              Response to Critiques of the Proposed Mail Protocol

   A number of people have responded to my proposal for a Mail Protocol
   (JEW RFC 524 -- 17140,2:y). In the current RFC, I've attempted to
   collect and respond to the questions, complaints, and suggestions
   that various individuals in the Network community have offered. I
   intend to critique myself in a forthcoming RFC.

   I hope that dialog on the protocol proposal will continue, and that
   others will join in the discussion. I will respond via RFC to any
   additional critiques I receive (I hope there'll be many).

I. QUESTIONS

   HOW DOES THE SERVER VERIFY AN ID?

      References:

         (DHC JBP RFC 539 -- 17644,3g:gy)

      Discussion:

         One postulates the existence of AT LEAST ONE host whose Mail
         server process implements the User Verification Function (JEW
         RFC 524 -- 17140,5f7:gy). Any process can contact that server,
         give him the name of any Individual in the Net and a test Id,
         and the server will determine whether or not the Individual and
         Id agree.

            The NIC, for one, will without question provide this
            service.

         With such support available to it, ANY FTP server process can
         then require (of any or all user processes that contact it) an
         ID command wherever it wishes within the user-server
         interchange (within the constraints of the Protocol). The
         server simply prompts for the Id, gets it, opens a connection
         to the User Verification Agent, presents to it the Individual's
         name and purported Id, receives a positive or negative
         response, and deals with the original user process accordingly.

Example:

     Suppose a user process opens a connection to UCLA-NMC's
     server process, invokes the Delivery function, and in the
     course of the interchange identifies the Author as Roberts
     at USC-ISI.

     The implementors at UCLA-NMC's server process chose to
     require proof, in all Delivery transactions, that the Author
     is who he claims he is. It therefore prompts for an Id in
     response to the AUTHOR command from the user process, and
     receives in return the command 'ID arpawheel <CA>'.

     UCLA-NMC's server then connects to the NIC's server, invokes
     the User Verification function there, specifying 'REQUESTOR
     roberts @ usc-isi <CA>' and 'ID arpawheel <CA>'. The NIC
     informs UCLA-NMS that the Id is incorrect.

     UCLA-NMC then rejects the original ID command.

Of course, the Protocol does not require that a server demand
Ids from users that contact it. Servers who choose not to
require proof of identity simply never prompt for ID commands,
and treat any they receive as NOPs. For such implementations
(which represent the current, FTP mail protocol situation), no
third-part interchanges are ever required.

Each user in the Net has a single Id that he uses throughout
the Net for purposes of sending and receiving mail. That Id
need not (but may, either coincidentally or by design) have any
other use. In particular, a user's Id is independent of the
passwords by which he gains access to accounts that he might
possess on hosts around the Net.

     Of course, a user could and might see to it that his
     passwords and Id are the same. The NIC, for example, might
     require that a user log in to its system with NIC ident and
     Id, rather than with host name and password, as it does
     currently.

I emphasize again that Ids have nothing whatsoever to do with
accounting. UCLA-NMC doesn't force the Author to prove his
identity so UCLA has someone to whom it can bill the resources
consumed in processing the Delivery transaction. It does so to
prevent Jim White from authoring a piece of mail and claiming
that Larry Roberts wrote it.

UCLA-NMC does have the option of requiring that a user
process log in before it delivers mail so that it can be
billed for the resources it uses. The appropriate commands
to require of the user process are USER, PASS, and ACCT.
But, the billing process is separable from that of
identifying Author, Clerk, etc.

The NIC, for example, in its role as a Distribution Agent,
might establish an account at UCLA-NMC to use whenever it
delivers mail there. UCLA-NMC will bill ALL of the NIC's
activity at UCLA to that account. But when the NIC delivers
a piece of mail it claims was authored by Larry Roberts,
UCLA-NMC may still wish to verify that claim. Hence the ID
command.

ACK, PROGRESS REPORT, OR REPLY WITH NO REFERENCE SERIAL NUMBER

References:

(DHC JBP RFC 539 -- 17644,3h:gy)

Discussion:

A Delivery of type POSITIVE or NEGATIVE ACKNOWLEDGMENT,
PROGRESS REPORT, or REPLY requires a Reference Serial Number of
the user process. Should the server determine that one is
lacking when the final EXIT command is given, he should reject
the EXIT command with an appropriate error response.

The same applies in the Distribution function: a Reference
Serial Number MUST be specified if the Delivery Type is
REPLY.

The Protocol document is deficient in that it doesn't state the
above.

II. COMPLAINTS

TERMINATING BOTH THE SUBSYSTEM AND FUNCTIONS WITH EXIT

References:

(AAM -- 17404,)

Discussion:

I have no objection to defining two terminating commands, one
to exit a function, the other to exit the subsystem. I guess
I'd suggest defining a command 'GO <CA>' to be used to
terminate a function.

I don't believe, however, that's it's necessary to distinguish
the two cases to avoid confusion by human users.

Even though the command language is ASCII, rather than binary,
and even though I've adopted Mike Padlipsky's concept of a
Unified USER Level Protocol', I don't consider that MP is a
protocol for direct use by humans (although nothing can STOP a
human user from speaking MP if he has access to a TELNET user
program and is determined to do so).

The concept I mean to extract from the UULP and exploit is its
model of a single process with many subsystems, not its
philosophy of a Network-standard command language for use by
human users (the latter may be a good idea, too, but it's not
the one I'm concerned with at the moment).

I don't think that designing a protocol to govern an exchange
between processes is the same task as designing a protocol to
mediate a conversation between a process and a human user.
Using ASCII commands suggests (as it did for FTP, RJE, etc.)
that the latter problem is the one being addressed; it's not.

  USING TELNET GO AHEAD TO TERMINATE CERTAIN COMMANDS

References:

(AAM -- 17404,)

(RCC -- 17822,1a:gy)

(DHC JBP RFC 539 -- 17644,3b:gy)

Discussion:

Agreed. My mistake.

I simply have a strong distaste for the current FTP convention
of terminating commands whose argument may itself contain CR LF
with 'CR LF . CR LF'. That seems a little extravagant to me.
Personally, I'd prefer a single NVT character as a delimiter.

<CA2> only terminates two MP commands (COMMENTS and TEXT).
Some NVT character (ESC? EXT? ...) can easily be chosen that
need not appear (and can therefore be prohibited from appearing
by the Protocol) in the argument to either of those commands.

SUBSYSTEM OR SEPARATE RJE-LIKE SERVER PROCESS

References:

(DHC JBP RFC 539 -- 17644,4a:gy)

(AAM -- 17404,)

(ADO RFC 552 -- 17809,3:y)

Discussion:

There are two separable issues here:

   (1) Server Process Proliferation of Not?

        If the consensus of the Network community is that
        Padlipsky's UULP approach to protocol design and
        implementation is in fact superior to the current scheme,
        which calls for the implementation of each new Network
        protocol as a distinct server process with its own
        contact socket, then we should begin to embrace that
        concept and begin reshuffling existing protocol
        implementations accordingly. Even more surely, NEW
        protocols (like MP), should be designed in accordance
        with the new standards, not the old.

        I think Buz Owen's suggestion (ADO RFC 552 -- 17809,3:y)
        -- that a skeletal UULP be defined, a socket assigned to
        server processes which implement it, and MP defined as a
        subsystem under it -- is excellent. I retract my
        suggestion (JEW RFC 524 -- 17140,3a2:gy) in favor of
        Owen's.

        I further suggest that the latest revision of FTP (NJN
        RFC 542 -- 17759,) be similarly implemented (i.e., as a
        UULP subsystem), rather then implemented temporarily
        under a new socket and later moved over to socket 3 as
        suggested in RFC 542.

(2) RJE's model for FTP Use or Not?

If both MP (as currently defined) and RJE were instated
as UULP subsystems, they would still embrace different
philosophies regarding their use of FTP. As the person
who proposed and fought for the current RJE model (i.e.,
to its use of FTP), I (still) believe it to be an
elegant one, more elegant by far then the one I've
proposed for MP.

An alternative I considered and discarded SOLELY for
reasons of efficiency (neglecting, perhaps, the issue of
cleanness of implementation), is that the command
currently defined as 'FILE <CA>' (JEW RFC 524 --
17140,4q2a:gy), both in specifying Content and in the
Citation Retrieval function, be 'FILE <fileaddr> <CA>'
instead.

    The server is then obliged to retrieve the Content of
    the Mail from the designated server process via a
    third-party exchange.

The redefined FILE command would be similar to the
LOCATION command, except that the former would specify
JUST Content (and none of the other Static Attributes),
and that the Server must retrieve the file (which may be
a temporary file created by the user process) in real
time, i.e. BEFORE it sends its response to the FILE
command.

This alternative eliminates the need to borrow the BYTE,
SOCK, PASV, TYPE, STRU, MODE, REST, and SITE commands
from FTP (JEW RFC 524 -- 17140,7c1:gy). It also allows
the user process the flexibility of specifying a file at
a host other than his own.

After some thought, I think I agree with Crocker and
Postel that theirs is the better implementation.

    As they point out, however, this implementation
    introduces the problem of somehow reconciling the
    desire to permit (in general) the transfer of mail
    files without requiring a login, with a server's
    inability to distinguish that case from the general
    case of file retrieval (for which many hosts will
    require a login).

USE OF THE DATE FORM 1/2/73 (JAN 2 OR FEB 1?)

    References:
      (RCC -- 17822,1b)
    Discussion:
      Agreed.

ORDER OF PARAMETER SPECIFICATION

    References:

    (DHC JBP RFC 539 -- 17644,31:gy)

    Discussion:

    The Protocol does not, as Crocker and Postel state, impose an
    order upon command specification within a function (see for
    example, JEW RFC 524 -- 17140,5f1b:gy).

    Having considered their suggestion only briefly, it does seem
    to me appropriate to impose some constraints on the order of
    parameter specification by the user. Off hand, the order
    suggested -- Dynamic, Optional, Static -- seems good.

III. SUGGESTED ADDITIONS

  FORWARDING AT DELIVERY TIME

    References:

    (DHC JBP 539 -- 17644,4b:g)

    Discussion:

    Including provision for the forwarding of mail at Delivery Time,
    in contrast to sometime after Delivery in response to a specific
    Forward request (i.e., function), seems to me a useful addition to
    the Protocol.

    As Crocker and Postel note, only one of the three mechanisms for
    such forwarding bears upon the Protocol (although the Protocol
    might mention the other two and either encourage or discourage
    their use).

    I suggest the following reply format, however, rather than the one
    suggested by Crocker and Postel (DHC JBP RFC 539 --
    17644,4b3c2:gy):

476 <localname> -- is his location.

DEFAULT SIGNATURE SHOULD BE THE AUTHOR

References:
   (DHC JBP 539 -- 17644,3c:gy)
Discussion:
   Agreed.

LEVELS OF INTERRUPT

References:

(DHC JBP 539 -- 17644,3d:gy)

Discussion:

   I see no value to defining numeric shades of urgency,
   unless the Protocol suggests some particular action the
   server might take in response to each one.

   The whole notion of flagging some pieces of mail as
   urgent seems to me useless unless the MP server process
   (not the human recipient) takes some kind of special
   action for urgent mail, BEFORE the human recipient
   would otherwise be apt to read the mail. If one
   accepts that argument, there's clearly no point to
   defining shades of urgency if they have meaning only to
   the human recipient. True, any pair of human users
   could privately agree on meanings, but it seems to me
   preferable to define those meanings formally or not at
   all.

WARNING THE SERVER OF THE SIZE OF MAIL

References:
   (DHC JBP RFC 539 -- 17644,3f:gy)
Discussion:
   Agreed. Further suggestions as to the implementation?

DISCOURAGING SERVERS FROM REQUIRING LOGINS

References:
   (DHC JBP RFC 539 -- 17644,3j:gy)
Discussion:
   Agreed. This is not a new issue.

IV. META-COMMENTS

   SIZE OF THE PROTOCOL DOCUMENT

      References:

         (RCC -- 17822,1e:gy)

      Discussion:

         I offer an apology for the format of the the Protocol document.
         It differs radically from that of previous Protocol documents
         (e.g., FTP, RJE), and is certainly not tutorial in its
         orientation. The glossary is a device I found useful in
         designing the Protocol. If the substance of the Protocol were
         agreed upon, then friendlier documentation would have to be
         written. The choice of approach was greatly affected by my own
         time constraints.

         As I find time, I would like to define the minimum
         implementation subsets that Clements requests. For the moment,
         consider the command breakdown below. It represents the case
         where the server permits only the function by which mail is
         delivered to users in his host. It has the following
         attributes:

            (1) It supports all of the functions of the current FTP mail
            protocol. In addition,

            (2) It makes specification of author and title explicit,
            avoiding the current problem of multiple headers (one
            supplied by the server, the other embedded by the user in
            the text of the message),

            (3) It allows the text of the message to reside at a third
            host, and

            (4) It permits multiple recipients.

         The breakdown is the following:

            COMMANDS THAT MUST BE IMPLEMENTED
            (Author and Title could be treated as NOPs)

               To enter the Mail subsystem:
                  MAIL <CA>
               To invoke the Delivery function:
                  DELIVER <CA>

```
    To specify the text of the message:
        FILE <CA>
        LOCATION <fileaddr> <CA>
        TEXT <string> <CA2>
    To identify author(s), recipient(s), and title:
        AUTHOR <individual> <CA>
        RECIPIENT <individual> <CA>
        TITLE <title> <CA>
    To exit the function or subsystem:
        ABORT <CA>
        EXIT <CA>


COMMANDS THAT CAN BE TREATED AS NOPS
(they can legally appear in the Delivery function)

    ACCESS <individual> <CA>
    ACCESSTYPES <accesstypes> <CA>
    CATALOG <catalog> <CA>
    CLERK <individual> <CA>
    COMMENTS <comments> <CA2>
    CREATIONDATE <datetime> <CA>
    DELIVERYTYPE <deliverytype> <CA>
    DISPOSITION <disposition> <CA>
    GENERALDELIVERY <CA>
    GREETING <greeting> <CA>
    ID <id> <CA>
    REFERENCESERIAL <serialnumber> <CA>
    SERIAL <serialnumber> <CA>
    SIGNATURE <signature> <CA>


COMMANDS THAT NEEDN'T BE RECOGNIZED
(they cannot legally appear in the Delivery function)

Commands that invoke unsupported functions:

    DISTRIBUTE <CA>
    FORWARD <CA>
    RECORD <CA>
    RETRIEVE <CA>
    UPDATE <CA>
    VERIFY <CA>


Miscellaneous parameter specification commands:

    ACKCONDITION <ackcondition> <CA>
    ACKTYPE <acktype> <CA>
    CITATIONTEMPLATE <citationtemp> <CA>
    CUTOFF <interval> <CA>
```

```
              FORWARDEE <individual> <CA>
              MONITOR <individual> <CA>
              PATHNAME <pathname> <CA>
              REPORTINTERVAL <interval> <CA>
              REQUESTOR <individual> <CA>
              UPDATETYPE <updatetype> <CA>
```

CA AND CA2 NOT EXPLAINED SOON ENOUGH

      References:
         (DHC JBP RFC 539 -- 17644,3a:gy)
      Discussion:
         Agreed.

CHANGE 'INTERRUPT' TO 'URGENT' OR 'PRIORITY'

      References:
         (DHC JBP RFC 539 -- 17644,3e:gy)
      Discussion:
         Agreed.
         How about 'URGENT'.

CARRY STATIC/DYNAMIC ATTRIBUTE DISTINCTION INTO FORMAL SYNTAX

      References:
         (DHC JBP RFC 539 -- 17644,3i:gy)
      Discussion:
         Agreed.

CRYPTIC DEFAULT DESCRIPTIONS

      References:
         (DHC JBP RFC 539 -- 17644,3k:gy)
      Discussion:
         Agreed.

       [This RFC was put into machine readable form for entry]
       [into the online RFC archives by Sergio Kleiman 12/99]
```