

Network Working Group  
Request for Comments: 1122

Internet Engineering Task Force  
R. Braden, Editor  
October 1989

## Requirements for Internet Hosts -- Communication Layers

### 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 is one RFC of a pair that defines and discusses the requirements for Internet host software. This RFC covers the communications protocol layers: link layer, IP layer, and transport layer; its companion RFC-1123 covers the application and support protocols.

### Table of Contents

1.	INTRODUCTION .....	5
1.1	The Internet Architecture .....	6
1.1.1	Internet Hosts .....	6
1.1.2	Architectural Assumptions .....	7
1.1.3	Internet Protocol Suite .....	8
1.1.4	Embedded Gateway Code .....	10
1.2	General Considerations .....	12
1.2.1	Continuing Internet Evolution .....	12
1.2.2	Robustness Principle .....	12
1.2.3	Error Logging .....	13
1.2.4	Configuration .....	14
1.3	Reading this Document .....	15
1.3.1	Organization .....	15
1.3.2	Requirements .....	16
1.3.3	Terminology .....	17
1.4	Acknowledgments .....	20
2.	LINK LAYER .....	21
2.1	INTRODUCTION .....	21

RFC1122

INTRODUCTION

October 1989

2.2	PROTOCOL WALK-THROUGH .....	21
2.3	SPECIFIC ISSUES .....	21
2.3.1	Trailer Protocol Negotiation .....	21
2.3.2	Address Resolution Protocol -- ARP .....	22
2.3.2.1	ARP Cache Validation .....	22
2.3.2.2	ARP Packet Queue .....	24
2.3.3	Ethernet and IEEE 802 Encapsulation .....	24
2.4	LINK/INTERNET LAYER INTERFACE .....	25
2.5	LINK LAYER REQUIREMENTS SUMMARY .....	26
3.	INTERNET LAYER PROTOCOLS .....	27
3.1	INTRODUCTION .....	27
3.2	PROTOCOL WALK-THROUGH .....	29
3.2.1	Internet Protocol -- IP .....	29
3.2.1.1	Version Number .....	29
3.2.1.2	Checksum .....	29
3.2.1.3	Addressing .....	29
3.2.1.4	Fragmentation and Reassembly .....	32
3.2.1.5	Identification .....	32
3.2.1.6	Type-of-Service .....	33
3.2.1.7	Time-to-Live .....	34
3.2.1.8	Options .....	35
3.2.2	Internet Control Message Protocol -- ICMP .....	38
3.2.2.1	Destination Unreachable .....	39
3.2.2.2	Redirect .....	40
3.2.2.3	Source Quench .....	41
3.2.2.4	Time Exceeded .....	41
3.2.2.5	Parameter Problem .....	42
3.2.2.6	Echo Request/Reply .....	42
3.2.2.7	Information Request/Reply .....	43
3.2.2.8	Timestamp and Timestamp Reply .....	43
3.2.2.9	Address Mask Request/Reply .....	45
3.2.3	Internet Group Management Protocol IGMP .....	47
3.3	SPECIFIC ISSUES .....	47
3.3.1	Routing Outbound Datagrams .....	47
3.3.1.1	Local/Remote Decision .....	47
3.3.1.2	Gateway Selection .....	48
3.3.1.3	Route Cache .....	49
3.3.1.4	Dead Gateway Detection .....	51
3.3.1.5	New Gateway Selection .....	55
3.3.1.6	Initialization .....	56
3.3.2	Reassembly .....	56
3.3.3	Fragmentation .....	58
3.3.4	Local Multihoming .....	60
3.3.4.1	Introduction .....	60
3.3.4.2	Multihoming Requirements .....	61
3.3.4.3	Choosing a Source Address .....	64
3.3.5	Source Route Forwarding .....	65

3.3.6	Broadcasts .....	66
3.3.7	IP Multicasting .....	67
3.3.8	Error Reporting .....	69
3.4	INTERNET/TRANSPORT LAYER INTERFACE .....	69
3.5	INTERNET LAYER REQUIREMENTS SUMMARY .....	72
4.	TRANSPORT PROTOCOLS .....	77
4.1	USER DATAGRAM PROTOCOL -- UDP .....	77
4.1.1	INTRODUCTION .....	77
4.1.2	PROTOCOL WALK-THROUGH .....	77
4.1.3	SPECIFIC ISSUES .....	77
4.1.3.1	Ports .....	77
4.1.3.2	IP Options .....	77
4.1.3.3	ICMP Messages .....	78
4.1.3.4	UDP Checksums .....	78
4.1.3.5	UDP Multihoming .....	79
4.1.3.6	Invalid Addresses .....	79
4.1.4	UDP/APPLICATION LAYER INTERFACE .....	79
4.1.5	UDP REQUIREMENTS SUMMARY .....	80
4.2	TRANSMISSION CONTROL PROTOCOL -- TCP .....	82
4.2.1	INTRODUCTION .....	82
4.2.2	PROTOCOL WALK-THROUGH .....	82
4.2.2.1	Well-Known Ports .....	82
4.2.2.2	Use of Push .....	82
4.2.2.3	Window Size .....	83
4.2.2.4	Urgent Pointer .....	84
4.2.2.5	TCP Options .....	85
4.2.2.6	Maximum Segment Size Option .....	85
4.2.2.7	TCP Checksum .....	86
4.2.2.8	TCP Connection State Diagram .....	86
4.2.2.9	Initial Sequence Number Selection .....	87
4.2.2.10	Simultaneous Open Attempts .....	87
4.2.2.11	Recovery from Old Duplicate SYN .....	87
4.2.2.12	RST Segment .....	87
4.2.2.13	Closing a Connection .....	87
4.2.2.14	Data Communication .....	89
4.2.2.15	Retransmission Timeout .....	90
4.2.2.16	Managing the Window .....	91
4.2.2.17	Probing Zero Windows .....	92
4.2.2.18	Passive OPEN Calls .....	92
4.2.2.19	Time to Live .....	93
4.2.2.20	Event Processing .....	93
4.2.2.21	Acknowledging Queued Segments .....	94
4.2.3	SPECIFIC ISSUES .....	95
4.2.3.1	Retransmission Timeout Calculation .....	95
4.2.3.2	When to Send an ACK Segment .....	96
4.2.3.3	When to Send a Window Update .....	97
4.2.3.4	When to Send Data .....	98

RFC1122

INTRODUCTION

October 1989

4.2.3.5	TCP Connection Failures .....	100
4.2.3.6	TCP Keep-Alives .....	101
4.2.3.7	TCP Multihoming .....	103
4.2.3.8	IP Options .....	103
4.2.3.9	ICMP Messages .....	103
4.2.3.10	Remote Address Validation .....	104
4.2.3.11	TCP Traffic Patterns .....	104
4.2.3.12	Efficiency .....	105
4.2.4	TCP/APPLICATION LAYER INTERFACE .....	106
4.2.4.1	Asynchronous Reports .....	106
4.2.4.2	Type-of-Service .....	107
4.2.4.3	Flush Call .....	107
4.2.4.4	Multihoming .....	108
4.2.5	TCP REQUIREMENT SUMMARY .....	108
5.	REFERENCES .....	112

RFC1122

INTRODUCTION

October 1989

## 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 communication protocol layers: link layer, IP layer, and transport layer. Its companion RFC, "Requirements for Internet Hosts -- Application and Support" [INTRO:1], covers the application layer protocols. This document should also be read in conjunction with "Requirements for Internet Gateways" [INTRO:2].

These documents are intended to provide guidance for vendors, implementors, and users of Internet communication software. They represent the consensus of a large body of technical experience and wisdom, contributed by the 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:

- o Some required features are more important than others, and some features are optional.

# 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.