第 17 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

はじめに

インターネットにおける技術革新は年々急速になってきているが、さらに最近では、多くの技術開発が同時多発的に発生し、それらが相互に協調しあって実験や評価が行われる傾向が強くなってきている。そのことは、従来の運用ネットワーク上での実験を極めて困難にしている。

実運用を目指して開発されている技術間においては開発時からさまざまな連係を考慮することが望ましく、標準化の早い段階における相互運用実験を行う必要性はきわめて高い。

そこで、実ネットワークにできるだけ近い特性を持ちつつも, 実験用に構築された仮設ネットワークテストベッドの構築の需要が高くなってきている。 [16]

WIDE プロジェクトでは、年 2 回、研究者全員が参加するワークショップが開催される。会期は 5 日間、参加者 250 人程度で、参加者のほとんどはネットワーク研究者であり、数百台の計算機が持ち込まれる。

このワークショップでは、会場に仮設ネットワークが構築される。このネットワークの用途は次の通りである：

1. ワークショップ参加者に対するインターネットへのアクセスサービスの提供
2. ワークショップ参加者に対するワークショップ内部での情報提供サービス
3. ネットワーク実験用テストベッド
    - 新規技術間の相互運用
    - 実装別の相互接続試験
    - 高速ネットワークの提供
    - その他

前のふたつの用途は一般的な利用目的であるため安定した運用が求められるが、3 番目の用途は実験用のネットワークであるため様々な技術導入が行われており、状況に応じて刻一刻とネットワーク構成が変化する。

会場は一般のホテルや研修センターで、ネットワークはワークショップのたびに仮設される。したがって、このネットワークは比較的大規模な仮設の実験ネットワークとして捉えることができよう。

そこで、ここでは、1997 年 9 月と 1998 年 3 月とに開催されたワークショップで構築したネットワークをケーススタディとし、その際に得られた経験を元に実験ネットワークについて議論を進めることにする。

第 2 章

1997 年秋のワークショップ

本章では、1997 年 9 月 2 日から 5 日に開催されたワークショップで構築したネットワークをケーススタディとし、その際に得られた経験を元に実験ネットワークについて議論を進めることにする。

2.1 概要

本ネットワークの全体構成図を図 2.1に示す。
対外接続は以下の 2 系統が用意された。

専用線

会期中は帯域幅 128K ビット /秒の専用線により WIDE バックボーンと接続された

衛星回線

帯域幅 2M ビット /秒の衛星回線 ((株) 日本サテライトシステムズ提供) により WIDE バックボーンと接続された

衛星を利用するにあたっては会場屋上に設置直径 1.2 メータのアンテナおよび衛星回線用設備を仮設した。

2.2 導入技術

評価実験用に導入された技術を以下に示す。

- バックボーン関連技術
  CSR(東芝および日立製作所による実装) と衛星回線技術が導入された。
- RSVP[162] 関連技術
  専用線には RSVP 対応ルータが設置された。また、QoS アプリケーションかつ実トラフィック発生源として日立製作所のインターネット電話『Talkware』が導入された。

- 次世代インターネットプロトコル IPv6[169]
  IPv6 が動作するプロトコルスタック実装と、 IPv6/IPv4 プロトコル変換の実装がそれぞれ複数導入された。

- WWW クラスタ
  複数の計算機 (6 台) をクラスタ化した負荷分散型 WWW キャッシュシステムが導入された。 その中では、単一のアドレスへの接続要求を複数の接続先に分散させるために横河電機による NAT 実装である『菫 (すみれ)』の改良版が利用されている。

- mobile サポート
  移動する機会の多いワークショップ内で通信の利便性を向上させるため、 複数の無線方式ネットワークが提供された。 同時に、mobileIP[112] への対応も行われ、 東芝と日立製作所の実装が導入された。

- マルチフィード DNS サーバ
  接続相手に応じて返答を変化させる DNS サーバ (横河電機『マルチフィード DNS(MFDNS) サーバ』)

- NAT ルータ
  プライベートアドレスとグローバルアドレスの変換を行う NAT ルータ (横河電機『菫 (すみれ)』、日立製作所のルータ NR60)

- DHCP サーバ
  WIDE 実装の DHCP(Dynamic Host Configuration Protocol) サーバ

2.3 実験項目

ワークショップ内ネットワークを利用して行われた実験を以下に示す。

- NAT を利用した経路選択手法の評価
  NAT 利用したパケット変換によって、行きの経路は専用線で戻りの経路は 衛星回線となるように経路制御する方式を実際に運用して動作の検証を行った。

- WWW キャッシュシステムにおける負荷分散システムの評価
  ロードバランシング WWW キャッシュの選択にアドレス変換技術による方式と、Proxy Auto Configuraton を用いることでユーザ側のブラウザに キャッシュサーバを選択させる方法を比較評価した。

- RSVP による帯域保証付きインターネット電話の評価
  帯域保証効果の実証のためにインターネット電話を利用した RSVP の有無による比較が行われた。

- IPv6 関連実験

  1. IPv6/IPv4 トンネルを利用してワークショップネットワークと 6Bone(IPv6 によるバックボーンネットワーク) を接続して運用
  2. WIDE プロジェクトの複数組織で行われている IPv6 プロトコルスタックの実装の相互接続実験および評価
  3. バックボーンとして敷設されている ATM 網の一部を利用して、複数の IPv6 セグメントを ATM を介して接続する実験
  4. IPv6 と IPv4 プロトコル間の相互変換実装の評価 (日立製作所/富士通研究所)

- マルチフィード DNS(MFDNS) サーバ運用および DNS フェイクの実証実験
  NAT 等で分離されたプライベートネットワークにおいて、DNS query に対する返答を書き換えることで透過的なネットワークを実現できることを実証した。

- FEC(マルチキャストに誤り訂正符号) の評価
  マルチキャスト音声伝達の際に FEC を利用して誤り訂正行うことで、IP パケットがランダムに廃棄される回線においても伝送品質劣化が起こらないことを 検証し信頼性の高いマルチキャストネットワーク実現の方法を検討した。

- CSR 評価実験
  CSR が有効性を検証するための試験として、会場内のビデオ中継トラフィックを利用した性能評価と、現在の実装の限界点を見つけるための負荷試験が行われた。

- セキュリティ強度実験
  インターネットで行われている不正アクセスの常套手段である IP アドレス偽造を用いたコネクションの不正リセット攻撃と、ネットワーク盗聴によるパスワード不正取得の手法を、実験ネットワーク上で行い、その手法の有効性とユーザの対策の状況について確認した。 本実験に関しては、2.6節で詳しく述べる。

2.4　測定

ネットワーク全体の挙動監視については、通常のネットワークに準じる方法を適用した。

- SNMP を利用した実験ネットワーク内の各ルータの負荷および専用線の帯域の利用率監視を行った

- 測定結果をリアルタイムに処理し、WWW などの手段を通してユーザに提示した。

2.5 コーディネーション

今回のワークショップのネットワークは、実際の 20 人強の実験担当者を中心として 4ヶ月程度の準備期間を持って設計された。メンバーのほとんどが研究者であり、ネットワークに対する知識は深い。設計に関する議論の場はメーリングリストを使用し、必要に応じて月一回程度の会合を開いた。

今回の実験ネットワークの設計および構築は WIDE プロジェクト内で閉じていたため、すでに各担当者間での面識があったこともあり、コミュニケーションをとることは比較的容易であったと思われる。基本的に運用時の情報交換は各実験担当者間で直接行われた。

2.6 セキュリティ強度実験

2.6.1 実験の目的

現在、インターネットにおけるセキュリティ確保のためにさまざまな研究が行われている。しかしながら、我々の多くは「日々利用しているプロトコルがどれだけセキュリティ的に脆弱なのか」を身をもって把握していない。このため、1997 年度夏合宿において、「IP security tiger team」と称し、我々が日々利用しているインターネットプロトコルがいかに脆弱かを示す実験を行った。

2.6.2 実験の概要

合宿前に実験のために以下のようなプログラムを作成し、各々を合宿ネットワーク上に接続されたホストで実行した。これにより、実際に合宿に持ち込まれているホスト群に対し攻撃を行い、合宿参加者に体験して頂いた。

tcpsniff: TCP による通信を盗聴し、暗号化されていない秘密情報 (例: パスワード) を抽出する

tcpreset: 他ホストの TCP による通信を、TCP 接続切断要求パケットを偽造し切断する

両プログラムは BPF[1]を利用して合宿ネットワーク上を流れるパケットを監視し、TCP による通信を検出する。`tcpreset` は検出した TCP による通信を切断するためのパケットを作成し合宿ネットワークに送出する。`tcpsniff` は通信に利用されている ftp や http などのプロトコルを判別し、各プロトコルにあわせ秘密情報を抽出する。

このように実際にセキュリティホールを攻撃するような実験を行う場合、合宿参加者に迷惑を及ぼしてはならない。このため、合宿開催前に以下のように実験の開催を周知徹底した。

[1] Berkeley Packet Filter

- 実験開催時には合宿参加者に予告する
- 実験は合宿ネットワークのうち、予告した一部分を用いる
- 実験担当者は誤って秘密を得てしまわないようなプログラムを作成する
- しかし、誤って秘密を得てしまった場合に、秘密を得てしまった事実を該当者に速やかに告げ、得てしまった秘密そのものは一切口外しない
- 実験が行われる行われないに関係なく、セキュリティ的に強いプロトコルの利用を推奨する

最後の項目は、具体的には telnet のかわりに ssh、login 時の UNIX password による認証のかわりに使い捨てパスワード、pop プロトコルの認証には USER/PASS による認証でなく APOP による認証を利用することを推奨した。

2.6.3　実験環境

合宿地では、プレナリを行った会議場のネットワークにおいて、tcpreset の実験を 1 度、tcpsniff の実験を 5 回実施した。

2.6.4　結果

tcpreset は正しく TCP による通信を切断することに成功し、合宿参加の方に危険性を実感して頂くことができた。実験を開催したのが深夜だったこともあって、体験者が小人数に限られてしまったのが残念である。

tcpsniff の実験については、表中では便宜上 5 回の実験に A から E までの名前をつけ区別している。tcpsniff の実験で検出された TCP セッションの本数を表 2.1に示す。それぞれ、実験を行う subnet ではあらかじめ実験の開催を予告しているので、多くの合宿参加者は通信をやめるか、他の subnet に移動してしまっている。このため、表 2.1の数値は、合宿の平常時に流れていた TCP セッションの本数とは大きく異なる。

既に述べたように実験を予告しているため、ここで検出されているトラフィックの大部分は合宿参加者が tcpsniff に検出されようとして故意に流しているものである。実際にパスワードの送信が検出された場合でも、ほとんどは実験参加者が入力したダミーのパスワードが検出されている。合宿前にセキュアなプロトコルを利用するよう推奨した甲斐あってか使い捨てパスワードシステム skey や、APOP による pop プロトコルの認証など、盗聴に強いプロトコルが多く利用されていた。

表 2.1: 実験開催日時と TCP セッションの本数

実験 id	時刻	時間	subnet	TCP 本数	telnet ssh	pop	http	ftp
A	9/2 深夜	15min	10.0.8.0/23	378	18	0	130	3
B	9/3 昼	15min	10.0.8.0/23	451	29	2	306	4
C	9/3 深夜	15min	10.0.8.0/23	438	59	7	8	15
D	9/4 昼	30min	10.0.8.0/23	1398	21	15	14	1
E	9/4 昼	10min	cisco の手前	189	27	39	39	1

2.6.5 考察

本実験はインターネットプロトコルがセキュリティ的に脆弱だということを合宿参加者に知らせることが目的となっており、啓蒙的な意味あいが強い。合宿参加者には合宿前の告知によりセキュリティ的に強いプロトコルを利用して頂いたし、実際に攻撃のデモンストレーションを行い関心を深めて頂いたので、おおむね実験の目的は果たせたと言えるだろう。上記に述べたように、実験を行う場合には実験を行うネットワークと実験の内容を前もって合宿参加者に通知した。これにより、実験は合宿参加者に対し悪影響を及ぼさなかった。しかし、予告する以上、IP security tiger team の実験を行うネットワークには合宿参加者の実トラフィックが流れず、現実味に欠けるものになってしまった。

この場を借りて、実験に御協力頂いた合宿参加者のみなさんに感謝致します。

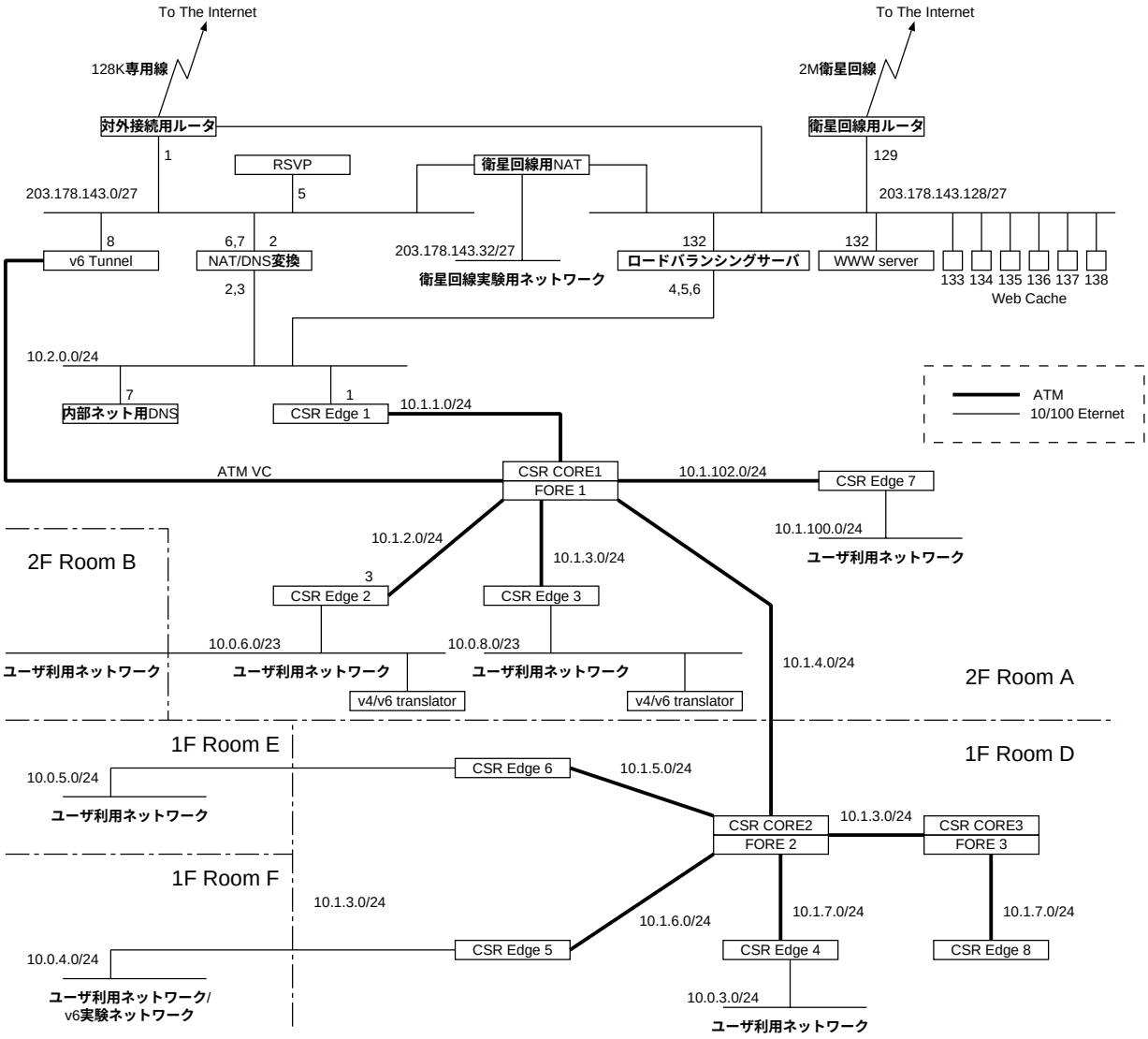


図 2.1: 97 年秋の仮設ネットワーク構成図

第 3 章

1998 年春のワークショップ

本章では、1998 年 3 月 16 日から 19 日に開催されたワークショップで構築したネットワークをケーススタディとし、1997 年秋のワークショップで議論した手法の評価を行う。

3.1 概要

春のワークショップにおけるネットワークは、安定したユーザサービスの提供と新しい技術による実験との両方を実現することを目標として構成した。

本ネットワークの全体構成図を図 3.1に示す。

対外接続は以下の 2 系統が用意された。

専用線

会期中は帯域幅 386K ビット /秒の専用線により WIDE バックボーンと接続された

衛星回線

帯域幅 2M ビット /秒の衛星回線により WIDE バックボーンと接続された

3.2 実験項目

本ネットワークでは、コーディネーションの一手法として仮設ネットワーク上に導入された技術だけでなく、ケーブリング、ユーザサービス、Web による情報公開等も実験として扱った。

実験ネットワーク全体のリーダー、サブリーダーは以下の 2 人が務めた。

- リーダー : 宇夫 陽次朗
- サブリーダー : 今泉 英明

各実験項目と担当者を以下に示し、次節以降に実験ごとの報告をまとめる。

- 対外線 (リーダー : 石井 公夫)
  - UDLR 相互接続実験 UDLR(泉山 英孝、竹井 淳、小松 大実、出水 法俊、朝枝 仁、西田 視磨、原 和弘、藤井 昇)
  - NAT によるプライベートネットワークの運用 (藤澤 慎一)
  - プロトコルによる経路制御 (藤澤 慎一)
  - 対外地上線における ALTQ を用いたトラフィック制御 (長 健二朗、石井 公夫)
- 内部ネットワーク
  - バックボーン技術 (リーダー : 新 善文、角川 宗近)
    - IPv4CSR の実験 (永見 健一、宇多 仁)
    - Comet による Gigatbit Ethernet および IEEE 1394 の実験 (陣崎 明、小林 伸治、古賀 久志)
    - IPv6 ネットワークの構築 (有賀 征爾、小原 泰弘、若井 宏美、関谷 勇司、廣瀬 謙治、増田 康人、矢野 大機)
    - IPv6 対応 CSR の実験 (神明 達哉)
    - Packet Redirection による HTTP Transparent Proxy の評価 (片山 洋平、坂本 佳則)
  - アプリケーション (リーダー : 今泉 英明)
    - IPSEC, ISAKMP (IKE) 相互接続実験 (藤江 正則、伊藤 純一郎、坂根 昌一、石井 秀治、渡部 謙、神明 達哉、鈴木 知見、木村 俊洋、佐藤 信、窪田 歩)
    - FEC (Forward Error Correction) (金井 久美子)
  - その他 (リーダー : 鈴木 麗)
    - School of Internet - 遠隔からの会議参加を支援するための実験 (大川恵子、伊集院百合、村上陽子、中村 謙、大橋克彦、河合敬一、廣石透、櫻井智明)
    - ネットワークトラブルチケットシステムの構築と運用 (宇多 仁、宇夫 陽次朗、鈴木 麗、本間 秀樹、矢野 大機)
    - 合宿ネットワークの成果報告書の作成 (鈴木 麗)
    - 合宿ネットワークの成果報告書の作成にむけた基本的なトラフィック収集と表示 (渡辺 恭人、矢野 大機)
    - 配置とユーザ・サービス (小原 泰弘)
    - camp-WEB サーバの運用 (大江 将史、荒木 靖宏、小原 泰弘、三宅 義久)

3.3 ALTQ を用いたトラフィック制御

3.3.1 実験の目的

ボトルネックリンクにおけるトラフィック制御の効果を検証すること。WIDE 合宿の地上線は 200 人を越える合宿参加者が外部にアクセスするための生命線であり、細い臨時回線に多様なトラフィックが集中する。このような状況で telnet 等のインタラクティブな通信の応答時間の改善や、ポリシに従った帯域割り当てを実現することは今後の重要な課題である。ALTQ は RTBone WG の一貫として公開されているキューイング機構の実装で、ALTQ を使って合宿ネットワークのトラフィック制御の効果を示す。

また、CBQ をライブなトラフィックに適用することによって、WAN 接続における CBQ のクラス分け、帯域の分配モデルを作る狙いもある。

3.3.2 実験の概要

地上線の両端の PC ルータで、ALTQ に含まれる CBQ と RED を使ったトラフィック制御を行なった。

トラフィック制御のクラス分けの概要は以下のようになっている。

- telnet、rlogin 等のインタラクティブ・トラフィックの帯域を確保
- DNS のトラフィックを優先
- ビデオ中継のトラフィックを確保
- 各クラスにはさらに RED をかけて、フローごとの公平性を上げる
- FEC や mbone のトラフィックが他のトラフィックに影響を与えない様に設定

合宿中のトラフィック情報はマルチキャストで合宿ネットワークに流し、合宿参加者が手元の PC で、事前に配布したモニタプログラムを使って、リアルタイムに各トラフィックの割合、パケットの落ち具合をモニタできるようにした。また、トラフィック情報をログに落しておいて後から解析可能とした。

3.3.3 実験環境

実験に使用した機器は、地上線の両端でルータとして機能した PC が 2 台、トラフィック・モニタ用に PC を 1 台使用した。地上線は 384kbps の臨時専用線で SFC と浜松にある合宿会場を繋ぎ、FreeBSD/ALTQ の動作するルータ PC で RISCom/N2 カードを使った。

また、合宿会場への接続は地上線の他に衛星経由の接続があり、メール、HTTP、FTP、Mbone などのバルクデータは衛星経由となるようにプロトコルで振り分けする手段をとった。

3.3.4　結果

実験ほぼ予定どおりに実施でき、また、ほぼ期待どおりの効果が確認できた。特に、合宿中に他の実験の設定ミスで大量のトラフィックが地上線に回り込む事態が発生したが、他のトラフィックにほとんど影響を与えなかった。

3.3.5　評価

合宿のライブ・トラフィックで 4 日間に渡る連続運転を通して、ALTQ の実装の安定性、スケーラビリティが確認できた。また、遠隔で設定変更をする際の問題点や注意点が明らかになった。

3.3.6　考察

WIDE 合宿の対外線に関して、バルクデータを衛星に振り分け、かつ、地上線でトラフィック制御を行なうと、128kbps の地上線でストレスなく telnet が利用できる環境が実現できる見通しがたった。

3.3.7　今後の課題

機能面では次のステップとして、運用していく上で改善すべき点がいくつか見つかった。今後も実際の運用を通して改善を続けて行きたい。また、誰でも CBQ の設定ができるようにするためには、分かりやすいドキュメントや設定ファイルの解説が必要である。さらに、トラフィック制御の効果をいかに分かりやすく示せるかは永遠の課題である。今回、トラフィックモニタの配布を行なったが、インストールがもっと簡単にならないと使うひとが少ないことがわかった。

3.3.8　関連情報

- Kenjiro Cho, “ALTQ Home Page”, http://www.csl.sony.co.jp/person/kjc/software.html, 1997. [170]

- Kenjiro Cho, “A Framework for Alternate Queueing: Towards Traffic Management by PC-UNIX Based Routers”, Proceedings of 1998 USENIX Annual Technical Conference, June 1998. [171]

- 長 健二朗, “PC Unix ルータによるトラフィック制御の実現”, インターネットコンファレンス’97 論文集, December 1997. [172]

3.4 NAT によるプライベートネットワークの運用

3.4.1 実験の目的

WIDE 合宿は 近年 参加者が 200 人を越え にもかかわらず 割当てられるアドレスは 24 bitmask (254 個分) であるため 全員 + 実験用機材 に一意の IP アドレスを割当てることが困難になってきている。 そこで IP アドレス、ポート番号を変換する NAT を合宿ネットワークの出口付近に置き、NAT の有効性を検証する。 あわせて NAT の耐久力も検証する。

3.4.2 実験の概要

NAT を合宿ネットワークと地上線との接点に置き、合宿ネットワークの外向きトラフィックのうち HTTP 以外を NAT に流す。

実験に必要な一部の ネットワークを除き 合宿ネットワーク内の大半の機器には 10/8 のアドレスを割り振り、default を NAT 側に向けてもらう。 このため 合宿ネットワークに住む人たちは NAT を経由しないと 外の世界には到達できない。

実際の設定は 以下のとおり (de0 は外側のインターフェイス名)。

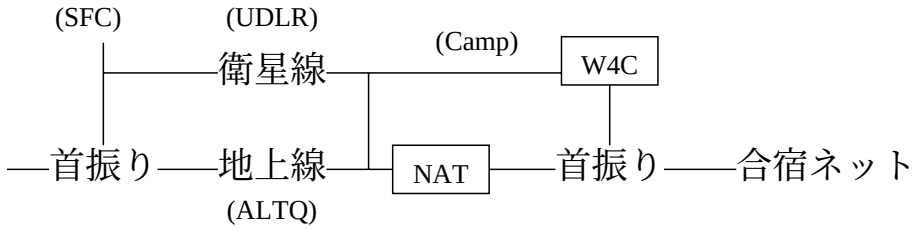
```
nat de0 10.0.0.0/8 to 203.178.143.3 port 28672 - 32767
```

ここでは 外向きに使用する port 番号の範囲を 28672 - 32767 に制限しているが、この範囲には特に意味はない。

3.4.3 実験環境

実験に使用した機材は BSD/OS 3.1 の動作する PC (K6 200MHz, メモリ 128MB) で NIC を 2 枚挿して NAT として使用した。

- 実験構成



NAT は 経路のディフォルトを地上線に向ける。 従って 合宿ネットワークから出て行くパケットは地上線を通って出て行き、帰りは プロトコルに従って 地上線か衛星線のいずれか を通って来る。 詳細は プロトコルによる経路制御 を参照のこと。

3.4.4　結果

NAT は合宿のトラフィックに耐え、十分に機能した。 若干の問題が発生したが、それ以外は安定した動作を示した。

合宿期間中を通じ 2 回ほど NAT が落ちた。 合宿期間中にはこの原因を特定できなかったので 合宿終了後に core を解析したところ ログ出力時のバグであることが判明した。 このバグは合宿終了後に修正した。

PORT を使用する FTP (traditional FTP) を通すことができた。 ただし 今の実装では相手方サーバーの FTP-DATA の始点ポート番号が 20 である という仮定をおいている。この結果 ftp.iij.ad.jp に対して PORT が通らないことが判明した。 ftp.iij.ad.jp では サーバーの始点ポート番号が 20 ではないので、この NAT は越えられない。 この問題に対する解はまだ無い

3.4.5　考察

本実験で NAT のログとして 以下のものが得られた。

- 1 秒 あたりのパケット数の最大値: 675
- 1 分 あたりのパケット数の最大値: 23954
- 1 時間あたりのパケット数の最大値: 531359

合宿地側の首振りルータで HTTP プロトコルは W4C 側に流したので NAT に流れ込むトラフィックは ネットワーク内で発生する量よりも減るが そのことを考慮しても 合宿ネットワーク程度の規模だと 生活するのに十分耐えることが確認できた。

3.4.6　今後の課題

合宿前の仮組みの時に マルチキャストパケットを受けると カーネルが落ちることが判明した。 合宿後に暫定的な変更を加えて落ちないようにしたが、NAT が マルチキャストをどう扱うべきか 十分に考慮する必要がある。

archie が NAT 越えができないことが判明した。ただし archie.kyoto-u.ac.jp に対してはパケットが通らないように見えるが、archie.iij.ad.jp に対しては パケットが通る。 これは現象が観測されただけで 対処はしていない。

今回 NAT は比較的安定した動作を見せたが それでも 2 回 落ちた。 実装をもっと安定させる必要がある。

NAT の動作としては ある程度安定してきた と言えるが 設定等はまだ判りずらい。 実際の運用をするうえでも 改善していきたい。

この NAT の機構を追加したことによるオーバーヘッド等の測定は 一切行っていない。カーネルに時間を測定できるような変更を加える等をして 実際に測定する必要がある。

3.5 プロトコルによる経路制御

3.5.1 実験の目的

始点アドレス、終点ポート番号等で経路制御を行なうルータを継ぎ、そのような経路制御が有効に働くかどうかを検証する。

3.5.2 実験の概要

首振りルータを SFC と合宿地に置く。 ただし この 2 台に依存関係は無い。

合宿地の首振りルータは 以下の終点ポートを持つパケットを W4C 側に、それ以外のパケットを NAT に流す。

- 80(HTTP),

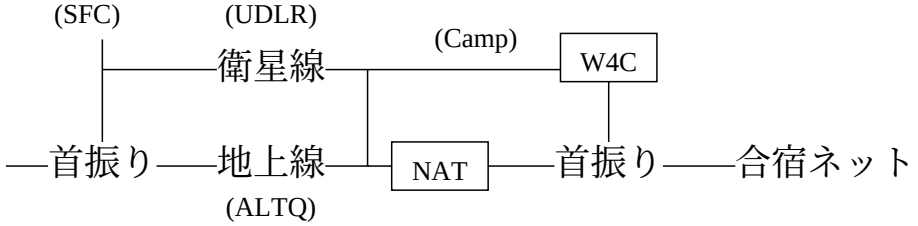
SFC 側の首振りルータは 以下の終点ポート番号を持つパケットを UDLR 側に、それ以外のパケットを ALTQ 側に流す。

- 20(FTP-DATA),
- 80(HTTP),
- 110(POP3),
- 143(IMAP2),
- 220(IMAP3),
- 443(HTTPS),
- 8080(HTTP)

3.5.3 実験環境

実験に使用した機材は BSD/OS 3.1 の動作する PC (SFC 側 Pentimu 133MHz、メモリ 32MB、合宿側 K6 200MHz, メモリ 128MB) で NIC を 2 枚挿して 首振りルータとして使用した。

- 実験構成



- 他の実験との関連

  合宿地では Web 関連の packet を W4C 側に流す。他 の packet を NAT 側に流す。SFC では FTP/WEB を UDLR 側に、telnet 他 を CBQ 側に 流す。

3.5.4　結果

本実験で 首振りルータのログとして 以下のものが得られた。

- 1 分あたりの最大 パケット数: 17651 (SFC 側)
- 1 分あたりの最大 パケット数: 18973 (合宿側)

首振りルータは SFC、合宿地 ともに十分に機能した。 合宿期間中に 何度か設定変更を行ったが、その変更に追随して パケットを新しい経路に流すことができた。 このことは首振りルータのログ以外にも W4C/ALTQ/UDLR 側からも確認することができた。

3.5.5　考察

実装は、予め設定された経路を覚えておき パケットを出力する際に覚えておいた経路を ip_output() に渡す という簡単なものであったが 十分に機能した。 経路の探索は線型であったが 覚えておく経路の数が 7 つ と少なかったため 大きな問題とはならなかった。 覚える経路の数がもっと増えると 探索は 線型ではなく hash 等を使わないと苦しくなるだろう。

3.5.6　今後の課題

今回は 経路を予め覚えておき、検索して渡す という実装方法をとったため、経路を覚えた後で該当する経路が変更される場合などに追随できない。 これに対応するには カーネル内で持っている経路制御表を IP アドレスやポート番号を見るように拡張する必要があると思われる。

今の首振りルータはパケットの向きを変えるだけで その相手が生きているかどうか には無頓着である。 実際に運用する時には 何らかの形で相手の生存を確認し 相手が死んでいる場合には別の経路に投げるように設定を自力で変更する等の処理が必要だろう。 ただこの機構をカーネルだけで実装するには荷が思いと思われる。 デーモンが必要になるのではないか。

この 首振りの機構を追加したことによるオーバーヘッド等の測定は 一切行っていない。カーネルに時間を測定できるような変更を加える等をして 実際に測定する必要がある。

3.6 IPv4CSR の実験

3.6.1 実験の概要

ラベルスイッチ技術は、次世代の高速ルータ技術として IETF MPLS WG(MultiProtocol Label Switching WG) で標準化が進められている。

ラベルスイッチ技術を利用した LSR(Label Switching Router) は、通常の Layer-3 パケットフローを、固定長ラベルに対応させ、固定長ラベルで転送を行なう。LSR の適応として、ラベルスイッチエンジンに ATM スイッチを用い方法がある (ATM-LSR)。CSR は、ATM-LSR の一種として実装されたものである。

1 つのラベルに対応するパケットストリームの粒度は、様々なレベルの定義がある。例えば、同一の宛先 IP アドレスと送信 IP アドレスの組を持つパケット流に対して 1 つのラベル (VPI/VCI) を割り当てることができる。この場合に必要な VC 数は、ネットワークのスケールに依存し、[173] で解析されているようなバックボーンのトラフィックにおいては、多くの VC が必要であることがあげられている。

しかし、キャンパスバックボーンレベルでは、必要な VC 数が少なく、適用可能であると考えられる。

この実験では、約 60 台のホストを収容する WIDE 合宿バックボーンに CSR 技術を適用した場合のカットスルーフロー数及びカットスルー VC 数を測定した。

CSR 技術を用いたバックボーントポロジーは、CSR CORE 1 台に Edge 4 台をスター状に 155Mbps ATM で接続した。1 台の Edge から Internet に接続し、3 台の Edge の下の 100M Ethernet にユーザが接続している。

上記の構成で、実運用トラフィックをかけて 4 日間連続して CSR を動作させた。この時の最大カットスルー数は、36 フローであり、平均カットするー数は、11 フローであった (図 3.2)。これより、上記のような規模のバックボーンにおける CSR で必要な VC 数は、最大 76 本であり、平均 22 本であることがわかる。

上記規模のネットワークに CSR を導入した場合は、必要な VC 数は、約 100 本程度であるという知見が、実ネットワーク上での評価から予想される。

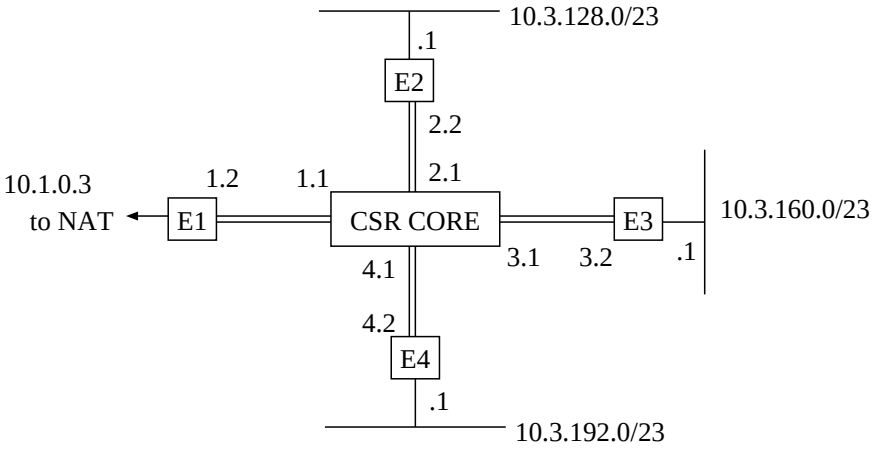
今後、多数の様々なネットワーク規模での評価を行なっていく予定である。

3.6.2 実験環境

- 実験構成

  Address 10.3.x.x/16

  図中の数字は、アドレスを示す。



3.6.3　関連情報

- Y.Katsube, K.Nagami, H.Esaki, “Toshiba’s Router Architecture Extensions for ATM : Overview”, IETF RFC2098, Feb., 1997. [174]
- K.Nagami, Y.Katsube, Y. Shobatake, A. Mogi, S. Matsuzawa,T. Jinmei, H. Esaki, “Toshiba’s Flow Attribute Notification Protocol (FANP) Specification”, IETF RFC2129, April, 1997. [42]
- S.Lin, N.Mckeown, “A Simulation sutudy of IP Switching”, ACM SIGCOMM 97. [173]
- ftp://ftp.wide.toshiba.co.jp/pub/csr
- http://infonet.aist-nara.ac.jp/member/nori-d/mlr/
- draft-nagami-csr-fanpv2-nd-00.txt
- draft-nagami-csr-fanpv2-dcmode-00.txt
- draft-ohba-csr-fanpv2-icmode-00.txt

3.7　Comet による Gigatbit Ethernet および IEEE 1394 の実験

3.7.1　実験の目的

- Gigabit Ethernet の可能性を試す

- IP/IEEE1394 相互接続へ向けた実験
- Comet の運用実験

3.7.2 実験の概要

本実験の実験項目は次の通りである。

- Gigabit Ethernet 接続試験
- Gigabit Ethernet 負荷試験
- (Comet による)IEEE1394 over IP

各社の Gigabit Ethernet 機器の相互接続性を確認し、その通信特性をスループット、遅延ジッタに関して評価する。スループットについては合宿ネットワークの内部バックボーンとして使用するとともに負荷トラフィックを意図的にかけ、MRTG でトラフィックを測定しつつ実用スループットを調べる。遅延ジッタについては IEEE1394 over IP のトラフィックを流し、画像の乱れ具合で画像パケット転送遅延ジッタを評価する。

3.7.3 実験環境

Gigabit Ethernet スイッチ 2 台、Comet 7 台、Workstation 2 台で合宿ネットワークの内部バックボーンの一部 (Comet バックボーン) を構成する。この Comet バックボーンでは 2 つある BOF 部屋の状況を本会議場と会場入口の 2ヶ所に IEEE1394 over IP で常時中継するのに加え、ユーザ接続用の Hub を本会議場、および 2 つの BOF 部屋に用意して多くの合宿参加者に使用してもらう。

IEEE1394 over IP は isochronous モードのデジタルビデオデータを IP Multicast として流す。IEEE1394 によるデジタルビデオは 1 チャンネルあたり約 30Mbps の帯域を使用する。Comet バックボーンは IP 的に 1 つのサブネットとして構成しているため、IEEE1394 over IP のトラフィックがユーザ接続用の 10Mbps Hub に流れ込むとそれだけで帯域を使い切ってしまい通信が行えなくなる。そこで、ユーザ接続用 Hub の手前に Comet を設置し、IEEE1394 over IP のパケットのみを落す Filtering Bridge として機能させる。この Filtering Bridge は本会議場用、BOF 部屋用の 2 つを用意する。

3.7.4 結果

IEEE1394 over IP によるデジタルビデオ転送は 2 つの BOF 部屋からそれぞれ送信し、本会議場と会場入口で受信するという形態で行った。2 チャンネルなので 60Mbps 以上の IP Multicast が定常的に流れていたことになるが、Gigabit Ethernet の負荷試験を行って

いる時以外は画像の乱れは確認できなかった。また、この IP Multicast は 2 台の Comet でフィルタリングしているため、本会議場等のユーザ接続用 Hub では IEEE1394 over IP のトラフィックの影響を受けること無く通信できることが確認できた。

Gigabit Ethernet 相互接続試験では、High Speed Network BOF 参加者が持ち寄った Gigabit Ethernet 機器を合宿ネットワークに組み込んで相互接続性、性能評価、負荷試験を行い、評価結果を WIDE プロジェクト内メーリングリストなどで配付した。持ち込んだ機器間で相互接続性の問題は無かった。IP Multicast のパケットが 90Mbps 程度定常的に流れている状態でも、ユーザ接続サービス等合宿ネットワーク内部バックボーンとしての動作にまったく問題無かった。合宿期間中、スイッチに流れたトラフィックや Multicast パケット数を MRTG で測定しログを採取した。スイッチを多段接続すると遅延のジッタにより IEEE1394 over IP の動画転送に多少の乱れが生じた。負荷試験では計 400Mbps 程度のトラフィックを Comet バックボーン内に流した。この状態では Gigabit Ethernet に直結したワークステーションでサービスしていた DHCP のサービスを受けにくくなるといった現象が観測されたが、接続性そのものは確保されていた。Comet による Filtering 機能もこの程度のトラフィックに耐えられることが確認できた。

3.7.5　今後の課題

実験中に Comet による Filtering Bridge が正しく動作しなくなることがあった。実装の安定化が今後の課題である。また、より詳細な解析をするためにトラフィックの流量や遅延といったデータをさらに詳細に取る必要がある。

3.7.6　関連情報

IEEE1394 WG

3.8　IPv6 ネットワークの構築

3.8.1　実験の目的

IPv6 になじみの少ない者が一から IPv6 ネットワークを構築する。その過程、ノウハウをドキュメント化する。つまり、「IPv6 ネットワーク構築手引書」のようなドキュメントを作ることがこの実験の第一目的である。このドキュメントの対象者は IPv4 は知っており、IPv4 でのネットワーク構築をしたことがある者である (つまり基本的なネットワーク構築の知識は割愛する)。

3.8.2 実験の概要

- IPv6 stack のインストール
- LAN の構築
- 6Bone への接続
- Registry への登録
- アドレスの自動設定
- トランスレータの設定

OS に IPv6 stack をインストールするところから始め、現在世界で運用されている IPv6 ネットワークである 6Bone につなぐまでを第一目標とする。

Registry System に登録をおこなうことで、global address の割り当てをおこない、これからプロバイダーなどが実際に IPv6 で接続性を提供する際の手順のリファレンスとなるようにする。

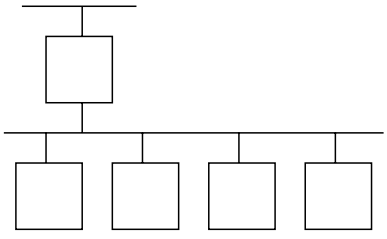
基本的なネットワークが構築できた段階で、トランスレータの設定をおこない既存の IPv4 ネットワークとの接続性も確保する。

次に、IPv6 の特徴の一つであるネットワークの自動設定をおこなう。

実験中におこったトラブル、失敗などを含めて、過程とノウハウは余さず記録し、文書とする。

3.8.3 実験環境

- 実験構成
  トポロジー例 (基本ネットワークのため簡単なトポロジーとする)。



今回は複雑なネットワークや快適なネットワークを提供するというのが目的ではなく、 IPv6 で簡単なネットワークを構築し、その過程を文書化することで IPv6 の普及をすすめるのが目的である。そのため、実際の実験ではあまりトポロジーは変更せず、トラブルの記録等を中心におこなった。

3.8.4　結果

最初に目的としていた、LAN の構築、6Bone への接続、アドレスの自動設定、トランスレータの設定等は行なうことができた。また、IPv6 stack として、NR60、Linux、FreeBSD(Hydrangea) などいくつかの実装を使用したことで、実際の運用上での問題等が発生した。

3.8.5　考察

自分たちが IPv6 ネットワークを構築する際に、実際の実装は現在既に十分にあるが、それを使うためのドキュメントが絶対的に不足していることを実感した。IPv6 はもう「動く」プロトコルとして存在するが、その普及のためには種々のドキュメント、啓蒙が必要であると思われる。

3.8.6　今後の課題

- ネットワーク構築手順の文書化
- 実験中に起こったトラブルの文書化
- 作成した文書を利用した IPv6 の啓蒙
- おこった問題点の実装へのフィードバック

3.8.7　関連情報

- WIDE Project IPv6 WG
  http://www.v6.wide.ad.jp/
- IETF IPng WG
  http://playground.Sun.COM/ipng/
- クリスチャン・ウイテマ著 プレンティスホール出版
  「IPv6 次世代インターネットプロトコル」[175]

3.9　IPv6 対応 CSR の実験

3.9.1　実験の目的

IPv6 対応 CSR を、実用ネットワーク上で運用し、安定して動作させること、および障害があればそれに対処することを目的とする。

3.9.2 実験の概要

IPv6 対応の CSR を合宿ネットにつなぎ、実用的なトラフィックを流す。IPv6 パケットがカットスルーされるかどうか、IPv4 CSR としても協調して動作するかどうか、全体に安定して動作するかどうか、といったことを検証する。

具体的には、以下の手順にしたがう:

1. IPv6 の telnet, ftp をカットスルーするという設定を行い、live traffic を流す。実際にカットスルーされるか、また不要になったカットスルーパスが解放されるか、といったことを確認する。

2. IPv6 のカットスルーを確認できたら、同時に IPv4 についても telnet, ftp, http などを対象にカットスルー設定を行う。IPv4/v6 の双方のカットスルーが安定して行えることを確認する。

3. 安定した動作を確認できれば、カットスルー率や VC 消費率など、各種統計情報の取得も行う。これは、1, 2 の段階でも並行して行うが、安定動作が確認できない段階では意味のある統計が得られない可能性が高いので、実質的にこの段階からが統計情報の収集フェーズとなる。

3.9.3 実験環境

図 3.3に、実験に用いたネットワークトポロジーを示す:

すなわち、IPv6 LAN を収容する CSR エッジルータ (E6-2) と、6bone へのゲートウェイとなる CSR エッジルータ (E6-1) との間に CSR コアルータを配置し、この 3 台の間でのカットスルーを試みる。

E6-2 は IPv6 LAN の環境設定を提供している。すなわち、IPv4 については DHCP サーバとして動作し、IPv6 については router advertisement メッセージを定期的に広告している。

6bone への接続には IPv6/IPv4 トンネリングを用いる。そのためには IPv4 のグローバルアドレスが必要になるため、NR60 をグローバルセグメントに配置し、E6-1 との間を結んでいる。プライベートアドレス側のルーティング情報がグローバルセグメントに流れることを防ぐために、NR60 と E6-1 の間では IPv4 パケットは流さない。

また、上記トポロジー図には含まれていないが、E6-1 からは同じ合宿ネット内の comet ネットワーク上に配置された socks 64 サーバとの間に IPv6/IPv4 トンネルが張られている。

3.9.4 結果

IPv6 についてはトラフィックそのものが少なかったものの、生活できる程度には安定して動作した。カットスルーも概ね問題なく成功した。ただし、細かい点で若干未解決の問題が残った。これについては後述する。

3.9.5　評価

本実験での定量的な評価としては、以下のものが得られた:

- IPv4 最大カットスルーフロー数: 18
- IPv6 最大カットスルーフロー数: 7
- エッジルータの DHCP を利用したユーザクライアント数の最大値: 20

3.9.6　今後の課題

全体としては安定して動作していたものの、定期的にカットスルーに失敗する現象が発生していたことがわかった。CSR のコントローラと ATM スイッチの間のやり取りがうまくいっていないことが原因で、今後その原因を特定して修正し、さらに安定性を高める必要がある。

一方、今回の実験を通じて、実用ネットワーク上での一定以上の安定性が得られたことから、今後はカットスルー率のような定量的データを積極的に取得し、システムの改善に役立てたい。

3.10　Packet Redirection による HTTP Transparent Proxy の評価

3.10.1　実験の目的

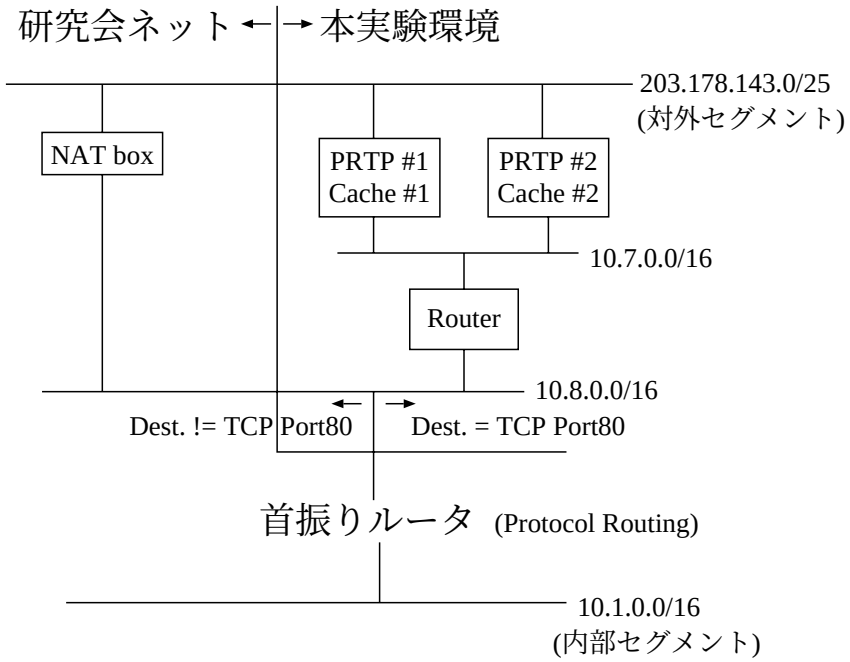
ある範囲の network を想定し、その The Internet の出口に、「Packet Redirection による HTTP Transparent Proxy」(以下 PRTP と略記) を配置したときの挙動を観察、評価する。

3.10.2　実験の概要

研究会ネットワークから The Internet へ出る経路上に PRTP を配置し、これを使って The Internet へ向かうすべての Port 80 番宛て TCP session を、宛先アドレスを別途設置したキャッシング代理サーバのそれに書き換え、HTTP 要求ヘッダを代理サーバ用の形式に書き換えることにより、代理サーバあての接続として扱い、透過的なキャッシングサービスを行なう。このとき起こる現象、報告される現象を記録し、評価、分析を行なう。また、PRTP を使用せず一般的なキャッシング代理サーバのみを用いて WWW キャッシングシステムを構成する場合 との比較を行なう。

3.10.3 実験環境

- ネットワーク構成



- 構成図作成の際に考慮したこと
  原理上、PRTP に障害が発生すると、ルータ同様、そこが経路途上となるすべての通信が途絶する。研究会ネットワークでは、本実験以外に様々な実験が行なわれており、本実験で使用する PRTP に障害が発生した場合に、研究会ネットワークの利用者が The Internet への到達性を失うことは、万に一つでも起こってはならない。したがって、本実験環境で使用する PRTP、キャッシングサーバは二重系とし、さらに、それでも障害が避けられなかった場合を考慮し、「首振ルータ」(Protocol Routing Router) で、本実験の扱い対象である ポート 80 番あての TCP パケット以外は本実験環境を経由しないよう、配慮した。

- このネットワークの動作概要
  内部セグメントに接続されている利用者の端末から発せられる The Internet あてのすべてのパケットは、「首振ルータ」に集まる。ここで、ポート 80 番あての TCP session のみ「Router」へ送り、それ以外は「NAT box」へ送る。「Router」へ集められたポート 80 番あて TCP session は、二重化されている PRTP へ向かう。

- 機材
  - ハードウェアと OS
    AT 互換機 (Pentium 100MHz) FreeBSD-2.2.5R

- 使用したソフトウェア
  - キャッシングサーバ
    Squid Internet Object Cache version 1.1.20

– PRTP は以下の組み合わせで構成

IP ヘッダのアドレス書き換え機能 IP Filter version 3.2.1
HTTP 要求ヘッダの書き換え機能 Transproxy version 0.3

- 他の実験との関連
  二つの異なる構成の比較を行なうが、この切り替えを、NAT 及び Protocol Routing Router (首振ルータ) の Operater に依頼する必要がある。

3.10.4　評価、まとめ

本書 6 節を参照されたい

3.10.5　関連情報

- 実験の報告詳細
  本書 6 節

- Squid Internet Object Cache
  http://squid.nlanr.net/

- IP Filter
  http://coombs.anu.edu.au/ipfilter/

- Transproxy
  ftp://ftp.nlc.net.au/pub/linux/www/transproxy-0.3.tgz

3.11　FEC (Forward Error Correction)

3.11.1　実験の目的

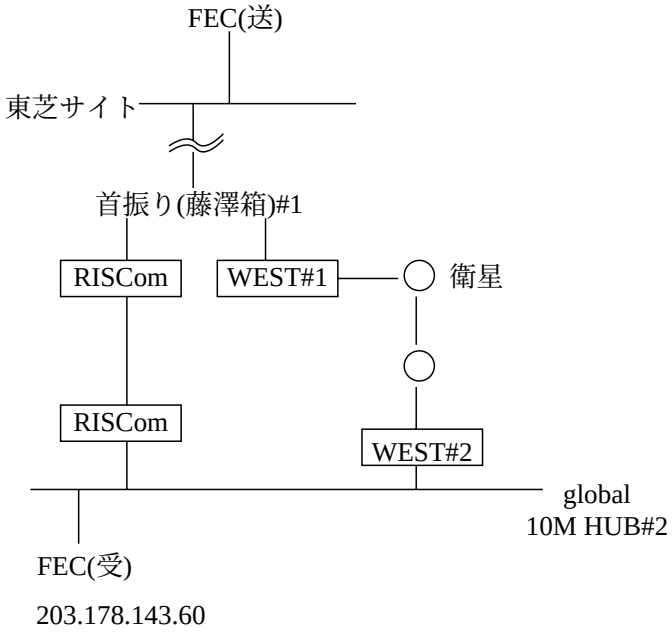
FEC を東芝サイトと合宿ネットに置き、real-traffic 上でのパフォーマンスを評価する。

3.11.2　実験の概要

FEC の受信ホストを合宿ネットの external につなぎ、東芝サイトからデータの送信を行なう。FEC のパケットセグメント化による影響や実用的なトラフィックでの FEC の受信状態を観測する。東芝から WIDE へ FEC した UDP でデータを流し、パケット廃棄の状態と合わせて FEC の振る舞いをチェックしていく。

3.11.3 実験環境

- 実験構成



- 他の実験との関連
  東芝と接続。FEC の性能評価で少々のパケットロスを期待しているので、東芝からの下りは帯域の小さい地上線 (384k) を通してもらう。→ ALTQ で制御してもらい、優先度を低くしてもらう。

3.11.4 結果

パケットの廃棄が長時間連続して発生しており、FEC で訂正できない誤りが予想よりも多かった。バースト廃棄の前後に生じる誤りに関しては、1/2 程度のパケットを誤りから救っていることが分かった。

3.11.5 考察

廃棄について最も低いプライオリティにすると、帯域を大きく使う別のコネクションが張られている間、FEC でフラグメントしたパケットがずっと廃棄され続けることになってしまい、結局、FEC の効果はほとんど発揮できなくなってしまう。全てのトラヒックが同じプライオリティの場合は、FEC にとってバースト廃棄の程度が小さくなった時間帯のみ訂正可能となった。

3.11.6　今後の課題

今回のネットワークのパケット廃棄はバースト性が高く、FEC でも訂正不可能なケースが多かった。FEC 単独ではなくルータで何らかのシステム (例えば RED) と組み合わせてみる必要がありそうだ。

3.11.7　関連情報

3.12　合宿ネットワークの成果報告書の作成

3.12.1　実験の目的

計画的に、合宿ネットワークで行われる実験の内容文書化し公開することによって、情報を共有する。ネットワーク全体の調整を円滑に進め、成果をまとめる作業を軽減する。

3.12.2　実験の概要

1. 合宿前

   各実験ごとに指定した形式に従った趣意書の提出を依頼し、公開した。実験の目的、内容の他に、必要となる環境、構築のスケジュール等、調整に必要な項目も洗い出し、また予想される結果も事前に文書化した。

   提出された趣意書に従って合宿ネットワークの構築のスケジュールを作成した。

2. 合宿中

   実験の状況、ネットワーク全体に起こるトラブル等を記録した。

3. 合宿後

   趣意書に、評価、考察等実験後に行う項目を追加し、提出を依頼した。これらを整形し、WIDE 報告書にまとめた。

3.12.3　実験環境

- 実験構成

  機材は使用しないが、情報の交換、公開にメール、Web などのツールを活用した。実験の記録にはトラブルチケットシステムを利用した。

- 他の実験との関連

  合宿ネットワーク上で行われるすべての実験に関連するメールで情報を収集し、Web チームと連携して公開を行う。

3.12.4 評価

早くから合宿ネットワーク全体での情報共有が可能となった。Web でも公開されたため、ネットワーク上で実験を行う人だけでなく、合宿参加者全員が情報を見ることができた。

合宿前に報告書の目次と書く項目を決め文書化したことで、まとめの際の作業が軽減された。

3.12.5 今後の課題

趣意書の形式を見直し、書きやすく見やすくなるよう検討する。今回はネットワーク構築に関する情報の共有と報告書の作成を目的としたが、今後は論文を書く際にも利用できる情報を文書化することも考慮する。

3.13 ネットワークトラブルチケットシステムの構築と運用

3.13.1 実験の目的

ネットワークの安定運用を目的としたトラブルチケットの導入および運用。ネットワークテストベッド運用技術の収集。

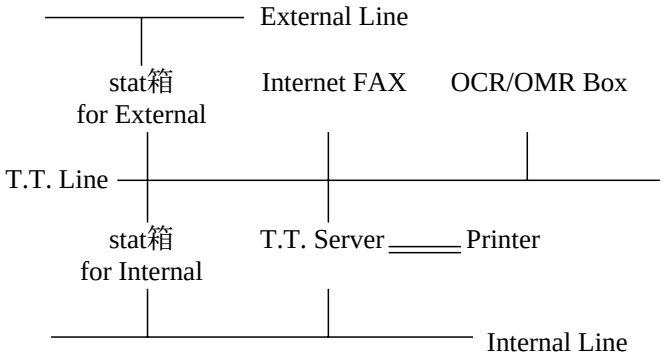
3.13.2 実験の概要

このシステムでは、ユーザからの報告に応じて、障害の分類/担当者への報告などといった処理をおこなう。

ネットワーク障害時にはネットワークを介した入力システムは実用的では無いという観点から、InternetFAX を利用した紙による入力インターフェイスを基本とする。ネットワークの利用が可能である場合には WWW の form による入力も可能とする。

3.13.3 実験環境

- ネットワーク構成



Trouble Ticket System がシステム内部での通信の為に用いるネットワークとして TT Line (private) を用意する。このネットワークを用いることで、実験ネットワークの影響を受けず安定的に動作可能な Trouble Ticket System を提供する事ができる。

3.13.4　結果

合宿前半は各実験から提出される定期レポートの収集を中心に行なわれた。この定期レポートシートは各実験の協力を得て数多く収集する事が出来、今回の実験のデータや合宿での実験の進め方などに関するノウハウが次回以降にも行かされると期待できる。

また、後半には Ticket 発行部分も部分的に完成し、Ticket の統合/分割は出来ないもののプロトタイプシステムを稼働させる事が出来た。これにより、障害の記録が発生時点から集中管理できるという体勢がとれた。

3.13.5　評価

各実験からの定期レポートが多数得られた事は、次回の合宿に生かす事が出来ると思われる。今までの合宿ネットワークでは、構築から撤収までの体系的な記録は取られておらず、今回収集できたこの記録は重要な収穫であったと確信できる。また、今回実トラフィック上で実験を行なったことにより、次回以降に実験を行なう際の課題が発見できた。

3.13.6　今後の課題

- 全実装の完成 (Log 分析／解析ツールの作成など含む)
- 入力フォーマットなどの最適化。
- 障害登録者への事後報告体系の確立。

3.13.7 関連情報

“ネットワークテストベットにおけるトラブルチケットシステムの設計と構築”. DSM 研究会. 情報処理学会, 1998.

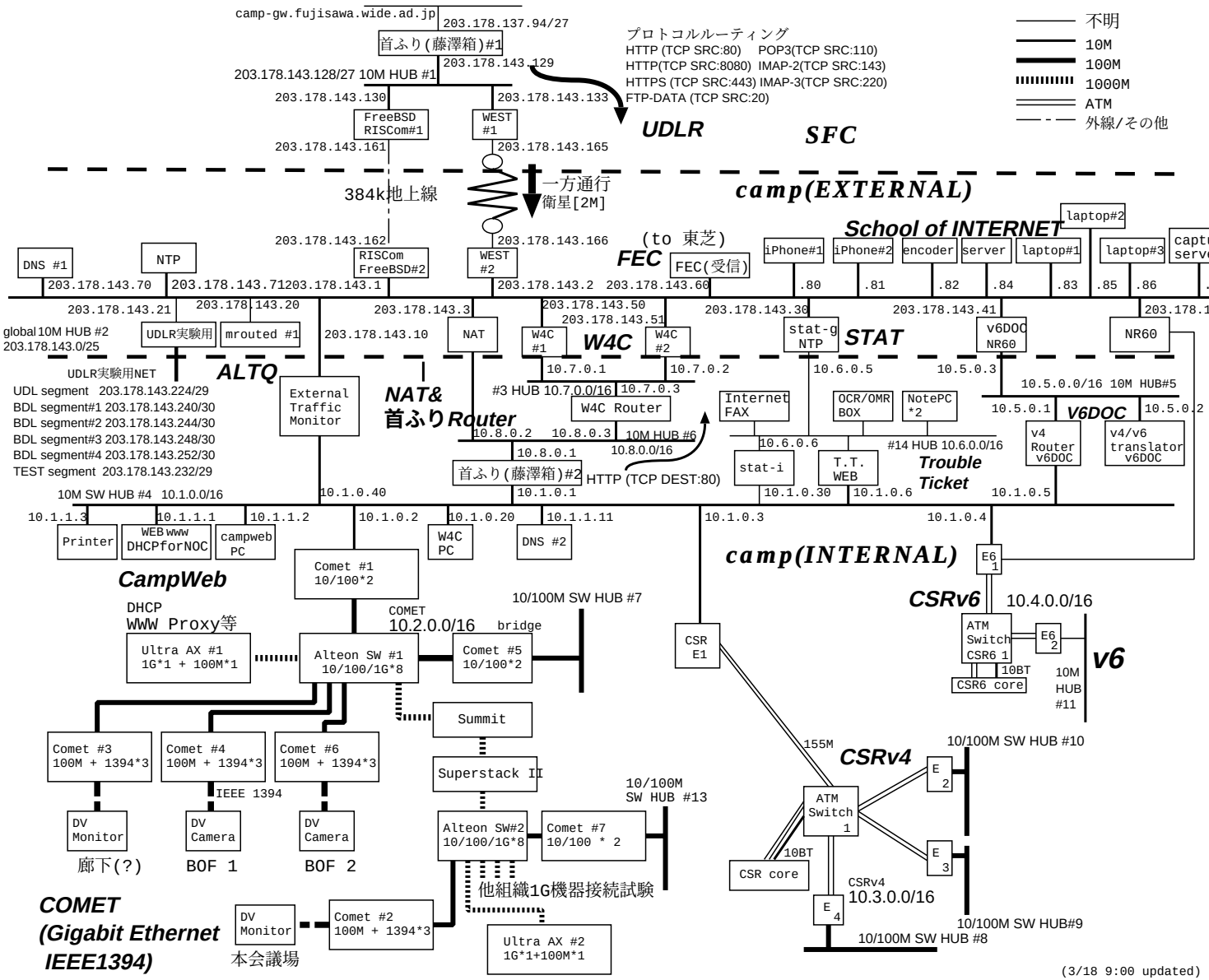


図 3.1: 98 年春の仮設ネットワーク構成図

diff
#12-> #13
cometのトポロジを大幅に変更
SOIにglobalアドレスを追加
ntpdをstat-gと統合統合
#13->#14
comet#7 の間違いを修正
#14->#15
cometの構成をくみかえ

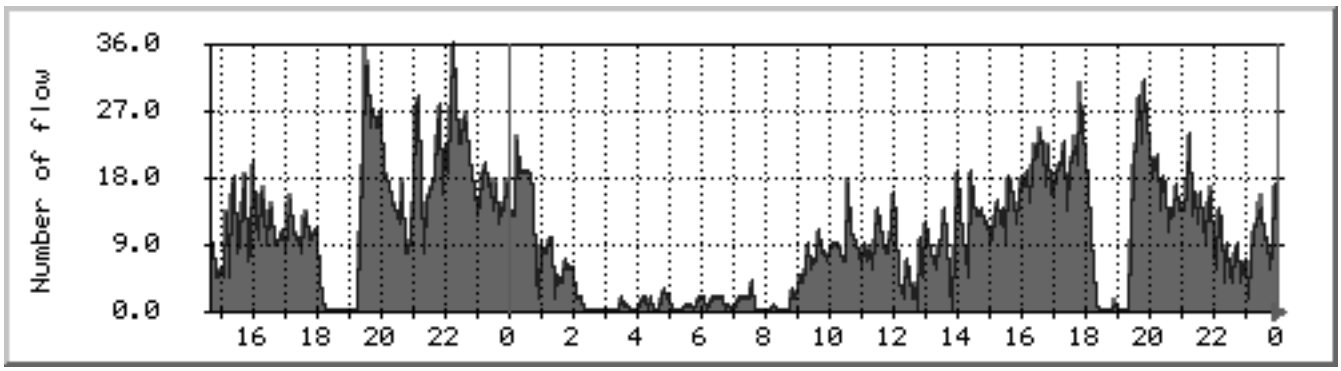


図 3.2: CSR CORE におけるカットスルーフロー数

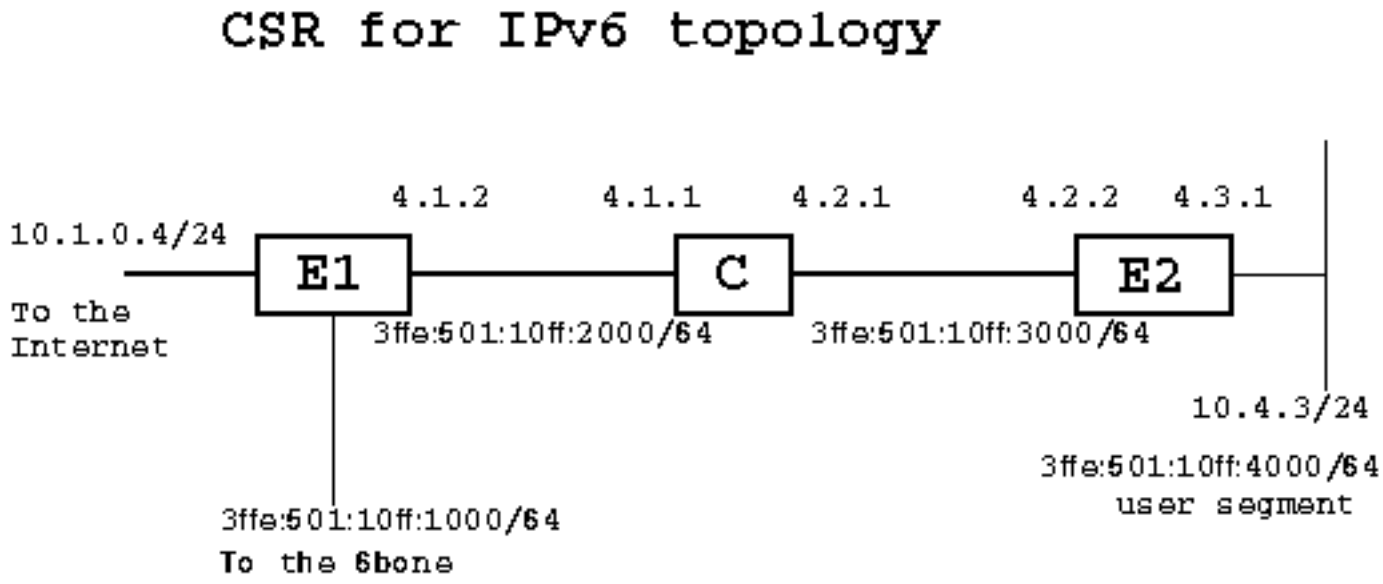


図 3.3: IPv6 CSR 実験ネットワークトポロジー

第 4 章

おわりに

本章では複数技術の相互運用および動作検証を行うためのテストベッドとなる実験ネットワークの構築について論じた。ケーススタディとして取り上げられた WIDE プロジェクトでのワークショップネットワークは、明確な方法論に基づいて構築されたネットワークではなかったこともあり、不十分な点も数多く指摘された。しかし、それ以上に大きな時間的・リソース的な制約があったにも関わらず、最先端技術の積極的な利用した大規模ネットワークを実際に構築・運用し、かつ、多数の実験結果を出すことができたことは評価に値すると思われる。

インターネットに対する安定性や信頼性への要求は今後ますます増大することが予想される。インターネットにおけるダイナミックな技術革新を維持しつつ、これらの要求も満たすためにも、今後このような実験ネットワークの設計運用技術は非常に重要となることが考えられる。

WIDE バックボーンは実運用を行いつつも様々な実験を行うことが可能な、世界で唯一のバックボーン規模実験ネットワークとして有名である。

インターネット技術開発の目標は実際のインターネット上で実運用されることである。WIDE バックボーンにおける実験およびその評価の方法論が確立されれば、現在は望むことができない規模の実験および評価を行うことが可能となり、実用化を行う上の重要なアドバンテージを期待できる。

同様に、NSPIXP シリーズに代表されるような、単一目的において構築される最先端技術評価実験を行う上での、適切なネットワーク構築手法および評価手法の確立も重要な課題である。

方法論の確立だけでなく、実運用する上でのノウハウの蓄積や、設計・運用の際の支援ツール群の整備も望まれている。

特にこのような形式のネットワークに対する測定技術についての研究や、ツール群の整備はほとんど行われていない。

また、大規模な仮設ネットワークを運用するための支援環境として、コーディネーション用の支援ツールや運用時のトラブルチケットシステムのさらなる整備が期待されている。

WIDE プロジェクトでは 1998 年 9 月、1999 年 3 月に行うワークショップにおいても実験用の仮設ネットワークを構築・運用することが予定されている。本論文で提示された方法論を適用して、その有効性を検証すると共に、運用経験を増すことで、更に一般的なノウハウを増強して実験ネットワーク構築の方法論を確立することを目指す。