

第 14 部

衛星通信によるネットワーク構築実験

第 1 章

はじめに

WISH ワーキンググループでは、インターネットにおける 1 対多型の通信を効率よく行なうため、VSAT 衛星通信局を用いた汎用のマルチキャスト型通信基盤を構築し [?], 1 対多型のプロトコルの確立とアプリケーション構築を行なっている。

また、衛星通信のもつ可搬性、地理的普遍性、動的な回線設定といった特色を活かすインターネットアーキテクチャを確立し、現実のインターネットに適用し、従来のネットワーク基盤では実現できなかった通信を行なっている。

本稿では、1996 年度における以下の研究、実験を報告する。

- 単方向リンクにおける動的経路制御
- アドレス変換技術を用いた経路制御
- 通信衛星による遠隔医療診断プロジェクト

なお、WISH ワーキンググループにおける衛星通信は、「デジタル衛星通信の大学間高度共同利用研究協議会」の実験可搬局免許を用いた (株) 日本サテライトシステムズの衛星通信回線、および (株) 日本サテライトシステムズとの随時分割契約による衛星通信専用サービスを用いて行なわれている。

第 2 章

衛星通信ネットワークを用いた単方向リンクにおける動的経路制御

2.1 はじめに

1996 年 6 月カナダのモントリオールで開かれた第 36 回 IETF において、単方向リンクにおける経路制御 (Unidirectional Link Routing: UDLR) に関する BoF が開かれた。

UDLR BoF でのテーマは、これまで WISH ワーキンググループが取り組んできたような、衛星ネットワークを単方向ネットワークとして使用した場合の経路制御の問題である。WISH ワーキンググループでも問題解決に向けた提案を行なっている。

UDLR BoF は、12 月のアメリカ サンノゼにおいて開かれた第 37 回 IETF において IETF Working Group へ発展し、1997 年度以降も活動が続いている。

本章では、IETF UDLR Working Group における議論を簡単にまとめ、WIDE プロジェクトが提案する方法について述べる。

2.2 経路制御プロトコル拡張方式とトンネリング方式

UDLR の解決に向けて、大きく分けて 2 つの方式が提案されている。一方は既存の経路制御プロトコルを拡張する方法で、もう一方は IP トンネリング機構を用いることによって経路制御プロトコルを変更することなく動作させる方法である。前者はフランス INRIA が提案し、後者は WIDE プロジェクトとアメリカ ヒューズ社が各々に提案している。

プロトコル拡張方式では、RIP[?]、OSPF[?] そしてマルチキャスト経路制御プロトコル DVMRP[?] といった各経路制御プロトコル毎に単方向リンク (Unidirectional Link: UDL) に対応する拡張を行う必要がある。OSPF のようなリンク状態型経路制御プロトコルでは、全てのルータが同一アルゴリズムに従って動作しなければならないため移行に伴う問題がある。

その点、トンネリング方式は単方向リンクと双方向リンク (Bidirectional Link: BDL) を統合し IP トンネリング技術を加えることで仮想的に Feed(衛星ネットワークを通じてパケットを送受信できる) と Receiver(衛星ネットワークを通じてパケットの受信のみができ

るノード、複数の設置が可能) 間をそれぞれ隣接ノードに見せかける。これにより多くの既存の経路制御プロトコルが拡張を加えることなく動作することを目的としている。また、Feed と各 Receiver にのみトンネリング機構を組み込めばすむので移行しやすい。

2.3 WIDE プロジェクトが提案するトンネリング方式

2.3.1 設計

本設計の最も重要な方針は、既存の経路制御プロトコルに手を加えずに動作させることである。

既存の経路制御プロトコルは1つのインターフェースで隣接ノードと双方向に通信できることを前提としているので単方向リンクと双方向リンクを使い分ける仮想インターフェースを用い、そのまま既存の経路制御プロトコルを動作させる方式を提案した。

これを実現するために、図 2.1 のような仮想ネットワークインターフェースを設計した。

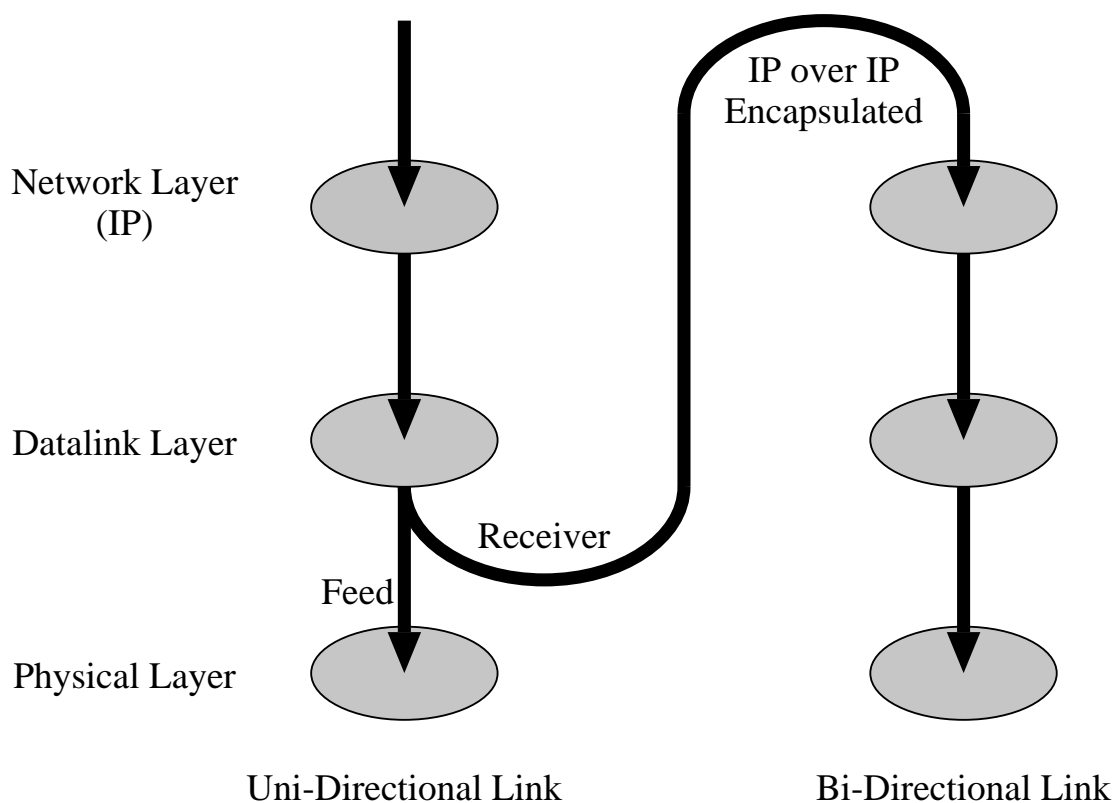


図 2.1: 仮想ネットワークインターフェース

Feed から Receiver へのパケットは、Feed から何も変更されずに udl ネットワークへ投

げられ Receivers へ届く。逆に、reciever から Feed へのパケットは、reciever で IP over IP [?] パケットにカプセル化され BDL ネットワークを通じて Feed へ送る。Feed では IP パケットを脱カプセル化して取り出す。

このような機構を用いて、Feed と Receiver 間で UDL を利用した双方向通信ができる。

2.3.2 実装

IP within IP パケットへのカプセル化の仕組みについて述べながら仮想インターフェースの実装について詳述する。

Receiver から Feed へのパスを、トンネリングを用いることによってあたかも隣接しているように見せるには、Receiver、Feed が自分の BDL と UDL の IP アドレス、相手の BDL と UDL の IP アドレスを知らなければならない。自分のアドレスについては管理者によって設定されるため明らかであるが、相手のアドレスを知る仕組みが必要となる。

現在の実装では相手のアドレスは静的に設定することによってこの問題を省いているが、2.3.4節で述べる動的なトンネリング形成機構を用いることで動的に相手のアドレスがわかる。

Feed と Receiver でそれぞれ相手の BDL ネットワークアドレスと UDL ネットワークアドレスがわかると、相手の (UDL ネットワークアドレス, BDL ネットワークアドレス) の組をカーネルに保持して UDL のネットワークインターフェースを設定する。

図 2.2 に示すネットワーク構成において動作例を示す。

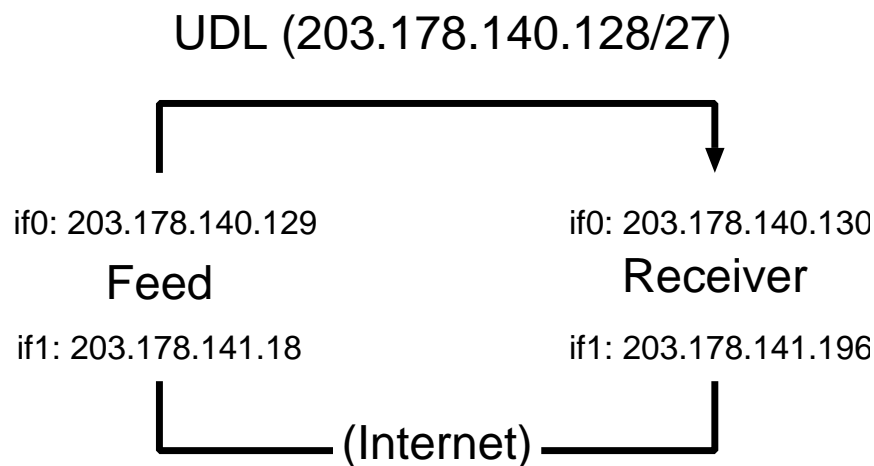


図 2.2: ネットワーク構成の例

Feed での UDL ネットワークインターフェース if0 は、
UDL IP アドレス ネットマスク
203.178.140.129 0xffffffe0

として設定され同時に、
BDL IP アドレス
203.178.141.18

と

相手の UDL IP アドレス 相手の BDL IP アドレス
203.178.140.130 203.178.141.196

の組を保持し、Feed を示すフラグをセットする。(相手の UDL IP アドレス, 相手の BDL IP アドレス) の組は Receiver の数に応じて用意される。

Receiver でも if0 は同様に
UDL IP アドレス ネットマスク
203.178.140.130 0xfffffe0

として設定され同時に、
BDL IP アドレス
203.178.141.196

と

相手の UDL IP アドレス 相手の BDL IP アドレス
203.178.140.129 203.178.141.18

の組を保持する。

2.3.3 経路制御プロトコルの動作

経路制御プロトコルとして OSPF、経路制御プログラムとして gated を用いた場合の構成について述べる。

Feed から Receiver への通信は実際に UDL が用いられる。Feed 側の gated.conf で if0 のコストを地上ネットワークを経由する経路よりも低いものを設定すればインターネットのパスとして UDL を優先する経路制御を行なえる。

逆に、Receiver から Feed への通信はいくつかのネットワークから構成される地上ネットワークを通るが、IP over IP トンネルを用いるためオーバーヘッドが生じインターネットのパスとしてなるべく利用しない方がよい。従って、Receiver 側の gated.conf において if0 のコストを地上ネットワークを通るコストよりも高く設定し、経路制御プロトコルに関連したパケット以外はトンネルネットワークを通過しないよう設定できる。

経路制御プロトコルとして RIP を用いる場合には、Receiver から Feed へ経路情報を流さないこともできる。

2.3.4 動的なトンネリング形成機構

- Feed は定期的に自分の (UDL IP アドレス, BDL IP アドレス) を送る
- 新たにネットワークに加わった Receiver がそのパケットを受け取ると自分の (UDL IP アドレス, BDL IP アドレス) を Feed に送り返す

- Feed、Receiver はそれぞれ相手の (UDL IP アドレス, BDL IP アドレス) が分かったのでトンネリングの設定を行う

2.3.5 まとめ

- 利点
 - インターネット全体に手を加える必要がなく、Feed、Receiver だけを変更すればよい。
 - 経路制御プロトコル毎に、それぞれを拡張する必要がない
- 欠点
 - Feed、Receiver はそれぞれ互いの BDL IP アドレスを知らないとトンネリングを用いることが出来ない。この問題の解決には、2.3.4節で前述したトンネリング形成機構で対応する。
 - Receiver から Feed への経路情報はオーバーヘッドの伴うトンネリングネットワークを通過する。しかし、経路情報に関するパケットだけなのでさほど大きな問題ではないと考えられる。

第 3 章

衛星回線と地上回線の統合利用のためのアドレス変換機構の研究

3.1 概要

衛星回線をインターネットの接続に使う場合、双方向通信路として用いる場合と、片方向通信路として用いる場合の 2 つの形態がある。特に、一般家庭や小規模事務所での衛星回線の利用を考える場合、後者の形態でも利用できることが望ましい。

従来のインターネットにおける経路制御は、通信路が双方向であることを前提に設計されている。これを、片方向通信路である衛星回線が経路に含まれるネットワークにそのまま用いた場合、経路制御に問題が発生する。本研究は、この問題をアドレス変換技術を用いて解決する手法を述べる。

また衛星回線は、広範囲に散らばった複数の地点で、同時に、ほぼ同一の品質で受信できるので、広域同報型のネットワークとしての利用に適している。反面、衛星の数や電波の周波数資源に限りがあるため、地上の有線回線よりも帯域拡大が難しい。このため、衛星回線の帯域を有効に使用することが必要である。衛星回線における経路制御は、衛星回線を経由すべきデータと地上回線を経由すべきデータを選択的に制御する技術が必要である。本研究は、この問題についても、解決する手法を述べる。

また、多数のエンドノードが接続されているネットワークを衛星回線及び地上回線に接続した場合、上記のアドレス変換技術を用いた解決法では、大量の IP アドレスを必要とし、現実的ではない。この問題に対処するため、IP Masquerading を用いて IP アドレスを節約する手法を述べる。

3.2 問題点と解決法

3.2.1 経路制御の問題

衛星回線と地上回線を持つネットワークの典型例として、図 3.1 のようなネットワークを考える。

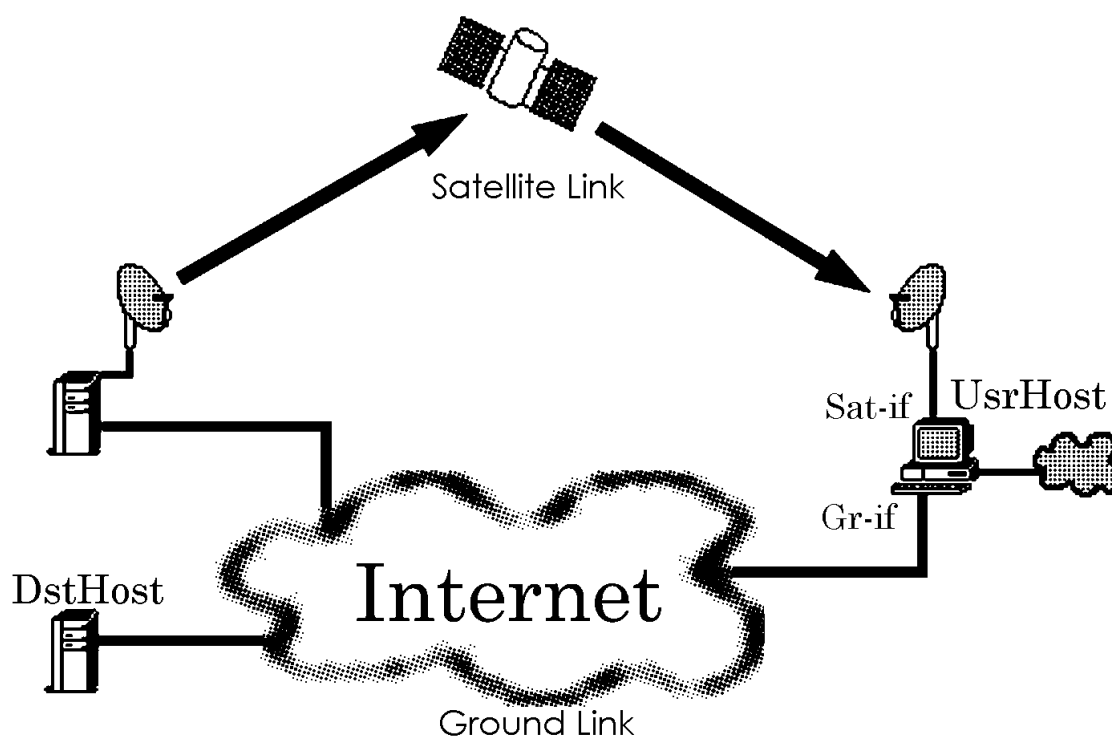


図 3.1: 衛星回線を含むネットワークポロジの例

ユーザのネットワークあるいはホスト (以下 UserHost と略す) がインターネット上の任意のホスト (以下 DstHost と略す) と通信する場合を考える。

UserHost は 2 つのインターフェースを持ち、1 つはダイヤルアップ等の地上回線 (Gr-if)、もう 1 つは受信専用の衛星回線 (Sat-if) である。

UserHost が DstHost と通信する場合、UserHost はパケットを Gr-if より送出する。このとき、送出されるパケットに付与されるアドレスは、以下のようになる。

Source Address : UserHost Gr-if Address
 Destination Address : DstHost Address

インターネット上のルータは送出パケットの Destination Address によって経路を決定するので、送出パケットは DstHost に到達する。DstHost は返信する際に、UserHost が送出したパケットの Source Address を Destination Address としてパケットを送出するので、返信されるパケットに付与されるアドレスは、次のようになる。

Source Address : DstHost Address
 Destination Address : UserHost Gr-if Address

このパケットの経路は、Destination Address によって決定されるので、地上回線を経由し、UserHost の Gr-if から受信される。

結果として、衛星回線は、存在するにも関わらず使用されない。

この問題点と解決法を、図 3.2 に示す。

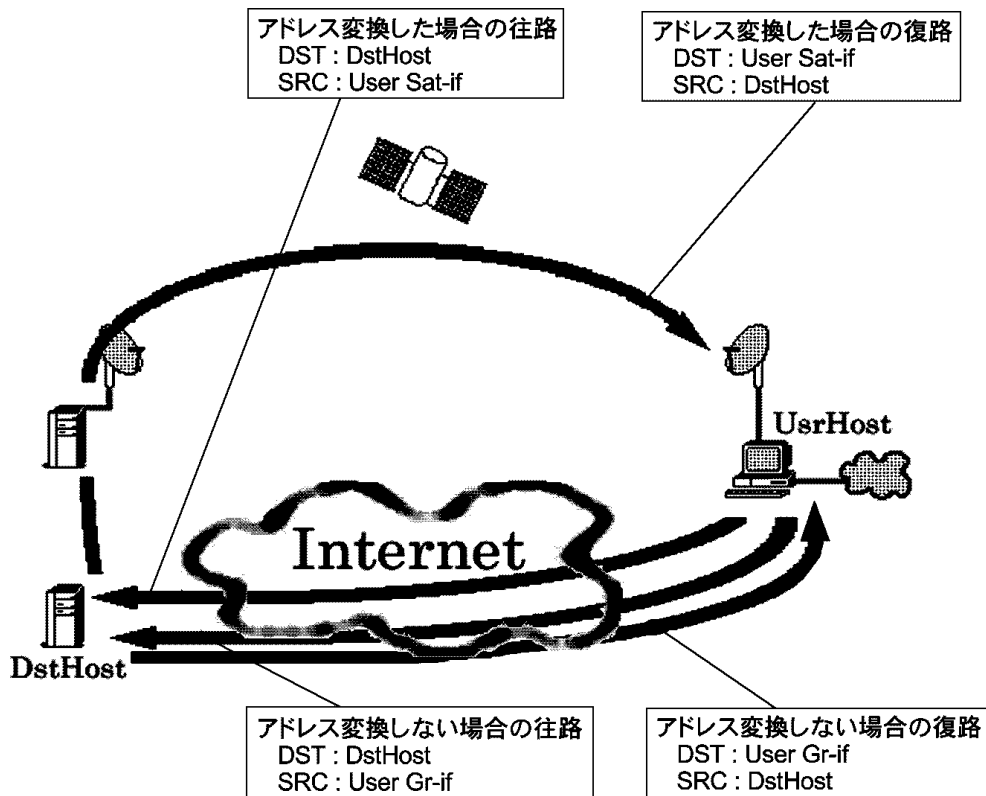


図 3.2: 経路制御の問題の解決法

図 3.2 において、DstHost から UserHost への経路が衛星回線を経由するように、UserHost がパケットを送出するときに、Source Address を UserHost Sat-if Address へ書き換える。こうすることによって、復路は衛星回線を経由する。

3.2.2 選択的経路制御の問題

3.2.1 節の手法を用いて、衛星回線への経路制御を行なった場合、衛星回線が存在する場合にはすべてのパケットが衛星回線を経由する。

衛星回線はその広域性を活かして、地理的に非常に広範囲に散らばるネットワーク、ホストを一度にカバーする。そのため、1 つの衛星回線に接続されるエンドノードの数は膨

大なものになる。それらがすべてのパケットを衛星回線を経由させて通信した場合、容易に衛星回線の容量を超過すると考えられ、前述の手法だけでは大規模性の点から現実的ではない。

このため、衛星回線は、特定のホストから発信されたパケットや、特定のホストから返信されるパケット等に限定して使用されることが望ましい。あるサーバのあるサービスは衛星回線経由、その他は地上回線経由、というように、選択的に衛星回線を使用する仕組みが必要である。

特定のホストとの通信時にだけ衛星回線を経由するようにするため、UserHost がパケットの Source Address を書き換える時に、Destination Address が特定のホストであった場合には Sat-if Address へ、それ以外の場合は Gr-if Address へ書き換える。こうすることで、特定のホストとの通信時にだけ、復路が衛星回線を経由する。

3.2.3 IP アドレスの節約

アドレス変換技術は本来、インターネット上で一意でないプライベートアドレスが振られたネットワークをインターネットに接続するために、プライベートネットワーク上の個々のアドレスとグローバルなアドレスを 1 対 1 対応で相互変換する技術である。

本研究で開発した技術では、プライベートネットワークのアドレスをグローバルな衛星回線ネットワークのアドレス、または地上回線ネットワークのアドレスに 1 対 1 対応で書き換える。この場合 IP アドレスは、ユーザのネットワークに接続されるホスト数の 2 倍 (地上回線に割り当てるアドレスと、衛星回線に割り当てるアドレス) 必要になる。

現在、IP アドレスの枯渇が問題になっており、1つのネットワークに対して2倍のIPアドレスが必要な前述の手法は、アドレス数の観点から現実的でない。

このため、IP Masquading 技術を用いて、必要なアドレス数を少なくすることが望まれる。これにより、複数のホストを持つネットワークを接続した場合でも、必要なIPアドレスは衛星+地上の2つで済み、IPアドレス数の節約になる。

3.2.4 アドレス変換機構の実装

3.2節に基づき、衛星回線用アドレス変換機構を実装し、諸問題を解決するための実験を行なった。

実験に際し、図3.3のような実験ネットワークを構築した。

ネットワークは、次の各部によって構成される。

- ネットワーク
 - プライベートネットワーク
 - 地上回線をエミュレーションするリンク
 - 衛星回線をエミュレーションするリンク

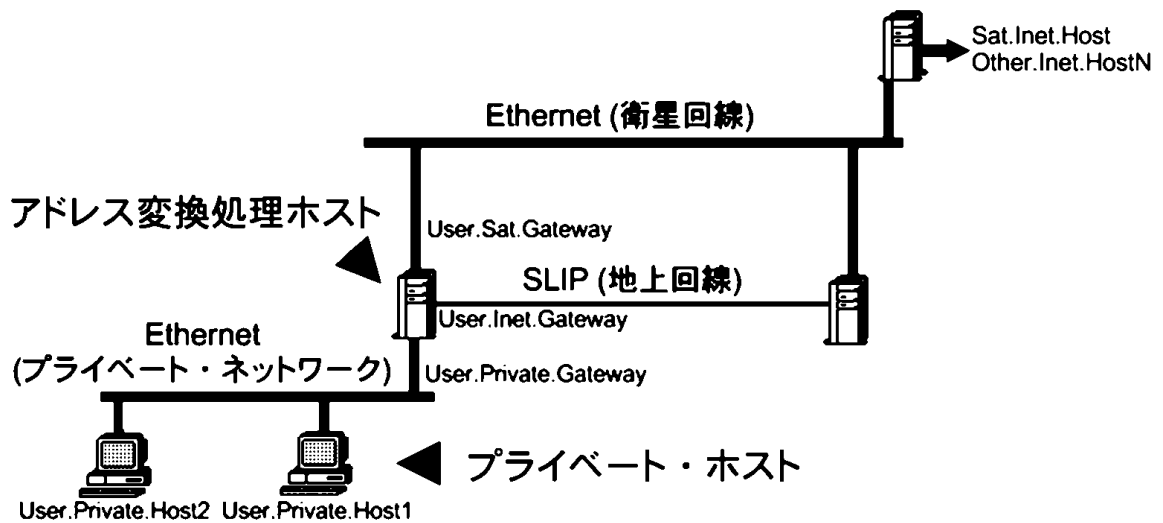


図 3.3: アドレス変換機構実験ネットワークポロジ－図

- 外部のネットワーク
- ホスト
 - プライベートホスト
 - アドレス変換処理ホスト
 - プライベートネットワークと外部の地上回線を接続するホスト
 - 衛星回線を経由するサービスを提供するホスト (衛星サービス提供ホスト)
 - その他のインターネット上のホスト

図 3.3において、各ホストのインターフェースには 3.1のアドレスが振られているものとする。

図 3.3において、各ホストの OS は表 3.2の通りである。

アドレス変換機能並びに IP Masquading 機能は、IP 層に実装した。書き換えるアドレスによって、2つのルーチンに分けて実装した。

| | | |
|-------------------|---------|----------------------|
| プライベートネットワーク上のホスト | | User.Private.HostN |
| アドレス変換処理ホスト | 衛星回線リンク | User.Sat.Gateway |
| | 地上回線リンク | User.Inet.Gateway |
| プライベートネットワークへのリンク | | User.Private.Gateway |
| インターネット上の任意のホスト | | Any.Inet.HostN |
| 衛星サービス提供ホスト | | Sat.Inet.HostN |
| その他のサービス提供ホスト | | Other.Inet.HostN |

表 3.1: 実験ネットワーク・アドレス表

| | |
|-------------|---------------------------------------|
| プライベートホスト | FreeBSD 2.1.5R 及び Microsoft Windows95 |
| アドレス変換処理ホスト | BSD/OS 2.1 |
| ISP ルータ | FreeBSD 2.1.5R |

表 3.2: 各ホストの OS

- ip_input ルーチンにおける実装

ip_input ルーチンには、下記の機能を実装した。

- プライベートホストへのアドレス並びにポート番号の変換
- アドレス変換処理ホスト地上回線インターフェースへのアドレス変換

- ip_output ルーチンにおける実装

ip_output ルーチンには、下記の機能を実装した。

- 衛星サービスホスト一覧からの検索 Destination Address が衛星サービスホストであれば、次の処理を実行する。
- アドレス変換処理ホスト衛星回線インターフェースへのアドレス並びにポート番号変換
- アドレス変換処理ホスト衛星回線インターフェースへのアドレス変換
- Destination Address がその他のサービスホストであれば、以下の処理を実行する。
- アドレス変換処理ホスト地上回線インターフェースへのアドレス並びにポート番号変換

3.3 衛星回線用アドレス変換機構の実装

3.2で述べた問題点を解決する手法として設計実装したアドレス変換機構の詳細を述べる。

3.3.1 衛星回線経由の経路制御

プライベートネットワークから送出されるパケットを衛星回線へ経由させるため、以下のようにアドレス変換を行なう。また、2つのIPアドレスで複数のプライベートネットワーク上のホストが通信できるように、ポート番号の変換を同時に行う。

```
送出時 SRC : User.Private.HostN(Port) → User.Sat.Gateway(Port+n)
        DST : Any.Inet.HostN           (書き換えなし)
受信時 SRC : Any.Inet.HostN           (書き換えなし)
        DST : User.Sat.Gateway(Port+n) → User.Private.HostN(Port)
```

アドレス変換処理ホストから送出されるパケットを衛星回線へ経由させるため、以下のようにアドレス変換を行う。

```
送出時 SRC : User.Inet.Gateway(Port) → User.Sat.Gateway(Port)
        DST : Any.Inet.HostN         (書き換えなし)
受信時 SRC : Any.Inet.HostN         (書き換えなし)
        DST : User.Sat.Gateway(Port) → User.Inet.Gateway(Port)
```

パケットは、ともに User.Inet.Gateway のインターフェースより外部に向かって送出される。

この結果、パケットは次のようにネットワークを通過する。

1. 往路

- (a) プライベートネットワークのホストから送出されたパケットは、アドレス変換処理ホストによって前述の規則に従いアドレスを変換される。
- (b) パケットの Destination Address により、インターネットの各ルータはパケットを地上回線経由で目的のホストへ配送する。

2. 復路

- (a) 目的ホストは、受信パケットの Source Address を 送出パケットの Destination Address に入れて返信する。
- (b) パケットの Destination Address により、インターネットの各ルータはパケットを衛星回線経由でアドレス変換処理ホストへ配送する。

- (c) アドレス変換処理ホストは、前述の規則に従って受信パケットのアドレスを変換する。
- (d) アドレス変換後の Destination Address に従い、各々の発信元へパケットは配送される。

3.3.2 選択的経路制御

プライベートネットワークから送出されるパケットが、衛星サービス提供ホストとの通信時にだけ衛星回線を経由するように、次のようにアドレス変換するかどうかを選択する。

1. アドレス変換処理ホストは、次のような衛星サービスを提供するホストの一覧を持つ。

| Satellite Services Address |
|----------------------------|
| Sat.Inet.Host1 |
| Sat.Inet.Host2 |
| ⋮ |
| Sat.Inet.HostN |

2. アドレス変換処理ホストは、送出されるパケットの Destination Address を衛星サービスホストの一覧から検索する。
 - Destination Address が衛星サービスホストである場合
3.3.1で述べた手順に従ってアドレスを変換する。
 - Destination Address が衛星サービスホストでない場合
プライベートホストから送出されるパケットは、3.3.1で述べた User.Sat.Gateway の代わりに、User.Inet.Gateway に変換し、ポート番号を変換し送出される。また、アドレス変換処理ホストから送出されるパケットは、アドレス変換を行わない。
3. プライベートネットワーク上のホスト、アドレス変換処理ホストから送出されるパケットは、ともに User.Inet.Gateway のインターフェースから外部に向かって送出される。

この結果、パケットは次のようにネットワークを通過する。

- Destination Address が衛星サービスホストである場合
衛星回線を経由してパケットが返信される。
- Destination Address がその他のサービスホストである場合
地上回線を経由してパケットが返信される。

3.4 評価

3.4.1 アドレス変換技術を用いることの優位性

前述の諸問題に関する解決へのアプローチとしてアドレス変換技術の他に、第 2 章で報告したように、IP トンネリングを用いて経路情報を配布するもの、経路制御プロトコルに変更を加えるものが提案されている。

それらの解決法と比較して、アドレス変換技術を用いた解決法が勝っている点は、以下の通りである。

- ルーティングプロトコルに変更を加える方法と比べ、ネットワークに対する特別な変更は、ユーザのネットワークにあるアドレス変換処理を行うホストに対してのみでよく、実装が容易である。
- IP トンネリングを用いる方法と比べ、大規模性がある。
- 経由する経路に選択性がある。
- 衛星回線だけではなく、他の片方向通信路にも応用可能である。

3.4.2 プロトコル/アプリケーションによる通信の可否

アドレス変換技術の使用により、プライベートホストからの通信は、プロトコルによって制約を受ける。

この実験では、表 3.3 のように、プロトコル/アプリケーションによる通信の可否を確認した。

| | |
|-------|--------------------------|
| 通信可能 | telnet , nslookup , http |
| 通信不可能 | icmp, ftp |

表 3.3: プロトコル/アプリケーションによる通信の可否

上記の通信不可能のもののうち、ftp はコントロールコネクションに IP アドレスをアスキーコードで書き込んで通信している [?] ので、そのアドレスと IP ヘッダのアドレスが異なることが原因である。

icmp については、icmp パケットが上位層のポート番号を含んでいないため、返却すべきプライベートホストを特定できないのが原因である。

