Internet Draft
draft-ietf-dnsop-dontpublish-unreachable-03.txt
Valid for six months
Category: Best Current Practice

Philip Hazel
University of Cambridge

February 2002

IP Addresses that should never appear in the public DNS

Status of this Memo

Abstract

This document specifies an Internet Best Current Practice for the Internet Community. It has two themes. Firstly, it reinforces the prohibition in [RFC 1918] about the appearance of private IP addresses in publicly visible DNS records, and extends the discussion to include IPv6 addresses.

Secondly, the document discusses the problems that can be caused by the appearance of public addresses, or indirect references to them, when the service implied by the address or reference is inaccessible from the public Internet.

Specifying a blanket prohibition in the second case is difficult because inaccessibility may arise from many causes, some possibly legitimate. Instead, the document points out some of the problems

that can arise, and suggests that other means of achieving the desired effects should be used wherever possible.

1. Introduction

The increasing use of firewalls, NAT boxes, and similar technology has resulted in the fragmentation of the Internet into regions whose boundaries do not allow general connectivity. There are two primary reasons for this:

(1) The perceived shortage of IPv4 addresses has caused increasing use of private IPv4 network addresses such as 10.0.0.0/8 on LANs. A number of such private address ranges are designated in [RFC 1918], and others may be also assigned by IANA.

[Note: For example, there's 169.254/16, which is mentioned in draft-ietf-zeroconf-ipv4-linklocal-04.txt, but since that's still a draft, I can't cite it.]

IPv6 addresses are not in short supply, but the IPv6 architecture uses a scoped address model, in which non-global addresses have limited reachability and domains of uniqueness. For instance, site-local addresses are reachable only within a particular site.

Hosts using private addresses that wish to communicate with the public Internet must do so via an address translation mechanism such as a NAT box. This allows a host with a private address to send packets to public Internet hosts, and to receive replies. However, unsolicited incoming packets cannot reach these hosts from outside their own private network.

(2) Increasing security concerns have caused many sites to install firewalls or to implement restrictions in their boundary routers in order to lock out certain kinds of connection to their hosts, even when the hosts are using public Internet addresses, though in many cases firewalls also provide NAT functionality.

Thus, there are two classes of host which some or all types of unexpected incoming packet from the public Internet cannot reach: those using truly private IPv4 or IPv6 addresses, and those using public addresses where access is blocked.

A number of instances have been observed where IP addresses that are never accessible from the public Internet have nevertheless been inserted into resource records in the public DNS. This document seeks to prohibit such behaviour in the case of truly private addresses, and to discourage it in the case of public, but unreachable, addresses.

Although this document is specifically concerned with the contents of the public DNS, the principle of not publishing private IP addresses

is applicable to any other form of general publication.

The keywords "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].

The phrase "address record" means an A record or an AAAA record, or any other kind of name-to-address record that may come into use.

2. Private network addresses

Examples of [RFC 1918] private host addresses are 10.0.0.1 and 172.16.42.53. In the case of IPv6, all link-local and site-local addresses are private.

Packets cannot be routed to such addresses from the public Internet. [RFC 1918] explains this in section 3, from where this paragraph is taken:

> Because private addresses have no global meaning, routing information about private networks shall not be propagated on inter-enterprise links, and packets with private source or destination addresses should not be forwarded across such links. Routers in networks not using private address space, especially those of Internet service providers, are expected to be configured to reject (filter out) routing information about private networks.

Because the same private addresses are in use in many different organizations, they are ambiguous. The appearance of private addresses in the DNS could therefore lead to unpredictable and unwanted behaviour. Consider this set of entries:

```
@       IN      MX  10  smtp
smtp    IN      A       10.1.2.3
smtp    IN      A       131.111.10.206
```

The MX record resolves to two IP addresses, one of which is private and one of which is public. Zones set up in this way have been seen, and some administrators apparently believe this is useful, because it allows mail on their local network to be delivered straight to the internal server (the one with address 10.1.2.3). However, this approach breaks down when a host on a foreign network that is also using the address 10.1.2.3 attempts to send mail to the domain.

In section 5 of [RFC 1918] there is a prohibition of the appearance of private addresses in publicly visible DNS records. It says:

> If an enterprise uses the private address space, or a mix of private and public address spaces, then DNS clients outside of the enterprise should not see addresses in the private address

space used by the enterprise, since these addresses would be ambiguous.

The wording "should not" is not a very strong prohibition, considering the interworking problems that ignoring it can cause. Therefore, this document makes a stronger statement:

Public DNS zones MUST NOT contain [RFC 1918] addresses, IPv6 link-local or site-local addresses, or any other addresses designated by IANA as private, in any resource records where the context makes them appear to be globally-meaningful addresses.

3. Public network addresses that are inacessible

The situation with public network addresses is more complicated because the Internet cannot in general be cleanly divided into "public" and "private" parts in this case. Examples of situations where the division is fuzzy are:

(1) A host with a public address that is behind a firewall may be accessible for SSH sessions, but not for SMTP sessions. That is, the blocking may apply only to certain ports.

(2) A host with a public address may make certain services available only to specific client hosts, for example, those in partner enterprises, or those in a specific geographic area.

(3) A host might respond to incoming packets only if the client host is using IPsec.

When a host is providing any service at all over the public Internet, a publicly visible address record is of course required to give access to that host.

However, for some protocols and services, additional DNS records are defined that reference hosts' address records. These are the NS record for name servers, the MX record for SMTP, and the SRV record for other services. The existence of such indirect records advertises the availability of the relevant service.

If these services are always inaccessible over the public Internet, it is bad practice to include the NS, MX or SRV records in public DNS zones, for the following reason:

A host that tries to connect to an unreachable address (or port) may not receive an immediate rejection; in many cases the connection will fail only after a timeout expires. The wasted effort ties up resources on the calling host and the network, possibly for some considerable time (SMTP timeouts, for example, are of the order of minutes). It may also cause a gratuitous slowing down of the application.

Furthermore, in the case of dial-up connections, ISDN, or other kinds of usage-based charged network connection, the wasted network resources may cost real money.

Public DNS zones SHOULD NOT contain NS, MX or SRV records that point to hosts for which the relevant services are never accessible over the public Internet. In other words, if there is no host that is able to make use of the service using the public Internet, the service SHOULD NOT be publicly advertised.

4. Other kinds of IPv6 address

4.1 Anycast addresses

Anycast addresses should be treated as global addresses with limited reachability.

4.2 Multicast addresses

Scoped multicast addresses (multicast addresses with a 4 bit scope value less than 0x0e) MUST NOT be put into public DNS zones. Globally-scoped multicast addresses MAY be put into public DNS zones.

4.3 IPv4-mapped addresses

IPv4-mapped addresses MUST NOT be put into public DNS zones, because their use is limited to an internal representation of IPv4 peers within the AF_INET6 socket API [RFC 2553].

4.4 IPv4-compatible addresses

IPv4-compatible addresses MUST NOT be put into public DNS zones. Although there might be a case for doing so in order to indicate that the node is willing to accept auto-tunnelled packets [RFC 2893], it is not clear that this transition mechanism will be widely used. It is therefore preferable to keep the DNS operationally "clean" by not allowing them.

5. Loopback addresses

The loopback addresses (127.0.0.1 for IPv4 and ::1 for IPv6) are another form of private address. There has been a practice of including them in DNS zones for two entirely different reasons.

5.1 The name "localhost"

Some hostmasters include records of this type in their zones:

```
localhost.some.domain.example.  A  127.0.0.1
```

The reason for doing this is so that other hosts in the domain that use the DNS for all their name resolution can make use of the unqualified name "localhost". This works because DNS resolvers normally add the local enclosing domain to unqualified names.

DNS zones MAY make use of this technique for the name "localhost" only, if it is required in their environment, but SHOULD avoid it if possible. See section 6.1 below for an alternative technique.

5.2 DNS "black lists"

There is an increasingly popular practice of creating "black lists" of misbehaving hosts (for example, open mail relays) in the DNS. The first of these was the "Realtime Blackhole List" (RBL). Such lists make use of address values in the 127.0.0.0/8 network in DNS address records to give information about listed hosts (which are looked up via their inverted IP addresses).

Such records are in specific "black list" domains, and are well understood not to be invitations to attempt connections to the addresses they publish. In other words, the values that appear in these records do not appear in a context where they are interpreted as IP addresses.

DNS zones MAY continue to make use of this technique.

5.3 Other uses of loopback networks

Apart from the exceptions mentioned in 5.1 and 5.2 above, the loopback addresses MUST NOT appear in address records in the public DNS, unless it is clear from the context that the value is not to be interpreted as an IP address.

5.4 References to loopback addresses

When address records that contain loopback addresses do exist, DNS zones MUST NOT contain indirect records (NS, MX or SRV) that reference them.

6. Alternative techniques

6.1 Handling "localhost"

Instead of including "localhost" within every domain for which a name server is authoritative, [RFC 1912] recommends setting up "localhost." as a top-level domain in each name server. [RFC 2606] reserves the name "localhost." for this purpose.

6.2 Splitting DNS zones

A site that is using private addresses may well want to use DNS lookups for address resolution on its hosts. The lazy way approach is simply to put the data into the public DNS zone, as in the example shown in section 2 above. Because this can cause problems for external hosts, this MUST NOT be done.

One approach that is commonly taken is to run a so-called "split DNS". Two different authoritative servers are created: one containing all the zone data is accessible only from within the private network. External DNS queries are directed to the second server, which contains a filtered version of the zone, without the private addresses.

6.3 SMTP servers behind firewalls

The complication of a split DNS is not normally needed if it is only SMTP traffic that is being blocked to a public address on a host behind a firewall. Setting up MX records like this:

```
plc.example.    MX   5   mail.plc.example.
                MX  10   public.plc.example.
```

where both hosts have public IP addresses, but the first is blocked at the firewall, SHOULD NOT be done. Only the publicly accessible host should be used:

```
plc.example.    MX  10   public.plc.example.
```

If a split DNS is in use, the host public.plc.example can use the internal version to route the mail onwards. However, most MTAs have configuration facilities to allow for explicit routing of mail, without the need to use a DNS lookup.

6.4 Specification of no SMTP service

MX records that point to host names whose address records specify the loopback address have been seen in the DNS. This seems to be a misguided attempt to specify "no SMTP service for this domain" more positively than just refusing connections to the SMTP port. (A refused connection is treated as a temporary error, because it might be the result of a system rebooting, for example.)

If such a facility is required, it SHOULD instead be done by arranging for the hosts in question to return

```
554 No SMTP service here
```

to all SMTP connections.

7. Security Considerations

This document is not known to create new security issues in the DNS, mail agents, etc. In some sense, it may reduce security exposure by insisting that a site's inappropriate internal data not be exposed.

8. IANA Considerations

No IANA actions are required by this document.

9. Acknowledgements

Randy Bush read an early draft of this document and suggested several improvements.

Draft 01 has benefitted from comments made by Daniel Senie, John Schnizlein, Robert Elz, Bert Hubert, and Stuart Cheshire.

Draft 02 has benefitted from comments made by David Keegel and Simon Josefsson.

Draft 03 has benefitted from comments made by Jun-ichiro itojun Hagino, David Terrell, Erik Nordmark, Matt Larson, and Zefram.

10. Author's Address

Philip Hazel
University of Cambridge Computing Service
New Museums Site, Pembroke Street
Cambridge CB2 3QH, England

Phone: + 44 1223 334714
Email: ph10@cam.ac.uk

11. References

[RFC 1912] Barr, D. "Common DNS Operational and Configuration Errors", RFC 1912, February 1996.

[RFC 1918] Rekhter, Y. et al "Address allocation for Private Internets", BCP 5, RFC 1918, February 1996.

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

[RFC 2553] Gilligan, S. et al "Basic Socket Interface Extensions for IPv6", RFC 2553, March 1999.

[RFC 2606] Eastlake, D. and Panitz, A. "Reserved Top Level DNS Names", BCP 32, RFC 2606, June 1999.

[RFC 2893] Gilligan, R. and Nordmark, E. "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000.

12. Changes made during development of this document

This section is provided for the convenients of those tracking the document. It will be removed from the final draft.

12.1 Changes made to the -00 version to create -01

. While leaving the MUSTs in for truly private addresses, I've tried to be more "educational" about the case of public addresses that are inaccessible, and backed down to SHOULD in those cases.

. I've pointed out the lack of a clear-cut public/private boundary, and tried to make the case for not advertising unavailable services without being so probititive in the wording. This includes using "never accessible" instead of "not accessible".

. Changed "hostmaster" to "zone" in a couple of cases.

. Included an example of bad MX practice with an [RFC 1918] address.

. Noted that [RFC 1918] is not the only list of private addresses.

. General tidying of the wording and rearrangement of the material.

. The Post Office changed our postcode!

12.2 Changes made to the -01 version to create -02

. Add NS to MX and SRV as another DNS record that advertises a service indirectly.

. Changed the address 1.2.3.4 in an example to a genuine real address to make it quite clear what I mean.

. Added "geographic area" as another example of a service restriction.

. Suggested why people might want something other than "connection refused" from hosts that don't provide SMTP service.

. Some other very minor rewording.

12.3 Changes made to the -02 version to create -03

. Added more words about IPv6, with detail supplied by Jun-ichiro itojun Hagino about specific kinds of IPv6 address.

. Added a references to RFCs 1912 and 2606 for the handling of "localhost" by setting it up as a TLD.

. Generalized ideas such as "black hole lists" to talk about the context of interpretation of addresses.

. Added a short statement about other (non-DNS) forms of publication.

Full Copyright Statement

Acknowledgement

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