論　文

単一方向衛星回線を含むネットワークの為のアドレス変換機構を用いたネットワークアーキテクチャ

西田　視磨[†]　　楠本　博之[†]　　村井　純[†]

Network Architecture using network address translation mechanism for network with unidirectional links

Mikiyo NISHIDA[†], Hiroyuki KUSUMOTO[†], and Jun MURAI[†]

あらまし
本論文では，広域単一方向の通信媒体である衛星通信と，双方向通信媒体である地上網を用い，非対称なトラフィック傾向を示す利用における有効なネットワークアーキテクチャを提案し実装した．単一方向の通信路は，既存のインターネットの経路制御アーキテクチャと親和性が低く，既存の経路制御技術では衛星通信のような広帯域の単一方向通信路を活かせない．本研究では，ネットワークアドレス変換機構を用いて，データ送信を要求する側が衛星通信路と地上網の複数のネットワークアドレスを使い分けて要求を送信側に送り，単一方向リンクを既存のインターネットの経路に統合し利用できるアーキテクチャを示した．さらに，ネットワークアドレス変換機構を実装し，実際の衛星通信路を用いた実験とLAN環境におけるシミュレーションを用いてその有効性を示した．現在，一般家庭や小規模事務所等におけるインターネットの利用は増大しており，そのトラフィック傾向は，利用者から外部ネットワークへ向かう通信よりも外部ネットワークからの情報獲得の通信が多くを占める．本アーキテクチャにより，このトラフィック傾向に適した通信路として広域の放送型通信媒体である衛星通信路を構築できる．

キーワード　インターネット，単一方向通信路，経路制御，衛星通信

1. 概　　要

一般家庭や小規模事務所などにおける使用者とインターネットを接続する通信路は，ISDN回線やモデムが一般的である．しかしこれらの接続方法は，帯域が狭く常時接続ではない欠点がある．また，広帯域常時接続を行う高速専用線接続は高価で，個人などでこれを持つのは難しい．一方，現在のインターネットのトラフィック傾向には，次のような顕著な特徴が見られる．使用者から外部のネットワークへ向かう「往路」のトラフィック量は少なく，逆に外部のネットワークから個人使用者へ向かう「復路」のトラフィックは非常に多い．従来の電話回線や専用線は，双方向の帯域が対称であり，このトラフィック傾向には適さない．このトラフィック傾向に適合する通信路として，地上網と単一方向通信路との組み合わせによる非対称のネットワークが考えられる．しかし，受信のみを行う単一方向の通信路を含むネットワークをインターネットへ接続する場合には，従来のインターネットにおける技術では解決できない問題が発生する．

単一方向の通信路をインターネット上で用いる際に発生する問題として，経路制御の問題がある．従来のインターネットにおける経路制御技術は，通信路の双方向性を前提にして設計されている．インターネットにおける経路制御は，経路情報を相互に交換することが基本となっている．単一方向の通信路では，受信側から発信側への経路情報の伝達ができないため，通信路が使用されない．単一方向の通信路を使用したネットワークを構築するには，この経路が使用されるような仕組みが必要である．

また，大規模性の問題も発生する．単一方向の通信媒体の例として，衛星回線やケーブルテレビ網が挙げられるが，これらは一つの通信路に非常に多くのノード

[†] 慶應義塾大学環境情報学部，神奈川県
Environmental Information, Keio University, 5322 Fujisawa-shi, Kanagawa, 252 Japan

表1　受信側ネットワークの分類
Table 1　Classification of receiving network.

タイプ	受信側ホスト数	受信側ホストに付与されるアドレス
1	単一	
2	複数	地上ネットワーク
3	複数	衛星ネットワーク

が接続される．このため，多数のノードが一つの通信路を共用するトポロジーが構築される．この通信路では発信側，受信側の双方で使用を限定したり使用の可否を選択するといった使用上の工夫が必要である．

これらを解決するために現在までに提案されている方法には，IP トンネリングを用いて単一方向通信路の復路に当たる接続性を仮想的に実現し経路情報を配布するもの [1]，経路制御プロトコルを変更して衛星回線への経路制御を行うもの [2] がある．しかし，これらの方法で前述の問題点を解決する場合，それぞれに欠点がある．IP トンネリングを用いる方法では，多数の受信側ネットワークに対して個々にトンネルを設定する必要があり，大規模性を欠く．経路制御プロトコルを変更する方法では，インターネット上の全てのルータにおいて，変更された経路制御プロトコルが動作していなければならない．インターネット上のルータの数は莫大であり，これら全ての経路制御プロトコルに改変を加えることは，非常にコストが高く，変更にも長い期間が必要である．本論文では，この問題を解決するためにアドレス変換技術 [3] を用いて経路を選択的に使用する手法を述べる．その動作原理を述べ，またその実装として，衛星回線を含むネットワークにおいての動作例と，単一方向の通信路を含むネットワークをシミュレートするネットワークを LAN 上で構築し実測した性能を示す．

2.では，単一方向の通信路をインターネットで使用する際の経路制御の問題について論ずる．3.では，アドレス変換技術を用いて経路制御の問題を解決する手法，選択的に衛星回線を使用する手法について述べる．4.では，アドレス変換技術を使用する際に問題となる IP Spoofing 防止機構との共用について述べる．5.では，この実装について述べる．6.では，性能評価について述べる．7.では，本論文のまとめについて述べる．

2. 単一方向通信路を含むネットワークにおける経路制御の問題

まず，単一方向の衛星回線を含むネットワークのトポロジーについて考える．

衛星回線は，衛星から中継される電波を受信できる範囲の全ての受信局が受信する．ここで言う受信局とは，衛星回線の受信設備を持つホストを指す．一つの電波の受信可能な地域は非常に広範囲にわたる．このため衛星回線は，広い地域に非常に多数の局が存在する．また，使用する電波の周波数資源には限りがあるので，衛星回線として設定できる回線数には物理的な上限が存在する．地上回線では，帯域を拡大するためには新たに物理的な回線を設置すればよいが，衛星回線はこのような無制限な帯域の拡大は不可能である．回線の設置には発信設備と受信設備が必要であるが，発信のための設備は受信設備と比較して非常に高価であるので，１つの発信局に対する受信局は複数存在するほうが効率がよい．

以上から，衛星回線は少数の送信局と多数の受信局を持つ形態をとることが現実的である．受信側ネットワークは，受信局単独あるいは他のホストととから構成されるネットワークである．受信側ネットワークを構成するホストを，受信側ホストと呼ぶ．少数の発信局はインターネット上で衛星回線を使用したサービスを提供する発信専用のホストとなる．この形態での使用では，データの流れは発信局から受信側ネットワークへの一方通行となる．

受信側ネットワークから外部のネットワークへの通信には，衛星回線は受信専用なので使用できない．そのため，使用者からの発信には従来の地上回線を使用する．従って衛星回線を使用するネットワークのトポロジーは，図 1のように少数の発信局と多数の受信側ネットワークを片方向の通信路で結び，受信側ネットワークが地上回線への接続を別個に持つ形態になる．

図 1の受信側ネットワークのトポロジーについて考える．受信側ネットワークは，受信側ネットワークに属するホストの数，各ホストに付与されたアドレスの種類によって，3 つに分類される．この分類を表 1に示す．

受信側ネットワークでは，衛星回線からの通信を受信するためのインターフェースと，地上回線へ接続するインターフェースの 2 つを持つ．それぞれのインターフェースには，インターネット上で一意に識別可能なネットワークのアドレスが個別に与えられる．これらのインターフェースおよびアドレスのうち，衛星回線に接続するものを衛星インターフェースおよび衛星側アドレス，地上回線に接続するものを地上イン

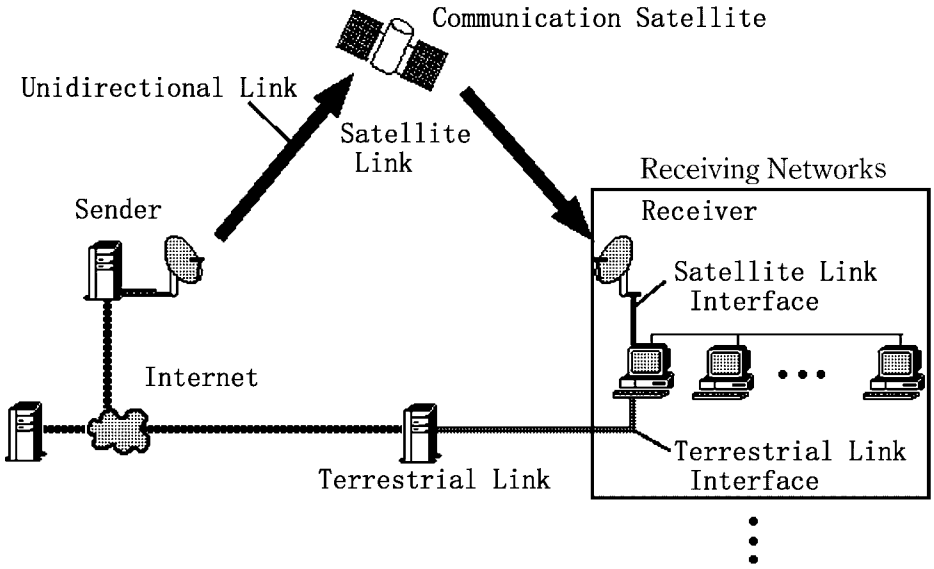

図1　衛星回線と地上回線を融合したトポロジーの図
Fig. 1　The topology of satellte and ground links.

表2　アドレス変換における受信側ネットワークの分類
Table 2　Classification of receiving network using NAT.

タイプ	受信側ホスト数	各インターフェースを持つホスト	受信側ホストに付与されるアドレス
1	単一	同一	
2	複数	同一	地上ネットワーク
3	複数	同一	衛星ネットワーク
4	複数	同一	プライベート・ネットワーク
5	複数	異なる	地上ネットワーク
6	複数	異なる	衛星ネットワーク
7	複数	異なる	プライベート・ネットワーク

ターフェース及び地上側アドレスと呼ぶ．受信側ネットワークと接続されている外部のネットワークのうち，地上インターフェースの接続しているものを地上ネットワーク，衛星インターフェースの接続しているものを衛星ネットワークと呼ぶ．

タイプ 1 の場合の経路制御を考える．受信側ホストから外部のネットワークへ送出されるパケットは地上インターフェースから送出されるので，発信元アドレスとして地上インターフェースのアドレスが付与される．このパケットは，地上回線を通り，宛先ホストへと配送される．宛先ホストからの返信パケットの Destination Address は，受信したパケットの Source Address，すなわち受信側ホストの地上インターフェースのアドレスとなる．インターネットの経路は，パケットの宛先アドレスに基づいて決定されるので，この場合の通信は衛星回線を使用しない．

タイプ 2 の場合の経路制御を考える．この場合の受信側ネットワークから送出されるパケットのアドレスは地上側のネットワークのアドレスとなる．経路はパケットに付与されたアドレスに基づいて制御されるので，この場合の通信は衛星回線を使用しない．

タイプ 3 の場合の経路制御を考える．この場合の受信側ネットワークから送出されるパケットのアドレスは衛星側のネットワークのアドレスとなるので，宛先ホストからの復路には衛星回線が使用される．しかし，地上インターフェースを持つホストの通信では，前述のホストが 1 台の場合と同様に，衛星回線を使用しない．

この 3 つの場合に関して，受信側ネットワーク上のホストに付与されたアドレスの種類にかかわらず，受信側ネットワーク上の全てのホストと外部のネットワークとの通信に衛星回線が使用されればよい．

表3 通常の送出パケットのアドレス(1)
Table 3 Addresses of normal sending packet.(1)

Source Address	UserHost Gr-if Address
Destination Address	DstHost Address

表4 アドレス書換時の送出パケットのアドレス(1)
Table 4 Addresses of sending packet that translated.(1)

Source Address	UserHost Sat-if Address
Destination Address	DstHost Address

表5 アドレス書換時の返信パケットのアドレス(1)
Table 5 Addresses of replying packet that translated.(1)

Source Address	DstHost Address
Destination Address	UserHost Sat-if Address

表6 通常の返信パケットのアドレス(1)
Table 6 Addresses of normal replying packet.(1)

Source Address	DstHost Address
Destination Address	UserHost Gr-if Address

表7 通常の送出パケットに付与されるアドレス(2)
Table 7 Addresses of normal sending packet.(2)

Source Address	UserHost-Gr Address
Destination Address	DstHost Address

表8 アドレス書換時の送出パケットのアドレス(2)
Table 8 Addresses of sending packet that translated.(2)

Source Address	UserHost-Sat Address
Destination Address	DstHost Address

表9 アドレス書換時の返信パケットのアドレス(2)
Table 9 Addresses of normal replying packet.(2)

Source Address	DstHost Address
Destination Address	UserHost-Sat Address

表10 通常の返信パケットのアドレス(2)
Table 10 Addresses of normal replying packet.(2)

Source Address	DstHost Address
Destination Address	UserHost-Gr Address

3. アドレス変換機構による衛星回線への選択的経路制御

3.1 アドレス変換の動作

2.で論じた経路制御の問題を解決するために，Source Address を書き換える手法を導入する．パケットの経路の決定には，パケットに付与された Destination Address が使用される．送出されたパケットに対する返信には，送出パケットの Source Address が Destination Address として使用される．従って，受信側ネットワークからパケットを送出する際に Source Address を衛星回線側のネットワークのアドレスに書き換えることによって，衛星回線を使用した通信が実現できる．Source Address の変換を導入する場合には，2.で論じた3つの分類に加え，受信側ネットワークにプライベートアドレスを付与する場合の分類が必要である．また，地上インターフェースと衛星インターフェースを持つホストが同一であるか，異なるかによっての区別が必要である．この分類を表2に示す．

タイプ1の場合のアドレス変換は次のようになる．受信側ホスト（以下 UserHost と略す）は，受信専用の衛星インターフェース（以下 Sat-if と略す）と，送受信を行う地上インターフェース（以下 Gr-if と略す）を持つ．UserHost が外部のネットワークと通信するときのパケットのアドレスは，表3のようになる．これを Gr-if から送出する際，表4のように書き換える．返信されるパケットは表5のようなアドレスが与えられる．このパケットは衛星回線を使用し Sat-if より受信される．UserHost は，Sat-if からこのパケットを受信した際，パケットのアドレスを表6のように書き換える．

タイプ2，5の場合のアドレス変換は次のようになる．受信側ホストの地上側アドレス（以下 UserHost-Gr と略す）と対になるように衛星側アドレス（以下 UserHost-Sat と略す）を割り当てる．受信側ホストが外部のネットワークと通信するときのパケットのアドレスは表7のようになる．地上インターフェースを持つホストはこのパケットのアドレスを表8のように書き換える．返信されるパケットに与えられるアドレスは表9のようになる．このパケットは衛星回線を使用し受信側ネットワークの衛星インターフェースから受信される．これを受信時に表10のように書き換える．受信側ネットワーク上に複数の受信局が存在する場合には，受信側ホストの地上側アドレスと対になる衛星側アドレスを受信局数分割り当て，任意の使用したい受信局を選択しそれに対応する衛星側アドレスに書き換える．

タイプ3，6の場合のアドレス変換は次のようになる．地上回線インターフェースを持つホストの通信において，タイプ1と同様のアドレス変換を行う．この場合には，Sat-if は受信側ネットワークが持つ衛星イン

ターフェースのアドレスになる．受信側ネットワークが受信局を複数持つ場合には，Sat-if は複数になる．アドレス変換時は，複数の Sat-if の中から使用したい任意の一つを選択し，そのアドレスに書き換える．

タイプ 4，7 の場合のアドレス変換は次のようになる．この場合は，受信側ネットワーク上のホストから外部へ向かうパケットのアドレスをタイプ 1 の場合と同様に変換する．受信側ネットワークが受信局を複数持つ場合には，タイプ 3，6 の場合と同様，複数の Sat-if から一つを選択する．また，返信されたパケットの宛先を受信時に識別するために，トランスポート層のポート番号を変換 [4] する．

タイプ 5，6，7 の場合には，送信時のアドレス変換を地上インターフェースを持つホストが提供し，受信時のアドレス変換を衛星インターフェースを持つホストが提供する．受信側ネットワークで地上インターフェースを持つホストと衛星インターフェースを持つホストの間で，書き換えたアドレスおよびポート番号の情報について同期を保つ必要がある．

この機構により，受信側ネットワークより送出されたパケットは地上回線を経由し，受信側ネットワークへの返信パケットは衛星回線を経由する．

3.2 アドレス変換による経路の選択

衛星回線を使用するか否かの制御には，送信側で行う制御と受信側で行う制御が考えられる．送信側での制御は，宛先となる受信局ごとに割り当てる帯域を制御することが考えられるが，本論文では送信側での制御に関しては論議の対象を外れるので，言及しない．ここでは，受信局側で衛星回線の使用を制御する手法について論じる．

3.1で述べたアドレス変換を行うホストは，事前に衛星回線へ経由すべき通信相手 (Satellite Service Host) の一覧表 (Service Hosts Table) を持っておく．この一覧表の構成を表 11に示す．

アドレス変換を実行する際，まずそのパケットの Destination Address が Service Host Table 中に存在するか否かを検索する．存在した場合は 3.の通りアドレス変換を行い，存在しない場合はアドレス変換を行わない．

その結果パケットの復路は，通信相手が衛星回線を使用すべきホストの場合は衛星回線を，それ以外の場合は地上回線を経由する．

3.3 アドレス変換の提供

アドレス変換機能を提供する際に必要な機能について考える．前述のパケットに与えられるアドレスは，ネットワーク層のパケットのヘッダに書かれたアドレスである．アドレス変換は，このアドレスを書き換えればよい．しかし，ネットワーク層ヘッダには誤り検出のためのチェックサムがあり，アドレスを書き換えただけでは，元のパケットのチェックサムと異なってしまう．ルータがパケットを受け取った際には，ルータがパケットのチェックサムを再計算して誤りの有無を検査し，誤りと判断した場合にはパケットを廃棄する．これを防ぐため，アドレスを書き換えた場合には，IP ヘッダのチェックサムも同時に再計算し，新たに書き換える機能を同時に提供する．

表 11　衛星サービスホスト表
Table 11　Table of satellite service hosts.

Satellite Services Address
Sat.Inet.Host1
Sat.Inet.Host2
：
Sat.Inet.HostN

インターネットの経路制御は，OSI7 層モデルに基づくネットワークアーキテクチャでは，ネットワーク層 (第 3 層) が提供するサービスである．従来ネットワーク層では，パケットの生存時間 (TTL) を減算し，チェックサムを再計算する機能を提供している．本機構のアドレス変換も，ネットワーク層アドレスを変換する．したってこの機能は，アドレス変換を行うホストのネットワーク層の機能として提供することが適当である．

3.4 他の手法との比較

広帯域な単一方向と狭帯域の双方向リンクを組み合わせて使用する手法は，トンネリング技術を使用するもの [1] や，データリンク層で単一方向リンクの使用を制御するケーブルテレビ網用モデムなどが，すでに実用化されている．これらの手法と本論文で提案する手法は，以下の点で異なる．

既存の手法では，単一方向のリンクを使用するか否は，単一方向リンクの送信側が決定する．本機構では，アドレス変換を行うか否かによって単一方向リンクが使用されるかどうかが決まり，これは受信側が行う．

また，既存の手法では，送信するパケットは動的なダイアルアップ又は他のネットワークを経由するトンネリングなどによって送信側のネットワークに送られる．受信側ネットワーク上のホストがインターネット上の任意のホストと通信する際には，受信側ネットワークから他の経路を経由して一旦送信側へ行き，目的のホ

ストへ到達する．これに対して，本論文で提案する機構では，受信側ネットワークの地上インターフェースから，通常の経路制御によって目的のホストへ送られる．この点で，本論文で提案する機構の方が柔軟性がある．

4. アドレス変換によって発生する問題

本論文で提案するアドレス変換機構は，パケットに与えられたネットワークアドレスをその経路途上に存在するホストが書き換える．そのため，セキュリティ技術，特に IP Spoofing [5] 防止機構が，本機構の動作の障害となる．本章では，アドレス変換技術を用いる上で IP Spoofing 防止機構と本機構を共存させるための手法について考察する．

衛星回線へのインターフェースを持つユーザホストと衛星サービスホストの間に，Source Address によってパケットをフィルタリングしているルータが存在する場合を考える．この場合，本機構ではパケットの Source Address を書き換えるので，このルータを通過する際にパケットの Source Address がルータに対して不正となる場合がある．この場合，ルータはパケットの通過を認めないので，このルータを越えてユーザホストと他のホストが通信することが不可能となる．これを回避するためには，ユーザホストの持つ衛星回線インターフェースのアドレスを Source Address に持つパケットがルータを通過できるように，ルータを設定する必要がある．

このような設定がセキュリティの方針上許されない場合には，ユーザホストがアドレス書き換えを行ったパケットは，ユーザホストの衛星回線インターフェースと同一のネットワークに属するホストまで IP トンネリングを用いてパケットを転送する手法が考えられる．この場合，アドレス変換を行ったパケットは，地上回線インターフェースのアドレスを付与されたパケット中にカプセル化され，衛星回線の属するネットワークまで転送されたのち，脱カプセル化され本来の宛先ホストへ転送される．この結果，ユーザホストから送出されたパケットが上述のルータを通過する際には，パケットの Source Address はこのルータに対して正当であるので，パケットはこのルータを通過する．その後パケットは，トンネルの終点で本来の，即ちアドレスを書き換えられたパケットとして再転送されるので，経路途上のルータを通過したものと同一の結果が得られる．

上述の問題は，3.1で述べたアドレス変換動作の分類全てについて適用される．

5. 実　　装

本機構は，パケットの選別，アドレス変換の選択，送信時のアドレス変換とポート番号変換，受信時のアドレス変換とポート番号変換の 4 つのモジュールからなる．実装では，アドレス変換，ポート番号変換の情報の同期をとるために，処理は同一ホストで提供することとした．異なるホスト上でこれらを提供する手法については，今後の課題である．これについては 5.6 で後述する．また，受信側ホストは複数とし，各ホストにはプライベートアドレスを付与することとした．これは，3.1で述べた分類のタイプ 4 に当たる．実装は，UNIX の OS 内のカーネルによって実行されるように実装した．アドレス変換機構は RFC1631 [3] に準じて実装した．

5.1 本機構の動作に必要な情報

カーネル内に本機構動作のために次の情報を保持する．

- 受信側ネットワークのアドレス
- 受信側ネットワークのネットマスク
- ホストの衛星回線インターフェースのアドレス
- ホストの地上回線インターフェースのアドレス
- 衛星サービスホストテーブル
- ポート変換テーブル
- ポート変換テーブルチェック間隔
- ポート変換テーブルエントリ保持時間

衛星サービスホストテーブルの構成を表 11に示す．ポート変換テーブルの構成を表 12に示す．ポート変換テーブルチェック間隔，ポート変換テーブルエントリ保持時間の単位は秒とした．

5.2 パケットの選別

パケットを受信した場合，またはホストがパケットを送信しようとする場合，パケットはパケット選別モジュールに送られる．

パケットのトランスポート層プロトコルを検索する．これが TCP，UDP でない場合には，通常の処理ルーチンへパケットを渡す．

パケットの Source Address と受信側ネットワークアドレスとネットマスクを比較し，このネットワークからのパケットであった場合には，アドレス変換の対象となるパケットであると判断し，アドレス変換の選択を行うモジュールにパケットを渡す．

表 12　ポート変換テーブル
Table 12　Table of port translation.

変換前アドレス	変換前ポート番号	変換後ポート番号	最新使用時刻
:	:	:	:

パケットの Source Address がこのホストの地上回線インターフェースのアドレスであった場合には，アドレス変換の対象となるパケットであると判断し，アドレス変換の選択を行うモジュールにパケットを渡す．
パケットの Destination Address がホストの衛星回線インターフェースであった場合には，ポート番号がポート変換テーブル中に存在するかを検索する．存在した場合には，書き換えるアドレスとしてポート変換テーブルのエントリを指定し，受信時アドレス変換モジュールへパケットを渡す．
上述のどれにも当てはまらなかった場合には，通常の処理ルーチンへパケットを渡す．
また，ポート変換テーブルチェック間隔で指定された時間ごとに，ポート変換テーブルを全検索し，最新の使用時刻が現在時刻よりエントリ保持時間以上古い場合，そのエントリを削除する．

5.3　アドレス変換の選択

このモジュールの処理は，従来のアドレス変換機構には存在しないものである．カーネルプロセス内に予め衛星回線を経由して受信したい宛先ホストのアドレスを保持しておく．このモジュールで，パケット選別モジュールから渡されたパケットの Destination Address がアドレス一覧のテーブル中に存在するかを検索する．存在した場合には，書き換えるべきアドレスに衛星回線インターフェースのアドレスを，存在しない場合には地上回線インターフェースのアドレスを指定し，送信時アドレス変換モジュールに渡す．

5.4　送信時アドレス変換

パケットの Source Address を，アドレス変換選択モジュールが指定したアドレスへ書き換え，ネットワーク層ヘッダのチェックサムを再計算して書き換える．変換後のポート番号は，変換前のパケットの Source Addrss とポート番号が一意に識別できるように決定しなければならない．変換後のポート番号を決定する際に，この処理の効率をよくするため，以下の手順を導入した．一般的な TCP の実装では，ポート番号は 1024 より大きく，そのホストの通信で使用されていないもののうち最小のものが使用されることを利用し，以下の手順により変換後のポート番号を決定する．

（1） 複数のホスト間で，変換後のポート番号が重複しないように，できるだけ簡単な変換方法を決める．トランスポート層のポート番号は 16 ビット値なので，受信側ホストの Source Address の情報を 2 バイト以上使って変換を考えるのは意味が薄く，Source Address の下位 1 バイトを使った変換を考える．Source Address の下位 7 ビットや 9 ビットといった半端なビット数を用いるのは変換の計算の効率が悪くなるので避ける．16 ビット値のポート番号を Sourcee Address の下位 8 ビットで区別される 256 個に分割して割り当てるため，Source Address の下位 8 ビットに 256 を乗じて変換後のポート番号の基準となる値を決める．前述のように，多くの TCP の実装では，個々のポート番号は 1024 より大きい未使用の番号が順次割り当てられるので，この値を各 Source Address ごとの基準となる番号に加算して変換後のポート番号の候補を決める．

変換後ポート番号の候補 = ($SourceAddress$ の下位 8 ビット) × 256 + 変換前のポート番号

（2） 候補の値が 65535 を越えていた場合には，ウェルノウン・ポートと重複しないように，次の式により，1024 から 65535 の範囲におさまるように再計算する．

次の変換後ポート番号の候補 = 変換後のポート番号の候補 − 65535 + 1024

（3） ポート変換テーブルを検索し，算出したポート番号と変換前のパケットの Source Address 及び変換前のポート番号の組がすでに使用されていないかを検査する．使用されていない場合，このポート番号を選択する．使用されており変換前のパケットの Source Address 及び変換前のポート番号の組が異なる場合には，変換後ポート番号を 1 ずつ加算し検査し，使用されていないポート番号を選択する．選択したポート番号と変換前のパケットの Source Address，ポート番号の組をテーブルに記憶する．テーブル中に存在し変換前のパケットの Source Address 及び変換前のポー

トの組が存在した場合は，テーブルに記憶された変換後のポート番号を選択する．

送出されるパケットのポート番号を選択されたポート番号に書き換え，トランスポート層ヘッダのチェックサムを再計算し，書き換える．アドレス変換処理を行ったときは，ポート変換テーブルの最新使用時刻に現在時刻を記憶する．その後，パケットは通常の処理ルーチンへ渡される．

5.5 受信時アドレス変換

ポート変換テーブルから，受信したパケットのポート番号を検索する．テーブル中の，検索したエントリの Source Address 及びポート番号の組に，パケットの Destination Address とポート番号を書き換え，ネットワーク層ヘッダのチェックサムを再計算し書き換える．アドレス変換処理を行ったときは，ポート変換テーブルの最新使用時刻に現在時刻を記憶する．
また，TCP のパケットであった場合，パケットの FIN フラグ，RST フラグが ON になっているかを検査し，ON になっていた場合，ポート変換テーブルのエントリを削除する．その後，パケットは通常の処理ルーチンへ渡される．

5.6 複数ホストによるアドレス変換の提供

本論文では，3.1で述べた分類のうち，地上インターフェースと衛星インターフェースを持つホストが同一であるアーキテクチャについて実装した．本節では，実装上の今後の課題である，地上及び衛星インターフェースを持つホストが異なる場合の実装方法について考察する．また，本節で述べる手法は，一つの受信側ネットワークが複数の単一方向リンク，双方向リンクを持つ場合に対しても有効である．
3.1で述べたとおり，地上及び衛星インターフェースを持つホストが異なる場合，送信時に行うアドレス変換と受信時に行うアドレス変換の機能を提供するホストが異なる．送信時アドレス変換と受信時アドレス変換は，動作時に表12に挙げたポート変換テーブルを参照し，更新する．このため，ポート変換テーブルを複数のホスト間で共有する必要がある．
これを実現するために次のような機構を考える．受信側ホストのいずれかが，ポート変換テーブルを保持する．このホストは，ネットワークを介してアドレスとポートの組からなる要求を受け取り，それを変換前のパケットの Source Address および変換前のポート番号として 5.4と同様の処理を行った後，変換後ポート番号を返答として返す機能を持つ．送信時アドレス変換，受信時アドレス変換を行うホストは，アドレス変換を行う際に，受信側ネットワークを介してポート変換テーブルを持つホストに対して上述の要求を送り，その返答に基づいてアドレスを変換する．
受信側ネットワークが外部への複数の単一方向・双方向リンクを持つ場合，アドレス変換を提供するホストは複数となる．この時にも，上述と同様にポート変換テーブルを共有する手法が有効である．

6. 評　　価

この章では，前述したアドレス変換機能の評価について述べる．実際に衛星回線へと地上回線への接続性を持つネットワーク上において，このネットワーク上のホストとインターネット上の特定のホストが通信する時に，選択的に衛星回線を経路として使用する機構が実現されたことを示す．また，実験環境として構築したネットワーク上で，本機構の性能を測定しアドレス変換機構を用いなかった場合と比較した結果を示す．実装は，FreeBSD 2.2.1-RELEASE 及び BSD/OS 2.1 上で動作しており，評価にはこの 2 つの実装を用いた．

6.1 本機構の動作環境

本機構を実装し，図 2に示すネットワーク上において動作させた．評価には FreeBSD 2.2.1-RELEASE 上の実装を用い，次に示す動作を実験で確認した．

- プライベートネットワーク上のホストの通信
  - 衛星サービスホストと通信する場合には，往路は地上回線，復路は衛星回線
  - その他のホストと通信する場合には，往復ともに地上回線
- アドレス変換処理ホストの通信
  - 衛星サービスホストと通信する場合には，往路は地上回線，復路は衛星回線
  - その他のホストと通信する場合には，往復ともに地上回線

6.2 性能評価

本機構の性能を計測するため，図 3に示すネットワークを構築した．このネットワークは，衛星回線並びに地上回線を持つネットワークをシミュレートする実験環境である．このネットワークで，地上回線をエミュレートする回線には SLIP を使用し，帯域は 38400bps に設定した．衛星回線をエミュレートする

表13　プライベートホストにおけるファイル転送の所要時間(単位・秒)
Table 13　FTP Time-consuming at private host.

	地上サービスホストとの通信	衛星サービスホストとの通信
なにもしない場合	280.5	3.8
	2805.4	41.3
アドレス変換のみ	280.5	3.9
	2805.5	41.6
アドレス・ポート変換	280.5	4.0
	2805.3	42.2

表14　アドレス変換処理ホストにおけるファイル転送の所要時間(単位・秒)
Table 14　FTP Time-consuming at address tanslating host.

	地上サービスホストとの通信	衛星サービスホストとの通信
なにもしない場合	280.0	4.8
	2800.0	50.0
アドレス変換	280.3	4.8
	2803.2	51.2

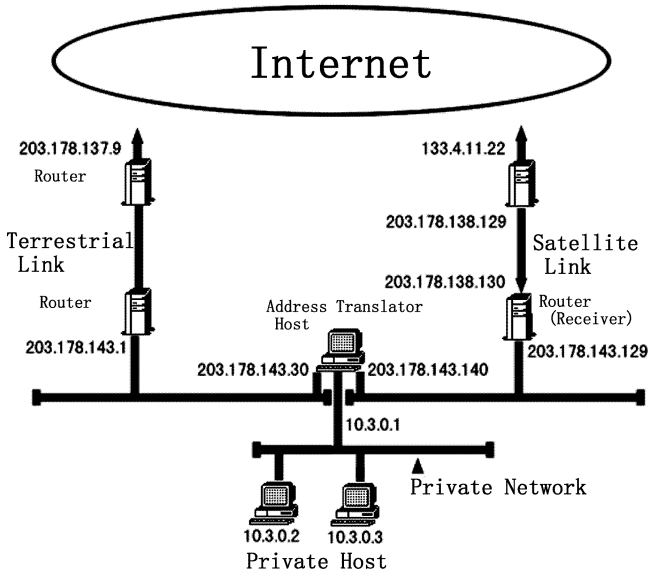

図2　動作実験ネットワーク・トポロジー図
Fig. 2　The topology of exercising network.

回線には Ethernet を使用し，帯域は 10Mbps とした．評価には，BSD/OS 2.1 上の実装を用いた．
アドレス変換を行わなかった場合，アドレス変換のみを行った場合，アドレス変換とポート番号変換を行った場合の 3 つの条件下で，測定ホストと衛星サービスホスト，地上サービスホスト間で 1MBytes，10MBytes の２つのファイルを FTP を用いて転送し，それにかかった時間を 0.1 秒の精度で計測した．表 13及び表 14にその結果を示す．表からわかるように，38400bps の帯域の回線で用いる場合，アドレス変換によるオーバーヘッドは計測されなかった．これは，アドレス変換処理によるオーバーヘッドが TCP によるオーバーヘッドより小さかったため，実際の性能に影響しなかったものと考えられる．10Mbps の回線で用いる場合，転送パケット量の少ない場合で約 5%，多い場合で約 2

7. ま と め

現在，衛星回線をインターネットの通信路として利用でき，一般家庭等に伸張することも容易である．しかし，このようなネットワークにおける経路制御の

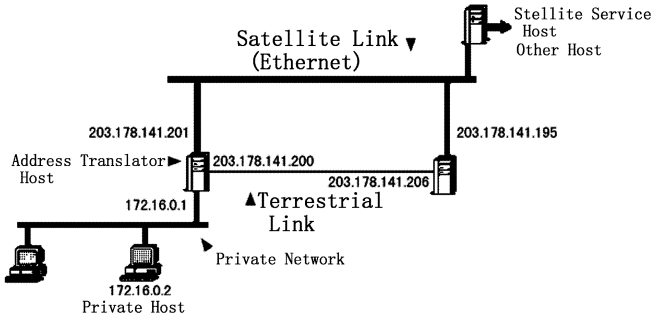

図3　実験環境ネットワーク・トポロジー図
Fig. 3　The topology of evaluating network.

アーキテクチャは提供されていない．近い将来，衛星回線を使用したインターネット接続が一般的となった場合，非常に多数のネットワークが衛星回線に接続されると予想されるが，これを支える大規模性を持った経路制御機構が必要である．

本論文では，衛星回線の受信側ネットワークが送信時にアドレスを変換し衛星回線を使用する手法について述べた．また，衛星回線の大規模性を確保するために衛星回線の使用を選択できるように送信時に宛先によって選択的にアドレス変換を行って，衛星回線の通信を制御する手法について述べた．このアドレス変換を使用した経路制御は，衛星回線と地上回線，プライベートネットワークをシュミレーションするテストベッド上で動作している．

謝辞

本研究に対して貴重な助言を頂いた,（株）日本サテライトシステムズの泉山英孝氏，ソニー（株）の藤井昇氏をはじめとするWIDEプロジェクトの方々，また実験に御協力頂いたUnSAT協議会の方々に感謝いたします．

文　献

[1] Hidetaka Izumiyama, Akihiro Tosaka, Akira Kato "Uni-directional Link Routing with IP tunneling approach", Internet-Draft, July 1997.
[2] Walid Dabbous, Emmanuel Duros, Thierry Ernst "Dynamic Routing in Networks with Unidirectional Links", Proceedings of the Second International Workshop on Satellite-based Information Services, Budapest, Hungary, Oct. 97.
[3] K. Egevang, P. Francis "The IP Network Address Translator (NAT)" RFC 1631, May 1994.
[4] P. Srisuresh, K. Egevang "The IP Network Address Translator (NAT)" Internet-Draft, September 1997.
[5] "IP Spoofing Attacks and Hijacked Terminal Connections" CERT Advisory CA-95:01 January 1995.

（平成9年10月31日受付）

西田　視磨

慶應義塾大学環境情報学部，1994年4月 慶應義塾大学環境情報学部入学

楠本　博之

慶應義塾大学環境情報学部専任講師，1985年3月 大阪大学理学研究科物理学専攻前期課程終了，1985年4月 電子技術総合研究所研究員，1989年10月 慶應義塾助手，1995年4月より現職，インターネットアーキテクチャ，コンピュータネットワークの研究に従事

村井　純　（正員）

慶應義塾大学環境情報学部教授，1984年慶應義塾大学工学部数理工学博士課程修了，1987年 博士号取得，1984年 東京工業大学総合情報処理センター助手，1987年 東京大学大型計算機センター助手，1990年 慶應義塾大学環境情報学部助教授，1996年4月より現職，1984年JUNETを設立，1988年WIDEプロジェクトを設立し，今日までその代表として指導にあたる．社団法人日本ネットワークインフォメーションセンター理事長，IAHC(Internet Adhoc Committee)委員