Network Working Group
Request for Comments: 3792
Category: Informational

P. Nesser, II
Nesser & Nesser Consulting
A. Bergstrom, Ed.
Ostfold University College

June 2004

Survey of IPv4 Addresses in Currently Deployed IETF Security 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

Copyright (C) The Internet Society (2004).

Abstract

This document seeks to document all usage of IPv4 addresses in currently deployed IETF Security 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 2
2. Document Organisation. 2
3. Full Standards 2
4. Draft Standards. 2
5. Proposed Standards 8
6. Experimental RFCs. 20
7. Summary of Results 22
   7.1. Standards. 23
   7.2. Draft Standards. 23
   7.3. Proposed Standards 23
   7.4. Experimental RFCs. 23
8. Security Considerations. 24
9. Acknowledgements 24

10. Normative Reference. 24
11. Authors' Addresses 24
12. Full Copyright Statement 25

1.0. 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, Operations and Management, Routing, Security, Sub-IP, and Transport).

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

2.0. Document Organization

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 its turn starting with RFC 1 and ending with (around) 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 the problems 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.

3.0. 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 2289 A One-Time Password System

There are no IPv4 dependencies in this specification.

4.0. 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 1864 The Content-MD5 Header Field

There are no IPv4 dependencies in this specification.

4.2. RFC 2617 HTTP Authentication: Basic and Digest Access Authentication

Section 3.2.1 The WWW-Authenticate Response Header include he following text:

> (Note: including the IP address of the client in the nonce would appear to offer the server the ability to limit the reuse of the nonce to the same client that originally got it. However, that would break proxy farms, where requests from a single user often go through different proxies in the farm. Also, IP address spoofing is not that hard.)

Section 4.5 Replay Attacks contains the text:

> Thus, for some purposes, it is necessary to protect against replay attacks. A good Digest implementation can do this in various ways. The server created "nonce" value is implementation dependent, but if it contains a digest of the client IP, a time-stamp, the resource ETag, and a private server key (as recommended above) then a replay attack is not simple. An attacker must convince the server that the request is coming from a false IP address and must cause the server to deliver the document to an IP address different from the address to which it believes it is sending the document. An attack can only succeed in the period before the time-stamp expires. Digesting the client IP and time-stamp in the nonce permits an implementation which does not maintain state between transactions.

Both of these statements are IP version independent and must rely on the implementers discretion.

4.3. RFC 2865 Remote Authentication Dial In User Service (RADIUS)

Section 3. Packet Format has the following notes:

Identifier

> The Identifier field is one octet, and aids in matching requests and replies. The RADIUS server can detect a duplicate request if it has the same client source IP address and source UDP port and Identifier within a short span of time.

and

> A RADIUS server MUST use the source IP address of the RADIUS UDP packet to decide which shared secret to use, so that RADIUS requests can be proxied.

This text is version neutral but implementers should allow for the use of both IPv4 and IPv6 addresses.

Section 5. Attributes defines a number of IP specific attributes:

```
 4      NAS-IP-Address
 8      Framed-IP-Address
 9      Framed-IP-Netmask
10      Framed-Routing
14      Login-IP-Host
22      Framed-Route
```

and definitions for the "value" field of the following type:

address 32 bit value, most significant octet first.

The attributes are further defined as follows:

5.4. NAS-IP-Address

Description

This Attribute indicates the identifying IP Address of the NAS which is requesting authentication of the user, and SHOULD be unique to the NAS within the scope of the RADIUS server. NAS-IP-Address is only used in Access-Request packets. Either NAS-IP-Address or NAS-Identifier MUST be present in an Access-Request packet.

Note that NAS-IP-Address MUST NOT be used to select the shared secret used to authenticate the request. The source IP address of the Access-Request packet MUST be used to select the shared secret.

A summary of the NAS-IP-Address Attribute format is shown below. The fields are transmitted from left to right.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         Address (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

4 for NAS-IP-Address.

Length

6

Address

The Address field is four octets.

5.8. Framed-IP-Address

Description

This Attribute indicates the address to be configured for the user. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that address, but the server is not required to honor the hint.

A summary of the Framed-IP-Address Attribute format is shown below. The fields are transmitted from left to right.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         Address (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

8 for Framed-IP-Address.

Length

6

Address

The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS Should allow the user to select an address (e.g., Negotiated). The value 0xFFFFFFFE indicates that the NAS should select an address for the user (e.g., Assigned from a pool of addresses kept by the NAS). Other valid values indicate that the NAS should use that value as the user's IP address.

5.9. Framed-IP-Netmask

Description

This Attribute indicates the IP netmask to be configured for the user when the user is a router to a network. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that netmask, but the server is not required to honor the hint.

A summary of the Framed-IP-Netmask Attribute format is shown below. The fields are transmitted from left to right.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         Address (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

9 for Framed-IP-Netmask.

Length

6

Address

The Address field is four octets specifying the IP netmask of the user.

5.14. Login-IP-Host

Description

"This Attribute indicates the system with which to connect the user, when the Login-Service Attribute is included. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint to the server that the NAS would prefer to use that host, but the server is not required to honor the hint."

A summary of the Login-IP-Host Attribute format is shown below. The fields are transmitted from left to right.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         Address (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

14 for Login-IP-Host.

Length

6

Address

The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS SHOULD allow the user to select an address. The value 0 indicates that the NAS SHOULD select a host to connect the user to. Other values indicate the address the NAS SHOULD connect the user to.

5.22. Framed-Route

Description

This Attribute provides routing information to be configured for the user on the NAS. It is used in the Access-Accept packet and can appear multiple times.

A summary of the Framed-Route Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|     Type      |    Length     |  Text ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Type

22 for Framed-Route.

Length

>= 3

Text

The Text field is one or more octets, and its contents are implementation dependent. It is intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain UTF-8 encoded 10646 [7] characters.

For IP routes, it SHOULD contain a destination prefix in dotted quad form optionally followed by a slash and a decimal length specifier stating how many high order bits of the prefix to use. That is followed by a space, a gateway address in dotted quad form, a space, and one or more metrics separated by spaces. For example, "192.168.1.0/24 192.168.1.1 1 2 -1 3 400". The length specifier may be omitted, in which case it defaults to 8 bits for class A prefixes, 16 bits for class B prefixes, and 24 bits for class C prefixes. For example, "192.168.1.0 192.168.1.1 1".

Whenever the gateway address is specified as "0.0.0.0" the IP address of the user SHOULD be used as the gateway address.

There are also several example authentication sequences that use the attributes discussed above and hence have IPv4 addresses.

Although the definitions in this RFC are limited to IPv4 addresses, the specification is easily extensible for new attribute types. It is therefore relatively simple to create new IPv6 specific attributes.

5.0. 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.

5.001. RFC 1413 Identification Protocol

There are no IPv4 dependencies in this specification.

5.002. RFC 1421 Privacy Enhancement for Internet Electronic Mail: Part I

There are no IPv4 dependencies in this specification.

5.003. RFC 1422 Privacy Enhancement for Internet Electronic Mail: Part II

There are no IPv4 dependencies in this specification.

5.004. RFC 1423 Privacy Enhancement for Internet Electronic Mail: Part III

There are no IPv4 dependencies in this specification.

5.005. RFC 1424 Privacy Enhancement for Internet Electronic Mail: Part IV

There are no IPv4 dependencies in this specification.

5.006. RFC 1510 The Kerberos Network Authentication Service (V5)

Although this specification specifies optional use of host addresses, there are no specific requirements that the addresses be IPv4. The specification has no IPv4 dependencies, but implementations might have issues.

5.007. RFC 1731 IMAP4 Authentication Mechanisms

There are no IPv4 dependencies in this specification.

5.008. RFC 1734 POP3 AUTHentication command

There are no IPv4 dependencies in this specification.

5.009. RFC 1828 IP Authentication using Keyed MD5

There are no IPv4 dependencies in this specification. The operations described operate on the entire IP packet without specifying that the IP packet be IPv4 or IPv6.

5.010. RFC 1829 The ESP DES-CBC Transform

There are no IPv4 dependencies in this specification. The operations described operate on the entire IP packet without specifying that the IP packet be IPv4 or IPv6.

5.011. RFC 1847 Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted

There are no IPv4 dependencies in this specification.

5.012. RFC 1848 MIME Object Security Services

There are no IPv4 dependencies in this specification.

5.013. RFC 1928 SOCKS Protocol Version

This specification is IPv6 aware and will function normally on either IPv4 and IPv6.

5.014. RFC 1929 Username/Password Authentication for SOCKS V5

There are no IPv4 dependencies in this specification.

5.015. RFC 1961 GSS-API Authentication Method for SOCKS Version 5

There are no IPv4 dependencies in this specification.

5.016. RFC 1964 The Kerberos Version 5 GSS-API Mechanism

There are no IPv4 dependencies in this specification.

5.017. RFC 1968 The PPP Encryption Control Protocol (ECP)

There are no IPv4 dependencies in this specification.

5.018. RFC 2015 MIME Security with Pretty Good Privacy (PGP)

There are no IPv4 dependencies in this specification.

5.019. RFC 2025 The Simple Public-Key GSS-API Mechanism (SPKM)

There are no IPv4 dependencies in this specification.

5.020. RFC 2082 RIP-2 MD5 Authentication

This RFC documents a security mechanism for an IPv4 only routing specification. It is expected that a similar (or better) mechanism will be developed for RIPng.

5.021. RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention

This document defines an IP version independent specification and has no IPv4 dependencies.

5.022. RFC 2195 IMAP/POP AUTHorize Extension for Simple Challenge/ Response

There are no IPv4 dependencies in this specification.

5.023. RFC 2203 RPCSEC_GSS Protocol Specification

There are no IPv4 dependencies in this specification.

5.024. RFC 2222 Simple Authentication and Security Layer (SASL)

There are no IPv4 dependencies in this specification.

5.025. RFC 2228 FTP Security Extensions

There are no IPv4 dependencies in this specification.

5.026. RFC 2243 OTP Extended Responses

There are no IPv4 dependencies in this specification.

5.027. RFC 2245 Anonymous SASL Mechanism

There are no IPv4 dependencies in this specification.

5.028. RFC 2246 The TLS Protocol Version 1.0

There are no IPv4 dependencies in this specification.

5.029. RFC 2284 PPP Extensible Authentication Protocol (EAP)

There are no IPv4 dependencies in this specification.

5.030. RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option

Although the specification enhancements have no IPv4 dependencies, it is an update to an IPv4 only routing specification.

5.031. RFC 2401 Security Architecture for the Internet Protocol

This specification is both IPv4 and IPv6 aware.

5.032. RFC 2402 IP Authentication Header

This specification is both IPv4 and IPv6 aware.

5.033. RFC 2403 The Use of HMAC-MD5-96 within ESP and AH

There are no IPv4 dependencies in this specification.

5.034. RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH

There are no IPv4 dependencies in this specification.

5.035. RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV

There are no IPv4 dependencies in this specification.

5.036. RFC 2406 IP Encapsulating Security Payload (ESP)

This specification is both IPv4 and IPv6 aware.

5.037. RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP

This specification is both IPv4 and IPv6 aware.

5.038. RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)

This specification is both IPv4 and IPv6 aware.

5.039. RFC 2409 The Internet Key Exchange (IKE)

There are no IPv4 dependencies in this specification.

5.040. RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec

There are no IPv4 dependencies in this specification.

5.041. RFC 2419 The PPP DES Encryption Protocol, Version 2 (DESE-bis)

There are no IPv4 dependencies in this specification.

5.042. RFC 2420 The PPP Triple-DES Encryption Protocol (3DESE)

There are no IPv4 dependencies in this specification.

5.043. RFC 2440 OpenPGP Message Format

There are no IPv4 dependencies in this specification.

5.044. RFC 2444 The One-Time-Password SASL Mechanism

There are no IPv4 dependencies in this specification.

5.045. RFC 2451 The ESP CBC-Mode Cipher Algorithms

There are no IPv4 dependencies in this specification.

5.046. RFC 2478 The Simple and Protected GSS-API Negotiation Mechanism

There are no IPv4 dependencies in this specification.

5.047. RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols

There are no IPv4 dependencies in this specification.

5.048. RFC 2511 Internet X.509 Certificate Request Message Format

There are no IPv4 dependencies in this specification.

5.049. RFC 2535 Domain Name System Security Extensions

There are no IPv4 dependencies in this specification. There are discussions of A and AAAA records in the document, but have no real implications on IPv4 dependency or on any IP related address records.

5.050. RFC 2536 DSA KEYs and SIGs in the Domain Name System (DNS)

There are no IPv4 dependencies in this specification.

5.051. RFC 2538 Storing Certificates in the Domain Name System (DNS)

Section 3.1 X.509 CERT RR Names

Some X.509 versions permit multiple names to be associated with subjects and issuers under "Subject Alternate Name" and "Issuer Alternate Name". For example, x.509v3 has such Alternate Names with an ASN.1 specification as follows:

```
GeneralName ::= CHOICE {
   otherName                   [0] INSTANCE OF OTHER-NAME,
   rfc822Name                  [1] IA5String,
   dNSName                     [2] IA5String,
   x400Address                 [3] EXPLICIT OR-ADDRESS.&Type,
   directoryName               [4] EXPLICIT Name,
   ediPartyName                [5] EDIPartyName,
   uniformResourceIdentifier   [6] IA5String,
   iPAddress                   [7] OCTET STRING,
   registeredID                [8] OBJECT IDENTIFIER
}
```

uses a potential IPv4 only address. It goes on with the following example:

> Example 2: Assume that an X.509v3 certificate is issued to /CN=James Hacker/L=Basingstoke/O=Widget Inc/C=GB/ with Subject Alternate names of (a) domain name widget.foo.example, (b) IPv4 address 10.251.13.201, and (c) string "James Hacker <hacker@mail.widget.foo.example>". Then the storage locations recommended, in priority order, would be
> (1) widget.foo.example,
> (2) 201.13.251.10.in-addr.arpa, and
> (3) hacker.mail.widget.foo.example.

Since the definition of X.509v3 certificates is not discussed in this document it is unclear if IPv6 addresses are also supported in the above mentioned field. The document does however refer to RFC 2459 for the definition of a certificate, and RFC 2459 is IPv6 and IPv4 aware -- so it seems this specification is IPv4 and IPv6 aware.

5.052. RFC 2539 Storage of Diffie-Hellman Keys in the Domain Name System (DNS)

There are no IPv4 dependencies in this specification.

5.053. RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Specification - OCSP

There are no IPv4 dependencies in this specification.

5.054. RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP

There are no IPv4 dependencies in this specification.

5.055. RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema

There are no IPv4 dependencies in this specification.

5.056. RFC 2623 NFS Version 2 and Version 3 Security Issues and the NFS Protocol’s Use of RPCSEC_GSS and Kerberos V5

There are no IPv4 dependencies in this specification.

5.057. RFC 2631 Diffie-Hellman Key Agreement Method

There are no IPv4 dependencies in this specification.

5.058. RFC 2632 S/MIME Version 3 Certificate Handling

There are no IPv4 dependencies in this specification.

5.059. RFC 2633 S/MIME Version 3 Message Specification

There are no IPv4 dependencies in this specification.

5.060. RFC 2634 Enhanced Security Services for S/MIME

There are no IPv4 dependencies in this specification.

5.061. RFC 2712 Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)

There are no IPv4 dependencies in this specification.

5.062. RFC 2743 Generic Security Service Application Program Interface Version 2 Update 1

There are no IPv4 dependencies in this specification.

5.063. RFC 2744 Generic Security Service API Version 2: C-bindings

There are no IPv4 dependencies in this specification.

5.064. RFC 2747 RSVP Cryptographic Authentication

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

5.065. RFC 2797 Certificate Management Messages over CMS

There are no IPv4 dependencies in this specification.

5.066. RFC 2817 Upgrading to TLS Within HTTP/1.1

There are no IPv4 dependencies in this specification.

5.067. RFC 2829 Authentication Methods for LDAP

There are no IPv4 dependencies in this specification.

5.068. RFC 2830 Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security (LDAP)

There are no IPv4 dependencies in this specification.

5.069. RFC 2831 Using Digest Authentication as a SASL Mechanism

There are no IPv4 dependencies in this specification.

5.070. RFC 2845 Secret Key Transaction Authentication for DNS (TSIG)

There are no IPv4 dependencies in this specification.

5.071. RFC 2847 LIPKEY - A Low Infrastructure Public Key Mechanism Using SPKM

There are no IPv4 dependencies in this specification.

5.072. RFC 2853 Generic Security Service API Version 2 : Java Bindings

The document uses the InetAddress variable which does not necessarily limit it to IPv4 addresses so there are no IPv4 dependencies in this specification.

5.073. RFC 2857 The Use of HMAC-RIPEMD-160-96 within ESP and AH

There are no IPv4 dependencies in this specification.

5.074. RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms

There are no IPv4 dependencies in this specification.

5.075. RFC 2930 Secret Key Establishment for DNS (TKEY RR)

There are no IPv4 dependencies in this specification.

5.076. RFC 2931 DNS Request and Transaction Signatures (SIG(0)s)

There are no IPv4 dependencies in this specification.

5.077. RFC 2935 Internet Open Trading Protocol (IOTP) HTTP Supplement

There are no IPv4 dependencies in this specification.

5.078. RFC 2941 Telnet Authentication Option

There are no IPv4 dependencies in this specification.

5.079. RFC 2942 Telnet Authentication: Kerberos Version 5

There are no IPv4 dependencies in this specification.

5.080. RFC 2943 TELNET Authentication Using DSA

There are no IPv4 dependencies in this specification.

5.081. RFC 2944 Telnet Authentication: SRP

There are no IPv4 dependencies in this specification.

5.082. RFC 2945 The SRP Authentication and Key Exchange System

There are no IPv4 dependencies in this specification.

5.083. RFC 2946 Telnet Data Encryption Option

There are no IPv4 dependencies in this specification.

5.084. RFC 2947 Telnet Encryption: DES3 64 bit Cipher Feedback

There are no IPv4 dependencies in this specification.

5.085. RFC 2948 Telnet Encryption: DES3 64 bit Output Feedback

There are no IPv4 dependencies in this specification.

5.086. RFC 2949 Telnet Encryption: CAST-128 64 bit Output Feedback

There are no IPv4 dependencies in this specification.

5.087. RFC 2950 Telnet Encryption: CAST-128 64 bit Cipher Feedback

There are no IPv4 dependencies in this specification.

5.088. RFC 2984 Use of the CAST-128 Encryption Algorithm in CMS

There are no IPv4 dependencies in this specification.

5.089. RFC 3007 Secure Domain Name System (DNS) Dynamic Update

There are no IPv4 dependencies in this specification.

5.090. RFC 3008 Domain Name System Security (DNSSEC) Signing Authority

There are no IPv4 dependencies in this specification.

5.091. RFC 3012 Mobile IPv4 Challenge/Response Extensions

This document is specifically designed for IPv4.

5.092. RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile

There are no IPv4 dependencies in this specification.

5.093. RFC 3041 Privacy Extensions for Stateless Address Autoconfiguration in IPv6

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

5.094. RFC 3062 LDAP Password Modify Extended Operation

There are no IPv4 dependencies in this specification.

5.095. RFC 3090 DNS Security Extension Clarification on Zone Status

There are no IPv4 dependencies in this specification.

5.096. RFC 3097 RSVP Cryptographic Authentication -- Updated Message Type Value

There are no IPv4 dependencies in this specification.

5.097. RFC 3110 RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)

There are no IPv4 dependencies in this specification.

5.098. RFC 3118 Authentication for DHCP Messages

This document is only designated for IPv4. It is expected that similar functionality is available in DHCPv6.

5.099. RFC 3207 SMTP Service Extension for Secure SMTP over Transport Layer Security

There are no IPv4 dependencies in this specification.

5.100. RFC 3275 (Extensible Markup Language) XML-Signature Syntax and Processing

There are no IPv4 dependencies in this specification.

5.101. RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

This specification is IPv4 and IPv6 aware.

5.102. RFC 3369 Cryptographic Message Syntax (CMS)

There are no IPv4 dependencies in this specification.

6.0. Experimental RFCs

Experimental RFCs typically define protocols that do not have widescale 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.

6.01. RFC 1004 Distributed-protocol authentication scheme

There are no IPv4 dependencies in this specification.

6.02. RFC 1411 Telnet Authentication: Kerberos Version 4

There are no IPv4 dependencies in this specification.

6.03. RFC 1412 Telnet Authentication: SPX

There are no IPv4 dependencies in this specification.

6.04. RFC 1507 DASS - Distributed Authentication Security Service

There are no IPv4 dependencies in this specification.

6.05. RFC 1851 The ESP Triple DES Transform

There are no IPv4 dependencies in this specification.

6.06. RFC 1949 Scalable Multicast Key Distribution (SMKD)

This specification assumes the use of IGMP and is therefore limited to IPv4 multicast. It is assumed that a similar mechanism may be defined for IPv6 multicasting.

6.07. RFC 2093 Group Key Management Protocol (GKMP) Specification

There are no IPv4 dependencies in this specification.

6.08. RFC 2094 Group Key Management Protocol (GKMP) Architecture

There are no IPv4 dependencies in this specification.

6.09. RFC 2154 OSPF with Digital Signatures

This OSPF option is IPv4 limited. See the following packet format:

7.2. Router Public Key Certificate

A router public key certificate is a package of data signed by a Trusted Entity. This certificate is included in the router PKLSA and in the router configuration information. To change any of the values in the certificate, a new certificate must be obtained from a TE.

```
                     1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 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
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|                          Router Id                            |
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|     TE Id     |   TE Key Id   |   Rtr Key Id  |    Sig Alg    |
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|                          Create Time                          |
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|        Key Field Length       |  Router Role  |  #Net Ranges  |
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|                          IP Address                           |
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|                         Address Mask                          |
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|           IP Address/Address Mask for each Net Range ...      /
| ...                                                           /
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|                       Router Public Key                       |
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
|                         Certification                         /
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
```

#NET RANGES The number of network ranges that follow. A network range is defined to be an IP Address and an Address Mask. This list of ranges defines the addresses that the Router is permitted to advertise in its Router Links LSA. Valid values are 0-255. If there are 0 ranges the router cannot advertise anything. This is not generally useful. One range with address=0 and mask=0 will allow a router to advertise any address.

IP ADDRESS & ADDRESS MASK Define a range of addresses that this router may advertise. Each is a 32 bit value. One range with address=0 and mask=0 will allow a router to advertise any address.

6.10. RFC 2522 Photuris: Session-Key Management Protocol

There are no IPv4 dependencies in this specification.

6.11. RFC 2523 Photuris: Extended Schemes and Attributes

There are no IPv4 dependencies in this specification.

6.12. RFC 2659 Security Extensions For HTML

There are no IPv4 dependencies in this specification.

6.13. RFC 2660 The Secure HyperText Transfer Protocol

There are no IPv4 dependencies in this specification.

6.14. RFC 2692 SPKI Requirements

There are no IPv4 dependencies in this specification.

6.15. RFC 2693 SPKI Certificate Theory

There are no IPv4 dependencies in this specification.

6.16. RFC 2716 PPP EAP TLS Authentication Protocol

There are no IPv4 dependencies in this specification.

6.17. RFC 2773 Encryption using KEA and SKIPJACK

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

6.18. RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols

There are no IPv4 dependencies in this specification.

7.0. Summary of Results

In the initial survey of RFCs 4 positives were identified out of a total of 124, broken down as follows:

Standards:	0 out of 1 or 0.00%
Draft Standards:	1 out of 3 or 33.33%
Proposed Standards:	1 out of 102 or 0.98%
Experimental RFCs:	2 out of 18 or 11.11%

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. The remaining instances are documented below.

7.1. Standards

7.2. Draft Standards

7.2.1. RADIUS (RFC 2865)

The problems have been resolved in RFC 3162, RADIUS and IPv6.

7.3. Proposed Standards

7.3.1. RIPv2 MD5 Authentication (RFC 2082)

This functionality has been assumed by the use of the IPsec AH header as defined in RFC 2402, IP Authentication Header.

7.3.2. Mobile IPv4 Challenge Response Extension (RFC 3012)

The problems are not being addressed and similar functions may be needed in Mobile IPv6.

7.3.3. Authentication for DHCP Messages (RFC 3118)

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

7.4. Experimental RFCs

7.4.1. Scalable Multicast Key Distribution (RFC 1949)

This specification relies on IPv4 IGMP Multicast and a new specification may be produced; however, the SMKD is not believed to be in use.

7.4.2. OPSF with Digital Signatures (RFC 2154)

This specification is IPv4-only, and relies on an IPv4-only routing protocol, OSPFv2. Due to increased focus on routing security, this specification may need to be revisited, and in that case it should support both OSPFv2 and OPSFv3.

8.0. Security Considerations

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

9.0. Acknowledgements

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

The editor, Andreas Bergstrom, would like to thank Pekka Savola for guidance and collection of comments for the editing of this document.

10.0. Normative Reference

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

11.0. Authors' Addresses

Please contact the author with any questions, comments or suggestions at:

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

Phone: +1 425 481 4303
Fax: +1 425 48
EMail: phil@nesser.com

Andreas Bergstrom (Editor)
Ostfold University College
Rute 503 Buer
N-1766 Halden
Norway

EMail: andreas.bergstrom@hiof.no

12.0. Full Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

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