小規模組織に適した IPv6ネットワークの設計と構築

東京工業大学 理学部
情報科学科
白砂 哲
(学籍番号 9514396)

平成10年度学士論文

指導教官 大野 浩之 講師

平成 11 年 3 月 5 日

目 次

1 はじめに 4

2 ネットワークの設計構築技法 5
2.1 ネットワーク形態の多様化と設計構築技法 5
2.2 ネットワーク設計構築技法の現状 5
2.3 運用技法の特徴と問題点 5
2.3.1 運用技法の分類 6
2.3.2 運用技法の比較 6
2.4 小規模組織ネットワークの研究意義 6
2.5 IPv4 の問題点 6
2.6 次世代インターネットプロトコル (IPv6) の特徴 7

3 小規模組織における IPv6 ネットワーク 10
3.1 小規模組織における IPv6 導入の利点 10
3.2 小規模組織における IPv6 の導入技法の分類 10
3.2.1 IPv6 ネットワークの新規構築 11
3.2.2 IPv4 からの移行 11
3.3 小規模組織が IPv6 を導入するための技術 12
3.3.1 IPv4 と共存するための技術 12
3.3.2 ホストの対応 14
3.3.3 アプリケーションの対応 14
3.3.4 セキュリティ 14
3.3.5 外部接続性 14

4 小規模組織における IPv6 ネットワークの構築 15
4.1 ネットワークの構築 15
4.2 IPv4 との共存 16
4.3 各ホストの対応 17
4.4 各種サーバの対応 17
4.5 アプリケーションの対応 17
4.6 セキュリティ 18
4.7 外部接続 18
4.8 IPv6 対応 INS ルータ 21

5 実験と評価 26
5.1 大野研究室 IPv6 ネットワーク運用実験 26
5.1.1 実験環境 26
5.1.2 メール環境 26
5.1.3 Web 環境 27
5.1.4 評価 28
5.2 IPv6 対応 INS ルータ 29
5.2.1 接続実験 29
5.2.2 評価 30

6 考察 32
6.1 ネットワーク運用技法の考察 32
6.2 INS ルータの考察 32
6.3 今後の課題 33
6.3.1 INS ルータの実装上の課題 33
6.3.2 ネットワーク構築技法の改良 35

7 おわりに 36

図の一覧

2.1 IPv4 ヘッダ 8
2.2 IPv6 ヘッダ 8

3.1 デュアルスタック 12
3.2 カプセル化 13
3.3 トンネル 13

4.1 IPv6 ネットワーク構成 15
4.2 IPv6 大野研究室ネットワーク構成 16
4.3 ブリッジ接続 19
4.4 2 組織以上とのブリッジ接続 例 1 19
4.5 2 組織以上とのブリッジ接続 例 2 20
4.6 PPP 接続 22
4.7 IP6 タスク 23
4.8 IPV6CP 25

5.1 PPP 実験環境 30

6.1 現在のタスク構成 33
6.2 タスク構成案 34

第1章

はじめに

インターネット利用者の爆発的な増加とともに、ネットワークを構築する組織が増加し、その形態も多様化してきた。特に、小規模な組織がその起動性を活用し、家庭内 LAN など、多様な形態のネットワークを構築する例が増加している。これらの多様な利用形態に対応したネットワーク構築技法が必要である。

ところで、現在インターネットで使われているネットワーク層プロトコル (以下 IPv4 と記す) には、アドレス空間の不足や経路表の増加などの深刻な問題がある。このため常時接続型プロバイダを利用しても、わずかなアドレスしか割り当てられないため、ネットワークを利用するには NAT などで疑似的に利用できるアドレス空間を増加させる必要がある。これらの問題を根本から解決するために、次世代インターネットプロトコル (以下 IPv6 と記す) への移行が始まり、大規模組織のネットワーク構築技法が小規模組織のネットワーク構築に必ずしも適用できないことは、IPv4 と同じである。そのため、小規模組織の IPv6 ネットワーク構築技法を確立し、小規模組織が IPv6 の恩恵を受けるための基盤を整備する必要がある。これにより、小規模組織のネットワークにおいても十分な大きさのアドレス空間を所有できる。また、接続先の変更が起こりやすい小規模組織にとって、IPv6 の特徴であるアドレスの自動設定は管理の負担を軽減できる。

家庭内ネットワークや SOHO などの小規模組織は外部ネットワークとの接続に、INS ルータを用いたダイアルアップ接続や、常時接続サービスを利用している。そのため、小規模組織が IPv6 を用いて外部の組織と接続するためには IPv6 に対応した INS ルータが必要であると考える。INS ルータは低価格であり、管理の手間がかからないので、資金や管理経験を期待できない小規模組織に適する。今回、既存の INS ルータに対して、新たに IPv6 のプロトコルスタックを実装した。

本研究では、小規模組織に適した IPv6 ネットワークの容易な構築を目的としている。そして、INS ルータを用いた IPv6 ネットワークの構築技法を提案する。次に、実在する小規模組織に本技法を適用し、実際に小規模組織に適した IPv6 ネットワークを構築する。さらに、構築したネットワークを運用評価し、本技法の有効性を検証する。

第2章

ネットワークの設計構築技法

本章では、ネットワークの設計構築技法について述べる。

2.1 ネットワーク形態の多様化と設計構築技法

近年のインターネット利用者の爆発的な増加によりネットワーク形態は多様化してきた。インターネットを用いたさまざまなサービスが開始され、利用形態が多様化して来きた。サービスの多様化により、サービスに応じたさまざまなネットワークが存在する。企業内ネットワークであるイントラネットや、零細企業が導入している SOHO などである。また教育機関もネットワークを導入し、図書館の検索サービスや学生の教育などに役立てている。一般家庭内においても数台の PC をつなぐためにネットワークが導入され、近い将来、家電製品もネットワークに接続される。以上に述べたさまざまな形態のネットワークを構築する技法が確立されていれば、ネットワークの構築、運用にかかる労力が軽減される。

2.2 ネットワーク設計構築技法の現状

今までのネットワーク構築は大規模組織によってなされてきた。例えば、大規模な研究機関、プロバイダ、大企業等である。大規模組織に適したネットワーク構築技法は、研究されてきたが、それらは小規模組織のネットワークには必ずしも適応できない。

2.3 運用技法の特徴と問題点

ネットワークの形態が多様化したため、すべてのネットワークを単一の技法により運用するのは合理的ではない。本節では、ネットワークの運用技法を分類し、比較する。

2.3.1　運用技法の分類

運用技法は大きく 2 つに分けられる。大規模組織におけるネットワーク運用技法と小規模組織におけるネットワーク運用技法である。

2.3.2　運用技法の比較

大規模組織におけるネットワークの現状を示す。

- 知識が十分にある管理者が存在する。
- 利用者と管理者が独立している。
- 資金が豊富である。

それに対して、小規模組織のおけるネットワークの現状を示す。

- 管理者の数が少ない、知識のある管理者がいない。
- 利用者が管理者を兼ねている場合が多い。
- 資金が限られている場合が多く、限られた資源を用いてネットワークを運用しなければならない。

よって、大規模組織におけるネットワークの運用技術を小規模組織におけるネットワーク運用技術として利用することはできない。それぞれ別の技術が必要である。

2.4　小規模組織ネットワークの研究意義

大規模組織に適したネットワークの構築技法は研究されてきた。しかし、小規模組織に適したネットワークの研究は十分ではない。

現在のネットワーク構築技術は、OSI の 7 階層モデルにおけるネットワーク層であるインターネットプロトコルに依存する所が大きい。時節では、インターネットプロトコルに着目し、考察する。

2.5　IPv4 の問題点

現在、インターネットのネットワーク層のプロトコルは、Internet Protocol Version4 (以下、IPv4 と略記する)[1] が用いられている。しかし、ここ数年におけるインターネットの爆発的な発展に伴い、さまざまな問題点が生じてきた。その問題点を以下に示す。

- インターネット利用者の増加や IP アドレスの無計画な割り当てのために、IP アドレスが不足する。

- ホスト数の増加に従い、経路表が増大する。

これは、IPv4 が 20 年近く前に作られたプロトコルであり、現在ほどのインターネットの普及を想定していなかったことに起因する。

例えば、現在の IP アドレスは、32 ビットである。これは、最大 2^{32} (約 43 億) 個のホストしか識別できないことを意味する。これは、一人一台以上の端末を持つ今の時代には適さない。

これらの問題に対処するため、以下の技術が考案された。

CIDR CIDR は IP アドレスのクラスの概念を取り払うことにより、IP アドレスの無駄な割り当てをなくし、集約的な経路制御を実現する。連続したクラス C アドレスを同一の組織に割り当て、経路表の増加を防ぐ。

しかし、CIDR の導入以前に割り当てられた IP アドレスについては、経路が集約されていない。また、プロバイダの変更による IP アドレスのつけ直しはネットワーク管理者が行なう必要があるため、人的なコストを要する。

NAT NAT は、組織内ではプライベートアドレスを用い、組織外とはプライベートアドレスをグローバルアドレスに変更して通信する仕組みである。しかし、IP アドレスがパケットのデータ部に入っている場合にはそれらも変更しなければならない。IP アドレスがデータ部のどの部分に入っているのかは、アプリケーションごとに異なるので、個別に対応しなければならない。FTP などのメジャーなアプリケーションは対応されているが、ネットワークの利用方法が多様化している現在、次々と新しいアプリケーションが作られる。新しいアプリケーションが作られるたびに個別に対応するのは現実的ではない。

2.6 次世代インターネットプロトコル (IPv6) の特徴

現在 IETF[2] において、Internet Protocol Version6 (以下、IPv6 と略記する)[3] の仕様が定まりつつある。IPv6 は、IPv4 の欠点を補い、IPv4 に置き換わるプトロコルである。

IPv6 の主な特徴を以下に述べる。

アドレス空間 アドレス空間が 32bit から 128bit に拡張された。2^{128} は非常に大きな値であり、IP アドレスの枯渇の心配はない。

ヘッダ IPv4 で使用頻度の少なかったヘッダフィールドを削り、ヘッダを簡略化した。図 2.1 が IPv4 のヘッダであり、図 2.2 が IPv6 のヘッダである。

各フィールドの説明と IPv4 ヘッダとの対応を書く。

またオプションを一般化し、拡張ヘッダとして実現した。これらは、中継するルータの負担が軽減するように設計されている。

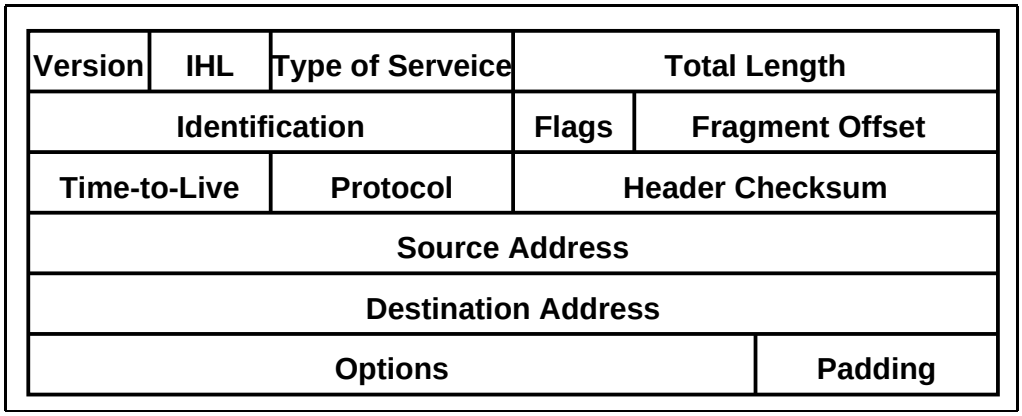

図 2.1 IPv4 ヘッダ

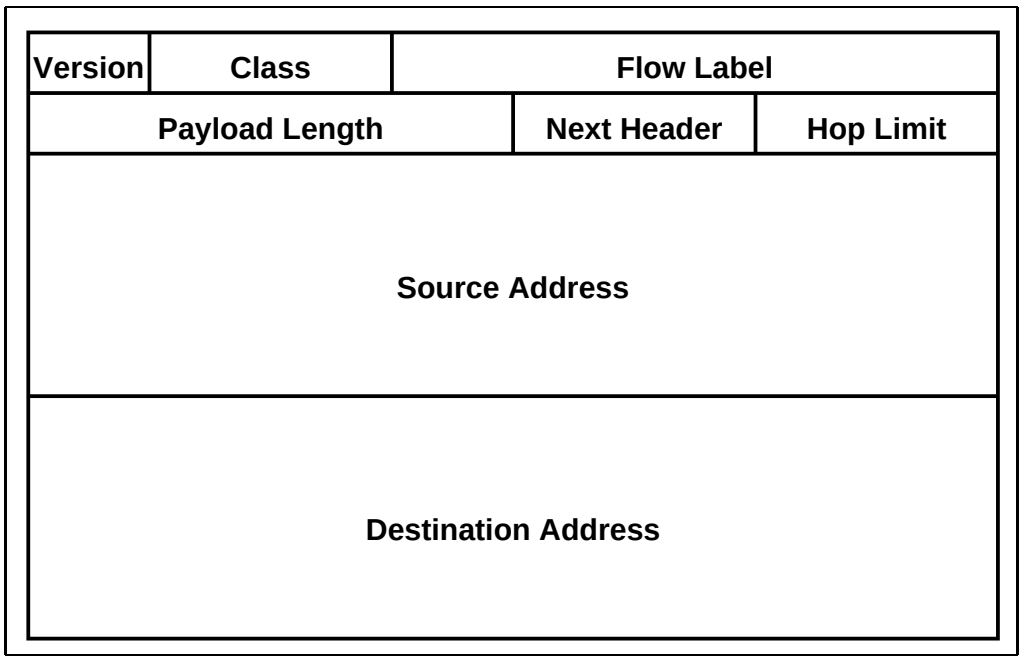

図 2.2 IPv6 ヘッダ

フローラベル フローラベルというフィールドを設け、ネットワーク層でのデータの流れに上位層から関与することができる枠組を提供した。これにより、リアルタイム通信が必要なマルチメディアコンテンツに対応できる。

セキュリティ 電子マネーなどにより、ネットワーク層レベルでのセキュリティが必要になっている。ネットワーク層における暗号化や認証を提供した。

アドレスアーキテクチャ アドレスに構造を持たすことにより、経路情報を集約した。また、アドレスの自動設定やエニーキャストなどの機能を提供した。

第3章

小規模組織における IPv6 ネットワーク

本章では、小規模組織における IPv6 ネットワークの導入技法と導入するために用いる技術について述べる。

3.1 小規模組織における IPv6 導入の利点

小規模組織は、専用線や INS 回線を用いてプロバイダに接続していることが多い。IPv4 アドレスの不足から、クラス C のアドレスをもらうことも難しくなってきている。家庭内でネットワークを持っている人は、プロバイダから 1 つのグローバルアドレスをもらい、NAT を用いてネットワークを運用している。NAT を用いてネットワークの外側にサービスを提供する場合、設定が必要になり、管理者の負担を増大させている。

IPv6 は膨大なアドレス空間をもつため、小規模組織にも大量のアドレスを割り振れる。よって、NAT を用いる必要はない。

また、小規模組織においては、接続先の ISP を変更することが多い。IPv4 では、そのたびにすべてのホストの IP アドレスを変更してきた。しかし、IPv6 においては、ルータの IP アドレスを設定すれば、ホストの IP アドレスは自動的に設定されるので管理の手間が軽減される。また、接続先の ISP が 2 箇所ある場合など、1 つのホストが 2 つの IP アドレスを同時に持てるので、柔軟な対応ができる。

3.2 小規模組織における IPv6 の導入技法の分類

小規模組織において IPv6 を導入する方法を分類する。小規模組織が既に IPv4 のネットワークを運用している場合と、ネットワークを新しく構築する場合の 2 種類が考えられる。既に IPv4 のネットワークを運用している場合は、IPv4 のネットワークを IPv6 のネットワークに移行する方法をとる。一方、新しくネットワークを構築する場合は、新規に IPv6 ネットワークを構築する方法をとる。

3.2.1 IPv6 ネットワークの新規構築

インターネットの拡大により、これから新たに IPv6 を導入する小規模組織が増大すると考えられる。IPv4 ネットワークを構築することも考えられるが、今後、IPv6 が普及することを考えると、IPv6 のネットワークを構築する方が良い。しかし、インターネットの大半のネットワークは IPv4 によって構築されているので、IPv4 のネットワークと共存するために、IPv4 と IPv6 の両方に対応したネットワークを構築することが必要とされる。

まず、ルータのプレフィックスを設定し、ネットワークの骨組みを構築する。IPv6 の特徴であるアドレスの自動設定により、ホストのアドレスは自動的に設定される。

3.2.2 IPv4 からの移行

現在、ほとんどの小規模組織のネットワークは IPv4 で構築されている。それらの組織は将来に備えて IPv6 に対応することが望まれる。

IPv6 に対応する方法として、以下の方法がある。

- IPv4 のネットワークを放棄し、IPv6 のネットワークとして再構築する。
- IPv4 のネットワークと別に IPv6 のネットワークを構築し、そちらに移行する。
- IPv4 のネットワークを IPv6 のネットワークに移行させる。

IPv4 のネットワークを放棄し、IPv6 のネットワークとして再構築する利点は、既存のネットワーク構成にとらわれることなく、IPv6 のネットワークを構築できることである。欠点としては、再構築している期間、IPv4 のサービスを停止しなければならないことである。常に動いている必要がない小人数のネットワークにおいて有効な手段である。

IPv4 のネットワークと別に IPv6 のネットワークを構築することの利点は、IPv4 のサービスを停止することなく、IPv6 のネットワークを構築できることである。欠点として、資金が余分にかかることがあげられる。資金が豊富にある組織にとっては有効な方法であるが、小規模組織の多くは、資金が豊富でないので適さない。

資金が少なく、恒常的なサービスを提供するネットワークにおいては、IPv4 のネットワークを IPv6 のネットワークに移行させるのが有効な手段であると考える。しかし、次のことに注意しなければならない。

- 既存のサービスを停止することなく IPv6 に移行する。

  既に IPv4 のネットワークで様々なサービスを提供しているのでそれらのサービスを停止することなく IPv6 に移行することが必要である。

- IPv6 に対応していないサービスが存在する。

  提供しているサービスが IPv6 に対応していないことが考えられる。移行の際にはこれらのサービスをどう扱うのかを考えなければならない。

3.3　小規模組織が IPv6 を導入するための技術

3.3.1　IPv4 と共存するための技術

IPv6 が IPv4 と共存するため、または IPv4 から IPv6 への移行するために、さまざまな技術、方法が利用できる。それらについて紹介、検討する。

デュアルスタック

IPv4 との互換性を保ちつつ IPv6 を使用するにはデュアルスタックと呼ばれる手法を用いる。デュアルスタックとは、IPv4 と IPv6 の両方のプロトコルを備えることである (図 3.1)。デュアルスタックのホストは、IPv4 のホストとは IPv4 を用いて通信し、IPv6 のホストとは IPv6 を用いて通信をする。

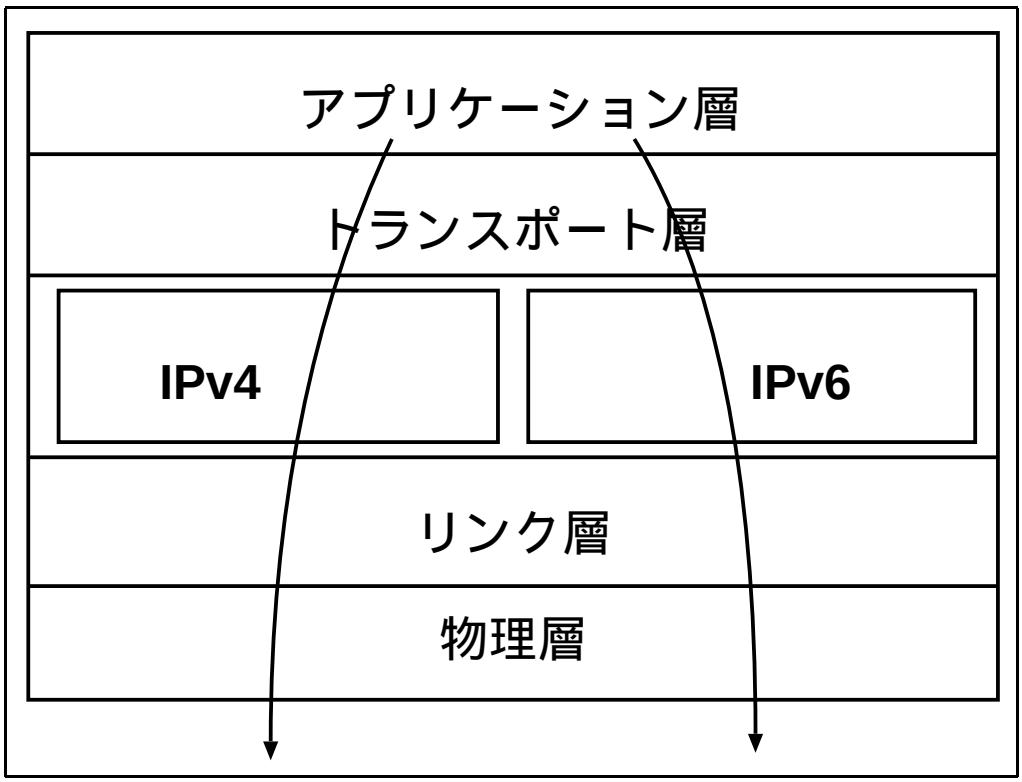

図 3.1 デュアルスタック

トンネルリング

IPv6 への移行の初期には、IPv4 だけを中継できるネットワーク (IPv4 ネットワーク) を介さなければ通信できないことが予想される。IPv6 のパケットを IPv4 のネットワーク内を転送するためにはトンネリングを用いる。まず、IPv6 のパケットを IPv4 のペイロー

ドとして格納する。このことをカプセル化 (図 3.2) と言う。そして、IPv4 ネットワーク内を転送する (図 3.3)。IPv6 だけを中継できるネットワーク (IPv6 ネットワーク) に到着すると、IPv4 のペイロードトから IPv6 のパケットを取り出す。

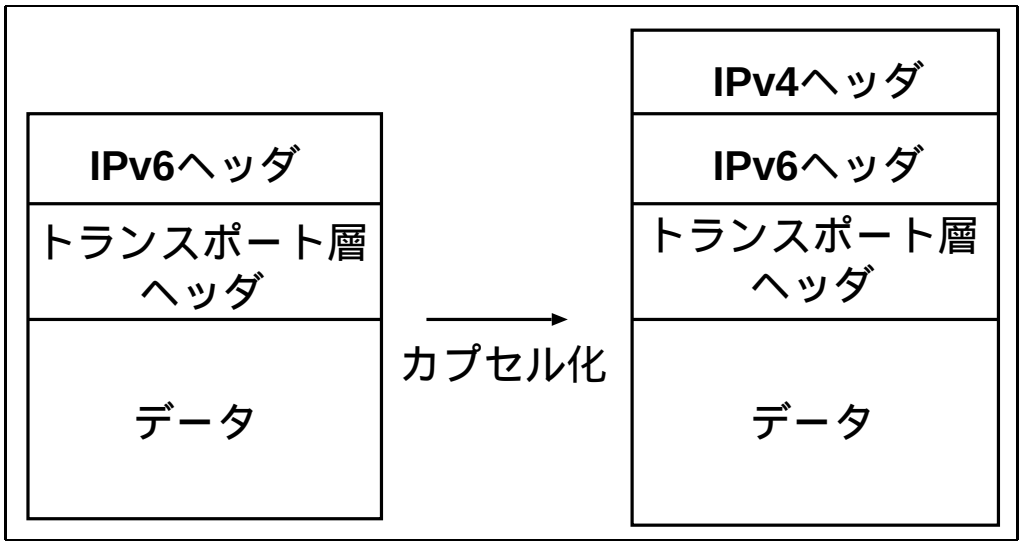

図 3.2 カプセル化

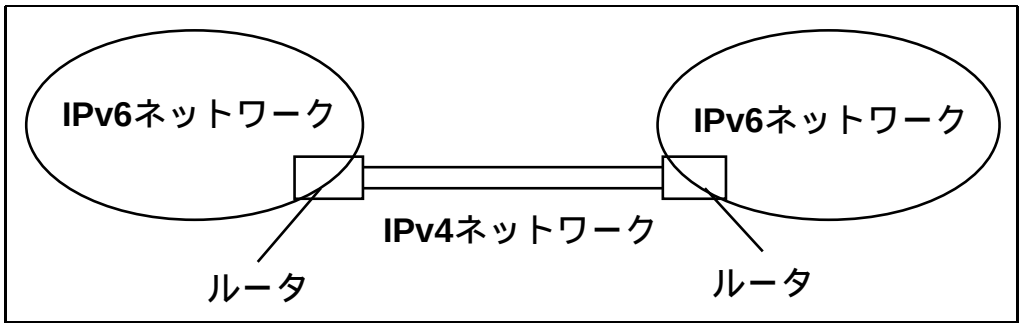

図 3.3 トンネル

逆に、移行の終期には、IPv6 だけのネットワークが増えてくるので、IPv4 ネットワーク同士が通信するためには、IPv4 のパケットを IPv6 のパケットにカプセル化し、IPv6 ネットワーク内を通す。

トランスレータ

すべての IPv4 のホストを IPv6 に対応させるのには、労力と時間がかかる。また、将来 IPv6 が十分に普及した状態であっても、管理者がいないなどの理由で IPv6 に対応しないホストも存在すると思われる。この場合、トランスレータを用い、IPv4 のパケットを

IPv6 のパケットに変換する。トランスレータにより、IPv4 しか備えていないホストでも IPv6 しか備えていないホストと通信できる。

3.3.2 ホストの対応

IPv6 のネットワークを構築するには、すべてのホストが IPv6 のプロトコルスタックを備えることが必要である。IPv4 を視野に入れるとデュアルスタックにするのが良い。現在開発が進められている IPv6 のプロコトルスタックはほとんど IPv4 と IPv6 のデュアルスタックとして作られているので、それらを使うのが良い。

3.3.3 アプリケーションの対応

アドレス長が変化したことにより、OS が提供するネットワーク API にも変化が加えられる [4]。このためアプリケーション側での変更も必要になった。

すべてのアプリケーションが IPv6 に対応するのが望ましいが、アプリケーションの数は膨大であり、既にメンテナンスされていない物もある。

従って、IPv4 のアプリケーションを IPv6 用に変換する機構が必要である。

3.3.4 セキュリティ

ネットワークを構築するに際してセキュリティにも気をつけなければならない。これは、大規模ネットワークだけでなく、小規模ネットワークにも言える。

外部からの侵入を防ぐためには、ファイアウォールを構築する。ファイアウォールを作る際には、ポリシを定め、それに従って設計することが必要である。

また、IPv6 ではネットワーク層で暗号化を行なう仕組みがある。それを用いて、通信の途中でデータの盗聴や改ざんを防ぐことが必要である。

3.3.5 外部接続性

家庭内ネットワークや SOHO などの小規模組織は外部ネットワークとの接続に、INS ルータを用いたダイアルアップ接続や、常時接続サービスを利用している。これらの接続方式では、通信速度は高速ではないので、高性能のルータは必要ではない。そこで、PC ルータか、低価格の INS ルータを用いることが多い。

PC ルータは、PC UXIX 等に IPv6 のプロトコルスタックをインストールすることで、作成する。この方法では、管理者にある程度の技能が必要とされる。

最近では、管理者の技能不足などから、既存の INS ルータを用いていることが多い。この場合には、メーカーが IPv6 に対応した INS ルータを製造することが必要となる。多くの場合は、ファームウェアのバージョンアップによって対応できる。

第4章

小規模組織における IPv6 ネットワークの構築

小規模ネットワークが IPv6 へ移行する例として、大野研究室ネットワークの事例を示す。

4.1 ネットワークの構築

大野研究室では、小規模組織用ネットワークの研究が既に行なわれている [5]。そのため、小規模組織用の IPv6 ネットワークを構築の実験をするのに適している。

ネットワークの構築する際、その組織や接続先の組織の運用ポリシを守る必要がある。東京工業大学キャンパス情報ネットワークである。Titanet の運用ポリシとして、IPv4 以外のパケットを東京工業大学の基幹ネットワークに流すことができない。そこで、大野研究室は、松下電送システムと INS 回線を用いて接続している (図 4.1)。松下電送システムは WIDE 6BONE につながっている。

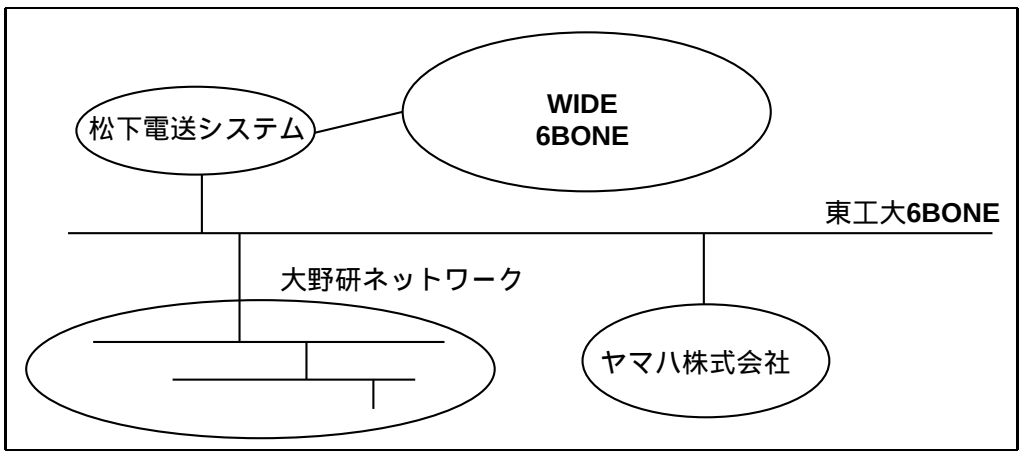

図 4.1 IPv6 ネットワーク構成

東京工業大学内で IPv6 ネットワークを組む組織のために東工大 6BONE を作り、その

運用を行なっている。東工大 6BONE の運用は IPv6 の普及にともない Titanet に受け継がれる予定である。現在は、共同研究を行なっているヤマハ株式会社と接続されている。

大野研究室の IPv6 ネットワークは東工大 6BONE に接続する形で構築した (図 4.1)。

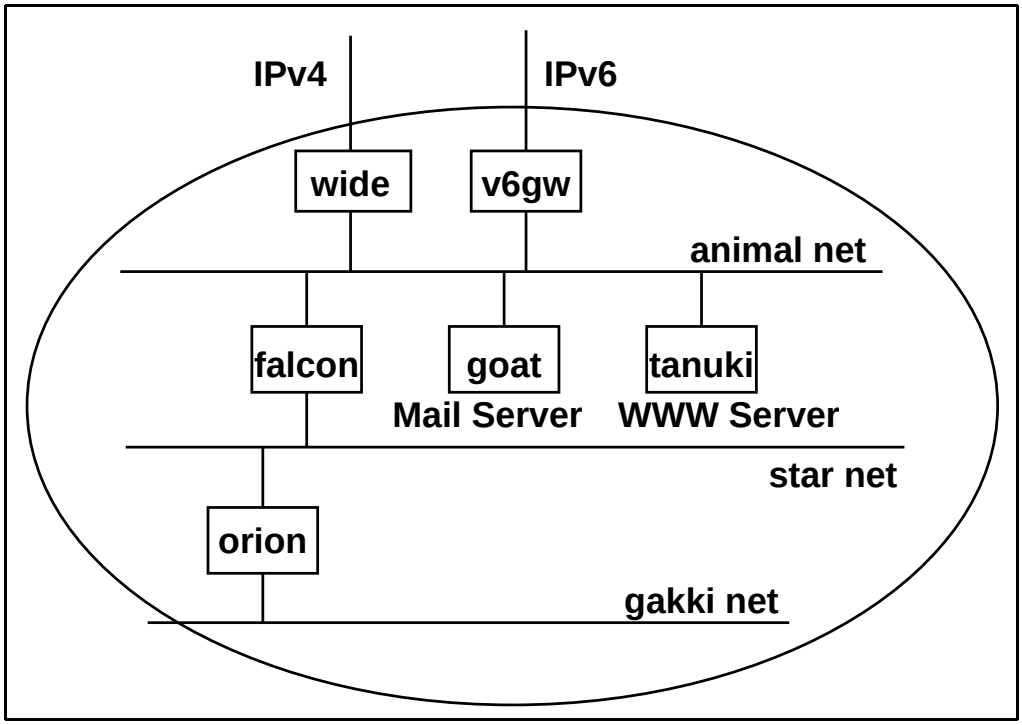

図 4.2 IPv6 大野研究室ネットワーク構成

IPv6 のパケットは東京工業大学の基幹ネットワークに通すことができたいので、IPv4 と IPv6 のネットワークは、外部との接続口が違う。

経路制御は、PC ルータである falcon と orion でルーティングデーモンを起動させており、RIP を用いて行なっている。

また、アドレスを動的に割り振るために falcon と orion では、router advertisement を送るためのデーモンを起動させておく。

4.2 IPv4 との共存

大野研究室のネットワークは、IPv4 のネットワークとして運用されている。そこでデュアルスタック戦術を用い、IPv6 のネットワークと IPv4 のネットワークが共存する形で構築した。よって、IPv4 で提供しているものを IPv4 と IPv6 両方を提供する物に置き換えた。

各ホストは、デュアルスタックにすることにより対応した。また、各種サービスは、IPv4 に対応したものを、IPv4 と IPv6 両方に対応したものに置き換えた。

4.3 各ホストの対応

大野研内の各ホストを IPv6 に対応させる。大野研究室では、統一した計算機プラットホームとして PICKLES 端末 [6][7] を利用している。PICKLES 端末は PICKLES プロジェクトの一環として大野研究室が開発している端末であり、PC UXIX の一種である BSD/OS を利用している。

PICKLES Version 2.00 DR3 からは、IPv6 対応となったため、大野研究室のほとんどのマシンは、IPv6 対応となった。PICKLES を IPv6 対応するために KAME[8] を用いた。

これにより、大野研内の各マシンが IPv4 と IPv6 のデュアルスタックとなった。

4.4 各種サーバの対応

DNS

DNS[9] は、goat で行なっている。bind は、IPv6 に対応しており、IPv6 用のレコードである AAAA レコードを扱える。ルータ、Web サーバ、メールサーバなどの主要なアドレスを AAAA レコードとして、登録する。

Mail サーバ

goat で行なっている Mail サーバを IPv6 に対応させた。MTA は qmail を用いているので、IPv6 に対応した qmail を導入した。

WWW サーバ

tanuki で行なっている WWW サーバを IPv6 に対応させた。サーバソフトは apache を用いていたので、IPv6 に対応した apache を導入した。

4.5 アプリケーションの対応

IPv4 で可能であったことを IPv6 でも可能にすることを目標に対応を行なった。

基本コマンド

telnet、ftp 等の基本的なコマンドは、KAME に含まれる。よって、KAME をインストールすることにより使用可能となる。

管理コマンド

基本コマンドと同様に基本的な管理コマンドは、KAME に含まれる。よって、KAME をインストールすることにより使用可能となる。

Mail

PICKLES では、MH を用いてメールサーバからメールを取得している。MH は、IPv6 に対応していないので、SSH を用いてトンネルを作り、メールを所得する。

個人マシンなどでは、IM を利用している利用者もいる。IM は IPv6 に対応しているので、メールサーバから直接メールを所得できる。

WWW ブラウザ

IPv6 に対応した Lynx を導入した。

今後、IPv6 に対応した mozilla を導入する。

4.6 セキュリティ

大野研では、外部からのログインには、SSH を用いている。IPv6 に対応した SSH を導入することにより、IPv6 で外部よりログインできる。

ファイアウォールは問題であった。IPv4 の外部との接続地点には、TCP Wrapper と Screend を用いて、アクセス制限をかけている TCP Wrapper は、IPv6 に対応した物が、存在したが、Screend は存在していない。TCP Wrapper と同じ働きをする ip6fw が FreeBSD には存在するので、ファイアウォールマシンを FreeBSD にすることも検討した。

現在は、普段はルーティングを止めており、必要な時のみ使う方針にしている。

4.7 外部接続

大野研究室では、松下電送システムを通して WIDE 6BONE に接続している。WIDE 6BONE とは IPv6 の実験ネットワークである。WIDE 6BONE にはさまざまな組織が接続し、実験を行っている。

松下電送システムとは、INS 回線を通して接続されている。現在、IPv6 対応の PPP[10] を備えた INS ルータが存在しないため、ブリッジを用いて接続している (図 4.3)。

また、大野研究室では、ヤマハ株式会社との接続も行っている。2 組織以上との接続方法を組織 A が、 組織 B と 組織 C に接続する例を用いて述べる。

まず、同一のセグメントに繋げる場合を考える図 4.4。

この方法の利点は、接続組織が増えてもセグメントや計算機を余分に必要としないことである。

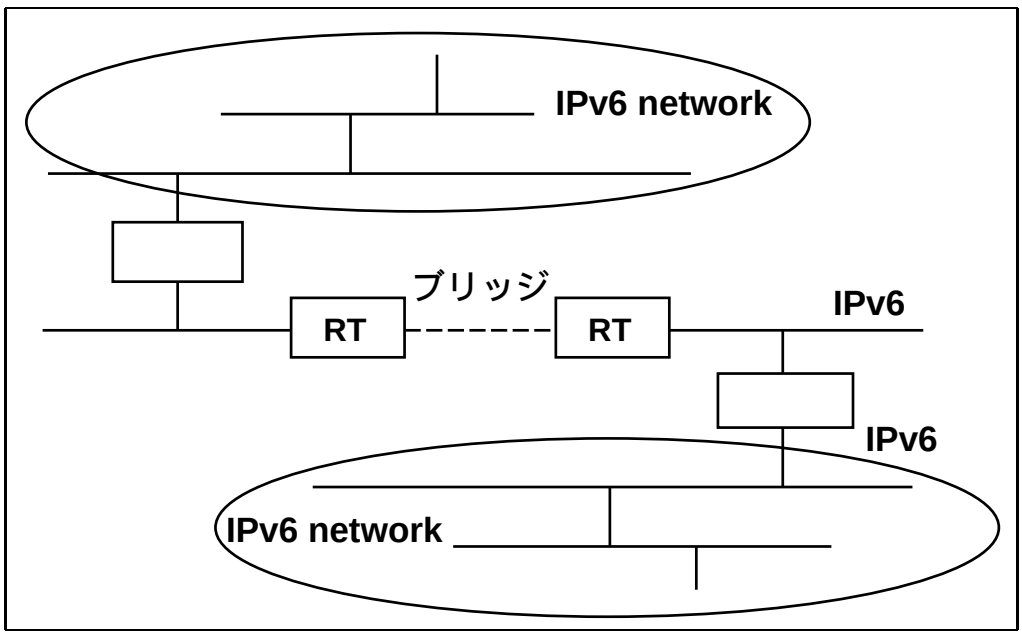

図 4.3 ブリッジ接続

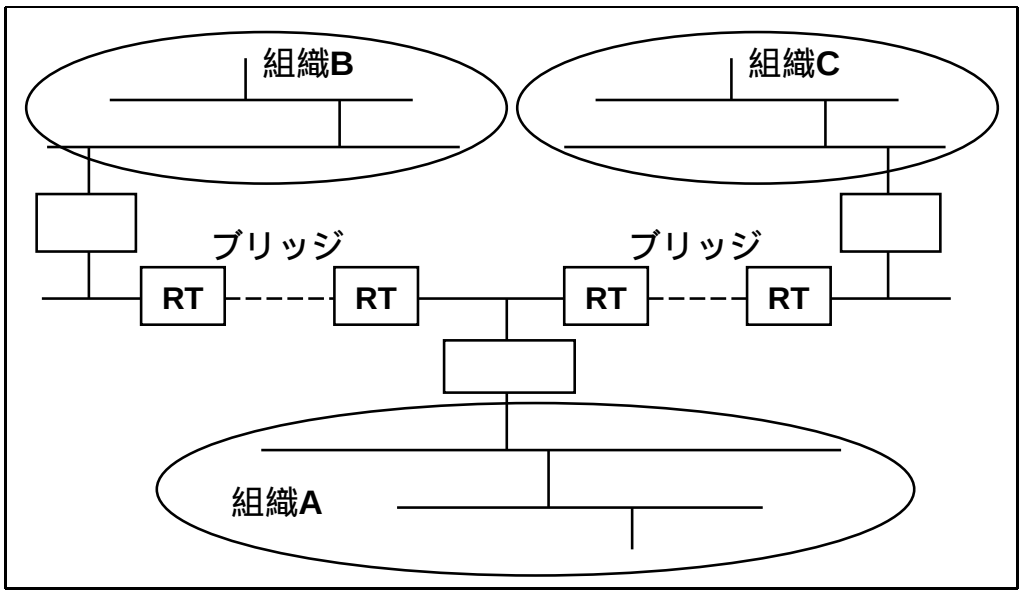

図 4.4 2 組織以上とのブリッジ接続 例 1

一方、この方式には以下に述べるような欠点がある。

- 発呼回数が多い。
- 組織 B と 組織 C が同じネットワークアドレスを使わなければならない。

などがあげられる。

組織 B と 組織 C は同一のセグメントにあるので、組織 A が組織 B と通信している時にも 組織 C に発呼してしまう。この問題は、イーサーネットアドレスでフィルタリングすることで対応できると考えられる。しかし、ブロードキャストの対応が困難である。

組織 B と 組織 C が同じネットワークアドレスを使うことは、接続先組織のポリシに反する可能性があるため解決は困難であることが多い。

そこで大野研究室がとった方式は、図 4.5 のように接続組織ごとに別のセグメントを用意する方法である。

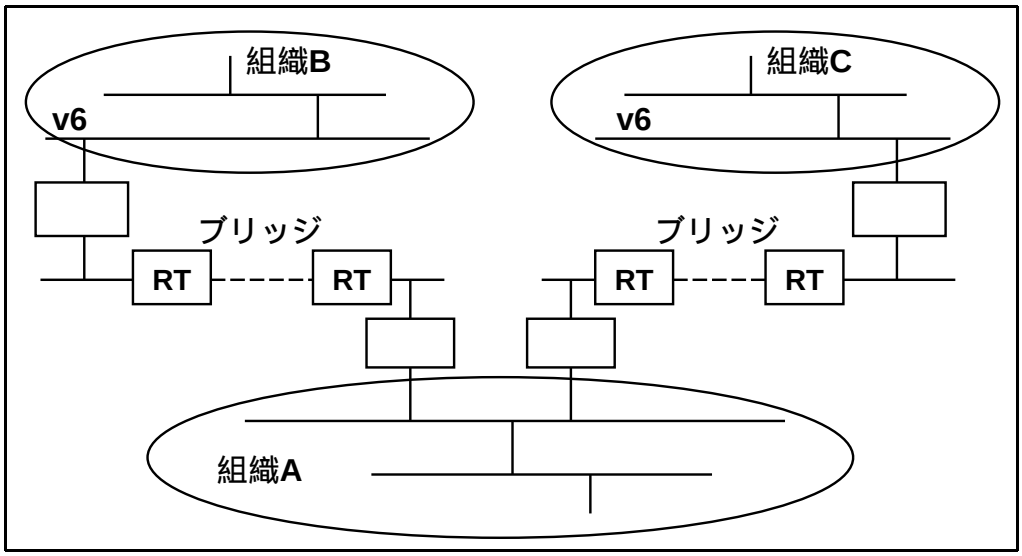

図 4.5 2 組織以上とのブリッジ接続 例 2

この方式の欠点を以下に示す。

- 接続組織が増えるたびにセグメントが余分に必要となる。
- 接続組織が増えるたびに PC が余分に必要となる。

アドレスの枯渇が叫ばれている現在、接続組織が増えるごとにセグメントを消費するのはよくない。また、接続組織ごとにセグメントと PC を用意するのは、小規模組織にとっては大変である。

INS ルータを IPv6 対応にすることで、ネットワーク資源の浪費などの問題点を防ぐことができる。次節では、この方式について詳しく述べる。

4.8 IPv6 対応 INS ルータ

意義

IPv6 に対応した INS ルータの意義を、以下に列挙する。

- IPv6 ネットワークに PPP で接続できる。これにより、小規模組織が IPv6 のネットワークに接続できる。
- 低価格で容易に IPv6 が導入できるので、IPv6 対応のプロバイダを経由し、小規模ネットワーク、一般家庭においても IPv6 に移行しやすくなる。
- 小規模ネットワーク、一般家庭が IPv6 に対応するので、プロバイダの IPv6 対応を促進し、インターネットの IPv6 化を早める。
- INS ルータに IPv4、IPv6 のトランスレータを実装されると、IPv4 のネットワークを IPv6 ネットワークにつなげられる。

大野研究室での例

IPv6 に対応した INS ルータを用いた接続の利点を、現在の大野研究室での外部接続の方法と比較しながら検討する。

前章で述べたように大野研究室では、図 4.5 に示すブリッジを用いて外部と接続している。IPv6 に対応した INS ルータを用いた例を図 4.6 に示す。本方式の特徴を以下に述べる。

- 無駄なセグメントを使う必要がなくなる。
- 無駄な PC を使う必要がなくなる。
- ブロードキャストにより無駄な発呼が生じなくなる。
- 不要なパケットが INS に流れ込まなくなる。
- 複数の組織と一度に繋げられる。
- ブリッジでは難しかったネットワークアドレスの動的な決定が実現する。

設計

IPv6 対応の INS ルータに必要な最小限の機能を以下に示す。

IPv6 ヘッダ処理 IPv6 のパケットのヘッダを処理し、上位層とのやりとりを行なう。

経路制御 IPv6 のアドレス空間に対応できる経路制御である。

ICMPv6[11] IPv6 対応の制御用メッセージの処理を行なう。

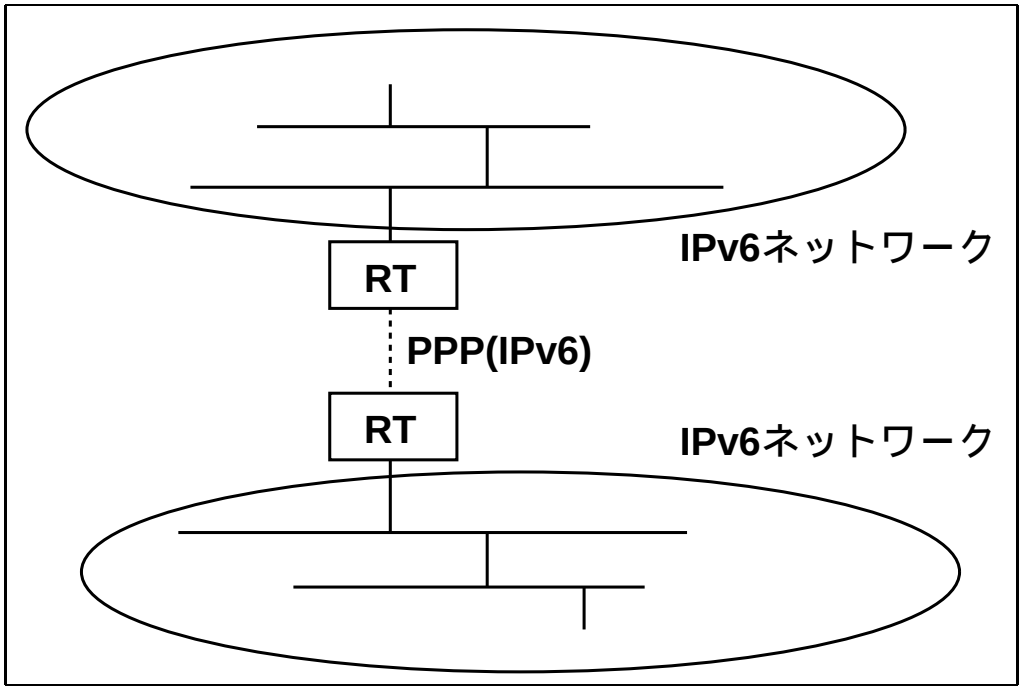

図 4.6 PPP 接続

NDP[12] アドレスの自動設定を行う。

PPP[10] IPv6 の PPP を使える。

実装

具体的な実装について述べる。

概要

ヤマハ株式会社の REMOTE ROUTER RT80i に IPv6 プロトコルスタックを実装する。

ヤマハ株式会社と NDA を結ぶことにより、ソースコードを得た。ルータのコードをすべて書き直すのは作業効率が悪いため、既存のコードに IPv6 のプロトコルを追加実装する。

現行の RT80i は、組み込みリアルタイム OS を用いている。マルチタスクで、メッセージ・パッシングを用いてタスク間で情報を伝達している。

IPv6 プロトコル

Ether、IPv4 プロトコルの処理を行う LAN タスクがある。LAN タスクの中に IPv6 を実装することも考えられるが、IP6 タスクとして独立させて実装することにする (図 4.7)。

タスクを独立することにより、以下の利点がある。

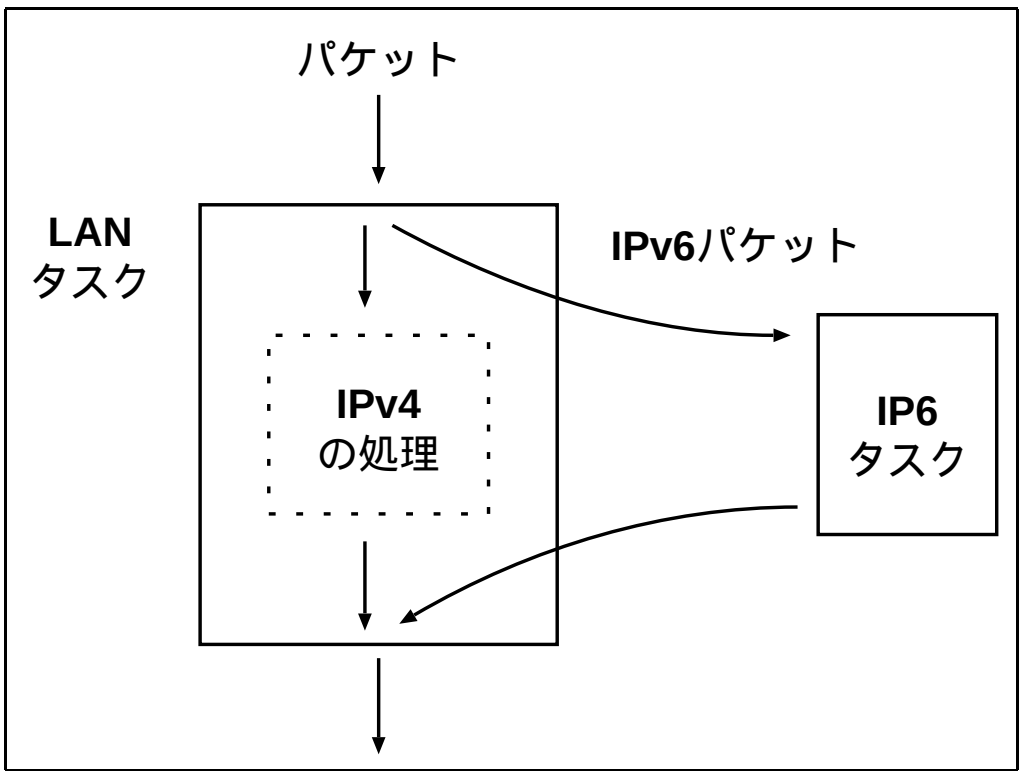

図 4.7 IP6 タスク

- 既存のコードにとらわれず、実装できる。
- IPv4 と IPv6 を別々に開発しやすくなる。

タスク内での処理は、以下の通りである。

- 自分宛のパケットは、各プロトコルに渡す。
- 自分宛以外のパケットは、ルーティングテーブルを検索し、フォワードする。

また、LAN タスクと IP6 タスクの間のメッセージを送受信するインターフェースを作成した。具体的には、LAN タスクで IPv6 のパケットを受け取った時には、メッセージとして IP6 タスクに渡し、逆に IP6 で IPv6 プロトコルの処理を終えたパケットは、LAN タスクに渡す。

ICMP

ICMP は IP6 タスクの中に実装した。
ICMP では、ping に関する処理、すなわち、Echo Request を受け取った時に、Echo Reply を返す処理を実装した。

NDP

NDP も IP6 タスクの中に実装される。
NDP においては、Neighbor Cash を作成し、Neighbor Solicitation、Neighbor Advertisement に関する処理をを実装した。
アドレス解決は、IPv4 では物理層で行っていた。IPv6 ではネットワーク層で行うので、Ether Address を インターフェース層に伝えなければならない。この問題は、LAN タスクに渡すメッセージに Ether Address を含めることによって解決した。

PPP

PPP は、PPP タスク内に実装されている。LCP は共通であるので、IPV6CP を IPCP と並列に実装する (図 4.8)。
LCP にも変更を加え、IPV6CP を扱えるようにした。
また、PPP タスクと LAN タスク間のインターフェースを実装した。

TCP

TCP は TCP タスクで実装されている。現在のコードを拡張し、IPv6 に対応させる。

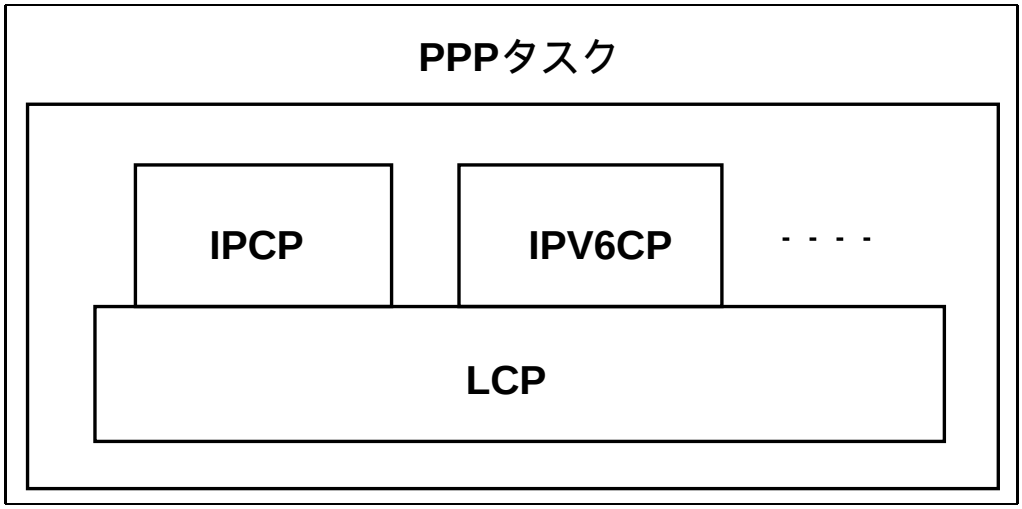

図 4.8 IPV6CP

アプリケーション

　いくつかのアプリケーションが独立したタスクとして存在する。それぞれ、IPv6 に対応させる。

第5章

実験と評価

本章では、大野研究室で構築した IPv6 ネットワークと INS ルータ に関する実験について述べ、評価する。

5.1 大野研究室 IPv6 ネットワーク運用実験

IPv6 を普及させるためと、IPv6 を使ってどの程度 IPv4 の代わりができるかを調べるために、v6 デーを実施した。

5.1.1 実験環境

falcon で IPv4 のルーティングを止めた。これにより、バリアセグメントにおいては、IPv4 と IPv6 の両方が使えるが、ネットワークの内部からバリアセグメントまでは、IPv6 を使わなければならない状況が出来上がった。

5.1.2 メール環境

送信

ネットワークの内部から外部に出るまでは、IPv6 を使ってメールを送信しなければならない。PICKLES 2.00 DR4 においては、qmail が IPv6 に対応しているので、次の方式をとる。

- localhost の qmail にメールを送る。
- localhost の qmail は IPv6 の SMTP を用いて、goat の qmail にメールを送る。
- goat の qmail は IPv4 の SMTP を用いて、送信先にメールを送る。

今回は、PICKLES 2.00 DR3 から PICKLES 2.00 DR4 への移行期であったので、PICKLES 2.00 DR3 のホストが数多く存在した。PICKLES 2.00 DR3 の qmail は IPv6 に対応していないので、次の方式をとる。

- ローカルホストの qmail にメールを送る。
- ローカルホストの qmail は IPv4 の SMTP を用いて、PICKLES 2.00 DR4 のホストの qmail にメールを送る。
- PICKLES 2.00 DR4 のホストの qmail は IPv6 の SMTP を用いて、goat の qmail にメールを送る。
- goat の qmail は IPv4 を用いて、送信先にメールを送る。

以上の方式によって、メールの送信を行なえた。

受信

メールを読むためには、メールサーバの goat からメールを POP を使い、所得しなければならない。
PICKLES では、MH を用いているので、次の方式でメールを POP する。

- IPv6 に対応した SSH を用い、ローカルホストの 10110 番ポートから gaot の 110 番ポートをトンネルで結ぶ。
- /etc/services の pop を 110 番ポートから 10110 番ポートに書き換える。
- ローカルホストから、MH でメールを POP する。

ローカルホストの POP のポートである 10110 番は、goat の 110 番につながっているので、goat の 110 番ポートから POP することになり、メールを所得できる。

5.1.3 Web 環境

バリアセグメント上のホストにプロキシをあげた。そのホストに SSH を使いトンネリングすることにより、外部のホストの閲覧が可能になる。
ネットワーク内の WWW サーバを IPv6 に対応させる作業が間に合わなかったため、試験的に IPv6 専用の WWW サーバを作った。そのサーバは、IPv6 に対応した Lynx を使うことにより閲覧できた。

5.1.4 評価

IPv6 だけを用いてもほぼ普段通りの生活を行なうことができた。
反省点と今後の課題を以下に書く。

- 事前の準備不足から、IPv6 を用いての外部接続ができなかった。大野研究室から松下電送システムまでの接続性は確認したが、その先へ接続できなかった。

  このことにより、IPv6 アドレスへのメールの送信、外部組織にある IPv6 の WWW サーバの閲覧などを行なうことができなかった。

- DNS の設定の誤りがあった。これにより、特定のホストへのログインできないなどの現象が起こった。これは、IPv6 のアドレスが 128 ビットと言うこともあり、人手による作業では、人為的なミスが発生することを意味している。将来、DNS の自動登録の機構が必要とされる。

- 今回、まだ IPv6 に対応できていないアプリケーションがあった、主なものを次に列挙する。

  DNS DNS に AAAA レコードを追加することはできるが、DNS への問い合わせは、IPv4 を用いて行なわれている。今後、IPv6 に対応した bind を導入する。

  lpd 今後、IPv6 に対応した lpd を導入する。

  NFS 今のところ、IPv6 に対応した NFS の実装がない。PICKLES のポリシでは自分のホームは小型のメディアに入れて持ち歩くので、その開発が進むと解決する。

  NIS 大野研究室のポリシとして、NIS は使われない方針であるが、一部の古いマシンでは未だに使われている。その使用を止めることで解決する。

- DNS の設定ミスが原因で、FTP に関する実験が行なえなかった。

今回の実験で、研究室内の IPv6 に対する知識が深まり、各種サービスが IPv6 に対応するなどの利益があった。
そこで、第 2 回 v6 デーを実施する予定である。それのための課題を示す。

- SSH から lssx への移行をする。lssx とは、大野研究室のメンバーが作った、IPv4 のクライアントを IPv6 のサーバにつなげるためのソフトである。これを用いることで、メールの POP や WWW の閲覧をするたびに SSH をする必要がなくなる。

- 第 1 回の v6 デーが終了した後、tanuki の WWW サーバが IPv6 に対応した。この動作確認を行なう。

- IPv6 に対応した lpd を導入し、IPv6 を用いてのプリントアウトを可能にする。

- IPv6 に対応した INS ルータを用いて外部接続する。

5.2 IPv6 対応 INS ルータ

IPv6 化された RT80i に対して行なった接続実験について述べる。

5.2.1 接続実験

実験環境

相互接続実験の機材を列挙する。

- PC(A) (PICKLES Version 2.00 DR3)
- PC(B) (FreeBSD 2.2.7-REREASE + KAME snap 19981214)
- RT80i (YAMAHA)
- ISDN 疑似交換機 第 3 電電 64 (株式会社ハウ)

ping6

PC(A) から、RT80i に向けて ping6 を実行する。
宛先の IPv6 アドレスは、

- RT80i のリンクローカルアドレス
- All Node マルチキャストアドレス
- All Router マルチキャストアドレス

すべての場合において正しく返答することが確認された。

NDP

RT80i に PC をつないで、NDP が働くかどうかを確認した。

- PC からの Neighbor Solicitation に対して、正しく Neighbor Advertisement を送った。
- Neighbor Cash にないアドレスに対し、Neighbor Solicitation を送信した。
- Neighbor Advertisement をうけとり、Neighbor Cash にアドレスを追加した。
- 有効期限が過ぎたアドレスに対し、Neighbor Solicitation を送信した。
- 有効期限が過ぎ、Neighbor Solicitation に反応しなかったアドレスを Neighbor Cash から削除した。

PPP

INS エミュレータによる実験　図 5.1 のような構成で、PPP の実験を行う。

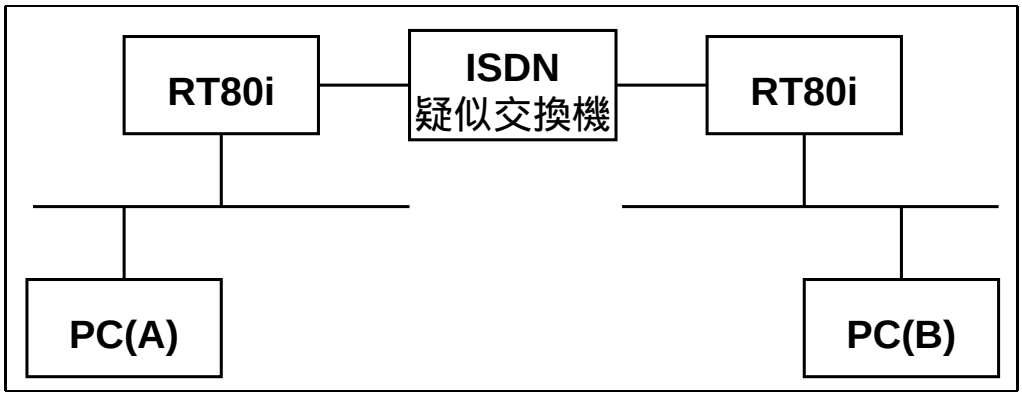

図 5.1 PPP 実験環境

対外接続実験　YAMAHA と対外接続実験を行う。

5.2.2　評価

以上の実験により、実装が済んだ機能については、どれも正しく動くことを確認した。

接続実験

前章の接続実験により、INS ルータが無事に機能することがが確かめられた。今回、確かめた機能を以下に列挙する。

- ICMP Echo の処理。
- NDP の処理。

これにより、Plug and Play での PC の接続が実現した。

環境整備

INS ルータを IPv6 に対応させたことにより、IPv6 のネットワークに PPP で接続するための環境が整った。

ブリッジ接続をしていた大野研究室は、INS ルータを用いた接続をすることにより、以下の利点がある。

- 接続するためには、IPv6 対応の INS ルータ以外に余分な機材を必要としない。

- 複数の組織との接続が一つのルータで行える。
- ネットワークアドレスを動的に獲得出来る。

これにより、IPv6 ネットワークへの PPP での接続が容易になったと思われる。

第6章

考察

本章では、本研究の考察と今後の課題を述べる。

6.1 ネットワーク運用技法の考察

現在、大野研では IPv4 と IPv6 のネットワークが共存しているが、IPv6 のネットワークを常時使うユーザはいない。これは、IPv4 に比べて、IPv6 のサービス、アプリケーションが十分でないことが原因である。それらのサービスを IPv6 対応にして行き、IPv6 だけで日常の作業ができるように移行していくことが必要である。

しかし、すべての IPv4 のアプリケーションが IPv6 に対応したとしても IPv6 への移行が進むとは考えられない。IPv6 への移行を促進するためには、IPv6 の特徴を生かしたアプリケーションが必要である。

今回の実験において、DNS の登録のミスがあった。これを防止するためには DNS の自動登録は必要である。IPv6 では、アドレスが動的に決まるので、それに応じて DNS に自動的に登録する仕組みが必要である。

今後、IPv6 の普及のために以下をおこなう。

- IPv6 対応の INS ルータを用いて対外接続を行なう。
- 研究室内のサービスをすべて IPv6 で提供する。
- 外部の IPv6 のサービスを積極的に利用する。

6.2 INS ルータの考察

INS ルータの実装が完了すると、IPv6 ネットワークに PPP で接続するための環境が整い、小規模組織のネットワークにおける IPv6 の導入が容易になる。

また、今回 IPv6 のプロトコルスタックを実装した RT80i は低価格であり、小規模ネットワーク、一般家庭において広く使われている。そのため、ファームウェアのバージョンアップにより、容易に IPv6 に移行できる。

6.3 今後の課題

6.3.1 INS ルータの実装上の課題

実装上の課題について述べる。

PPP タスク、IP6 タスク、LAN タスクの問題

後から、IP6 タスクを足したためにタスク構成が複雑になってしまった。IPv6 の PPP でパケットを送受信する時の流れを図 6.1 に示す。

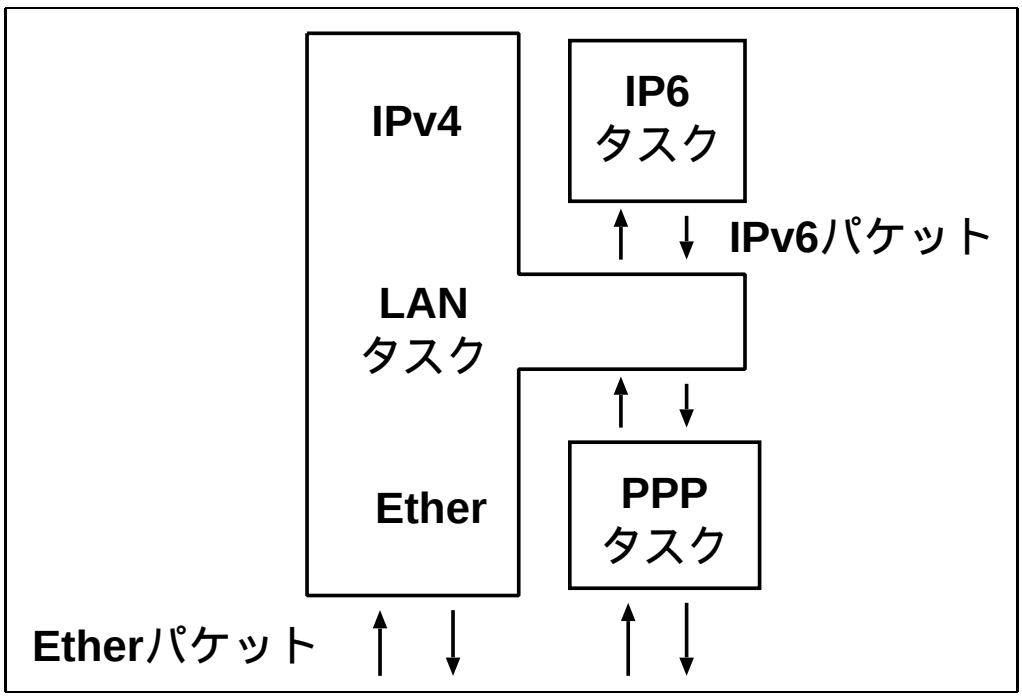

図 6.1 現在のタスク構成

これを解決するために IPv4 もタスクを独立させてた時の流れを図 6.2 に示す。このようにすることにより、各タスクの役割が明確になり、開発がしやすくなる。既存のコードを大きく書き換えるため、ヤマハ株式会社との協力が必要である。

Router Advertisement

現在、アドレスの自動設定ができているのはリンクローカルアドレスのみである。グローバルアドレスをホストに設定するためには、Router Advertisement を実装する必要がある。

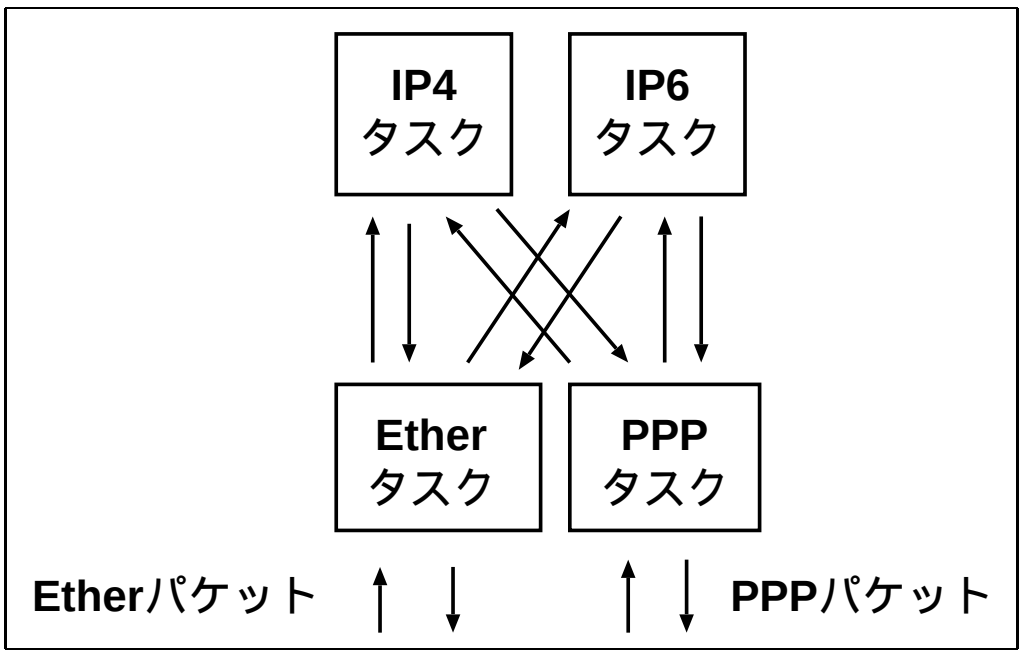

図 6.2 タスク構成案

ユーザインターフェース

現在、IPv6 アドレスのプレフィックス等の設定をユーザが設定できない。実装のテストをしてもらうために、ユーザからの各種の設定が可能になるようにユーザインターフェースを拡張する必要がある。

ルーティング

現在、スタティックなルーティングしかできていないが、RIPng を実装し、ダイナミックルーティングを可能にする必要がある。それにともない、ルーティングの処理の見直しも必要である。また、BGP の実装も考える。

上位層の実装

UDP、TCP などの上位層を実装する。これらは、ユーザインターフェースやルーティングデーモンを作成するために必要である。

IP Sec

IP パケットの暗号化、認証を行なう機構である。IPv6 では、この昨日は必須の物となっている。今後は、IP Sec を実装し、セキュリティーの向上をはかる。

トランスレータ

IPv4 から IPv6 への移行するにあたり、トランスレータが必要である。そこで、トランスレータを実装する。トランスレータにはさまざまな種類が存在するため、考察する必要がある。

6.3.2 ネットワーク構築技法の改良

IPv6 に対応していないアプリケーションが存在するため、IPv6 のネットワークが利用されない。この問題を解決するために、SOCKS5[13] を用いたトランスレータの導入を考える。これにより、IPv4 のアプリケーションを IPv6 のアプリケーションのように使うことができる。

また、トランスレータを 導入することで、ネットワーク内をすべて IPv6 で運用できる。IPv4 のネットワークと通信する時には、トランスレータにのより、IPv6 のパケットが IPv4 のパケットに変換される。

DNS についても改良する必要がある。IPv6 アドレスは、自動的にアドレスを割り振るので、従来の DNS の登録方式に合わない。現在、IETF においてアドレスの DNS への自動登録の仕様 [14] が定まりつつある。それを用いて DNS の自動登録を行なうのが良い。

第7章

おわりに

近年の急激なインターネットの発展にともないネットワーク形態が多様化した。そのためそれぞれのネットワーク形態に適した様々なネットワークの構築技法が必要となる。本研究では、小規模組織に適した IPv6 ネットワークの構築に着目し、実際に、IPv6 ネットワークを構築し評価を行なった。また、IPv6 ネットワークの外部接続の形態を考え、INS ルータを IPv6 に対応させ、このルータがインターネットの IPv6 化に果たす役割について述べた。今後、IPv4 から IPv6 への移行が本格化するにつれ、IPv6 に対応した INS ルータの重要度が増すと思われる。

謝辞

まず最初に、本研究を進めるにあたり、指導して下さった大野浩之講師に感謝します。

ヤマハ株式会社の小池恒行さん、広瀬良太さん、木村俊洋さんには、RT80i の解説を丁寧にして頂きました。また、卒論のアドバイスや接続実験でお世話になりました。本研究を進めるにあたって、尽力をつくしてくれた高山明さんに感謝致します。

最後に、研究生活を支えて下さり、様々な助言を与えてくれた大野研究室のメンバーに感謝します。

参考文献

[1] Jon Postel. Internet Protocal. Request for Comment: 791, Internet Engineering Task Force, September 1981.

[2] *The Internet Engineering Task Force*. http://www.ietf.org.

[3] Stephen E. Deering and Robert M. Hinden. Internet Protocal, Version 6 (IPv6) Specification. Request for Comment: 2460, Internet Engineering Task Force, December 1998.

[4] Jim Bound Robert E. Gilligan, Susan Thomson and W. Richard Stevens. Basic Socket Interface Extensions for IPv6. Request for Comment: 2133, Internet Engineering Task Force, April 1997.

[5] 上田仁. 多様な利用形態に対応した小規模組織用ネットワークに関する研究. 修士論文, 東京工業大学大学院情報理工学研究科, February 1999.

[6] Masahiko KIMOTO and Hiroyuki OHNO. A way to the ubiquitous computing: Design and implementation of the PICKLES information kiosk. In *International Workshop on Asia-Paciffic area advanced research information sharing technology, Internet Workshop '98*, March 1998.

[7] 木本雅彦, 大野浩之. 自律型ネットワーク端末 (PICKLES) を用いたシステム運用技法. 分散システム運用技術 シンポジウム'98 論文集, February 1998.

[8] *KAME Project*. http://www.kame.net/.

[9] Erik Nordmark Thomas Narten and William Allen Simpson. Neighbor Discovery for IP Version 6 (IPv6). Request for Comment: 2461, Internet Engineering Task Force, December 1998.

[10] Dimitry Haskin and Ed Allen. IP Version 6 over PPP. Request for Comment: 2472, Internet Engineering Task Force, December 1998.

[11] Alex Conta and Stephen Deering. Internet Control Message Protocol (ICMPv6) for the Internet Protocal Version 6 (IPv6) Specification. Request for Comment: 2463, Internet Engineering Task Force, December 1998.

[12] Erik Nordmark Thomas Narten and William Allen Simpson. Neighbor Discovery for IP Version 6. Request for Comment: 2461, Internet Engineering Task Force, December 1998.

[13] Marcus Leech. SOCKS Protocol Version 5. Request for Comment: 1928, Internet Engineering Task Force, March 1996.

[14] Christian Huitema Matt Crawford and Susan Thomson. DNS Extensions to Support IP Vesion 6. Internet Draft, Internet Engineering Task Force, December 1998.