draft-ietf-dnsop-inaddr-required-06.txt

INTERNET-DRAFT D. Senie
Category: BCP Amaranth Networks Inc.
Expires in six months February 2005

Encouraging the use of DNS IN-ADDR Mapping

Status of this Memo

Abstract

Mapping of addresses to names has been a feature of DNS. Many sites, implement it, many others don't. Some applications attempt to use it as a part of a security strategy. The goal of this document is to encourage proper deployment of address to name mappings, and provide guidance for their use.

Copyright Notice

1. Introduction

The Domain Name Service has provision for providing mapping of IP addresses to host names. It is common practice to ensure both name to address, and address to name mappings are provided for networks. This practice, while documented, has never been required, though it is generally encouraged. This document both encourages the presence of

these mappings and discourages reliance on such mappings for security checks.

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. Discussion

From the early days of the Domain Name Service [RFC883] a special domain has been set aside for resolving mappings of IP addresses to domain names. This was refined in [RFC1035], describing the .IN-ADDR.ARPA in use today. For the in the IPv6 address space, .IP6.ARPA was added [RFC3152]. This document uses IPv4 CIDR block sizes and allocation strategy where there are differences and uses IPv4 terminology. Aside from these differences, this document can and should be applied to both address spaces.

The assignment of blocks of IP address space was delegated to three regional registries. Guidelines for the registries are specified in [RFC2050], which requires regional registries to maintain IN-ADDR records on the large blocks of space issued to ISPs and others.

ARIN's policy requires ISPs to maintain IN-ADDR for /16 or larger allocations. For smaller allocations, ARIN can provide IN-ADDR for /24 and shorter prefixes. [ARIN]. APNIC provides methods for ISPs to update IN-ADDR, however the present version of its policy document for IPv4 [APNIC] dropped the IN-ADDR requirements that were in draft copies of this document. As of this writing, it appears APNIC has no actual policy on IN-ADDR. RIPE appears to have the strongest policy in this area [RIPE302] indicating Local Internet Registries should provide IN-ADDR services, and delegate those as appropriate when address blocks are delegated.

As we can see, the regional registries have their own policies for recommendations and/or requirements for IN-ADDR maintenance. It should be noted, however, that many address blocks were allocated before the creation of the regional registries, and thus it is unclear whether any of the policies of the registries are binding on those who hold blocks from that era.

Registries allocate address blocks on CIDR [RFC1519] boundaries. Unfortunately the IN-ADDR zones are based on classful allocations. Guidelines [RFC2317] for delegating on non-octet-aligned boundaries exist, but are not always implemented.

3. Examples of impact of missing IN-ADDR

These are some examples of problems that may be introduced by reliance on IN-ADDR.

Some applications use DNS lookups for security checks. To ensure validity of claimed names, some applications will look up IN-ADDR records to get names, and then look up the resultant name to see if it maps back to the address originally known. Failure to resolve matching names is seen as a potential security concern.

Some FTP sites will flat-out reject users, even for anonymous FTP, if the IN-ADDR lookup fails or if the result of the IN-ADDR lookup when itself resolved, does not match. Some Telnet servers also implement this check.

Web sites are in some cases using IN-ADDR checks to verify whether the client is located within a certain geopolitical entity. This approach has been employed for downloads of crypto software, for example, where export of that software is prohibited to some locales. Credit card anti-fraud systems also use these methods for geographic placement purposes.

The popular TCP Wrappers program found on most Unix and Linux systems has options to enforce IN-ADDR checks and to reject any client that does not resolve. This program also has a way to check to see that the name given by a PTR record then resolves back to the same IP address. This method provdes more comfort but no appreciable additional security.

Some anti-spam (anti junk email) systems use IN-ADDR to verify the presence of a PTR record, or validate the PTR value points back to the same address.

Many web servers look up the IN-ADDR of visitors to be used in log analysis. This adds to the server load, but in the case of IN-ADDR unavailability, it can lead to delayed responses for users.

Traceroutes with descriptive IN-ADDR naming proves useful when debugging problems spanning large areas. When this information is missing, the traceroutes take longer, and it takes additional steps to determine that network is the cause of problems.

Wider-scale implementation of IN-ADDR on dialup, wireless access and other such client-oriented portions of the Internet would result in lower latency for queries (due to lack of negative caching), and lower name server load and DNS traffic.

4. Recommendations

4.1 Delegation Recommendations

Regional Registries and any Local Registries to whom they delegate should establish and convey a policy to those to whom they delegate blocks that IN-ADDR mappings are recommended. Policies should recommend those receiving delegations to provide IN-ADDR service and/or delegate to downstream customers.

Network operators should define and implement policies and procedures which delegate IN-ADDR to their clients who wish to run their own IN-ADDR DNS services, and provide IN-ADDR services for those who do not have the resources to do it themselves. Delegation mechanisms should permit the downstream customer to implement and comply with IETF recommendations application of IN-ADDR to CIDR [RFC2317].

All IP address space assigned and in use should be resolved by IN-ADDR records. All PTR records must use canonical names.

All IP addresses in use within a block should have an IN-ADDR mapping. Those addresses not in use, and those that are not valid for use (zeros or ones broadcast addresses within a CIDR block) need not have mappings.

It should be noted that due to CIDR, many addresses that appear to be otherwise valid host addresses may actually be zeroes or ones broadcast addresses. As such, attempting to audit a site's degree of compliance may only be done with knowledge of the internal subnet architecture of the site. It can be assumed, however, any host that originates an IP packet necessarily will have a valid host address, and must therefore have an IN-ADDR mapping.

4.2 Application Recommendations

Applications SHOULD NOT rely on IN-ADDR for proper operation. The use of IN-ADDR, sometimes in conjunction with a lookup of the name resulting from the PTR record provides no real security, can lead to erroneous results and generally just increases load on DNS servers. Further, in cases where address block holders fail to properly configure IN-ADDR, users of those blocks are penalized.

5. Security Considerations

This document has no negative impact on security. While it could be argued that lack of PTR record capabilities provides a degree of anonymity, this is really not valid. Trace routes, whois lookups and other sources will still provide methods for discovering identity.

By recommending applications avoid using IN-ADDR as a security mechanism this document points out that this practice, despite its use by many applications, is an ineffective form of security. Applications should use better mechanisms of authentication.

6. IANA Considerations

There are no IANA considerations for this document.

7. References

7.1 Normative References

[RFC883] P.V. Mockapetris, "Domain names: Implementation specification," RFC883, November 1983.

[RFC1035] P.V. Mockapetris, "Domain Names: Implementation Specification," RFC 1035, November 1987.

[RFC1519] V. Fuller, et. al., "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy," RFC 1519, September 1993.

[RFC2026] S. Bradner, "The Internet Standards Process -- Revision 3", RFC 2026, BCP 9, October 1996.

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

[RFC2050] K. Hubbard, et. al., "Internet Registry IP Allocation Guidelines", RFC2050, BCP 12, Novebmer 1996.

[RFC2317] H. Eidnes, et. al., "Classless IN-ADDR.ARPA delegation," RFC 2317, March 1998.

[RFC3152] R. Bush, "Delegation of IP6.ARPA," RFC 3152, BCP 49, August 2001.

7.2 Informative References

[ARIN] "ISP Guidelines for Requesting Initial IP Address Space," date unknown, <http://www.arin.net/regserv/initial-isp.html>http://www.arin.net/regserv/initial-isp.html

[APNIC] "Policies For IPv4 Address Space Management in the Asia Pacific Region," APNIC-086, 13 January 2003.

[RIPE302] "Policy for Reverse Address Delegation of IPv4 and IPv6

Address Space in the RIPE NCC Service Region", RIPE-302, April 26,

2004.
<http://www.ripe.net//ripe/docs/rev-del.html>http://www.ripe.net//ripe/docs/rev-del.html

8. Acknowledgements

Thanks to Peter Koch and Gary Miller for their input, and to many people who encouraged me to write this document.

9. Author's Address

Daniel Senie
Amaranth Networks Inc.
324 Still River Road
Bolton, MA 01740

Phone: (978) 779-5100

EMail: <mailto:dts@senie.com>dts@senie.com

10. Full Copyright Statement

Intellectual Property

Copies of IPR disclosures made to the IETF Secretariat and any

Acknowledgement

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