから、無線チャネルの干渉やネットワークの性能、エラーレートなどをネットワーク上の問題をレポートすることが

できる。したがって、合宿においては、無線基地局の設置位置調整や運用中の問題点を把握することが容易となり、より、完成度の高い無線ネットワークの運用が実現できた。

一方、センサから取得したデータを用い事後追跡調査を行ったり、記録データを外部へ送るには、Windows OS 上で動作するソフトウェアにおいて、GUI 操作が必要であるため、機能が低かった。また、本サーバが停止した場合は、記録も停止する。したがって、耐障害性やデータ処理の利便性において、難があることが明確となった。

WIDE 研究会における運用を通して、様々な利点、欠点が明確になった。そして、運用を通して、本システムは、無線ネットワーク運用を強力にサポートするシステムであることが明確となった。今後は、継続した運用や開発元への問題点の報告を通して、より有効な運用方法について、検討していきたいと思う。

謝辞

この運用機会をくださった PC メンバの皆様、WIDE 合宿参加者の皆様、そして、WIDE プロジェクトに対し、深く御礼申し上げます。

2.2.2 中小規模ネットワーク向けマルチホーム技術 実証実験

概要

マルチホーム化された中小規模のネットワークにおける対外回線の信頼性および利便性の向上を目的とした技術として「中小規模ネットワーク向けマルチホーム技術」を提案し、検討してきた。2005 年 9 月に開催された WIDE 合宿にて同技術を WIDE 合宿のネットワークに適用し、同技術が実際のトラフィックを運ぶネットワークにおいて適用できることを実証した。本文書は、同実証実験について報告するものである。

実験目的

同実験の目的は以下の 3 項目である。

- 実トラフィックに対する提案アーキテクチャの有効性の実証
- エンドユーザおよび運用者の立場からの実運用時の使用感の把握
- 新しい問題および実用に向けた積み残し課題の把握

300 人規模以上のユーザが日常的にトラフィックを発生させる実際のネットワークにおいて動作させ、提案アーキテクチャの有効性を確認することで提案アーキテクチャの有効性を実証する。また、同技術を用いたネットワークを、エンドユーザおよび運用者の立場から利用することで、同技術を用いたネットワークの実際の使用感を把握し、同技術の利便性の向上に役立てる。さらに、同技術を実際のネットワークで利用することで、新しい問題の発見や同技術の実運用に向けた積み残し課題の洗い出しと整理を行う。

実験内容

今回の実験では、論理的に複数の対外回線を UR にて収容したうえで、複数の対外回線において仮想的に障害を発生させ、UR にて対外回線をミリ秒単位で切替、高速切替されるマルチホーム環境を構築した。また、複数の対外回線が利用可能な場合には、複数の対外回線を用いたロードバランスも行った。

今回の実験トポロジを図 2.2 に示す。

今回の実験では、インターネット上に DR を 2 台設置し、それらの DR から WIDE camp network のアドレスブロックを広告した。合宿地からインターネットへの対外線は、物理的には衛星回線および ADSL 回線の 2 種、論理的には、衛星回線、ADSL 回線のセッション 2 回線の合計 3 回線とした。UR では、論理的な対外線として 3 つの回線を収容し、WIDE camp network からインターネットへの回線として利用した。UR では、それらの 3 本の回線に対する

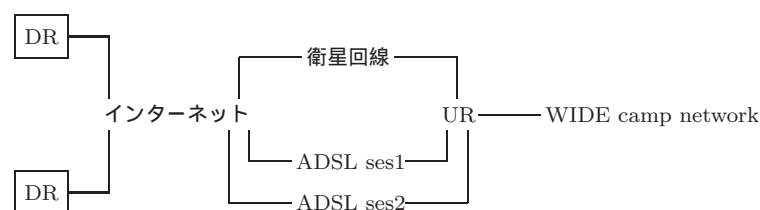


図 2.2. 実験トポロジ

各々のインターフェースの CoA を DR に通知し、3本のトンネルを確立、利用した。

URの上流にL2スイッチを設置し、同L2スイッチを操作して一定の確率でURの上位リンクをVLANグループに入れたりグループから外したりするスクリプトを動かす、仮想的な障害をエミュレートした。このスクリプトにより、合宿開催期間中およそ合計400回程度の対外回線の障害を仮想的に発生させた。

今回の実験では、インターネット上のホストから、URの対外回線用のインターフェースのアドレス、CoA1、CoA2、CoA3、および、URの内部インターフェースのアドレス、HoAに対する到達性を定期的に測定することで、WIDE camp networkとインターネット上のホストの間のネットワークの到達性を確認した。

実験結果

実験の結果、同技術を適用しなかった場合パケットロス率は80%を超える状態が頻発するほどの仮想障害を発生させていたが、同技術の適用によりパケットロス率は、定常的に最大でも20%程度に抑制することができ、提案技術によって大幅に改善されることが確認でき、提案アーキテクチャの有効性が確認された。

その一方で、今回は複数リンク上でのロードバランスを行っていたことと、衛星リンクのパケットロスが頻発したことに起因して、WIDE camp network内のエンドユーザのホストからインターネット上の任意のホストの間の通信において低い値ではあるが一定のパケットロスが発生し続ける結果となり、部分的に通信性能の劣化が見られる状態となった。これは、ロードバランスによって衛星リンクと地上回線を経由するフローがアプリケーション非依存に混在する状態となったため、結果的にはユーザの使用感としては性能劣化を感じるということであり、提案アーキテクチャによって本質的に著しい性能劣化が見られるということではない。これは複数リンクでのアプリケーション毎の振り分けなどを利用することで回避可能である。

また、同技術によって構築されたネットワーク構成の複雑さに起因する同ネットワークを運用する際のデバッグの困難さという問題が、提案技術を利用した際の運用者の視点から明らかとなった。

今後の課題

今後の課題としては、今回の実験によって明らかとなった、アプリケーション振り分けの必要性を重視し、複数回線の冗長化を行いつつ複数の回線が利用可能な状態では、可能な限りエンドユーザのアプリケーション毎振り分けの要求に沿った振り分けを行うしくみを検討する必要があると考えられる。また、提案アーキテクチャによって複雑な構成となったネットワークを視覚的にも分かりやすくするツールなどを用いて、デバッグ時の問題把握を容易にするなどのしくみもあわせて検討する必要があると考えられる。

2.2.3 多数のノードを収容した大規模ネットワークを用いた、移動ネットワークの実証デモンストラーション

The network mobility technology in the Internet area has been discussed for a long time and the specification has been finally published as RFC3963 from IETF. We had created an actual mobile network which contains a few hundreds of nodes to prove the technology works in a real environment. We confirmed that the technology works well basically however, we faced a long service disruption while moving. In this paper, we discuss the detailed configuration of the mobile network and the problem faced during the operation.

Purpose of this demonstration

The NEMO Basic Support (NEMO), which is specified as RFC3963[47], adds a mobility function to IPv6 routers. With the function, an entire IPv6 network served by a mobile router, which is a router with a NEMO function, can be a mobile network. The nodes inside the mobile network can use static IPv6 addresses which never change regardless of the attachment point of the mobile router.

One of possible applications of this technology is to provide a network in moving entities, such as buses, trains, airplanes, etc. Those moving entities may connect various network access points depending on its location. The address assigned to a mobile router from the router of each access

point will differ depending on each access point, since IPv6 addresses are usually assigned based on the network topology. The NEMO technology hides the address change of the mobile router and provides seamless access to the Internet from the nodes inside the mobile network.

In this demonstration, we accommodated the entire temporarily created network for the WIDE[308] 2005 autumn meeting under a mobile router and tried to prove the technology. The mobile router changed its point of attachment from time to time, providing seamless access to the nodes in the meeting network. The number of attendees of the meeting was almost 250 and most of them used their laptop computers to connect to the meeting network. We can think this network as a kind of moving entities which carries many people who are connected to the inside network and it is a realistic example of transportation system, like a train.

Overview of NEMO Basic Support

NEMO is an extension of Mobile IPv6[146], which is a protocol that adds a mobility function to an IPv6 node. While Mobile IPv6 focuses on an IPv6 node, NEMO focuses IPv6 networks. The NEMO protocol is quite similar to the Mobile IPv6 protocol. A router which supports NEMO is called a mobile router (MR). An MR has a static IPv6 address which is called a home address (HoA). An HoA is used to identify an MR. We can access an MR by specifying its HoA at any time. An MR also has IPv6 network(s) to serve static networks. We call such a network as a mobile network. An HoA never change even if an MR changes its point of attachment. An MR sends a message which binds its HoA and a care-of address (CoA) to its home agent (HA) whenever it changes its CoA. A CoA is an address that an MR acquires on the network to which the MR currently connects. An HA is a special node which maintains the binding information of an MR. An HA keeps the latest binding information to track the location of an MR. During the exchange

procedure of binding information, an HA and an MR also exchange the information of mobile networks that the MR is serving. Such information may be pre-configured on the both nodes, or piggybacked on a exchange message, or exchanged using dynamic routing protocols. After exchanging the information, an HA and an MR create an IPv6 over IPv6 tunnel between them. All traffic received by an MR from the nodes inside its mobile networks will be sent to the tunnel and forwarded by the HA. Also, all traffic destined to mobile networks are routed to the HA by the routing mechanism and forwarded to the MR using the tunnel connection. The network prefixes of mobile networks that an MR is serving never change even if the MR changes its point of attachment. Therefore, all IPv6 nodes which are connected to the mobile networks of the MR can have static IPv6 addresses.

Network topology

Figure 2.3 depicts the topology we used. The network created at the meeting site has a network 2001:200:0:fff::/64, which is a mobile network. The MR provided the mobile network to users who participated in the meeting. The home address of the MR was 2001:200:0:ffe::4649/64 and the MR connected to two different networks while the meeting was being held. One network was extended from the WIDE Nara NOC (Network Operation Center), which is located at Nara prefecture, Japan. The network prefix was 2001:200:0:8ff::/64. The other network was extended from the WIDE K2 NOC, which is located at Kanagawa prefecture, Japan. The network prefix was 2001:200:0:80bb::/64. The MR acquired two different IPv6 addresses as CoAs based on its attached network. Each time the MR changed its CoA, the MR sent a message to its HA to notify that the current attachment point had been changed. The HA was located at the WIDE Fujisawa NOC which is located at Kanagawa prefecture. The address was 2001:200:0:ffe::1000. The routing information for the mobile network

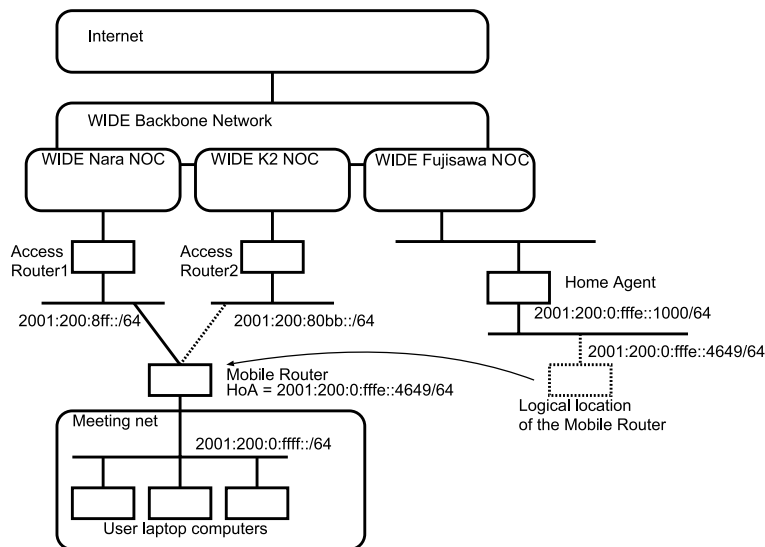


Fig. 2.3. The network topology of the demonstration

(2001:200:0:fff::/64) was advertised from the HA so that all traffic to the mobile network was routed to the HA. The HA forwards all traffic destined to the mobile network to the tunnel interface between the HA and the MR. On the other hand, all traffic generated from the IPv6 nodes inside the mobile network are forwarded by the MR to the HA using the tunnel connection.

The IPv6 connections between two WIDE NOCs and Access Routers were created using IPv6 over IPv4 tunnels, because we could not get native IPv6 connection services at the meeting place.

The physical network topology is shown in figure 2.4. The dotted objects mean that they are parts of IPv4 network. The IPv4 connections to the meeting place were provided by two different ISPs, ISP-1 and ISP-2. These two ISPs and WIDE are inter-connected at one of the Internet Exchange Points in Japan. The tunnel connections which were used to create two IPv6 networks were created over the two IPv4 ISP connections respectively. We chose this configuration because we wanted to use different ISPs over those two tunnels as much as possible. If we only used one ISP service to get IPv4 access and created two IPv6 over IPv4 tunnels over the one single IPv4 ISP connection, the most part of the tunnel

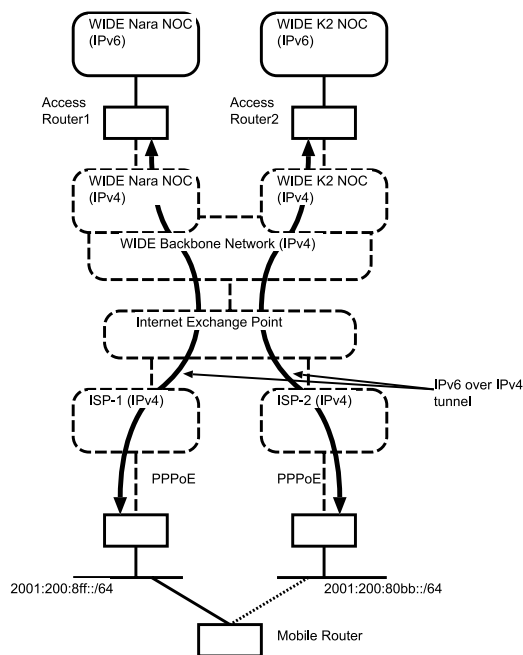


Fig. 2.4. The physical network topology of the demonstration

path would be same, since the WIDE network and ISPs in Japan usually share only one exchange point. The IPv4 path from the meeting place to the exchange point will be same even if we have two different IPv6 over IPv4 tunnels. As figure 2.4 shows, we have archived almost different tunnel paths by using two different ISPs for the IPv4 connections.

System configuration

We used the SHISA Mobile IPv6/NEMO[307] protocol stack in the demonstration. The hardware specification and software configuration are described in table 2.2.

The SHISA stack can be available from the KAME project[305] home page as a part of the KAME IPv6 protocol stack software. In this demonstration, we used FreeBSD5.4-RELEASE with the KAME snapshot as an MR and NetBSD2.0.2 with the KAME snapshot as an HA. We also used GNU Zebra[313] and ospf6d on the HA to advertise the routing information of the MR (2001:200:0:fff::/64) and the network behind the MR (2001:200:0:fff::/64).

Table 2.2. System configuration

Node	Hardware	Software
MR	Pentium4 1.8 G, 256 MB memory	FreeBSD5.4-RELEASE + SHISA 20050905 snapshot
HA	Pentium4 1.8 G, 256 MB memory	NetBSD2.0.2 + SHISA 20050829 snapshot, GNU Zebra ospf6d

Movement frequency

The meeting was held for 3 days. During the meeting, we changed the movement frequency dynamically based on the user request. The figure 2.5 is the user interface which we used at the meeting. The movement frequency is changed every 10 minutes based on the total number of

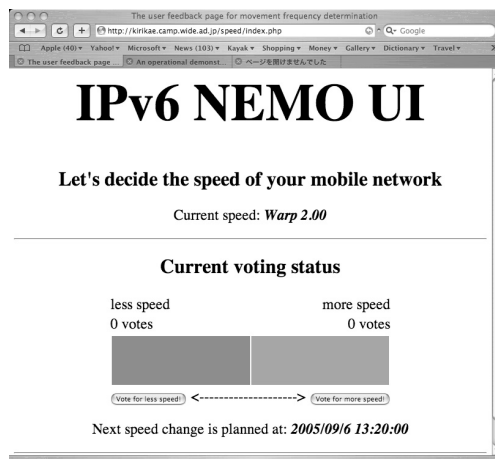


Fig. 2.5. The user interface to vote the movement frequency

users who requested more frequent movement and less frequent movement. If the number of people who requested more frequency is greater than the number of people who requested less frequency, the movement frequency will be increased. If the comparison is opposite, the frequency will be decreased.

At the initial stage of the demonstration, we set the minimum frequency to every 20 seconds and the maximum frequency to every 60 seconds with 5 seconds as a step. However, from the day 2 of the meeting, we changed the minimum frequency to every 60 seconds and the maximum frequency to 300 seconds with 60 seconds as a step, because of the problem discussed in next section.

Result and consideration

Figure 2.6 depicts the transition of the movement frequency during the meeting. As we mentioned in the previous section, the frequency was very high in the first day of the meeting. We can see the frequency is changing dynamically and randomly, which means the participants votes their request to increase or decrease the frequency based on their feeling of the speed of the network movement. The data of the latter half of the third day is not correct because of our misconfiguration of the switch configuration that changes the point of attachment of the MR. We manually stopped the movement for trouble shooting of the network and the movement frequency became more than 300 seconds, which could not be set by the frequency voting system.

We had changed the range of the frequency that the users can change from the day 2, since we got a lot of request that the service disruption time was too long when changing the point of attachment of the MR. In fact, there was about 20 seconds connection disruption during the MR is changing its attached network. The table 2.3 shows the packet loss rate using ICMPv6 echo/echo reply messages from a node inside the mobile network and the MR itself. The destination address is one of the IPv6 nodes located in

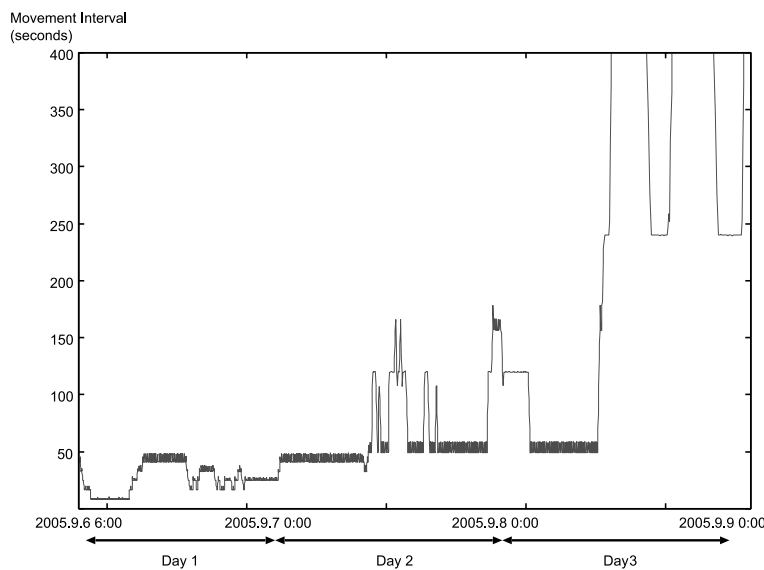


Fig. 2.6. Transition of movement frequency

Table 2.3. Packet loss rate

From	Sent/Received	Loss rate
Node inside	10842/7408	31.7%
MR	2280/2249	1.4%

the WIDE K2 NOC.

The packet loss rate of the MR is not very big. The rate is almost the same value when we are operating a mobile host, which is a node supporting the Mobile IPv6 protocol. However, the loss rate from the node inside the mobile network was high. Considering that the packet loss rate is low at the MR even when the node is acting as an MR, the difference between host behavior and router behavior seems to be the reason of the problem. The main differences of them are 1) packet forwarding function and 2) routing function. We have not found the reason of this problem. In SHISA implementation, the routing information on the MR is almost static, that is, all packets from the mobile network are simply routed to the tunnel interface. We guess that the problem is in forwarding function of the MR implementation.

Conclusion and future steps

We provided a mobile network to a large scale realistic network which has over 250 people in it. The MR basically could move between two

different networks with one problem of service disruption during handover. We used only one network interface of the MR to connect to the Internet. However, if we use two or more interfaces simultaneously, the service disruption time should be shortened or even it can be omitted. In other words, as long as we use only one interface, we cannot avoid the disruption completely. We are considering to use multiple interfaces simultaneously by utilizing the multiple CoA registration mechanism proposed in [294] and planning to perform the same kind demonstration near future to prove NEMO is usable in a real environment.

Acknowledgment

We thank to the program committees of the WIDE meeting, the WIDE backbone network operators, the SHISA project members and the Nautilus6 project[306] members.

2.2.4 研究会ネットワーク上でのサンプリング計測の運用

本節の内容は第 IV 部第 2 章に記載されている。詳しくは第 IV 部第 2 章を参照されたい。

2.2.5 合宿アンケートや、所属 WG などの情報を利用した WIDE 内人間関係の可視化

概要

現在、人間の振る舞いに注目した、社会ネットワーク(インターネットより高次のネットワーク構造)の構成手法や、特性に注目し研究を行っている。合宿参加者に対して、興味を持ったワーキンググループについてアンケートを取り、この結果をもとに、興味にもとづいた WIDE 内の人間関係グラフを作成し、分析を行う。今回の合宿では、このアンケートへの協力を呼びかけるために、ポスターにて趣旨の説明と協力の呼びかけを行った。

実験目的

合宿などから得られる情報(今回はアンケートにて、興味を持ったワーキンググループについて尋ねる)をもとにして、興味にもとづいた WIDE 内の人間関係のネットワークを構成することができると考えている。今回の合宿では、このアンケートへの協力を呼びかけるために、ポスターにて趣旨の説明を行った。

実験内容

合宿では、実験のデータ収集を行った。合宿参加者を対象としたアンケートによって、WIDE 内の興味のあるワーキンググループを回答していただいた。このデータから WIDE 内における、広義の意味での SNS を構成する。これによって、WIDE 内での興味の分布や、ワーキンググループ間の相関関係などを明らかにする。

実験結果

今回の実験では、191 名から 58 ワーキンググループに対しての 1011 回答が得られた。実験結果は現在分析中で、今後の合宿や論文での発表を行う。

今後は、このデータを利用して WIDE 内における興味に基づいた人間関係ネットワークを構成し、passive SNS の構成や、dynamic SNS の構成についての考察の参考情報とする予定である。また、所属研究室(奈良先端科学技術大学院大学インターネット工学講座)内においても人間関係グラフを作成し、inter SNS の構成手法についても考察を進める。

2.3 まとめ

本合宿のテーマは活発な実験による合宿の活性化であり、このテーマに沿うように5つの実験が行われた。PC は出来る限り多くの合宿参加者に実験に参加してもらえるようなネットワーク設計・構築を行い、どうしても安定した接続性が必要な参加者のためにターミナルスペースを設けた。合宿中は、IPv4 接続は安定したが、IPv6 接続は不安定であった。また、ターミナルスペースはあまり利用されなかった。結果的には本合宿のテーマは実現できたように思う。

