移動環境における IPv6 自動設定機能の効果的な使用法

神 明 達 哉[†]　伊藤 純一郎[††]　角 川 宗 近[†††]

IPv6 では，近隣探索 (Neighbor Discovery) 機能を利用してホストのネットワーク設定を自動化しているが，この機能には移動環境との相性の観点から問題がある．具体的には，移動前に設定されたネットワークプレフィクスの有効期限が長いために，移動後にも以前のネットワークに接続しているかのようにふるまってしまうということがあげられる．本稿では，プレフィクスを通知したルータへの到達性を確認することで，移動前のプレフィクスの誤使用を防ぐという拡張を提案する．また，この拡張の実際のシステムへの実装とその効果についても示す．

An effective method of using IPv6 auto configuration under mobile environments

JINMEI Tatuya,[†] ITOH Jun-ichiro[††]
and SUMIKAWA Munechika [†††]

An IPv6-capable host can configure itself using Neighbor Discovery protocol, but it is not designed with mobility so well. For example, since the default lifetime of network prefix defined by IPv6 specification is relatively long for mobile hosts, a mobile host sometimes behaves as if it is connected with an old network after moving from the network. This paper describes an extension, in which a host associates a network prefix with routers that advertise the prefix so that it can detect its movement from a network and do not use the prefix of the old network. Implementation and effectiveness of the extension is also shown.

1. はじめに

IPv6 （IP version6）[1] は，現在インターネットの標準として使用されている IPv4 の後継として IETF （Internet Engineering Task Force）で標準化が進められている次世代ネットワークプロトコルである．

IPv6 の特徴のひとつに，近隣探索（Neighbor Discovery）プロトコル[2] によるホストの自動設定機能がある．たとえば，ホストの IPv6 アドレスは，ルータから定期的に通知されるネットワークプレフィクスとホスト自身の固有情報とから自動的に生成される．

ルータから通知されるネットワークプレフィクスにはその情報の一部として有効期限（lifetime）が設定されている．この有効期限が切れたプレフィクスはそのリンクでは無効とみなされ，またそのプレフィクスを用いて生成したアドレスは使用不可能となる．この機能を用いて，たとえばネットワークのリナンバリングをユーザに意識させずに実施できる．この有効期限は固定的な環境を想定しているため，通常比較的長い値に設定される．

移動環境において自動設定機能を利用する際には，この有効期限の長さに起因する問題が生じることがある．たとえば，移動前に設定したアドレスは移動先では一般に無効であるが，仕様に従えばこのアドレスは期限が切れるまでは有効とみなされる．このため，移動前のアドレスが移動先における通信のソースアドレスとして誤って使用される可能性がある．

本稿では，プレフィクスとそれを通知したルータとを関連付け，ルータの到達可能性から古いプレフィクスを検出して排除するという方法を提案する．まず 2節で自動設定機能の概要を述べ，続く 3節で移動環境における問題を具体的に説明する． 4節では提案する解決法を詳細に説明し， 5節でその実装と実際の移動環境での効果を示す．最後に，残る課題を 6節で概観する．

なお，本稿で述べる研究は，IPv6 の基本的な機能の実装とその検証を目的とする KAME プロジェクト[☆]の一環として行ったものである．5節で示す実装は KAME

† 東芝 研究開発センター
Research and Development Center, Toshiba Corporation
†† インターネットイニシアティブ 技術研究所
Research Laboratory, Internet Initiative Japan Inc.
††† 日立製作所 サーバ開発本部
Server & Network Development Division, Hitachi, Ltd.

☆ http://www.kame.net/

プロジェクトの成果物として公開されている．

2. IPv6 の自動設定機能

本節では，IPv6 の近隣探索機能によるホストの自動設定機能について説明する．なお，本節以降，ルータとホストを区別する必要のない場面において，ネットワーク機器一般を指してノード とよぶ．

IPv6 対応ルータは，接続するインタフェース上の全ノードマルチキャストアドレス（All-Nodes Multicast Address）[4] 宛にルータ通知（router advertisement）メッセージを一定間隔で送信する．通常，ルータ通知メッセージにはプレフィクス情報オプション（prefix information option）が含まれる．このオプションにはそのリンク上で有効な IPv6 アドレスのプレフィクスが格納されており，ホストはこれを用いて自身の設定を行う．

具体的には，プレフィクス情報オプションで与えられたプレフィクスに，ホスト自身が持つ識別子を付け加えて IPv6 アドレスを生成する．この識別子は，通常イーサネットの MAC アドレスのような一意性の高いものをもとに生成する．さらにホストは，与えられたプレフィクスを持つアドレスは自身と同じリンクに接続されているものとみなし，そのアドレスへの通信の際にはルータを介さずにリンク層アドレスの解決を直接試みる．

ホストはまた，ルータ通知メッセージのソースアドレスをデフォルトルートのネクストホップとして利用する．リンク外のアドレス，すなわち，プレフィクス情報オプションで与えられたプレフィクスに適合しないアドレスへのパケットは，まずこのルータへ送られる．

同じリンク上に複数のルータが存在する場合，それぞれのルータが個別にルータ通知メッセージを送信してもよい．このとき，ホストはそれらの複数のメッセージのすべてを設定用の情報として利用する．とくに，各メッセージのソースアドレスをリストにして管理し，各々をネクストホップとして利用可能なルータとみなす．このルータをデフォルトルータとよび，このリストをデフォルトルータリスト（default routerlist）とよぶ．

以上の過程を模式的に示したものが図 1である．

図 1において， R1 および R2 はルータ， H1 および H2 はホストである． R1, R2 が送信するルータ通知メッセージをそれぞれ RA1, RA2 で表す．それぞれのメッセージにはプレフィクス情報オプションが 1 つずつ含まれており，そのプレフィクスはそれぞれ P1, P2 である． R1， R2 が送信したルータ通知メッセージはリンク上にマルチキャストされる．全ノードマルチキャストアドレスにはすべての IPv6 ノードが参加しているため， H1， H2 はともに RA1， RA2 を受信し，各々のデフォルトルータリストに R1， R2 が付け加えられる．また， H1 は固有の識別子として I1 を持ち，プレフィクス情報オプションによって与えられたプレフィクス P1, P2 に I1 を付け加えてグローバルアドレス P1:I1 および P2:I1 を生成する． H2 も同様に P1:I2 および P2:I2 を生成する．

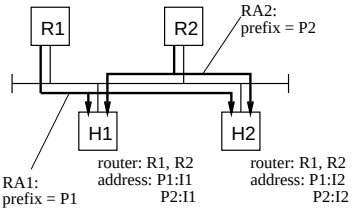

図 1 ルータ通知メッセージによる IPv6 のホスト自動設定
Fig. 1 IPv6 host autoconfiguration using a router advertisement message

通常，ルータ通知メッセージは 10 分程度の間隔をおいて送信される．ブート直後，あるいは移動直後など，ホストが新たにリンクに接続した場合，この間隔を待たずに設定できるよう，ホストはルータ要請（router solicitation）メッセージを送信してルータ通知を促すことができる．このメッセージは全ルータマルチキャストアドレス（All-Routers Multicast Address[4]）宛に送信される．要請を受け取ったルータはただちにルータ通知を返す．ホストはそのルータ通知を受信して上述の通りに設定を行う．

ルータ通知メッセージ自身とプレフィクス情報オプションには，それぞれ情報の有効期限を示すフィールドが含まれている．ホストはルータ通知メッセージを受け取るたびにルータやプレフィクスの有効期限を更新する．何らかの理由によりルータ通知メッセージが有効期限を超えて途絶えた場合には，対応するルータやプレフィクスは無効となる．ルータが無効になった場合には，対応するルータはデフォルトルータリストから削除される．また，プレフィクスが無効になった場合には，そのプレフィクスから生成したアドレスも無効となり，そのプレフィクスに適合するアドレスはリンク外のものとみなされる．

3. 移動環境における問題点

2節で述べた自動設定は，移動ホストの移動先でのネットワーク設定にも用いることができる．すなわち，移動先のネットワークに接続した後，まずルータ要請メッセージを送信する．その応答として移動先のルータからルータ通知を受け，その内容にもとづいて新しいア

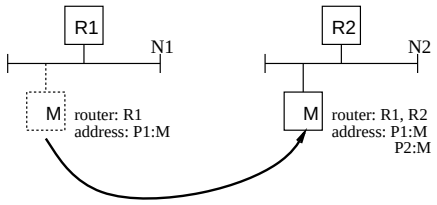

図 2　移動ホストの自動設定
Fig. 2　Autoconfiguration for a mobile host

ドレスとデフォルトルータを設定すればよい．

ただしこの場合，移動前のアドレスやデフォルトルータをそのまま使用し続けることのないように注意しなければならない．このことを具体的な例で示す．

いま，移動ホスト M がネットワーク N1 から別のネットワーク N2 に移動したとする（図 2参照）．

移動前には，M には N1 内のルータ R1 によるルータ通知によってアドレス P1:M が設定され，また M のデフォルトルータリストには R1 が含まれている．移動後には N2 内のルータ R2 からのルータ通知によってアドレス P2:M が追加され，R2 が M のデフォルトルータリストに追加される．このとき，R1 および P1 がともに有効期限内であるとすると，移動後の通信において以下のような問題が起こり得る．

(1) N2 外のノードへパケットを送信する際に，デフォルトルータとして R1 が使用される可能性がある．R1 は N2 には存在しないので，通信は成功しない．

(2) N2 外のノードへパケットを送信する際に，ソースアドレスとして P1:M が使用される可能性がある．このようなパケットは途中のルータの設定によってはフィルタリングの対象になる．また，仮に配送されたとしても，その応答パケットは通常 P1:M 宛に送られるため，移動先では受信できない．とくに，ACK パケットを受け取れないため TCP による通信が不可能となる．

(3) プレフィクス P1 に適合するアドレスは同一リンク内にあると判断されるため，そのようなアドレスへのパケットはルータには送られず，N2 でのアドレス解決の対象となる．結果として通信は成功しない．

以上の問題のうち，1については IPv6 の近隣探索機能に含まれる到達不能検出（Neighbor Unreachability Detection, NUD[2]）の仕組みによって解決できる．すなわち，移動直後は古いルータ R1 を使用する可能性もあるが，その時点で R1 が到達不能であることを検出できる．それ以後は到達可能である R2 が優先されるため，問題は解消する．

また，近隣探索プロトコルの仕様で定められているデフォルトのルータ有効期限は 30 分であり，数時間単位での移動の後では，移動前のルータはすでに期限切れとなっていることも期待できる．

一方，2および 3に対しては，プレフィクス P1 に対する有効期限が切れない限り解決できない．与えられたプレフィクスが無効になるのはその有効期限が切れたときだけだからである．しかし，近隣探索プロトコルの仕様で定められているデフォルトの有効期限は 30 日であり，その期限を待つのは一般的な移動環境に対しては現実的ではない．一方，有効期限を必要以上に短く設定すると，移動しない環境において一時的なルータの不良のためにアドレスが削除されてしまうといった不都合を生む．また，移動先において有効期限を自由に設定できるという保証もない．

移動直後にプレフィクスを強制的に無効にするという方法も考えられるが，この方法には以下の 2 つの問題がある:

- “移動直後” という状態の判別が困難である．このような判断の基準としてはたとえば，サスペンド状態からの復帰やインタフェースのキャリア検出などが挙げられる．しかし，前者は至近距離での移動でサスペンドを行わないような場合に検出不能となる．また，後者はインタフェースカードやデバイスドライバの仕様によっては利用不可能な場合がある．
- 実際に移動していないにも関わらず移動したと誤認する場合がある．たとえば，サスペンド状態からの復帰によって移動したと判別する場合，仮に一時的にルータが不良になっている期間に復帰したとすると，移動したと誤認されてプレフィクスが無効になってしまう．ルータが不良になっている間はルータ通知は送信されないので，本来は可能であるはずの同一リンク内通信にも障害が生じる．

そこで本稿では，プレフィクスとそれを通知したルータの到達性を関連させて管理することで，実際に移動したときにのみ古いプレフィクスが無効化されるようなモデルを提案する．モデルの詳細は次節で説明する．

4. 提案するモデル

4.1 定　　義

本稿で提案するモデルでは，プレフィクスを，それを通知したルータのリストとの組で管理する．このリストは，複数のルータがそのプレフィクスを通知している場合には複数の要素から生成される．

各プレフィクスについて，それを通知したあるルータ

がデフォルトルータリストから削除される際には，同時にプレフィクスの持つリストからも削除される．したがって，すべてのルータがデフォルトルータリストから削除された場合などには，リストは空となる．

各プレフィクスは，付随するルータのリストが空でないか，または，当該プレフィクスを含めて通知されたすべてのプレフィクスに付随するリストが空である場合に *attached* であるとよぶ．そうでない場合，すなわち，そのプレフィクスに付随するリストが空であり，かつ，そのプレフィクス以外に空でないリストを持つプレフィクスが存在する場合，そのプレフィクスは *detached* であるとよぶ．

各ホストは，以下に記述するように，ネットワークの状態変化に応じて管理する各プレフィクスを操作する．

- プレフィクス情報オプション付きルータ通知を受信したとき，オプションで与えられたプレフィクスに付随するリストに通知を送信したルータを加える．
- ルータ R がデフォルトルータリストから削除されたとき，各プレフィクスの持つリストから R を削除する．

その上で，ホストはすべてのプレフィクスを調べ，定義にしたがってそれぞれのプレフィクスの状態を attached または detached に設定する．パケット送信の際には，detached なプレフィクスは無視される．すなわち，attached なプレフィクスによって生成されたアドレスだけをソースアドレスとして使用する．また，attached なプレフィクスに適合するアドレスだけを同一リンク上のノードのアドレスとみなす．したがって，detached なプレフィクスはどちらの用途にも使われない．

4.2 適 用 例

このモデルを具体的な移動環境に適用した例を示す．このモデルのもとでは，図 1におけるホスト H1 の状態は図 3のようになる．すなわち，プレフィクス P1，P2 はそれぞれ，そのプレフィクスを通知したルータ R1，R2 を要素とするリスト（R1），（R2）とともに管理される．

次に，移動ホストの場合を考える．いま，図 2において，移動後に R1 がデフォルトルータリストから削除された状態を考える．このときの M の状態を本モデルにしたがって図示すると図 4のようになる．

ルータ R1 が削除されたことにより，ネットワーク N1 において R1 から与えられたプレフィクス P1 のリストは空となる．一方，移動後のネットワーク N2 のルータ R2 によって与えられたプレフィクス P2 のリストには R2 が存在しているため，P1 は detached，P2 は attached となる．したがって，これ以後の通信においては，宛先が N2 内であるか N2 外であるかに関わらず，ソースアドレスとして P2:M が使用され，N2 外へのパケットはデフォルトルータである R2 に送られる．この規則は P1 に適合するアドレスへ向けてパケットを送る場合にも適用されることに注意が必要である．すなわち，P1 は有効期限内ではあるが detached であるため，それに適合するアドレスは N2 上に存在するものとはみなされない．

本モデルでは，移動しないままルータが一時的な不良に陥った場合も正しく処理できる．いま，図 4において R2 が不良になり，M のデフォルトルータリストから削除された状態を考える（図 5）．

この場合，M の保持するプレフィクス P1，P2 の双方について対応するルータのリストが空であるため，P1 および P2 の状態はともに attached となり，アドレス P1:M と P2:M はともにソースアドレスとして有効となる．この例では，ネットワーク N2 内の唯一のルータであった R2 が機能していないため，M にとって可能な通信は N2 内に閉じたものとなる．その宛先は通常 P2

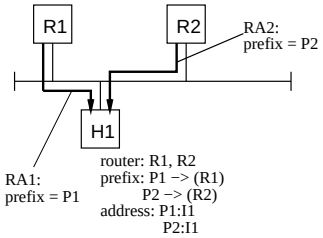

図 3 提案するモデルのもとでの自動設定
Fig. 3 Example of autoconfiguration under the proposed model

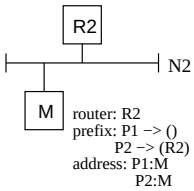

図 4 提案するモデルのもとでの移動例
Fig. 4 Example of host moving under the proposed model

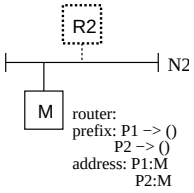

図 5 ルータに不良が生じた場合
Fig. 5 Example of failure of a local router

に適合すると考えられるため，同じプレフィクスを持つアドレス P2:M をソースアドレスとして用いればよい．

以上の例を有効に機能させるためには，移動前の，あるいは不良をおこしたルータを迅速に検出する必要がある．ルータの有効期限は通常数十分単位で設定されるので，数時間単位での移動後には移動前のルータは自然に削除される．一方，至近距離での移動やルータ不良の場合には到達不能検出機能の利用が有効である．ただし，近隣探索の仕様に厳密にしたがえば，ルータの到達不能性が検出された場合にもそのルータがデフォルトルータリストから削除されることはない．この仕様にしたがっている実装においては，プレフィクスの持つルータリストの定義を，到達可能なルータのリストとすればよい．

本モデルを用いた場合でも，移動したという事実の検出が困難であることには変わりはない．この検出は実装レベルで行っており，5.2節で説明する．

5. 実際のシステムへの実装

4節で提案したモデルを，FreeBSD 2.2.7 をベースに，KAME プロジェクトによって IPv6 対応させた OS の上に実装した．また，本実装は BSD/OS 3.1 および NetBSD 1.3.2 上へも移植されている．ソースコードは 1節の脚注に示した URL から取得可能である．

本節では，実装の詳細とその効果について説明する．

5.1 カーネル内の実装

本実装では，4節のモデルを実現するためにカーネル内で以下の 3 つの構造体を使用する．

nd_prefix構造体　ルータから通知されたプレフィクスの情報を管理するための構造体．有効期限や対応する IPv6 アドレス，detached であるか attached であるかのフラグなどの情報が格納される．プレフィクスを通知したルータのリストであるnd_pfxrouter構造体（後述）へのポインタも含まれる．ひとつの構造体がひとつのプレフィクスを表し，複数のプレフィクスはnd_prefix構造体のリンクリストで構成する．

nd_pfxrouter構造体　各プレフィクスを通知したルータを表す構造体．後述するnd_defrouter構造体へのポインタを持つ．

nd_defrouter構造体　デフォルトルータを管理するための構造体．デフォルトルータリストの要素に相当する．ルータの有効期限やネットワークインタフェースなどの情報が格納される．デフォルトルータリストはこの構造体のリンクリストで表現される．

以上のデータ構造の，実際のネットワークにおける使用例を見るために，図 6のような環境を考える．

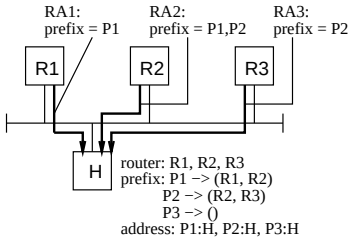

図 6　ネットワーク構成例
Fig. 6　Configuration of a sample network

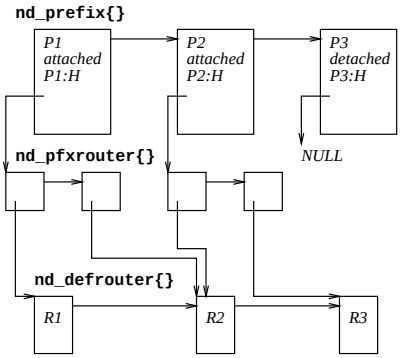

図 7　カーネル内のデータ構造
図 8　Data structure used in kernel

ホスト H が接続しているネットワークには R1, R2, R3 の 3 つのルータが存在し，R1 はプレフィクス P1 を，R2 は P1 と P2 を，R3 は P2 を，それぞれ通知している．H は P1, P2 以外にプレフィクス P3 を通知されているが，P3 を通知したルータはこのネットワーク上には存在しないため，P1, P2 は attached，P3 は detached となる．ホスト H はまた，通知された 3 つのプレフィクスから生成されるアドレス P1:H, P2:H, P3:H を持つ．

カーネル内で図 6に対応する構造を示したものが図 8である．ただし，説明に必要な情報以外は図では省略してある．

図 8に示されるように，3 つのプレフィクスに対応する 3 つのnd_prefix構造体がリンクリストで結合されている．先頭の構造体がプレフィクス P1 に対応しており，その状態が attached であること，対応するアドレスとして P1:H を持つことが示されている．nd_prefix構造体にはnd_pfxrouter構造体へのポインタが含まれており，個々のnd_pfxrouter構造体はnd_defrouter構造体を指す．nd_defrouter構造体には実際のルータの情報が保持される．プレフィクス P3 は対応するルータを持たないため，P3 に対応するnd_prefix構造体か

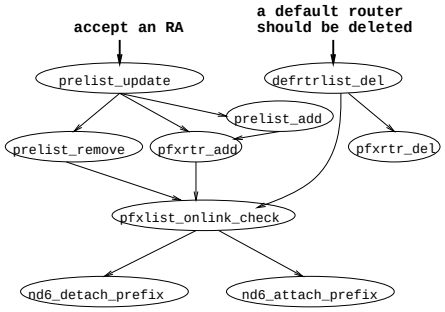

図 9　カーネル内での制御の流れ
Fig. 9　Control flow in kernel

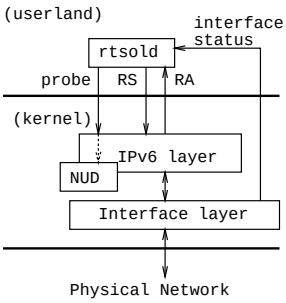

図 10　システム全体の構成
Fig. 10　System configuration

らnd_pfxrouter構造体へのポインタはNULLとなる．

図 9にカーネル内の制御の流れを示す．楕円は個々の関数を表し，細い矢線は関数呼び出しを表している．

prelist_ではじまる 3 つの関数は，nd_prefix構造体の追加（add），削除（delete），情報更新（update）を行う．pfxrtr_ではじまる 2 つの関数は，nd_pfxrouter構造体の追加（add），削除（del）を行う．また，defrtrlist_del関数はnd_defrouter構造体，すなわちデフォルトルータリストからの削除を行う．

pfxlist_onlink_check関数は，各プレフィクスの状態が変化したかどうかを確認し，変化に応じてnd6_detach_prefix関数またはnd6_attach_prefix関数を呼び出す．この 2 つの関数によって，カーネル内経路表への変更など，状態変化に伴うシステムの変更がなされる．

図 9の最上部は，ルータ通知を受信したとき，あるいはデフォルトルータリストからルータを削除したときにプレフィクスの状態変化が起こり得ることを意味している．これは 4節で示した 2 つの場合に対応している．

(1) ルータ通知を受信したとき．
prelist_update関数によってプレフィクス情報オプションが処理される．この関数はオプションの内容およびホストの状態にしたがって，プレフィクスの追加，既存のプレフィクスへのルータの追加，無効になったプレフィクスの削除のいずれかを行い，pfxlist_onlink_check関数を呼び出してプレフィクスの状態変化に対応する．

(2) デフォルトルータリストからルータが削除されたとき．
pfxrtr_del関数によって各プレフィクスの持つルータのリストからそのルータを削除し，pfxlist_onlink_check関数を呼び出す．

5.2　ユーザー空間との連携

5.1節で述べたカーネル内の実装は，それ自体単独で機能する．すなわち，特別なユーザ空間のプロセスを必要とすることなく，デフォルトルータリストの変化からカーネルが自動的に移動の有無を検出し，それに応じてプレフィクスの状態を変化させる．

しかし，3節で述べたように，この方法だけではデフォルトルータリストからルータが削除されないような短時間での移動に対しては十分ではない．それを補うため，本実装ではユーザ空間のデーモンも併用する．このデーモンは，移動の検出とそれに応じたルータ要請メッセージの送信を役割とするもので，rtsoldとよばれる．

rtsoldを含めたシステム全体の概要を図 10に示す．

rtsoldはネットワークインタフェースの状態を監視しており，キャリアのない状態からキャリアを検出すると移動の可能性があるものとみなしてルータ要請メッセージを送信し，返送されたルータ通知メッセージからカーネル内と同様にデフォルトルータのリストを構成する．この操作のたびに，rtsoldはリスト内の各ルータあてに空のパケットを送信する．これによってカーネル内で到達不能検出が引き起こされ，到達性のないルータから通知されたプレフィクスを排除できるようになる．

インタフェースカードによってはキャリアの状態を CPU に伝えないものもある．また，カードの仕様として可能であっても，ネットワークドライバでその機能を実現していない場合もある．そこでrtsoldは起動時にキャリア検出が可能かどうかを確認し，不可能な場合には 1 分間隔でルータ要請メッセージとルータ宛の空パケットを送信する．

5.3　使　用　例

本実装を実際に移動環境で使用した効果を具体的な例で示す．想定する環境は図 2と同様である．

図 11に，ネットワーク N1 において実行したいくつかのネットワークコマンドの出力結果を示す．ただし，図 11では説明に無関係な出力を省略し，長い行は見やすく

```
[1]% ifconfig ep0
ep0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 3ffe:501:100f:1000:260:8ff:feb2:5cfe prefixlen 64

[2]% ndp -p
3ffe:501:100f:1000::/64 if=ep0
  flags=LA, vltime=2592000, pltime=604800, expire=29d23h58m58s
  advertised by
    fe80::200:39ff:fecd:4107

[3]% ping6 -n -c 1 3ffe:501:100f:1000:2a0:c9ff:fe55:e0c9
PING6(56=40+8+8 bytes) 3ffe:501:100f:1000:260:8ff:feb2:5cfe -->
                       3ffe:501:100f:1000:2a0:c9ff:fe55:e0c9

[4]% ping6 -n -c 1 3ffe:501:100f:0:200:f8ff:fe01:61cf
PING6(56=40+8+8 bytes) 3ffe:501:100f:1000:260:8ff:feb2:5cfe -->
                       3ffe:501:100f:0:200:f8ff:fe01:61cf
```

図 11 移動前のネットワークでの操作例

Fig. 11 Operation on a network before move

```
[5]% ifconfig ep0
ep0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 3ffe:501:100f:1000:260:8ff:feb2:5cfe prefixlen 64 detached
        inet6 3ffe:501:100f:2000:260:8ff:feb2:5cfe prefixlen 64

[6]% ndp -p
3ffe:501:100f:2000::/64 if=ep0
  flags=LA, vltime=2592000, pltime=604800, expire=29d23h59m45s
  advertised by
    fe80::260:97ff:fe94:6e1
3ffe:501:100f:1000::/64 if=ep0
  flags=LA, vltime=2592000, pltime=604800, expire=29d23h58m41s
  No advertising router

[7]% ping6 -n -c 1 3ffe:501:100f:1000:2a0:c9ff:fe55:e0c9
PING6(56=40+8+8 bytes) 3ffe:501:100f:2000:260:8ff:feb2:5cfe -->
                       3ffe:501:100f:1000:2a0:c9ff:fe55:e0c9
```

図 12 移動後のネットワークでの操作例

Fig. 12 Operation on a network after move

なるよう折り返してある．以後の出力例においても同様である．

ifconfigコマンドの出力から，現在3ffe:501:100f:1000:260:8ff:feb2:5cfe というアドレスだけが設定されていることがわかる．2 つ目のndpコマンドは近隣探索に関連するシステムの状態を出力する．ここではオプションでプレフィクス関連の情報を表示するように指示している．この結果から，3ffe:501:100f:1000::/64というプレフィクスがfe80::200:39ff:fecd:4107というルータによって通知されていることがわかる．その後に続く 2 つの ping6 コマンドの出力は，設定されたアドレスが実際のパケットのソースアドレスとして使用されていることを示している．なお，2 つの出力のうち最初のものは N1 上への出力であり，後のものは N1 外への通信である．

次に，ホスト M がネットワーク N2 に移動し，システムが移動を検出した状態での出力例を図 12に示す．

ifconfigコマンドの出力結果において，以前のアドレスにdetachedという表示が追加されていることがわかる．これは，このアドレスは detached なプレフィクスから生成されたもので，新たな通信のプレフィクスとしては使用されないことを意味している．実際，ndpコマンドの結果によれば，移動前のネットワーク N1 のプレフィクスである3ffe:501:100f:1000::/64 を通知しているルータは存在していない．ping6 コマンドの結果からは，N1 で使われていたプレフィクスを持つアドレスへの通信にも新しいアドレスを使っていることがわかる．また，図 12には現れていないが，このパケットは実際に N2 内のルータ R2 に送られている．

```
[8]% ifconfig ep0
ep0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 3ffe:501:100f:1000:260:8ff:feb2:5cfe prefixlen 64
        inet6 3ffe:501:100f:2000:260:8ff:feb2:5cfe prefixlen 64

[9]% ndp -p
3ffe:501:100f:2000::/64 if=ep0
  flags=LA, vltime=2592000, pltime=604800, expire=29d23h59m15s
  No advertising router
3ffe:501:100f:1000::/64 if=ep0
  flags=LA, vltime=2592000, pltime=604800, expire=29d23h57m7s
  No advertising router

[10]% ping6 -n -c 1 3ffe:501:100f:1000:2a0:c9ff:fe55:e0c9
PING6(56=40+8+8 bytes) 3ffe:501:100f:1000:260:8ff:feb2:5cfe -->
                       3ffe:501:100f:1000:2a0:c9ff:fe55:e0c9

[11]% ping6 -n -c 1 3ffe:501:100f:2000:2a0:c9ff:fe55:e0c9
PING6(56=40+8+8 bytes) 3ffe:501:100f:2000:260:8ff:feb2:5cfe -->
                       3ffe:501:100f:2000:2a0:c9ff:fe55:e0c9
```

図 13 ルータに不良がある環境での操作例

Fig. 13 Operation on a network which has no valid router

最後に，ネットワーク N2 においてルータ R2 が不良になった場合の操作例を図 13に示す．

図 13では，ifconfig コマンドの出力結果からdetachedの表示が消えている．これは，ndpコマンドの結果からわかるように，すべてのプレフィクスについて，通知するルータが存在していないからである．このような場合には，2 つのプレフィクスはともに現在のネットワーク上に存在するものとみなされ，ping6コマンドの出力結果では，それぞれ宛先のプレフィクスに適合するソースアドレスが選ばれている．このうち，プレフィクス3ffe:501:100f:1000::/64についてはネットワーク N2 外のものであるため通信は成功しないが，すべてのルータが不良となっている環境においてはソースアドレスの如何に関わらず通信は成功しないので，実用上の問題はない．

6. 課　　題

5.3節で示したように，本稿で示したモデルと実装は実際の移動環境において十分な機能を提供するが，モデルおよび実装の両面において今後解決すべき課題が残されている．本節ではその課題を概観する．また，Mobile IPv6 との関係についても述べる．

6.1 到達不能検出にかかる時間

本モデルおよびその実装は，移動前のルータや不良ルータを到達不能検出によって迅速に排除できることを前提としている．しかし，実際には到達不能性の検出はネットワークごとに固有に与えられる到達可能期間（reachable time）に依存している．移動先のネットワークにおいてこの期間がたとえば数十分単位の大きな値に設定されている場合には，本実装による移動検出は

有効には働かない．

ただし，現存するネットワークでは，到達可能期間をこのような大きな値に設定するメリットは存在しない．したがって，ネットワークの設定誤りを除けば実際上の問題は少ないといえる．

6.2 ルータの識別法

ルータ通知メッセージのソースアドレスは，近隣探索プロトコルの仕様によりリンクローカルアドレスを用いるように定められている．このため，本実装ではカーネルとユーザ空間の双方でリンクローカルアドレスを用いてルータを識別する．しかし，リンクローカルアドレスの一意性はそのリンクの外では保証されない．このため，理論上は移動前のルータと移動先のルータが同じリンクローカルアドレスを用いていることも起こり得る．この場合も本実装は有効には機能しない．

ただし，現在の IPv6 のアドレス体系では，ノードの識別子には 64 ビットの空間が用いられ，しかもこの識別子は通常イーサネットアドレスのような一意性の高いものをもとに生成される．したがって，実際の環境では識別子，すなわちアドレスの衝突はほとんど起こり得ないと考えてよい．

6.3 移動検出法

5.2節で述べたように，本実装では移動の検出にインタフェースの状態監視または定期的な探索パケットの送信を用いている．定期的なパケット送信はネットワーク資源の浪費であり，望ましくない．また，移動検出のタイミングがパケットの送信間隔に依存するという問題もある．インタフェースの状態監視はネットワーク資源の観点からは望ましいが，現在の実装ではシステム内での定期的なポーリングによって実現されており，システム資源の効率の観点からは問題がある．

これらの問題は，インタフェースの状態変化を非同期に取得するユーザインタフェースによってほぼ解消できる．そのようなインタフェースの検討，実装は今後の課題である．

6.4 Mobile IPv6 との関係

移動環境において IPv6 を使う場合， Mobile IPv6[5] を利用するという方法もある． Mobile IPv6 は移動の事実そのものをユーザから隠蔽することを目的としており，移動ホストを識別するためにホームアドレスとよばれる固定のアドレスを利用する．その結果として， 3節で述べた問題のうち，古いソースアドレスの誤使用については Mobile IPv6 によっても対処できる．

しかし， Mobile IPv6 を用いた場合でも，移動前のネットワークプレフィクスを移動後のリンク内のものとみなしてしまう問題には対処できない．また， Mobile IPv6 では，移動先において気付アドレス (care-of address) とよばれるグローバルアドレスを取得する必要がある．このアドレスを自動設定機能を用いて取得する場合には，やはり古い気付アドレスの誤使用を避けなければならない．

したがって， Mobile IPv6 が利用できる環境においても，こうした場面において本稿で述べた方法を併用することで，移動環境への適応性が増すといえる．

7. おわりに

本稿では， IPv6 のホスト自動設定機能について，その概要と移動環境下で使用した場合の問題点を説明し，その解決法としてプレフィクスとルータを関連させて管理する方法を提案した．また，その実装例を示し，実際の環境下で有効に機能することも示した．

自動設定機能は， IPv6 の主要な改良点のひとつである．ルータにネットワーク情報を設定するだけでホストの自動設定が実現できること，基本仕様の一部として常に利用できることなどから，本質的に移動環境との相性もよい．実際の利用環境において障害となる問題を解消する本稿の方法によって，移動環境でのネットワーク利用，とくに IPv6 の利用が進むものと期待できる．

本稿の最後では，提案する実装における問題についても触れた．とくに，ネットワークの変化を非同期に取得するインタフェースの実現は， IPv6 に限らず広く移動環境において有用と考えられる．今後はこうした拡張機能の可能性についても検討したい．

謝辞　本稿の内容は， KAME プロジェクト内での議論に負うものが大きい．また，実装へのコメント，効果の検証などの面でも KAME プロジェクトのメンバーの多大な協力をいただいた．プロジェクトのすべてのメンバーに感謝したい．

参考文献

1) Deering, S and Hinden, R: Internet Protocol, Version 6 (IPv6) Specification, Internet Draft (1998)
2) Narten, T and Nordmark, S and Simpson, W. A.: Neighbor Discovery for IP Version 6 (IPv6), Internet Draft (1998)
3) Thomson, S and Narten, T: IPv6 Stateless Address Autoconfiguration, Internet Draft(1998)
4) Hinden, R and Deering, S: IP Version 6 Addressing Architecture, RFC 2373(1998)
5) Johnson, D. B. and Perkins, C: Mobility Support in IPv6 Internet Draft(1998)