NAPT を越えた端末の移動時の TCP コネクション維持による移動透過性保証プロトコル

清水 智行† 中村 素典‡ 美濃 導彦‡
†京都大学大学院情報学研究科
‡京都大学総合情報メディアセンター
E-mail: †shimizu@mm.media.kyoto-u.ac.jp, ‡{motonori, minoh}@media.kyoto-u.ac.jp

概要 現在のインターネットにおいて，一つの IP アドレスを複数の端末が共有する，ないしファイヤウォールとして利用する目的で，NAPT がよく利用される．このような状況ではネットワーク層による移動透過性の保証に限界があり，トランスポート層における保証手法が必要となる．本稿では，NAPT の関与した移動にも対応可能な再接続手順の制御を行なうための手法として，TCP コネクション維持プロトコルを提案する．このプロトコルは，端末の移動情報を交換するプロトコルと拡張された TCP，さらに TCP コネクションを中継するプロキシで構成されている．これによって，移動時における NAPT の関与の有無に関わらず，端末の移動後に通信を再開させることが可能となる．

A Protocol for Mobility Support to Sustain TCP Connections against Host Migration over NAPT

Tomoyuki SHIMIZU† Motonori NAKAMURA‡ Michihiko MINOH‡
†Graduate School of Informatics, Kyoto University
‡Center for Information and Multimedia Studies, Kyoto University
E-mail: †shimizu@mm.media.kyoto-u.ac.jp, ‡{motonori, minoh}@media.kyoto-u.ac.jp

Abstract A NAPT (Network Address Port Translator) is often used to let multiple hosts share one IP address. A protocol to support migration over a NAPT should be designed not on the network layer but on the transport layer, to support host mobility against migration over a NAPT. We propose a TCP Connection Sustaining Protocol, which consists of three protocols; a protocol to let each hosts know where the other migrates to, extended TCP and a protocol to intermediate TCP connections. These protocols enable TCP connections to sustain even if every host migrates over a NAPT.

1 はじめに

近年，インターネットは企業や研究機関のみならず，一般の家庭においても日常的に利用されるようになりつつある．機器の小型化や低価格化，携帯電話や無線 LAN などの普及に伴い，通信端末を持ち運んでさまざまな場所からインターネットに接続するという利用形態も一般的となりつつある．

しかし，インターネットに接続されている通信端末を移動させるとき，場所によってイーサネットと無線 LAN を切り替えたり，移動に伴って無線 LAN のアクセスポイントが切り替わったりすることによって，IP アドレスが変化することが想定される．このような状況において，移動中に通信が途切れないようにすることは現状では困難である．

端末が移動しても常に同じ IP アドレスを継続して使用できるようにする手法として，Mobile IP[1]がある．Mobile IP では，端末の移動先のサブネットワークにある中継ノードに対して，IP パケットをカプセル化して転送することによって，移動端末が常に同じ IP アドレスを使用したまま，端末の移動先にパケットが中継されることによって，通信が維持される．しかし，Mobile IP はネットワーク層における手法であるため，トランスポート層においてポート番号の変換が存在する場合においては利用できない．

家庭においてインターネットを利用する場合，複数の端末を同時にネットワークに接続するために，NAPT(Network Address Port Translator)を利用し

て一つの IP アドレスを複数の端末が共有するといった利用形態が一般的となりつつある. NAPT は IP アドレスとポート番号の変換を用いて, IP アドレスの共有を可能にする装置である.

従って, NAPT の関与する端末の移動が発生したときに端末間の通信を維持するためには, 移動前後における NAPT によって変換される前の IP アドレスとポート番号によって, 移動前に通信を行なっていた端末同士であるかどうかを確認(以下, ペア確認と呼ぶ)して, 通信の再開を行なう仕組みが必要となる.

また, 端末が移動している間に相手端末も移動した場合, 互いに移動先の IP アドレスとポート番号を通知することができないため, 移動後に通信を再開することが不可能となる.

そこで本稿では, 端末が移動している間に相手端末も移動した場合及びNAPTを越えた端末移動が発生した場合の両方に対応可能な, TCP コネクションの維持を支援するためのプロトコルを提案する.

以下, 2 章では端末移動時における TCP コネクション維持のための従来手法とその問題点について述べる. 3 章では移動透過性保証プロトコルについて述べるについて述べる. 4 章では本手法を実装して評価を行なった結果を示し, 5 章で本稿をまとめる.

2 トランスポート層における移動透過性

一般に, 通信端末を持ち運んだり, 状況に応じて通信媒体を切り替えたりすることによって, 端末が使用する IP アドレスが変化すると, それまでに行なっていた通信は切断される. 以下, 端末の持ち運び等によって端末の持つ IP アドレスが変化することを, 端末の移動と呼ぶ.

トランスポート層において移動透過性を実現する手法として, An End-to-End Approach to Host Mobility[2]がある. これは, 端末の移動が発生したときに, TCP コネクションの確立手順(3 ウェイハンドシェイク)と同様の手順によって, 同期要求である SYN とその応答である ACK を 3 段階で交換しながら, 移動先の IP アドレスとペア確認に必要な情報を交換して, 移動先において通信を再開するものである(図 1). 移動先 IP アドレスとペア確認に必要な情報(移動前の IP アドレス, コネクション再開回数等が含まれる)は, TCP オプション[3]として TCP ヘッダに添付される. このオプションを Migrate オプションと呼ぶ. 以下では, Migrate オプションを付与した SYN を MSYN と呼ぶ.

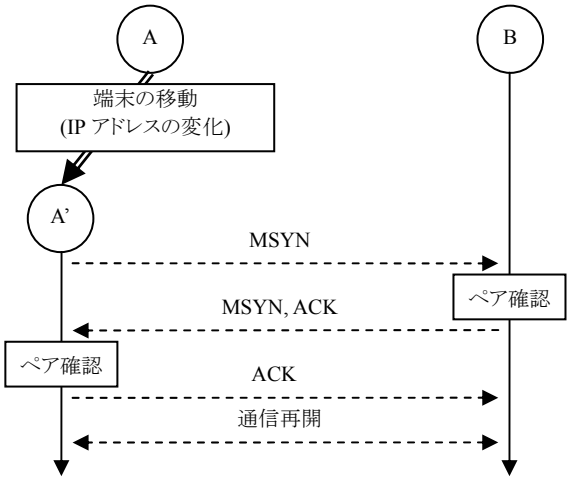

図 1: TCP コネクションの再開手順

しかし, 実際には手法[2]では対処できない端末移動の事例が存在する.

第一に, 互いに通信している 2 つの端末のうち, 片方の端末が移動している間, もう片方の端末も移動してしまったとき(以下, 端末の同時移動と呼ぶ)である. このとき, 互いに自端末の移動先を相手端末に伝えることができない(図 2).

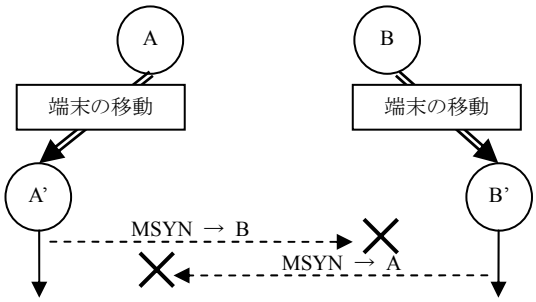

図 2: 端末の同時移動

第二に, 端末の移動の前後において NAPT が 2 端末間の経路上に存在するときである. この場合, NAPT の存在によって通信再開が不可能となる場合がある.

NAPT[3]は, 複数の端末が限られた数の IP アドレスを共有して通信できるようにするために, 変換したポート番号によってそれぞれの通信を区別し, 多重化する装置である(図 3).

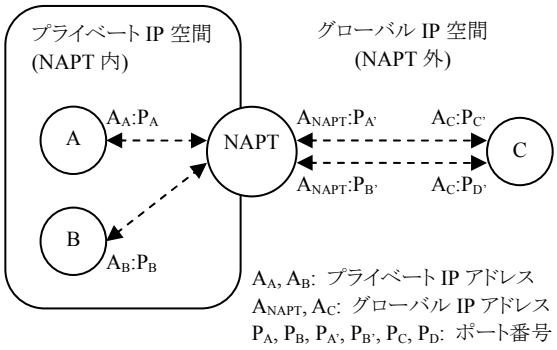

図 3: NAPT

図 3 のような状況において NAPT 配下のプライベート IP 空間に属する(以下, NAPT 内または内部と呼ぶ)の端末 A, B が移動したとき, ペア確認のために移動前の IP アドレスとポート番号を端末 C に送信したとしても, 端末 C が記憶している NAPT によって変換された IP アドレスとポート番号とは異なるものとなり, ペア確認に失敗する.

また, グローバル IP 空間に属する(以下, NAPT 外または外部と呼ぶ)の端末から NAPT 内の端末へ接続を要求することは不可能である(図 4). この性質を NAPT による接続の片方向性と呼ぶ. この性質を利用して, 一種のファイヤウォールとして利用されることもある.

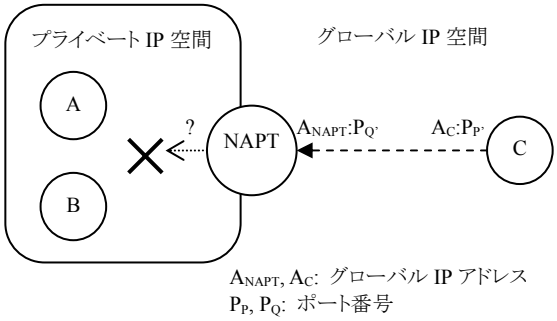

図 4: NAPT による接続の片方向性

従って, 移動した端末が, NAPT 外から NAPT 内の端末へ MSYN を送信しても, NAPT 内の端末へは届かず, 通信を再開することはできない.

また, NAPT 内の端末は, 相手端末が NAPT 外に移動したとき, 相手端末から MSYN を受信することができなくなるため, 相手端末が移動したかどうかを知ることもできなくなる.

3 移動透過性保証プロトコル

2 章で提起した問題を解決するために, 移動透過性保証プロトコルを提案する. 移動透過性保証プロトコルは, 移動先情報交換プロトコル, 拡張 TCP, 対称型 TCP プロキシで構成され, これらのプロトコルの連携によって, 端末の同時移動, 及び NAPT の関与した移動が発生したときにも移動透過性が保証される.

3.1 移動先情報交換プロトコル

2 章で述べたように, 端末の同時移動が発生した場合, もしくは NAPT 内の端末と通信している外部の端末が移動した場合には, どちらの端末も相手端末の移動先を知る手段がないために, 相手端末に対して MSYN を送信することができず, TCP コネクションを維持することができない.

そこで, 端末の移動に関する情報の交換を支援するサーバ(以後, 移動情報管理サーバと呼ぶ)を置き, このサーバを経由して, 端末の移動先の IP アドレスとポート番号を相手端末に通知するためのプロトコルとして, 移動先情報交換プロトコルを定義する.

移動情報管理サーバは, 端末がどのように移動したとしてもその移動先から通信可能となるようにするために, グローバル IP アドレスの空間に配置し, NAPT やファイヤウォールの影響を受けないようにする必要がある.

移動先情報交換プロトコルは, 移動前情報交換と移動後情報交換の 2 つの手順に分かれる.

3.1.1 移動前情報交換

移動前情報交換は, 自端末が直接持つ IP アドレスと, 自端末に見えている相手端末の IP アドレスを, 相手端末との間で交換する手順である. これによって, NAPT によるアドレス変換の影響があっても, 移動後に端末間の対応関係を正しく確認できる. この手順は, 端末が移動する前に完了させる必要がある.

3.1.2 移動後情報交換

移動後情報交換は, 端末が移動したときに, 移動情報管理サーバを経由して移動先に関する情報を交換する手順である.

移動前情報交換が完了している端末は, 移動したときに, 両端末の移動前の IP アドレスと, 移動後の IP アドレスを移動情報管理サーバに送信する. これらの情報をあわせて移動情報を呼ぶ. サーバ

は同時に複数の端末ペアの移動を扱うので，受信した移動情報を比較することによって，移動前に互いに通信していた端末の組を検出する．

移動情報のうち，移動前の IP アドレスについては NAPT によって変換される前後の両方の IP アドレスが必要である．

3.1.3 NAPT の検出と再開手順

移動情報として移動後に端末が直接持っている IP アドレスを含めることによって，サーバは IP アドレスの変換を検出して，その端末が NAPT 内に存在するかどうかを判断することができる．このとき，NAPT による接続の片方向性を考慮して，移動情報管理サーバが移動前に通信していた端末の組のうちどちらの端末が相手端末に MSYN パケットを送信させることが可能であるかを判断させる．

- 両端末が NAPT 外の場合: どちらの端末も相手端末に MSYN を送信することが可能である．ここでは，後にサーバに移動情報を送信した方が MSYN を送信することとする．
- 片方の端末が NAPT 内の場合: NAPT 内にいるほうの端末が NAPT 外の相手端末に MSYN を送信することが可能である．
- 両方の端末が NAPT 内の場合: どちらからも MSYN を相手端末に送信できない．従って，NAPT 外から TCP コネクションを中継する仕組みを利用する(3.3 節参照)．

移動情報管理サーバは，以上の基準によってどちらの端末が MSYN を送信するかを判断し，MSYN パケットを送信すべき端末にその相手端末の移動先を通知する．この通知を受けた端末は，4 章で述べる手順によって TCP コネクションの再開を行なう．

3.2 コネクション維持を可能とした拡張 TCP

NAPT による IP アドレスとポート番号の変換に対応したペア確認を行ない，かつ 3.1 節で述べた移動先情報交換プロトコルによってサーバから相手端末の移動先の通知を受けたときに，TCP コネクションを再開できるようにするために，手法[2]を拡張する．

3.2.1 アドレス・ポート変換への対応

NAPT によるアドレスとポートの変換の影響があっても，移動後にペア確認が正しく行なわれるようにするために，最初に TCP コネクションを確立するときに次の情報を交換する．

- 自端末が直接持っている IP アドレスとポート番号
- 自端末に見えている相手端末の IP アドレスとポート番号

これらは，SYN パケットに TCP オプションを付与することによって交換する．この TCP オプションを Migrate-Permit オプションと呼ぶ．Migrate-Permit オプションによって，相手端末が MSYN による TCP コネクションの再開に対応しているかどうかを確認することもできる．

これにより，端末移動が発生したときに，Migrate オプションに NAPT によって変換される前後の IP アドレスとポート番号を付与することによって，ペア確認が変換による影響を受けずに正しく行なわれる．

また，MSYN には，Migrate-Permit オプションも同時に付与することによって，端末の移動先において NAPT が存在するかどうかを知ることができるようにする．

3.2.2 TCP 状態遷移機械の拡張

2 章で述べたように，端末が移動して MSYN を相手端末に送信しても，相手端末に届かない場合がある．このような場合においても，3.1 節で述べた移動先情報交換プロトコルによって，相手端末の移動先の通知を受けてから再度 TCP コネクションの再開を行なうようにするためには，最初の MSYN パケットに対する応答がなかった場合，すぐには TCP コネクションを切断せず，再度 MSYN を送信するか，相手端末から MSYN を受信するまで待機するように，TCP を拡張する必要がある．

そこで，TCP の状態遷移機械に 2 つの状態 `MIG_SENT` と `MIG_WAIT` を追加する．

端末が移動して，MSYN パケットを送信すると，TCP は `MIG_SENT` 状態に移る．ここで，MSYN が相手端末に届き，正常に MSYN の 3 ウェイハンドシェイクが完了すると，TCP コネクションが再開される．

MSYN が相手端末に届かず，タイムアウトとなった場合は，`MIG_WAIT` 状態に遷移する．その後，相手端末から MSYN を受信した場合は，MSYN の

3 ウェイハンドシェイクの手順によって TCP コネクションを再開する. 移動情報管理サーバから相手端末の移動先の通知を受けた場合は, 再度 MSYN を相手端末の移動先に送信し, TCP コネクションの再開を試みる.

MIG_WAIT 状態においてタイムアウトが発生した場合は, TCP コネクションの再開を諦めて切断する.

3.3 対称型 TCP プロキシ

3.3.1 プロキシによるコネクションの中継

3.1 節で述べたように, TCP コネクションを再開すべき 2 つの端末がいずれも NAPT 内に存在する場合は, 互いに MSYN を相手端末に届けることができない. このような状況において通信を再開できるようにするためには, NAPT 外に TCP コネクションを中継する仕組みが必要である.

そこで, 両端末から MSYN を受信して TCP コネクションを中継するプロキシを用意する(図 5). このように, 中継の対象となる両方の端末から MSYN を受信することによって機能するプロキシを対称型 TCP プロキシと呼ぶこととする.

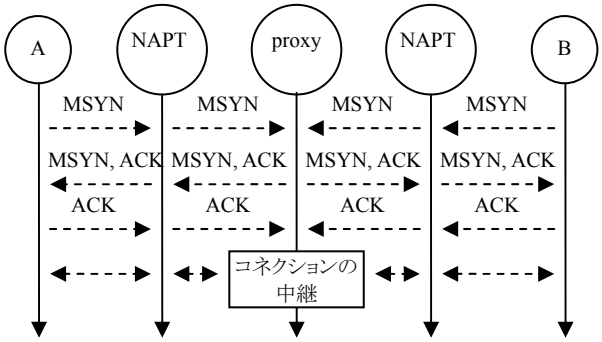

図 5: 対称型 TCP プロキシ

3.1 節で述べた移動先情報交換プロトコルにおいて, 移動情報管理サーバが対称型 TCP プロキシを利用するべきと判断した場合, 移動情報管理サーバは対称型 TCP プロキシサーバに, コネクション中継用のポート番号の確保を要求する. 移動情報管理サーバは, TCP コネクションを再開する両端末に対して, プロキシサーバの IP アドレスと確保されたポート番号を相手端末の移動先として通知する.

これにより, 両端末はプロキシサーバに対して MSYN を送信し, プロキシサーバとの間で 3 ウェイハンドシェイクが行なわれ, TCP コネクションが中継される.

3.3.2 コネクション中継時の端末移動

2 端末間の TCP コネクションが対称型 TCP プロキシによって中継されているとき, 片方の端末が移動すると, プロキシサーバと移動した端末の間で, MSYN による 3 ウェイハンドシェイクが行なわれる.

このとき, プロキシサーバは Migrate オプションに付与された Migrate-Permit オプションによって, 移動端末が NAPT 内であるかどうかを判定する.

もし端末の移動先が NAPT 内である場合, プロキシサーバは MSYN の 3 ウェイハンドシェイクの完了後, TCP コネクションの中継を再開する.

端末の移動先が NAPT 外である場合は, プロキシを使わずとも TCP コネクションを再開できるものと考えられる. 従って, プロキシサーバは MSYN の 3 ウェイハンドシェイクを RST の送信によって拒否する. このとき, MSYN を送信した端末は, 3.1 節で述べた移動情報管理サーバに移動情報を送信して, 相手端末の移動先の通知を待つこととなる.

4 実験

移動先情報交換プロトコルと拡張 TCP, TCP コネクション中継プロキシの動作と機能を評価するため, 計算機上にこれらのプロトコルを実装し, 実験を行なった.

実験を行なうにあたって, 移動端末として PC を 2 台(A, B), 移動情報管理サーバとして PC を 1 台(C)用意し, NAPT の関与する移動を検証するため, NAPT と DHCP の機能を有する小型ルータを 2 台用意した. いずれの PC も OS として Red Hat Linux 7.2 日本語版を使用した. また, パケット観測用に PC を 1 台(D)用意し, B, C と同じセグメント上に D を配置してパケットを観測した. 端末 D の OS として Windows 2000 を使用した.

まず, 図 6 に示すネットワーク構成において端末 B から端末 A にファイルを転送し, その途中で端末 B を NAPT 外の別の IP アドレスへ, 端末 A を別の NAPT 内へ移動させ, TCP コネクションの再開を検証した. 端末 B においてパケットを観測した結果を図 7 に示す. また, 端末 B において観測しているため, 端末 A の IP アドレスとして, NAPT の IP アドレスが記述されている.

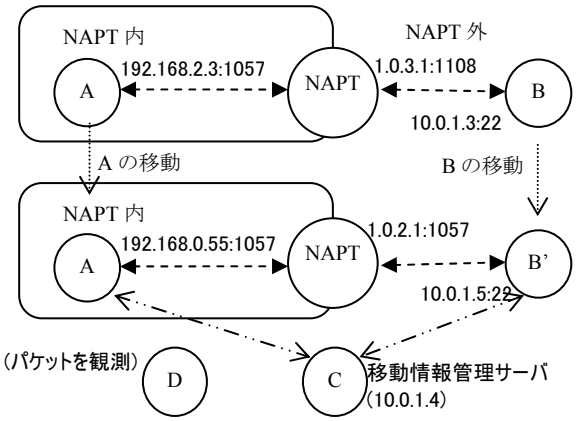

図 6: 実験環境

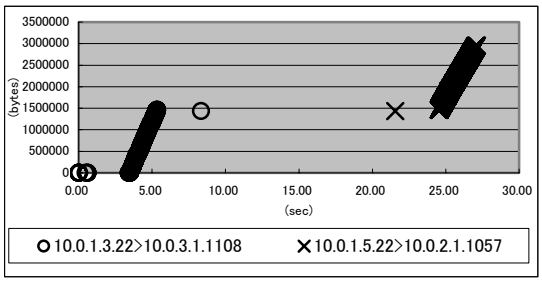

図 7: 端末移動時におけるパケットの観測結果

この結果では，端末 A，B 両方の移動が完了するまでに約 16(= 21 – 5)秒かかっている．その後，端末 A (192.168.0.55)が端末 B(10.0.1.5)に対して MSYN パケットを送信し，TCP コネクションの再開を行なっている．

コネクションの再開に要した時間は，約 3(= 24 – 21)秒であった．これは，端末 A におけるパケットの最小再送時間である 3 秒に近い値である．

5 まとめ

本稿は端末の移動中に通信相手の端末も移動した場合，及び NAPT が端末間の通信経路上に存在する場合において，移動によって端末の IP アドレスが変化したときに，サーバを経由して移動先の IP アドレスを端末間で交換し，NAPT によって接続要求が遮られない向きで接続要求を送信するように手順を管理することによって，TCP コネクションの再開を可能とするプロトコルを提案した．

また，両端末が NAPT の配下にある場合は，TCP コネクションを擬似的に維持するための対称型 TCP プロキシが，NAPT の外側から TCP コネクションを中継する．

本稿ではコネクション型通信である TCP のみを扱ったが，同じくポート番号を扱うプロトコルである UDP においても，IP アドレスとポート番号の変化に対処する仕組みを議論すること自体は可能である．

しかし，UDP はコネクションレス通信であり，接続手順を持たないプロトコルであるため，実際の通信再開手順の設計が困難である．従って，移動透過性を保証する仕組みを UDP に追加するためには，通信再開のための仕組みをどう追加するかを考察することが課題である．

参考文献

[1] C. E. Perkins: IP Mobility Support, RFC 2002 (1996).

[2] Alex C. Snoeren and Hari Balakrishnan: An End-to-End Approach to Host Mobility, 6th ACM/IEEE International Conference on Mobile Computing and Networking (2000).

[3] Jon Postel: Transmission Control Protocol, RFC 793 (1981).

[4] P. Srisuresh, Jasmine Networks, K. Egevang, Intel Corporation: Traditional IP Network Address Translator (Traditional NAT), RFC 3022 (2001).