Network Working Group
Internet-Draft
Expires: April 18, 2004

D. Plonka
University of Wisconsin

October 19, 2003

Embedding Globally Routable Internet Addresses Considered Harmful
draft-plonka-embed-addr-00

Status of this Memo

Copyright Notice

Abstract

Vendors of consumer electronics and network gear have produced and sold hundreds of thousands of Internet hosts with globally routable Internet Protocol addresses embedded within their products' firmware. These products are now in operation world-wide and primarily include, but are not necessarily limited to, low-cost routers and middleboxes for personal or residential use.

This "hard-coding" of globally routable IP addresses within the host's firmware presents significant problems to the operation of the Internet and to the management of its address space.

This document means to clarify best current practices in the Internet community. It denouces the practice of embedding references to

unique, globally routable IP addresses in Internet hosts, describes some of the resulting problems, and considers selected alternatives. It is also intended to remind the Internet community of the ephemeral nature of unique, globally routable IP addresses and that the assignment and use of such addresses is temporary and therefore should not be used in fixed configurations.

1. Introduction

Internet hosts should not contain globally routable Internet Protocol addresses embedded within firmware or elsewhere as part of their default configuration influencing their run-time behavior.

Ostensibly, this practice arose as an attempt to implement of "zero configuration" with neither peer review nor the use of a proposed or standard Internet protocol to do so. Unfortunately, products which rely on such embedded IP addresses initially may appear convenient to both the product's designer and its operator or user, but this dubious benefit comes at the expense of others in the Internet community.

2. Problems

In a number cases, the embedding of IP addresses has caused Internet products to rely on a single central Internet service, which can result in a collapse when the aggregate workload overwhelms that service. When fixed addresses are embedded in an ever-increasing number of client IP hosts, this practice runs directly counter to the design intent of hierarchically deployed services that would otherwise be robust solutions.

The reliability, scalability, and performance of many Internet services require that the pool of users not directly access a service by IP address. Instead they rely on a level of indirection provided by the DNS, RFC 2219 [2]. DNS permits the service operator to reconfigure the resources for maintenance and load-balancing without the participation of the users. For instance, a load-balancing technique in common use today employs multiple DNS records with the same name which are then doled out in a round-robin fashion by the Berkeley Internet Name Daemon (BIND) and other DNS server implementations. This enables the operator to distribute the user request load across a set of servers with discrete IP addresses, which generally remain unknown to the user.

Furthermore, embedding globally unique IP addresses taints the IP address blocks in which they reside, lessening the usefulness and portability of those IP address blocks and increasing the cost of operation. Unsolicited traffic may continue to be delivered to the embedded addresses for historical reasons, even after the IP address or block has been reassigned. IP address blocks containing addresses that have been embedded into the configuration of many Internet hosts become encumbered by their historical use. This may interfere with the ability of the Internet Assigned Numbers Authority (IANA) and the Internet Registry (IR) hierarchy to usefully reallocate IP address blocks. This is of particular concern as the IPv4 address space nears exhaustion. Note that, to facilitate IP address reuse, RFC 2050 [3], encourages Internet Service Providers (ISPs) to treat address assignments as "loans".

Because consumers are not necessarily capable, experienced operators of Internet hosts, they are not able to be relied upon to implement a fix if and when problems arise. As such, a significant responsibility lies with the manufacturer or vendor of the Internet host to avoid embedding IP addresses.

3. Recommendations

Network product manufacturers should not assume that their products will only be deployed on a single (mythical) global Internet, that they happen to observe today. A myriad of private internets in which these products will be used will often not allow these hosts to establish end-to-end communications with arbitrary hosts on the global Internet.

Vendors should, by default, disable unnecessary features in their products. This is especially true of features that generate unsolicited traffic. In this way these hosts will be conservative regarding the unsolicited Internet traffic they produce. For instance, one of the most common uses of embedded IP addresses has been the hard-coding of addresses of well know public Simple Network Time Protocol (SNTP RFC 2030 [4]) servers, even though only a small fraction of the users benefits from these products even having some notion of the current date and time.

Vendors should provide an operator interface for every feature that generates unsolicited IP traffic. Non-default configuration should be required to enable these features so that, as a consequence, the operator becomes aware that the feature exists. This will mean that it is more likely that the product's owner or operator can participate in problem determination and mitigation if and when problems arise.

Internet hosts should use the Domain Name System to determine the routable IP addresses associated with the Internet services they require. However, note that simply hard-coding DNS names rather than IP addresses is not a panacea. Entries in the domain name space are also ephemeral and can change owners for various reasons including such as acquisitions and litigation. A given vendor ought not assume that it will retain control of a given zone indefinitely.

Whenever possible, default configurations, documentation, and example configurations for Internet hosts should use Private Internet Addresses, as defined by RFC 1918 [1], rather than unique, globally routable IP addresses.

Service providers and enterprise network operators should advertise the identities of suitable local services. For instance, the DHCP protocol, as defined by RFC 2132 [5], enables one to configure a server to answer queries regarding available servers to clients that ask for them. Unless the advertisement of local services is ubiquitous, designers may resort to ad hoc mechanisms which rely on central services.

Operators that provide public services on the global Internet, such as the the NTP community, should deprecate the advertisement of the explicit IP addresses of public services. These addresses are ephemeral, and their widespread citations in indexes of public services interferes with these services to be reconfigured to scale with unexpected, increased load.

4. Security Considerations

Embedding or "hard-coding" IP addresses within a host's configuration almost always means that some sort of host-based trust model is being employed, and that the Internet host with the given address is trusted in some way. Due to the ephemeral roles of routable IP addresses, the practice of embedding them within products' firmware or default configurations presents a security risk.

An Internet host designer may be tempted to implement some sort of remote control mechanism within a product, by which its Internet host configuration can be changed without reliance on, interaction with, or even the knowledge of its operator or user. This raises security issues of its own. If such a scheme is implemented, this should be fully disclosed to the customer, operator, and user so that an informed decision can be made, in accordance with local security or privacy policy. Furthermore, the significant possibility of malicious parties exploiting such a remote control mechanism may completely negate any potential benefit of the remote control scheme.

5. Conclusion

As larger number of homogenous hosts continue to be deployed, it is particularly important that both designers and other members of the Internet community are diligent in assessing host implementation quality and reconfigurability. Unique, globally routable IP addresses should not be embedded within a host's fixed configuration because doing so excludes the ability to remotely influence hosts when the unsolicited traffic they generate causes problems for the for those operating the IP addresses to which the traffic is destined.

References

[1] Rekhter, Y., "Address Allocation for Private Internets", RFC 1918, BCP 5, February 1996.

[2] Hamilton, M., "Use of DNS Aliases for Network Services", RFC 2219, BCP 17, October 1997.

[3] Hubbard, K., "INTERNET REGISTRY IP ALLOCATION GUIDELINES", RFC 2050, BCP 12, November 1996.

[4] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 2030, October 1996.

[5] Alexander, S., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

Author's Address

David J. Plonka
University of Wisconsin - Madison
DoIT, room b263
1210 W. Dayton Street
Madison, WI 53705
US

Phone: +1 608 265 5184
EMail: plonka@doit.wisc.edu
URI: http://net.doit.wisc.edu/~plonka/

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

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