Network Working Group
Request for Comments: 1637
Obsoletes: 1348
Category: Experimental
B. Manning
Rice University
R. Colella
NIST
June 1994

DNS NSAP Resource Records

Status of this Memo

This memo defines an Experimental Protocol for the Internet community. This memo does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Abstract

The Internet is moving towards the deployment of an OSI lower layers infrastructure. This infrastructure comprises the connectionless network protocol (CLNP) and supporting routing protocols. Also required as part of this infrastructure is support in the Domain Name System (DNS) for mapping between names and NSAP addresses.

This document defines the format of one new Resource Record (RR) for the DNS for domain name-to-NSAP mapping. The RR may be used with any NSAP address format. This document supercedes RFC 1348.

NSAP-to-name translation is accomplished through use of the PTR RR (see STD 13, RFC 1035 for a description of the PTR RR). This paper describes how PTR RRs are used to support this translation.

1. Introduction

The Internet is moving towards the deployment of an OSI lower layers infrastructure. This infrastructure comprises the connectionless network protocol (CLNP) [6] and supporting routing protocols. Also required as part of this infrastructure is support in the Domain Name System (DNS) [8] [9] for mapping between domain names and OSI Network Service Access Point (NSAP) addresses [7] [Note: NSAP and NSAP address are used interchangeably throughout this memo].

This document defines the format of one new Resource Record (RR) for the DNS for domain name-to-NSAP mapping. The RR may be used with any NSAP address format.

NSAP-to-name translation is accomplished through use of the PTR RR (see RFC 1035 for a description of the PTR RR). This paper describes how PTR RRs are used to support this translation.

This memo assumes that the reader is familiar with the DNS. Some familiarity with NSAPs is useful; see [2] or [7] for additional information.

2. Background

The reason for defining DNS mappings for NSAPs is to support CLNP in the Internet. Debugging with CLNP ping and traceroute is becoming more difficult with only numeric NSAPs as the scale of deployment increases. Current debugging is supported by maintaining and exchanging a configuration file with name/NSAP mappings similar in function to hosts.txt. This suffers from the lack of a central coordinator for this file and also from the perspective of scaling. The former is the most serious short-term problem. Scaling of a hosts.txt-like solution has well-known long-term scaling difficiencies.

A second reason for this work is the proposal to use CLNP as an alternative to IP: "TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing" [1]. For this to be practical, the DNS must be capable of supporting CLNP addresses.

3. Scope

The methods defined in this paper are applicable to all NSAP formats. This includes support for the notion of a custom-defined NSAP format based on an AFI obtained by the IAB for use in the Internet.

As a point of reference, there is a distinction between registration and publication of addresses. For IP addresses, the IANA is the root registration authority and the DNS a publication method. For NSAPs, addendum two of the network service definition, ISO8348/Ad2 [7] is the root registration authority and this memo defines how the DNS is used as a publication method.

4. Structure of NSAPs

NSAPs are hierarchically structured to allow distributed administration and efficient routing. Distributed administration permits subdelegated addressing authorities to, as allowed by the delegator, further structure the portion of the NSAP space under their delegated control. Accomodating this distributed authority requires that there be little or no a priori knowledge of the structure of NSAPs built into DNS resolvers and servers.

For the purposes of this memo, NSAPs can be thought of as a tree of identifiers. The root of the tree is ISO8348/Ad2 [7], and has as its immediately registered subordinates the one-octet Authority and Format Identifiers (AFIs) defined there. The size of subsequently-defined fields depends on which branch of the tree is taken. The depth of the tree varies according to the authority responsible for defining subsequent fields.

An example is the authority under which U.S. GOSIP defines NSAPs [3]. Under the AFI of 47, NIST (National Institute of Standards and Technology) obtained a value of 0005 (the AFI of 47 defines the next field as being two octets consisting of four BCD digits from the International Code Designator space [4]). NIST defined the subsequent fields in [3], as shown in Figure 1. The field immediately following 0005 is a format identifier for the rest of the U.S. GOSIP NSAP structure, with a hex value of 80. Following this is the three-octet field, values for which are allocated to network operators; the registration authority for this field is delegated to GSA (General Services Administration).

The last octet of the NSAP is the NSelector (NSel). In practice, the NSAP minus the NSel identifies the CLNP protocol machine on a given system, and the NSel identifies the CLNP user. Since there can be more than one CLNP user (meaning multiple NSel values for a given "base" NSAP), the representation of the NSAP should be CLNP-user independent. To achieve this, an NSel value of zero shall be used with all NSAP values stored in the DNS. An NSAP with NSel=0 identifies the network layer itself. It is left to the application retrieving the NSAP to determine the appropriate value to use in that instance of communication.

```
               |--------------|
               | <-- IDP -->  |
               |--------------|-------------------------------------|
               | AFI |  IDI   |            <-- DSP -->              |
               |-----|--------|-------------------------------------|
               | 47  |  0005  | DFI | AA |Rsvd | RD |Area | ID |Sel |
               |-----|--------|-----|----|-----|----|-----|----|----|
        octets |  1  |   2    |  1  | 3  |  2  | 2  |  2  | 6  | 1  |
               |-----|--------|-----|----|-----|----|-----|----|----|

                     IDP    Initial Domain Part
                     AFI    Authority and Format Identifier
                     IDI    Initial Domain Identifier
                     DSP    Domain Specific Part
                     DFI    DSP Format Identifier
                     AA     Administrative Authority
                     Rsvd   Reserved
                     RD     Routing Domain Identifier
                     Area   Area Identifier
                     ID     System Identifier
                     SEL    NSAP Selector

                  Figure 1: GOSIP Version 2 NSAP structure.
```

When CLNP is used to support TCP and UDP services, the NSel value used is the appropriate IP PROTO value as registered with the IANA. For "standard" OSI, the selection of NSel values is left as a matter of local administration. Administrators of systems that support the OSI transport protocol [5] in addition to TCP/UDP must select NSels for use by OSI Transport that do not conflict with the IP PROTO values.

In the NSAP RRs in Master Files and in the printed text in this memo, NSAPs are often represented as a string of "."-separated hex values. The values correspond to convenient divisions of the NSAP to make it more readable. For example, the "."-separated fields might correspond to the NSAP fields as defined by the appropriate authority (ISOC, RARE, U.S. GOSIP, ANSI, etc.). The use of this notation is strictly for readability. The "."s do not appear in DNS packets and DNS servers can ignore them when reading Master Files. For example, a printable representation of the first four fields of a U.S. GOSIP NSAP might look like

```
                        47.0005.80.005a00
```

and a full U.S. GOSIP NSAP might appear as

47.0005.80.005a00.0000.1000.0020.00800a123456.00.

Other NSAP formats have different lengths and different administratively defined field widths to accomodate different requirements. For more information on NSAP formats in use see RFC 1629 [2].

5. The NSAP RR

The NSAP RR is defined with mnemonic "NSAP" and TYPE code 22 (decimal) and is used to map from domain names to NSAPs. Name-to-NSAP mapping in the DNS using the NSAP RR operates analogously to IP address lookup. A query is generated by the resolver requesting an NSAP RR for a provided domain name.

NSAP RRs conform to the top level RR format and semantics as defined in Section 3.2.1 of RFC 1035.

```
                                    1  1  1  1  1  1
      0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                                               |
    /                                               /
    /                      NAME                     /
    |                                               |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                  TYPE = NSAP                  |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                  CLASS = IN                   |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                      TTL                      |
    |                                               |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                   RDLENGTH                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    /                     RDATA                     /
    /                                               /
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

where:

* NAME: an owner name, i.e., the name of the node to which this resource record pertains.

* TYPE: two octets containing the NSAP RR TYPE code of 22 (decimal).

* CLASS: two octets containing the RR IN CLASS code of 1.

* TTL: a 32 bit signed integer that specifies the time interval in seconds that the resource record may be cached before the source of the information should again be consulted. Zero values are interpreted to mean that the RR can only be used for the transaction in progress, and should not be cached. For example, SOA records are always distributed with a zero TTL to prohibit caching. Zero values can also be used for extremely volatile data.

* RDLENGTH: an unsigned 16 bit integer that specifies the length in octets of the RDATA field.

* RDATA: a variable length string of octets containing the NSAP. The value is the binary encoding of the NSAP as it would appear in the CLNP source or destination address field. A typical example of such an NSAP (in hex) is shown below. For this NSAP, RDLENGTH is 20 (decimal); "."s have been omitted to emphasize that they don't appear in the DNS packets.

```
39840f80005a0000000001e13708002010726e00
```

5.1 Additional Section Processing

[The specification in this section is necessary for completeness in describing name server support for TUBA. For the time being, name servers participating in TUBA demonstrations MAY ELECT to implement this behavior; it SHOULD NOT be the default behavior of name servers because the IPng sweepstakes are still outstanding and further consideration is required for truncation and other issues.]

RFC 1035 describes the additional section processing (ASP) required when servers encounter NS records during query processing. From Section 3.3.11, "NS RDATA format":

> NS records cause both the usual additional section processing to locate a type A record, and, when used in a referral, a special search of the zone in which they reside for glue information.

For TUBA, identical ASP is required on type NSAP records to support servers and resolvers that use CLNP, either because of preference or because it is the only internetworking protocol available (i.e., in the absense of IPv4). Thus, NS records cause ASP which locates a type NSAP record in addition to a type A record. Both type A and NSAP records should be returned, if available.

6. NSAP-to-name Mapping Using the PTR RR

The PTR RR is defined in RFC 1035. This RR is typically used under the "IN-ADDR.ARPA" domain to map from IPv4 addresses to domain names.

Similarly, the PTR RR is used to map from NSAPs to domain names under the "NSAP.INT" domain. A domain name is generated from the NSAP according to the rules described below. A query is sent by the resolver requesting a PTR RR for the provided domain name.

A domain name is generated from an NSAP by reversing the hex nibbles of the NSAP, treating each nibble as a separate subdomain, and appending the top-level subdomain name "NSAP.INT" to it. For example, the domain name used in the reverse lookup for the NSAP

```
47.0005.80.005a00.0000.0001.e133.ffffff000162.00
```

would appear as

```
0.0.2.6.1.0.0.0.f.f.f.f.f.f.3.3.1.e.1.0.0.0.0.0.0.0.0.0.a.5.0.0. \
                    0.8.5.0.0.0.7.4.NSAP.INT.
```

[Implementation note: For sanity's sake user interfaces should be designed to allow users to enter NSAPs using their natural order, i.e., as they are typically written on paper. Also, arbitrary "."s should be allowed (and ignored) on input.]

7. Master File Format

The format of NSAP RRs (and NSAP-related PTR RRs) in Master Files conforms to Section 5, "Master Files," of RFC 1035. Below are examples of the use of these RRs in Master Files to support name-to-NSAP and NSAP-to-name mapping.

The NSAP RR introduces a new hex string format for the RDATA field. The format is "0x" (i.e., a zero followed by an 'x' character) followed by a variable length string of hex characters (0 to 9, a to f). The hex string is case-insensitive. "."s (i.e., periods) may be inserted in the hex string anywhere after the "0x" for readability. The "."s have no significance other than for readability and are not propagated in the protocol (e.g., queries or zone transfers).

```
;;;;;;
;;;;;; Master File for domain nsap.nist.gov.
;;;;;;


@       IN      SOA     emu.ncsl.nist.gov.  root.emu.ncsl.nist.gov. (
                                     1994041800   ; Serial  - date
                                     1800         ; Refresh - 30 minutes
                                     300          ; Retry   - 5 minutes
                                     604800       ; Expire  - 7 days
                                     3600 )       ; Minimum - 1 hour
        IN      NS      emu.ncsl.nist.gov.
        IN      NS      tuba.nsap.lanl.gov.
;
;
$ORIGIN nsap.nist.gov.
;
;     hosts
;
bsdi1    IN   NSAP  0x47.0005.80.005a00.0000.0001.e133.ffffff000161.00
         IN   A      129.6.224.161
         IN   HINFO PC_486    BSDi1.1(TUBA)
;
bsdi2    IN   NSAP  0x47.0005.80.005a00.0000.0001.e133.ffffff000162.00
         IN   A      129.6.224.162
         IN   HINFO PC_486    BSDi1.1(TUBA)
;
cursive  IN   NSAP  0x47.0005.80.005a00.0000.0001.e133.ffffff000171.00
         IN   A      129.6.224.171
         IN   HINFO PC_386    DOS_5.0/NCSA_Telnet(TUBA)
;
infidel  IN   NSAP  0x47.0005.80.005a00.0000.0001.e133.ffffff000164.00
         IN   A      129.6.55.164
         IN   HINFO PC/486    BSDi1.0(TUBA)
;
;     routers
;
cisco1   IN   NSAP  0x47.0005.80.005a00.0000.0001.e133.aaaaaa000151.00
         IN   A      129.6.224.151
         IN   A      129.6.225.151
         IN   A      129.6.229.151
;
3com1    IN   NSAP  0x47.0005.80.005a00.0000.0001.e133.aaaaaa000111.00
         IN   A      129.6.224.111
         IN   A      129.6.225.111
         IN   A      129.6.228.111
```

```
;;;;;;
;;;;;; Master File for reverse mapping of NSAPs under the
;;;;;;     NSAP prefix:
;;;;;;
;;;;;;          47.0005.80.005a00.0000.0001.e133
;;;;;;


@      IN      SOA    emu.ncsl.nist.gov.  root.emu.ncsl.nist.gov. (
                                 1994041800   ; Serial  - date
                                 1800         ; Refresh - 30 minutes
                                 300          ; Retry   - 5 minutes
                                 604800       ; Expire  - 7 days
                                 3600 )       ; Minimum - 1 hour
       IN      NS     emu.ncsl.nist.gov.
       IN      NS     tuba.nsap.lanl.gov.
;
;
$ORIGIN 3.3.1.e.1.0.0.0.0.0.0.0.0.0.a.5.0.0.0.8.5.0.0.0.7.4.NSAP.INT.
;
0.0.1.6.1.0.0.0.f.f.f.f.f.f  IN    PTR  bsdi1.nsap.nist.gov.
;
0.0.2.6.1.0.0.0.f.f.f.f.f.f  IN    PTR  bsdi2.nsap.nist.gov.
;
0.0.1.7.1.0.0.0.f.f.f.f.f.f  IN    PTR  cursive.nsap.nist.gov.
;
0.0.4.6.1.0.0.0.f.f.f.f.f.f  IN    PTR  infidel.nsap.nist.gov.
;
0.0.1.5.1.0.0.0.a.a.a.a.a.a  IN    PTR  cisco1.nsap.nist.gov.
;
0.0.1.1.1.0.0.0.a.a.a.a.a.a  IN    PTR  3com1.nsap.nist.gov.
```

8. Security Considerations

Security issues are not discussed in this memo.

9. Authors' Addresses

Bill Manning
Rice University -- ONCS
P.O. Box 1892
6100 South Main
Houston, Texas 77251-1892
USA

Phone: +1.713.285.5415
EMail: bmanning@rice.edu

Richard Colella
National Institute of Standards and Technology
Technology/B217
Gaithersburg, MD 20899
USA

Phone: +1 301-975-3627
Fax: +1 301 590-0932
EMail: colella@nist.gov

10. References

[1] Callon R., "TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing", RFC 1347, DEC, June 1992.

[2] Colella, R., Gardner, E., Callon, R., and Y. Rekhter, "Guidelines for OSI NSAP Allocation inh the Internet", RFC 1629, NIST, Wellfleet, Mitre, T.J. Watson Research Center, IBM Corp., May 1994.

[3] GOSIP Advanced Requirements Group. Government Open Systems Interconnection Profile (GOSIP) Version 2. Federal Information Processing Standard 146-1, U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, April 1991.

[4] ISO/IEC. Data interchange - structures for the identification of organization. International Standard 6523, ISO/IEC JTC 1, Switzerland, 1984.

[5] ISO/IEC. Connection oriented transport protocol specification. International Standard 8073, ISO/IEC JTC 1, Switzerland, 1986.

[6] ISO/IEC. Protocol for Providing the Connectionless-mode Network Service. International Standard 8473, ISO/IEC JTC 1, Switzerland, 1986.

[7] ISO/IEC. Information Processing Systems -- Data Communications -- Network Service Definition Addendum 2: Network Layer Addressing. International Standard 8348/Addendum 2, ISO/IEC JTC 1, Switzerland, 1988.

[8] Mockapetris, P., "Domain Names -- Concepts and Facilities", STD 13, RFC 1034, USC/Information Sciences Institute, November 1987.

[9] Mockapetris, P., "Domain Names -- Implementation and Specification", STD 13, RFC 1035, USC/Information Sciences Institute, November 1987.