[Docs] [txt|pdf] [Errata]

Updated by: 1349, 2181, 5321, 5966 STANDARD
Errata Exist
Network Working Group Internet Engineering Task Force
Request for Comments: 1123 R. Braden, Editor
October 1989

# Requirements for Internet Hosts -- Application and Support

## Status of This Memo

This RFC is an official specification for the Internet community. It incorporates by reference, amends, corrects, and supplements the primary protocol standards documents relating to hosts. Distribution of this document is unlimited.

## Summary

This RFC is one of a pair that defines and discusses the requirements for Internet host software. This RFC covers the application and support protocols; its companion RFC-1122 covers the communication protocol layers: link layer, IP layer, and transport layer.

## Table of Contents

1. INTRODUCTION ..... 5
1.1 The Internet Architecture ..... 6
1.2 General Considerations ..... 6
1.2.1 Continuing Internet Evolution ..... 6
1.2.2 Robustness Principle ..... 7
1.2.3 Error Logging ..... 8
1.2.4 Configuration ..... 8
1.3 Reading this Document ..... 10
1.3.1 Organization ..... 10
1.3.2 Requirements ..... 10
1.3.3 Terminology ..... 11
1.4 Acknowledgments ..... 12

2. GENERAL ISSUES ..... 13
2.1 Host Names and Numbers ..... 13
2.2 Using Domain Name Service ..... 13
2.3 Applications on Multihomed hosts ..... 14
2.4 Type-of-Service ..... 14
2.5 GENERAL APPLICATION REQUIREMENTS SUMMARY ..... 15





3. REMOTE LOGIN -- TELNET PROTOCOL ..... 16
3.1 INTRODUCTION ..... 16
3.2 PROTOCOL WALK-THROUGH ..... 16
3.2.1 Option Negotiation ..... 16
3.2.2 Telnet Go-Ahead Function ..... 16
3.2.3 Control Functions ..... 17
3.2.4 Telnet "Synch" Signal ..... 18
3.2.5 NVT Printer and Keyboard ..... 19
3.2.6 Telnet Command Structure ..... 20
3.2.7 Telnet Binary Option ..... 20
3.2.8 Telnet Terminal-Type Option ..... 20
3.3 SPECIFIC ISSUES ..... 21
3.3.1 Telnet End-of-Line Convention ..... 21
3.3.2 Data Entry Terminals ..... 23
3.3.3 Option Requirements ..... 24
3.3.4 Option Initiation ..... 24

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

3.4.1 Character Set Transparency ..... 25
3.4.2 Telnet Commands ..... 26
3.4.3 TCP Connection Errors ..... 26
3.4.4 Non-Default Telnet Contact Port ..... 26
3.4.5 Flushing Output ..... 26
3.5. TELNET REQUIREMENTS SUMMARY ..... 27

4. FILE TRANSFER ..... 29
4.1 FILE TRANSFER PROTOCOL -- FTP ..... 29
4.1.1 INTRODUCTION ..... 29
4.1.2. PROTOCOL WALK-THROUGH ..... 29
4.1.2.1 LOCAL Type ..... 29
4.1.2.2 Telnet Format Control ..... 30
4.1.2.3 Page Structure ..... 30
4.1.2.4 Data Structure Transformations ..... 30
4.1.2.5 Data Connection Management ..... 31
4.1.2.6 PASV Command ..... 31
4.1.2.7 LIST and NLST Commands ..... 31
4.1.2.8 SITE Command ..... 32
4.1.2.9 STOU Command ..... 32
4.1.2.10 Telnet End-of-line Code ..... 32
4.1.2.11 FTP Replies ..... 33
4.1.2.12 Connections ..... 34
4.1.2.13 Minimum Implementation; RFC-959 Section ..... 34
4.1.3 SPECIFIC ISSUES ..... 35
4.1.3.1 Non-standard Command Verbs ..... 35
4.1.3.2 Idle Timeout ..... 36
4.1.3.3 Concurrency of Data and Control ..... 36
4.1.3.4 FTP Restart Mechanism ..... 36
4.1.4 FTP/USER INTERFACE ..... 39





4.1.4.1 Pathname Specification ..... 39
4.1.4.2 "QUOTE" Command ..... 40
4.1.4.3 Displaying Replies to User ..... 40
4.1.4.4 Maintaining Synchronization ..... 40
4.1.5 FTP REQUIREMENTS SUMMARY ..... 41
4.2 TRIVIAL FILE TRANSFER PROTOCOL -- TFTP ..... 44
4.2.1 INTRODUCTION ..... 44
4.2.2 PROTOCOL WALK-THROUGH ..... 44
4.2.2.1 Transfer Modes ..... 44
4.2.2.2 UDP Header ..... 44
4.2.3 SPECIFIC ISSUES ..... 44
4.2.3.1 Sorcerer's Apprentice Syndrome ..... 44
4.2.3.2 Timeout Algorithms ..... 46
4.2.3.3 Extensions ..... 46
4.2.3.4 Access Control ..... 46
4.2.3.5 Broadcast Request ..... 46
4.2.4 TFTP REQUIREMENTS SUMMARY ..... 47

5. ELECTRONIC MAIL -- SMTP and RFC-822 ..... 48
5.1 INTRODUCTION ..... 48
5.2 PROTOCOL WALK-THROUGH ..... 48
5.2.1 The SMTP Model ..... 48
5.2.2 Canonicalization ..... 49
5.2.3 VRFY and EXPN Commands ..... 50
5.2.4 SEND, SOML, and SAML Commands ..... 50
5.2.5 HELO Command ..... 50
5.2.6 Mail Relay ..... 51
5.2.7 RCPT Command ..... 52
5.2.8 DATA Command ..... 53
5.2.9 Command Syntax ..... 54
5.2.10 SMTP Replies ..... 54
5.2.11 Transparency ..... 55
5.2.12 WKS Use in MX Processing ..... 55
5.2.13 RFC-822 Message Specification ..... 55
5.2.14 RFC-822 Date and Time Specification ..... 55
5.2.15 RFC-822 Syntax Change ..... 56
5.2.16 RFC-822 Local-part ..... 56
5.2.17 Domain Literals ..... 57
5.2.18 Common Address Formatting Errors ..... 58
5.2.19 Explicit Source Routes ..... 58
5.3 SPECIFIC ISSUES ..... 59

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

5.3.1.2 Receiving strategy ..... 61
5.3.2 Timeouts in SMTP ..... 61
5.3.3 Reliable Mail Receipt ..... 63
5.3.4 Reliable Mail Transmission ..... 63
5.3.5 Domain Name Support ..... 65





5.3.6 Mailing Lists and Aliases ..... 65
5.3.7 Mail Gatewaying ..... 66
5.3.8 Maximum Message Size ..... 68
5.4 SMTP REQUIREMENTS SUMMARY ..... 69

6. SUPPORT SERVICES ..... 72
6.1 DOMAIN NAME TRANSLATION ..... 72
6.1.1 INTRODUCTION ..... 72
6.1.2 PROTOCOL WALK-THROUGH ..... 72
6.1.2.1 Resource Records with Zero TTL ..... 73
6.1.2.2 QCLASS Values ..... 73
6.1.2.3 Unused Fields ..... 73
6.1.2.4 Compression ..... 73
6.1.2.5 Misusing Configuration Info ..... 73
6.1.3 SPECIFIC ISSUES ..... 74
6.1.3.1 Resolver Implementation ..... 74
6.1.3.2 Transport Protocols ..... 75
6.1.3.3 Efficient Resource Usage ..... 77
6.1.3.4 Multihomed Hosts ..... 78
6.1.3.5 Extensibility ..... 79
6.1.3.6 Status of RR Types ..... 79
6.1.3.7 Robustness ..... 80
6.1.3.8 Local Host Table ..... 80
6.1.4 DNS USER INTERFACE ..... 81
6.1.4.1 DNS Administration ..... 81
6.1.4.2 DNS User Interface ..... 81
6.1.4.3 Interface Abbreviation Facilities ..... 82
6.1.5 DOMAIN NAME SYSTEM REQUIREMENTS SUMMARY ..... 84
6.2 HOST INITIALIZATION ..... 87
6.2.1 INTRODUCTION ..... 87
6.2.2 REQUIREMENTS ..... 87
6.2.2.1 Dynamic Configuration ..... 87
6.2.2.2 Loading Phase ..... 89
6.3 REMOTE MANAGEMENT ..... 90
6.3.1 INTRODUCTION ..... 90
6.3.2 PROTOCOL WALK-THROUGH ..... 90
6.3.3 MANAGEMENT REQUIREMENTS SUMMARY ..... 92

7. REFERENCES ..... 93





## 1. INTRODUCTION

This document is one of a pair that defines and discusses the requirements for host system implementations of the Internet protocol suite. This RFC covers the applications layer and support protocols. Its companion RFC, "Requirements for Internet Hosts -- Communications Layers" [INTRO:1] covers the lower layer protocols: transport layer, IP layer, and link layer.

These documents are intended to provide guidance for vendors

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

wisdom, contributed by members of the Internet research and vendor communities.

This RFC enumerates standard protocols that a host connected to the Internet must use, and it incorporates by reference the RFCs and other documents describing the current specifications for these protocols. It corrects errors in the referenced documents and adds additional discussion and guidance for an implementor.

For each protocol, this document also contains an explicit set of requirements, recommendations, and options. The reader must understand that the list of requirements in this document is incomplete by itself; the complete set of requirements for an Internet host is primarily defined in the standard protocol specification documents, with the corrections, amendments, and supplements contained in this RFC.

A good-faith implementation of the protocols that was produced after careful reading of the RFC's and with some interaction with the Internet technical community, and that followed good communications software engineering practices, should differ from the requirements of this document in only minor ways. Thus, in many cases, the "requirements" in this RFC are already stated or implied in the standard protocol documents, so that their inclusion here is, in a sense, redundant. However, they were included because some past implementation has made the wrong choice, causing problems of interoperability, performance, and/or robustness.

This document includes discussion and explanation of many of the requirements and recommendations. A simple list of requirements would be dangerous, because:

- Some required features are more important than others, and some features are optional.
- There may be valid reasons why particular vendor products that



are designed for restricted contexts might choose to use different specifications.

However, the specifications of this document must be followed to meet the general goal of arbitrary host interoperation across the diversity and complexity of the Internet system. Although most current implementations fail to meet these requirements in various ways, some minor and some major, this specification is the ideal towards which we need to move.

These requirements are based on the current level of Internet architecture. This document will be updated as required to provide additional clarifications or to include additional information in those areas in which specifications are still evolving.

This introductory section begins with general advice to host software vendors, and then gives some guidance on reading the rest of the document. Section 2 contains general requirements that may be applicable to all application and support protocols. Sections 3, 4, and 5 contain the requirements on protocols for the three major applications: Telnet, file transfer, and electronic mail, respectively. Section 6 covers the support applications: the domain name system, system initialization, and management. Finally, all references will be found in Section 7.

## 1.1 The Internet Architecture

For a brief introduction to the Internet architecture from a host viewpoint, see Section 1.1 of [INTRO:1]. That section also contains recommended references for general background on the Internet architecture.

## 1.2 General Considerations

There are two important lessons that vendors of Internet host

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

### 1.2.1 Continuing Internet Evolution

The enormous growth of the Internet has revealed problems of management and scaling in a large datagram-based packet communication system. These problems are being addressed, and as a result there will be continuing evolution of the specifications described in this document. These changes will be carefully planned and controlled, since there is extensive participation in this planning by the vendors and by the organizations responsible for operations of the networks.



Development, evolution, and revision are characteristic of computer network protocols today, and this situation will persist for some years. A vendor who develops computer communication software for the Internet protocol suite (or any other protocol suite!) and then fails to maintain and update that software for changing specifications is going to leave a trail of unhappy customers. The Internet is a large communication network, and the users are in constant contact through it. Experience has shown that knowledge of deficiencies in vendor software propagates quickly through the Internet technical community.

### 1.2.2 Robustness Principle

At every layer of the protocols, there is a general rule whose application can lead to enormous benefits in robustness and interoperability:

> "Be liberal in what you accept, and
> conservative in what you send"

Software should be written to deal with every conceivable error, no matter how unlikely; sooner or later a packet will come in with that particular combination of errors and attributes, and unless the software is prepared, chaos can ensue. In general, it is best to assume that the network is filled with malevolent entities that will send in packets designed to have the worst possible effect. This assumption will lead to suitable protective design, although the most serious problems in the Internet have been caused by unenvisaged mechanisms triggered by low-probability events; mere human malice would never have taken so devious a course!

Adaptability to change must be designed into all levels of Internet host software. As a simple example, consider a protocol specification that contains an enumeration of values for a particular header field -- e.g., a type field, a port number, or an error code; this enumeration must be assumed to be incomplete. Thus, if a protocol specification defines four possible error codes, the software must not break when a fifth code shows up. An undefined code might be logged (see below), but it must not cause a failure.

The second part of the principle is almost as important: software on other hosts may contain deficiencies that make it unwise to exploit legal but obscure protocol features. It is unwise to stray far from the obvious and simple, lest untoward effects result elsewhere. A corollary of this is "watch out



for misbehaving hosts"; host software should be prepared, not just to survive other misbehaving hosts, but also to cooperate to limit the amount of disruption such hosts can cause to the shared communication facility.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

# 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.