POP3 Extension Mechanism and Error Codes

Status of this memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Copyright Notice

Copyright (C) The Internet Society 1997. All Rights Reserved.

Introduction

The POP3 protocol [POP3] includes a number of optional commands and some useful protocol extensions have also been published. Currently these optional features and extensions can only be detected by probing. This has resulted in some clients including manual configuration options for POP3 server capabilities.

Because one of the most important features of POP3 is its simplicity, it is not desirable to have a lot of extensions. However, some extensions are necessary such as ones that provide improved security [POP-AUTH]. This specification defines a mechanism to detect such extensions and the availability of optional commands. Included is an initial set of currently implemented capabilities which vary between server implementations.

This also extends POP3 error messages so that machine parsible codes can be provided to the client.

This is an preliminary proposal. Please do not implement it. Comments can be sent directly to the author.

0. Feedback Requested

This is a moderately dangerous proposal as it might encourage haphazard extension of the POP3 protocol. However, it is believed that the benefit of being able to discover capabilities outwieghs this. Do you agree?

The error codes would be ugly to current clients, but shouldn't cause interoperability problems. It is speculated that the ability to communicate more precise error information to the client outwieghs the ugliness impact on existing POP3 client error messages. Do you agree?

I know of at least two POP3 servers which offer the LOGIN-DELAY facility unannounced today. I am also told that at least one client fails to communicate with these servers when the facility is enabled. Formalizing it would encourage those clients to hold the connection open rather than re-connecting to download each message as the user reads them. This is probably a good thing, but that client vendor probably dislikes the idea. Should LOGIN-DELAY be left in this specification or should it remain an unannounced facility of deployed POP3 servers?

Suggestions for more initial error codes or more capabilities which document variation in deployed POP3 servers is requested.

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. The POP3 CAPA command

The POP3 CAPA command will return a list of capabilities supported by the POP3 server. It is available in both AUTHORIZATION state and TRANSACTION state. Additional capabilities MAY become available in TRANSACTION state, but all capabilities listed in AUTHORIZATION state MUST also be available.

CAPA

Arguments: none

Restrictions: none

Discussion:
If the server responds to the CAPA command with -ERR, that indicates the capability command is not implemented and the client will have to probe for capabilities as before. If the server responds with +OK, that will be followed by a list of capabilities, one per line. Each capability name MAY be followed by an "=" sign and arguments. The capability list is terminated by a line containing a termination octet (".") and a CRLF pair.

Possible Responses:
+OK -ERR

Examples:

```
C: CAPA
S: +OK Capability list follows
S: TOP
S: UIDL
S: USER
S: APOP
S: SASL=CRAM-MD5 KERBEROS_V4
S: LOGIN-DELAY=240
S: OVERLAP
S: .
```

3. Initial Set of Capabilities

This section defines an initial set of POP3 capabilities. These include the optional POP3 commands, already published POP3 extensions and behavior variations between POP3 servers which can impact clients.

3.1. POP3 Optional Command Capabilities

The "TOP" capability indicates the "TOP" command is available. The "UIDL" capability indicates the "UIDL" command is available. The "APOP" capability indicates that APOP authentication is supported, although it may not be available to all users. The "USER" capability indicates that the USER and PASS commands are supported, although they may not be available to all users.

3.2. POP3 SASL capability

The POP3 AUTHentication command [POP-AUTH] permits the use of SASL [SASL] authentication mechanisms with POP3. The "SASL" capability indicates that the AUTH command is available and that it supports an optional base64 encoded second argument for an initial client response as described in the SASL specification. The argument to the SASL capability is a space separated list of SASL mechanisms which are supported.

3.3. LOGIN-DELAY capability

POP3 clients often login frequently to check for new mail. Unfortunately, the process of creating a connection, logging in the user and opening the user's maildrop can be very resource intensive on the server. A number of deployed POP3 servers try to reduce server load by requiring a delay between logins. The LOGIN-DELAY capability includes a decimal number argument which indicates the number of seconds required between logins for a given user. Clients which permit the user to configure a mail check interval can use this capability to determine the minimum permissible interval. Servers which advertise LOGIN-DELAY SHOULD enforce it.

3.4. OVERLAP capability

The OVERLAP capability indicates the server is capable of accepting multiple commands at a time (up to the window size of the underlying transport layer). Some POP3 clients have an option to indicate the server supports "Overlapped POP3 commands." This capability removes the need to configure that at the client. This is roughly synonymous with the ESMTP PIPELINING extension [PIPELINING].

4. Furture Extensions to POP3

Future extensions to POP3 are discouraged as POP3's usefulness lies in its simplicity. Extensions which offer capabilities supplied by IMAP [IMAP4] or SMTP [SMTP] are strongly discouraged and unlikely to be permitted on the IETF standards track.

Clients MUST NOT require the presence of any extension for basic functionality.

Capabilities beginning with the letter "X" are reserved for experimental non-standard extensions and their use is discouraged. All other capabilities MUST be defined in a standards track or IESG approved experimental RFC.

5. POP3 response codes

POP3 is currently only capable of indicating success or failure to most commands. Unfortunately, clients often need to know more information about the cause of a failure in order to gracefully recover. This is especially important in response to a failed login.

This specification amends the POP3 standard to permit an optional response code, enclosed in square brackets, at the beginning of the human readable text portion of a "+OK" or "-ERR" response. Clients supporting this extension MAY remove any information enclosed in square brackets prior to displaying human readable text to the user. Immediately following the open square bracket "[" character is a response code which is interpreted in a case-insensitive fashion by the client.

The response code is hierarchical, with a "/" separating levels of detail about the error. Clients MUST ignore unknown hierarchical detail about the response code. This is important, as it could be necessary to provide further detail for response codes in the future. For example, ENCRYPT-NEEDED/TLS and ENCRYPT-NEEDED/SSH might indicate a suggestion to use the TLS or SSH protocols respectively for encryption.

Examples:

```
    C: USER mrose
    S: -ERR [ENCRYPT-NEEDED] You need to activate encryption before
            logging in.
```

5.1. POP3 response codes

This specification defines some POP3 response codes which can be used to determine the reason for a failed login. Additional response codes MAY be defined by publication in an RFC (standards track or IESG approved experimental RFCs are preferred).

LOGIN-DELAY
This occurs on a -ERR response to an AUTH, USER, PASS or APOP command and indicates that the user has logged in recently and will not be allowed to login again until the login delay period has expired.

PASS-EXPIRED
This occurs on a -ERR response to an AUTH, USER, PASS or APOP command and indicates the user will not be allowed to login until his password/passphrase is changed.

ENCRYPT-NEEDED
This occurs on an -ERR response to an AUTH, USER or APOP command and indicates that the requested authentication mechanism is only permitted underneath a security layer. The client MAY take action to activate a security layer and repeat the same AUTH, USER or APOP command or try an AUTH command with a stronger mechanism. The client SHOULD record the fact that encryption is needed for that user, server and mechanism combination.

AUTH-TOO-WEAK
This occurs on an -ERR response to an AUTH, USER or APOP command and indicates that the mechanism is too weak and is no longer permitted for that user by site policy. This allows a mechanism to be disabled on a per-user rather than a per-server level which is useful if different users have different security requirements or for transitioning from plaintext USER/PASS to a more secure mechanism. The client SHOULD record the fact that the user, server and mechanism combination is no longer permitted.

TRANSITION-NEEDED
This occurs on an -ERR response to an AUTH or APOP command. It indicates that the server has an entry for the specified user in a legacy authentication database but does not yet have credentials to offer the requested mechanism. A client which receives this error code MAY do a one-time login using the USER/PASS commands or another plaintext mechanism (preferably protected by a privacy layer) to initialize

credentials for the requested mechanism.

6. Security Considerations

A capability list can reveal information about the server's authentication capabilities which can be used to determine if certain attacks will be successful. However, allowing clients to automatically detect availability of stronger mechanisms and alter their configurations to use them can improve overall security at a site.

The TRANSITION-NEEDED error code can be insertted by an active attacker in an attempt to get the client to send the user's password unencrypted. Clients SHOULD prompt the user to get permission prior to transition. The additional error codes will allow gradual upgrading of security services on a per-user basis so they can improve overall security at a site.

7. References

[IMAP4] Crispin, M., "Internet Message Access Protocol - Version 4rev1", RFC 2060, University of Washington, December 1996.

<ftp://ds.internic.net/rfc/rfc2060.txt>

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

<ftp://ds.internic.net/rfc/rfc2119.txt>

[PIPELINING] Freed, "SMTP Service Extension for Command Pipelining", RFC 2197, Innosoft, September 1997.

<ftp://ds.internic.net/rfc/rfc2197.txt>

[POP3] Myers, J., Rose, M., "Post Office Protocol - Version 3", RFC 1939, Carnegie Mellon, Dover Beach Consulting, Inc., May 1996.

<ftp://ds.internic.net/rfc/rfc1939.txt>

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

<ftp://ds.internic.net/rfc/rfc1734.txt>

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

<ftp://ds.internic.net/rfc/rfc2222.txt>

8. Full Copyright Statement

Copyright (C) The Internet Society 1997. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implmentation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

9. Author's Address

Chris Newman
Innosoft International, Inc.
1050 Lakes Drive
West Covina, CA 91790 USA

Email: chris.newman@innosoft.com