Network Working Group
Request for Comments: 3790
Category: Informational

C. Mickles, Ed.

P. Nesser, II
Nesser & Nesser Consulting

June 2004

Survey of IPv4 Addresses in Currently Deployed IETF Internet Area Standards Track and Experimental Documents

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document seeks to document all usage of IPv4 addresses in currently deployed IETF Internet Area documented standards. In order to successfully transition from an all IPv4 Internet to an all IPv6 Internet, many interim steps will be taken. One of these steps is the evolution of current protocols that have IPv4 dependencies. It is hoped that these protocols (and their implementations) will be redesigned to be network address independent, but failing that will at least dually support IPv4 and IPv6. To this end, all Standards (Full, Draft, and Proposed) as well as Experimental RFCs will be surveyed and any dependencies will be documented.

Table of Contents

1. Introduction

This document is part of a document set aiming to document all usage of IPv4 addresses in IETF standards. In an effort to have the information in a manageable form, it has been broken into 7 documents conforming to the current IETF areas (Application, Internet, Management & Operations, Routing, Security, Sub-IP and Transport).

This specific document focuses on usage of IPv4 addresses within the Internet area.

For a full introduction, please see the introduction [1] document.

2. Document Organization

The following sections 3, 4, 5, and 6 each describe the raw analysis of Full, Draft, and Proposed Standards, and Experimental RFCs. Each RFC is discussed in turn starting with RFC 1 and ending in (about) RFC 3100. The comments for each RFC are "raw" in nature. That is, each RFC is discussed in a vacuum and problems or issues discussed do not "look ahead" to see if any of the issues raised have already been fixed.

Section 7 is an analysis of the data presented in Sections 3, 4, 5, and 6. It is here that all of the results are considered as a whole and the problems that have been resolved in later RFCs are correlated.

3. Full Standards

Full Internet Standards (most commonly simply referred to as "Standards") are fully mature protocol specification that are widely implemented and used throughout the Internet.

3.1. RFC 791 Internet Protocol

This specification defines IPv4; IPv6 has been specified in separate documents.

3.2. RFC 792 Internet Control Message Protocol

This specification defines ICMP, and is inherently IPv4 dependent.

3.3. RFC 826 Ethernet Address Resolution Protocol

There are no IPv4 dependencies in this specification.

3.4. RFC 891 DCN Local-Network Protocols

There are many implicit assumptions about the use of IPv4 addresses in this document.

3.5. RFC 894 Standard for the transmission of IP datagrams over Ethernet networks

This specification specifically deals with the transmission of IPv4 packets over Ethernet.

3.6. RFC 895 Standard for the transmission of IP datagrams over experimental Ethernet networks

This specification specifically deals with the transmission of IPv4 packets over experimental Ethernet.

3.7. RFC 903 Reverse Address Resolution Protocol

There are no IPv4 dependencies in this specification.

3.8. RFC 919 Broadcasting Internet Datagrams

This specification defines broadcasting for IPv4; IPv6 uses multicast so this is not applicable.

3.9. RFC 922 Broadcasting Internet datagrams in the presence of subnets

This specification defines how broadcasts should be treated in the presence of subnets. IPv6 uses multicast so this is not applicable.

3.10. RFC 950 Internet Standard Subnetting Procedure

This specification defines IPv4 subnetting; similar functionality is part of IPv6 addressing architecture to begin with.

3.11. RFC 1034 Domain Names: Concepts and Facilities

In Section 3.6, "Resource Records", the definition of A record is:

```
RDATA           which is the type and sometimes class dependent
                data which describes the resource:

                A          For the IN class, a 32 bit IP address
```

And Section 5.2.1, "Typical functions" defines:

1. Host name to host address translation.

   This function is often defined to mimic a previous HOSTS.TXT based function. Given a character string, the caller wants one or more 32 bit IP addresses. Under the DNS, it translates into a request for type A RRs. Since the DNS does not preserve the order of RRs, this function may choose to sort the returned addresses or select the "best" address if the service returns only one choice to the client. Note that a multiple address return is recommended, but a single address may be the only way to emulate prior HOSTS.TXT services.

2. Host address to host name translation

   This function will often follow the form of previous functions. Given a 32 bit IP address, the caller wants a character string. The octets of the IP address are reversed, used as name components, and suffixed with "IN-ADDR.ARPA". A type PTR query is used to get the RR with the primary name of the host. For example, a request for the host name corresponding to IP address 1.2.3.4 looks for PTR RRs for domain name "4.3.2.1.IN-ADDR.ARPA".

There are, of course, numerous examples of IPv4 addresses scattered throughout the document.

3.12. RFC 1035 Domain Names: Implementation and Specification

Section 3.4.1, "A RDATA format", defines the format for A records:

```
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ADDRESS                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

where:

ADDRESS A 32 bit Internet address.

Hosts that have multiple Internet addresses will have multiple A records.

A records cause no additional section processing. The RDATA section of an A line in a master file is an Internet address expressed as four decimal numbers separated by dots without any embedded spaces (e.g.,"10.2.0.52" or "192.0.5.6").

And Section 3.4.2, "WKS RDATA", format is:

```
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ADDRESS                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|       PROTOCOL        |                       |
+--+--+--+--+--+--+--+--+                       |
|                                               |
/                   <BIT MAP>                   /

/                                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

where:

ADDRESS   An 32 bit Internet address

PROTOCOL   An 8 bit IP protocol number

<BIT MAP>   A variable length bit map. The bit map must be a multiple of 8 bits long.

The WKS record is used to describe the well known services supported by a particular protocol on a particular internet address. The PROTOCOL field specifies an IP protocol number, and the bit map has one bit per port of the specified protocol. The first bit corresponds to port 0, the second to port 1, etc. If the bit map does not include a bit for a protocol of interest, that bit is assumed zero. The appropriate values and mnemonics for ports and protocols are specified in RFC1010.

For example, if PROTOCOL=TCP (6), the 26th bit corresponds to TCP port 25 (SMTP). If this bit is set, a SMTP server should be listening on TCP port 25; if zero, SMTP service is not supported on the specified address.

The purpose of WKS RRs is to provide availability information for servers for TCP and UDP. If a server supports both TCP and UDP, or has multiple Internet addresses, then multiple WKS RRs are used.

WKS RRs cause no additional section processing.

Section 3.5, "IN-ADDR.ARPA domain", describes reverse DNS lookups and is clearly IPv4 dependent.

There are, of course, numerous examples of IPv4 addresses scattered throughout the document.

3.13. RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks

This specification specifically deals with the transmission of IPv4 packets over IEEE 802 networks.

3.14. RFC 1044 Internet Protocol on Network System's HYPERchannel: Protocol Specification

There are a variety of methods used in this standard to map IPv4 addresses to 32 bits fields in the HYPERchannel headers. This specification does not support IPv6.

3.15. RFC 1055 Nonstandard for transmission of IP datagrams over serial lines: SLIP

This specification is more of an analysis of the shortcomings of SLIP which is unsurprising. The introduction of PPP as a general replacement of SLIP has made this specification essentially unused. No update need be considered.

3.16. RFC 1088 Standard for the transmission of IP datagrams over NetBIOS networks

This specification documents a technique to encapsulate IP packets inside NetBIOS packets.

The technique presented of using NetBIOS names of the form IP.XX.XX.XX.XX will not work for IPv6 addresses since the length of IPv6 addresses will not fit within the NetBIOS 15 octet name limitation.

3.17. RFC 1112 Host Extensions for IP Multicasting

This specification defines IP multicast. Parts of the document are IPv4 dependent.

3.18. RFC 1132 Standard for the transmission of 802.2 packets over IPX networks

There are no IPv4 dependencies in this specification.

3.19. RFC 1201 Transmitting IP traffic over ARCNET networks

The major concerns of this specification with respect to IPv4 addresses occur in the resolution of ARCnet 8bit addresses to IPv4 addresses in an "ARPlike" method. This is incompatible with IPv6.

3.20. RFC 1209 The Transmission of IP Datagrams over the SMDS Service

This specification defines running IPv4 and ARP over SMDS. The methods described could easily be extended to support IPv6 packets.

3.21. RFC 1390 Transmission of IP and ARP over FDDI Networks

This specification defines the use of IPv4 address on FDDI networks. There are numerous IPv4 dependencies in the specification.

In particular the value of the Protocol Type Code (2048 for IPv4) and a corresponding Protocol Address length (4 bytes for IPv4) needs to be created. A discussion of broadcast and multicast addressing techniques is also included, and similarly must be updated for IPv6 networks. The defined MTU limitation of 4096 octets of data (with 256 octets reserved header space) should remain sufficient for IPv6.

3.22. RFC 1661 The Point-to-Point Protocol (PPP)

There are no IPv4 dependencies in this specification.

3.23. RFC 1662 PPP in HDLC-like Framing

There are no IPv4 dependencies in this specification.

3.24. RFC 2427 Multiprotocol Interconnect over Frame Relay

There are no IPv4 dependencies in this specification.

4. Draft Standards

Draft Standards represent the penultimate standard level in the IETF. A protocol can only achieve draft standard when there are multiple, independent, interoperable implementations. Draft Standards are usually quite mature and widely used.

4.1. RFC 951 Bootstrap Protocol (BOOTP)

This protocol is designed specifically for use with IPv4, for example:

> Section 3. Packet Format
>
> All numbers shown are decimal, unless indicated otherwise. The BOOTP packet is enclosed in a standard IP UDP datagram. For simplicity it is assumed that the BOOTP packet is never fragmented. Any numeric fields shown are packed in 'standard network byte order', i.e., high order bits are sent first.

In the IP header of a bootrequest, the client fills in its own IP source address if known, otherwise zero. When the server address is unknown, the IP destination address will be the 'broadcast address' 255.255.255.255. This address means 'broadcast on the local cable, (I don't know my net number)'.

```
    FIELD   BYTES   DESCRIPTION
    -----   -----   ---

[...]
       ciaddr  4       client IP address;
                       filled in by client in bootrequest if known.

       yiaddr  4       'your' (client) IP address;
                       filled by server if client doesn't
                       know its own address (ciaddr was 0).

       siaddr  4       server IP address;
                       returned in bootreply by server.

       giaddr  4       gateway IP address,
                       used in optional cross-gateway booting.
```

Since the packet format is a fixed 300 bytes in length, an updated version of the specification could easily accommodate an additional 48 bytes (4 IPv6 fields of 16 bytes to replace the existing 4 IPv4 fields of 4 bytes).

4.2. RFC 1188 Proposed Standard for the Transmission of IP Datagrams over FDDI Networks

This document is clearly informally superseded by RFC 1390, "Transmission of IP and ARP over FDDI Networks", even though no formal deprecation has been done. Therefore, this specification is not considered further in this memo.

4.3. RFC 1191 Path MTU discovery

The entire process of PMTU discovery is predicated on the use of the DF bit in the IPv4 header, an ICMP message (also IPv4 dependent) and TCP MSS option. This is not compatible with IPv6.

4.4. RFC 1356 Multiprotocol Interconnect on X.25 and ISDN

Section 3.2 defines an NLPID for IP as follows:

> The value hex CC (binary 11001100, decimal 204) is IP. Conformance with this specification requires that IP be supported.

See section 5.1 for a diagram of the packet formats.

Clearly a new NLPID would need to be defined for IPv6 packets.

4.5. RFC 1534 Interoperation Between DHCP and BOOTP

There are no IPv4 dependencies in this specification.

4.6. RFC 1542 Clarifications and Extensions for the Bootstrap Protocol

There are no new issues other than those presented in Section 4.1.

4.7. RFC 1629 Guidelines for OSI NSAP Allocation in the Internet

There are no IPv4 dependencies in this specification.

4.8. RFC 1762 The PPP DECnet Phase IV Control Protocol (DNCP)

There are no IPv4 dependencies in this specification.

4.9. RFC 1989 PPP Link Quality Monitoring

There are no IPv4 dependencies in this specification.

4.10. RFC 1990 The PPP Multilink Protocol (MP)

Section 5.1.3, "Endpoint Discriminator Option", defines a Class header field:

Class
The Class field is one octet and indicates the identifier address space. The most up-to-date values of the LCP Endpoint Discriminator Class field are specified in the most recent "Assigned Numbers" RFC. Current values are assigned as follows:

0 Null Class

1 Locally Assigned Address

2 Internet Protocol (IP) Address

3 IEEE 802.1 Globally Assigned MAC Address

4 PPP Magic-Number Block

5 Public Switched Network Directory Number

A new class field needs to be defined by the IANA for IPv6 addresses.

4.11. RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)

There are no IPv4 dependencies in this specification.

4.12. RFC 2067 IP over HIPPI

Section 5.1, "Packet Formats", contains the following excerpt:

> EtherType (16 bits) SHALL be set as defined in Assigned Numbers: IP = 2048 ('0800'h), ARP = 2054 ('0806'h), RARP = 32,821 ('8035'h).

Section 5.5, "MTU", has the following definition:

> The MTU for HIPPI-SC LANs is 65280 bytes.
>
> This value was selected because it allows the IP packet to fit in one 64K byte buffer with up to 256 bytes of overhead. The overhead is 40 bytes at the present time; there are 216 bytes of room for expansion.

```
HIPPI-FP Header                   8 bytes
HIPPI-LE Header                  24 bytes
IEEE 802.2 LLC/SNAP Headers       8 bytes
Maximum IP packet size (MTU) 65280 bytes
                             ------------
                  Total      65320 bytes (64K - 216)
```

This definition is not applicable for IPv6 packets since packets can be larger than the IPv4 limitation of 65280 bytes.

4.13. RFC 2131 Dynamic Host Configuration Protocol

This version of DHCP is highly predicated of IPv4. It is not compatible with IPv6.

4.14. RFC 2132 DHCP Options and BOOTP Vendor Extensions

This is an extension to an IPv4-only specification.

4.15. RFC 2390 Inverse Address Resolution Protocol

There are no IPv4 dependencies in this specification.

4.16. RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

This document defines IPv6 and has no IPv4 issues.

4.17. RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)

This document defines an IPv6 related specification and has no IPv4 issues.

4.18. RFC 2462 IPv6 Stateless Address Autoconfiguration

This document defines an IPv6 related specification and has no IPv4 issues.

4.19. RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

This document defines an IPv6 related specification and has no IPv4 issues.

4.20. RFC 3596 DNS Extensions to support IP version 6

This specification defines the AAAA record for IPv6 as well as PTR records using the ip6.arpa domain, and as such has no IPv6 issues.

5. Proposed Standards

Proposed Standards are introductory level documents. There are no requirements for even a single implementation. In many cases, Proposed are never implemented or advanced in the IETF standards process. They, therefore, are often just proposed ideas that are presented to the Internet community. Sometimes flaws are exposed or they are one of many competing solutions to problems. In these later cases, no discussion is presented as it would not serve the purpose of this discussion.

5.1. RFC 1234 Tunneling IPX traffic through IP networks

The section "Unicast Address Mappings" has the following text:

> For implementations of this memo, the first two octets of the host number will always be zero and the last four octets will be the node’s four octet IP address. This makes address mapping trivial for unicast transmissions: the first two octets of the host number are discarded, leaving the normal four octet IP address. The encapsulation code should use this IP address as the destination address of the UDP/IP tunnel packet.

This mapping will not be able to work with IPv6 addresses.

There are also numerous discussions on systems keeping a "peer list" to map between IP and IPX addresses. The specifics are not discussed in the document and are left to the individual implementation.

The section "Maximum Transmission Unit" also has some implications on IP addressing:

> Although larger IPX packets are possible, the standard maximum transmission unit for IPX is 576 octets. Consequently, 576 octets is the recommended default maximum transmission unit for IPX packets being sent with this encapsulation technique. With the eight octet UDP header and the 20 octet IP header, the resulting IP packets will be 604 octets long. Note that this is larger than the 576 octet maximum size IP implementations are required to accept. Any IP implementation supporting this encapsulation technique must be capable of receiving 604 octet IP packets.
>
> As improvements in protocols and hardware allow for larger, unfragmented IP transmission units, the 576 octet maximum IPX packet size may become a liability. For this reason, it is recommended that the IPX maximum transmission unit size be configurable in implementations of this memo.

5.2. RFC 1256 ICMP Router Discovery Messages

This specification defines a mechanism very specific to IPv4.

5.3. RFC 1277 Encoding Network Addresses to Support Operation over Non-OSI Lower Layers

Section 4.5, "TCP/IP (RFC 1006) Network Specific Format" describes a structure that reserves 12 digits for the textual representation of an IP address.

This 12 octet field for decimal versions of IP addresses is insufficient for a decimal version of IPv6 addresses. It is possible to define a new encoding using the 20 digit long IP Address + Port + Transport Set fields in order to accommodate a binary version of an IPv6 address, port number and Transport Set. There are several schemes that could be envisioned.

5.4. RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)

This specification defines a mechanism for devices to assign IPv4 addresses to PPP clients once PPP negotiation is completed. Section 3, "IPCP Configuration Options", defines IPCP option types which embed the IP address in 4-byte long fields. This is clearly not enough for IPv6.

However, the specification is clearly designed to allow new Option Types to be added and Should offer no problems for use with IPv6 once appropriate options have been defined.

5.5. RFC 1377 The PPP OSI Network Layer Control Protocol (OSINLCP)

There are no IPv4 dependencies in this specification.

5.6. RFC 1378 The PPP AppleTalk Control Protocol (ATCP)

There are no IPv4 dependencies in this specification.

5.7. RFC 1469 IP Multicast over Token-Ring Local Area Networks

This document defines the usage of IPv4 multicast over IEEE 802.5 Token Ring networks. This is not compatible with IPv6.

5.8. RFC 1552 The PPP Internetworking Packet Exchange Control Protocol (IPXCP)

There are no IPv4 dependencies in this specification.

5.9. RFC 1570 PPP LCP Extensions

There are no IPv4 dependencies in this specification.

5.10. RFC 1598 PPP in X.25 PPP-X25

There are no IPv4 dependencies in this specification.

5.11. RFC 1618 PPP over ISDN

There are no IPv4 dependencies in this specification.

5.12. RFC 1663 PPP Reliable Transmission

There are no IPv4 dependencies in this specification.

5.13. RFC 1752 The Recommendation for the IP Next Generation Protocol

This document defines a road map for IPv6 development and is not relevant to this discussion.

5.14. RFC 1755 ATM Signaling Support for IP over ATM

There are no IPv4 dependencies in this specification.

5.15. RFC 1763 The PPP Banyan Vines Control Protocol (BVCP)

There are no IPv4 dependencies in this specification.

5.16. RFC 1764 The PPP XNS IDP Control Protocol (XNSCP)

There are no IPv4 dependencies in this specification.

5.17. RFC 1973 PPP in Frame Relay

There are no IPv4 dependencies in this specification.

5.18. RFC 1981 Path MTU Discovery for IP version 6

This specification describes an IPv6 related specification and is not discussed in this document.

5.19. RFC 1982 Serial Number Arithmetic

There are no IPv4 dependencies in this specification.

5.20. RFC 1995 Incremental Zone Transfer in DNS

Although the examples used in this document use IPv4 addresses, (i.e., A records) there is nothing in the specification to preclude full and proper functionality using IPv6.

5.21. RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)

There are no IPv4 dependencies in this specification.

5.22. RFC 2003 IP Encapsulation within IP

This document is designed for use in IPv4 networks. There are many references to a specified IP version number of 4 and 32-bit addresses. This is incompatible with IPv6.

5.23. RFC 2004 Minimal Encapsulation within IP

This document is designed for use in IPv4 networks. There are many references to a specified IP version number of 4 and 32-bit addresses. This is incompatible with IPv6.

5.24. RFC 2005 Applicability Statement for IP Mobility Support

This specification documents the interoperation of IPv4 Mobility Support; this is not relevant to this discussion.

5.25. RFC 2022 Support for Multicast over UNI 3.0/3.1 based ATM Networks

This specification specifically maps IPv4 multicast in UNI based ATM networks. This is incompatible with IPv6.

5.26. RFC 2043 The PPP SNA Control Protocol (SNACP)

There are no IPv4 dependencies in this specification.

5.27. RFC 2097 The PPP NetBIOS Frames Control Protocol (NBFCP)

There are no IPv4 dependencies in this specification.

5.28. RFC 2113 IP Router Alert Option

This document provides a new mechanism for IPv4. This is incompatible with IPv6.

5.29. RFC 2125 The PPP Bandwidth Allocation Protocol (BAP) / The PPP Bandwidth Allocation Control Protocol (BACP)

There are no IPv4 dependencies in this specification.

5.30. RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)

There are no IPv4 dependencies in this specification.

5.31. RFC 2181 Clarifications to the DNS Specification

There are no IPv4 dependencies in this specification. The only reference to IP addresses discuss the use of an anycast address, so but one can assume that these techniques are IPv6 operable.

5.32. RFC 2225 Classical IP and ARP over ATM

From the many references in this document, it is clear that this document is designed for IPv4 only. It is only later in the document that it is implicitly stated, as in:

```
ar$spln -  length in octets of the source protocol address. Value
           range is 0 or 4 (decimal).  For IPv4 ar$spln is 4.

ar$tpln -  length in octets of the target protocol address. Value
           range is 0 or 4 (decimal).  For IPv4 ar$tpln is 4.
```

and:

For backward compatibility with previous implementations, a null IPv4 protocol address may be received with length = 4 and an allocated address in storage set to the value 0.0.0.0. Receiving stations must be liberal in accepting this format of a null IPv4 address. However, on transmitting an ATMARP or InATMARP packet, a null IPv4 address must only be indicated by the length set to zero and must have no storage allocated.

5.33. RFC 2226 IP Broadcast over ATM Networks

This document is limited to IPv4 multicasting. This is incompatible with IPv6.

5.34. RFC 2241 DHCP Options for Novell Directory Services

This is an extension to an IPv4-only specification.

5.35. RFC 2242 NetWare/IP Domain Name and Information

This is an extension to an IPv4-only specification, for example:

PREFERRED_DSS (code 6)

Length is (n * 4) and the value is an array of n IP addresses, each four bytes in length. The maximum number of addresses is 5 and therefore the maximum length value is 20. The list contains the addresses of n NetWare Domain SAP/RIP Server (DSS).

NEAREST_NWIP_SERVER (code 7)

Length is (n * 4) and the value is an array of n IP addresses, each four bytes in length. The maximum number of addresses is 5 and therefore the maximum length value is 20. The list contains the addresses of n Nearest NetWare/IP servers.

PRIMARY_DSS (code 11)

Length of 4, and the value is a single IP address. This field identifies the Primary Domain SAP/RIP Service server (DSS) for this NetWare/IP domain. NetWare/IP administration utility uses this value as Primary DSS server when configuring a secondary DSS server.

5.36. RFC 2290 Mobile-IPv4 Configuration Option for PPP IPCP

This document is designed for use with Mobile IPv4. There are numerous referrals to other IP "support" mechanisms (i.e., ICMP Router Discover Messages) that specifically refer to the IPv4 of ICMP.

5.37. RFC 2308 Negative Caching of DNS Queries (DNS NCACHE)

Although there are numerous examples in this document that use IPv4 "A" records, there is nothing in the specification that limits its effectiveness to IPv4.

5.38. RFC 2331 ATM Signaling Support for IP over ATM - UNI Signaling 4.0 Update

There are no IPv4 dependencies in this specification.

5.39. RFC 2332 NBMA Next Hop Resolution Protocol (NHRP)

This document is very generic in its design and seems to be able to support numerous layer 3 addressing schemes and should include both IPv4 and IPv6.

5.40. RFC 2333 NHRP Protocol Applicability

This document is very generic in its design and seems to be able to support numerous layer 3 addressing schemes and should include both IPv4 and IPv6.

5.41. RFC 2335 A Distributed NHRP Service Using SCSP

There are no IPv4 dependencies in this specification.

5.42. RFC 2363 PPP Over FUNI

There are no IPv4 dependencies in this specification.

5.43. RFC 2364 PPP Over AAL5

There are no IPv4 dependencies in this specification.

5.44. RFC 2371 Transaction Internet Protocol Version 3.0 (TIPV3)

This document states:

TIP transaction manager addresses take the form:

<hostport><path>

The <hostport> component comprises:

<host>[:<port>]

where <host> is either a <dns name> or an <ip address>; and <port> is a decimal number specifying the port at which the transaction manager (or proxy) is listening for requests to establish TIP connections. If the port number is omitted, the standard TIP port number (3372) is used.

A <dns name> is a standard name, acceptable to the domain name service. It must be sufficiently qualified to be useful to the receiver of the command.

An <ip address> is an IP address, in the usual form: four decimal numbers separated by period characters.

And further along it states:

A TIP URL takes the form:

tip://<transaction manager address>?<transaction string>

where <transaction manager address> identifies the TIP transaction manager (as defined in Section 7 above); and <transaction string> specifies a transaction identifier, which may take one of two forms (standard or non-standard):

i. "urn:" <NID> ":" <NSS>

A standard transaction identifier, conforming to the proposed Internet Standard for Uniform Resource Names (URNs), as specified by RFC2141; where <NID> is the Namespace Identifier, and <NSS> is the Namespace Specific String. The Namespace ID determines the syntactic interpretation of the Namespace Specific String. The Namespace Specific String is a sequence of characters representing a transaction identifier (as defined by <NID>). The rules for the contents of these fields are specified by RFC2141 (valid characters, encoding, etc.).

This format of <transaction string> may be used to express global transaction identifiers in terms of standard representations. Examples for <NID> might be <iso> or <xopen>, e.g.,

tip://123.123.123.123/?urn:xopen:xid

Note that Namespace Ids require registration.

ii. <transaction identifier>

A sequence of printable ASCII characters (octets with values in the range 32 through 126 inclusive (excluding ":") representing a transaction identifier. In this non-standard case, it is the combination of <transaction manager address> and <transaction identifier> which ensures global uniqueness, e.g.,

tip://123.123.123.123/?transid1

These are incompatible with IPv6.

5.45. RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

This specification documents a method for transmitting IPv6 packets over Ethernet and is not considered in this discussion.

5.46. RFC 2467 Transmission of IPv6 Packets over FDDI Networks

This specification documents a method for transmitting IPv6 packets over FDDI and is not considered in this discussion.

5.47. RFC 2470 Transmission of IPv6 Packets over Token Ring Networks

This specification documents a method for transmitting IPv6 packets over Token Ring and is not considered in this discussion.

5.48. RFC 2472 IP Version 6 over PPP

This specification documents a method for transmitting IPv6 packets over PPP and is not considered in this discussion.

5.49. RFC 2473 Generic Packet Tunneling in IPv6 Specification

This specification documents an IPv6 aware specification and is not considered in this discussion.

5.50. RFC 2484 PPP LCP Internationalization Configuration Option

There are no IPv4 dependencies in this specification.

5.51. RFC 2485 DHCP Option for The Open Group's User Authentication Protocol

This is an extension to an IPv4-only specification.

5.52. RFC 2486 The Network Access Identifier

There are no IPv4 dependencies in this specification.

5.53. RFC 2491 IPv6 over Non-Broadcast Multiple Access (NBMA) Networks

This specification documents a method for transmitting IPv6 packets over NBMA networks and is not considered in this discussion.

5.54. RFC 2492 IPv6 over ATM Networks

This specification documents a method for transmitting IPv6 packets over ATM networks and is not considered in this discussion.

5.55. RFC 2497 Transmission of IPv6 Packets over ARCnet Networks

This specification documents a method for transmitting IPv6 packets over ARCnet networks and is not considered in this discussion.

5.56. RFC 2507 IP Header Compression

This specification is both IPv4 and IPv6 aware.

5.57. RFC 2526 Reserved IPv6 Subnet Anycast Addresses

This specification documents IPv6 addressing and is not discussed in this document.

5.58. RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels

This specification documents IPv6 transmission methods and is not discussed in this document.

5.59. RFC 2563 DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients

This is an extension to an IPv4-only specification.

5.60. RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification

This specification documents IPv6 transmission method over Frame Relay and is not discussed in this document.

5.61. RFC 2601 ILMI-Based Server Discovery for ATMARP

This specification is both IPv4 and IPv6 aware.

5.62. RFC 2602 ILMI-Based Server Discovery for MARS

This specification is both IPv4 and IPv6 aware.

5.63. RFC 2603 ILMI-Based Server Discovery for NHRP

This specification is both IPv4 and IPv6 aware.

5.64. RFC 2610 DHCP Options for Service Location Protocol

This is an extension to an IPv4-only specification.

5.65. RFC 2615 PPP over SONET/SDH

There are no IPv4 dependencies in this specification.

5.66. RFC 2625 IP and ARP over Fibre Channel

This document states:

> Objective and Scope:
>
> The major objective of this specification is to promote interoperable implementations of IPv4 over FC. This specification describes a method for encapsulating IPv4 and Address Resolution Protocol (ARP) packets over FC.

This is incompatible with IPv6.

5.67. RFC 2661 Layer Two Tunneling Protocol (L2TP)

There are no IPv4 dependencies in this specification.

5.68. RFC 2671 Extension Mechanisms for DNS (EDNS0)

There are no IPv4 dependencies in this specification.

5.69. RFC 2672 Non-Terminal DNS Name Redirection

This document is only defined for IPv4 addresses. An IPv6 specification may be needed.

5.70. RFC 2673 Binary Labels in the Domain Name System

This document is only defined for IPv4 addresses. An IPv6 specification may be needed.

5.71. RFC 2675 IPv6 Jumbograms

This document defines a IPv6 packet format and is therefore not discussed in this document.

5.72. RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5

There are no IPv4 dependencies in this specification.

5.73. RFC 2685 Virtual Private Networks Identifier

There are no IPv4 dependencies in this specification.

5.74. RFC 2686 The Multi-Class Extension to Multi-Link PPP

There are no IPv4 dependencies in this specification.

5.75. RFC 2687 PPP in a Real-time Oriented HDLC-like Framing

There are no IPv4 dependencies in this specification.

5.76. RFC 2688 Integrated Services Mappings for Low Speed Networks

There are no IPv4 dependencies in this specification.

5.77. RFC 2710 Multicast Listener Discovery (MLD) for IPv6

This document defines an IPv6 specific specification and is not discussed in this document.

5.78. RFC 2711 IPv6 Router Alert Option

This document defines an IPv6 specific specification and is not discussed in this document.

5.79. RFC 2728 The Transmission of IP Over the Vertical Blanking Interval of a Television Signal

The following data format is defined:

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |0|    group    |         uncompressed IP header (20 bytes)     |
 +-+-+-+-+-+-+-+-+                                               +
 |                                                               |
 :                             ....                              :
 +               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |               |        uncompressed UDP header (8 bytes)      |
 +-+-+-+-+-+-+-+-+                                               +
 |                                                               |
 +               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |               |              payload  (<1472 bytes)           |
 +-+-+-+-+-+-+-+-+                                               +
 |                                                               |
 :                              ....                             :
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                             CRC                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

This is incompatible with IPv6.

5.80. RFC 2734 IPv4 over IEEE 1394

This specification is IPv4 only.

5.81. RFC 2735 NHRP Support for Virtual Private Networks

This specification implies only IPv4 operations, but does not seem to present any reason that it would not function for IPv6.

5.82. RFC 2765 Stateless IP/ICMP Translation Algorithm (SIIT)

This specification defines a method for IPv6 transition and is not discussed in this document.

5.83. RFC 2766 Network Address Translation - Protocol Translation (NAT-PT)

This specification defines a method for IPv6 transition and is not discussed in this document.

5.84. RFC 2776 Multicast-Scope Zone Announcement Protocol (MZAP)

This specification is both IPv4 and IPv6 aware and needs no changes.

5.85. RFC 2782 A DNS RR for specifying the location of services

There are no IPv4 dependencies in this specification.

5.86. RFC 2794 Mobile IP Network Access Identifier Extension for IPv4

This is an extension to an IPv4-only specification.

5.87. RFC 2834 ARP and IP Broadcast over HIPPI-800

This document uses the generic term "IP Address" in the text but it also contains the text:

```
   The HARP message has several fields that have the following format
   and values:

     Data sizes and field meaning:
       ar$hrd  16 bits  Hardware type
       ar$pro  16 bits  Protocol type of the protocol fields below
       ar$op   16 bits  Operation code (request, reply, or NAK)
       ar$pln   8 bits  byte length of each protocol address
       ar$rhl   8 bits  requester’s HIPPI hardware address length (q)
       ar$thl   8 bits  target’s HIPPI hardware address length (x)
       ar$rpa  32 bits  requester’s protocol address
       ar$tpa  32 bits  target’s protocol address
       ar$rha  qbytes   requester’s HIPPI Hardware address
       ar$tha  xbytes   target’s HIPPI Hardware address

     Where:
       ar$hrd  - SHALL contain 28. (HIPARP)

       ar$pro  - SHALL contain the IP protocol code 2048 (decimal).

       ar$op   - SHALL contain the operational value (decimal):
                 1  for   HARP_REQUESTs
                 2  for   HARP_REPLYs
                 8  for InHARP_REQUESTs
                 9  for InHARP_REPLYs
                 10 for   HARP_NAK
       ar$pln  - SHALL contain 4.
```

And later:

```
   31    28         23  21          15         10     7         2   0
   +-----+---------+-+-+-----------+---------+-----+---------+-----+
 0 |      04       |1|0|         000         |      03       |  0  |
   +---------------+-+-+---------------------+---------------+-----+
 1 |                              45                               |
   +-----+-+-------+-----------------------+-----------------------+
 2 |[LA] |W|MsgT= 0|          000          |   Dest. Switch Addr   |
   +-----+-+-------+-----------------------+-----------------------+
 3 |   2   |   2   |          000          |  Source Switch Addr   |
   +---------------+---------------+-------+-----------------------+
 4 |             00 00             |                               |
   +-------------------------------+                               |
 5 |                         Destination ULA                       |
   +-------------------------------+-------------------------------+
 6 |             [LA]              |                               |
   +-------------------------------+                               |
 7 |                            Source ULA                         |
   +===============+===============+===============+===============+
 8 |       AA      |      AA       |       03      |      00       |
   +---------------+---------------+---------------+---------------+
 9 |       00      |      00       |        Ethertype (2054)       |
   +---------------+---------------+-------------------------------+
10 |             hrd (28)          |           pro (2048)          |
   +---------------+---------------+---------------+---------------+
11 |             op (ar$op)        |     pln (6)   |   rhl (q)     |
   +---------------+---------------+---------------+---------------+
12 |    thl = (x)  |   Requester IP Address upper  (24 bits)       |
   +---------------------------------------------------------------+
13 | Req. IP lower |      Target IP Address upper  (24 bits)       |
   +---------------+-----------------------------------------------+
14 | Tgt. IP lower | Requester HIPPI Hardware Address bytes 0 - 2  |
   +---------------+-----------------------------------------------+
15 |         Requester HIPPI Hardware Address bytes 3 - 6          |
   +-----------------------------------------------+---------------+
16 |         Requester HW Address bytes 7 - q      | Tgt HW byte 0 |
   +---------------+---------------+---------------+---------------+
17 |          Target  HIPPI Hardware Address bytes 1 - 4           |
   +---------------------------------------------------------------+
18 |          Target  HIPPI Hardware Address bytes 5 - 8           |
   +---------------+---------------+---------------+---------------+
19 |Tgt HW byte 9-x|     FILL      |     FILL      |     FILL      |
   +---------------+---------------+---------------+---------------+
                        HARP - InHARP Message
```

This is incompatible with IPv6.

5.88. RFC 2835 IP and ARP over HIPPI-6400

This document states:

The Ethertype value SHALL be set as defined in Assigned Numbers:

IP 0x0800 2048 (16 bits)

This is limited to IPv4, and similar to the previous section, incompatible with IPv6. There are numerous other points in the documents that confirm this assumption.

5.89. RFC 2855 DHCP for IEEE 1394

This is an extension to an IPv4-only specification.

5.90. RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering

This document defines a specification to interact with IPv6 and is not considered in this document.

5.91. RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers

This document defines a transition mechanism for IPv6 and is not considered in this document.

5.92. RFC 2916 E.164 number and DNS

There are no IPv4 dependencies in this specification.

5.93. RFC 2937 The Name Service Search Option for DHCP

This is an extension to an IPv4-only specification.

5.94. RFC 3004 The User Class Option for DHCP

This is an extension to an IPv4-only specification.

5.95. RFC 3011 The IPv4 Subnet Selection Option for DHCP

This is an extension to an IPv4-only specification.

5.96. RFC 3021 Using 31-Bit Prefixes for IPv4 P2P Links

This specification is specific to IPv4 address architecture, where a modification is needed to use both addresses of a 31-bit prefix. This is possible by IPv6 address architecture, but in most cases not recommended; see RFC 3627, Use of /127 Prefix Length Between Routers Considered Harmful.

5.97. RFC 3024 Reverse Tunneling for Mobile IP, revised

This is an extension to an IPv4-only specification.

5.98. RFC 3046 DHCP Relay Agent Information Option

This is an extension to an IPv4-only specification.

5.99. RFC 3056 Connection of IPv6 Domains via IPv4 Clouds

This is an IPv6 related document and is not discussed in this document.

5.100. RFC 3068 An Anycast Prefix for 6to4 Relay Routers

This is an IPv6 related document and is not discussed in this document.

5.101. RFC 3070 Layer Two Tunneling Protocol (L2TP) over Frame Relay

There are no IPv4 dependencies in this specification.

5.102. RFC 3074 DHC Load Balancing Algorithm

There are no IPv4 dependencies in this specification.

5.103. RFC 3077 A Link-Layer Tunneling Mechanism for Unidirectional Links

This specification is both IPv4 and IPv6 aware and needs no changes.

5.104. RFC 3115 Mobile IP Vendor/Organization-Specific Extensions

This is an extension to an IPv4-only specification.

5.105. RFC 3145 L2TP Disconnect Cause Information

There are no IPv4 dependencies in this specification.

5.106. RFC 3344 IP Mobility Support for IPv4

There are IPv4 dependencies in this specification.

5.107. RFC 3376 Internet Group Management Protocol, Version 3

This document describes of version of IGMP used for IPv4 multicast. This is not compatible with IPv6.

5.108. RFC 3402 Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm

There are no IPv4 dependencies in this specification.

5.109. RFC 3403 Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database

There are no IPv4 dependencies in this specification.

5.110. RFC 3513 IP Version 6 Addressing Architecture

This specification documents IPv6 addressing and is not discussed in this document.

5.111. RFC 3518 Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP)

There are no IPv4 dependencies in this specification.

6. Experimental RFCs

Experimental RFCs typically define protocols that do not have wide scale implementation or usage on the Internet. They are often propriety in nature or used in limited arenas. They are documented to the Internet community in order to allow potential interoperability or some other potential useful scenario. In a few cases they are presented as alternatives to the mainstream solution to an acknowledged problem.

6.1. RFC 1149 Standard for the transmission of IP datagrams on avian carriers

There are no IPv4 dependencies in this specification. In fact the flexibility of this specification is such that all versions of IP should function within its boundaries, presuming that the packets remain small enough to be transmitted with the 256 milligrams weight limitations.

6.2. RFC 1183 New DNS RR Definitions

There are no IPv4 dependencies in this specification.

6.3. RFC 1226 Internet protocol encapsulation of AX.25 frames

There are no IPv4 dependencies in this specification.

6.4. RFC 1241 Scheme for an internet encapsulation protocol: Version 1

This specification defines a specification that assumes IPv4 but does not actually have any limitations which would limit its operation in an IPv6 environment.

6.5. RFC 1307 Dynamically Switched Link Control Protocol

This specification is IPv4 dependent, for example:

3.1 Control Message Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Identifier                   |   Total length                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Function                     |   Event Status                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Endpoint 1                                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Endpoint 2                                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Message                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Body                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Endpoint addresses: 32 bits each

The internet addresses of the two communicating parties for which the link is being prepared.

6.6. RFC 1393 Traceroute Using an IP Option

This document uses an IPv4 option. It is therefore limited to IPv4 networks, and is incompatible with IPv6.

6.7. RFC 1433 Directed ARP

There are no IPv4 dependencies in this specification.

6.8. RFC 1464 Using the Domain Name System To Store Arbitrary String Attributes

There are no IPv4 dependencies in this specification.

6.9. RFC 1475 TP/IX: The Next Internet

This document defines IPv7 and has been abandoned by the IETF as a feasible design. It is not considered in this document.

6.10. RFC 1561 Use of ISO CLNP in TUBA Environments

This document defines the use of NSAP addressing and does not use any version of IP, so there are no IPv4 dependencies in this specification.

6.11. RFC 1712 DNS Encoding of Geographical Location

There are no IPv4 dependencies in this specification.

6.12. RFC 1735 NBMA Address Resolution Protocol (NARP)

This document defines a specification that is IPv4 specific, for example:

4. Packet Formats

NARP requests and replies are carried in IP packets as protocol type 54. This section describes the packet formats of NARP requests and replies:

NARP Request

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Version    |   Hop Count   |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Code       |            Unused             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Source IP address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| NBMA length   |                 NBMA address                  |
+-+-+-+-+-+-+-+-+                                               |
|                  (variable length)                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Source and Destination IP Addresses
  Respectively, these are the IP addresses of the NARP requester
  and the target terminal for which the NBMA address is desired.

And:

NARP Reply

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Version    |   Hop Count   |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Code     |            Unused             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Source IP address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| NBMA length   |                 NBMA address                  |
+-+-+-+-+-+-+-+-+                                               |
|                   (variable length)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Source and Destination IP Address
  Respectively, these are the IP addresses of the NARP requester
  and the target terminal for which the NBMA address is desired.

This is incompatible with IPv6.

6.13. RFC 1768 Host Group Extensions for CLNP Multicasting

This specification defines multicasting for CLNP, which is not an IP protocol, and therefore has no IPv4 dependencies.

6.14. RFC 1788 ICMP Domain Name Messages

This specification is used for updates to the in-addr.arpa reverse DNS maps, and is limited to IPv4.

6.15. RFC 1797 Class A Subnet Experiment

This document is specific to IPv4 address architecture, and as such, has no IPv6 dependencies.

6.16. RFC 1819 Internet Stream Protocol Version 2 (ST2) Protocol Specification - Version ST2+

This specification is IPv4 limited. In fact it is the definition of IPv5. It has been abandoned by the IETF as feasible design, and is not considered in this discussion.

6.17. RFC 1868 ARP Extension - UNARP

This specification defines an extension to IPv4 ARP to delete entries from ARP caches on a link.

6.18. RFC 1876 A Means for Expressing Location Information in the Domain Name System

This document defines a methodology for applying this technology which is IPv4 dependent. The specification itself has no IPv4 dependencies.

6.19. RFC 1888 OSI NSAPs and IPv6

This is an IPv6 related document and is not discussed in this document.

6.20. RFC 2009 GPS-Based Addressing and Routing

The document states:

> The future version of IP (IP v6) will certainly have a sufficient number of bits in its addressing space to provide an address for even smaller GPS addressable units. In this proposal, however, we assume the current version of IP (IP v4) and we make sure that we manage the addressing space more economically than that. We will call the smallest GPS addressable unit a GPS-square.

This specification does not seem to have real IPv4 dependencies.

6.21. RFC 2143 Encapsulating IP with the SCSI

This specification will only operate using IPv4. As stated in the document:

> It was decided that the ten byte header offers the greatest flexibility for encapsulating version 4 IP datagrams for the following reasons: [...]

This is incompatible with IPv6.

6.22. RFC 2345 Domain Names and Company Name Retrieval

There are no IPv4 dependencies in this specification.

6.23. RFC 2443 A Distributed MARS Service Using SCSP

This document gives default values for use on IPv4 networks, but is designed to be extensible so it will work with IPv6 with appropriate IANA definitions.

6.24. RFC 2471 IPv6 Testing Address Allocation

This is an IPv6 related document and is not discussed in this document.

6.25. RFC 2520 NHRP with Mobile NHCs

This specification is both IPv4 and IPv6 aware and needs no changes.

6.26. RFC 2521 ICMP Security Failures Messages

There are no IPv4 dependencies in this specification.

6.27. RFC 2540 Detached Domain Name System (DNS) Information

There are no IPv4 dependencies in this specification.

6.28. RFC 2823 PPP over Simple Data Link (SDL) using SONET/SDH with ATM-like framing

There are no IPv4 dependencies in this specification.

6.29. RFC 3123 A DNS RR Type for Lists of Address Prefixes

This specification is both IPv4 and IPv6 aware and needs no changes.

6.30. RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP

This specification is both IPv4 and IPv6 aware and needs no changes.

6.31. RFC 3180 GLOP Addressing in 233/8

This document is specific to IPv4 multicast addressing.

7. Summary of the Results

In the initial survey of RFCs 52 positives were identified out of a total of 186, broken down as follows:

Standards:	17 out of 24 or 70.83%
Draft Standards:	6 out of 20 or 30.00%
Proposed Standards:	22 out of 111 or 19.91%
Experimental RFCs:	7 out of 31 or 22.58%

Of those identified many require no action because they document outdated and unused protocols, while others are document protocols that are actively being updated by the appropriate working groups. Additionally there are many instances of standards that should be updated but do not cause any operational impact if they are not updated.

7.1. Standards

7.1.1. RFC 791 Internet Protocol

RFC 791 has been updated in the definition of IPv6 in RFC 2460.

7.1.2. RFC 792 Internet Control Message Protocol

RFC 792 has been updated in the definition of ICMPv6 in RFC 2463.

7.1.3. RFC 891 DCN Networks

DCN has long since been ceased to be used, so this specification is no longer relevant.

7.1.4. RFC 894 IP over Ethernet

This problem has been fixed by RFC 2464, A Method for the Transmission of IPv6 Packets over Ethernet Networks.

7.1.5. RFC 895 IP over experimental Ethernets

It is believed that experimental Ethernet networks are not being used anymore, so the specification is no longer relevant.

7.1.6. RFC 922 Broadcasting Internet Datagrams in the Presence of Subnets

Broadcasting is not used in IPv6, but similar functionality has been included in RFC 3513, IPv6 Addressing Architecture.

7.1.7. RFC 950 Internet Standard Subnetting Procedure

Broadcasting is not used in IPv6, but similar functionality has been included in RFC 3513, IPv6 Addressing Architecture.

7.1.8. RFC 1034 Domain Names: Concepts and Facilities

The problems have been fixed by defining new resource records for IPv6 addresses.

7.1.9. RFC 1035 Domain Names: Implementation and Specification

The problems have been fixed by defining new resource records for IPv6 addresses.

7.1.10. RFC 1042 IP over IEEE 802

This problem has been fixed by RFC 2470, Transmission of IPv6 Packets over Token Ring Networks.

7.1.11. RFC 1044 IP over HyperChannel

No updated document exists for this specification. It is unclear whether one is needed.

7.1.12. RFC 1088 IP over NetBIOS

No updated document exists for this specification. It is unclear whether one is needed.

7.1.13. RFC 1112 Host Extensions for IP Multicast

The IPv4-specific parts of RFC 1112 have been updated in RFC 2710, Multicast Listener Discovery for IPv6.

7.1.14. RFC 1122 Requirements for Internet Hosts

RFC 1122 is essentially a requirements document for IPv4 hosts. Similar work is in progress [2].

7.1.15. RFC 1201 IP over ARCNET

This problem has been fixed by RFC 2497, A Method for the Transmission of IPv6 Packets over ARCnet Networks.

7.1.16. RFC 1209 IP over SMDS

No updated document exists for this specification. It is unclear whether one is needed.

7.1.17. RFC 1390 Transmission of IP and ARP over FDDI Networks

This problem has been fixed by RFC 2467, Transmission of IPv6 Packets over FDDI Networks.

7.2. Draft Standards

7.2.1. RFC 951 Bootstrap Protocol (BOOTP)

This problem has been fixed by RFC 2462, IPv6 Stateless Address Autoconfiguration, and RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6).

7.2.2. RFC 1191 Path MTU Discovery

This problem has been fixed in RFC 1981, Path MTU Discovery for IP version 6.

7.2.3. RFC 1356 Multiprotocol Interconnect on X.25 and ISDN

This problem can be fixed by defining a new NLPID for IPv6. Note that an NLPID has already been defined in RFC 2427, Multiprotocol Interconnect over Frame Relay.

7.2.4. RFC 1990 The PPP Multilink Protocol (MP)

A new class identifier ("6") for IPv6 packets has been registered with the IANA by the original author, fixing this problem.

7.2.5. RFC 2067 IP over HIPPI

No updated document exists for this specification. It is unclear whether one is needed.

7.2.6. RFC 2131 DHCP

This problem has been fixed in RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6).

Further, the consensus of the DHC WG has been that the options defined for DHCPv4 will not be automatically "carried forward" to DHCPv6. Therefore, any further analysis of additionally specified DHCPv4 Options has been omitted from this memo.

7.3. Proposed Standards

7.3.1. RFC 1234 Tunneling IPX over IP

No updated document exists for this specification. In practice, the similar effect can be achieved by the use of a layer 2 tunneling protocol. It is unclear whether an updated document is needed.

7.3.2. RFC 1256 ICMP Router Discovery

This problem has been resolved in RFC 2461, Neighbor Discovery for IP Version 6 (IPv6).

7.3.3. RFC 1277 Encoding Net Addresses to Support Operation Over Non OSI Lower Layers

No updated document exists for this specification; the problem might be resolved by the creation of a new encoding scheme if necessary. It is unclear whether an update is needed.

7.3.4. RFC 1332 PPP Internet Protocol Control Protocol (IPCP)

This problem has been resolved in RFC 2472, IP Version 6 over PPP.

7.3.5. RFC 1469 IP Multicast over Token Ring

The functionality of this specification has been essentially covered in RFC 2470, Transmission of IPv6 Packets over Token Ring Networks.

7.3.6. RFC 2003 IP Encapsulation within IP

This problem has been fixed by defining different IP-in-IP encapsulation, for example, RFC 2473, Generic Packet Tunneling in IPv6 Specification.

7.3.7. RFC 2004 Minimal Encapsulation within IP

No updated document exists for this specification. It is unclear whether one is needed.

7.3.8. RFC 2022 Support for Multicast over UNI 3.0/3.1 based ATM Networks

No updated document exists for this specification. It is unclear whether one is needed.

7.3.9. RFC 2113 IP Router Alert Option

This problem has been fixed in RFC 2711, IPv6 Router Alert Option.

7.3.10. RFC 2165 SLP

The problems have been addressed in RFC 3111, Service Location Protocol Modifications for IPv6.

7.3.11. RFC 2225 Classical IP & ARP over ATM

The problems have been resolved in RFC 2492, IPv6 over ATM Networks.

7.3.12. RFC 2226 IP Broadcast over ATM

The problems have been resolved in RFC 2492, IPv6 over ATM Networks.

7.3.13. RFC 2371 Transaction IPv3

No updated document exists for this specification. It is unclear whether one is needed.

7.3.14. RFC 2625 IP and ARP over Fibre Channel

There is work in progress to fix these problems

7.3.15. RFC 2672 Non-Terminal DNS Redirection

No updated document exists for this specification. It is unclear whether one is needed.

7.3.16. RFC 2673 Binary Labels in DNS

No updated document exists for this specification. It is unclear whether one is needed.

7.3.17. IP over Vertical Blanking Interval of a TV Signal (RFC 2728)

No updated document exists for this specification. It is unclear whether one is needed.

7.3.18. RFC 2734 IPv4 over IEEE 1394

This problem has been fixed by RFC 3146, Transmission of IPv6 Packets Over IEEE 1394 Networks.

7.3.19. RFC 2834 ARP & IP Broadcasts Over HIPPI 800

No updated document exists for this specification. It is unclear whether one is needed.

7.3.20. RFC 2835 ARP & IP Broadcasts Over HIPPI 6400

No updated document exists for this specification. It is unclear whether one is needed.

7.3.21. RFC 3344 Mobility Support for IPv4

The problems have been resolved by RFC 3775 and RFC 3776 [3, 4].

Since the first Mobile IPv4 specification in RFC 2002, a number of extensions to it have been specified. As all of these depend on MIPv4, they have been omitted from further analysis in this memo.

7.3.22. RFC 3376 Internet Group Management Protocol, Version 3

This problem is being fixed by MLDv2 specification [5].

7.4. Experimental RFCs

7.4.1. RFC 1307 Dynamically Switched Link Control Protocol

No updated document exists for this specification. It is unclear whether one is needed.

7.4.2. RFC 1393 Traceroute using an IP Option

This specification relies on the use of an IPv4 option. No replacement document exists, and it is unclear whether one is needed.

7.4.3. RFC 1735 NBMA Address Resolution Protocol (NARP)

This functionality has been defined in RFC 2491, IPv6 over Non-Broadcast Multiple Access (NBMA) networks and RFC 2332, NBMA Next Hop Resolution Protocol (NHRP).

7.4.4. RFC 1788 ICMP Domain Name Messages

No updated document exists for this specification. However, DNS Dynamic Updates should provide similar functionality, so an update does not seem necessary.

7.4.5. RFC 1868 ARP Extension - UNARP

This mechanism defined a mechanism to purge ARP caches on a link. That functionality already exists in RFC 2461, Neighbor Discovery for IPv6.

7.4.6. RFC 2143 IP Over SCSI

No updated document exists for this specification. It is unclear whether one is needed.

7.4.7. RFC 3180 GLOP Addressing in 233/8

Similar functionality is provided by RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses, and no action is necessary.

8. Security Considerations

This memo examines the IPv6-readiness of specifications; this does not have security considerations in itself.

9. Acknowledgements

The author would like to acknowledge the support of the Internet Society in the research and production of this document. Additionally the author would like to thanks his partner in all ways, Wendy M. Nesser.

The editor, Cleveland Mickles, would like to thank Steve Bellovin and Russ Housley for their comments and Pekka Savola for his comments and guidance during the editing of this document. Additionally, he would like to thank his wife, Lesia, for her patient support.

Pekka Savola helped in editing the latest versions of the document.

10. References

10.1. Normative References

[1] Nesser II, P. and A. Bergstrom, Editor, "Introduction to the Survey of IPv4 Addresses in Currently Deployed IETF Standards", RFC 3789, June 2004.

10.2 Informative References

[2] Loughney, J., Ed., "IPv6 Node Requirements", Work in Progress, January 2004.

[3] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[4] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[5] Vida, R. and L. Costa, Eds., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

11. Authors' Addresses

Cleveland Mickles, Editor
Reston, VA 20191
USA

EMail: cmickles.ee88@gtalumni.org

Philip J. Nesser II
Nesser & Nesser Consulting
13501 100th Ave NE, #5202
Kirkland, WA 98034
USA

EMail: phil@nesser.com

12. Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.