

VIP: 仮想インターネットプロトコル

寺岡文男、横手靖彦、所 真理雄
(株) ソニーコンピュータサイエンス研究所

コンピュータネットワークの普及とコンピュータの小型化・高性能化に伴い、ユーザは自分のコンピュータと共に広域ネットワーク内を移動するようになる。このような環境ではホスト移動透過性が重要になる。筆者らはホスト移動透過性を実現するための新しいネットワーク・アーキテクチャを提案しているが、本論文ではこのアーキテクチャをインターネット・プロトコル (IP) に適用した仮想インターネットプロトコル (VIP) を提案する。VIP を使用することにより、ホストの移動に関わりなく相手ホストと IP データグラムの通信ができるようになる。

VIP: Virtual Internet Protocol

Fumio Teraoka, Yasuhiko Yokote, and Mario Tokoro
Sony Computer Science Laboratory Inc.
3-14-13 Higashigotanda, Shinagawa-ku, Tokyo 141, Japan

Expansion of computer networks and miniaturization of computers lead to migration of users with their computers across wide area networks. In such environment, host migration transparency becomes more and more important. The authors proposed a new network architecture to provide host migration transparency. This paper proposes Virtual Internet Protocol (VIP) by applying the architecture to Internet Protocol (IP). VIP enables the communication of IP datagram regardless of the migration of target hosts.

1 はじめに

現在のコンピュータの利用形態は大きく 2 つに分類できる。1 つは固定されたコンピュータ (または端末) を利用する形態であり、もう 1 つは携帯型のコンピュータを持ち運び、スタンドアロンで使用したり電話線などを使って固定されたコンピュータの端末として使用する形態である。近い将来、高機能で通信機能も豊富なコンピュータが携帯可能なほど小型化され、コンピュータネットワークもさらに普及して世界規模の分散計算機環境が構築されると、各ユーザは自分のコンピュータを携帯し、移動した先々でネットワークに接続して使用するようになるであろう。しかしいつもと同じ計算機環境を得るために、異なったネットワークに接続するたびにシステムの再設定や再コンパイルの必要があるのなら、ユーザはコンピュータを持ち運ばないであろう。従って、ユーザが広域ネットワークのどの地点にコンピュータを接続しても常に同じ計算機環境をユーザに提供するという性質、すなわち「ホスト移動透過性」が重要になる。

ホスト移動とは、簡単にはホストがあるサブネットワークから別のサブネットワークに移動することであると定義できる。従ってホスト移動はホストのネットワークアドレスの変化を伴う。OSI のネットワークアーキテクチャ [ISO 84] や DARPA のプロトコル群のような既存のプロトコルはホストの移動を考慮していない。また Mach [Accetta 86]、V-system [Cheriton 88]、Chorus [Rozier 88] などの分散システムも開発されており、これらはネットワーク透過性は実現しているが、ホスト移動はやはり考慮していない。例外として Amoeba は同報通信パケットが届くサブネットワークの範囲でホスト移動をサポートしている [Tanenbaum 91]。しかしこれらのシステムでは、移動ホストと通信するためにはユーザが相手ホストの位置を考慮しなければならない。

筆者らは、ホスト移動透過性はネットワークレイヤで実現すべきであると考え、ホスト移動透過性を提供する新しいネットワークアーキテクチャを提案している [Teraoka 91b]。本論文ではこのアーキテクチャをインターネットプロトコル (IP) に適用し、仮想インターネットプロトコル (VIP) を提案する。VIP を使用することにより、相手ホストの移動に関わりなく IP データグラムの通信が可能になる。第 2 章ではホスト移動透過性とは何か、どのレイヤで実現すべきか、について議論する。第 3 章ではホスト移動透過性を実現するために「仮想ネットワーク」という概念を導入し、これを効率良く実現するために従来のネットワークレイヤを 2 つのサブレイヤに分割する。第 4 章では「拡散キャッシュ法」

に基づいた仮想ネットワークプロトコルを提案する。第 5 章で本論文のまとめを述べる。

2 ホスト移動透過性

広域ネットワークは多くのローカル・ネットワーク (またはサブネットワーク) の相互接続によって構成されており、コンピュータは一時には 1 つのサブネットワークに接続されている。このような環境では、ホスト移動とはホストがあるサブネットワークから他のサブネットワークへ接続点を変えることであると定義できる。従ってホスト移動はホストのネットワークアドレスの変化を伴う。ネットワークアプリケーションはアプリケーション・エンティティが相互に通信しながらユーザにそのサービスを提供する。ホストが移動してそのホストのネットワークアドレスが変化すると、そのホスト上のアプリケーション・エンティティの識別子も変化してしまうため、それまでと同じ計算機環境を得るには、システムの再設定やソフトウェアの再コンパイルが必要になってしまう。このようにユーザレベルにおけるホスト移動透過性とは、「ホストを広域ネットワークのどの地点に接続しても、いつも同じ計算機環境が得られること」と定義できる。一方アプリケーション・エンティティの識別子は、一般的に「ホストの識別子 + ホスト内での識別子」という構造を持っている。ホストの識別子がホスト移動によって変化しなければ、アプリケーション・エンティティは相手の移動を意識すること無く、常に相手を正しく認識して通信することができる。そうすればアプリケーション・エンティティはホスト移動に関わらず、常に同じ計算機環境をユーザに提供できる。従ってシステムレベルにおけるホスト移動透過性とは「位置や移動に関わらないホストの識別子を提供すること」と定義できる。

OSI のネットワーク・アーキテクチャは 7 層モデルに基づいている。このアーキテクチャに従えば、第 4 層 (トランスポートレイヤ) 以下のレイヤが end-to-end の通信を提供する。このうち、第 2 層 (データリンクレイヤ) は特定の通信媒体上での point-to-point の通信手段を提供し、第 3 層 (ネットワークレイヤ) は相互に接続されたサブネットワーク間での最終的な host-to-host の通信を提供する。このサービスの上にトランスポートレイヤが end-to-end の通信を提供するのである。従って広域ネットワークにおいてホストを認識するのはネットワークレイヤであり、ホスト移動透過性すなわちホスト移動に関わらないホストの識別子を提供するのはネットワークレイヤのサービスであると考えられる。

ホスト移動透過性をネットワークレイヤが実現した場合、トランスポートレイヤは相手ホストを位置や移動に関わらない識別子で指定することになる。ネットワークレイヤはこの識別子を元にパケットを相手ホストに届けなければならない。このように、ホスト移動透過性をネットワークレイヤで実現する場合、通常のサービスに加えてネットワークレイヤには次の 2 つのサービスが必要になる。

- 「移動透過ホストアドレスング」：位置や移動に関わらないホストの識別子を上位レイヤに提供する機能。
- 「移動透過コネクションレス型通信」：相手ホストの位置や移動に関わらずにコネクションレス型通信を行なう機能。

次章でこの 2 つのサービスを効率良く提供するネットワークアーキテクチャを提案する。

3 仮想ネットワーク

3.1 概念

既存のネットワークではホストのネットワークレイヤ・アドレスは以下のような階層構造を持っている。

- (a) area address + ID + SEL
- (b) network number + host number

(a) は OSI [ISO 90] のネットワークレイヤ・アドレスであり、(b) は XNS [Xerox 81] や DARPA-IP [SRI 81] のネットワークアドレスである。ここで area address はルーティング・ドメイン、ID はそのドメイン内でユニークな番号、SEL はパケットを受け取る上位レイヤのエンティティを表すセレクトである。XNS では host number はシステムを通じて一意であり、network number はルーティングを容易にするために付加されている。DARPA-IP では network number はシステムを通じて一意であり、host number はそのネットワークの中で一意である。一般的にホストアドレスは (b) のような 2 階層の階層構造を持っていると仮定できる。このようなアドレスを規定しているネットワークでは、ホストが他のネットワークに移動すればそのホストのアドレスも変化してしまう。

筆者らはネットワークレイヤでホスト移動透過性を実現するために「仮想ネットワーク」という概念を導入した [Teraoka 91b]。仮想ネットワークとは現実のネット

ワークの上に存在する論理的なネットワークである。現実のネットワークを以後「物理ネットワーク」と呼ぶことにする。仮想ネットワークは相互接続された論理的なネットワークを物理ネットワーク上に形成する。トランスポートレイヤからは仮想ネットワークの世界のみが見えるようになる。各ホストは 1 つの物理ネットワークに接続されると同時に 1 つの仮想ネットワークにも接続される。物理ネットワーク上でホストが移動しても、仮想ネットワークの世界ではホストは移動しない。すなわち、各ホストは常に 1 つの仮想ネットワークに接続されていると考えるのである。このようなネットワークを、そのホストの「固有ネットワーク」と名付ける。各ホストは物理ネットワークにおいてネットワークアドレス (これは「物理ネットワークアドレス」(PN-アドレス)とも呼べる) を持つが、これと同時に仮想ネットワークにおいては「仮想ネットワークアドレス」(VN-アドレス)をも持つ。ホストは仮想ネットワーク上では移動しないので、たとえホストが物理ネットワーク上で移動してもそのホストの VN-アドレスは変化しない。ホストの PN-アドレスはそのホストの物理ネットワーク上での位置を表し、パケットの経路制御に利用される。トランスポートレイヤからは相手ホストがどこに移動しても VN-アドレスで相手を指定することができるようになる。基本的には PN-アドレスはトランスポートからは見えない。VN-アドレスと PN-アドレスは同じフォーマットを持つ。

ホストの仮想ネットワークアドレスと物理ネットワークアドレスの関係は、仮想メモリシステムにおける仮想アドレスと物理アドレスの関係と似ている。仮想メモリシステムにおいては、プログラムが物理メモリのどこに配置されようともそのプログラム中で使われている仮想アドレスは変化しない。同様に物理ネットワーク上でホストがどこに移動してもそのホストは仮想ネットワークアドレスで指定できる。

3.2 プロトコル階層

トランスポートレイヤは相手ホストを VN-アドレスで指定するので、パケットを配送するには VN-アドレスに対応する PN-アドレスに変換する必要がある。ネットワークレイヤはホスト間通信サービスを提供しており、これはパケットの中継、経路制御等のファンクションで実現されている。仮想ネットワークのためのアドレス変換はこのようなネットワークレイヤの基本的なファンクションとは異質であるので、本ネットワーク・アーキテクチャではネットワークレイヤを以下に示す 2 つのサブ

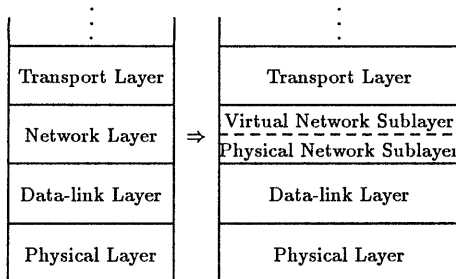


図 1: プロトコル階層

レイヤに分割する。(図 1 参照)。

- 「仮想ネットワーク・サブレイヤ」(VN-サブレイヤ): 物理ネットワーク上でのホストの位置を隠蔽する。ホストには仮想ネットワークアドレス (VN-アドレス) が割り当てられる。VN-アドレスは対応する物理ネットワークアドレス (PN-アドレス) に変換される。
- 「物理ネットワーク・サブレイヤ」(PN-サブレイヤ): 従来のネットワークレイヤである。このサブレイヤはパケットの中継、経路制御情報の交換等を行なう。ホストには物理ネットワークアドレス (PN-アドレス) が割り当てられる。

この分割により、(物理) ネットワークレイヤ・ヘッダとトランスポートレイヤ・ヘッダの間に VN-サブレイヤ・ヘッダが追加される。もし受信したパケットの(物理) ネットワークレイヤ・ヘッダが、上位レイヤとして VN-サブレイヤを指定していれば、このパケットは VN-サブレイヤに渡される。そうでなければ VN-サブレイヤはバイパスされ、そのパケットはトランスポートレイヤに渡される。このように、受信されたパケットが VN-サブレイヤ・ヘッダを持っていなかったり、受信したホストが VN-サブレイヤを実装していない場合は、VN-サブレイヤをバイパスすることが可能である。

4 仮想インターネットプロトコル

仮想ネットワークの概念を DARPA-IP に適用させたものが仮想インターネットプロトコル (VIP) である [Teraoka 91a]。従来の IP レイヤは VIP-サブレイヤと IP-サブレイヤという 2 つのサブレイヤに分割される。IP-サブレイヤの役割は従来の IP-レイヤのものと同じである。VIP-サブレイヤはホスト移動透過性を提供する。

4.1 IP-アドレスと VIP-アドレス

第 3.1 章で述べたようにホストは VN-アドレスと PN-アドレスという 2 つのアドレスを持つ。VIP においては、VN-アドレスとして VIP-アドレスを導入する。従来の IP アドレスは PN-アドレスとして働く。両方のアドレスのフォーマットは同じである。ホストが移動すると IP-アドレスは変化するが VIP-アドレスは不変である。トランスポートレイヤは VIP-アドレスを用いて相手ホストを指定するので、相手ホストの移動や位置に関わりなく相手ホストと通信を行なうことができる。VIP の環境では、PN-アドレスとしての IP-アドレスはトランスポートレイヤからは見えなくなる。各ホストは通常接続されている 1 つのネットワークを持つ。これがそのホストの固有ネットワークである。固有ネットワークにおけるホストのアドレスが、そのホストの VIP-アドレスとなる。固有ネットワークにおいては VIP-アドレスと IP-アドレスは等しい値を持つ。

ホストが固有ネットワーク以外のネットワークに接続されるとき、PN-アドレスとしての IP-アドレスをそのホストに割り当てなくてはならない。このような IP-アドレス割り当てには、reverse-arp のようなプロトコルを用いればよい。すなわち各ローカルネットワークに割り当てサーバを導入し、移動ホストが同報通信した割り当て要求に対し、サーバがアドレスプールから IP-アドレスを割り当てるようにすればよい。

4.2 拡散キャッシュ法

VIP-サブレイヤは VIP-アドレスを IP-アドレスに変換しなければならない。アドレス変換にはいくつかの可能な方法が考えられる。本論文では、アドレス変換のオーバーヘッドをなるべく小さくするために「拡散キャッシュ法」を導入する。この方法は遅延評価の範疇に入る。この方法では、各ゲートウェイ/ホストはアドレス変換のためのキャッシュを保持する。送信側ホストが受信側ホストの IP-アドレスを知らない場合、送信側ホストは相手ホストが固有ネットワークに接続されていると仮定する。すなわち送信側は受信側ホストの IP-アドレスが VIP-アドレスと等しいと仮定するのである。送信されたパケットは受信側ホストの固有ネットワークに向かって転送されていく。経路上のゲートウェイが受信側ホストに関するキャッシュを保持していればそのゲートウェイでアドレス変換が行なわれ、パケットは受信側ホストの物理的な位置にフォワードされる。

基本的にホストの IP-アドレスと VIP-アドレスの関

係は、そのホストの固有ネットワーク内のホスト/ゲートウェイで管理される。最悪の場合、移動ホストに対して送信されたパケットはそのホストの固有ネットワークでフォワードされる。しかし通信が行なわれるにつれてキャッシュの情報が他のゲートウェイにも拡散していくため、多くのパケットは経路上のゲートウェイでフォワードされることになる。(第 4.5 章参照)。さらに移動ホストからパケットを受信すればそのホストの IP-アドレスがわかるので、それ以降は移動ホストに直接パケットを送信することができるようになる。キャッシュ情報の拡散は次の 2 つの事象による。1 つは VIP-サブレイヤのコントロールパケット送信、もう 1 つは通常のデータパケット送信である。コントロールパケットはホストがネットワークに接続されたり切断されたりするときに送信される。送信側ホストの VIP-アドレスおよび IP-アドレスはどちらのパケットタイプのヘッダにも含まれているので、ゲートウェイはパケットを中継するときにヘッダの内容を盗み見て自分のローカルキャッシュを更新するのである。

各ゲートウェイ/ホストで保持されるキャッシュを「アドレス変換テーブル」(AMT)と呼ぶ。ゲートウェイ/ホストがパケットを受信したとき、送信側ホストの IP-アドレスが VIP-アドレスと異なっていると送信側ホストに関する AMT エントリが作成/更新される。AMT エントリは次の 4 つのフィールドからなる。

- 仮想ネットワークアドレス (AMT_{VnAddr}): エントリに対するキーの役割を果たす。
- 物理ネットワークアドレス (AMT_{PnAddr}): 求めたい値。
- 送信側アドレス・タイムスタンプ (AMT_{SrcTS}): このエントリが無効かどうかを判断するためのタイムスタンプ。
- アイドル時間 (AMT_{idle}): 使用されていないエントリを消去するためのタイマ。

4.3 ヘッダフォーマット

本論文で提案している VIP パケットヘッダは、IP パケットヘッダのオプションとして実装することを考えている。こうすることにより、ゲートウェイが VIP を実装していなくてもそのゲートウェイは VIP パケットを中継することが可能になる。VIP ヘッダは次の 8 つのフィールドからなる (図 2 参照)。

- オプションタイプ ($VIP_{OptType}$) およびオプション長 (VIP_{OptLen})。これらのフィールドはオプションのために IP で定義されている。 $VIP_{OptType}$ フィールドには VIP を示す値がセットされる。 VIP_{OptLen} にはこれら 2 つのフィールドを含む VIP ヘッダの長さ (20 バイト) がセットされる。
- プロトコル (VIP_{proto})。上位レイヤプロトコル、すなわち TCP または UDP を示す。
- VIP タイプ (VIP_{type})。VIP パケットのタイプを示す。以下に示す 5 つのタイプがある。
 - $VipData$: 通常のデータパケット。
 - $VipDisc$: 送信側ホストがネットワークから切断されようとしていることを伝えるパケット。
 - $VipConn$: 送信側のホストがネットワークに接続されたことを伝えるパケット。
 - $VipConnAck$: $VipConn$ パケットの確認応答パケット。
 - $VipErrObs$: 無効な AMT エントリが発見されたことを示すエラー通知パケット。
- 送信側 VIP-アドレス ($VIP_{SrcAddr}$) および受信側 VIP-アドレス ($VIP_{DestAddr}$)。
- 送信側アドレス・タイムスタンプ (VIP_{SrcTS})。送信側ホストにおける送信開始時の時刻を示す。送信側ホストに関する AMT エントリが作成/更新されるとき、このフィールドの値が AMT_{SrcTS} フィールドにセットされる。AMT エントリの更新は、このフィールドの値が AMT エントリの AMT_{SrcTS} フィールドの値より新しいときに行なわれる。
- 受信側アドレス・タイムスタンプ (VIP_{DestTS})。受信側ホストの VIP-アドレスが IP-アドレスに変換されるとき、このフィールドには AMT エントリの AMT_{SrcTS} フィールドの値がセットされる。アドレス変換は、このフィールドの値が受信側ホストに関する AMT エントリの AMT_{SrcTS} フィールドの値より古いときに行なわれる。

受信側ホストに関する AMT エントリが無効になっているかを判断するため、2 つのタイムスタンプ、すなわちパケットの VIP_{DestTS} フィールドと AMT エントリの AMT_{SrcTS} フィールド、が比較される。これはシステムに含まれるすべてのホストでクロックの同期が必要であることを求めている。なぜなら、これら 2 つの

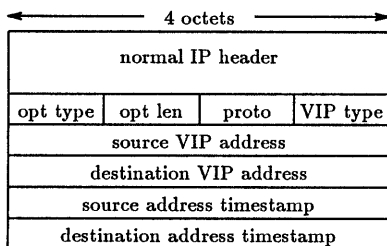


図 2: VIP ヘッダフォーマット

タイムスタンプは同一のホストのクロックから発生しているからである。システムに含まれる各ホストのクロックが単調に増加しさえすれば、AMT が無効かどうかのチェックは正しく行なわれる。

4.4 送受信処理

送信、中継、受信の手続きは以下の通りである。送信側ホストが受信側ホストに関する AMT エントリを保持していた場合、送信側ホストは AMT エントリに保持されている値をパケットの IP ヘッダの destination IP address フィールドにセットする。そうでない場合、送信側ホストは受信側ホストの IP-アドレスが VIP-アドレスに等しいと仮定する。送信されたパケットはゲートウェイをホップしていく。各ゲートウェイでは、必要であれば送信側ホストに関する AMT エントリが作成/変更され、また必要であれば受信側ホストに関する AMT エントリに従って、パケットの IP ヘッダ中の destination IP address が修正され、パケットが中継される。受信側ホストでは、送信側ホストに関する AMT エントリが作成/変更される。

IP においてパケットをサブネットワークに送出するとき、そのサブネットの最大送信長がパケット長よりも小さいと、パケットはより小さなフラグメントに分割される可能性がある。これらのフラグメントは、受信側ホストで元のパケットに組み立てられる。この処理は fragmentation(分割) と reassembly(再組み立て) と呼ばれる。パケットの分割が起こると、IP のオプションとして IP ヘッダに組み込まれている VIP ヘッダは各フラグメントにコピーされなければならない。IP においては送信側/受信側の IP アドレスと ID フィールドがフラグメントの識別子として使用されるが、VIP では送信側/受信側の VIP アドレスが IP アドレスの代わりに用いられる。

また IP においては 8 つのオプションが定義されている。これらのオプションは、Loose/Strict Source Routing

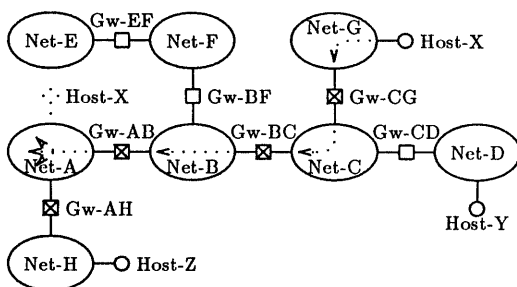


図 3: ネットワークへの接続

を除いて VIP と整合している。ソース・ルーティングという考え方自体は移動適過という考え方とは矛盾するので、これら 2 つのオプションは使うべきではないと考える。しかしこれらのオプションは IP アドレスと VIP アドレスが常に等しい固定されたホストに対しては適用可能である。

4.5 ホスト移動

図 3 にホスト移動時のパケットの流れを示す。図において、楕円はサブネットワーク、小さな円はホスト、正方形はゲートウェイを表す。図では Host-X が Net-A から Net-G へ移動している。ここで Host-X の固有ネットワークは Net-A と仮定する。この移動により Host-X の IP-アドレスは変化するが、VIP-アドレスは不変である。移動後¹ Host-X は ConnNotify パケットを自分の固有ネットワークである Net-A へ送信する。このパケットは VIP-アドレスと新しい IP-アドレスを含んでおり、Net-G、Net-C および Net-B を通過するので、Gw-CG、Gw-BC および Gw-AB は Host-X の新しい IP-アドレスを知る。パケットは最終的には Net-A に到着し、Net-A 内の各ホストに Host-X の IP-アドレスを知らせるため、Net-A 内で同報通信される。Gw-AB は Host-X に確認応答 (ack) パケットを返送する。図で×印のついたゲートウェイは Host-X の新しい IP-アドレスを知っているものであることを示す。

パケットのフォワード手続きを図 4 に示す。図において Host-Y は Host-X の VIP-アドレスは知っているが、新しい IP-アドレスは知らないものとする。従って Host-Y はパケットの IP ヘッダの destination IP address フィールドに Host-X の VIP-アドレスをセットする。Host-X の固有ネットワークは Net-A であるので、パケットは Net-A へ向かう。パケットが Gw-BC に達したとき Gw-

¹ ホストがネットワークから切断されるときの手続きは後述。

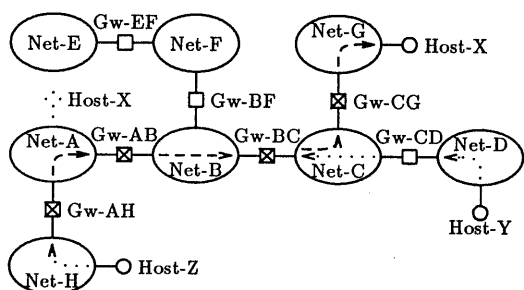


図 4: パケットのフォワーディング

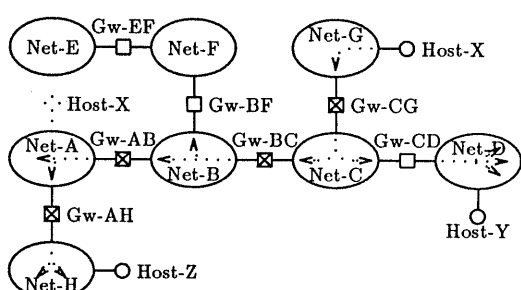


図 5: ネットワークからの切断

BC は Host-X の VIP-アドレスを対応する IP-アドレスに変換する。従ってパケットは Host-X へフォワードされる。同様に Host-Z が Host-X の新しい IP-アドレスを知らなければ、パケットは Net-A に到達後、Host-X にフォワードされる。図において、細い破線は目的ホストの IP-アドレスが正しくセットされていないパケットの軌跡を示し、太い破線は目的ホストの IP-アドレスが正しくセットされているパケットの軌跡を表す。Host-X が Host-Y にパケットを送れば、Host-Y と同様に Gw-CD も Host-X の IP-アドレスを知ることになる。このように Host-X と他のホスト間での通信が行なわれるにつれて、Host-X に関するキャッシュ情報がより広く拡散していく。AMT エントリと VIP-サブレイヤヘッダはタイムスタンプ・フィールドを持っているので、無効になった AMT エントリが目的ホストの VIP-アドレスを無効になった IP-アドレスに変換することは無く、パケットの経路のループは発生しない。

図 5 にホストがネットワークから切断されるときのパケットの流れを示す。図において Host-X は Net-G から切断されようとしている。このとき Host-X は *DiscNotify* パケットを Net-G 内に同報通信する。このパケットは Host-X の VIP-アドレスを含む。Gw-CG がこのパケットを受信すると、Gw-CG は Host-X に関する AMT エントリを消去し、さらに Gw-CG は Host-X に関する AMT エントリを持っていたので、Net-C 側にこのパケットを同報通信する。同様に Gw-BC もこのパケットを Net-B 内に同報通信する。しかし、Gw-BF は Host-X に関する AMT エントリを持っていないので、このパケットを受信しても何もしない。このように大部分の Host-X に関する AMT エントリは Host-X がネットワークから切断されるときに消去される。コントロールパケットは関係の無いネットワークには伝わらない。

4.6 無効キャッシュエントリ

ホストがネットワークから切断されるとき、*DiscNotify* パケットが送信されてそのホストに関する大部分の AMT エントリが消去される。しかし、無効になったキャッシュが残る可能性もある。無効になった IP-アドレスを見つけたゲートウェイ/ホストは、*ObsoleteCache* コントロールパケットを送信ホストに返送する。*ObsoleteCache* パケットの転送経路上で、ゲートウェイ/ホストが対応する AMT エントリを保持している場合は、そのエントリも消去される。またある時間アクセスされない AMT エントリは自動的に消去される。しかし、ホストの固有ネットワークに保持されているエントリは、アクセスされなくても消去されない。

4.7 ネットワークの分離に対する耐故障性

最悪の場合、移動ホストに対するパケットはそのホストの固有ネットワークでフォワードされる。従って移動ホストの現在位置と固有ネットワークの間でネットワークの分離が発生すると、問題が生じる可能性がある。たとえば図 4 における Gw-AB のクラッシュである。これには 2 つのケースが考えられる。1 つは Host-X が Net-G に接続された後に Gw-AB がクラッシュした場合、もう 1 つは Gw-AB がクラッシュした後に Host-X が Net-G に接続された場合である。前者の場合、接続のための手続きは完了しているので、ネットワークが分離しても Host-X に関する情報は Gw-CG や Gw-BC に伝播している。後者の場合、Host-X が送信した *ConnNotify* パケットは固有ネットワークに到達できない。しかしいくつかのゲートウェイ、たとえば Gw-CG や Gw-BC はこのパケットを受信できる。従って分離されたネットワークの同じ側に存在するホストは移動ホストと通信するこ

とが可能である²。しかしこのままでは固有ネットワークは移動ホストの新しい IP-アドレスを知ることができない。この問題は ConnNotify パケットの再送で解決できる。移動ホストは ack パケットを受信するまで、ある間隔で ConnNotify パケットの再送を続ける。

5 結論

近い将来大規模な相互接続された無線ネットワークが構築されることが予想されるが、このような環境ではホスト移動透過性が非常に重要になる。本論文では、OSI の 7 レイヤモデルに従えばホスト移動透過性はネットワークレイヤで提供すべきであると主張し、仮想ネットワークという概念を導入した。さらにこの概念を DARPA-IP に適用し、VIP を提案した。VIP では従来の IP レイヤは VIP サブレイヤと IP サブレイヤに分割され、各ホストは位置や移動に依存する識別子である IP アドレスと、位置や移動に依存しない識別子である VIP アドレスを持つ。またアドレス変換のオーバーヘッドを最小限に抑えるため、拡散キャッシュ法を導入した。この方法は遅延評価の一種である。このアーキテクチャを用いることにより、データリンクとして無線ネットワークが広範囲で利用可能になれば、他のネットワークに移動しているホストは移動中もコネクション・オリエンテッド・モードの通信を続けることができるようになる [Teraoka 91b]。VIP は現在 Muse オペレーティングシステム [Yokote 91] に実装中である。

謝辞

本研究に対して貴重な助言をいただいたカーネギーメロン大学の徳田英幸博士、慶應義塾大学の村井 純博士、Wide プロジェクトのメンバーの方々および SonyCSL の研究員に感謝致します。

参考文献

[Accetta 86] Mike Accetta, Robert Baron, David Golub, Richard Rashid, Avadis Tevanian, and Michael Young. *Mach: A New Kernel Foundation For UNIX Development*. Technical Report, Department of Computer Science, Carnegie-Mellon University, August 1986.

²Internet においては、EGP のような経路制御プロトコルを修正しなければならない。

[Cheriton 88] David R. Cheriton. THE V DISTRIBUTED SYSTEM. *Communications of the ACM*, Vol.31, No.3, pp.314-333, March 1988.

[ISO 84] ISO. *Information processing systems - Open Systems Interconnection - Basic Reference Model*. 1984. ISO7498.

[ISO 90] ISO. *Intermediate System to Intermediate System Intra-Domain Routing Exchange Protocol for use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service (ISO 8473)*. February 1990. ISO DP 10589.

[Rozier 88] M. Rozier, V. Abrossimov, F. Armand, I. Boule, M. Gien, M. Guillemont, F. Herrmann, C. Kaiser, S. Langlois, P. Léonard, and W. Neuhauser. Chorus Distributed Operating Systems. *Computing Systems*, Vol.1, No.4, Fall 1988.

[SRI 81] SRI. *Internet Protocol*. September 1981. RFC791.

[Tanenbaum 91] Andrew S. Tanenbaum. In his lecture in sony computer science laboratory inc. January 1991.

[Teraoka 91a] Fumio Teraoka. *The Virtual IP Protocol Specification*. Technical Report SCSL-TM-91-007, Sony Computer Science Laboratory Inc., February 1991.

[Teraoka 91b] Fumio Teraoka, Yasuhiko Yokote, and Mario Tokoro. A Network Architecture Providing Host Migration Transparency. In *Proceedings of SIGCOMM'91 Symposium on Communications Architectures and Protocols*, September 1991.

[Xerox 81] Xerox. *Internet Transport Protocols*. XEROX CORPORATION, December 1981. XSI5 028112.

[Yokote 91] Yasuhiko Yokote, Fumio Teraoka, Atsushi Mitsuzawa, Nobuhisa Fujinami, and Mario Tokoro. The Muse Object Architecture: A New Operating System Structuring Concept. *Operating System Review*, Vol.25, No.2, April 1991.