Network Working Group
INTERNET-DRAFT

T. Tornkvist
SERC, Melbourne

11 January 1998

Notification - An extension to the Post Office Protocol version 3
<draft-tornkvist-pop3-01.txt>

Abstract

This memo describes an optional extension to the Post Office Protocol version 3 (POP3), which introduces a possibility for a POP3 client to be notified by a POP3 server whenever the clients mail-drop is accessed.

Status of this Memo

Table of Contents

1. Conventions Used in this Document 1
2. Introduction 2
3. Operation 2
4. NTFY Sent by the Client 3
5. NTFY Sent by the Server 4
6. Alteration to the UPDATE State 4
7. New capabilities 5
8. Security Considerations 5
9. References 6
10. Author's address 6

1. Conventions Used in this Document

The key words "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT",

and "MAY" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [KEYWORDS].

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

2. Introduction

The Post Office Protocol version 3, as described in [POP3], is a simple and low-cost method of enabling mail access. The host making use of the POP3 service is referred to here as the "client", and the host providing the service as the "server". When a client wants to retrieve mail from a server, a TCP connection to the server is established. The client then uses various POP3 commands to access the mail-drop. Thus every time a client wants to check for new mail he has to poll the server. For a mail-drop which seldom receives new mails this is obvious not economical. It may also be a security issue since repeated attempts to access the server are more vulnerable to interception. This memo tries to remedy this by introducing the concept of notification, and describes how a client can request that the server shall notify the client when any changes have been made to the clients mail-drop.

3. Operation

Two new POP3 command named NTFY and +NTFY are added. The NTFY command is used by the client in order to request the server that it should notify the client whenever the clients mail-drop is accessed. The +NTFY command is used by the server to notify a client that the clients mail-drop has been accessed.

After the server has sent a +NTFY command, both the client and the server MUST enter the AUTHORIZATION state, as described in [POP3].

As soon as a server tries to establish a TCP connection to be used for notification, it also removes the request for notification. It is up to the client to issue a new NTFY command if he wants to be notified again.

The client can only issue the NTFY command in the TRANSACTION state.

A request for notification will not be activated until the POP3 session enters the UPDATE state. During the TRANSACTION state it is possible to cancel the request for notification as described in the chapter: "NTFY Sent by the Client".

4. NTFY Sent by the Client

This command can only be sent when the client is in the TRANSACTION state.

```
NTFY timeout [hostname port-number [timestamp]]
```

Arguments:

a timeout value in minutes, specified as an integer, greater or equal to zero, an optional hostname and port-number that specifies where to deliver the notification, an optional timestamp to be used as an APOP challenge

Restrictions:

may only be given in the TRANSACTION state

Discussion:

The POP3 server issues a positive response if requests for notification can be serviced. The timeout value specifies for how long time the server shall maintain the request for notification. A timeout value of zero shall remove any existing request for notification at the server.

A server shall only store one request per user. Hence, a zero timeout value need not be accompanied by any other argument. As a result of this, a request for notification should not be activated until the POP3 session enters the UPDATE state.

A server which implements this command must be able to serve timeout values ranging from 0 - 255. However, by using the capability extension [CAPA], a server may however announce a greater maximim value for the timeout (see also the chapter: "New Capabilities"). A negative timeout value should result in an error response.

If APOP authentication is to be used. A challenge timestamp can be include as the last argument. Later, when the server issues the notification, it sends the corrsponding digest message (see also the description of +NTFY command and the chapter: "Security Considerations").

Possible Responses:

+OK
-ERR

```
        Examples:
            C: NTFY 60 campari.rmit.edu.au 9411
            S: +OK Request for notification accepted

            C: NTFY 300 campari.rmit.edu.au 9411
            S: -ERR Timeout value too big
            C: NTFY 255 campari.rmit.edu.au 9411
            S: +OK Request for notification accepted

            C: NTFY 0
            S: +OK Request for notification removed
```

5. +NTFY Sent by the Server

When a client is to be notified about changes made to his mail-drop, the server establish a TCP connection to the specified host and port number. As soon this is done, the request for notification is erased from the server. This is done regardless if the connection was successful or not.

```
      +NTFY name [digest]

         Arguments:
             A name, specifying the mail-drop in question, and
             if APOP authentication is to be used, a digest
             argument.

         Restrictions:
             Only one attempt to contact the client will be made.

         Discussion:
             As soon the server has sent this command, both the
             client and the server are supposed to enter the
             AUTHORIZATION state. The digest argument shall correspond
             to the msg-id sent by the client in a preceding NTFY
             command.

         Examples:
             S: +NTFY mrose c4c9334bac560ecc979e58001b3e22fb
```

6. Alteration to the UPDATE State

A server which has received a request for notification shall not make it valid until the UPDATE state has been entered. This is needed so that a client can change or clear a request for notification previously done in the same POP3 session.

7. New capabilities

For those servers which implements capabilities [CAPA]. The following new capability SHOULD be used.

```
      CAPA tag:
        NTFY capability

      Arguments:
        The maximum timeout value the server will
        maintain a request for notification.

      Added commands:
        NTFY
        +NTFY

      Standard commands affected:
        none

      Announced states / possible differences:
        both / no

      Commands valid in states:
        TRANSACTION

      Specific reference:
        this document

      Discussion:
        The NTFY capability indicates that the server implements
        the method described in this memo for handling request
        for notification. The timeout value returned is the maximum
        time in minutes the server will maintain such a request.
        A server MUST at least be able to maintain a request for
        notification for 255 minutes.
```

8. Security Considerations

After a client has been notified by a server, the session MUST enter the AUTHORIZATION state. The main reason for this is to not introduce a new method for POP3 authentication. Ways to perform POP3 authentication is described in [POP3], [POP-AUTH] and [SASL].

NB: When APOP is used for authentication, it is important that a client really check that the digest, sent from the server in the +NTFY command, really match the challenge most previously sent by the client. This MUST be done in order to avoid possible masquerade

attacks, where an attacker may have obtained the host and port information (e.g by sniffing earlier packets being sent).

9. References

[CAPA]   Gellens, R. and Newman, C. and Lundblade, L. "POP3 Extension Mechanism", RFC 2449, Nov-1998.

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

[POP3]   Myers, J. and M. Rose, "Post Office Protocol -- Version 3", STD 53, RFC 1939, May 1996.

[POP-AUTH]   Myers, J., "POP3 AUTHentication command", RFC 1734, December 1994.

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

10. Author's address

Torbjorn Tornkvist
SERC (Software Engineering Research Center)
110 Victoria St, Carlton
Victoria 3053
AUSTRALIA

Phone: +61 3 9925 4089
Fax: +61 3 9925 4094
Email: tobbe@serc.rmit.edu.au