Network Working Group
Request for Comments: 1900
Category: Informational

B. Carpenter
Y. Rekhter
IAB

February 1996

Renumbering Needs Work

Status of this Memo

Abstract

Renumbering, i.e., changes in the IP addressing information of various network components, is likely to become more and more widespread and common. The Internet Architecture Board (IAB) would like to stress the need to develop and deploy solutions that would facilitate such changes.

Table of Contents

1. Motivation

Hosts in an IP network are identified by IP addresses, and the IP address prefixes of subnets are advertised by routing protocols. A change in such IP addressing information associated with a host or subnet is known as "renumbering".

Renumbering may occur for a variety of reasons. For example, moving an IP host from one subnet to another requires changing the host's IP address. Physically splitting a subnet due to traffic overload may also require renumbering. A third example where renumbering may happen is when an organization changes its addressing plan. Such changes imply changing not only hosts' addresses, but subnet numbers as well. These are just three examples that illustrate possible scenarios where renumbering could occur.

Increasingly, renumbering will be needed for organizations that require Internet-wide IP connectivity, but do not themselves provide a sufficient degree of address information aggregation. Unless and until viable alternatives are developed, extended deployment of Classless Inter-Domain Routing (CIDR) is vital to keep the Internet routing system alive and to maintain continuous uninterrupted growth of the Internet. With current IP technology, this requires such organizations to use addresses belonging to a single large block of address space, allocated to their current service provider which acts as an aggregator for these addresses. To contain the growth of routing information, whenever such an organization changes to a new service provider, the organization's addresses will have to change. Occasionally, service providers themselves may have to change to a new and larger block of address space. In either of these cases, to contain the growth of routing information, the organizations concerned would need to renumber their subnet(s) and host(s). If the organization does not renumber, then some of the potential consequences may include (a) limited (less than Internet-wide) IP connectivity, or (b) extra cost to offset the overhead associated with the organization's routing information that Internet Service Providers have to maintain, or both.

Currently, renumbering is usually a costly, tedious and error-prone process. It normally requires the services of experts in the area and considerable advance planning. Tools to facilitate renumbering are few, not widely available, and not widely deployed. While a variety of ad hoc approaches to renumbering have been developed and used, the overall situation is far from satisfactory. There is little or no documentation that describes renumbering procedures. While renumbering occurs in various parts of the Internet, there is little or no documented experience sharing.

2. DNS versus IP Addresses

Within the Internet architecture an individual host can be identified by the IP address(es) assigned to the network interface(s) on that host. The Domain Name System (DNS) provides a convenient way to associate legible names with IP addresses. The DNS name space is independent of the IP address space. DNS names are usually related to the ownership and function of the hosts, not to the mechanisms of addressing and routing. A change in DNS name may be a sign of a real change in function or ownership, whereas a change in IP address is a purely technical event.

Expressing information in terms of Domain Names allows one to defer binding between a particular network entity and its IP address until run time. Domain Names for enterprises, and Fully Qualified Domain Names (FQDNs, see RFC 1594) for servers and many user systems, are

expected to be fairly long-lived, and more stable than IP addresses. Deferring the binding avoids the risk of changed mapping between IP addresses and specific network entities (due to changing addressing information). Moreover, reliance on FQDNs (rather than IP addresses) also localizes to the DNS the changes needed to deal with changing addressing information due to renumbering.

In some cases, both the addresses and FQDNs of desk top or portable systems are allocated dynamically. It is only a highly responsive dynamic DNS update mechanism that can cope with this.

3. Recommendations

To make renumbering more feasible, the IAB strongly recommends that all designs and implementations should minimise the cases in which IP addresses are stored in non-volatile storage maintained by humans, such as configuration files. Configuration information used by TCP/IP protocols should be expressed, whenever possible, in terms of Fully Qualified Domain Names, rather than IP addresses. Hardcoding IP addresses into applications should be deprecated. Files containing lists of name to address mappings, other than that used as part of DNS configuration, should be deprecated, and avoided wherever possible.

There are times when legacy applications which require configuration files with IP addresses rather than Domain Names cannot be upgraded to meet these recommendations. In those cases, it is recommended that the configuration files be generated automatically from another file which uses Domain Names, with the substitution of addresses being done by lookup in the DNS.

Use of licensing technology that is based upon the IP address of a host system makes renumbering quite difficult. Therefore, the use of such technology should be strongly discouraged.

The development and deployment of a toolkit to facilitate and automate host renumbering is essential. The Dynamic Host Configuration Protocol (DHCP) is clearly an essential part of such a toolkit. The IAB strongly encourages implementation and wide-scale deployment of DHCP. Dynamic router discovery (RFC 1256) and service location (work in progress in the IETF) also belong in this toolkit. Support for dynamic update capabilities to the Domain Name System (DNS) that could be done with sufficient authentication would further facilitate host renumbering. The IAB strongly encourages progression of work in this area towards standardization within the IETF, with the goal of integrating DHCP and dynamic update capabilities to provide truly autoconfigurable TCP/IP hosts.

The IAB strongly encourages sharing of experience with renumbering and documenting this sharing within the Internet community. The IAB suggests that the IETF (and specifically its Operational Requirements Area) may be the most appropriate place to develop such documentation. The IAB welcomes the creation of the PIER (Procedures for Internet and Enterprise Renumbering) working group.

4. Security Considerations

Renumbering is believed to be compatible with the Internet security architecture, as long as addresses do not change during the lifetime of a security association.

Acknowledgements

This document is a collective product of the Internet Architecture Board.

Useful comments were received from several people, especially Michael Patton, Steve Bellovin, Jeff Schiller, and Bill Simpson.

Authors' Addresses

Brian E. Carpenter
Group Leader, Communications Systems
Computing and Networks Division
CERN
European Laboratory for Particle Physics
1211 Geneva 23, Switzerland

Phone: +41 22 767-4967
Fax: +41 22 767-7155
Telex: 419000 cer ch
EMail: brian@dxcoms.cern.ch

Yakov Rekhter
cisco Systems
170 West Tasman Drive
San Jose, CA 95134

Phone: (914) 528-0090
EMail: yakov@cisco.com