Network Working Group   R. Droms
INTERNET DRAFT   Bucknell University
                                                        J. Waters
                                                         P. Gross
                                                        R. Hagens
                                                          P. Ford
                                                              MCI
                                                    February 1996
                                             Expires August 1996

                   RFI: Enterprise Network Renumbering
                 <**draft-ietf-pier-solicitation2-00.txt**>

Status of this memo

   This document is an Internet-Draft. Internet-Drafts are working
   documents of the Internet Engineering Task Force (IETF), its areas,
   and its working groups. Note that other groups may also distribute
   working documents as Internet-Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as ``work in progress.''

   To learn the current status of any Internet-Draft, please check the
   ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow
   Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe),
   munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or
   ftp.isi.edu (US West Coast).

Abstract

   Because of the urgent need for, and substantial difficulty in,
   renumbering IP networks, the PIER working group is compiling a series
   of documents to assist sites in their renumbering efforts. The
   intent of these documents is to provide both educational and
   practical information to the Internet community. The intent of these
   document is to provide both educational and practical information to
   the Internet community. To this end the PIER WG is soliciting
   information from vendors and other members of the Internet community
   about issues and problems hat organizations should consider when
   undertaking their renumbering process.

[1](1). Introduction

   Because of the interdependence between the IP address assigned to a

computer and the network to which it is attached, it may be necessary
to change a computer's IP address if the computer is moved or the
architecture of the network changes. For example, moving a computer
to a new location, changes in the local network architecture or
changing internet service provider may require that individual
computers be assigned new IP addresses. Such reassignment of IP
addresses is sometimes called "renumbering".

There are immediate and increasingly severe requirements to renumber
both small- and large-scale networks. The Procedures for
Internet/Enterprise Renumbering Working Group of the IETF (PIER WG)
requests specific input for producing concrete guidance for the
renumbering task. The PIER WG invites you to participate in this
effort through your response to this RFI and appreciates your
responses to the questions in the RFI as well as any other input you
would like to provide.

Renumbering can be a resource-intensive activity. It may require
that many individual computers, physically dispersed throughout an
organization, be visited by trained support staff to modify network
configuration information. Changes in the network addresses of
server may also require reconfiguration of individual computers.
These and other interdependencies between names, addresses and
services may require careful planning and coordination of address
reconfiguration to minimize disruptions in service.

1.1 Purpose of document

The PIER WG proposes to write a document that will provide
guidelines, advice and hints to network administrators who are faced
with the job of renumbering their networks. While every network is
different, network administrators can use the information in this
document to better understand the problems they may face in
renumbering and to help design and plan a renumbering strategy.

1.2 Description of document

The PIER WG will compile the information provided by vendors into a
document that includes principles, guidelines, advice and practical
experience. The intended audience will be network architects,
engineers and administrators, as well as anyone else involved in the
planning, design, implementation and operation of TCP/IP internets.
The PIER WG expects to publish the document as an informational RFC.
Because the technology and experience with renumbering will depend
and change over time, the PIER WG will maintain the document and
publish future revisions so as to guarantee the currency of the
contents. The document will be made available along with other PIER
WG documents through http://www.isi.edu:80/div7/pier/papers.html.

1.3 Vendor participation

To ensure that the end document contains the broadest possible
spectrum of information, the PIER WG invites vendors of network
software and hardware systems to submit information for publication
in the document. The responses will be edited and compiled into a
document that includes both general advice about renumbering and
specific recommendations from vendors about hardware and software
systems.

2. Motivation/Context

One strong motivation for this document is the use of route
aggregation in the Public Internet. Currently, many organizations
obtain network addresses directly from a central authority
independent of their Internet Service Provider (ISP). Route
aggregation agreements and policies will likely lead to "provider-
based addressing", in which ISPs obtain blocks of addresses which are
then assigned to the customers of that ISP. Under provider-based
addressing, an organization may be required to renumber if it decides
to switch over to a new ISP, or if its current ISP adopts a policy of
requiring use of addresses assigned to the ISP.

An organization may also need to renumber some or all of its TCP/IP
hosts when it restructures its internal network architecture. For
example, an organization may find that it needs to add a new internal
subnet to accommodate bandwidth requirements. Or, an organization
may have some hosts such as laptops, projection units on carts or
laboratory equipment that move between subnets within the internal
network. In all of these cases, the affected hosts must be
renumbered as they move among subnets.

Renumbering may affect more than just the host itself. Other hosts,
both inside and outside of the organization, that need to communicate
with the renumbered host must learn of its new network address. DNS
servers are particularly problematic, as their operation affects the
accessibility of all other hosts in an organization, and their
addresses are known to (potentially) several other DNS servers.

3. Assumptions/constraints

To better focus the responses to this RFI, this section gives some
assumptions about the internet environment and technologies that are
to be considered in support of renumbering. Constraining the
procedures in the end document according to these assumptions will
help ensure that the end document provides advice and recommendations

that are as relevant as possible to a wide audience of current
network managers.

3.1 Current technologies and practices

The recommendations to appear in this document will be based on
current and near-term technologies. The scenarios that will require
renumbering will be based on IPv4 and current policies and agreements
such as CIDR and provider-based addressing. The renumbering
strategies will be based on the use of the Dynamic Host Configuration
Protocol (DHCP), as specified in RFC1541, and current capabilities of
readily available DHCP client and server implementations (both
commercial and freely available). The strategies will also discuss
the use of the Domain Name System (DNS), but will not assume the
availability of the dynamic update extensions to DNS currently under
development. Other current technologies such as Router Discovery
will also be considered.

3.2 Scope of renumbering and automation

In general, the procedures in the end document will seek to provide a
"90% solution" in which manual intervention is minimized where
possible using current and near-term technology.

The document will not require a "flag day" cutover of all networked
devices (although such a process may be feasible in some instances);
instead, procedures will accommodate a transition period in which the
renumbered internet may operate under more than one numbering scheme.
The body of the document will discuss renumbering in an ideal
environment in which mechanisms such as DHCP are available.
Transition strategies to implement, e.g., DHCP will be discussed
separately.

In addition to renumbering host computers, the document will discuss
strategies for renumbering routers and other network infrastructure
components. Some transition strategies may depend on specific
capabilities in routers, such as the ability to define multiple IP
subnets on a single physical network segment.

3.3 Impacts of renumbering

The first impact of renumbering is the requirement to assign new IP
addresses to all of the IP hosts attached to renumbered networks. As
most contemporary IP stacks do not make any provision for the
assignment of multiple IP to a network interface, the procedures in
this document do not involve a transition period in which hosts may
be assigned more than one IP address. Thus, for any specific host,
there will be a hard transition point at which the host discards its

old IP address and begins using a new IP address. As it is unlikely
that manual assignment of addresses to hosts is feasible in any but
the simplest networks, DHCP will be proposed as the mechanism for
passing new IP addresses to hosts. Because existing transport
protocols cannot accommodate dynamic changes in IP addresses, the
procedures in this document further assume that renumbered hosts will
shutdown all existing connections and reestablish those connections
using a new IP address.

Changes to the IP address of a server not only affects that server
but also the clients of that server, which must be made aware of the
server's new IP address. Propagating a server's new address is
usually accomplished through DNS. This document will address
procedures for updating DNS records during renumbering, and will
discuss use of recently proposed updates to the DNS protocol that
accommodate dynamic updates to DNS record. The use of DHCP for
passing server addresses to IP hosts will also be discussed.

In addition to hosts - both clients and servers - all of the network
infrastructure components such as routers and bridges must be
reconfigured during renumbering. While many of these components can
be managed via management protocols such as SNMP, there are no
mechanisms available today that automatically renumber and
reconfigure infrastructure components. This document, therefore,
assumes that those components will be reconfigured manually.

4. Definitions

* Servers - provides a service at an IP address; clients have to be
            notified of a change in the address of that server
* Clients - use a service; have to be notified of changes to servers,
            servers may have to be notified for identification and
            authorization
* Hosts   - standalone; no other network infrastructure requires
            knowledge of the network address assigned to this host

5. Renumbering strategies

Section 5 of this RFI is a series of questions to guide responses to
the RFI. Individual respondents may not answer every question.
Respondents need not restrict themselves to these questions;
suggestions about other information and areas of advice are welcome.

5.1 Analyzing network requirements and designing a new numbering plan

For many network managers, developing a new numbering plan, in which

each of an organization's subnets is assigned a network number, will
be the first step in a renumbering strategy. This section asks about
the components of a numbering plan and what a network manager should
consider when developing a numbering strategy. The questions will
assume that the network manager has developed a basic internet
architecture that identifies subnets, assigns hosts to subnets and
specifies interconnections between subnets.

* What are the basic components of numbering strategy, such as
  network numbers, subnet masks, and routing infrastructure?
* What are the functional requirements of the various subnets - how
  many hosts might be attached to each subnet?
* Should the organization's internet use a private address space as
  suggested in RFC1597?
* What other requirements and specifications should be considered
  before assigning network addresses to subnets?
* When should different subnet masks be used on an organizations
  subnets; how should an appropriate mask size be selected - e.g.,
  what is an appropriate ratio of hosts to addresses within a subnet?

5.2 Issues in renumbering

The next series of questions asks about specific groups of internet
hosts or infrastructure components. Please answer these questions as
appropriate to your specific hardware or software systems.

5.2.1 Desktop personal computers

* Does your PC or Macintosh system include support for automated
  configuration mechanisms??
* How might automated allocation of IP addresses and other
  configuration information through DHCP be used in your system for
  renumbering?
* What other mechanisms for automated configuration, such as router
  discovery, does your system include?
* What actions must be coordinated with desktop system renumbering,
  such updating DHCP server configuration with new numbering plan?
* How are DNS entries updated as new IP addresses are assigned?
* What other interactions must be accommodated such as server
  authorizations based on IP addresses?

5.2.2 Server computers

* Does your server computer system include support for DHCP?
* Do you recommend automated configuration of servers?
* What manual configuration of server computers must take place in
  response to renumbering?
* What notification must clients be given when a server computer is

      renumbered?
   * What client authentication and authorization mechanisms are used?

5.2.3 Desktop UNIX computers

   * Does your desktop UNIX system include support for DHCP?
   * What other mechanisms for automated configuration, such as router
     discovery, does your system include?
   * How might automated allocation of IP addresses and other
     configuration information through DHCP be used in your system for
     renumbering?
   * What manual configuration, such as modifications to /etc/hosts,
     /etc/resolv.conf, entries in a NIS database, must be coordinated
     with renumbering?
   * What actions must be coordinated with desktop system renumbering,
     such updating DHCP server configuration with new numbering plan?
   * How are DNS entries updated as new IP addresses are assigned?
   * What other interactions must be accommodated such as server
     authorizations based on IP addresses?

5.2.4 UNIX server computers

   * Does your UNIX server system include support for DHCP?
   * Do you recommend automated configuration of UNIX servers?
   * What notification must clients be given when a server computer is
     renumbered?

5.2.5 Other computer systems

   * What specific actions must be taken to renumber other computer
     systems?

5.2.6 Manual configuration

   * When is manual configuration appropriate; what systems should be
     assigned IP addresses manually?
   * How is manual configuration coordinated with automated
     configuration mechanisms such as DHCP?

5.2.7 Other equipment - printers, etc.

   * What other network equipment such as printers, terminal servers,
     etc., do you provide or support?
   * Do these systems include support for automated configuration
     mechanisms?
   * How might automated allocation of IP addresses and other
     configuration information through DHCP be used in your system for
     renumbering?

  * What other mechanisms for automated configuration, such as router
    discovery, does your system include?

5.2.8 DNS servers

  * What steps must be taken to coordinate the renumbering of DNS
    servers with internal DNS clients?
  * What steps must be taken to coordinate the renumbering of DNS
    servers with other DNS servers within an organization?
  * What steps must be taken to coordinate the renumbering of DNS
    servers managed by other organizations?
  * What modifications must be made to the DNS database configuration
    database in response to renumbering?

5.2.9 DNS information

  * How are DNS entries - including A record, PTR record and any other
    DNS record types - updated in coordination with renumbering?

5.2.10 Other servers - NNTP, NTP, SMTP, WWW

  * Are there any special actions that must be taken when renumbering
    other servers?
  * Are there any special actions that must be taken when renumbering
    DHCP servers used to support renumbered clients?
  * Are there any specific steps that must be taken to notify other
    servers outside the organization of changes to server addresses?

5.2.11 Routers

  * Can your routers support multiple addresses and subnet masks in
    each interface, to enable a transition strategy involving
    simultaneous use of old and new network addresses?
  * What steps must be taken to change router addresses?
  * What other changes must be made to router configuration; e.g.,
    routing protocols, BOOTP/DHCP relay agents, SNMP, etc.?

5.2.12 Other network infrastructure components

  * What steps must be taken to change any addresses in bridges, hubs
    and other network infrastructure components?
  * Can other network infrastructure components support multiple
    addresses on subnets, to enable a transition strategy involving
    simultaneous use of old and new network addresses?

5.2.13 Firewalls

  * What steps must be taken to change any addresses in firewalls?

    * What steps must be taken to accommodate changing addresses of other
      renumbered devices that will forward packets through firewalls?
    * What other authentication and authorization mechanisms must be
      changed to support internally and externally initiated connections?

5.2.14 Routing protocols

    * How must devices that interact with routing protocols be
      reconfigured to accommodate new network addresses?
    * Can any routing protocols support multiple addresses on subnets, to
      enable a transition strategy involving simultaneous use of old and
      new network addresses?

5.2.15 Advertising new internal subnets to the Public Internet

    * What steps must be taken to advertise the new numbering scheme to
      the Public Internet?

5.2.16 Testing and error conditions

    * How can an organization test its renumbering plan prior to formal
      implementation?
    * How can an organization plan for problems in the renumbering
      process?
    * What pitfalls should an organization be aware of?

5.3 Renumbering implementation plans

   Because of the complex interdependencies among addresses that may be
   configured into or otherwise known to IP hosts, organizations will
   need to review their internal network architectures, their
   connections to the Public Internet and develop a systematic plan for
   graceful renumbering.

   Many factors will affect the implementation strategy for an
   organization. The scale and complexity of the organization's
   internet will determine the time scale over which renumbering can be
   implemented. The existence of services which must always be
   available implies that some network hosts cannot be restarted during
   the renumbering process. The availability of staff during non-work
   hours and the need for availability of network resources during work
   hours will determine when the renumbering can take place.

   The answers to the questions in the remainder of this section are
   intended to provide guidance to organizations as they analyze their
   network architecture and develop an implementation plan for
   renumbering.

The PIER WG has developed document soliciting case studies from
organizations that have renumbered their enterprise networks. If
your organization has recently gone through or is planning a
renumbering process, please consider documenting your experience as
requested in draft-ietf-pier-solicitation-00.

5.3.1 Network architecture

Because of the expectation that renumbering will become more frequent
in the future, organizations should consider renumbering as a key
design principle when designing a network architecture, numbering
plan and support systems.

* What factors of scale and complexity should an organization
  consider in developing an implementation plan for renumbering?
* What types of services (e.g., DNS, mail, access to Public Internet)
  are likely to be required to be available without interruption
  during renumbering?
* What technologies or capabilities will ease the renumbering process
  by allowing a transition period in which both old and new numbering
  schemes are used in parallel?

5.3.2 Support infrastructure

* What questions should an organization ask to determine if
  renumbering can take place during normal work hours?
* If the renumbering is to take place during non-work hours, what
  staff should be available to implement and support the renumbering
  process?
* What staffing issues (e.g., availability of help desk staff capable
  of solving problems caused by renumbering) should an organization
  consider?

5.3.3 Types of renumbering scenarios

* What internal network architectures are likely to be useful as
  initial models for organizations as they begin to plan for
  renumbering? For example:
  - Single network: no subnetting, probably small, one connection to
    Internet
  - Monolithic: few subnets, medium-sized, central control of all
    servers
  - Heterogeneous: many subnets, many infrastructure components,
    little central control of addresses, names, access control

5.3.4 Example renumbering transition plans

* What implementation models might an organization consider, such as:

      - Renumbering with cutover day in which every network device is
        renumbered at once.
      - Renumbering individual subnets while leaving the remainder of the
        network unchanged.
      - Renumbering with transition periods in which there are multiple
        subnets on physical networks.

5.3.5 Tools

   * What protocol or infrastructure tools can an organization use to
     reduce the effort and errors in renumbering?
   * What tools can an organization use to diagnose and repair problems
     caused by renumbering?

5.4 Transition to renumberable state

   The recommendations in this document may be based on an ideal
   operational model in which many tools, practices and other techniques
   that ease renumbering are already integrated into the organization
   network infrastructure. Many organizations may not have that
   renumbering infrastructure in place. The questions in this section
   ask about actions an organization might want to take to make their
   network infrastructure more amenable to renumbering.

   * What IP stack functions should be included in hosts (e.g., DHCP)?
   * What servers can be installed that better support renumbering
     (e.g., DHCP, dynamic DNS)?
   * What IGPs should be considered that will support transition
     renumbering strategies?
   * What other techniques and tools should be installed in anticipation
     of renumbering?

6. Security

   This Internet Draft does not address security issues.

7. Authors' Addresses

   Ralph Droms
   Computer Science Department
   323 Dana Engineering
   Bucknell University
   Lewisburg, PA 17837

   Phone: +1.717.524.1145
   E-Mail: droms@bucknell.edu

    Jack Waters
    Phill Gross
    Rob Hagens
    Peter Ford
    MCI Telecommunications Corp.
    2100 Reston Pkwy.
    Reston, VA 22091

    Phone: +1.703.715.7146 (Jack Waters)
    E-Mail: waters@mci.net (Jack Waters)