

Network Working Group
Request for Comments: 2821
Obsoletes: 821, 974, 1869
Updates: 1123
Category: Standards Track

J. Klensin, Editor
AT&T Laboratories
April 2001

Simple Mail Transfer Protocol

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

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

This document is a self-contained specification of the basic protocol for the Internet electronic mail transport. It consolidates, updates and clarifies, but doesn't add new or change existing functionality of the following:

- the original SMTP (Simple Mail Transfer Protocol) specification of [RFC 821](#) [30],
- domain name system requirements and implications for mail transport from [RFC 1035](#) [22] and [RFC 974](#) [27],
- the clarifications and applicability statements in [RFC 1123](#) [2], and
- material drawn from the SMTP Extension mechanisms [19].

It obsoletes [RFC 821](#), [RFC 974](#), and updates [RFC 1123](#) (replaces the mail transport materials of [RFC 1123](#)). However, [RFC 821](#) specifies some features that were not in significant use in the Internet by the mid-1990s and (in appendices) some additional transport models. Those sections are omitted here in the interest of clarity and brevity; readers needing them should refer to [RFC 821](#).

It also includes some additional material from [RFC 1123](#) that required amplification. This material has been identified in multiple ways, mostly by tracking flaming on various lists and newsgroups and problems of unusual readings or interpretations that have appeared as the SMTP extensions have been deployed. Where this specification moves beyond consolidation and actually differs from earlier documents, it supersedes them technically as well as textually.

Although SMTP was designed as a mail transport and delivery protocol, this specification also contains information that is important to its use as a 'mail submission' protocol, as recommended for POP [[3](#), [26](#)] and IMAP [[6](#)]. Additional submission issues are discussed in [RFC 2476](#) [[15](#)].

[Section 2.3](#) provides definitions of terms specific to this document. Except when the historical terminology is necessary for clarity, this document uses the current 'client' and 'server' terminology to identify the sending and receiving SMTP processes, respectively.

A companion document [[32](#)] discusses message headers, message bodies and formats and structures for them, and their relationship.

Table of Contents

| | |
|--|----|
| 1. Introduction | 4 |
| 2. The SMTP Model | 5 |
| 2.1 Basic Structure | 5 |
| 2.2 The Extension Model | 7 |
| 2.2.1 Background | 7 |
| 2.2.2 Definition and Registration of Extensions | 8 |
| 2.3 Terminology | 9 |
| 2.3.1 Mail Objects | 10 |
| 2.3.2 Senders and Receivers | 10 |
| 2.3.3 Mail Agents and Message Stores | 10 |
| 2.3.4 Host | 11 |
| 2.3.5 Domain | 11 |
| 2.3.6 Buffer and State Table | 11 |
| 2.3.7 Lines | 12 |
| 2.3.8 Originator, Delivery, Relay, and Gateway Systems | 12 |
| 2.3.9 Message Content and Mail Data | 13 |
| 2.3.10 Mailbox and Address | 13 |
| 2.3.11 Reply | 13 |
| 2.4 General Syntax Principles and Transaction Model | 13 |
| 3. The SMTP Procedures: An Overview | 15 |
| 3.1 Session Initiation | 15 |
| 3.2 Client Initiation | 16 |
| 3.3 Mail Transactions | 16 |
| 3.4 Forwarding for Address Correction or Updating | 19 |

| | |
|--|----|
| 3.5 Commands for Debugging Addresses | 20 |
| 3.5.1 Overview | 20 |
| 3.5.2 VRFY Normal Response | 22 |
| 3.5.3 Meaning of VRFY or EXPN Success Response | 22 |
| 3.5.4 Semantics and Applications of EXPN | 23 |
| 3.6 Domains | 23 |
| 3.7 Relaying | 24 |
| 3.8 Mail Gatewaying | 25 |
| 3.8.1 Header Fields in Gatewaying | 26 |
| 3.8.2 Received Lines in Gatewaying | 26 |
| 3.8.3 Addresses in Gatewaying | 26 |
| 3.8.4 Other Header Fields in Gatewaying | 27 |
| 3.8.5 Envelopes in Gatewaying | 27 |
| 3.9 Terminating Sessions and Connections | 27 |
| 3.10 Mailing Lists and Aliases | 28 |
| 3.10.1 Alias | 28 |
| 3.10.2 List | 28 |
| 4. The SMTP Specifications | 29 |
| 4.1 SMTP Commands | 29 |
| 4.1.1 Command Semantics and Syntax | 29 |
| 4.1.1.1 Extended HELLO (EHLO) or HELLO (HELO) | 29 |
| 4.1.1.2 MAIL (MAIL) | 31 |
| 4.1.1.3 RECIPIENT (RCPT) | 31 |
| 4.1.1.4 DATA (DATA) | 33 |
| 4.1.1.5 RESET (RSET) | 34 |
| 4.1.1.6 VERIFY (VRFY) | 35 |
| 4.1.1.7 EXPAND (EXPN) | 35 |
| 4.1.1.8 HELP (HELP) | 35 |
| 4.1.1.9 NOOP (NOOP) | 35 |
| 4.1.1.10 QUIT (QUIT) | 36 |
| 4.1.2 Command Argument Syntax | 36 |
| 4.1.3 Address Literals | 38 |
| 4.1.4 Order of Commands | 39 |
| 4.1.5 Private-use Commands | 40 |
| 4.2 SMTP Replies | 40 |
| 4.2.1 Reply Code Severities and Theory | 42 |
| 4.2.2 Reply Codes by Function Groups | 44 |
| 4.2.3 Reply Codes in Numeric Order | 45 |
| 4.2.4 Reply Code 502 | 46 |
| 4.2.5 Reply Codes After DATA and the Subsequent <CRLF>.<CRLF> | 46 |
| 4.3 Sequencing of Commands and Replies | 47 |
| 4.3.1 Sequencing Overview | 47 |
| 4.3.2 Command-Reply Sequences | 48 |
| 4.4 Trace Information | 49 |
| 4.5 Additional Implementation Issues | 53 |
| 4.5.1 Minimum Implementation | 53 |
| 4.5.2 Transparency | 53 |
| 4.5.3 Sizes and Timeouts | 54 |

| | |
|--|----|
| 4.5.3.1 Size limits and minimums | 54 |
| 4.5.3.2 Timeouts | 56 |
| 4.5.4 Retry Strategies | 57 |
| 4.5.4.1 Sending Strategy | 58 |
| 4.5.4.2 Receiving Strategy | 59 |
| 4.5.5 Messages with a null reverse-path | 59 |
| 5. Address Resolution and Mail Handling | 60 |
| 6. Problem Detection and Handling | 62 |
| 6.1 Reliable Delivery and Replies by Email | 62 |
| 6.2 Loop Detection | 63 |
| 6.3 Compensating for Irregularities | 63 |
| 7. Security Considerations | 64 |
| 7.1 Mail Security and Spoofing | 64 |
| 7.2 "Blind" Copies | 65 |
| 7.3 VRFY, EXPN, and Security | 65 |
| 7.4 Information Disclosure in Announcements | 66 |
| 7.5 Information Disclosure in Trace Fields | 66 |
| 7.6 Information Disclosure in Message Forwarding | 67 |
| 7.7 Scope of Operation of SMTP Servers | 67 |
| 8. IANA Considerations | 67 |
| 9. References | 68 |
| 10. Editor's Address | 70 |
| 11. Acknowledgments | 70 |
| Appendices | 71 |
| A. TCP Transport Service | 71 |
| B. Generating SMTP Commands from RFC 822 Headers | 71 |
| C. Source Routes | 72 |
| D. Scenarios | 73 |
| E. Other Gateway Issues | 76 |
| F. Deprecated Features of RFC 821 | 76 |
| Full Copyright Statement | 79 |

1. Introduction

The objective of the Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently.

SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel. While this document specifically discusses transport over TCP, other transports are possible. Appendices to RFC 821 describe some of them.

An important feature of SMTP is its capability to transport mail across networks, usually referred to as "SMTP mail relaying" (see section 3.8). A network consists of the mutually-TCP-accessible hosts on the public Internet, the mutually-TCP-accessible hosts on a firewall-isolated TCP/IP Intranet, or hosts in some other LAN or WAN environment utilizing a non-TCP transport-level protocol. Using

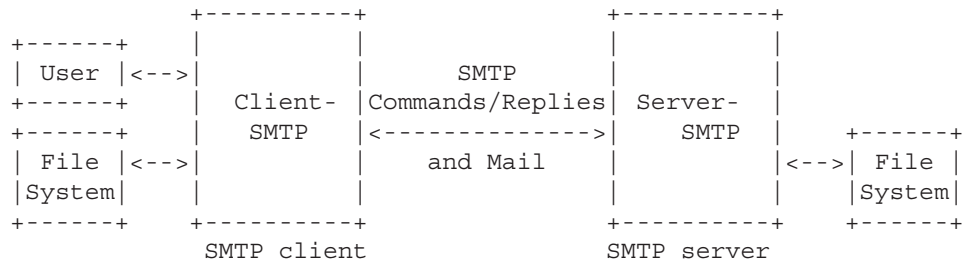
SMTP, a process can transfer mail to another process on the same network or to some other network via a relay or gateway process accessible to both networks.

In this way, a mail message may pass through a number of intermediate relay or gateway hosts on its path from sender to ultimate recipient. The Mail eXchanger mechanisms of the domain name system [22, 27] (and section 5 of this document) are used to identify the appropriate next-hop destination for a message being transported.

2. The SMTP Model

2.1 Basic Structure

The SMTP design can be pictured as:



When an SMTP client has a message to transmit, it establishes a two-way transmission channel to an SMTP server. The responsibility of an SMTP client is to transfer mail messages to one or more SMTP servers, or report its failure to do so.

The means by which a mail message is presented to an SMTP client, and how that client determines the domain name(s) to which mail messages are to be transferred is a local matter, and is not addressed by this document. In some cases, the domain name(s) transferred to, or determined by, an SMTP client will identify the final destination(s) of the mail message. In other cases, common with SMTP clients associated with implementations of the POP [3, 26] or IMAP [6] protocols, or when the SMTP client is inside an isolated transport service environment, the domain name determined will identify an intermediate destination through which all mail messages are to be relayed. SMTP clients that transfer all traffic, regardless of the target domain names associated with the individual messages, or that do not maintain queues for retrying message transmissions that initially cannot be completed, may otherwise conform to this specification but are not considered fully-capable. Fully-capable SMTP implementations, including the relays used by these less capable

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.