Network Working Group   R. Braden
Request for Comments: 1127   ISI
                                                           October 1989

                A Perspective on the Host Requirements RFCs

Status of This Memo

   This RFC is for information only; it does not constitute a standard,
   draft standard, or proposed standard, and it does not define a
   protocol. Distribution of this memo is unlimited.

Summary

   This RFC contains an informal summary of the discussions and
   conclusions of the IETF Working Group on Host Requirements while it
   was preparing the Host Requirements RFCs. This summary has several
   purposes: (1) to inform the community of host protocol issues that
   need further work; (2) to preserve some history and context as a
   starting point for future revision efforts; and (3) to provide some
   insight into the results of the Host Requirements effort.

1. INTRODUCTION

   A working group of the Internet Engineering Task Force (IETF) has
   recently completed and published a monumental standards document on
   software requirements for Internet hosts [RFC-1122, RFC-1123]. This
   document has been published as two RFC's: "Requirements for Internet
   Hosts -- Communication Layers", referred to here as "HR-CL", and
   "Requirements for Internet Hosts -- Application and Support",
   referred to here as "HR-AS". Together, we refer to them as the Host
   Requirements RFCs, or "HR RFCs".

   Creation of the Host Requirements document required the dedicated
   efforts of about 20 Internet experts, with significant contributions
   from another 20. The Host Requirements working group held 7 formal
   meetings over the past 20 months, and exchanged about 3 megabytes of
   electronic mail. The HR RFCs went through approximate 20 distinct
   drafts.

   This group of people struggled with a broad range of issues in host
   implementations of the Internet protocols, attempting to reconcile
   theoretical and architectural concerns with the sometimes conflicting
   imperatives of the real world. The present RFC recaps the results of
   this struggle, with the issues that were settled and those that
   remain for future work. This exegesis has several goals:

Braden   [Page 1]

     (1) to give the Internet technical community some insight into the
          results of the host requirements effort;

     (2) to inform the community of areas that need further work; and

     (3) to preserve some history and context of the effort as a starting
          point for a future revision.

1.1 GOALS OF THE HOST REQUIREMENTS RFCs

   The basic purpose of the Host Requirements RFCs is to define the
   requirements for Internet host software. However, the document goes
   far beyond a simple prescription of requirements, to include:

   (a) a bibliography of the documents essential to an implementor;

   (b) corrections and updates to the original standards RFC's;

   (c) material to fill gaps in the previous specifications;

   (d) limitations on implementation choices, where appropriate;

   (e) clarification of important issues and the intent of the
        protocols; and

   (f) documentation of known solutions to recurring problems as well
        as implementation hints.

   Broadly speaking, the Host Requirements working group started from
   the following goals for Internet host software:

   (1) Interoperability

   (2) Extensibility

   (3) Functionality

   (4) Efficiency

   (5) Architectural Purity

   Of these, interoperability was clearly preeminent, while
   architectural purity had the lowest priority. It is more difficult
   to assign relative importance to extensibility, functionality, and
   efficiency, as it varied from one topic to another.

   At a more technical level, the working group pursued a set of general
   goals that included the following:

    *   Discourage hosts from unexpectedly acting as gateways.

    *   Discourage the use of bad IP addresses.

    *   Eliminate broadcast storms.

    *   Discourage gratuitous Address Mask Reply messages.

    *   Facilitate the use IP Type-of-Service for routing and queueing.

    *   Encourage implementations of IP multicasting.

    *   Encourage TCP connection robustness.

    *   Encourage (mandate!) implementation of known TCP performance
            enhancements.

    *   Encourage user interfaces that support the full capabilities of
            the protocols.

    *   Encourage more complete implementations of FTP.

    *   Encourage robust mail delivery

    *   Discourage the source-routing of mail in the Internet.

    *   Encourage error logging.

In addition to these general technical goals, the working group
decided to discourage the use of certain protocol features: e.g., the
IP Stream Id option, ICMP Information Request and Reply messages, the
RFC-795 TOS mappings, WKS records in the Domain Name System, and FTP
Page structure.

The HR RFC tries to deal only with the software implementation, not
with the way in which that software is configured and applied. There
are a number of requirements on Internet hosts that were omitted from
the HR RFC as administrative or configuration issues.

The HR RFCs contain many, many detailed requirements and
clarifications that are straightforward and (almost) non-
controversial.

Indeed, many of these are simply restatements or reinforcement of
requirements that are already explicit or implicit in the original
standards RFC's. Some more cynical members of the working group
refer to these as "Read The Manual" provisions. However, they were
included in the HR RFCs because at least one implementation has

failed to abide by these requirements. In addition, many provisions
of the HR RFCs are simply applications of Jon Postel's Robustness
Principle [1.2.2 in either RFC].

However, not all issues were so easy; the working group struggled
with a number of deep and controversial technical issues. Where the
result was a reasonable consensus, then definite, firm
recommendations and requirements resulted. We list these settled
issues in Section 2. Section 2 also lists a number of areas where
the HR RFCs fill gaping holes in the current specifications by giving
extended discussions of particular issues.

However, in some other cases the working group was unable to reach a
crisp decision or even a reasonable consensus; we list these open
issues in Section 3. Future discussion is needed to ascertain which
of these issues really do have "right answers", and which can
reasonably be left as implementation choices. Section 4 contains
some other areas that the working group did not tackle but which need
further work outside the context of the HR RFCs (although the outcome
may be reflected in a future revision). Finally, Appendix I lists
specific issues for consideration by a future HR RFC revision effort,
while Appendix II lists the issues that are relevant to a revision of
the Gateway Requirements RFC.

It should be noted that this categorization of issues is imperfect; a
few issues appear (legitimately) in more than one category.

For brevity, we do not attempt to define all the terminology or
explain all the concepts mentioned here. For those cases where
further clarification is needed, we include (in square brackets)
references to the corresponding sections of the HR RFCs.

2. SETTLED ISSUES

Here are the areas in which the Host Requirements working group was
able to reach a consensus and take a definite stand.

-    ARP Cache Management   [CL 2.3.2.1]

     Require a mechanism to flush out-of-date ARP cache entries.

-    Queueing packets in ARP   [CL 2.3.2.2]

     Recommend that ARP queue unresolved packet(s) in the link layer.

-    Ethernet/802.3 Interoperability   [CL 2.3.3]

     Impose interoperability requirements for Ethernet and IEEE 802.3

encapsulation.

-    Broadcast Storms   [CL 2.4, 3.2.2]

     Require many provisions to prevent broadcast storms.

     In particular, require that the link-layer driver pass a flag to
     the IP layer to indicate if a packet was received via a link-
     layer broadcast, and require that this flag be used by the IP
     layer.

-    Bad IP addresses

     Include numerous provisions to discourage the use of bad IP
     addresses.

-    Address Mask Replies   [CL 3.2.2.9]

     Discourage gratuitous ICMP Address Mask Reply messages.

-    Type-of-Service

     Include various requirements on IP, transport, and application
     layers to make Type-of-Service (TOS) useful.

-    Time-to-Live   [CL 3.2.1.7]

     Require that Time-to-Live (TTL) be configurable.

-    Source Routing   [CL 3.2.1.8(e)]

     Require that host be able to act as originator or final
     destination of a source route.

-    IP Multicasting   [CL 3.3.7]

     Encourage implementation of local IP multicasting.

-    Reassembly Timeout   [CL 3.3.2]

     Require a fixed reassembly timeout.

-    Choosing a Source Address   [CL 3.3.4.3, 3.4, 4.1.3.5, 4.2.3.7]

     Require that an application on a multihomed host be able to
     either specify which local IP address to use for a new TCP
     connection or UDP request, or else leave the local address
     "wild" and let the IP layer pick one.

-       TCP Performance   [CL 4.2.12.15, 4.2.3.1-4]

        Require TCP performance improvements.

-       TCP Connection Robustness   [CL 4.2.3.5, 4.2.3.9]

        Encourage robustness of TCP connections.

-       TCP Window Shrinking   [CL 4.2.2.16]

        Discourage the shrinking of TCP windows from the right.

-       Dotted-Decimal Host Numbers   [AS 2.1]

        Recommend that applications be able to accept dotted-decimal
        host numbers in place of host names.

-       Telnet End-of-Line   [AS 3.3.1]

        Include compatibility requirements for Telnet end-of-line.

-       Minimal FTP   [AS 4.1.2.13]

        Enlarge the minimum FTP implementation.

-       Robust Mail Delivery   [AS 5.3.2, 5.3.4, 6.1.3.4]

        Recommend the use of long timeouts and of alternative addresses
        for multihomed hosts, to obtain robust mail delivery.

-       Source-Routing of Mail   [AS 5.2.6, 5.2.16, 5.2.19]

        Discourage the use of source routes for delivering mail. (This
        was one of the few cases where the working group opted for the
        architecturally pure resolution of an issue.)

-       Fully-Qualified Domain Names   [AS 5.2.18]

        Require the use of fully-qualified domain names in RFC-822
        addresses.

-       Domain Name System Required   [AS 6.1.1]

        Require that hosts implement the Domain Name System (DNS).

-       WKS Records Detracted   [AS 2.2, 5.2.12, 6.1.3.6]

        Recommend against using WKS records from DNS.

-       UDP Preferred for DNS Queries [AS 6.1.2.4, 6.1.3.2]

        Require that UDP be preferred over TCP for DNS queries.

-       DNS Negative Caching [AS 6.1.3.3]

        Recommend that DNS name servers and resolvers cache negative
        responses and temporary failures.

Finally, here is a list of areas in which the HR RFCs provide
extended discussion of issues that have been inadequately documented
in the past.

-       ARP cache handling   [CL 2.3.2.1]

-       Trailer encapsulation   [CL 2.3.1]

-       Dead gateway detection algorithms   [CL 3.3.1.4]

-       IP multihoming models   [CL 3.3.4]

        (Note that this topic is also one of the significant contentious
        issues; see the next section.)

-       Maximum transmission unit (MTU and transport-layer maximum-
        segment size (MSS) issues   [CL 3.3.2, 3.3.3, 3.4, 4.1.4,
        4.2.2.6]

-       TCP silly-window syndrome (SWS) avoidance algorithms
        [CL 4.2.3.3, 4.2.3.4]

-       Telnet end-of-line issues   [AS 3.3.1]

-       Telnet interrupt/SYNCH usage   [AS 3.2.4]

-       FTP restart facility   [AS 4.1.3.4]

-       DNS efficiency issues   [AS 6.1.3.3]

-       DNS user interface: aliases and search lists   [AS 6.1.4.3]

There are some other areas where the working group tried to produce a
more extended discussion but was not totally successful; one example
is error logging (see Appendix I below).

3. OPEN ISSUES

   For some issues, the disagreement was so serious that the working
   group was unable to reach a consensus. In each case, some spoke for
   MUST or SHOULD, while others spoke with equal fervor for MUST NOT or
   SHOULD NOT. As a result, the HR RFCs try to summarize the differing
   viewpoints but take no stand; the corresponding requirements are
   given as MAY or OPTIONAL. The most notorious of these contentious
   issues are as follows.

   -     Hosts forwarding source-routed datagrams, even though the hosts
         are not otherwise acting as gateways   [CL 3.3.5]

   -     The multihoming model   [CL 3.3.4]

   -     ICMP Echo Requests to a broadcast or multicast address
         [CL 3.2.2.6]

   -     Host-only route caching   [CL 3.3.1.3]

   -     Host wiretapping routing protocols   [CL 3.3.1.4]

   -     TCP sending an ACK when it receives a segment that appears to be
         out-of-order   [CL 4.2.2.21]

   There was another set of controversial issues for which the HR RFCs
   did take a compromise stand, to allow the disputed functions but
   circumscribe their use. In many of these cases, there were one or
   more significant voices for banning the feature altogether.

   -     Host acting as gateways   [CL 3.1]

   -     Trailer encapsulation   [CL 2.3.1]

   -     Delayed TCP acknowledgments   [CL 4.2.3.2]

   -     TCP Keep-alives   [CL 4.2.3.6]

   -     Ignoring UDP checksums   [CL 4.1.3.4]

   -     Telnet Go-Aheads   [AS 3.2.2]

   -     Allowing 8-bit data in Telnet NVT mode   [AS 3.2.5]

4.   OTHER FUTURE WORK

     General Issues:

     (1) Host Initialization Procedures

          When a host system boots or otherwise initializes, it needs
          certain network configuration information in order to communicate;
          e.g., its own IP address(es) and address mask(s). In the case of
          a diskless workstation, obtaining this information is an essential
          part of the booting process.

          The ICMP Address Mask messages and the RARP (Reverse ARP) protocol
          each provide individual pieces of configuration information. The
          working group felt that such piecemeal solutions are a mistake,
          and that a comprehensive approach to initialization would result
          in a uniform mechanism to provide all the required configuration
          information at once. The HR working group recommends that a new
          working group be established to develop a unified approach to
          system initialization.

     (2) Configuration Options

          Vendors, users, and network administrators all want host software
          that is "plug-and-play". Unfortunately, the working group was
          often forced to require additional configuration parameters to
          satisfy interoperability, functionality, and/or efficiency needs
          [1.2.4 in either RFC]. The working group was fully aware of the
          drawbacks of configuration parameters, but based upon extensive
          experience with existing implementations, it felt that the
          flexibility was sometimes more important than installation
          simplicity.

          Some of the configuration parameters are forced for
          interoperability with earlier, incorrect implementations. Very
          little can be done to ease this problem, although retirement of
          the offending systems will gradually solve it. However, it would
          be desirable to re-examine the other required configuration
          options, in an attempt to develop ways to eliminate some of them.

     Link-Layer Issues:

     (2) ARP Cache Maintenance

          "Proxy ARP" is a link-layer mechanism for IP routing, and its use
          results in difficult problems in managing the ARP cache.

          Even without proxy ARP, the management dynamics of the IP route

cache interact in subtle ways with transport-layer dynamics;
introducing routing via proxy ARP brings a third protocol layer
into the problem, complicating the inter-layer dynamics still
further.

The algorithms for maintaining the ARP cache need to be studied
and experimented with, to create more complete and explicit
algorithms and requirements.

(3) FDDI Bit-order in MAC addresses

On IEEE 802.3 or 802.4 LAN, the MAC address in the header uses the
same bit-ordering as transmission of the address as data. On
802.5 and FDDI networks, however, the MAC address in the header is
in a different bit-ordering from the equivalent 6 bytes sent as
data. This will make it hard to do MAC-level bridging between
FDDI and 802.3 LAN's, for example, although gateways (IP routers)
can still be used.

The working group concluded that this is a serious but subtle
problem with no obvious fix, and that resolving it was beyond the
scope of the HR working group.

IP-Layer Issues

(4) Dead Gateway Detection

A fundamental requirement for a host is to be able to detect when
the first-hop gateway has failed. The early TCP/IP
experimentation was based on the ARPANET, which provided explicit
notification of gateway failure; as a result, dead gateway
detection algorithms were not much considered at that time. The
very general guidelines presented by Dave Clark [RFC-816] are
inadequate for implementors. The first attempt at applying these
guidelines was the introduction of universal gateway pinging by
TOPS-20 systems; this quickly proved to be a major generator of
ARPANET traffic, and was squelched. The most widely used
implementation of the Internet protocols, 4.2BSD, solved the
problem in an extra-architectural manner, by letting the host
wiretap the gateway routing protocol (RIP). As a result of this
history, the HR working group was faced with an absence of
documentated techniques that a host conforming to the Internet
architecture could use to detect dead gateways.

After extensive discussion, the working group agreed on the
outline of an appropriate algorithm. A detailed algorithm was in
fact written down, to validate the discussion in the HR RFCs.
This algorithm, or a better one, should be tried experimentally

and documented in a new RFC.

(5) Gateway Discovery

A host needs to discover the IP addresses of gateways on its
connected networks. One approach, begun but not finished by
members of the HR working group, would be to define a new pair of
ICMP query messages for gateway discovery. In the future, gateway
discovery should be considered as part of the complete host
initialization problem.

(6) MTU Discovery

Members of the HR working group designed IP options that a host
could use to discover the minimum MTU of a particular Internet
path [RFC-1063]. To be useful, the Probe MTU options would have
to be implemented in all gateways, which is an obstacle to its
adoption. Code written to use these options has never been
tested. This work should be carried forward; an effective MTU
choice will become increasingly important for efficient Internet
service.

(7) Routing Advice from Gateways

A working group member produced a draft specification for ICMP
messages a host could use to ask gateways for routing advice
[Lekashman]. While this is not of such pressing importance as the
issues listed previously, it deserves further consideration and
perhaps experimentation.

(8) Dynamic TTL Discovery

Serious connectivity problems have resulted from host software
that has too small a TTL value built into the code. HR-CL
specifies that TTL values must be configurable, to allow TTL to be
increased if required for communication in a future Internet;
conformance with this requirement would solve the current
problems. However, configurable parameters are an operational
headache, so it has been suggested that a host could have an
algorithm to determine the TTL ("Internet diameter") dynamically.
Several algorithms have been suggested, but considerably more work
would be required to validate them. This is a lower-priority
problem than issues (4)-(6).

(9) Dynamic Discovery of Reassembly Timeout Time

The maximum time for retaining a partially-reassembled datagram is
another parameter that creates a potential operational headache.

An appropriate reassembly timeout value must balance available
reassembly buffer space against reliable reassembly. The best
value thus may depend upon the system and upon subtle delay
properties (delay dispersion) of the Internet. Again, dynamic
discovery could be desirable.

(10) Type-of-Service Routing in Hosts

As pointed out previously, the HR RFCs contain a number of
provisions designed to make Type-of-Service (TOS) useful. This
includes the suggestion that the route cache should have a place
or specifying the TOS of a particular route. However, host
algorithms for using TOS specifications need to be developed and
documented.

(11) Using Subnets

An RFC is needed to provide a thorough explanation of the
implications of subnetting for Internet protocols and for network
administration.

Transport-Layer Issues:

(12) RST Message

It has been proposed that TCP RST (Reset) segments can contain
text to provide an explicit explanation of the reason for the
particular RST. A proposal has been drafted [CLynn].

(13) Performance Algorithms

HR-CL contains a number of requirements on TCP performance
algorithms; Van Jacobson's slow start and congestion avoidance,
Karn's algorithm, Nagle's algorithm, and SWS prevention at the
sender and receiver. Implementors of new TCPs really need more
guidance than could possibly be included in the HR RFCs. The
working group suggested that an RFC on TCP performance is needed,
to describe each of these issues more deeply and especially to
explain how they fit together.

Another issue raised by the HR RFCs is the need for validation (or
rejection) of Van Jacobson's fast retransmit algorithm.

Application-Layer Issues:

(14) Proposed FTP extensions

A number of minor extensions proposed for FTP should be processed

and accepted or rejected. We are aware of the following
proposals:

(a) Atomic Store Command

     The FTP specification leaves undefined the disposition of a
     partial file created when an FTP session fails during a store
     operation. It was suggested that this ambiguity could be
     resolved by defining a new store command, Store Atomic (STOA).
     The receiver would delete the partial file if the transfer
     failed before the final data-complete reply had been sent.
     This assumes the use of a transfer mode (e.g., block) in which
     end-of-file can be distinguished from TCP connection failure,
     of course.

(b) NDIR Command

     "NDIR would be a directories-only analogue to the NLST command.
     Upon receiving an NDIR command an FTP server would return a
     list of the subdirectories to the specified directory or file
     group; or of the current directory if no argument was sent.
     ... The existing NLST command allows user FTPs to implement
     user-interface niceties such as a "multiple get" command. It
     also allows a selective (as opposed to generative) file-naming
     user interface: the user can pick the desired file out of a
     list instead of typing its name." [Matthews]

     However, the interface needs to distinguish files from
     directories. Up to now, such interfaces have relied on a bug
     in many FTP servers, which have included directory names in the
     list returned by NLST. As hosts come into conformance with
     HR-AS, we need an NDIR command to return directory names.

(c) Adaptive Compression

     It has been suggested that a sophisticated adaptive data
     compression algorithm, like that provided by the Unix
     "compress" command, should be added as an alternative FTP
     transfer mode.

(15) SMTP: Global Mail Addressing

   While writing requirements for electronic mail, the working group
   was urged to set rules for SMTP and RFC-822 that would be
   universal, applicable not only to the Internet environment but
   also to the other mail environments that use one or both of these
   protocols. The working group chose to ignore this Siren call, and
   instead limit the HR RFC to requirements specific to the Internet.

However, the networking world would certainly benefit from some
global agreements on mail routing. Strong passions are lurking
here.

(16) DNS: Fully Replacing hosts.txt

As noted in HR-AS [AS 6.1.3.8], the DNS does not yet incorporate
all the potentially-useful information included in the DDN NIC's
hosts.txt file. The DNS should be expanded to cover the hosts.txt
information. RFC-1101 [RFC-1101] is a step in the right
direction, but more work is needed.

5. SUMMARY

We have summarized the results of the Host Requirements Working
Group, and listed a set of issues in Internet host protocols that
need future effort.

6. REFERENCES

[RFC-1122] Braden, R., Editor, "Requirements for Internet Hosts --
Communications Layers", RFC 1122, IETF Host Requirements Working
Group, October 1989.

[RFC-1123] Braden, R., Editor, "Requirements for Internet Hosts --
Application and Support", RFC 1123, IETF Host Requirements Working
Group, October 1989.

[RFC-1009] Braden, R., and J. Postel, "Requirements for Internet
Gateways", RFC 1009, USC/Information Sciences Institute, June 1987.

[RFC-1101] Mockapetris, P., "DNS Encoding of Network Names and Other
Types", RFC 1101, USC/Information Sciences Institute, April 1989.

[RFC-1063] Mogul, J., C. Kent, C. Partridge, and K. McCloghrie, "IP
MTU Discovery Options", RFC-1063, DEC, BBN, & TWG, July 1988.

[RFC-816] Clark, D., "Fault Isolation and Recovery", RFC-816, MIT,
July 1982.

[CLynn] Lynn, C., "Use of TCP Reset to Convey Error Diagnostics",
Internal Memo, BBN, December 1988.

[Lekashman] Message to ietf-hosts mailing list from John Lekashman,
14 September 1988.

[Matthews] Message to Postel from Jim Matthews, 3 August 1989.

APPENDIX I -- ISSUES FOR FUTURE REVISION

   In order to complete the HR RFCs, it was necessary to defer some
   technical issues. These issues should be considered by the parties
   responsible for the first update of the HR RFCs.

   The issues pending at the time of publication are listed here, in
   order by protocol layer.

   General Issue:

      Error Logging

      The working group felt that more complete and explicit guidance on
      error logging procedures is needed than is presently contained in
      Section 1.2.3 (both HR RFCs).

   Link Layer Issues:

   -    Stolen IP Address

      How should a host react when it detects through ARP traffic that
      some other host has "stolen" its IP address?

   IP Layer Issues:

   -    "Raw Mode" Interface

      HR-CL could define an optional "raw mode" interface from the
      application layer to IP.

   -    Rational Fragmentation

      When a host performs intentional fragmentation, it should make the
      first fragment as large as possible (this same requirement should
      be placed on gateways).

   -    Interaction of Multiple Options

      HR-CL does not give specific rules for the interactions of
      multiple options in the same IP header; this issue was generally
      deferred to a revision of the Gateway Requirements RFC. However,
      this issue might be revisited for hosts.

   -    ICMP Error for Source-Routed Packet

      It was suggested that when a source-routed packet arrives with an
      error, any ICMP error message should be sent with the

corresponding return route. This assumes that the ICMP error
message is more likely to be delivered successfully with the
source route than without it.

-    "Strong" IP Options and ICMP Types

The HR RFCs takes the general approach that a host should ignore
whatever it does not understand, so that possible future
extensions -- e.g., new IP options or new ICMP message types --
will cause minimum problems for existing hosts. The result of
this approach is that when new facilities are used with old hosts,
a "black hole" can result. Several people have suggested that
this is not always what is wanted; it may sometimes be more useful
to obtain an ICMP error message from the old host. To quote
Jeremey Siegel:

   "The basic premise is that if an option is to have any real
   meaning at all within an '[upward] compatible' environment, it
   must be known whether or not the option actually *carries* its
   meaning. An absurd analogy might be programming languages: I
   could make a compiler which simply ignored unknown sorts of
   statements, thereby allowing for future expansion of the
   language.

   Right now, there are four "classes" of options; only two are
   defined. Take one of the other classes, and define it such
   that any options in that class, if unrecognized, cause an ICMP
   error message. Thus anyone who wants to propose a "strong"
   option (one which requires full participation by all systems
   involved to operate correctly) can assign it to that class.
   Options in the current classes may still be passed through if
   they are unknown; only "weak" options will be assigned to these
   classes in the future."

-    Network Mask

As explained in HR-CL [CL 3.1.2.3], we believe that a possible
future transition for the interpretation of IP addresses may be
eased if hosts always treat an IP address as an indivisible 32-
bit number. However, there are various circumstances where a host
has to distinguish its own network number. Charlie Lynn has
suggested that indivisibility can be retained if a host is
configured with both an address mask (indicating subnetting) and a
network mask (with network but not subnet bits).

-    WhoAmI Query

The following requirement is needed: for a multihomed host, a

UDP-based application should (must?) be able to query the
communication layers to obtain a list of all local IP addresses
for the host.

-    New Destination Unreachable codes

For each of the new ICMP Destination Unreachable codes defined in
HR-CL [CL 3.2.2.1], it should be documented whether the error is
"soft" or "hard".

-    ICMP Error Schizophrenia

Section 3.3.8 of HR-CL requires a host to send ICMP error
messages, yet in nearly all individual cases the specific
requirements say that errors are to be silently ignored. The
working group recognized this contradiction but was unwilling to
resolve it.

At every choice point, the working group opted towards a
requirement that would avoid broadcast storms. For example, (1)
ICMP errors cannot be sent for broadcasts, and also (2) individual
errors are to be silently ignored. This is redundant; either
provision (1) or (2) alone, if followed, should eliminate
broadcast storms. The general area of responses to errors and
broadcast storms could be reassessed and the individual decisions
reviewed.

Transport-Layer Requirements:

-    Delayed ACK Definition

A more precise and complete definition of the conditions for
delaying a TCP ACK segment may be desirable; see Section 4.2.3.2
of HR-CL.

Telnet Requirements:

-    Flushing Output

The DISCUSSION in Section 3.2.4 of HR-AS concerns three possible
ways for a User Telnet to flush output. It would be helpful for
users and implementers if one of these could be recommended over
the others; however, when the working group discussed the matter,
there seemed to be compelling arguments for each choice. This
issue needs more study.

-    Telnet LineMode Option

     This important new option is still experimental, but when it
     becomes a standard, implementation should become recommended or
     required.

  FTP Requirements:

-    Reply Codes

  A number of problems have been raised with FTP reply codes.

  (a) Access Control Failures

     Note that a 550 message is used to indicate access control
     problems for a read-type operation (e.g., RETR, RNFR), while a 553
     message is used for the same purpose for a write-type operation
     (e.g., STOR, STOU, RNTO).

     LIST, NLST, and STAT may fail with a 550 reply due to an access
     control violation.

     MKD should fail with a 553 reply if a directory already exists
     with the same name.

  (b) Directory Operations (RFC-959 Appendix II)

     An RMD may result in a 450 reply if the directory is busy.

     Many of the reply codes shown in the text of Appendix II are
     wrong. A positive completion for CWD should be 250. The 521 code
     shown for MKD should be 553 (see above), while the 431 shown for
     CWD should be a 550.

  (c) HELP and SITE Commands

     The positive completion reply to a HELP command should be code
     214.

     HELP or SITE with an invalid argument should return a 504 reply.

-    Bidirectional FTP

     The FTP specification allows an implementation in which data
     transfer takes place in both directions simultaneously, although
     few if any implementations support this. Perhaps HR-AS should
     take a stand for or against this.

SMTP Requirements:

-    Offline SEND

     Some on the working group felt that the SMTP SEND command,
     intended to display a message immediately on the recipient's
     terminal, should produce an error message if delivery must be
     deferred.

-    Header-like Fields

John Klensin proposed:

     "Header-like fields whose keywords do not conform to RFC822 are
     strongly discouraged; gateways SHOULD filter them out or place
     them into the message body. If, however, they are not removed,
     Internet hosts not acting as gateways SHOULD NOT utilize or
     inspect them. Hence address-like subfields of those fields SHOULD
     NOT be altered by the gateway."

-    Syntax of Received: Line

     The precise syntax of a revised Received: line (see Section 5.2.8
     of HR-AS) could be given. An unresolved question concerned the
     use of "localhost" rather than a fully-qualified domain name in
     the FROM field of a Received: line. Finally, new syntax was
     proposed for the Message Id field.

Appendix II -- Gateway Issues

   The working group identified a set of issues that should be
   considered when the Gateway Requirements RFC [RFC-1009] ("GR RFC") is
   revised.

-    All-Subnets Broadcast

     This facility is not currently widely implemented, and HR-CL warns
     users of this fact. The GR RFC should take a stand on whether or
     not gateways ought to implement the necessary routing.

-    Rational Fragmentation

     When a gateway performs intentional fragmentation, it should make
     the first fragment as large as possible.

-    Illegal Source Address

     It has been suggested that a gateway should not forward a packet

containing an illegal IP source address, e.g., zero.

-    Option Processing

     Specific rules should be given for the order of processing
     multiple options in the same IP header. Two approaches have been
     used: to process options in the order presented, or to parse them
     all and then process them in some "canonical" order.

     The legality should also be defined for using broadcast or
     multicast addresses in IP options that include IP addresses.

Security Considerations

   A future revision of the Host Requirements RFCs should incorporate a
   more complete discussion of security issues at all layers.

Author's Address

   Robert Braden
   USC/Information Sciences Institute
   4676 Admiralty Way
   Marina del Rey, CA 90292-6695

   Phone: (213) 822 1511

   EMail: Braden@ISI.EDU