第VIII部

IP Version 6

第 8 部
IP Version 6

第 1 章　はじめに

この章では IPv6 分科会の成果について報告する。IPv6 分科会が研究の対象としているのは、IPv6、IPsec、Mobile IPv6 である。これらに関し、実装、標準化活動、普及活動に取り組んでいる。

IPv6 分科会の報告書は以下のように構成される。

- 第 1 章のこれ以降では、KAME プロジェクトの活動内容や IETF の現状に関して説明する。
- 第 2、3、4、5、6 章では、WIDE プロジェクト v6 分科会が公開したインターネット・ドラフトのいくつかを掲載する。
- 第 7 章では、N+I IPv6 Showcase、第 54 回 IETF 横浜、および、Global IPv6 Summit という 3 つの IPv6 関連のイベントについて報告する。

1.1 KAME のロードマップ

2002 年 4 月に KAME プロジェクトは、第 3 期を 2 つの年度に分け、それぞれに以下のような目標を設定した。

2002 年度

新たなプロトコルの実装やプロトコルの更新への追随

2003 年度

第 3 期の終了後、各 BSD がそれぞれ独自に IPv6、IPsec、MobileIP6 を保守できるよう技術移転

2002 年 4 月に計画した 2002 年度に実装する具体的な項目、および 2003 年 2 月時点での自己評価は、以下の通り：

(Web で は http://www.kame.net/roadmap-2002.html にて公開。「→」が自己評価部分。)

1.1.1 IPv6

- DNS サーバ探索
  - エニーキャストを利用した DNS サーバ探索をできるだけ早く完了させる。
  - →DHCPv6 ベースは実装完了。エニーキャストベースも実装完了。
- DHCPv6
  - DNS サーバの IPv6 アドレスを通知するための、およびアドレス空間を割り当てるための DHCPv6 を横浜の IETF までに実装する。
  - → 仕様が変更され続けているので、随時対応中。現状では最新のドラフトに基づいた実装完了。
- ICMPv6 名前検索
  - 最終仕様待ち。
  - → 暫定実装あり。最終仕様待ち。
- Source Specific Multicast(SSM)
  - 2002 年 9 月までに SSM を実装。
  - → 実装完了。
- Multicast DNS
  - 仕様が頻繁に変るので辛いが、2003 年 3 月までに仕様が固まることを期待。現在の実装は、適宜仕様に追従させる。
  - → 暫定実装あり。最終仕様待ち。
- スコープ付きアドレスの経路制御
  - 2003 年 3 月までに、現在の経路表をスコープ付きアドレスをあらかじめ考慮した形に書き換える。
  - → 作業中。
- X ウインドウシステム
  - 2002 年 9 月までに、X ウインドウシステムを IPv6 に対応させ、XF86 グループへ提供する。
  - →IPv6 トランスポート部分は実装済。周辺部を検討中。
- Virtual Router Redundancy Protocol(VRRP)
  - 2003 年 3 月までに VRRP を実装する。
  - →FreeBSD での実装終了。他 OS へ移植中。

1.1.2 IPv6(優先度の低い項目)

- ルータ選択
  - 時間があれば 2003 年 3 月までに、ルータ選択機能を実装する。この変更には、ルータ通知の実装をカーネル空間からユーザ空間へ移動させることも含まれる。
  - → 一部実装済み。

- ISATAP
  - 時間があれば 2003 年 3 月までに、ISPTAP を実装する。
  - → 実装完了。

1.1.3 MobileIP6

仕様が頻繁に変るので計画を立てにくいが、大まかな予定は以下の通り。

- 実装
  - 横浜の IETF までにドラフト 17 を実装。
  - →2002 年 8 月　ドラフト 17 実装完了。2002 年 9 月　ドラフト 18 実装完了。
  - Connectathon までに次のドラフトを実装。
  - →2002 年 12 月　ドラフト 19 実装完了。Connectathon 2003 までにドラフト 20 を実装予定。
- 相互接続試験
  - 2002 年 9 月に開催される ETSI のテストへ参加。
  - → ドラフト 18 に対応した実装を持って参加した。
  - 2003 年冬に connectathon のテストへ参加。
  - → 参加予定。第 4 回 TAHI の相互接続試験イベントには、ドラフト 19 に対応した実装を持って参加した。

1.1.4 IPsec

- IPsec アーキテクチャの改訂版
  - 仕様が公開されれば、それに追従。
  - →ESP v3 は公開されているが実装は未着手。その他は仕様が決まっていない。
- IPsec ポリシ
  - KAME の IPsec ポリシの機能と API を 2002 年 9 月までに明文化する。2003 年 3 月までに、他のプロジェクトと協力して共通の IPsec ポリシ機構を設計し、それに従って実装する。
  - →IPsec ポリシの機能の明文化は作業中。API の明文化は完了。共通のポリシ機構に関しては未着手。
- 鍵管理プロトコル (KMP)
  - IKEv1 に代わる KMP の標準化は 2004 年 3 月までには終らないと予想される。そこで KAME としては、たとえば JFK のような単純な鍵交換プロトコルを実装して 終りにする。
  - → 未着手。
- IPsec の最小要求仕様
  - 2002 年 9 月までに、IPsec の最小要求仕様を明文化する。
  - → 完了。

1.2 大臣賞受賞

10 月は政府が定める情報化月間である。 KAME プロジェクトは、平成 14 年情報化促進企業等に選ばれ、2002 年 10 月 1 日に総務大臣から表彰された。

受賞内容は以下の通り：

平成 14 年情報化促進貢献企業等表彰 (総務大臣表彰)

次世代インターネットプロトコル IPv6 の研究開発及び成果の公開を通じて、IPv6 の研究開発、標準化及び実用化を国際的に先導し、IPv6 の普及に多大な貢献をした。

1.3 他組織との交流

2002 年 8 月 3 日から 9 月 4 日にかけて神明が、ISC(Internet Software Consortium) に再び滞在した。 今回の滞在の目的は、知り合いを増やすこと、作業体制の確立、BIND 9 の改良などである。

IPv6 個別アドレスによる待ち受けや、仕様から削除された機能 (A6 など) の整理といった成果があがった。

1.4 IETF 関連

IETF での IPv6 に関する分科会の動向は以下の通り：

ipv6 分科会

IETF IPv6 分科会の議長を長年務めた Steve Deering 氏が、Cisco から長期休暇を得て、議長を退いた。今後 IPv6 分科会は、Nokia の Bob Hinden 氏と Wind River の Margaret Wasserman 氏で運営されていく。

ngtrans 分科会

IPv6 への移行方法やツールに関して議論していたが、役割を終え終了した。

v6ops 分科会

運用を議論するための v6ops という分科会ができた。萩野が議長に選出された。

IETF に投稿したドラフトの一覧を以下に示す。(† 印は本報告書に掲載されていることを意味する。)

- Unidentified issues in IPv6 deployment/operation †

- Requirements for IPv6 prefix delegation †
- SMTP operational experience in mixed IPv4/IPv6 environements †using ICMPv6 node information query
- IPv4-Mapped Addresses on the Wire Considered Harmful †
- Requirements for Plug and Play IPsec for IPv6 applications †
- Use of ICMPv6 node information query for reverse DNS lookup
- Name resolution in zeroconf environment
- IPv4-Mapped Address API Considered Harmful
- An analysis of IPv6 anycast
- Advanced Sockets API for IPv6
- IPv6 Scoped Address Architecture
- Well known site local unicast addresses to communicate with recursive DNS servers
- IPv6 Node Requirements

第2章 Unidentified issues in IPv6 deployment/operation

2.1 Abstract

This document tries to identify issues in IPv6 deployment/operation, that are yet to be addressed. The document covers broad range of problems, and therefore, may capture problems that should be discussed in multiple IETF working groups.

2.2 Addressing

2.2.1 Reverse mapping of IPv6 addresses

As described in [143] , many applications assume or require that there is a PTR DNS RR (for reverse lookups) corresponding to a given IP address. Some applications even use the fact whether or not an address has a PTR RR as some sort of access control. The assumption or requirement sometimes causes problems such as denial of services or delay to establish a connection. The situation may become worse in IPv6, because the possibility of the lack of PTR RRs will be much popular. For example, PTR RRs for IPv6 temporary addresses will tend not to be registered due to its property of anonymity. There will not be PTR RRs for site-local or link-local addresses either due to the scope limitation. We will also see inconsistency in the transition period from ip6.int. to ip6.arpa. as the top level domain of reverse lookup. Thus, it is particularly important for IPv6 to make it common practice not to rely on the existence of PTR RRs both in the development of applications and in operation.

If an application wants to provide a readable hint about an IPv6 address, it can use other mechanisms than DNS. For example, ICMPv6 node information queries and responses [46] can be used as a simple method for the address to name translation.

2.2.2 How to use site-local addresses

IPv6 site-local addresses (scoped addresses in general) may be useful for network operators in some situation. For example, if IBGP connections within a site are only configured with site-local peers, the configuration will not have to be changed even if the site renumbers its global prefix(es). However, it is risky to depend on site-local addresses. Consider an IGP router in a site that is only accessed within the site. The router does not have to have a global address just to forward packet and join an IGP, even if it may forward packets with global source or destination addresses. The router, however, still has to be configured with a global address, in order to return an ICMPv6 error (such as ICMPv6 too big) outside the site. It is therefore recommended that any IPv6 node which may process packets with global addresses should always have a global address.

Site-local addresses may have other characteristics that may introduce confusion. For instance, site-local addresses will not be registered in DNS due to the limited reachability. Unlike IPv4 private address space, an IPv6 site cannot be nested according to the model of scoped addresses de-

scribed in [50]. A site-border node (typically a router) should have a great care to qualify the site zones. We'll need a guideline on how to use site-local addresses safely.

[The topic has been actively discussed in ipv6wg recently]

2.2.3 How to use multicast for service location purposes

IPv6 adopted the notion of multicasting at the beginning of its history. It should mean that we can rely on multicast in IPv6 networks much more than in IPv4 networks. This is the case in the link-local scope. For larger scopes, however, the situation is same as IPv4; IPv6 multicast routing is not widely deployed.

Meanwhile, some fundamental protocols such as SLP depend on (larger- scope) multicast to some extent. Those protocols are basically designed to work even without multicast, but the barriers to introduce those protocols will be reduced very much with the existence of multicast.

To resolve the dilemma, it should be considered that an appropriate usage model of multicast for such "minimal" purposes. That will include if there is an essential problem to deploy multicast (even for the minimal purposes), and, if not, what is the requirement to use multicast appropriately.

2.2.4 How to use anycast for service location purposes

IPv6 anycasting is expected to take an important part of some sort of service location mechanisms. Anycast has an advantage over multicast to deploy in terms of routing, while it may introduce additional issues due to its characteristics [62].

It is thus necessary to compare anycast and multicast by a fair measure, and to make a recommendation on the transport for service location purposes.

2.2.5 Prefix Management

To provide a commercial IPv6 subscription service which is fully plug- and-play from end-user's point of view, some mechanism to assign one (or more) address prefix(es) to the customer's network is needed. This mechanism could be used to transmit other informations such as global IP address of an appropreate DNS server and so on. [there is an ongoing discussion at ipv6wg]

2.3 Routing

2.3.1 Basic function on routing

There needs to be an improved version of BGP specification. BGP4+ operation is documented in [116], however, there are issues that need clarification, such as:

- operation of IX with link-local address only [83]
- selection of router ID for IPv6-only routers [52]

As for IGP, development is being done on RIPng, OSPFv3 and IS-IS each individually. It proceeds with the confirmation of the interoperability between the different routers of each protocol. However, we need more experiences and clarifications regarding to the redistribution of routing information between IGPs ("redistribute" in CISCO terminology).

Route aggregation isn't being discussed with a context of the routing control very much though it is one of the most important subjects. Route aggregation is particularly important as there are a lot more bits to be routed across ASes, and within ASes. For instance, an AS with /35 pTLA address space will need to handle 2^{13} /48 customers. Likewise, an AS with /16 TLA address space will need to handle 2^{32} /48 customers. This is an operational issue — implementations are capable of doing aggregation already, the problem is how we would/should operate it.

2.3.2 Multihome

Routing aggregation is strongly required for IPv6. From IPv4 routing practices, however, ISPs tend to announce less-aggregated routes from multiple ASes in order to improve route redundancy. Even with the fact this introduces route explo-

sion in the core backbones, it is not feasible to just force the ISPs to follow the route aggregation policy. Every ISP will then rush into getting an sTLA, or it will just ignore IPv6.

Thus, we need to analyze and gather operational experiences regarding to multihoming. IPv6 nodes can be configured with multiple addresses, which might help us address the issues [76]. Some operational compromise might be necessary, considering the tradeoff between the number of routes in the core backbones and the flexibility of inter-ISP multi-homing. [being discussed at multi6 wg]

2.4 32 bit IDs

In some protocols, there are identifier fields whose width is 32 bit even for IPv6. In some protocols, they are assigned locally. However, there are protocols such as BGP in which it is much convenient if globally unique identifiers can be assigned. Insufficient bitwidth in ID field will impact scalability of protocol, and it will contribute to operational difficulties. If those identifier fields have wider bitwidth, it will be easier to manage IDs.

One question is, how much more bitwidth we really need.

- With 128 bit, we will be able to use global IPv6 address directly. (handling of scoped address could be troublesome)
- With 64 bit, we could use EUI-64 or we could use format like 16 bit prefix + 32 bit AS number + 16 bit ID. Note: EUI-64 itself is not guaranteed to be universally unique as some vendors ship ether cards with the same MAC address. We have to be careful if we use EUI-64.
- In some cases, 32bit ID may be sufficient due to the limited scope of the identity. For instance, OSPFv3 router ID needs to be unique within an IGP domain (need not be unique worldwide). However, the use of 32 bit ID will impose management headaches within IPv6-only (or IPv6-dominated) networks, as we need to maintain mapping table between 32 bit ID and 128 bit IPv6 address.

Current 16 bit AS number space is considered to be exhausted much earlier than the exhaustion of IPv4 address space, and 32 bit AS number is being proposed. Therefore, we must at least support 32 bit AS numbers (hence ID must be wider than 32 bits).

There is a proposal for BGP which describes the way of assigning globally unique identifiers based on the 16 bit AS numbers [52]. 32 bit identifiers are used in BGP-4, OSPFv3, NTPv3, and others.

2.5 DNS related issues

2.5.1 DNS server discovery

Still there is active discussion on the way how the end node finds an appropriate DNS server nearby. The candidates include using anycast, using multicast, and using DHCPv6.

2.5.2 DNS Transport

Supporting IPv6 in DNS indicates bigger response packets because IPv6 addresses along with IPv4 address have to be filled in the additional section in some cases. This may break the current 512 byte payload size limitation. Once more than one person proposed to mandate EDNS0 if IPv6 transport is used to query DNS. Yet there is no clear consensus.

2.5.3 DNS space partition

When a zone is available on IPv6-only DNS servers, that particular zone is not able to be resolved from IPv4 world. So IPv6-only DNS server may partition the DNS space. There is a proposal in which until virtually all DNS servers are IPv6 ready every zone has to be resolvable from IPv4. This can be implementated by configuring a secondary server which has access to IPv4.

2.5.4 Fixing broken DNS servers for IPv6 deployment

There are broken DNS servers that return NXDOMAIN against AAAA queries, when it should return NOERROR with empty return records. When deploying IPv6/v4 dual stack node, it be-

comes problem because dual stack nodes would query AAAA first, see NXDOMAIN error, and won't try to query A records. These broken DNS servers need to be corrected.

2.5.5 Making root DNS servers IPv6 ready

To make it possible to operate IPv6-only (or IPv6-dominated) network, it is necessary to provide IPv6-capable root DNS servers. However, due to the packet size limitation it is not easy to add more root DNS servers. See section 4.2 as well for the packet size issue. [being discussed at dnsop]

2.5.6 Making registries IPv6 ready

ccTLD, gTLD and other servers need to become IPv6 ready. Additionally, top level domains (including root) should provide AAAA glue RRs for sub zones that support IPv6 transport.

2.5.7 Name registration to DNS

With stateless address autoconfiguration, it is easier for a node to obtain global/site-local IPv6 addresses. However, it is still unclear how name/address mapping should be registered to DNS.

2.6 SNMP

Two major issues with regards to IPv6 exist in SNMP.

1. SNMP transport to IPv6
2. MIB extension

2.6.1 SNMP transport on IPv6

To support IPv6 transport in SNMP, there is only one place in SNMP protocol specification where IPv4 address is expected: Trap PDU.

In Trap-PDU, an "Agent Address" field contains the source address of the trap originator, which currently expects IPv4 Address (IpAddress – defined in RFC1155). To define specification is relatively easy (because SNMP is ASN.1 based system) but all trap-capable managers must reflect this change, which is not easy.

With SNMPv3, traps and informs are identified with snmpContext, and there is no IpAddress any more. It should be the best way to transition to SNMPv3 for supporting SNMP transport on IPv6. We will need to carefully diagnose implementation/deployment status of SNMPv3.

2.6.2 MIB extension

To be used in production environment, we have to review, re-define or add SMI/MIB for IPv6 management. This is not easy. There are several IPv6 related MIBs defined already, but these are not enough. One of the example we are aware of is, since interface MIB is counting layer-2 traffic in octets, it is impossible to distinguish IPv4/IPv6 traffic in dual-stack environment.

2.7 Security

Security mechanisms that are used in current IPv4 networks excessively depend on denying incoming connections to a site to be protected (e.g. firewall).

However, considering a transition to IPv6, we cannot ignore the existence of Peer-to-Peer (P2P) applications. This indicates that the current model of security protection will not fit for IPv6 networks. Thus, we must discuss a new security model that enables bi-directional communication securely in order to support such P2P applications.

P2P applications might be used widely in a personal communication area. From the viewpoint of such a personal usage, we must consider not only security but also the usability of a security mechanism, and we need to discuss the balance of security and usability.

Consideration of security is undoubtedly mandatory for designing a protocol. In IPv6, IPsec is mandatory, so all protocols on IPv6 may use IPsec. However, protocol designers must not terminate their security consideration by saying "using IPsec makes the protocol secure." If a protocol designer decides to use IPsec, he/she must clearly show the usage model of IPsec, at

least how IPsec will be used, what infrastructure will be needed, what sorts of configuration will be required.

2.8 Application Specific Issues

2.8.1 Public Access Service and Hot Spot Service

There are number of security considerations to support IPv6 in public accessible area, such as airports and terminal rooms. For example, if a non-authorized node advertises router advertisement, a host may not communicate with any hosts other than in local network [85]. A malicious node on link can reset most of communication by sending wrong neighbor advertisement for any other node including routers [111].

These problems are not IPv6-specific, but more important to be resolved for deployment scenario to reach the Internet everywhere.

2.8.2 RADIUS

The attributes to assign IPv6 addresses, and to forward request using IPv6 transport are defined in [17]. Some RADIUS servers can handle IPv6 related attributes, and are even accessible via IPv6 transport. But most of RADIUS clients cannot configure IPv6 RADIUS server addresses.

2.8.3 DBMS

To handle IP addresses in DBMS, it is reasonable to make a query with address and prefix to get a list of hosts or acts on a specific network. It should accept a query with IPv6 address and prefix. Though it depends on the usage, the IPv6 address may be a scoped address, such as a link-local address, or a site-local address. In that case, zone-id and node-id should be added in the query. The zone-id is used to disambiguate the scoped address in a specific node. The node-id is also required because the uniqueness of zone-id is only guaranteed within a node. There is no standard format of node-id.

2.8.4 Platform-dependent APIs

There are various non-POSIX network APIs and libraries. Some of them need to be extended to handle IPv6 (like when they take 32 bit binary as an IPv4 address), or modified internally (like when they take a URL). Also, non-network APIs, such as database programming primitives, need to be modified to handle IPv6 addresses.

2.9 Education

2.9.1 Transition to IPv6 API

Though we have POSIX standard socket API that supports IPv6 [127], many of the existing educational materials (books, webpages) still use IPv4-only API. To help programmers, these documents have to be converted to use IPv6-capable APIs.

Transition tools, such as IPv6 socket scrabber from Sun, might help. It may also be possible to issue compile-time warnings when IPv4-only APIs are used.

There are wide variety of educational materials available for IPv4 and its internals, such as Stevens' "TCP/IP illustrated". There has to be an IPv6 variant of those.

2.10 Operation

2.10.1 Host/router requirements

Even though IPv6 base specification work is completed, related specifications, such as DHCPv6, are still being worked. Therefore, implmentation/RFC conformance status of vendor products varies. There should be an IETF document that specifies requirements to IPv6 hosts/routers. [NOTE: there is an ongoing discussion/attempt in ipv6wg]

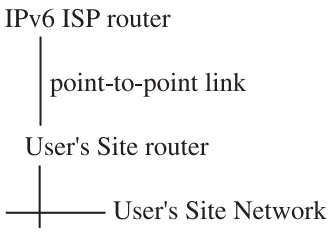
第3章 Requirements for IPv6 prefix delegation

This section describes requirements about how

an IPv6 address prefix should be delegated to an IPv6 subscriber's network (or "site").

3.1 Motivation

With the deployment of IPv6 [136] ,several commercial ISPs are ready to offer their services to the public in conjunction with widely deployed IP subscription method such as ADSL and so on. But, thinking about following situation of IPv6 commercial service as one of the most likely examples,



though it is needed a standardized way to delegate one or more IPv6 address prefix(es) from the IPv6 ISP to the User's site automatically, it is not identified clearly yet.

Originally, it seemed that just RA (Router Avertisement) considered as good enough to be used for P-P link between ISP and User's site, but according to the NCCs' recommendations, one site should be delegated /48 usually.

So, ISP which now would like to start its own IPv6 commercial service TODAY, need to have some method other than RA protocol which only can handle one signle /64 prefix but something else or enhanced

1. to delegate not just one signle /64 prefix to the user
2. to satisfy all the other (standard) requirements which is needed to realize commercial service

Therefore, this documents clarifies requirements for IPv6 address prefix delegation from the ISP to the site, especially from the (commercial) ISP point of view to boost IPv6 business quick as possible.

Requirements for prefix delegation management Focusing commercial IPv6 ISP service, there are several kinds of category of requirements for the mechanism/protocol to delegate one or more IPv6 prefixes from ISP to a site.

3.1.1 layer 2 consideration

The method should work on any layer 2 technologies. In other words, it should be layer 2 technology independent. Though, at the same time, it should be noted that now ISP would like to have a solution for Point-to-Point link which has own authentication mechanism first. PPP link with CHAP authentication is a good example. (Simulated) Ethernet and IEEE802.11 (wireless LAN) should be covered in near future, but they have low priority (just) for now. It should be clarified that the method should work with all L2 protocols either with authentication mechanism or without, but ISP would like to take advantage of a L2 protocol's authentication mechanism if it exits.

3.1.2 accounting

It should provide accounting capability such as logging about by whom, when and what prefix(es) is used for the service with proper authentication techniques.

3.1.3 kinds of prefixes

It should be able to delegate both statically and dynamically assigned prefix assignment by authenticated identification, depended by resources and/or any reasons.

3.1.4 negotiation between ISP and site

ISP may deny the service, due to various reasons such as there is no contract or bad financial credit etc. Also ISP should be able to use one single technique to pass parameters of the prefix such as scope (global and/or site), prefix length (/48, /64 or any other length) and any other appropriate related information to the site. On the other hand, a site should be able to request multiple prefixes to the ISP. Also a site should be able to pass parameters of the prefix such as scope (global and/or site), prefix length (/48, /64 or any other

length), number of prefixes and so on to the ISP to negotiate.

3.1.5 less impact on ISP equipments

ISP usually use some kind of equipment to provide subscription service to the users such as access concentrating router, PPP server and so on. This may aggregate thousands or more connections toward the ISP's backbone. Prefix delegation mechanism must be compatible with this situation.

第4章 SMTP operational experience in mixed IPv4/IPv6 environments

This section talks about SMTP operational experiences in IPv4/v6 dual stack environments. As IPv6-capable SMTP servers are deployed, it has become apparent that certain configurations are necessary in IPv6-capable MX DNS records for stable dual-stack (IPv4 and IPv6) SMTP operation. This document clarifies the problems that exist in the transition period between IPv4 SMTP and IPv6 SMTP. It also defines operational requirements for stable IPv4/v6 SMTP operation.

4.1 Introduction

Deliveries of mail messages to the final mail drop is not always done by direct IP communication with submiter and final receiver, and there may be some intermediate hosts to relay the messages. So it is difficult to

know at message submission (also at receiver side) that all intermediate relay hosts are properly configured. It is not so easy to configure all the system with consistency since mail message delivery system is rather complex on DNS setting than other Internet services. For the transition state from IPv4 to IPv6, both IPv4 and IPv6 interoperability should be kept more carefully.

There are several technologies defined for the transition from IPv4 to IPv6. This document concentrates on SMTP issues in a dual-stack environment. After all, there are no special SMTP considerations for translators; If there is SMTP traffic from an IPv6 MTA to an IPv4 MTA over an IPv6-to-IPv4 translator, the IPv4 MTA will consider this normal IPv4 SMTP traffic. Protocols like IDENT [102], however, may require special consideration when translators are used.

The following sections explain how to make IPv4 SMTP and IPv6 SMTP coexist in a dual-stack environment.

This document does not discuss the problems encountered when the sending MTA and the receiving MTA have no common protocol (e.g. the sending MTA is IPv4-only while the receiving MTA is IPv6-only). Such a situation should be resolved by making either side dual-stack or by making either side use a protocol translator.

4.2 Basic DNS resource record definitions for mail routing

Mail messages on the Internet are delivered based on domain name system generally. MX RRs are looked up to know destination hosts associated with domain part of a mail address. Similar to the way RFC's for IPv6 DNS lookup [139] use IN class for both IPv4 and IPv6, IN MX records will be used for both IPv4 and IPv6 on mail message routing, hosts which have IPv6 transport and want to be delivered with the IPv6 transport must define IPv6 IP addresses for the host name as well as IPv4 IP addresses.

A MX RR have two data, a preference value and the name of destination host. IP addresses for the destination host are also looked up to make SMTP transport [35]. In IPv4 environment, IPv4 IP addresses are defined with A RRs.

For example, IPv6 only site may have the following DNS definitions:

```
example.org.        IN MX   1 mx1.example.org.
                    IN MX   10 mx10.example.org.
mx1.example.org.    IN AAAA 3ffe:501:ffff::1
mx10.example.org.   IN AAAA 3ffe:501:ffff::2
```

In transition period from IPv4 to IPv6, there are

many IPv4 sites, and such sites will not have mail interoperability with IPv6 only sites. For the transition period, every IPv6 sites should have both transport for each domain part of mail addresses, e.g, for example:

```
example.org.        IN MX   1 mx1.example.org.
                    IN MX   10 mx10.example.org.
mx1.example.org.    IN AAAA 3ffe:501:ffff::1
                    IN A    192.0.2.1
mx10.example.org.   IN AAAA 3ffe:501:ffff::2
                    IN A    192.0.2.2
```

But, every host may not support dual stack operation, some host entries may have only IPv4 or IPv6 RRs:

```
example.org.        IN MX   1 mx1.example.org.
                    IN MX   10 mx10.example.org.
mx1.example.org.    IN AAAA 3ffe:501:ffff::1
mx10.example.org.   IN A    192.0.2.1
```

In the following sections, how sender side operates with IPv4/IPv6 combined RR definitions (section 3), and how receiver side should define RRs to keep interoperability with both IPv4 and IPv6 Internet (section 4) are considered.

4.3 SMTP sender algorithm in a dual-stack environment

In a dual-stack environment MX records for a domain resemble the following:

```
example.org.        IN MX   1 mx1.example.org.
                    IN MX   10 mx10.example.org.
mx1.example.org.    IN A    192.0.2.1
                                    ; dual-stack
                    IN AAAA 3ffe:501:ffff::1
mx10.example.org.   IN AAAA 3ffe:501:ffff::2
                                    ; IPv6 only
```

For a single MX record there are many possible final states, including: (a) one or more A records for the IPv4 destination, (b) one or more AAAA records for the IPv6 destination, (c) a mixture of A and AAAA records. Because multiple MX records may be defined using different preference values, multiple addresses based on multiple MX's must be traversed. Domains without MX records and failure recovery cases must be handled properly as well.

The algorithm for an SMTP sender is basically the same as that for an IPv4-only sender, but it now includes AAAA lookups of MX records for SMTP-over-IPv6 delivery. IPv4/v6 dual stack destinations should be treated just like multi-homed destinations as described in RFC2821 [77] section 5. When there is no reachable destionation address record found (for example, the sender MTA is IPv4 only and there are no A records available) the case should be treated just like MX records without address records, and deliveries never fail because of no known address if other addresses are available related to other MX records.

```
; if the sender MTA is IPv4 only, email deli-
very to a.example.org
; should fail with the same error as deliveries
to b.example.org.
a.example.org.      IN MX    1 mx1.a.example.org.
mx1.a.example.org.  IN AAAA  3ffe:501:ffff::1
                                    ; IPv6 only
b.example.org.      IN MX    1 mx1.b.example.org.
mx1.b.example.org.  IN HINFO "NO ADDRESS RECORDS"
```

An algorithm for SMTP sender in a dual-stack environment is as follows:

1. Lookup the MX record for the destination domain. If a CNAME record is returned, go to the top of step (1) with replacing the destination domain by the query's result. If any MX records are returned, go to step (2) with the query's result (Implicit MX). If NO_DATA (i.e. empty answer with NOERROR(0) RCODE) is returned, there is no MX record but other records (e.g. SOA, NS or A etc.) may be found. Go to step (3). If HOST_NOT_FOUND (i.e. empty answer with NXDOMAIN(3) RCODE) is returned, there is no such domain. Raise a permanent email delivery failure. Finish.
   NOTE: Some guard mechanism must required to break circular CNAME references.
2. Compare each host name in MX records with the name of sending host. If there is a record

which has the same name, drop MX records which have equal to or larger than preference value of the matched MX record (including itself). If multiple MX records remain, sort the MX records in ascending order based on their preference values. Loop over steps (3) to (9) on each host name in MX records in a sequence. If no MX records remain, the sending host must be the primary MX host. Other routing rule should be applied. Finish.

3. If the sending MTA has IPv4 capability, lookup the A record. Keep the resulting address until step (5).
4. If the sending MTA has IPv6 capability, lookup the AAAA record.
   NOTE: IPv6 addresses for hosts defined by MX records may be informed in additional information section of DNS querie's result as well as IPv4 addresses. If there is no additional address information for the MX hosts, separate queries for A or AAAA records should be sent. There is no way to query A and AAAA records at once in current DNS implementation.
5. If there is no A or AAAA record present, try the next MX record (go to step (3)).
   NOTE: If one or more address records are found, some MTA implementation may sort addresses based on the implementation's preference of A or AAAA records. To encourage the transition from IPv4 SMTP to IPv6 SMTP, AAAA records should take precedence. But this type of sorting is optional.
6. For each of the addresses, loop over steps (7) to (9).
7. Try to make a TCP connection to the destination. If successful, go to step (9).
8. If unsuccessful and there is another available address, try the next available address. Go to step (7). If all addresses are not reachable and if a list of MX records is being traversed, try the next MX record (go to step (3)). If there is no list of MX records, or if the end of the list of MX records has been reached, raise a temporary email delivery failure. Finish.
9. Try an SMTP protocol negotiation according to RFC2821 [77]. If a transient failure condition reported, try the next MX record (go to step (3)). If an error condition reported, raise a permanent email delivery error, and further MX records are not tried. Finish. If successful, SMTP delivery has succeeded. Finish.

4.4 MX configuration in the recipient domain

4.4.1 Ensuring reachability for both protocol versions

If a site has dual-stack reachability, the site SHOULD configure both A and AAAA records for its MX hosts. This will help both IPv4 and IPv6 senders to reach the site efficiently.

4.4.2 Reachability between the primary and secondary MX

When registering MX records in a DNS database in a dual-stack environment, reachability between MX hosts must be considered carefully. Suppose all inbound email is to be gathered at the primary MX host, "mx1.example.org.":

```
example.org.  IN MX 1   mx1.example.org.
              IN MX 10  mx10.example.org.
              IN MX 100 mx100.example.org.
```

If "mx1.example.org" is an IPv6-only node, and the others are IPv4-only nodes, there is no reachability between the primary MX host and the other MX hosts. When email reaches one of the lower MX hosts, it cannot be relayed to the primary MX host based on MX preferencing mechanism.

```
; This configuration is troublesome.
; No secondary MX can reach mx1.example.org.
example.org.  IN MX 1   mx1.example.org.
                                ; IPv6 only
              IN MX 10  mx10.example.org.
                                ; IPv4 only
              IN MX 100 mx100.example.org.
                                ; IPv4 only
```

The easiest possible configuration is to configure the primary MX host as a dual-stack node. By do-

ing so, secondary MX hosts will have no problem reaching the primary MX host.

```
; This configuration works well.
; The secondary MX hosts are able to relay
email to the primary MX host
; without any problems.
example.org.  IN MX 1   mx1.example.org.
                                  ; dual-stack
              IN MX 10  mx10.example.org.
                                  ; IPv4 only
              IN MX 100 mx100.example.org.
                                  ; IPv6 only
```

It may not be needed that the primary MX host and lower MX hosts reach directly one another with IPv4 or IPv6 transport. For example, it is possible to establish a routing path with UUCP or an IPv4/v6 translator. It is also possible to drop messages into single mailbox with shared storage using NFS or something else offered by a dual-stack server. It is receiver site's matter that all messages delivered to each MX hosts must be reached to recipient's mail drop. In such cases, dual-stack MX host may not be listed in the MX list.

4.5 Operational experience

Many of the existing IPv6-ready MTA's appear to work in the way documented in section 3.

From past experiments and operational experience, it is known that most of the existing IPv4-only MTA's will not be confused by AAAA records that are registered for MX hostnames. No experiments were conducted with A6 records.

There were, however, cases where IPv6-ready MTA's were confused by broken DNS servers. When attempting to canonify a hostname, some broken name servers return SERVFAIL (RCODE 2), a temporary failure, on AAAA record lookups. Upon this temporary failure, the email is queued for a later attempt. In the interest of IPv4/v6 interoperability, these broken DNS servers should be fixed.

4.6 Open issues

How should scoped addresses in email addresses be interpreted on MTA's? As email is relayed between MTA's, interpretation of scoped addresses can be different between MTA's. After all, intermediate MTA's may be in different scope zones than the originator. If a scoped IPv6 address is returned as the result of a DNS lookup, how should MTA's behave?

If scoped addresses in "route-addr" specifications [48] are considered, e.g.

```
<@kame.net,@[fec0::1]:itojun@itojun.org>
```

it gets even trickier. Luckily, the route-addr form was obsoleted by RFC2822 [117].

第 5 章　IPv4-Mapped Addresses on the Wire Considered Harmful

The IPv6 Addressing Architecture [129] defines the "IPv4-mapped IPv6 address." These addresses are used in the IPv6 basic API [127] to denote IPv4 addresses using AF_INET6 sockets. These addresses are used in protocol proposals such as SIIT [54] to denote IPv6 communication using AF_INET6 sockets. Therefore, IPv4-mapped addresses have two different meanings, and they are not distinguishable from the user-land applications.

This draft discusses security threats due to this ambiguity of IPv4-mapped address. It also discusses threats due to the additional complexities introduced by IPv4-mapped addresses. Finally, it proposes to resolve these problems by forbidding protocols from using IPv4-mapped addresses for IPv6 communications.

5.1 Dual meaning of IPv4-mapped address

Basic Socket Interface Extensions for IPv6 [127] defines the use of IPv4-mapped address with AF_INET6 sockets. IPv4-mapped addresses are used to represent IPv4 addresses using the IPv6 API (e.g., on AF_INET6 sockets). The API is designed with IPv4/v6 dual stack nodes in mind. When an IPv4 packet reaches an IPv4/v6 dual

stack node, the node's IPv4 layer will process it, then pass it to the transport layer. When the transport layer finds an AF_INET6 listening socket, it will pass the packet to the listening socket as if it was from the corresponding IPv4-mapped address. In this document, we will refer to this as the "basic API behavior."

Some of the IPv6 translation protocols, such as SIIT [54], use IPv4-mapped addresses actual IPv6 packets on the wire. These protocols are designed for use with IPv6-only nodes. When an IPv6 packet containing these addresses reaches a node, the node's IPv6 layer will process it, then pass it to the transport layer. When the transport layer finds an AF_INET6 listening socket, it will pass the packet to the listening socket with the IPv4-mapped address intact. In this document, we will refer to this as the "SIIT behavior."

5.2 Threats due to the use of IPv4-mapped address on wire

When an application using the AF_INET6 API receives an IPv4-mapped addresses (for example, returned by getpeername(2) or recvfrom(2)), it cannot detect if the packet received by the node actually used IPv4 (basic API behavior) or IPv6 (SIIT behavior).

This ambiguity creates an opportunity that a malicious party can exploit in order to deceive victim nodes. For example:

- If an attacker transmits an IPv6 packet with ::ffff:127.0.0.1 in the IPv6 source address field, he might be able to bypass a node's access controls by deceiving applications into believing that the packet is from the node itself (e.g., the IPv4 loopback address, 127.0.0.1). The same attack might be performed using the node's IPv4 interface address instead.
- If an attacker transmits an IPv6 packet with IPv4-mapped addresses in the IPv6 destination address field corresponding to IPv4 addresses inside a site's security perimeter (e.g., ::ffff:10.1.1.1), he might be able to bypass IPv4 packet filtering rules and traverse a site's firewall.
- If an attacker transmits an IPv6 packet with IPv4-mapped addresses in the IPv6 source and destination fields to a protocol that swaps IPv6 source and destination addresses, he might be able to use a node as a proxy for certain types of attacks. For example, this might be used to construct broadcast multiplication and proxy TCP port scan attacks.

5.3 Recommended solution

Forbid the use of IPv4-mapped address on wire.

The IPv6 node requirements:

- IPv6 nodes MUST NOT generate packets that contain IPv4-mapped addresses in any network layer field. Specifically, the IPv6 header, routing header, options headers, and any other chained headers MUST NOT contain IPv4-mapped addresses.
- IPv6 nodes SHOULD NOT generate packets that contain IPv4-mapped addresses in any field. (As a particular exception, it MAY be acceptable for fields referring to third-party nodes to contain IPv4-mapped addresses. Implementors must ensure that, where this is allowed, it is done with great care.)
- IPv6 nodes MUST silently discard packets that contain IPv4-mapped address in IPv6 header fields, or IPv6 extension header fields.

The IPv6 router requirements:

- IPv6 routers MUST NOT forward packets that contain IPv4-mapped addresses in any field the router processes. Specifically, the IPv6 header, routing header, and the hop-by-hop options headers parsed by the router MUST NOT contain IPv4-mapped addresses.
- IPv6 routers MUST NOT advertise any prefixes into a routing protocol that are within the IPv4-mapped address space. Further, IPv6 routers MUST appropriately discard and/or ignore any received prefixes within the IPv4-mapped address space.

Standards requirements:

- The IPv6 address architecture document

[Hinden, 1998] MUST explicitly state that IPv4-mapped addresses are exclusively for uses local to a node as specified in the basic API [127] and MUST never appear in the wire.

- Any document that suggests the use of IPv4-mapped addresses in packets on the wire SHOULD be modified to remove such usage. This will remove the threat due to the use of IPv4-mapped address on wire.

An alternate solution is to deprecate IPv4-mapped addresses from the basic API. Due to the wide deployment of applications that use IPv6 basic API, further study of this option's feasibility is required. This solution is not mutually exclusive with the recommended solution.

5.4 Suggested implementation tips

5.4.1 System (e.g., kernel and library) developers

- Drop any IPv6 native packet with IPv4-mapped addresses in any of IPv6 header fields as well as IPv6 extension header fields. (N.B., this will make the system incompatible with the current version of SIIT [54])
- Drop any IPv6 DNS response that contains IPv4-mapped addresses.

第 6 章　Requirements for Plug and Play IPsec for IPv6 applications

This section describes requirements about how IPsec is supplemented for IPv6 Plug and Play applications.

6.1 Motivation

6.1.1 Reasons to employ IPv6

IPv6 is the economically valid choice for peer-to-peer applications that require global IP addresses because IPv6 global addresses are abundant (IPv4 global addresses are not, especially in Asia.) Such peer-to-peer applications often require authentication and secrecy mechanisms, which are provided by IPsec.

Another IPv6 advantage over IPv4 is the Plug and Play feature based on Stateless Address Auto Configuration [140] technologies, which enable IPv6 users to use IPv6 devices without configurations. This zero-configuration feature of IPv6 encourages manufacturers of embedded devices to choose IPv6 instead of IPv4 because embedded devices are often difficult to configure before use. This is where the current IPsec is not optimized. The following are examples of such embedded peer-to-peer IPv6 applications:

- Video camera and display connected with IP networks
- On-Line games without central servers
- Remote control of home appliances

6.1.2 Another IPv6 Employment Reasoning: IPv6 myth, "IPv6 is secured by IPsec"

There is another reason for Internet users to choose IPv6. IPv6 is believed to be equipped with IPsec as default, and many users choose IPv6 because of IPsec. However, IPsec is independent from version numbers of IP, and IPv6 does not have special advantages for IPsec. We have two options to cope with this myth:

(a) Educate users

(b) Design supplemental architecture, which enables most communications among IPv6 devices to be encrypted by IPsec without too much configurations

This document covers option (b), and we call this kind of IPsec as "Plug and Play IPsec."

6.2 Requirements

6.2.1 Credentials

Credentials should not be PKI based. The reasons why we avoid employing PKI are:

- Maintenance of X.509 certificates is complicated for embedded devices
- Deployment of PKI, as the global infrastructure, can be the rate-determining step of deployment of IPv6 peer-to-peer applications

Many IPv6 applications assume embedded devices without keyboard and display. For embedded devices, maintaining X.509 certificate, such as Certificate Update and Certificate Revocation Handling, is too heavy and often diminishes the usability. There are also obstacles to deploy globally available PKI and its arrival is not foreseeable. Because of the above reasons, credentials should be non-PKI based.

6.2.2 Security Policy

Master security policy should be maintained outside IPsec devices and should be dynamically installed when needed because some embedded devices do not have strong human interfaces to manipulate security policies. Decision whether to accept a proposal to establish SA or not should be asked of outside servers each time. However, we should not mandate the existence of this outside server because there are many situations in which such servers are not available, and IP layer authentication and Man-in-the-Middle protection are not important.

6.2.3 Optional authentication and zero-configuration mode (Plug and Play IPsec)

As mentioned above, authentication should be an option. In this authentication-less mode, IPv6 IPsec devices can establish IPsec SAs without any pre-configuration. Devices should be able to discover whether the peer supports the same kind of IPsec without disturbing communications with legacy devices. In such zero-configuration mode, we can accept Man-in-the-Middle attack vulnerability.

After the establishment of this security level of IPsec SAs, authentication, authorization, accounting, and Man-in-the-Middle prevention are added on to those SAs. We call this kind of gradual IPsec application as "Progressive IPsec." Application should be able to start communication from any phase. If an application does not care about strict security, that application does not have to wait to start communication until SA is established. If an application cares about security very much, the application should just wait until the full-range of security is provided after the last phase of SA establishment. This implicitly requires APIs that exchange SA status between the application layer and the IPsec layer.

6.3 Considerations

6.3.1 Man-in-the-Middle attack mitigation

Man-in-the-Middle attack cannot be mitigated without pre-configuration (Inter-lock Protocol [133] may be the solution, but it's not practical to apply to IP communications.) Assuming no pre-configuration, just Diffie-Hellman without authentication will work for some situations such as wireless LAN.

6.3.2 Just Diffie-Hellman before every communication

Just "key-exchange-before-all-the-communication" does not work because it forces delay on all the communications regardless of this kind of IPsec supports. Key exchange should be triggered not by data packets but by some IPsec discovery procedures during data communications. This procedure should not hinder communicating with legacy devices, and also be achieved without pre-configurations in order to actualize Plug and Play IPsec.

6.4 Conclusion

In order to deploy IPv6 peer-to-peer applications and IPv6 itself, we need the Plug and Play IPsec. The features of the Plug and Play IPsec are as follows:

- Configuration-less IPsec application to every IPv6 communication
- Optioned full-range security features
- Disuse of PKI
- External security policy management

The architecture could be developed using the IKE(v2) core.

第 7 章　イベント

この章では、IPv6 の現状を示すために、N+I IPv6 Showcase、第 54 回 IETF 横浜、および、Global IPv6 Summit に関して報告する。

7.1 N+I IPv6 Showcase

N+I 2002 Tokyo は 2002 年 7 月 3 日から 7 月 5 日にかけて幕張メッセで開催され、その中に設けられた IPv6 Showcase は今回で 3 回目の試みとなった。

シスコシステムズ、日立製作所、マイクロソフトがプラチナスポンサー。また、ゴールドスポンサーに 4 社、シルバースポンサーに 3 社、その他の参加が 25 社、3 団体と盛大なブースとなった。

2001 年のテーマは IPv6 で接続された家庭ネットワークだった。2002 年は前年を越えるべくテーマを広げ、ブースを IPv6 で有機的に繋がった町に見立てた。町には、ステージと 4 つのゾーンを設けた。

7.1.1 家庭ゾーン

家庭ゾーンは、2001 年の「ポポちゃんの部屋」の延長であり、家庭用のルータや家電、ゲーム機を展示した。

特筆すべきは、SANYO のデジタルカメラであろう。IPv6 を喋るアダプタを付ければ、内部の画像を HTTP で閲覧できる。近い将来、IPv6 の機能と無線 LAN がデジタルカメラの内部に組み込まれることだろう。

今後このデジタルカメラのように、IPv6 の特性を活かした製品が出てくることだろう。

7.1.2 ISP ゾーン

ISP ゾーンには、5 つのラックを立て、ルータや DSL のバックエンドである BAS(Broadband Access Server) といった製品を展示した。ルータのほとんどは、IPv6 パケットの転送をハードウェアで実現しており、IPv4 のそれと遜色ない性能を出していた。また、OSPF v3 や ISIS の実装も進んでいた。

7.1.3 アドレス空間の配布

家庭ゾーンと ISP ゾーンでは、ISP から家庭へ IPv6 のアドレス空間を配布するデモを用意した。IPv4 であれば PPP を使って、アドレスを 1 つ取得できる。IPv6 では、DHCPv6 を使って「アドレス空間」を取得できる。

これまで ADSL を用いて家庭を IPv6 で接続しようとすると、前出の BAS が IPv4 しかサポートしていないため、IPv6 over IPv4 トンネルを利用せざるを得ない状況だった。8 月より NTT コミュニケーションズが ACCA と組んで、アドレス空間の自動配布のサービスを始めたことは特筆すべきである。

7.1.4 モバイルゾーン

モバイルゾーンでは、インターネット自動車と Mobile IPv6 を喋るノードを展示した。

2001 年もインターネット自動車を展示していたが、それはモバイル・ノードとしての機能しか持っていなかった。2002 年は、車内にネットワークを構築し、ネットワークごと移動するモバイル・ネットワークが実現されていた。

モバイル・ルータのおかげで、Mobile IPv6 の機能を持っていないノードも移動しながら通信できる。たとえば、Mobile IPv6 を実装していない Windows 2000 が車内に設置され、実際にインターネットと通信できていた。

Mobile IPv6 を実装としては、いくつかの PDA とホーム・エージェントを展示した。iPAQ にはヘルシンキ大学の Mobile IPv6 を組み込んだ Linux が搭載されていた。Zaurus もほぼ同様だが、カーネルとしては USAGI Linux を使用していた。KAME プロジェクトは、KAME の実装をカメラ付きの Vaio に搭載し、モバイル・サーバとしてデモをした。PDA 自体がかわいらしいこともあり、このゾーンは好評だった。

7.1.5 一般ゾーン

一般ゾーンは、上記の分類に当てはまらない IPv6 製品を展示した。アクセンス・テクノロジーが IPv6 対応の Radius サーバを出展し、上記の BAS と連動してデモをしていた。

7.1.6 ステージ

ステージでは、スポンサーよる製品紹介、および Mobile IPv6 やアドレス空間の自動配布など最新技術の説明があった。

7.1.7 IPv6 Showcase の所感

IPv6 Showcase は最も人気を博したブースの 1 つであり、2001 年にも増して IPv6 の重要性をアピールできたと思う。

7.2 第 54 回 IETF 横浜

第 54 回目の IETF は、7 月 14 日から 7 月 19 日にかけて、パシフィコ横浜で開催された。スポンサーを富士通、ホストを WIDE プロジェクトが務めた。

IETF は年 3 回の会合の内、2 回をアメリカ、1 回をアメリカ以外の国で開催することになっている。アメリカ以外の国は、貢献度によって選択されるので、日本での開催は、日本人の活動が評価されてた結果だと考えてよい。

約 2000 名の参加者があり、アメリカ以外の国での開催としては、ロンドンに次ぐ規模になった。また、IPv6 が最も進んだ日本での実施なので、意図的に IPv6 色が強く出されたことも特徴として挙げられるだろう。

KAME プロジェクトは NOC(Network Operation Center) メンバーとしてネットワークの構築運営に携わるとともに、主目的である標準化作業においても IPv6 や Mobile IPv6 の分科会に積極的に関わった。

以下では、ネットワーク、標準化作業、パネルに分けて報告する。

7.2.1 ネットワーク

今回の IETF では、文字通り、いつでもどこでも IPv6 が利用できる環境が提供された。

成田空港はアジアのハブを目指している割りには、無線 LAN によるインターネット環境がなく、シンガポールのチャンギ空港と比べて見劣りしていたが、ワールドカップを期にようやく無線 LAN サービスが無料で提供されるようになった。(現在 IPv4 の無線 LAN サービスは有料となった。)

会場への主要交通機関である成田エクスプレスのグリーン車にも、期間限定であるが無線 LAN が提供された。インターネットへの接続には FOMA が利用され、移動通信を実現していた。

富士通と WIDE プロジェクトからなる NOC チームは、端末室の机に RJ 45 端子を出すと共に、すべての会議室を無線 LAN でカバーした。

また、隣接するインターコンチネンタルホテルや、非公式ながら近くのスターバックスも無線 LAN でカバーした。

むろんこれらのネットワークでは、すべて IPv6 を利用可能にした。IETF の参加者は、あたかも IPv6 を呼吸しているかのように身近に感じられたことだろう。なお全体会議での挙手によると、参加者の 7 割程度が IPv6 を利用していた。

7.2.2 標準化作業

IPv6 分科会で話し合われた内容の内、重要なのは、アドレス空間の配布方式や DNS サーバ探索。これらを優先的に標準化していくことになった。日本で IPv6 のビジネスを展開していく上で不可欠な技術なので、早急な仕様策定が望まれている。

発表者の内、4 名は日本人だった。KAME からは、神明と萩野が、スコープ付アドレスや Anycast について発表した。

IPv6 分科会からの要請で、非公式だが休憩時間に日本での IPv6 の応用 (ゲーム機、自動車、家電) を紹介する機会が設けられた。

7.2.3 全体会議

全体会議では、IPv6 のパネルが企画され、KAME プロジェクトの神明、角川、萩野がパネリストとして発表した。このパネルの主旨は、IPv6 の夢ではなく、現実を客観的に伝えることである。

角川の「『IPv4 ではユーザ当り 5 ドルかかるが、IPv6 なら 3 ドルでできる』のような分りやすい説明が IPv6 のビジネス展開には必要」という言葉が印象的だった。

7.2.4 IETF に対する所感

この IETF を通じて、IPv6 懐疑派の懸念は一掃された感があり、IETF 全体で IPv6 をサポートしていく機運が高まると期待したい。

7.3 Global IPv6 Summit

2002 年 12 月に、Global IPv6 Summit in Japan をパシフィコ横浜で開催した。今回で 3 回目であり、

表 7.1.　配信の仕様

帯域	500.04 Kpbs
音声コーデック	Windows Media Audio 9 128 Kbps、44 KBz、Stereo、CBR
映像コーデック	Windows Media Video 9 320 × 240、29.97 fps、CBR
経路制御方式	PIM-SM

2002 年は本会議に加えて 4 つのワークショップを設けた。

スポンサーは、IIJ、NTT コミュニケーションズ、シスコシステムズ、6WIND、ジュニパーネットワークス、東芝、NEC、パワードコム、日立製作所、富士通、マイクロソフトである。

7.3.1 プログラム

全体のプログラムは以下の通り。(括弧内は参加者数。† 印は同時通訳あり。)

- 2002 年 12 月 18 日 (一日目、ワークショップ)
  - IPv6 ネットワーク設定ノウハウ (139)
  - IPv6 の組み込み分野への適用 (151) †
  - 企業ネットワークでの IPv6 利用 (97)
  - IPv6 ネットワークプログラミング (89) †
- 2002 年 12 月 18 日 (二日目、本会議) (476) †
  - IPv6 デプロイメントの展望
  - 家庭 IPv6 ネットワークおよび IPv6 家電の進捗と今後の展望
  - IPv6 が開く日本の次世代情報産業の展望

アンケート結果によれば、4 つのワークショップの内 3 つが好評、本会議は 3 つのパネルとも好評であった。

本会議の内容は、SOI が収録し、英訳して web で公開される予定である。

7.3.2 IPv6 マルチキャスト

IPv6 マルチキャストの普及を促進するために、本会議の映像とオリジナル音声 (通訳音声はなし) をマイクロソフトの協力を得て IPv6 インターネットに向けて放送した。配信の仕様は表の通りである。

この配送実験に参加した ISP および IX は、IIJ、NTT コミュニケーションズ、NEC、WIDE プロジェクト、NSPIXP6 である。また協力組織は、KDDI、フリービット、早稲田大学、日立製作所、マイクロソフト、IPv6 普及・高度化推進協議会である。

これまで、一つの ISP が IPv6 のマルチキャスト放送を実験したことはあったが、このように複数の ISP が参加したことは初めてであり、意義が高い。今回は単一の PIM ドメインでの実験となったが、将来複数の PIM ドメインでの運用へつながると期待できる。