Network Working Group
Request for Comments: 1204

S. Yeh
D. Lee
Netix Communications, Inc.
February 1991

Message Posting Protocol (MPP)

Status of this Memo

This memo describes a protocol for posting messages from workstations (e.g., PCs) to a mail service host. This RFC specifies an Experimental Protocol for the Internet community. Discussion and suggestions for improvement are requested. Please refer to the current edition of the "IAB Official Protocol Standards" for the standardization state and status of this protocol. Distribution of this memo is unlimited.

1. INTRODUCTION

Operating systems for personal computers do not provide a mechanism for user authentication. However, such a mechanism is crucial for electronic mail system since authenticating message sender's identity is important in preventing mail forgery. Hence, adding personal computers to an electronic mail network requires an agent (message posting server) to authenticate sender's identity and then submit mail to the message delivery system (e.g., Sendmail, MMDF) on behalf of the sender at a PC. The Netix Message Posting Protocol is developed to be the interface between the message posting server and the PC (client). The protocol is designed to use TCP and is based on the command and reply structures defined for Simple Mail Transfer Protocol (RFC 821) and File Transfer Protocol (RFC 959).

2. SPECIFICATIONS

2.1. Command List

```
USER <SP> <username> <CRLF>
PASS <SP> <password> <CRLF>
DATA <CRLF>
NOOP <CRLF>
QUIT <CRLF>
```

2.2. Reply List

```
220 Message Posting Service Ready.
221 Closing Connection.
250 Command OK.
```

354 Enter mail, end with <CRLF>.<CRLF>
451 Local error encountered.
500 Command unrecognized.
501 Argument syntax error.
503 Illegal command sequence.
530 Authentication Failure.
550 Error.

2.3. Command and Reply Descriptions

USER <SP> <username> <CRLF>

The USER command informs the message posting server about the username of the user trying to submit mail to the network. The required argument for the USER command is a string specifying the message sender's username.

The USER command can only be used under three conditions:

- when the session with the message posting server has just started;

- right after a message text (terminated by the "<CRLF>.<CRLF>" sequence) has been successfully submitted to the message posting server;

- right after a USER command that gets the reply code 501.

List of possible reply codes for the USER command:

- 250 The username of the message sender has been accepted.

- 451 Internal error has occurred in the message posting server.

- 501 Syntax error detected in the username argument.

- 503 The USER command has been used under an inappropriate condition (i.e., one that is not specified above).

It is recommended that the message posting server should return 250 even if the username is not recognized by the message posting server, as long as the username is syntactically correct. This is an attempt to prevent the message posting server from releasing too much information about the user database. Client should not be able to test the existence of a certain username.

PASS <SP> <password> <CRLF>

The PASS command is used to inform the message posting server about the password associated with the username previously specified. The required argument for the PASS command is a string specifying the message sender's password.

The PASS command can only be used under two conditions:

- right after a USER command that gets the reply code 250;

- right after a PASS command that gets the reply code 501.

List of possible reply codes for the PASS command:

- 250 The password has been accepted and verified to be correctly associated with the username previously specified.

- 451 Internal error has occurred in the message posting server.

- 501 Syntax error detected in the password argument.

- 503 The PASS command has been used under an inappropriate condition (i.e., one that is not specified above).

- 530 The password provided is not the one associated with the username previously specified.

DATA <CRLF>

The DATA command is used to inform the message posting server to get ready to accept a mail message text. No argument is expected. (This command has the same meaning as the DATA command defined in RFC 821.)

The DATA command can only be used under two conditions:

- right after a PASS command that gets the reply code 250;

- right after a mail message text has been successfully accepted from the client.

List of possible reply codes for the DATA command:

- 354 The message posting server is ready to accept the mail message text.

- 451 Internal error has occurred in the message posting server.

- 503 The DATA command has been used under an inappropriate condition (i.e., one that is not specified above).

Upon receiving the reply code 354 for the DATA command, the client should submit the mail message text to message posting server and terminate the text by the sequence "<CRLF>.<CRLF>" as defined in RFC 821. If the message text includes the "<CRLF>.<CRLF>" sequence, then the sequence is replaced by the "<CRLF>..<CRLF>" sequence as defined in RFC 821. The extra "." token will not be included in the final copy of the submitted message.

Upon receiving the mail message text terminated by the "<CRLF>.<CRLF>" sequence, list of possible reply codes is:

- 250 The mail message text has been successfully queued for delivery.

- 451 Internal error has occurred in the message posting server and the mail message text has not been queued.

NOOP <CRLF>

The NOOP command does not cause any action to be performed by the message posting server. Instead, it tests the status of the message posting server. No argument is expected.

The NOOP command cannot be used under one condition:

- right after a DATA command that gets the reply code 354 (i.e., when the message posting server is expecting the client to submit the mail message text).

List of possible reply codes for the NOOP command:

- 250 The message posting server has not encountered any internal error.

- 451 Internal error has occurred in the message posting server during the current session.

QUIT <CRLF>

The QUIT command is used to terminate the session with the message posting server. No argument is expected.

The QUIT command can be used under any condition. The message posting server should always return the reply code 221 for the QUIT command.

3. IMPLEMENTATION OF THE MESSAGE POSTING SERVER

There are several issues to be considered when implementing the message posting server:

- secured environment
- port number assignment
- handling of idle client
- local/remote password database
- message queuing
- handling of message delivery failure

3.1 Secured Environment

The message posting server is responsible for authenticating message senders and submitting mail to the message delivery system. Hence, it should be running in a secured environment, such as running on a system (UNIX, VMS, MS-DOS) with well restricted physical and network access.

3.2 Port Number Assignment

Port 218 is assigned for the Netix Message Posting Protocol.

3.3 Handling of Idle Client

The message posting server should terminate a session if the client has been idle for too long, to release the resource allocated for the session.

3.4 Local/Remote Password Database

To take advantage of existing password databases, such as the passwd file in UNIX, the message posting server can use FTP and POP3 to perform the username and password checking with the appropriate server.

For network that does not have any password database, the message posting server should let the system administrator specify a local password file on the host that the message posting server is running.

3.5 Message Queuing

The message posting server should attempt to submit accepted messages to the message delivery system as soon as possible.

3.6 Handling of Message Delivery Failure

Failure in delivering messages should be handled by the message delivery system and the message posting server should not interfere.

4. REFERENCES

[1] Postel, J., "Simple Mail Transfer Protocol", RFC 821, USC/Information Sciences Institute, August 1982.

[2] Postel, J., and J. Reynolds, "File Transfer Protocol", RFC 959, USC/Information Sciences Institute, October 1985.

Security Considerations

Security issues are discussed in section 3.1.

Authors' Addresses

Shannon Yeh
Netix Communications, Inc.
15375 Barranca Parkway, Suite A-215
Irvine, CA 92718

Phone: (714) 727-9335

Email: yeh@netix.com

David Lee
Netix Communications, Inc.
15375 Barranca Parkway, Suite A-215
Irvine, CA 92718

Phone: (714) 727-9335

EMail: dlee@netix.com