                   REMOTE WRITE PROTOCOL - VERSION 1.0

Status of this Memo

1. Background

   It is often convenient to use electronic communication somewhat
   lighter than electronic mail. Sometimes even the use of the talk(1)
   *) program seems like overkill. We like to offer to user something
   like UNIX **) command write(1) ***) except that it can also pass
   messages through the network instead of the single host.

   There have been few programs offering this kind of service, but they
   have either based on SUN-RPC protocol or used a strictly undocumented
   protocol.

   This document describes a simple Remote Write Protocol (RWP) that
   should have been documented at least 10 years ago. But late is
   better than never. Version number of the RWP protocol in this
   document is 1.0.

2. Overview

   RWP is a simple protocol that can be used to relay short messages
   through the network to other users. RWP looks pretty much like
   Simple Mail Transfer Protocol (SMTP) ****) though it is a bit more
   complicated due to the interactive nature of the RWP session.

   The idea behind the RWP session is that client program that is
   relaying message to the host in which the target user is logged in
   opens the tcp or udp connection to the server program running in the
   target machine Then the client gives the sender's and recipient's
   identification (usually login ids), actual message body and tells the
   server to deliver a message to the user. On tcp-connection server
   returns a status from each action taken. On udp-connection no
   responses are sent. RWP sessions through udp are implemented to
   support message broadcasting.

Rinne   [Page 1]

Message delivering methods are not defined within this document, but
the basic method could be a simple write to users terminal. This is
basically what UNIX command write(1) does. Depending on server
implementation, the delivery method could be configurable personally
by each user.

3. Description

Server program answers to each command submitted by a response. All
responses have two parts: three number unique response code and a
short textual explanation of the response. Also whenever the server
is ready to accept new commands a notification is submitted to the
client.

There are three kinds of commands in RWP. The first group is for
querying a status of the server. The second group is actual message
handling commands and the last set of commands are for RWP session
control.

When the server is ready to receive a command from the client, it
sends a message code 100 to the client. This message is for example
as follows:

            100 Ready.

 Server commands are as follows:

 Status Query

    HELP   Gives a short help message that contains legal
            RWP commands. Help lines have code 510. Example RWP
            implementation *****) gives a following response to
            HELP command:

                510 Valid commands are:
                510   BYE,   DATA,   HELP,   HELO,
                510   RSET,   SEND,   PROT,   QUIT,
                510   VRFY,   VER
                510   FROM senderlogin
                510   FHST senderhost
                510   TO   recipentlogin [tty]
                510   FWDS current_hop_count

    HELO   Says hello to the server. Server response to HELO
            command has code 500. For example:

                500 Hello remote.host. This is local.host speaking.

        PROT   Asks the RWP protocol version from the server.
                  Response code to PROT command is 502. Protocol
                  version described in this document is RWP 1.0 and the
                  response is as follows:

                      502 RWP version 1.0.

        VRFY   After the recipient of the message is set by to command
                  described later, the possibility of message delivery
                  can be queried by VRFY command. If message can be
                  delivered the response code is 108. If message is
                  about to be forwarded the response code is 110 and
                  message is either form:

                      110 Recipient ok to forward.

                  or if the server can tell the destination of the
                  forwarding:

                      110 Recipient ok to forward <user@host.domain>.

                  Other possible response codes are 669, 670, 671, 674
                  and 677 and they all indicate that message delivery is
                  by one way or another currently impossible.
                  Description of the codes is later in this document.

                  After the SEND command the server may also give
                  autoreply from the remote user before the actual
                  response code. Autoreply lines are ones of code 300.

        VER   Asks the version of the server program. Response code
                  to VER command is 501 and the textual part of the
                  response is the name and the version number of the RWP
                  server, for example:

                      501 Rwrited version 1.0.

    Message Handling:

        FROM senderlogin
                  Tells the server the identification information of the
                  sender of the message. Usually this id information is
                  user's login id. Response code to successful FROM
                  command is 105, for example:

                      105 Sender ok.

     TO recipentlogin [tty]
             Tells the server the identification information of the
             intended recipient of the message. Usually this id
             information is user's login id. If tty is submitted,
             the message is delivered to that tty. If tty is
             submitted between brackets '[]' the tty given is
             treated as a hint only. Response code to successful
             TO command is 106.

     FHST original.host [forwarder1.host forwarder2.host ...]
             Tells the server the host name that the message
             originates to and the path of the hosts that has
             forwarded the message. The host name of the machine
             that is currently submitting the message to the server
             should not be in the path list.

             This information is relevant if message is forwarded
             and it is not originally coming from the host that is
             forwarding it. Response code to successful FHST
             command is 111.

     DATA   Tells the server to start receive the body of the
             message. Response code to DATA command is 200, for
             example:

             200 Enter message. Single dot '.' on line terminates.

             After response 200 the message lines are submitted to
             the server one after another. Message is terminated
             by the line that contains a single dot '.'. The
             termination of the message is acknowledged by the
             server with the response code 107. Server does not
             notify client about receiving the single message
             lines. If empty message is submitted (i.e. single dot
             is on the first line) the response code is 672 and
             DATA command only cancels possible previous DATA
             command. Because of this all dots or at least dots
             that are standing alone in the line have to be quoted.

     SEND   Sends the message. If commands FROM, TO and DATA are
             successfully given before SEND command, the message is
             delivered to the target user. If delivery is
             successful the response code is 103. If message is
             not delivered directly to the target user but instead
             forwarded to another host the response code is 104.
             Response codes 669, 670 and 671, 677 indicate an error
             on message delivery and codes 673, 674, 675 indicate
             that either command FROM, TO or DATA has not been

                    successfully given before SEND command. After the
                    SEND command the server may also give autoreply from
                    the remote user before the actual response code.
                    Autoreply lines are ones of code 300.

        FWDS n   Tells the server that message has been forwarded n
                    times. If the server forwards the message to the
                    another server, it increments the counter and tells
                    the remote server the current count of forwards.
                    Response code to the FWDS command is 110 if n is less
                    than the server specific forward limit. If this limit
                    is exceeded the response code is 676. If the response
                    code is 676 the client can either quit the session and
                    fail the message or it can give the message to the
                    server despite the fact that the forward limit is
                    exceeded. If the message is given when forward limit
                    is exceeded, the server tries to deliver it, but does
                    not forward it to another server. If forward count is
                    given as -1, the message is considered as a autoreply
                    and never forwarded.

    Session Control:

        RSET   Resets the RWP session. FROM, TO and DATA -commands
                    that are given before are canceled and they have to
                    be given again before SEND command can be used. Also
                    possible FWDS and FHST commands are canceled.

        BYE   Terminates the RWP session. Server gives a response
                    code 101 and closes the connection.

        QUIT   Is the synonym to bye, but it's a lot more impolite.
                    Response code is however 101 as in bye.

    Server specific command:

        QUOTE command

                    Relay a command to the server. If the QUOTE command
                    is successfully completed response code 112 is
                    returned. If QUOTE command is failed the response
                    code is 678. If RWP server doesn't recognize the
                    given QUOTE command the response code is 679.

                    Currently reserved QUOTE commands are AGENT, CHARSET,
                    IDENT, KEY and KEYID.

4. Response Codes

   Here are all legal response codes of RWP server followed by short
   textual explanation. Only the numeral codes are important and texts
   can contain practically anything, however in response code 110 there
   is possibly useful information between '<' and '>' characters. No
   characters '<' or '>' should be present in other responses. Also
   response 502 has possibly interesting information about the RWP
   protocol version the server supports.

   100 Ready.

      The RWP server is ready to accept next command.

   101 Goodbye.

      The RWP server is closing connection.

   103 Message delivered.

      The SEND command is successfully completed and the message is
      delivered directly to its destination.

   104 Message forwarded.

      The SEND command is completed and message is forwarded to the
      user.

   105 Sender ok.

      The FROM command successful.

   106 Recipient ok.

      The TO command successful.

   107 Message ok.

      The DATA command successful.

   108 Recipient ok to send.

      The VRFY command successful and direct message delivery is
      possible.

   109 RSET ok.

      The RWP server has received the RSET command and reset itself.

   110 Ok to forward.

      or

   110 Ok to forward <user@host.domain>.

      The VRFY command successful and direct message delivery by
      forwarding is possible. If response has also forwarding
      address the client can either forward the message itself or
      give it to server for forwarding.

   111 Original sender host ok.

      The FHST command successful and original sender host is set as
      given by the client.

   200 Enter message. Single dot '.' on line terminates.

      The RWP server is ready to receive the message. Single dot on
      message line terminates the message.

   300 |I'm not in right now but I'll be back tomorrow
   300 |at 8 o'clock a.m.

      Automatical response to the delivered message. Every line of
      this user defined reply message is delivered in its own 300
      line. Response code 300 lines may appear only after SEND
      command before response code 103 (message delivered). Client
      receiving autoreply 300 should show the text of the autoreply
      to the user. Actual autoreply line begins after the '|'
      -character in the line.

   500 Hello remote.host. This is local.host speaking.

      Response to the HELO command. This message can also occur in
      the beginning of the conversation without the VER command and
      it can be ignored.

   501 Rwrited version X.X.

      Response to the VER command. This message can also occur in
      the beginning of the conversation without the VER command and
      it can be ignored.

      502 RWP version 1.0.

          Response to the VER command. This message can also occur in
          the beginning of the conversation without the VER command and
          it can be ignored.

      510 Valid commands are:
      510   BYE,   DATA,   HELP,   HELO,
      510   RSET,   SEND,   PROT,   QUIT,
      510   VRFY,   VER
      510   FROM senderlogin
      510   FHST senderhost
      510   TO   recipentlogin
      510   FWDS current_hop_count

          Response to the HELP command.

      511 Information to the user.

          Server specific informational response. These responses may
          occur anytime during the conversation. The client can ignore
          them.

      512 Debug information to the user.

          Server specific informational response. Reserved for server
          debugging. These messages may occur anytime during the
          conversation. The client can ignore them.

      666 FATAL ERROR!

          The RWP server got into the fatal error situation and is about
          to exit immediately. Client programs are strongly encouraged
          to close the connection.

      668 Syntax error.

          The RWP server has received an invalid command.

      669 Permission denied.

          The RWP server is unable to deliver the message because the
          target user has denied the send permission.

      670 User not logged in.

          The RWP server is unable to deliver the message because the
          target user is not logged in.

671 No such user.

   The RWP server is unable to deliver the message because the
   target user does not exist. Error code 670 can be used to
   replace this message.

672 No message.

   The DATA command is terminated with empty message body. No
   SEND command can be executed before a new DATA command is
   given.

673 FROM command required.

   Tried to give the SEND command before FROM.

674 TO command required.

   Tried to give the SEND command before TO.

675 DATA command required.

   Tried to give the SEND command before DATA.

676 Forward limit exceeded.

   Response to the FWDS command that had an argument that
   exceeded the server specific limit of message forwarding
   steps.

677 Unable to forward message.

   or

677 Unable to forward message to <user@host.domain>.

   Response to the SEND or VRFY command if message forwarding is
   attempted and the server specific limit of message forwarding
   steps has been exceeded or if message forwarding has otherwise
   failed. If message forwarding fails with message 669, 670 or
   671, server will not use response 667 but gives response but
   instead it gives the response analogous with the error
   occured. If message 677 includes address the message was to
   be forwarded, the client may try to deliver it itself.

698 Unknown error.

   RWP server has faced an internal error that is not fatal.

   699 Unknown error.

      RWP server has faced an unknown error that is not fatal.

5. RWP Compliant Software

   Simple RWP 1.0 compliant server and client software RWrite-1.1 will
   be available during the fall 1994.

6. Security of RWP

   RWP version 1.0 does not offer any mean to verify the identity of the
   user connecting the RWP server program. It's possible to identify
   the sender using ident-service, but not all hosts currently support
   that. This vulnerability is analogous with the weakness of the SMTP
   protocol. Cryptographic user verification and message hiding method
   is under development and is to be defined in RWP version 2.0 during
   the year 1995.

   RWP server also may offer a way to the intruder to get to know user
   ids within the target host by trying the TO and VRFY commands. This
   vulnerability is also present in SMTP. It is however possible to
   build servers so that they never give message 671 (no such user) but
   use response 670 (user not logged in) instead.

   Another way to increase security even within RWP-1.0 described in the
   document is to design RWP servers so that they do not deliver
   messages directly to user but instead connect to some kind of RWP
   agent process that is executed by each user willing to receive RWP
   messages. This user configurable message agent could then decide
   whether to deliver the message to the user and which way of delivery
   to use. Message agent is the best way to prevent hostile user from
   sending uncontrolled message flood to the user's terminal.

   Sample implementation (RWrite-1.0) of the RWP server includes the
   support for user configuration files in which each user can either
   allow or deny messages from some user(s), host(s) or network
   domains(s). Support for message agents is currently under
   development.

   The user that is receiving the message should be able to define
   characters to be stripped from the incoming messages to prevent
   terminal mess-up.

7. RWP Connection Type

   It is suggested that tcp (and udp) port 18 should be allocated for
   rwp in future versions of RFCs listing the reserved tcp/udp/rpc
   ports. Currently port 18 is assigned to the service called Message
   Send Protocol (msp) that is not known to be implemented. Actually
   port 18 is not currently defined at all in the /etc/services -file of
   the any common UNIX-like system. Entry for /etc/services -file is as
   follows

       rwrite   18/udp   # RWP rwrite
       rwrite   18/tcp   # RWP rwrite

   Given that RWP compliant daemon program is /usr/sbin/rwrited the
   entry for /etc/inetd.conf -file would be:

       rwrite   stream tcp nowait nobody /usr/sbin/rwrited rwrited

8. Character quotation

   To offer a safe method to transfer various character sets RWP defines
   a method to quote characters in both message and autoreply. RWP uses
   quotation similar to MIME 'quoted-printable' encoding. Quoted
   character is presented as a '=' -sign followed by a two character hex
   code. This means also that all '='-signs have to be quoted.
   Quotation is also needed when message contains a line with only a
   single dot '.' in it.

    For example:
                       '.' -> =2E
                       '=' -> =3D
                       '\a' -> =07
                       '\t' -> =09

9. Security Considerations

   Security issues are not discussed in this memo.

10. Author's Address

   Timo J. Rinne
   Helsinki University of Technology.
   Cirion oy
   PO-BOX 250
   FIN-00121
   Helsinki, Finland

   EMail: Timo.Rinne@hut.fi