IP端末の可動性を提供する仮想サブネットワークシステムに関する検討

長谷川 輝之　　井戸上 彰　　加藤 聰彦

国際電信電話（株）　研究所

ノートパソコン等の移動可能な端末の普及に伴い、これらを移動先のネットワークに収容して、その端末が本来接続されているホームネットワークのコンピュータや、インターネットの各種サーバと通信可能とすることが望まれている。IP端末に対して可動性を提供する方式として、動的にIPアドレスを付け替えるDHCPや、移動透過なIP通信の実現を目的としたIETFのMobile-IPをはじめとする諸方式が提案されている。しかし、これらの方法には、セキュリティ、経路選択、既存装置の使用可能性などに関する問題点が指摘されている。そこで筆者らは、既存のコンピュータおよびルータをそのまま利用してIP端末に可動性を提供し、さらに移動端末からホームネットワーク以外のコンピュータと通信を行う場合にも最適な経路選択が可能な、仮想サブネットワークシステムを検討した。本稿ではその方式の概要と、システムの実装結果について述べる。

A Vitural Sub-network System Supporting Mobility of IP Terminals

Teruyuki Hasegawa　　Akira Idoue　　Toshihiko Kato

KDD R & D Laboratories

Ohara 2-1-15, Kamifukuoka, Saitama 356, JAPAN
E-Mail:{teru, idoue, kato}@hsc.lab.kdd.co.jp

According to the wide spread of mobile computer terminals, it is required to connect them to remote networks and to allow them to communicate with home computers and Internet servers. There are some mechanisms studied on the IP terminal mobility, including DHCP assigning IP addresses dynamically and Mobile-IP supporting seemless mobility. However, there are some problems identified for those methods on security, route optimization, and compatibiliy with existing IP terminals. So we have proposed a virtual sub-network system which can accomodate existing IP routers and terminals without any modifications, and which selects an optimal route for the communication with networks other than the home network. This paper describes the mechanism and the results of implementation of our system.

1 はじめに

近年、ノートパソコン等の移動可能なコンピュータ端末が広く普及しており、それに伴い、これらを移動先のネットワークに収容して、その端末が本来接続されているホームネットワークのコンピュータや、インターネットの各種サーバと通信可能とすることが望まれている。IP 端末に対して可動性を提供する方式として、動的に IP アドレスを付け替える DHCP (Dynamic Host Configuration Protocol) [1] や、移動透過な IP 通信の実現を目的とした IETF の Mobile-IP をはじめとする諸方式 [2-5] が提案されている。しかし、これらの方法には、セキュリティ、経路選択、既存装置の使用可能性などに関する問題点が指摘されている [6]。そこで筆者らは、既存のコンピュータおよびルータをそのまま利用して IP 端末に可動性を提供し、さらに移動端末からホームネットワーク以外のコンピュータと通信を行う場合にも最適な経路選択が可能な、仮想サブネットワークシステムを検討した。本稿ではその概要について述べる

2 設計方針

仮想サブネットワークシステムの設計にあたり、以下の方針を立てた。

(1) 遠隔とホームのサブネットワークに、仮想サブネットワークゲートウェイ (VSG : Virtual Subnetwork Gateway) を用意する。

(2) 遠隔サブネットワークに移動端末を接続する時点で、ホームサブネットワークにアクセスできる端末かどうかの認証を行う。

(3) 遠隔サブネットワークで移動端末が送信する IP パケットは、原則として、全て遠隔の VSG(VSGr) が受信して処理する。一方、ホームサブネットワークで送信される移動端末宛の IP パケットは、全てホームの VSG(VSGh) が取り込んで処理する。

(4) ホームサブネットワークとの間で転送される IP パケットは、VSGr と VSGh 間で中継する。

(5) ホームサブネットワーク以外の端末に対して、移動端末から TCP による通信を開始する場合は、VSGr が宛先の端末と直接通信する。

3 通信手順

以下では、移動端末を遠隔サブネットワークに接続し、他の端末との IP 接続を行うための通信手順について説明する。

3.1 移動端末の認証とホームサブネットワークへのコネクション確立

図 1に示すように、移動端末 (図中 C) を遠隔サブネットワークに接続し、VSG を介した通信を行うために、以下の手順により、VSG 間で移動端末の認証ならびにパケット転送用 TCP コネクションの確立を行う。

(1) VSGr と VSGh に以下の情報を登録しておく。

・ 移動端末の IP アドレス (Cip) と MAC アドレス (Cmac)。

・ ホームサブネットワークのネットワークアドレスとサブネットマスク。

・ 相手 VSG の IP アドレス (VHip または VRip)。

(2) VSGr は、VSGh との間に認証用 TCP コネクションを (既に設定済でなければ) 設定する。

(3) VSGr から VSGh に対して、Cmac と Cip をパラメータとして認証要求を送信する。

(4) VSGh は、受信した認証要求の正当性をチェックし、正しい場合は VSGr へ認証確認を返す。

(5) VSGr では、認証が成功すると、さらに、VSGh との間にパケット転送用の TCP コネクションを (既に設定済でなければ) 設定する。VSGh では Cip とパケット転送用 TCP コネクションの対応を記録する。

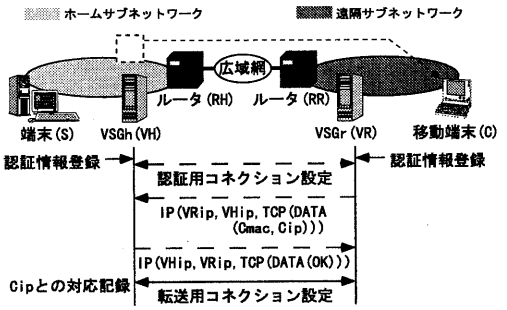

図 1: 移動端末の認証と転送用 TCP コネクションの確立

3.2 ARP を用いた移動端末の収容

IP を使用する端末は、自身と同じサブネットワークに属する他の端末やルータに IP パケットを転送するために、相手端末の MAC アドレスを

調べる ARP (Address Resolution Protocol) を使用する。VSG では、これを利用して移動端末を収容する (図 2参照)。以下にその手順を示す。

(1) 移動端末では、ホームサブネットワークの端末 (S) やルータ (RH) と通信する前に、ARPrequest パケットをブロードキャストする。

(2) VSGr は、ARPrequest の発IP アドレスが、登録された移動端末のもの (Cip) であれば、その着 IP アドレス (Sip) に対応する MAC アドレスとして VSGr の MAC アドレス (VRmac) を ARPreply パケットで返す。これにより、移動端末は宛先が VRmac である MAC フレームを用いて IP パケットを送出する。従って、VSGr は移動端末が送信する IP パケットを全て取り込むことが可能となる。

(3) 一方、ホームサブネットワークでは、移動端末宛の ARPrequest に対して、VSGh が自身の MAC アドレス (VHmac) を ARPreply パケットで返すことにより、移動端末宛の IP パケットを全て取り込む。

ただし、遠隔サブネットワークに接続された、同一のホームサブネットワークに属する移動端末間の通信については、以下の手順により、移動端末間で直接通信を行わせる (図 2参照)。

(1) VSGr は、ARPrequest の発着 IP アドレスが、共に、登録済かつ同一ホームサブネットワークに属する移動端末のもの ((Cip,C'ip) またはその逆) であれば、ARPreply による応答を行わない。

(2) ARP によるアドレス解決は、移動端末間において通常通り行われる。その結果、移動端末間で直接 IP パケットが交換される。

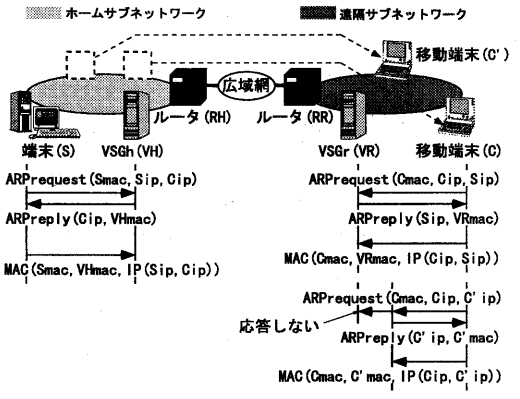

図 2: ARP を用いた移動端末の収容

3.3 ホームサブネットワークの端末との通信

移動端末とホームサブネットワークに接続された端末との間で交換される IP パケットは、図 3) に示すように、全て VSGr と VSGh 間に設定されたパケット転送用の TCP コネクションを用いてカプセル化され転送される。以下にその手順を示す。

(1) VSGr は、移動端末から受信した IP パケットの宛先 IP アドレスを調べ、登録されたホームサブネットワーク宛であれば、パケット転送用の TCP コネクションを用いて、IP パケットをカプセル化し、VSGh へ転送する。

(2) VSGh では、転送された IP パケットからもとの IP パケットを取り出し、ホームサブネットワークの端末へ送信する。

(3) 一方、ホームサブネットワークの端末から移動端末宛の IP パケットは、VSGh により取り込まれ、VSGr へ転送される。

(4) VSGr は、転送された IP パケットからもとの IP パケットを取り出し、宛先の移動端末へ送信する。

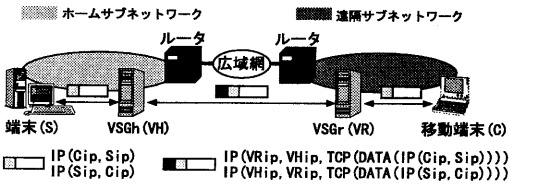

図 3: ホームサブネットワークの端末との通信

3.4 ホーム以外のサブネットワークの端末との通信

移動端末が、遠隔サブネットワークからホーム以外のサブネットワークの端末と通信する場合は、以下で説明するように、使用している上位プロトコル等に応じた手順を用いる。

3.4.1 移動端末からの TCP 発信に対する手順

図 4のように、移動端末から相手端末に TCP コネクション確立を要求した場合は、VSGr が、通信の開始から終了まで、一貫して移動端末の代理として通信 (以下、代理通信と呼ぶ) を行うことで、ホームネットワークを経由しない通信が可能であ

る。以下では、代理通信を実現するための具体的な手順について説明する。

(1) VSGr は、移動端末から受信した IP パケットを解析し、TCP パケットの場合は (2) 以降の処理を行う。そうでない場合は、3.4.2節の手順に従って IP パケットを処理する。

(2) パケットが、TCP コネクションを確立するための SYN パケットであれば、VSGr は、代理通信を行うために、TCP ポート番号 (VRport) を取得し、このコネクションを管理するためのテーブルを生成する。そして、受信した SYN パケットの発信側の IP アドレス (Cip) と TCP ポート番号 (Cport) を、VSGr の IP アドレス (VRip) と VRport に書き換え、遠隔サブネットワークのルータを介して相手端末に送信する。

(3) SYN 以外のパケットの場合は、VSGr は、発着の IP アドレス (Cip,Hip) と TCP ポート (Cport,Hport) からコネクション管理テーブルを検索し、あればその情報に従って発信側の IP アドレスと TCP ポート番号を書き換えて送信する。ない場合は、3.4.2節の手順に従って IP パケットを処理する。

(4) 一方、相手端末からの IP パケットは、宛先として VRip と VRport を持つ。VSGr では、自身宛の IP パケットが受信されると、コネクション管理テーブルを検索して、移動端末に中継すべきパケットと自身宛の通常の TCP/IP パケットを識別する。そして、前者であれば、TCP と IP のヘッダを書き換えて移動端末へ送信する。

(5) VSGr では、TCP のコネクションの解放または切断を監視し、TCP の手順に従ってコネクションテーブルを解放する。

(6) 上記の手順を用いる場合、チェックサムの検査は、TCP コネクションの確立、解放、切断に関わるパケットについてのみ行い、データ転送中の処理オーバヘッドを削減する。

3.4.2 TCP 発信以外に対する手順

コネクションレス型の UDP や ICMP を用いた通信では、TCP と異なり通信開始・終了を識別することが困難である。また、相手端末から確立された TCP コネクションでは、相手端末が宛先に移動端末の IP アドレスを指定してパケットを送信するため、3.4.1節の手順を使用することが不可能である。そこで、このような場合は以下の手順

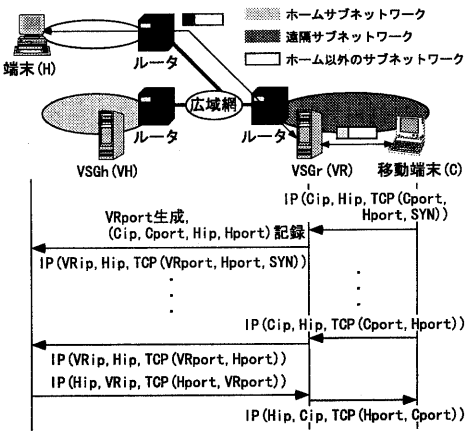

図 4: ホーム以外のサブネットワークとの通信 (1)

により通信を行う (図5参照)。

(1) 移動端末から受信した IP パケットについては、VSGr の設定に応じて、以下に示す手順のどちらかを用いる。

[設定 1] VSGr は、移動端末から受信した IP パケットを、そのまま遠隔サブネットワークのルータ経由で相手端末に送信する。

[設定 2] VSGr は、移動端末から受信した IP パケットを、カプセル化して VSGh に転送する。VSGh は、もとの IP パケットを取り出して、ホームサブネットワークのルータ経由で相手端末に送信する。

(2) 一方、相手端末からの IP パケットは、ホームサブネットワークのルータを経由して VSGh に取り込まれ、カプセル化されて VSGr に転送される。VSGr は、もとの IP パケットを取り出して、移動端末へ送信する。

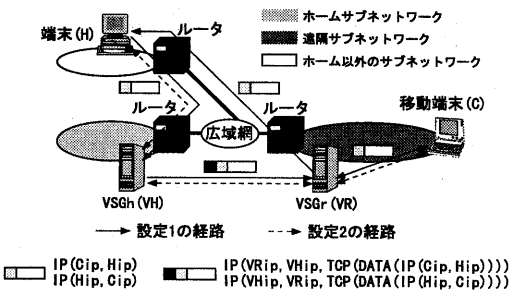

図 5: ホーム以外のサブネットワークとの通信 (2)

4 VSGの実装

4.1 プログラム構成

3節の手順を実現するVSGを、PC上で動作するUNIX OSであるLinux 2.0.28上に実装した。図6にVSGのプログラム構成を示す。VSGプログラムは、ユーザプロセスとして動作するVSGデーモンプログラムと、カーネル内で動作するVSGカーネルモジュールにより構成される。以下、前者をVSGデーモン、後者をVSGカーネルと呼ぶ。VSGデーモンでは、移動端末の登録/削除/認証などの管理機能、ならびに、VSG間のパケット転送機能を実現する。一方、VSGカーネルでは、移動端末またはホームネットワークの端末になりすますためのARP処理やIP処理、ならびに、TCPの代理通信処理を実現する。なお、VSGデーモンとVSGカーネルの間では、OSの提供するNETLINKドライバを用いて送受信パケットや制御メッセージの交換を行っている。また、OSの提供するIP、ARPモジュールのソースコードを変更し、EthernetドライバからIPもしくはARPに入力されたパケットは、全てVSGカーネルを経由させ、VSGカーネルで必要なパケットを選別することとした。

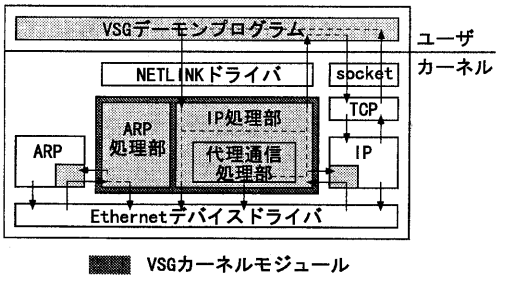

図 6: VSGのプログラム構成

4.2 処理の流れ

VSGプログラムにおける処理の流れは以下の通りである。

(1) 認証ならびに転送用のTCPコネクションは、それぞれ、VSGデーモン間でsocketインタフェースを用いて設定される。移動端末の認証に成功すると、双方のVSGデーモンは、VSGカーネルに移動端末のIPアドレスと対応するVSG処理(VSGr側もしくはVSGh側)を通知する。

(2) VSGデーモンでは、転送用コネクションから受信したIPパケットをNETLINKドライバ経由で、VSGカーネルのIP処理部に渡す。また逆にIP処理部から受信したIPパケットについては、対応する転送用コネクションから出力する。

(3) VSGカーネルのARP処理部は、移動端末発もしくは移動端末宛のARPrequestを選別して、必要に応じてVSGのMACアドレスを持つARPreplyを返す。

(4) IP処理部は、VSGデーモンもしくはOSのIPからIPパケットを受け取る。VSGデーモンからのIPパケットは、OSのIPルーチングテーブルを参照して、適切なデバイスから出力する。一方、IPからの入力については、発着IPアドレスから、処理すべきパケットを選別し、さらに上位プロトコル等に応じて、パケットをVSGデーモン、代理通信処理部、デバイスドライバのいずれかに渡す。

(5) 代理通信処理部は、TCPパケットの種別ならびに対応するコネクション管理テーブルを調査し、必要に応じて、テーブルの生成/削除やパケットヘッダの書き換えを行う。パケットはIP処理部を通じてデバイスから出力する。なお、代理通信に必要なVSGrのTCPポート番号については、一定数を予めカーネルから確保しておく。

4.3 動作検証

VSGプログラムの動作を検証するため、2台のIBM/PC互換機(Pentium(P5) 166MHz/Pentium Pro 200MHz)上にプログラムを実装し、3節で述べたネットワーク環境を構築して、端末間のIP接続を確認した。この際、端末として2台のノートPC(P5 150MHz/90MHz)を使用し、LANならびに広域網はイーサネットで構築した。なお、図3、4の環境における端末間のftpファイル転送のスループットは、共に4Mbps程度であった。

5 考察

(1) 1節で述べたように、IP端末の可動性を提供する方式は多く提案されている。本方式の特徴およびこれらの方式との比較は、以下のようになる。

・ 本方式は、DHCP [1]と異なり、移動端末への着信なども含めた、移動透過な可動性の実現を目的としている。

・ 可動性を提供するためには、VSGを追加するのみで、移動端末やルータなどの設備に新しい機

能を追加する必要はない。この特徴は、新規プロトコルを導入したり、ルータや端末に別プログラムを追加するVIP [3] やHMSP [4] と異なり、本システムの導入を容易にしている。

・ 本方式では、遠隔サブネットワークとホームサブネットワークの間で交換されるデータはすべてVSGrとVSGhを経由して中継される。これはMobile-IP [2] と異なる特徴である。これにより、VSGrとVSGhの間にTCP通信を高速化するゲートウェイ機能 [7] を追加するなど、可動性の提供に加えて、他の付加機能の追加が可能となる。

・ 本方式は、ホーム以外のネットワークのコンピュータと通信する場合は、移動端末からのTCP発信時に、VSGrからの最適な経路を選択することができる。これは、必ずホームのネットワークを中継するMobile-IPや、データリンクレベルの機能を用いた仮想サブネットワークシステム [5] などに対する利点である。

(2) 現在多くの組織においては、外部からの組織内のLANへのアクセスに対するセキュリティを確保するために、ファイアウォールを採用している。このようなLANにおいては、以下のような手順を用いることにより、本方式を使用することができる。ホームのLANにおいてファイアウォールが使用されている場合は、VSGrからVSGhへのTCPコネクションの着信を許可する設定を追加するのみでよい。また、遠隔のLANにおいては、VSGrからのTCPコネクションの発信のみを許可する設定を行い、また、3.4.2節で述べたTCP発信以外に対する手順については、VSGh経由でパケットを転送する設定2を用いる。

(3) ホーム以外のサブネットワークとのUDP、ICMPを用いた通信においても、上位プロトコルの処理やICMPメッセージの内容から通信の開始・終了を識別できる場合は、TCPと同様の代理通信が実現できる。例えば、pingで使用するICMP echoのrequestとreplyに対して、以下の手順が考えられる。

・VSGrでは、移動端末からのICMP echo requestのヘッダを書き換え相手端末に送信する。この際、書き換え前後のヘッダの一部を記録しておく。

・ VSGr宛のICMP echo replyが戻ると、元のヘッダを復元し移動端末に送信する。

・ 連続したICMP echo request受信ならびにパケット紛失を考慮して、ヘッダの記録は一定時間保持した後に削除する。

(4) 設置すべきVSGの数は、サブネットワーク毎に1つとなり、例えば、ホームのLANが複数のサブネットワークから構成される場合は、それぞれ1つのVSGhが必要となる。これはMobile-IP、HMSP、データリンクレベルの機能による仮想サブネットワークシステムなどと同様である。しかし、ホームのコンピュータから移動端末への発信を行わないという条件の下では、ホームのLAN全体に対して、1つのVSGhのみで対応することも可能であると考えられる。

(5) VSGを介した通信のスループットは4Mbps程度であるが、これはVSGがLANから受信したパケットを再度同一LANへ送信するため、LAN内のトラヒックが2倍になり、イーサネットの帯域がボトルネックとなることが原因である。これに対処するため、VSGプログラムでは、取り込んだパケットをIPルーチングして別セグメントから送信することを可能としている。端末間のスループットを向上させるためには、この機能を用いるか、または100Base-T等の高速ネットワークを用いることが必要であると考えられる。

6 おわりに

本稿では、IPレベルのプロトコル処理を用いて、移動端末をそのまま他のサブネットワークに収容して、他の端末との移動透過なIP接続を可能とする、仮想サブネットワークシステムについて検討を行った。さらに、検討結果に基づき、システムを実装しその動作を検証した。最後に日頃御指導頂くKDD研究所村上所長に感謝します。

参考文献

[1] R. Droms, "Dynamic Host Configuration Protocol," RFC 1541, Oct. 1993.
[2] C. Perkins, "IP Mobility Support," RFC2002, Oct. 1996.
[3] F. Teraoka, et. al., "VIP : A Protocol Providing Host Mobility," CACM, Vol.37, No.8 Aug. 1994.
[4] 重野他, "インタネット上でホスト移動をサポートするプロトコルHMSP," 信学論, Vol.J80-B-I No.3, March 1997.
[5] 執行他, "バーチャルLANにおけるアドレス解決方式の一検討," 1996信学総合全大, B-809, Mar. 1996.
[6] 寺岡, "移動透過な通信を実現するプロトコル," 信学会誌, Vol.80, No.4, April 1997.
[7] 長谷川他, "広域ATM網を介したLAN間接続のためのTCPゲートウェイの実装と評価," 信学論, Vol.J79-B-I No.5, May 1996.