Internet Engineering Task Force
INTERNET-DRAFT
Expires: December 23, 2002

IPv6 working group
WIDE project
June 23, 2002

Unidentified issues in IPv6 deployment/operation
draft-itojun-jinmei-ipv6-issues-00.txt

J. HAGINO
T. JINMEI

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To view the list Internet-Draft Shadow Directories, see http://www.ietf.org/shadow.html.

Distribution of this memo is unlimited.

The internet-draft will expire in 6 months. The date of expiration will be December 23, 2002.

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.

1. Addressing

1.1. Reverse mapping of IPv6 addresses

As described in [Senie, 2001] , 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 [Crawford, 2002] can be used as a simple method for the address to name translation.

1.2. 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 described in [Deering, 2002] . 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]

1.3. 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.

1.4. 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 [Hagino, 2001] .

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.

1.5. 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. Routing

2.1. Basic function on routing

There needs to be an improved version of BGP specificaiton. BGP4+ operation is documented in [RFC2545], however, there are issues that need clarification, such as:

o operation of IX with link-local address only [Kato, 2001]

o selection of router ID for IPv6-only routers [Dupont, 2002]

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 terminlogy).

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.

2.2. 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 explosion 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 [RFC3178]. 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]

3. 32bit IDs

In some protocols, there are identifier fields whose width is 32bit 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 128bit, we will be able to use global IPv6 address directly. (handling of scoped address could be troublesome)

- With 64bit, we could use EUI-64 or we could use format like 16bit prefix + 32bit AS number + 16bit 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 32bit ID will impose management headaches within IPv6-only (or IPv6-dominated) networks, as we need to maintain mapping table between 32bit ID and 128bit IPv6 address.

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

There is a proposal for BGP which describes the way of assigning

globally unique identifiers based on the 16bit AS numbers [Dupont, 2002]
.

32bit identifiers are used in BGP-4, OSPFv3, NTPv3, and others.

4. DNS related issues

4.1. 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.

4.2. DNS Transport

Supporting IPv6 in DNS indicates bigger response packets because IPv6 addresses along with IPv4 address have to be filled in the additional secion 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.

4.3. 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.

4.4. 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 becomes 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.

4.5. 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]

4.6. 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.

4.7. 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.

5. SNMP

Two major issues with regards to IPv6 exist in SNMP.

(1) SNMP transport to IPv6

(2) MIB extension

5.1. 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 realtively 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.

5.2. 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.

6. 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.

7. Application Specific Issues

7.1. Public Access Service and Hot Spot Service

There are number of security considerations to support IPv6 in public accessiable 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 [Kempf, 2002] . A malicious node on link can reset most of communication by sending wrong neighbor advertisement for any other node including routers [Nordmark, 2002] .

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

7.2. RADIUS

The attributes to assign IPv6 addresses, and to forward request using IPv6 transport are defined in [Aboba, 2001] . 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.

7.3. 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 acls 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.

7.4. 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 32bit 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.

8. Education

8.1. Transition to IPv6 API

Though we have POSIX standard socket API that supports IPv6 [RFC2553], 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.

9. Operation

9.1. 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]

10. Security consideration

A section in this document discusses how protocols on top of IPv6 should be designed with respect to security. In summary, just saying "use IPsec" is not enough; every protocol has to diagnose and describe how IPsec should be applied, how IPsec security policy should be configured, and how IPsec security associations should be established. Also, interaction of IPsec with non-global and/or non-unicast address needs careful consideration.

References

Senie, 2001.
Daniel Senie, "Requiring DNS IN-ADDR Mapping" in draft-ietf-dnsop-inaddr-required-02.txt (July 2001). work in progress material.

Crawford, 2002.
Matt Crawford, "IPv6 Node Information Queries" in draft-ietf-ipngwg-icmp-name-lookups-09.txt (May 2002). work in progress material.

Deering, 2002.
S. Deering, B. Haberman, T. Jinmei, E. Nordmark, A. Onoe, and B. Zill, "IPv6 Scoped Address Architecture" in draft-ietf-ipngwg-scoping-arch-04.txt (June 2002). work in progress material.

Hagino, 2001.
Jun-ichiro itojun Hagino and K. Ettikan, "An analysis of IPv6 anycast" in draft-ietf-ipngwg-ipv6-anycast-analysis-00.txt (July 2001). work in progress material.

Kato, 2001.
Akira Kato and Bill Manning, "BGP4+ Peering Using IPv6 Link-local Address" in draft-kato-bgp-ipv6-link-local-00.txt (September 20, 2001). work in progress material.

Dupont, 2002.
Francis Dupont and Alain Durand, "BGP4 router ID for IPv6 only routers" in draft-dupont-durand-idr-ipv6-bgp-routerid-01.txt (January 15, 2002). work in progress material.

Kempf, 2002.
James Kempf, "Securing IPv6 Neighbor Discovery Using Address Based Keys (ABKs)" in draft-kempf-secure-nd-00.txt (Feb 28, 2002). work in progress material.

Nordmark, 2002.
Erik Nordmark and James Kempf, "Threat Analysis for IPv6 Public Multi-Access Links" in draft-kempf-ipng-netaccess-threats-01.txt (June 13, 2002). work in progress material.

Aboba, 2001.
Bernard Aboba, Glen Zorn, and Dave Mitton, "RADIUS and IPv6" in draft-aboba-radius-ipv6-07.txt (February 2001). work in progress material.

Change history

None.

Acknowledgements

(to be filled)

Author's address

IPv6 working group, WIDE project
Fujisawa, Kanagawa JAPAN

Editors' address

Jun-ichiro itojun HAGINO
Research Laboratory, Internet Initiative Japan Inc.
Takebashi Yasuda Bldg.,
3-13 Kanda Nishiki-cho,
Chiyoda-ku,Tokyo 101-0054, JAPAN
Tel: +81-3-5259-6350
Fax: +81-3-5259-6351
Email: itojun@iijlab.net

Tatuya JINMEI
Research and Development Center, Toshiba Corporation
1 Komukai Toshiba-cho, Kawasaki-shi
Kanagawa 212-8582, JAPAN
Tel: +81-44-549-2230
Fax: +81-44-520-1841
Email: jinmei@isl.rdc.toshiba.co.jp