Network Working Group
Request for Comments: 1627
Category: Informational

E. Lear
Silicon Graphics, Inc.
E. Fair
Apple Computer, Inc.
D. Crocker
Silicon Graphics, Inc.
T. Kessler
Sun Microsystems, Inc.

July 1994

Network 10 Considered Harmful
(Some Practices Shouldn't be Codified)

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

SUMMARY

Re-use of Internet addresses for private IP networks is the topic of the recent RFC 1597 [1]. It reserves a set of IP network numbers, for (re-)use by any number of organizations, so long as those networks are not routed outside any single, private IP network. RFC 1597 departs from the basic architectural rule that IP addresses must be globally unique, and it does so without having had the benefit of the usual, public review and approval by the IETF or IAB. This document restates the arguments for maintaining a unique address space. Concerns for Internet architecture and operations, as well as IETF procedure, are explored.

INTRODUCTION

Growth in use of Internet technology and in attachments to the Internet have taken us to the point that we now are in danger of running out of unassigned IP network numbers. Initially, numbers were formally assigned only when a network was about to be attached to the Internet. This caused difficulties when initial use of IP substantially preceded the decision and permission to attach to the Internet. In particular, re-numbering was painful. The lesson that we learned was that every IP address ought to be globally unique, independent of its attachment to the Internet. This makes it possible for any two network entities to communicate, no matter where either might be located. This model is the result of a decades-long evolution, through which the community realized how painful it can be to convert a network of computers to use an assigned number after

using random or default addresses found on computers just out of the box. RFC 1597 abrogates this model without benefit of general IETF community discussion and consensus, leaving policy and operational questions unasked and unanswered.

KEEP OUR EYES ON THE PRIZE: AN ARCHITECTURAL GOAL AND VIOLATION

A common -- if not universal -- ideal for the future of IP is for every system to be globally accessible, given the proper security mechanisms. Whether such systems comprise toasters, light switches, utility power poles, field medical equipment, or the classic examples of "computers", our current model of assignment is to ensure that they can interoperate.

In order for such a model to work there must exist a globally unique addressing system. A common complaint throughout the community is that the existing security in host software does not allow for every (or even many) hosts in a corporate environment to have direct IP access. When this problem is addressed through proper privacy and authentication standards, non-unique IP addresses will become a bottleneck to easy deployment if the recommendations in RFC 1597 are followed.

The IP version 4 (IPv4) address space will be exhausted. The question is simply: when?

If we assert that all IP addresses must be unique globally, connected or not, then we will run out of IP address space soon.

If we assert that only IP addresses used on the world-wide Internet need to be globally unique, then we will run out of IP address space later.

It is absolutely key to keep the Internet community’s attention focused on the efforts toward IP next generation (IPng), so that we may transcend the limitations of IPv4. RFC 1597 produces apparent relief from IPv4 address space exhaustion by masking those networks that are not connecting to the Internet, today. However, this apparent relief will likely produce two results: complacency on the large part of the community that does not take the long term view, and a very sudden IP address space exhaustion at some later date.

Prior to IPng deployment, it is important to preserve all the semantics that make both the Internet and Internet technology so very valuable for interoperability. Apple Computer, IBM, and Motorola could not collaborate as easily as they have to produce the PowerPC without uniquely assigned IP addresses. The same can be said of the Silicon Graphics merger with MIPS. There are many, many more examples

that can be cited.

It should be noted that a scheme similar to RFC 1597 can be implemented at the time that we actually run out of assignable IPv4 address space; it simply requires that those organizations which have been assigned addresses but are not yet connected to the Internet return their addresses to IANA. It is important that the IAB (and IANA as its agent) reassert their ownership of the IP address space now, to preclude challenges to this type of reassignment.

OPERATIONAL ISSUES

RFC 1597 Implementations

Methods are needed to ensure that the remaining addresses are allocated and used frugally. Due to the current problems, Internet service providers have made it increasingly difficult for organizations to acquire public IP network numbers. Private networks have always had the option of using addresses not assigned to them by appropriate authorities. We do not know how many such networks exist, because by their nature they do not interact with the global Internet. By using a random address, a company must take some care to ensure it is able to route to the properly registered owner of that network.

RFC 1597 proposes to solve the routing problem by assigning numbers that will never be used outside of private environments. Using such standard numbers introduces a potential for clashes in another way. If two private networks follow RFC 1597 and then later wish to communicate with each other, one will have to renumber. The same problem occurs if a private network wishes to become public. The likely cost of renumbering is linear to the number of hosts on a network. Thus, a large company with 10,000 hosts on a network could incur considerable expense if it either merged with another company or joined the Internet in such a way as to allow all hosts to directly access the outside network.

The probability of address clashes occurring over time approach 100% with RFC 1597. Picking a random network number reduces the chances of having to renumber hosts, but introduces the routing problems described above. Best of all, retrieving assigned numbers from the appropriate authority in the first place eliminates both existing and potential address conflicts at the cost of using a part of the address space.

Apple Computer once believed that none of its internal systems would ever speak IP directly to the outside world, and as such, network operations picked IP class A network 90 out of thin air to use.

Apple is only now recovering from this error, having renumbered some 5,000 hosts to provide them with "desktop" Internet access. Unless the Internet community reaffirms its commitment to a globally unique address space, we condemn many thousands of organizations to similar pain when they too attempt to answer the call of the global Internet.

Another timely example of problems caused by RFC 1597 is Sun's use of Internet multicasting. Sun selectively relays specific multicast conferences. This has the effect of making many hosts at Sun visible to the Internet, even though they are not addressable via IP unicast routing. If they had non-global addresses this would not work at all. It is not possible to predict which machines need global addresses in advance. Silicon Graphics has a similar configuration, as is likely for others, as well.

Some might argue that assigning numbers to use for private networks will prevent accidental leaks from occurring through some sort of convention a'la Martian packets. While the proposal attempts to create a standard for "private" address use, there is absolutely no way to ensure that other addresses are not also used.

Hence, the "standard" becomes nothing but a misleading heuristic. In fact, it is essential that routers to the global Internet advertise networks based only on explicit permission, rather than refusing to advertise others based on implicit prohibition, as supported by the policy formally created in RFC 1597.

Security Issues

Administrators will have a hard time spotting unauthorized networks, when their network has been breached (either intentionally or unintentionally) because the other networks might have the same numbers as those normally in the routing tables. More over, an inadvertent connection could possibly have a double whammy effect of partitioning two operational networks.

It is worth emphasizing that IP providers should filter out all but authorized networks. Such a practice would not only prevent accidents but also enhance the security of the Internet by reducing the potential number of points of attack.

Internet multicasting adds a new dimension to security. In some cases it may possible to allow multicasting through firewalls that completely restrict unicast routing. Otherwise unconnected networks might well need unique addresses, as illustrated in the example above.

Problems with Examples

RFC 1597 gives several examples of IP networks that need not have globally unique address spaces. Each of those cases is plausible, but that does not make it legitimate to ENCOURAGE non-uniqueness of the addresses. In fact, it is equally plausible that globally unique IP addresses will be required, for every one of the scenarios described in RFC 1597:

- Airport displays are public information and multicasting beyond the airport might be useful.

- An organization's machines which, today, do not need global connectivity might need it tomorrow. Further, merging organizations creates havoc when the addresses collide.

- Current use of firewalls is an artifact of limitations in the technology. Let's fix the problem, not the symptom.

- Inter-organization private links do not generate benefit from being any more correct in guessing which machines want to interact than is true for general Internet access.

This is another point that warrants repetition: the belief that administrators can predict which machines will need Internet access is quite simply wrong. We need to reduce or eliminate the penalties associated with that error, in order to encourage as much Internet connectivity as operational policies and technical security permit. RFC 1597 works very much against this goal.

Problems With "Advantages" And More Disadvantages

RFC 1597 claims that Classless Inter-Domain Routing (CIDR) will require enterprises to renumber their networks. In the general case, this will only involve those networks that are routed outside of enterprises. Since RFC 1597 addresses private enterprise networks, this argument does not apply.

The authors mention that DCHP-based tools [2] might help network number transition. However, it is observed that by and large such tools are currently only "potential" in nature.

Additionally, with the onslaught of ISDN, slip, and PPP in host implementations, the potential for a workstation to become a router inadvertently has never been greater. Use of a common set of addresses for private networks virtually assures administrators of having their networks partitioned, if they do not take care to carefully control modem connections.

Finally, RFC 1597 implies that it may be simple to change a host's IP address. For a variety of reasons this may not be the case, and it is not the norm today. For example, a host may be well known within a network. It may have long standing services such as NFS, which would cause problems for clients were its address changed. A host may have software licenses locked by IP address. Thus, migrating a host from private to global addressing may prove difficult. At the very least, one should be careful about addressing well known hosts.

POLICY ISSUES

IANA Has Overstepped Their Mandate

For many years, IANA has followed an assignment policy based on the expectation of Internet connectivity for ALL assignees. As such it serves to encourage interconnectivity. IANA assignment of the network numbers listed in RFC 1597 serves to formally authorize behavior contrary to this accepted practice. Further, this change was effected without benefit of community review and approval.

RFC 1597 specifies a new operational requirement explicitly: network service providers must filter the IANA assigned network numbers listed in RFC 1597 from their routing tables. This address space allocation is permanently removed from being used on the Internet.

As we read RFC 1601 [3], this action is not within the purview of IANA, which should only be assigning numbers within the current standards and axioms that underlie the Internet. IP network numbers are assigned uniquely under the assumption that they will be used on the Internet at some future date. Such assignments violate that axiom, and constitute an architectural change to the Internet. RFC 1602 [4] and RFC 1310 [5] also contain identical wording to this effect in the section that describes IANA.

While RFC 1597 contains a view worthy of public debate, it is not ready for formal authorization. Hence, we strongly encourage IANA to withdraw its IP address assignments documented by RFC 1597 forthwith.

The IAB should review the address assignment policies and procedures that compose IANA's mandate, and reaffirm the commitment to a globally unique IP address space.

COMMENTS AND CONCLUSIONS

The Internet technology and service is predicated on a global address space. Members of the Internet community have already experienced and understood the problems and pains associated with uncoordinated private network number assignments. In effect the proposal attempts

to codify uncoordinated behavior and alter the accepted Internet addressing model. Hence, it needs to be considered much more thoroughly.

RFC 1597 gives the illusion of remedying a problem, by creating formal structure to a long-standing informal practice. In fact, the structure distracts us from the need to solve these very real problems and does not even provide substantive aid in the near-term.

In the past we have all dreaded the idea of having any part of the address space re-used. Numerous luminaries have both written and spoke at length, explaining why it is we want direct connections from one host to another. Before straying from the current architectural path, we as a community should revisit the reasoning behind the preaching of unique addressing. While RFC 1597 attempts to change this model, its costs and limitations for enterprises can be enormous, both in the short and long term.

REFERENCES

[1] Rekhter, Y., Moskowitz, B., Karrenberg, D., and G. de Groot, "Address Allocation for Private Internets", T.J. Watson Research Center, IBM Corp., Chrysler Corp., RIPE NCC, RFC 1597, March 1994.

[2] Droms, R., "Dynamic Host Configuration Protocol", RFC 1541, Bucknell University, October 1993.

[3] Huitema, C., "Charter of the Internet Architecture Board (IAB)", RFC 1601, IAB, March 1994.

[4] Internet Architecture Board, Internet Engineering Steering Group, "The Internet Standards Process -- Revision 2", IAB, IESG, RFC 1602, March 1994.

[5] Internet Activities Board, "The Internet Standards Process", RFC 1310, IAB, March 1992.

[6] Internet Activities Board, "Summary of Internet Architecture Discussion", Notes available from ISI, [ftp.isi.edu: pub/IAB/IABmins.jan91Arch.txt], IAB, January 1991.

SECURITY CONSIDERATIONS

See the section, "Security Issues".

AUTHORS' ADDRESSES

Eliot Lear
Silicon Graphics, Inc.
2011 N. Shoreline Blvd.
Mountain View, CA
94043-1389

Phone: +1 415 390 2414
EMail: lear@sgi.com

Erik Fair
Apple Computer, Inc.
1 Infinite Loop
Cupertino, CA 95014

Phone: +1 408 974 1779
EMail: fair@apple.com

Dave Crocker
Silicon Graphics, Inc.
2011 N. Shoreline Blvd.
Mountain View, CA
94043-1389

Phone: +1 415 390 1804
EMail: dcrocker@sgi.com

Thomas Kessler
Sun Microsystems Inc.
Mail Stop MTV05-44
2550 Garcia Ave.
Mountain View, CA 94043

Phone: +1 415 336 3145
EMail: kessler@eng.sun.com