移動するネットワークのための透過的な通信機構の設計

石井 公夫† 寺岡 文男‡ 村井 純†
ishii@sfc.wide.ad.jp tera@csl.sony.co.jp jun@wide.ad.jp

†慶應義塾大学 ‡ソニーCSL

携帯型コンピュータと各種通信機器の普及により、移動しながらインターネットにアクセスして使用するモーバイルコンピューティング環境が現実のものとなってきている。こういった状況に対しホストが移動しながら透過的かつ連続的に通信をおこなうための方式がいくつか提案されているが、現状では単一のホストの移動しか考慮されていない。本稿ではネットワーク単位での移動を実現するための様々な方式を提案し、それぞれの持つ技術的な問題点を述べ、さらに応用についても議論する。

1 はじめに

近年のコンピュータの小型軽量化は著しく、移動しながらインターネットをはじめとするネットワークに接続して利用する、いわゆるモーバイルコンピューティング環境が現実的のものとなりつつある。

このような状況のなか、インターネット上でのホスト移動をサポートするプロトコルの研究がいくつかおこなわれている。代表的なものにWIDE/Sonyが開発中のVirtual Internet Protocol(VIP)[1]という方式と、現在Internet Engineering Task Force(IETF)で標準化作業がすすめられているMobile IP[2]という方式があるが、両方式とも単独のホストの移動しか考慮されていない。

しかし将来のモーバイルコンピューティング環境を考えた場合、現在のようにホストを持ち歩きながらインターネットを利用できるというだけでは、今後登場するであろう様々な利用方法・利用形態への対応は難しい。よってホストが単独で移動する場合だけでなく、いくつかのホストや機器がLANを形成しており、それがインターネットへの接続先を次々に変更しながら移動する、いわゆる移動ネットワークも考慮する必要がある。もちろん移動ネットワークといっても、利用者から見た場合たとえネットワークが物理的に移動しても、現在おこなっているファイル転送などの作業は継続できなければ実用的とはいえない。このように通信を継続しながらのネットワーク単位の移動が実現することにより、現状では不可能であった以下のような様々な利用形態が考えられる。

- 自動車や飛行機などの乗物からインターネットへのアクセス
- 複数の接続先(プロバイダ等)を切り替えて、家庭内LANからインターネットへアクセス
- 移動対応でない通常のホストでも移動ネットワーク内からインターネットへアクセス

近い将来、自動車には当然LANが構築されていることが予想される。ここでは例として車内に接続されたホストからインターネットへのアクセスおこなうことを考える。まず走行中は携帯電話などの帯域の狭い無線機器からアクセスせざるを得ないので、キャッシュなどを用いてなるべく通信量を減らす工夫が必要であるが、ガソリンスタンドで給油中もしくはサービスエリアで駐車中には帯域の広い光ファイバー等を接続し、キャッシュのデータなどを更新するというような利用法がおそらく一般的になるだろう。そのためには利用者やアプリケーションから見て、接続先の切り替えが透過的におこなわれる必要がある。

また飛行機も同様で、例えば日本からアメリカへの飛行を考えた場合、機内LANは最初は成田へ光ファイバーで、次に日本上空では無線でアクセスするが、無

Design of a Transparent Communication Architecture for Network Migration
Kimio ISHII†, Jun MURAI†
†Keio University
Fumio TERAOKA‡
‡Sony Computer Science Laboratory

線が届かなくなると衛星経由に切り替え、そして最後にはまたアメリカの空港へ無線でアクセスするというような接続形態が可能になり、その間利用者の通信は連続しておこなえる。

家庭内LANの場合を考えると、LANそれ自体が物理的に移動するわけではないが、接続先を切り替えることはネットワークが移動することと等価と考えられる。具体的な用途として考えられることとして、ある時間以降に電話料金が固定になる場合、その時間になるまでは大学等へ接続していて、その時間以降は契約しているプロバイダに、現在のセッションを継続したまま接続先を変更するということなどが挙げられる。

個々で従来のホストの移動と、ネットワークの移動の相違点について述べる。まず最も大きな違いとして挙げられることは、移動ホストを実現するには、移動したい全てのホストが移動対応でなければならないという条件があるのに対して、移動ネットワークを実現するにはルータとなるホストを除けば、内部にあるホストは移動対応に修正する必要がないという点である。前述のVIPやMobile IPというプロトコルを用いて移動ホストを実現するには、システムを変更したり、特殊なアプリケーションを常時動作させるなどをして移動に対応させているが、移動ネットワーク内にいれば、通常のホストでも透過的に通信がおこなえるので、すべての既存のホストを移動対応にすることに比べて非常に現実的である。しかし当然ながらあるホストが移動ネットワーク内から離脱して単独で移動する場合は、そのホストは移動対応になっている必要がある。

2 移動するネットワークの問題点

本来のインターネットのアーキテクチャは、当然ながらネットワークが移動することなどは全く考慮されていない。考慮されていないだけでなく、経路制御やそれに伴うアドレスの割り当てポリシーなどはネットワークは移動しない、すなわちネットワーク間のトポロジーが変化しないことが前提となっている。本章ではこういった状況においてネットワークが移動すると仮定した場合どのような問題が生じるのかを検討する。

2.1 移動ネットワークの定義

まず移動ネットワークとは何か定義する。移動ネットワークは用途に応じて様々な構成がとられ、その接続形態等は規定されるべきではないが、今回は以下のような簡単な構成のネットワークのみを対象とする。

- 単一の物理セグメントである
  → イーサネットならば1セグメント
  → 無線LANならば1つのエリア内
- ルータとなるホストが一台だけ存在する
  → これをモーバイルルータと呼び移動ネットワーク内部へのトラフィックは全てこのルータを経由する
- 移動ネットワーク内部のホストのすべてが移動対応であるとは限らない

また移動ネットワークは以下に示すように状態を遷移するが、切り離されて移動中という場合は、通常のルータが故障している場合と同様にみなし、今回はその状態を特別に考慮することはしない。

1. 正規のネットワークに接続されている
2. 現在いるネットワークからの離脱
3. 切り離されて移動中
4. 新たなネットワークで接続交渉
5. 新たなネットワークに接続される

移動のたびに2〜5が繰り返される。

2.2 移動ネットワークの問題点

移動ネットワークには当然アドレスをつける必要があるが、そのアドレスには以下のような種類が考えられる。

- クラスCのアドレスを新規に取得する
- クラスBのアドレスを用いている組織の場合、使われていないアドレスを割り当ててもらう
- プライベートアドレスを用いる

プライベートアドレス[3]を用いる方法については、NATの解説とともに後述する。よって以下の議論は移動ネットワークのアドレスが、あるクラスCもしくはあるクラスBの一部であると仮定する。

移動ネットワークが新規接続をした後、モーバイルルータが経路情報をアナウンスし、それが瞬時にインターネット上へ伝播すれば、理論上は問題なく通信をおこうことができる。しかし以下に述べる理由によりそれは現実的ではない。

1. IP アドレスの枯渇問題が憂慮されている現在、移動ネットワーク用に新規にアドレスを取得できる可能性はほとんどない

2. モーバイルルータが経路情報をアナウンスする時、OSPF の場合は認証が必要であるため、新規接続先のネットワーク側との事前の調整がなければ経路をアナウンスできない [4]

3. 運用上の問題として全てのホストやルータが可変長ネットマスク (VLSM) 対応の経路表を持ち、OSPF 等を利用して経路情報を交換できるわけではない

4. 同一の自律システム (AS) 内での移動の場合でも、接続先のネットワークのルータがセキュリティ対策のため、経路情報のフィルタリングをおこなっている場合が多いので、経路情報は伝播しない可能性が高い

5. 最近はアドレスの枯渇以上に経路情報の増大が問題になっており、経路情報の集約がおこなわれているため、本来所属している AS とは異なる AS に移動した時には、その経路情報は伝播できない [5]

6. たとえ経路情報をアナウンスすることが可能であったとしても、現実には伝播するためにはある程度の時間がかかり、その間は通信がおこなえない

3 既存の移動ホスト対応プロトコル

前述したように、通常のインターネットの仕組みの中で移動ネットワークを実現することは問題点が多すぎて不可能である。よって移動ネットワークの実現には次に挙げる移動ホスト対応プロトコルを利用する。

- VIP 方式の拡張
- Mobile IP 方式の拡張
- NAT の利用

本章では現在提案されているホスト移動対応プロトコルの中で、WIDE/Sony が開発中の VIP と、IETF で標準化がすすめられている Mobile IP の二種類の方式の概要を紹介する。

また NAT は移動ホスト対応プロトコルというわけではないが、NAT の仕組みに関しては後述する。

3.1 VIP 方式

VIP 方式は OSI の 7 層モデルのネットワーク層を VIP 層と IP 層の 2 つに分ける。VIP 層でのアドレスはホストの識別子をあらわし、IP 層でのアドレスはネットワーク上の位置情報をあらわしている。移動ホストは移動先のネットワークで DHCP[6] 等を用いて一時的に IP アドレスを取得し、それをホームルータに通知する。ホームルータの Address Mapping Table(AMT) と呼ばれるテーブルには VIP アドレスと IP アドレスの組合せが登録される。さらに通知のパケットが通過した、途中にある VIP 対応のルータにも同じ AMT のエントリがキャッシュされる。

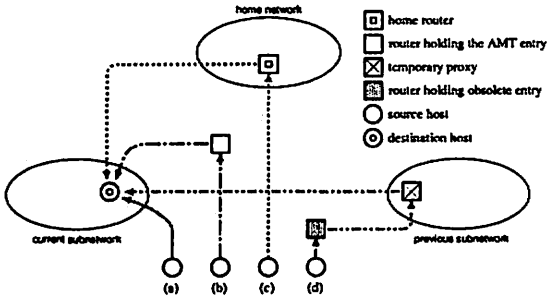

図 1: VIP 方式の通信

通常のホストと移動ホストの通信を考えると、移動ホストの VIP アドレス宛のパケットは経路情報に従ってホームルータへ向かうが、途中に VIP 対応のルータがあれば、その AMT に VIP アドレスと IP アドレスの組合せがキャッシュされているため、その移動ホスト宛のパケットはアドレス変換されて、現在接続している位置に転送される。もちろん途中にキャッシュされていなくとも、ホームルータまでパケットが届けばアドレス変換されて転送される。なお実装には IP オプションを使用している。

3.2 Mobile IP 方式

Mobile IP 方式の場合、移動ホストの IP アドレスは移動しても変わらない。しかし移動先のネットワークには訪問先エージェント (FA) が存在しなければならない。FA はセグメント内にその存在をビーコンを用いて定期的にアナウンスし、移動ホストはネットワークに新規接続した後、それを聞くことにより FA を見つけ出し、FA とデータリンクレベルで通信して、FA に

移動ホストの存在を通知する。FA はさらに移動ホストのホームエージェント (HA) にそれを通知する。HA には移動ホストの IP アドレスと FA の IP アドレスの組合せのテーブルが生成される。

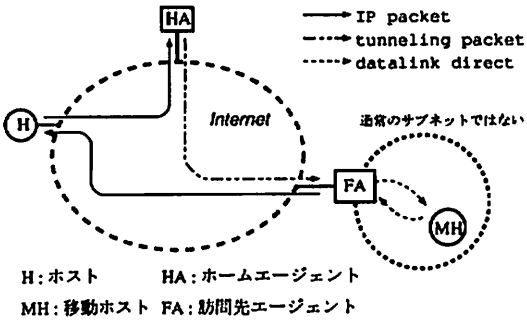

図 2: Mobile IP 方式の通信

通常のホストと移動ホストとの通信を考えると、移動ホスト宛のパケットは経路情報に従って HA に到着する。テーブルを検索してその移動ホストと対応する FA のエントリを索き、パケットを IP in IP でカプセル化して FA にトンネリング [7] する。FA はそのパケットを脱カプセル化して、データリンク層のプロトコルを用いて移動ホストに直接そのパケットを転送する。

現在の実装においては、トンネリングに関してはネットワークインターフェイスを用い、データリンクレベルでの通信はホスト単位の経路制御と ARP テーブルの操作で対応している。

4 VIP の拡張による実現

この章では VIP を拡張して移動ネットワークを実現する三通りの方法を解説する。

以下の議論のため、例として移動ネットワークは 133.138.194.0/24 というアドレスを持ち、そのホームルータは HR1 とし、133.4.34.0/27 というセグメントに新規接続する場合を考える。またこの移動ネットワークに接続して来るよその移動ホストを X とし、X のホームルータは HR2 とする。

4.1 アドレス全付け替え方式

最初の方式は、VIP のモデルはそのままで、移動先でアドレスブロックを取得し、移動ネットワーク内の全ての機器にアドレスを再割り当てする。

4.1.1 通常の動作

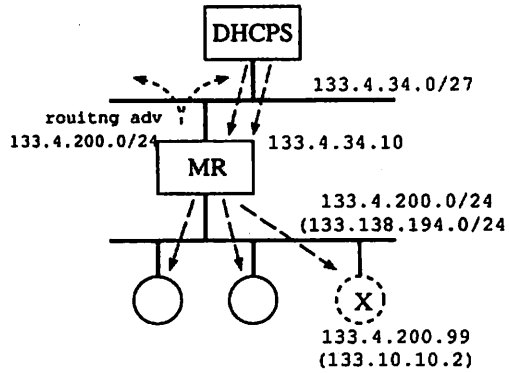

図 3: アドレス全付け替え方式

1. モーバイルルータ (MR) が DHCP サーバから自分用のアドレスに 133.4.34.10 を取得する
2. 移動ネットワークのネットマスク分のアドレスブロック 133.4.200.0/24 を DHCP サーバから取得し、その経路情報をアナウンスする
3. モーバイルルータ自身が DHCP サーバとなり、取得したアドレスブロック 133.4.200.0/24 を移動ネットワーク内の機器に対して再割り当てをする
4. ホームルータ HR1 の AMT にはネットワーク対ネットワークという組合せの対応が生成される

ここで移動ネットワーク内の 133.138.194.5(この時点では 133.4.200.5 というアドレスがついている) というホストが移動ネットワークを離脱して、よそのネットワークに接続され、一時的に 133.113.10.10 というアドレスを取得したとする。HR1 の AMT は表 1のようになり、最長一致アルゴリズムにより 133.138.194.5 宛のパケットは、HR1 で正しく 133.113.10.10 にアドレス変換され転送される。

133.138.194.0/24	→	133.4.200.0/24
133.138.194.5/32	→	133.113.10.10/32

表 1: HR1 の AMT その 1

4.1.2 よその移動ホストが接続

よその移動ホスト X が接続されると、X は DHCP を用いて MR から 133.4.200.99 というアドレスを取得する。HR2 には表 2 という AMT が生成され、通常のホストから X へのパケットは、既存の VIP の場合と全く同じように経路情報に従い HR2 に到達しアドレス変換され 133.4.200.99 に到達する。

133.10.10.2/32	→	133.4.200.99/32

表 2: HR2 の AMT その 1

4.1.3 問題点

- この場合、移動ネットワーク内の機器は全て VIP/DHCP に対応している必要がある
- 動的にアドレスブロックを取得するためには DHCP の機能の拡張が必要である
- 移動ネットワークのネットマスクが接続先のネットマスクより狭い場合には、接続先のネットワークの経路制御が可変長ネットマスクに対応していなければならない
- 取得したアドレスブロックの経路情報を、モーバイルルータが OSPF を用いてアナウンスするためには認証が必要である

4.2 アドレス無変更方式-1

前述したアドレス全付け替え方式は、移動ネットワーク内の全ての機器が VIP/DHCP 対応でなければならないという非常に現実的でない条件がある。

以下で述べる二通りの方式では移動ネットワーク内の機器のアドレスは変更せずに、すなわち移動ネットワークのアドレスが不変であっても、通信をおこなうことが可能である。

4.2.1 通常の動作

1. モーバイルルータ (MR) が DHCP サーバから自分用のアドレスに 133.4.34.10 を取得する
2. 移動ネットワークのネットマスク分のアドレスブロック 133.4.200.0/24 を DHCP サーバから取得し、その経路情報を MR がアナウンスする

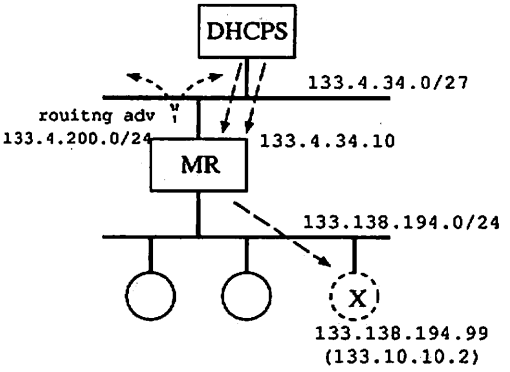

図 4: アドレス無変更方式-1

3. ホームルータ HR1 の AMT にはネットワーク対ネットワークの組合せの対応が生成される
4. 移動ネットワーク内の機器宛のパケットは、HR1 でまずアドレス変換され、MR において元に戻され、通常の経路制御に基づき転送される

ここで移動ネットワーク内の 133.138.194.5 というホストが移動ネットワークを離脱して、よそのネットワークに接続され、一時的に 133.113.10.10 というアドレスを取得したとすると、HR1 の AMT は表 1 と同じになり、最長一致のアルゴリズムにより 133.138.194.5 宛のパケットは、正しく 133.113.10.10 にアドレス変換され転送される。

4.2.2 よその移動ホストが接続

よその移動ホスト X が接続されると、X は DHCP を用いて 133.138.194.99 というアドレスを一時的に取得する。HR2 には表 3 の AMT が生成される。

133.10.10.2/32	→	133.138.194.99/32

表 3: HR2 の AMT その 2

通常のホストが移動ホスト X(133.10.10.2) 宛のパケットを送信すると、経路情報に従い HR2 に到達する。HR2 でアドレス変換がなされ 133.138.194.99 へ転送される。このパケットは経路情報に従い今度は HR1 に到達するが、HR1 には表 1 の AMT があるのでさらにアドレス変換され 133.4.200.99 に向かう。経路情報に従いモーバイルルータまで到達すると宛先が元に戻

され、すなわち宛先が 133.138.194.99 になりXに到達する。

4.2.3 問題点

- 動的にアドレスブロックを取得するためにはDHCPの機能の拡張が必要である
- 移動ネットワークのネットマスクが接続先のネットマスクより狭い場合には、接続先の組織の経路制御が可変長ネットマスクに対応していなければならない
- 取得したアドレスブロックの経路情報をモーバイルルータがOSPFを用いてアナウンスするためには認証が必要である

4.3 アドレス無変更方式-2

この方法はDHCPの拡張を必要とせず、モーバイルルータが経路をアナウンスする必要もないためにもっとも実現が容易である。二種類のアドレス無変更方式は全く同じ実装になる。

4.3.1 通常の動作

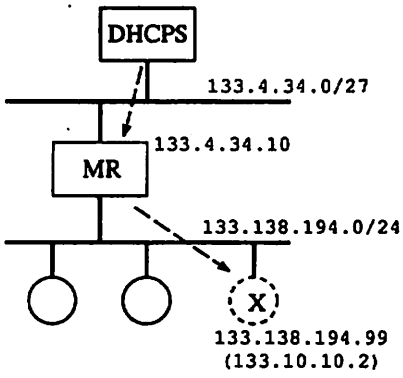

図 5: アドレス無変更方式-2

1. モーバイルルータ (MR) が DHCP サーバから自分用のアドレスに 133.4.34.10 を取得する
2. ホームルータ HR1 の AMT にはネットワーク対ネットワークの組合せの対応が生成される
3. 移動ネットワーク内の機器宛のパケットは、HR1でまずアドレス変換され、MR において元に戻され、通常の経路制御に基づき転送される

ここで移動ネットワーク内の 133.138.194.5 というホストが移動ネットワークを離脱して、よそのネットワークに接続され、一時的に 133.113.10.10 というアドレスを取得したとすると、HR1 の AMT は表 4のようになり、最長一致のアルゴリズムにより 133.138.194.5 宛のパケットは、正しく 133.113.10.10 にアドレス変換され転送される。

133.138.194.0/24	→	133.4.34.10/32
133.138.194.5/32	→	133.113.10.10/32

表 4: HR1 の AMT その 2

4.3.2 よその移動ホストが接続

よその移動ホスト X(133.10.10.2) が接続されると、X は DHCP を用いて 133.138.194.99 というアドレスを一時的に取得する。HR2 には表 3と同じ AMT が生成される。

通常のホストが X 宛にパケットを送信すると、経路情報に従い HR2 に到達する。HR2 でアドレス変換がなされ 133.138.194.99 へ転送される。このパケットは経路情報に従い今度は HR1 に到達するが、HR1 では表 4の AMT に基づき、さらにアドレス変換され 133.4.34.10 に向かう。経路情報に従い MR まで到達すると宛先が元に戻され、すなわち宛先が 133.138.194.99 になり X に到達する。

4.3.3 問題点

- ネットワーク対ホストという多対一の組合せの対応は、識別子と位置情報の一対一の組合せの対応という VIP のモデルにそぐわない

5 Mobile IP の拡張による実現

以下の議論のため、例として移動ネットワークは 133.138.194.0/24 というアドレスを持ち、そのホームエージェント (HA) の HA1 のアドレスは 133.138.192.2 とし、133.4.34.0/27 というセグメントに新規接続する場合を考える。133.4.34.0/27 に存在する訪問先エージェント (FA) のアドレスは 133.4.34.10 である。またこの

移動ネットワークに接続して来るよその移動ホストをXとし、Xのホームエージェントは HA2(133.138.192.2) とする。

5.1 通常の動作

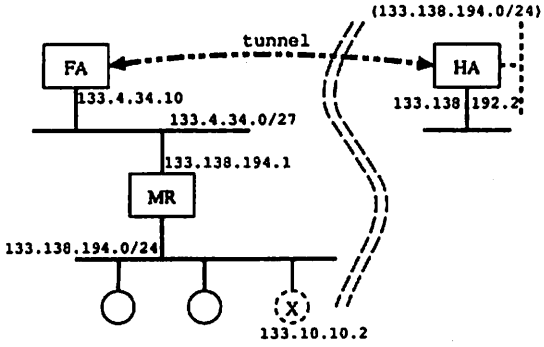

図 6: Mobile IP での実現

1. ホームエージェント HA1 は移動ネットワーク用の経路情報をアナウンスしている
2. モーバイルルータ (MR) は移動先のネットワークに接続すると、FA からのビーコンを聞き FA のアドレス等を知り FA に登録要求をおこなう
3. FA はそれを受けて HA1 に登録要求を転送する
4. HA1 は登録要求によって FA にトンネルを張り、移動ネットワークの経路はそのトンネリング用のインターフェイスを示す
5. FA に転送されてきた移動ネットワーク宛のパケットは、FA と MR 間をデータリンクレベルのプロトコルを用いて MR に転送される

アドレスが 133.20.20.20 の通常のホストから、移動ネットワーク内の 133.138.194.7 という機器へのパケットの様子を図 7に示す。

5.2 よその移動ホストが接続

移動ホスト X のアドレスは 133.10.10.2 であり、その HA である HA2 のアドレスは 133.10.10.1 であるとする。また移動ネットワークの FA は MR が兼任している。X は MR(133.138.194.1) を FA として HA2 に

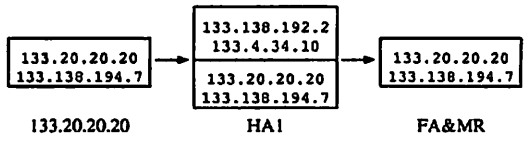

図 7: パケットヘッダの遷移その 1

登録する。ここであるホスト (133.20.20.20) から移動ホスト X へのパケットの様子を見ると以下の図 8のようになる。

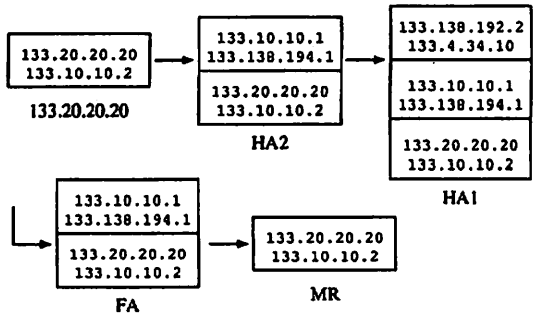

図 8: パケットヘッダの遷移その 2

5.3 問題点

- データリンクの種類分の直接通信する機構を作る必要があるので実装の効率が悪い
- トンネリングはエラーが起きた場合の通知や、無限ループの検出、フラグメントの問題などがあるため扱いが難しい
- 移動ネットワーク内に、よその移動ホストが接続してくると、トンネリングが二段階になり、さらに扱いが難しくなる

6 NAT による実現

Network Address Translator(NAT)[8] と呼ばれる方式は、当初は IP アドレスの枯渇を解消するために考案された。最近は企業などはセキュリティ対策からファイアウォール (防火壁) を構築して、インターネットと

直接接続するホストを制限し、ファイアウォールの内部はプライベートアドレスを使用するという方法が一般的に用いられているが、NATはこうした接続形態と相性がよいため、最近は当初の目的から離れた使い方をされる場合が多い。

6.1 NATの仕組み

NATルータはアドレスプールを持っており、ファイアウォールの内部のホストから接続要求があった場合、内部のアドレスとアドレスプールのうちの一つのアドレスとの対応を生成し、動的にパケットのアドレスを書き換えるという方法をとる。よって同時にファイアウォール内部の一定数以上のホストがインターネットへアクセスすることはできない。またファイアウォールの機能として当然ではあるが、インターネットから内部のホストへのアクセスが基本的には不可能である。しかし一部のホストについて静的なアドレスの対応を設定した場合、外部から内部のそのホストへのアクセスは可能である。

6.2 NATでの実現

NAT用のルータをモーバイルルータとして使用して、移動ネットワークにプライベートアドレスをつけた場合、前述したように移動ネットワーク内の機器からはインターネットにアクセスできるが、逆にインターネット上のホストから移動ネットワーク内の機器へは通常アクセスできない。この制限により例えば車内LANに接続されているGPSに外部からアクセスして、その車の位置情報を得るなどという応用が不可能になってしまう。

さらに移動ネットワーク内のホストが離脱して別のネットワークに接続した場合と、よその移動ホストが接続してきた場合には透過的な通信がおこなえない。

すなわちNAT方式は透過的に通信を継続しながら移動ネットワークを実現するという今回の目的には対応できない。

7 まとめ

現在のインターネットにおいて、ネットワークが移動することは非常に難しい。その理由は経路制御がネットワークのトポロジーが変化しないことを前提としているからである。よって各種の移動ホスト対応プロトコルをネットワーク単位での移動に対応できるように設計しなおたが、結果としてネットワーク単位での移動が現実的に可能であるのはVIP方式を拡張した場合だけである。NAT方式はそもそも移動を考慮しておらず、Mobile IP方式の拡張はトンネリングが多段になることにより制御が複雑になりすぎて実用的ではないことが判明した。

今後はVIPを改造して実装と実験をおこない、ネットワーク単位の移動への対応だけでなく、従来のホスト単位での移動においても同一のプロトコルで共存できることを確認する。また現在の設計では移動ホストが移動ネットワークに接続された場合に冗長な経路を通るが、AMTのエントリを工夫することにより最適な経路を通ることが可能かどうか検討し、さらに移動ネットワークのトポロジーが複雑な場合と、移動ネットワークに別の移動ネットワークが接続する場合の動作についても検討する予定である。

参考文献

[1] Fumio Teraoka, Keisuke Uehara, Hideki Sunahara and Jun Murai, *VIP: A Protocol Providing Host Mobility*, CACM, Vol37, No 8, Aug 1994

[2] C. Perkins, *IP Mobility Support*, Internet Draft: draft-ietf-mobileip-protocol-12.txt, Sep 1995

[3] Y. Rekhter, R. Moskowitz, D. Karrenberg, G. de Groot, *Address Allocation for Private Internets*, RFC1597, Mar 1994

[4] J. Moy, *OSPF Version 2*, RFC1583, Mar 1994

[5] V. Fuller, T. Li, J. Yu, K. Varadhan, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*, RFC1519, Sep 1993

[6] R. Droms, *Dynamic Host Configuration Protocol*, RFC1541, Oct 1993

[7] C. Perkins, *IP Encapsulation within IP*, Internet Draft: draft-ietf-mobileip-ip4inip4-00.txt, Jul 1995

[8] P. Francis, K. Egevang, *The IP Network Address Translator (Nat)*, RFC1631, May 1994