                    ON-DEMAND MAIL RELAY (ODMR)
                     SMTP with Dynamic IP Addresses

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Table of Contents

1. Abstract

   With the spread of low-cost computer systems and Internet
   connectivity, the demand for local mail servers has been rising.
   Many people now want to operate a mail server on a system which has

only an intermittent connection to a service provider. If the system
has a static IP address, the ESMTP ETRN command [ETRN] can be used.
However, systems with dynamic IP addresses (which are very common
with low-cost connections) have no widely-deployed solution.

This memo proposes a new service, On-Demand Mail Relay (ODMR), which
is a profile of SMTP [SMTP, ESMTP], providing for a secure,
extensible, easy to implement approach to the problem.

2. Conventions Used in this Document

Because the client and server roles reverse during the session, to
avoid confusion, the terms "customer" and "provider" will be used in
place of "client" and "server", although of course this protocol may
be useful in cases other than commercial service providers and
customers.

In examples, "P:" is used to indicate lines sent by the provider, and
"C:" indicates those sent by the customer. Line breaks within a
command are for editorial purposes only.

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY"
in this document are to be interpreted as defined in [KEYWORDS].

Examples use 'example.net' as the provider, and 'example.org' and '
example.com' as the customers.

3. Comments

Private comments should be sent to the author. Public comments may
be sent to the IETF Disconnected SMTP mailing list,
<ietf-disconn-smtp@imc.org>. To subscribe, send a message to
<ietf-disconn-smtp-request@imc.org> containing the word SUBSCRIBE as
the body.

4. Description

On-Demand Mail Relay is a restricted profile of SMTP [SMTP, ESMTP].
Port 366 is reserved for On-Demand Mail Relay. The initial client
and server roles are short-lived, as the point is to allow the
intermittently-connected host to request mail held for it by a
service provider.

The customer initiates a connection to the provider, authenticates,
and requests its mail. The roles of client and server then reverse,
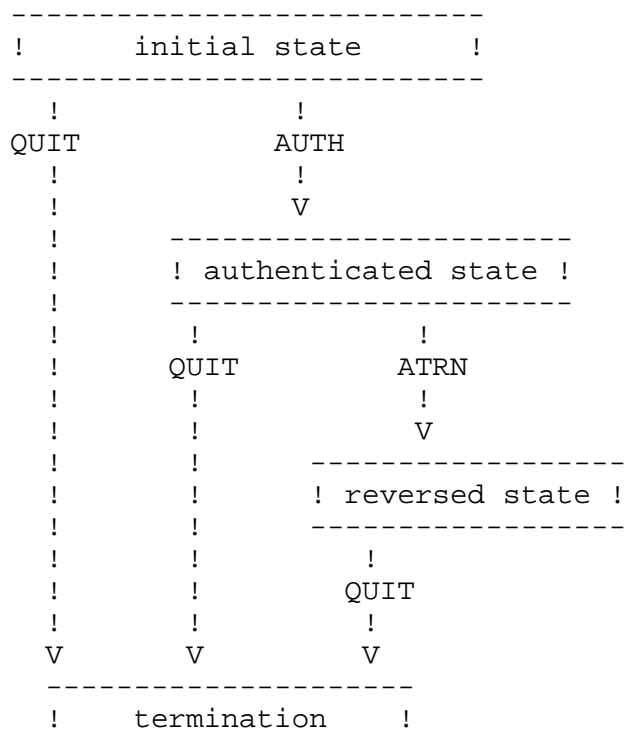and normal SMTP [SMTP, ESMTP] proceeds.

The provider has an On-Demand Mail Relay process listening for
connections on the ODMR port. This process does not need to be a
full SMTP server. It does need to be an SMTP client with access to
the outgoing mail queues, and as a server implement the EHLO, AUTH,
ATRN, and QUIT commands.

An MTA normally has a mail client component which processes the
outgoing mail queues, attempting to send mail for particular domains,
based on time or event (such as new mail being placed in the queue,
or receipt of an ETRN command by the SMTP server component). The
On-Demand Mail Relay service processes the outgoing queue not on a
timer or new mail creation, but on request.

The provider side has normal SMTP server responsibilities [SMTP],
including generation of delivery failure notices, etc. as needed.

5. States

The On-Demand Mail Relay service has three states: an initial state,
an authenticated state, and a reversed state. The state progression
is illustrated in the following diagram:

```
    ---------------------------
    !       initial state      !
    ---------------------------
     !                 !
    QUIT              AUTH
     !                 !
     !                 V
     !          ----------------------
     !          ! authenticated state !
     !          ----------------------
     !        !               !
     !       QUIT            ATRN
     !        !               !
     !        !               V
     !        !        ------------------
     !        !        ! reversed state !
     !        !        ------------------
     !        !            !
     !        !           QUIT
     !        !            !
     V        V            V
    --------------------
    !      termination   !
    --------------------
```

(Note that in the reversed state, commands are sent by the provider,
not the customer.)

5.1. Initial State

In the initial state, the provider is the server and the customer is
the client. Three commands are valid: EHLO, AUTH, and QUIT.

5.1.1. EHLO

The EHLO command is the same as in [ESMTP]. The response MUST
include AUTH and ATRN.

5.1.2. AUTH

The AUTH command is specified in [AUTH]. The AUTH command uses a
[SASL] mechanism to authenticate the session. The session is not
considered authenticated until a success response to AUTH has been
sent.

For interoperability, implementations MUST support the CRAM-MD5
mechanism [CRAM]. Other SASL mechanisms may be supported. A site
MAY disable CRAM-MD5 support if it uses more secure methods. The
EXTERNAL mechanism [SASL] might be useful in some cases, for example,
if the provider has already authenticated the client, such as during
a PPP connection.

5.1.3. QUIT

The QUIT command is the same as in [SMTP].

5.2. Authenticated State

The authenticated state is entered after a successful AUTH command.
Two commands are valid in the authenticated state: ATRN and QUIT.

5.2.1. ATRN (Authenticated TURN)

Unlike the TURN command in [SMTP], the ATRN command optionally takes
one or more domains as a parameter. The ATRN command MUST be
rejected if the session has not been authenticated. Response code
530 [AUTH] is used for this.

The timeout for this command MUST be at least 10 minutes to allow the
provider time to process its mail queue.

An ATRN command sent with no domains is equivalent to an ATRN command
specifying all domains to which the customer has access.

If the authentication used by the customer does not provide access to
all of the domains specified in ATRN, the provider MUST NOT send mail
for any domains to the customer; the provider MUST reject the ATRN
command with a 450 code.

If the customer does have access to all of the specified domains, but
none of them have any queued mail, the provider normally rejects the
ATRN command with response code 453. The provider MAY instead issue
a 250 success code, and after the roles are reversed, send a QUIT
following the EHLO.

The provider MAY also reject the ATRN command with a 450 response to
indicate refusal to accept multiple requests issued within a
particular time interval.

If the customer has access to all of the specified domains and mail
exists in at least one of them, the provider issues a 250 success
code.

If the server is unable to verify access to the requested domains
(for example, a mapping database is temporarily unavailable),
response code 451 is sent.

    [ABNF] for ATRN:

    atrn   = "ATRN" [SP domain *("," domain)]

    domain   = sub-domain 1*("." sub-domain)

    sub-domain   = (ALPHA / DIGIT) *(ldh-str)

    ldh-str   = *(ALPHA / DIGIT / "-") (ALPHA / DIGIT)

5.3. Reversed State

After the provider has sent a success reply to the ATRN command, the
roles reverse, and the customer becomes the server, and the provider
becomes the client.

After receiving the success response to ATRN, the customer sends a
standard SMTP initial greeting line. At this point normal SMTP
[SMTP, ESMTP] commands are used. Typically the provider sends EHLO
after seeing the customer's greeting, to be followed by MAIL FROM and
so on.

5.4. Other Commands

   The provider MAY reject all commands other than EHLO, AUTH, ATRN, and
   QUIT with response code 502.

6. Example On-Demand Mail Relay Session

       P: 220 EXAMPLE.NET on-demand mail relay server ready
       C: EHLO example.org
       P: 250-EXAMPLE.NET
       P: 250-AUTH CRAM-MD5 EXTERNAL
       P: 250 ATRN
       C: AUTH CRAM-MD5
       P: 334 MTg5Ni42OTcxNzA5NTJASVNQLkNPTQo=
       C: Zm9vYmFyLm5ldCBiOTEzYTYwMmM3ZWRhN2E0OTViNGU2ZTczMzRkMzg5MAo=
       P: 235 now authenticated as example.org
       C: ATRN example.org,example.com
       P: 250 OK now reversing the connection
       C: 220 example.org ready to receive email
       P: EHLO EXAMPLE.NET
       C: 250-example.org
       C: 250 SIZE
       P: MAIL FROM: <Lester.Tester@dot.foo.bar>
       C: 250 OK
       P: RCPT TO: <l.eva.msg@example.com>
       C: 250 OK, recipient accepted
       ...
       P: QUIT
       C: 221 example.org closing connection

7. Response Codes

   The response codes used in this document are:

   250 Requested mail action okay, completed
   450 ATRN request refused
   451 Unable to process ATRN request now
   453 You have no mail
   502 Command not implemented
   530 Authentication required [AUTH]

8. Security Considerations

   Because access to the On-Demand Mail Relay server is only useful with
   a prior arrangement between the parties (so the provider is the
   target of MX records for the customer's domains and thus has mail to
   relay), it may be useful for the provider to restrict access to the
   On-Demand Mail Relay port. For example, the ODMR server could be

configurable, or a TCP wrapper or firewall could be used, to block
access to port 366 except within the provider's network. This might
be useful when the provider is the customer's ISP. Use of such
mechanisms does not reduce the need for the AUTH command, however,
but can increase the security it provides.

Use of SASL in the AUTH command allows for substitution of more
secure authentication mechanisms in the future.

See sections 5.1.2 and 5.2.1 for additional security details.

9. Acknowledgments

This memo has been developed in part based on comments and
discussions which took place on and off the IETF-disconn-smtp mailing
list. Special thanks to Chris Newman and Ned Freed for their
comments.

10. References

    [ABNF]   Crocker, D. and P. Overell, "Augmented BNF for Syntax
                Specifications: ABNF", RFC 2234, November 1997.

    [AUTH]   Myers, J., "SMTP Service Extension for Authentication",
                RFC 2554, March 1999.

    [CRAM]   Klensin, J., Catoe, R. and P. Krumviede, "IMAP/POP
                AUTHorize Extension for Simple Challenge/Response", RFC
                2195, September 1997.

    [ESMTP]   Klensin, J., Freed, N., Rose, M., Stefferud, E. and D.
                Crocker, "SMTP Service Extensions", RFC 1869, November
                1995.

    [ETRN]   De Winter, J., "SMTP Service Extension for Remote Message
                Queue Starting", RFC 1985, August 1996.

    [KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate
                Requirement Levels", BCP 14, RFC 2119, March 1997.

    [SASL]   Myers, J., "Simple Authentication and Security Layer
                (SASL)", RFC 2222, October 1997.

    [SMTP]   Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC
                821, August 1982.

11. Author's Address

     Randall Gellens
     QUALCOMM Incorporated
     5775 Morehouse Dr.
     San Diego, CA 92121-2779
     U.S.A.

     Phone: +1.619.651.5115
     EMail: randy@qualcomm.com

12. Full Copyright Statement

Acknowledgement