Internet Draft
draft-irtf-rrg-ilnp-dns-01.txt
Expires: 26 OCT 2012
Category: Experimental

RJ Atkinson
Consultant
SN Bhatti
U. St Andrews
Scott Rose
US NIST
March 26, 2012

DNS Resource Records for ILNP
draft-irtf-rrg-ilnp-dns-01.txt

STATUS OF THIS MEMO

groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This document is not on the IETF standards-track and does not specify any level of standard. This document merely provides information for the Internet community.

This document is part of the ILNP document set, which has had extensive review within the IRTF Routing Research Group. ILNP is one of the recommendations made by the RG Chairs. Separately, various refereed research papers on ILNP have also been published during this decade. So the ideas contained herein have had much broader review than the IRTF Routing RG. The views in this document were considered controversial by the Routing RG, but the RG reached a consensus that the document still should be published. The Routing RG has had remarkably little consensus on anything, so virtually all Routing RG outputs are considered controversial.

ABSTRACT

This note describes additional optional Resource Records for use with the Domain Name System (DNS). These optional resource records are for use with the Identifier-Locator Network Protocol (ILNP). This document is a product of the IRTF Routing RG.

TABLE OF CONTENTS

1. INTRODUCTION

The Identifier-Locator Network Protocol (ILNP) was developed to explore a possible evolutionary direction for the Internet Architecture. An description of the ILNP architecture is available in a separate document [ILNP-ARCH]. Implementation and engineering details are largely isolated into a second document [ILNP-ENG].

The Domain Name System (DNS) is the standard way that Internet nodes locate information about addresses, mail exchangers, and other data relating to remote Internet nodes [RFC1034] [RFC1035]. More recently, the IETF have defined standards-track security extensions to the DNS. [RFC4033] These security extensions can be used to authenticate signed DNS data records and can also be used to store signed public keys in the DNS. Further, the IETF have defined a standards-track approach to enable secure dynamic update of DNS records over the network [RFC3007].

This document defines several new optional data Resource Records. This note specifies the syntax and other items required for independent implementations of these DNS resource records. The reader is assumed to be familiar with the basics of DNS, including familiarity with [RFC1034] [RFC1035].

The concept of using DNS to support mobile nodes or mobile networks has been proposed earlier, more than once, independently, by several other researchers; for example, please see [SB00] [SBK01] and [PHG02].

1.1 Terminology

In this document, the term "ILNP-enabled" applied to a DNS component (either authoritative server or cache) is used to indicate that the component attempts to include other ILNP RRTypes to the Additional section of a DNS response to increase performance and reduce the number of follow-up queries for other ILNP RRTypes. These other RRsets are added to the Additional section if space permits and only when the QTYPE equals ID, L64, L32, or LP. There is no method for a server to signal that it is ILNP-enabled.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described

in RFC 2119 [RFC2119].

2. NEW RESOURCE RECORDS

This document specifies several new and closely related DNS data Resource Records (RRs). These new RR types have the mnemonics "ID", "L32", "L64", and "LP". These resource record types are associated with a Fully-Qualified Domain Name (FQDN), that is hereafter called the "owner name". These are part of work on the Identifier-Locator Network Protocol (ILNP) [ILNP-ARCH].

2.1 "ID" Resource Record

An ID record has the following logical components:

```
     <owner name>  IN  ID  <preference>   <I>
```

In the above <owner name> is the owner name string, <preference> is an unsigned 16-bit value, while <I> is an unsigned 64-bit value.

The <preference> field indicates the owner name's relative preference for this ID record among other ID records associated with this owner name. Lower preference values are preferred over higher preference values.

The <I> field complies with the syntactic rules of IPv6 Interface Identifiers. Unlike IPv6 Interface Identifiers, which are bound to a specific *interface* of a specific node, <I> values are bound to a specific *node* -- and may be used with *any interface* of that node.

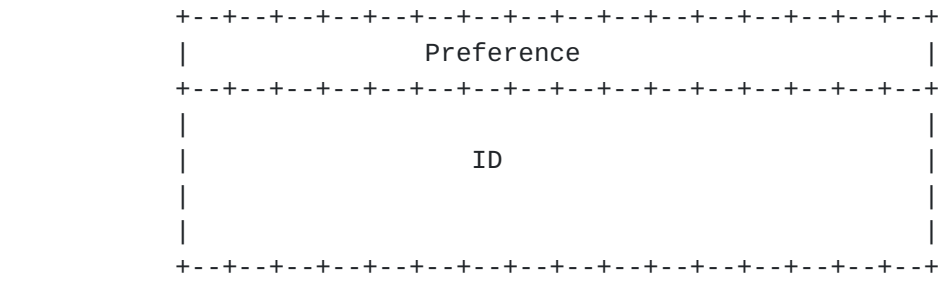
An "ID" record has the DNS TYPE of ID and a numeric value of <to be assigned by IANA>. An ID record is a member of the Internet ("IN") CLASS in the DNS. Each ID record is associated with a owner name entry in the DNS.

ID records are present only for owner name values that are ILNP-capable nodes. This restriction is important; ILNP-capable nodes use the presence of ID records in the DNS to learn that a correspondent node is also ILNP-capable. While erroneous ID records in the DNS for an owner name that is not ILNP-capable would not prevent communication, such erroneous DNS records could increase the delay at the start of an IP communications session.

Of course, a particular node's owner name might have an ID record in the DNS and yet that node might be temporarily disconnected from the Internet.

A given owner name may have zero or more ID records at a given time. In normal operation, nodes that support the Identifier-Locator Network Protocol (ILNP) will have at least one valid ID record.

The ID DNS record has the following RDATA format:



where:

Preference A 16-bit unsigned integer which specifies the preference given to this RR among others at the same owner. Lower Preference values are preferred over higher Preference values.

ID A 64-bit unsigned integer.

ILNP-enabled DNS servers and DNS caches SHOULD attempt to return all L32, L64, and LP records associated with the owner name of the ID RRset in the Additional section of the response if space permits.

2.2 "L32" Resource Record

An "L32" record has the DNS TYPE of "L32" and a numeric value of <to be assigned by IANA>. An L32 record is a member of the Internet ("IN") CLASS in the DNS. Each L32 record is associated with an owner name entry in the DNS. The Preference field indicates the owner name's relative preference for this particular L32 record among other L32 records for the same owner name.

An L32 record has the following logical components:

```
<owner name>  IN  L32  <preference>   <L>
```

In the above, <owner name> is the owner name, <preference> is an unsigned 16-bit value, while <L> is an unsigned 32-bit value that

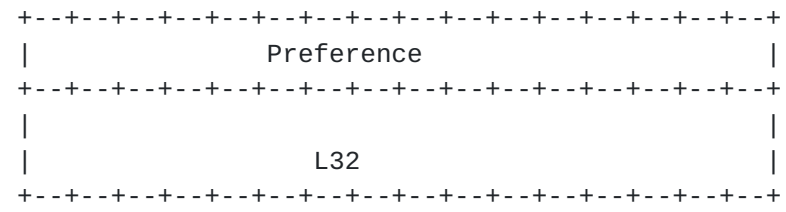
names a subnetwork where the owner is directly attached.

The Preference field indicates the owner name's relative preference for this L32 record among other L32, L64, and LP records associated with this owner name. Lower values are preferred over higher values.

A given owner name might have zero or more L32 values at a given time. An ILNP-capable IPv4 host SHOULD have at least 1 Locator (i.e., L32 or LP) DNS resource record while it is connected to the Internet. An ILNP-capable multi-homed IPv4 host normally will have multiple Locator values while multi-homed. An IPv4 host that is NOT ILNP-capable MUST NOT have an L32 or LP record in its DNS entries. A node that is not currently connected to the Internet might not have any L32 values in the DNS associated with its <owner name>.

A DNS owner name that is naming a subnetwork, rather than naming a host, MAY have an L32 record as a wild-card entry, thereby applying to entries under that DNS owner name. This deployment scenario probably is most common if the named subnetwork is, was, or might become, mobile.

The L32 DNS record has the following RDATA format:



where:

Preference A 16-bit unsigned integer which specifies the preference given to this RR among others at the same owner. Lower Preference values are preferred over higher Preference values.

L32 A 32-bit unsigned integer that names a subnetwork.

ILNP-enabled DNS servers and DNS caches SHOULD attempt to return all ID, L64, and LP records for the same owner name of the L32 RRset in the Additional section of the response if space permits.

2.3 "L64" Resource Record

An "L64" record has the DNS TYPE of "L64" and a numeric value of <to be assigned by IANA>. An L64 record is a member of the Internet ("IN") CLASS in the DNS. Each L64 record is associated with an owner name entry in the DNS.

An L64 record has the following logical components:

```
     <owner name>  IN  L64  <preference>   <L>
```

In the above, <owner name> is the owner name, <preference> is an unsigned 16-bit value, while <L> is an unsigned 64-bit value that names a subnetwork where <owner name> is directly attached.

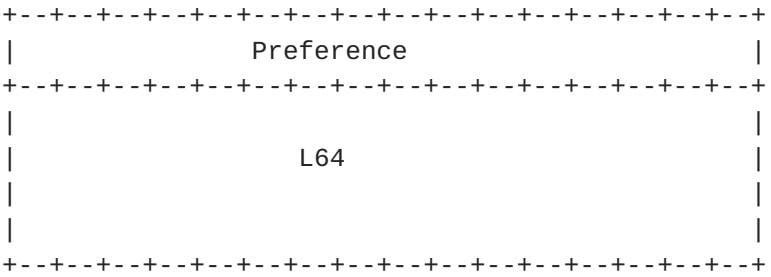
The Preference field indicates the owner name's relative preference for this L64 record among other L32, L64, and LP records associated with this owner name. Lower Preference values are preferred over higher Preference values.

A given owner name may have zero or more L64 values at a given time. An ILNP-capable multi-homed host connected to the Internet will normally have multiple Locator (i.e., L64 or LP) values while multi-homed.

A DNS owner name that is naming a subnetwork, rather than naming a host, MAY have an L64 record as a wild-card entry, thereby applying to all entries under that DNS owner name. This deployment scenario is most common if the named subnetwork is, was, or might become, mobile.

A DNS owner name that names a single node that is NOT ILNP-capable MUST NOT have an L64 record in the DNS. A node that is not currently connected to the Internet commonly might not have any L64 or LP values in the DNS associated with its owner name.

The L64 DNS record has the following RDATA format:



where:

Preference	A 16-bit unsigned integer which specifies the preference given to this RR among others at the same owner. Lower Preference values are preferred over higher Preference values.
L64	A 64-bit unsigned integer that names a subnetwork.

The Preference field indicates the owner name's relative preference for this LP record among other L32, L64, and LP records associated with this owner name. Lower values are preferred over higher values.

ILNP-enabled DNS servers and DNS caches SHOULD attempt to return all ID, L32, and LP RRsets associated with the owner name of the L64 RRset in the Additional section of the response if space permits.

2.4 "LP" Resource Record

As described in [ILNP-ARCH], the LP resource record provides one level of indirection within the DNS in naming a Locator value. This is useful in several deployment scenarios, such as for a multi-homed site where the multi-homing is handled entirely by the site's border routers (e.g. via Locator rewriting) or in some mobile network deployment scenarios [ILNP-ADV].

An "LP" record has the following logical components:

```
     <owner name>  IN  LP  <preference>   <target-name>
```

An LP record has the DNS TYPE of LP and a numeric value of <to be assigned by IANA>. An LP record is a member of the Internet ("IN") CLASS in the DNS. Each LP record is associated with an owner name entry in the DNS, and points to a second Fully-Qualified Domain Name (shown above as <target-name>).

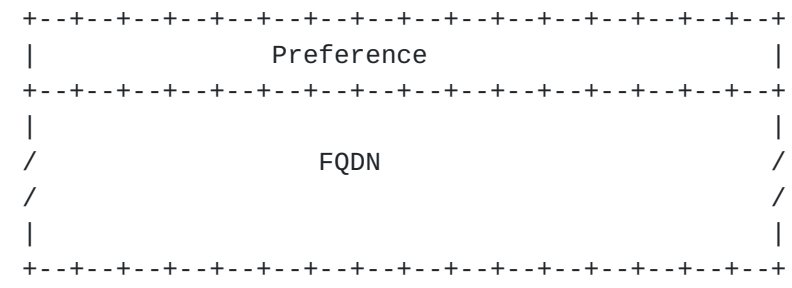
LP records MUST NOT be present for owner name values that are not ILNP-capable nodes. This restriction is important; ILNP-capable nodes use the presence of "LP" records in the DNS to infer that a correspondent node is also ILNP-capable. While erroneous "LP" records in the DNS for an owner name would not prevent communication, presence of such erroneous DNS records could increase the delay at the start of a communications session.

Of course, a particular node might have an LP record in the DNS

and yet temporarily be disconnected from the Internet.

In the above <owner name> is the owner name, while <target-name> is any other valid domain name string. It is invalid to have an LP record with the same value in both the <owner name> and <target-name> values. A given owner name will have zero or more LP records at a given time.

The LP DNS record has the following RDATA format:



where:

Preference A 16-bit unsigned integer which specifies the preference given to this RR among others at the same owner. Lower Preference values are preferred over higher Preference values.

FQDN A Fully-Qualified Domain Name that has one or more L64 records in the DNS. This is referred to as the <target-name> above.

The Preference field indicates the owner name's relative preference for this LP record among other L32, L64, and LP records associated with this owner name. Lower values are preferred.

ILNP-enabled DNS servers and DNS caches SHOULD attempt to return all ID, L32, and L64 RRsets associated with the owner name of the LP RRset in the Additional section of the response if space permits.

3. USAGE EXAMPLE

Given a domain name, one can use the Domain Name System (DNS) to discover the set of ID records, the set of L32 records, the set of L64 records, and the set of LP records that are associated with that owner name.

As these DNS records are only used with the Identifier-Locator Network Protocol (ILNP), these records MUST NOT be present for a node that does not support ILNP. This lookup process is considered to be in the "forward" direction.

The Preference fields associated with the ID, L32, L64, and LP records are used to indicate the owner name's preference for others to use one particular ID, L32, L64, or LP record, rather than use another ID, L32, L64, or LP record also associated with that owner name. Lower Preference field values are preferred over higher Preference field values.

It is possible that a client querying for one of these record types will not receive all ID, L32, L64, and LP RR's in a single response. Credible anecdotal reports indicate at least one DNS recursive cache implementation actively drops all Additional Data records that were not expected by that DNS recursive cache. So even if the authoritative DNS server includes all the relevant records in the Additional Data section of the DNS response, the querying client might not receive all of those Additional Data records. DNS caches also might purge some ILNP RRsets before others, for example if ID RRsets have a longer DNS TTL value than Locator-related (e.g. LP, L32, L64) RRsets. So a client sending queries toa DNS cache cannot be certain if they have obtained all available RRtypes for a given owner name. Therefore, the DNS client SHOULD send follow-up DNS queries for RRTYPE values that were missing and are desired, to ensure that the client receives all the necessary information.

Note that for nodes likely either to be mobile or to be multi-homed, the DNS TTL values for L32 and L64 records normally will be very low, as those values might change frequently. However, the DNS TTL values for ID and LP records normally will be quite long, as those values are not normally impacted by node location changes. Previous trace-driven DNS simulations from MIT [JSBM02] and more recent experimental DNS validation from U. of St Andrews [BA11] both indicate use of very short DNS TTL values is not problematic.

Any ID value associated with a DNS owner name can be used with any or all Locator values associated with that same DNS owner name.

4. SECURITY CONSIDERATIONS

These new DNS resource record types do not create any new vulnerabilities in the Domain Name System.

Existing mechanisms for DNS security can be used unchanged with these record types [RFC4033] [RFC3007]. As of this writing, those mechanisms are believed to be widely implemented in currently available DNS servers.

In situations where authentication of DNS data is a concern, the DNS Security extensions SHOULD be used [RFC4033].

If these DNS records are updated dynamically over the network, then the Secure Dynamic DNS Update [RFC3007] mechanism SHOULD be used to secure such transactions.

5. IANA CONSIDERATIONS

IANA is requested to allocate each of these DNS Resource Records (enumerated above in Section 2) a Data RRTYPE value according to the procedures of Section 3.1 and 3.1.1 on pages 7 through 9 of RFC 6195 [RFC6195].

6. REFERENCES

6.1 Normative References

[RFC1034] P. Mockapetris, "Domain names - Concepts and Facilities", RFC-1034, 1 November 1987

[RFC1035] P. Mockapetris, "Domain names - Implementation and Specification", RFC-1035, 1 November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3007] B. Wellington, "Secure Domain Name System Dynamic Update", RFC 3007, RFC Editor, November 2000.

[RFC3597] A. Gustafsson, "Handling of Unknown DNS Resource Record (RR) Types", RFC 3597, September 2003.

[RFC4033] R. Arends, R. Austein, M. Larson, D. Massey, & S. Rose, "DNS Security Introduction & Requirements", RFC 4033, RFC Editor, March 2005.

[RFC6195] D. Eastlake 3rd, "Domain Name System IANA Considerations", RFC 6195, March 2011.

[ILNP-ARCH] R. Atkinson & S. Bhatti, "ILNP Architecture",

draft-irtf-rrg-ilnp-arch, January 2012.

[ILNP-ADV] R. Atkinson & S. N. Bhatti,
"Optional Advanced Deployment Scenarios for ILNP",
draft-irtf-rrg-ilnp-adv, March 2012

[ILNP-ENG] R. Atkinson & S. Bhatti, "ILNP Engineering and Implementation Considerations",
draft-irtf-rrg-ilnp-eng, March 2012.

6.2 INFORMATIVE REFERENCES

[BA11] S. Bhatti & R. Atkinson,
"Reducing DNS Caching",
Proc. GI2011 - 14th IEEE Global Internet Symposium,
Shanghai, China. 15 Apr 2011.
http://dx.doi.org/10.1109/INFCOMW.2011.5928919

[JSBM02] J. Jung, E. Sit, H. Balakrishnan, and R. Morris,
DNS performance and the effectiveness of caching.
IEEE/ACM Trans. Netw. 10, 5 (October 2002), 589-603.
http://dx.doi.org/10.1109/TNET.2002.803905

[PHG02] Andreas Pappas, Stephen Hailes, Raffaele Giaffreda,
"Mobile Host Location Tracking through DNS",
IEEE London Communications Symposium,
London, England, UK, September 2002.
<http://www.ee.ucl.ac.uk/lcs/papers2002/LCS072.pdf>

[SB00] Alex C. Snoeren and Hari Balakrishnan. 2000.
"An End-To-End Approach To Host Mobility", Proc.
6th Conference on Mobile Computing And Networking
(MobiCom), ACM, Boston, MA, USA, pp. 155-166,
August 2000.

[SBK01] Alex C. Snoeren, Hari Balakrishnan, & M. Frans
Kaashoek, "Reconsidering Internet Mobility",
Proceedings of 8th Workshop on Hot Topics in
Operating Systems (HotOS), IEEE Computer Society,
Washington, DC, USA, May 2001.

ACKNOWLEDGEMENTS

Steve Blake, Stephane Bortzmeyer, Mohamed Boucadair, Noel Chiappa, Wes George, Steve Hailes, Joel Halpern, Mark Handley, Volker Hilt, Paul Jakma, Dae-Young Kim, Tony Li, Yakov Rehkter, Bruce Simpson, Robin Whittle and John Wroclawski (in alphabetical order) provided review and feedback on earlier versions of this

document. Steve Blake provided an especially thorough review of an early version of the entire ILNP document set, which was extremely helpful. We also wish to thank the anonymous reviewers of the various ILNP papers for their feedback.

RFC EDITOR NOTE

This section is to be removed prior to publication.

This document is written in English, not American. So English spelling is used throughout, rather than American spelling. This is consistent with existing practice in several other RFCs, for example RFC-5887.

This document tries to be very careful with history, in the interest of correctly crediting ideas to their earliest identifiable author(s). So in several places the first published RFC about a topic is cited rather than the most recent published RFC about that topic.

Authors' Addresses:

RJ Atkinson
Consultant
San Jose, CA
95125 USA

Email: rja.lists@gmail.com

SN Bhatti
School of Computer Science
University of St Andrews
North Haugh, St Andrews
Fife, Scotland, UK
KY16 9SX

Email: saleem@cs.st-andrews.ac.uk

Scott Rose
US National Institute for Standards & Technology
100 Bureau Drive
Gaithersburg, MD
20899 USA

Email: scottr.nist@gmail.com

[NOTE: Appendix A is to be removed by the
RFC Editor prior to publication.]

Appendix A:

DNS RRTYPE PARAMETER ALLOCATION TEMPLATE

When ready for formal consideration, this template is
to be submitted to IANA for processing by emailing the
template to dns-rrtype-applications@ietf.org.

A. Submission Date: To be determined.

B. Submission Type:
[X] New RRTYPE

C. Contact Information for submitter:
Name: R. Atkinson
Email Address: rja.lists@gmail.com
International telephone number: unlisted
Other contact handles:

D. Motivation for the new RRTYPE application?

Support for an experimental set of IP extensions
that replace the concept of an "IP Address" with
distinct "Locator" and "Identifier" values.

E. Description of the proposed RR type.

Please see draft-rja-ilnp-dns-07.txt for a full
description.

F. What existing RRTYPE or RRTYPEs come closest to filling that
need and why are they unsatisfactory?

The AAAA record combines both Locator and Identifier,
so has significantly different semantics than having
separate L64 and ID record values. The AAAA record also
lacks scalability and flexibility in the context of the
experimental protocol extensions that will use the ID
and L64 records, as any valid ID record value for a node
can be used on the wire with any valid L64 record value
for the same node.

The CNAME record is closest conceptually to an "LP"
record, but a CNAME is a node name referral scheme,

while the LP record is indicating that the given node has the same routing prefix as some other domain name, but does not necessarily have any other values that are the same.

Lastly, the AAA and CNAME RR Types lack a preference field to rank responses. Such preference information is useful with ILNP.

G. What mnemonic is requested for the new RRTYPE (optional)?

As described in this draft, "ID", "L32", "L64", and "LP".

H. Does the requested RRTYPE make use of any existing IANA Registry or require the creation of a new IANA sub-registry in DNS Parameters?

Existing registry of DNS Resource Record (RR) data TYPE values should be used.

I. Does the proposal require/expect any changes in DNS servers/resolvers that prevent the new type from being processed as an unknown RRTYPE (see [RFC3597]) ?

No.

J. Comments:

This document defines "ILNP-enabled" DNS servers or DNS caches as a DNS server (authoritative or recursive) that include other ILNP RRTypes in the Additional section of a DNS response that match a QNAME (if size permits). This is to reduce the number of client follow-up DNS queries and only applies when the QTYPE is either ID, L32, L64, or LP. There is no signalling mechanism for this Additional section processing, and this is believed to be compatible with existing non-ILNP-enabled DNS servers and clients.

No changes are required for existing deployed DNS servers or DNS caches.