

Network Working Group  
Request for Comments: 2499  
Category: Informational

A. Ramos  
ISI  
July 1999

## Request for Comments Summary

RFC Numbers 2400-2499

### Status of This Memo

This RFC is a slightly annotated list of the 100 RFCs from RFC 2400 through RFCs 2499. This is a status report on these RFCs. This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

### Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

### Note

Many RFCs, but not all, are Proposed Standards, Draft Standards, or Standards. Since the status of these RFCs may change during the standards processing, we note here only that they are on the standards track. Please see the latest edition of "Internet Official Protocol Standards" for the current state and status of these RFCs. In the following, RFCs on the standards track are marked [STANDARDS-TRACK].

RFC ---	Author -----	Date ----	Title -----
2499	Ramos	July 1999	Request for Comments Summary

This memo.

2498	Mahdavi	Jan 1999	IPPM Metrics for Measuring Connectivity
------	---------	----------	---

This memo defines a series of metrics for connectivity between a pair of Internet hosts. It builds on notions introduced and discussed in RFC 2330, the IPPM framework document. This memo defines an Experimental Protocol for the Internet community.

2497      Souvatzis              Jan 1999              Transmission of IPv6 Packets  
   over ARCnet Networks

This memo specifies a frame format for transmission of IPv6 packets and the method of forming IPv6 link-local and statelessly autoconfigured addresses on ARCnet networks. It also specifies the content of the Source/Target Link-layer Address option used by the Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement and Redirect messages described in, when those messages are transmitted on an ARCnet. [STANDARDS-TRACK]

2496      Fowler                  Jan 1999              Definitions of Managed Objects  
   for the DS3/E3 Interface Type

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes objects used for managing DS3 and E3 interfaces. This document is a companion document with Definitions of Managed Objects for the DS0 (RFC 2494), DS1/E1/DS2/E2 (RFC 2495), and the work in progress SONET/SDH Interface Types. [STANDARDS-TRACK]

2495      Fowler                  Jan 1999              Definitions of Managed Objects  
   for the DS1, E1, DS2 and E2  
   Interface Types

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes objects used for managing DS1, E1, DS2 and E2 interfaces. This document is a companion document with Definitions of Managed Objects for the DS0 (RFC 2494), DS3/E3 (RFC 2496), and the work in progress, SONET/SDH Interface Types. [STANDARDS-TRACK]

2494      Fowler                  Jan 1999              Definitions of Managed Objects  
   for the DS0 and DS0 Bundle  
   Interface Type

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes objects used for managing DS0 and DS0 Bundle interfaces. This document is a companion document with Definitions of Managed Objects for the DS1/E1/DS2/E2 (RFC 2495), DS3/E3 (RFC 2496), and the work in progress, SONET/SDH Interface Types. [STANDARDS-TRACK]

2493      Tesink                      Jan 1999                      Textual Conventions for MIB  
Modules Using Performance  
History Based on 15 Minute  
Intervals

This document defines a set of Textual Conventions for MIB modules which make use of performance history data based on 15 minute intervals.  
[STANDARDS-TRACK]

2492      Armitage                    Jan 1999                    IPv6 over ATM Networks

This document is a companion to the ION working group's architecture document, "IPv6 over Non Broadcast Multiple Access (NBMA) networks". It provides specific details on how to apply the IPv6 over NBMA architecture to ATM networks. This architecture allows conventional host-side operation of the IPv6 Neighbor Discovery protocol, while also supporting the establishment of 'shortcut' ATM forwarding paths (when using SVCs). Operation over administratively configured Point to Point PVCs is also supported. [STANDARDS-TRACK]

2491      Armitage                    Jan 1999                    IPv6 over Non-Broadcast  
Multiple Access (NBMA) networks

This document describes a general architecture for IPv6 over NBMA networks. [STANDARDS-TRACK]

2490      Pullen                        Jan 1999                    A Simulation Model for IP  
Multicast with RSVP

This document describes a detailed model of IPv4 multicast with RSVP that has been developed using the OPNET simulation package, with protocol procedures defined in the C language. This memo provides information for the Internet community.

2489      Droms                            Jan 1999                    Procedure for Defining New  
DHCP Options

This document describes the procedure for defining new DHCP options. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

2488      Allman                      Jan 1999                      Enhancing TCP Over Satellite  
Channels using Standard  
Mechanisms

The Transmission Control Protocol (TCP) provides reliable delivery of data across any network path, including network paths containing satellite channels. While TCP works over satellite channels there are several IETF standardized mechanisms that enable TCP to more effectively utilize the available capacity of the network path. This document outlines some of these TCP mitigations. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

2487      Hoffman                      Jan 1999                      SMTP Service Extension for  
Secure SMTP over TLS

This document describes an extension to the SMTP service that allows an SMTP server and client to use transport-layer security to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers. [STANDARDS-TRACK]

2486      Aboba                              Jan 1999                      The Network Access Identifier

This document proposes syntax for the Network Access Identifier (NAI), the userID submitted by the client during PPP authentication. [STANDARDS-TRACK]

2485      Drach                              Jan 1999                      DHCP Option for The Open  
Group's User Authentication  
Protocol

This document defines a DHCP option that contains a list of pointers to User Authentication Protocol servers that provide user authentication services for clients that conform to The Open Group Network Computing Client Technical Standard. [STANDARDS-TRACK]

2484      Zorn                      Jan 1999              PPP LCP Internationalization  
Configuration Option

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol (LCP), which allows negotiation of an Authentication Protocol for authenticating its peer before allowing Network Layer protocols to transmit over the link. [STANDARDS-TRACK]

2483      Mealling                  Jan 1999              URI Resolution Services  
Necessary for URN Resolution

Retrieving the resource identified by a Uniform Resource Identifier (URI) is only one of the operations that can be performed on a URI. One might also ask for and get a list of other identifiers that are aliases for the original URI or a bibliographic description of the resource the URI denotes, for example. This applies to both Uniform Resource Names (URNs) and Uniform Resource Locators (URLs). Uniform Resource Characteristics (URCs) are discussed in this document but only as descriptions of resources rather than identifiers. This memo defines an Experimental Protocol for the Internet community.

2482      Whistler                      Jan 1999              Language Tagging in Unicode  
Plain Text

This document proposed a mechanism for language tagging in plain text. This memo provides information for the Internet community.

2481      Ramakrishnan                  Jan 1999              A Proposal to add Explicit  
Congestion Notification (ECN)  
to IP

This note describes a proposed addition of ECN (Explicit Congestion Notification) to IP. This memo defines an Experimental Protocol for the Internet community.

2480      Freed                            Jan 1999              Gateways and MIME Security  
Multiparts

This document examines the problems associated with use of MIME security multiparts and gateways to non-MIME environments. [STANDARDS-TRACK]

2479      Adams                      Dec 1998                      Independent Data Unit  
Protection Generic Security Service  
Application Program Interface  
(IDUP-GSS-API)

The IDUP-GSS-API extends the GSS-API for applications requiring protection of a generic data unit (such as a file or message) in a way which is independent of the protection of any other data unit and independent of any concurrent contact with designated "receivers" of the data unit. This memo provides information for the Internet community.

2478      Baize                      Dec 1998                      The Simple and Protected  
GSS-API Negotiation Mechanism

This document specifies a Security Negotiation Mechanism for the Generic Security Service Application Program Interface (GSS-API). [STANDARDS-TRACK]

2477      Aboba                      Jan 1999                      Criteria for Evaluating  
Roaming Protocols

This document describes requirements for the provisioning of "roaming capability" for dialup Internet users. "Roaming capability" is defined as the ability to use multiple Internet service providers (ISPs), while maintaining a formal, customer-vendor relationship with only one. This memo provides information for the Internet community.

2476      Gellens                      Dec 1998                      Message Submission

This memo describes a low cost, deterministic means for messages to be identified as submissions, and specifies what actions are to be taken by a submission server. [STANDARDS-TRACK]

2475      Blake                      Dec 1998                      An Architecture for  
Differentiated Services

This document defines an architecture for implementing scalable service differentiation in the Internet. This memo provides information for the Internet community.

2474      Nichols                      Dec 1998                      Definition of the  
Differentiated Services Field  
(DS Field) in the IPv4 and  
IPv6 Headers

This document defines the IP header field, called the DS (for differentiated services) field. [STANDARDS-TRACK]

2473      Conta                        Dec 1998                      Generic Packet Tunneling in  
IPv6 Specification

This document defines the model and generic mechanisms for IPv6 encapsulation of Internet packets, such as IPv6 and IPv4. [STANDARDS-TRACK]

2472      Haskin                        Dec 1998                      IP Version 6 over PPP

This document defines the method for transmission of IP Version 6 packets over PPP links as well as the Network Control Protocol (NCP) for establishing and configuring the IPv6 over PPP. It also specifies the method of forming IPv6 link-local addresses on PPP links. [STANDARDS-TRACK]

2471      Hinden                        Dec 1998                      IPv6 Testing Address Allocation

This document describes an allocation plan for IPv6 addresses to be used in testing IPv6 prototype software. This memo defines an Experimental Protocol for the Internet community.

2470      Crawford                        Dec 1998                      Transmission of IPv6 Packets  
over Token Ring Networks

This memo specifies the MTU and frame format for transmission of IPv6 packets on Token Ring networks. [STANDARDS-TRACK]

2469      Narten                      Dec 1998                      A Caution On The Canonical  
   Ordering Of Link-Layer Addresses

Protocols such as ARP and Neighbor Discovery have data fields that contain link-layer addresses. In order to interoperate properly, a sender setting such a field must insure that the receiver extracts those bits and interprets them correctly. In most cases, such fields must be in "canonical form". Unfortunately, not all LAN adaptors are consistent in their use of canonical form, and implementations may need to explicitly bit swap individual bytes in order to obtain the correct format. This document provides information to implementors to help them avoid the pitfall of using non-canonical forms when canonical forms are required. This memo provides information for the Internet community.

2468      Cerf                              Oct 1998                      I REMEMBER IANA

A long time ago, in a network, far far away, a great adventure took place!. This memo provides information for the Internet community.

2467      Crawford                      Dec 1998                      Transmission of IPv6 Packets  
   over FDDI Networks

This document specifies the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on FDDI networks. [STANDARDS-TRACK]

2466      Haskin                              Dec 1998                      Management Information Base  
   for IP Version 6: ICMPv6 Group

This document is one in the series of documents that define various MIB object groups for IPv6. Specifically, the ICMPv6 group is defined in this document. [STANDARDS-TRACK]

2465      Haskin                              Dec 1998                      Management Information Base  
   for IP Version 6: Textual  
   Conventions and General Group

This document is one in the series of documents that provide MIB definitions for for IP Version 6. Specifically, the IPv6 MIB textual conventions as well as the IPv6 MIB General group is defined in this document. [STANDARDS-TRACK]



2464      Crawford              Dec 1998              Transmission of IPv6 Packets  
   over Ethernet Networks

This document specifies the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on Ethernet networks. It also specifies the content of the Source/Target Link-layer Address option used in Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement and Redirect messages when those messages are transmitted on an Ethernet. [STANDARDS-TRACK]

2463      Conta                  Dec 1998              Internet Control Message  
   Protocol (ICMPv6) for the  
   Internet Protocol Version 6  
   (IPv6) Specification

This document specifies a set of Internet Control Message Protocol (ICMP) messages for use with version 6 of the Internet Protocol (IPv6). [STANDARDS-TRACK]

2462      Thomson                 Dec 1998              IPv6 Stateless Address  
   Autoconfiguration

This document specifies the steps a host takes in deciding how to autoconfigure its interfaces in IP version 6. [STANDARDS-TRACK]

2461      Narten                    Dec 1998              Neighbor Discovery for IP  
   Version 6 (IPv6)

This document specifies the Neighbor Discovery protocol for IP Version 6. [STANDARDS-TRACK]

2460      Deering                    Dec 1998              Internet Protocol, Version 6  
   (IPv6) Specification

This document specifies version 6 of the Internet Protocol (IPv6), also sometimes referred to as IP Next Generation or IPng. [STANDARDS-TRACK]

2459      Housley                      Jan 1999                      Internet X.509 Public Key  
   Infrastructure Certificate and  
   CRL Profile

This memo profiles the X.509 v3 certificate and X.509 v2 CRL for use in the Internet. [STANDARDS-TRACK]

2458      Lu                              Nov 1998                      Toward the PSTN/Internet  
   Inter-Networking --Pre-PINT  
   Implementations

This document contains the information relevant to the development of the inter-networking interfaces underway in the Public Switched Telephone Network (PSTN)/Internet Inter-Networking (PINT) Working Group. This memo provides information for the Internet community.

2457      Clouston                      Nov 1998                      Definitions of Managed Objects  
   for Extended Border Node

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines objects for monitoring and controlling network devices with APPN (Advanced Peer-to-Peer Network) EBN (Extended Border Node) capabilities. This memo identifies managed objects for the EBN architecture. [STANDARDS-TRACK]

2456      Clouston                      Nov 1998                      Definitions of Managed Objects  
   for APPN TRAPS

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines objects for receiving notifications from network devices with APPN (Advanced Peer-to-Peer Network) and DLUR (Dependent LU Requester) capabilities. This memo identifies notifications for the APPN and DLUR architecture. [STANDARDS-TRACK]

2455      Clouston              Nov 1998              Definitions of Managed Objects  
   for APPN

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines objects for monitoring and controlling network devices with APPN (Advanced Peer-to-Peer Networking) capabilities. This memo identifies managed objects for the APPN protocol. [STANDARDS-TRACK]

2454      Daniele                Dec 1998              IP Version 6 Management  
   Information Base for the User  
   Datagram Protocol

This document is one in the series of documents that define various MIB objects for IPv6. Specifically, this document is the MIB module which defines managed objects for implementations of the User Datagram Protocol (UDP) over IP Version 6 (IPv6). [STANDARDS-TRACK]

2453      Malkin                 Nov 1998              RIP Version 2

This document specifies an extension of the Routing Information Protocol (RIP) to expand the amount of useful information carried in RIP messages and to add a measure of security. [STANDARDS-TRACK]

2452      Daniele                Dec 1998              IP Version 6 Management  
   Information Base for the  
   Transmission Control Protocol

This document is one in the series of documents that define various MIB objects for IPv6. Specifically, this document is the MIB module which defines managed objects for implementations of the Transmission Control Protocol (TCP) over IP Version 6 (IPv6). [STANDARDS-TRACK]

2451      Pereira                 Nov 1998              The ESP CBC-Mode Cipher  
   Algorithms

This document describes how to use CBC-mode cipher algorithms with the IPsec ESP (Encapsulating Security Payload) Protocol. It not only clearly states how to use certain cipher algorithms, but also how to use all CBC-mode cipher algorithms. [STANDARDS-TRACK]

2450      Hinden                      Dec 1998              Proposed TLA and NLA  
Assignment Rules

This document proposes rules for Top-Level Aggregation Identifiers (TLA ID) and Next-Level Aggregation Identifiers (NLA ID). This memo provides information for the Internet community.

2449      Gellens                      Nov 1998              POP3 Extension Mechanism

This memo updates RFC 1939 to define a mechanism to announce support for optional commands, extensions, and unconditional server behavior.  
[STANDARDS-TRACK]

2448      Civanlar                      Nov 1998              AT&T's Error Resilient Video  
Transmission Technique

This document describes a set of techniques for packet loss resilient transmission of compressed video bitstreams based on reliable delivery of their vital information-carrying segments. This memo provides information for the Internet community.

2447      Dawson                          Nov 1998              iCalendar Message-Based  
Interoperability Protocol (iMIP)

This document specifies a binding from the iCalendar Transport-independent Interoperability Protocol (iTIP) to Internet email-based transports. [STANDARDS-TRACK]

2446      Silverberg                      Nov 1998              iCalendar Transport-Independent  
Interoperability Protocol (iTIP)  
Scheduling Events, BusyTime,  
To-dos and Journal Entries

This document specifies how calendaring systems use iCalendar objects to interoperate with other calendar systems. It does so in a general way so as to allow multiple methods of communication between systems.  
[STANDARDS-TRACK]

2445      Dawson                      Nov 1998                      Internet Calendaring and  
Scheduling Core Object  
Specification (iCalendar)

This memo has been defined to provide the definition of a common format for openly exchanging calendaring and scheduling information across the Internet. [STANDARDS-TRACK]

2444      Newman                      Oct 1998                      The One-Time-Password SASL  
Mechanism

OTP provides a useful authentication mechanism for situations where there is limited client or server trust. Currently, OTP is added to protocols in an ad-hoc fashion with heuristic parsing. This specification defines an OTP SASL mechanism so it can be easily and formally integrated into many application protocols. [STANDARDS-TRACK]

2443      Luciani                      Nov 1998                      A Distributed MARS Service  
Using SCSP

This document describes a method for distributing a MARS service within a LIS. This method uses the Server Cache Synchronization Protocol (SCSP) to synchronize the MARS Server databases within a LIS. When SCSP is used to synchronize the caches of MARS Servers in a LIS, the LIS defines the boundary of an SCSP Server Group (SG). [STANDARDS-TRACK]

2442      Freed                      Nov 1998                      The Batch SMTP Media Type

This document defines a MIME content type suitable for tunneling an ESMTP transaction through any MIME-capable transport. This memo provides information for the Internet community

2441      Cohen                      Nov 1998                      Working with Jon  
Tribute delivered at UCLA,  
October 30, 1998

This memo provides information for the Internet community.

2440      Callas                      Nov 1998                      OpenPGP Message Format

This document is maintained in order to publish all necessary information needed to develop interoperable applications based on the OpenPGP format. [STANDARDS-TRACK]

2439 Villamizar Nov 1998 BGP Route Flap Damping

A usage of the BGP routing protocol is described which is capable of reducing the routing traffic passed on to routing peers and therefore the load on these peers without adversely affecting route convergence time for relatively stable routes. [STANDARDS-TRACK]

2438 O'Dell Oct 1998 Advancement of MIB specifications on the IETF Standards Track

This document specifies the process which the IESG will use to determine if a MIB specification document meets these requirements. It also discusses the rationale for this process. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

2437 Kaliski Oct 1998 PKCS #1: RSA Cryptography Specifications Version 2.0

This memo is the successor to RFC 2313. This document provides recommendations for the implementation of public-key cryptography based on the RSA algorithm. This memo provides information for the Internet community.

2436 Brett Oct 1998 Collaboration between ISOC/IETF and ITU-T

This document describes the collaboration process between the ITU-T and ISOC/IETF. This memo provides information for the Internet community.

2435 Berc Oct 1998 RTP Payload Format for JPEG-compressed Video

This memo describes the RTP payload format for JPEG video streams. [STANDARDS-TRACK]

2434	Narten	Oct 1998	Guidelines for Writing an IANA Considerations Section in RFCs
------	--------	----------	---

This document discusses issues that should be considered in formulating a policy for assigning values to a name space and provides guidelines to document authors on the specific text that must be included in documents that place demands on the IANA. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

2433	Zorn	Oct 1998	Microsoft PPP CHAP Extensions
------	------	----------	-------------------------------

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP defines an extensible Link Control Protocol and a family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols. This memo provides information for the Internet community.

2432	Dubray	Oct 1998	Terminology for IP Multicast Benchmarking
------	--------	----------	---

The purpose of this document is to define terminology specific to the benchmarking of multicast IP forwarding devices. This memo provides information for the Internet community.

2431	Tynan	Oct 1998	RTP Payload Format for BT.656 Video Encoding
------	-------	----------	---

This document specifies the RTP payload format for encapsulating ITU Recommendation BT.656-3 video streams in the Real-Time Transport Protocol (RTP). [STANDARDS-TRACK]

2430	Li	Oct 1998	A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)
------	----	----------	---

This document describes the Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) for Internet Service Providers (ISPs). This memo provides information for the Internet community.

2429      Bormann              Oct 1998              RTP Payload Format for the  
   1998 Version of ITU-T  
   Rec. H.263 Video (H.263+)

This document specifies an RTP payload header format applicable to the transmission of video streams generated based on the 1998 version of ITU-T Recommendation H.263. [STANDARDS-TRACK]

2428      Allman              Sep 1998              FTP Extensions for IPv6 and NATs

This paper specifies extensions to FTP that will allow the protocol to work over IPv4 and IPv6. [STANDARDS-TRACK]

2427      Brown              Sep 1998              Multiprotocol Interconnect  
   over Frame Relay

This memo describes an encapsulation method for carrying network interconnect traffic over a Frame Relay backbone. It covers aspects of both Bridging and Routing. [STANDARDS-TRACK]

2426      Dawson              Sep 1998              vCard MIME Directory Profile

This memo defines the profile of the MIME Content-Type for directory information for a white-pages person object, based on a vCard electronic business card. [STANDARDS-TRACK]

2425      Howes              Sep 1998              A MIME Content-Type for  
   Directory Information

This document defines a MIME Content-Type for holding directory information. [STANDARDS-TRACK]

2424      Vaudreuil              Sep 1998              Content Duration MIME Header  
   Definition

This document describes the MIME header Content-Duration that is intended for use with any timed media content (typically audio/\* or video/\*). [STANDARDS-TRACK]



2423      Vaudreuil              Sep 1998              VPIM Voice Message MIME  
   Sub-type Registration

This document describes the registration of the MIME sub-type multipart/voice-message for use with the Voice Profile for Internet Mail (VPIM). [STANDARDS-TRACK]

2422      Vaudreuil              Sep 1998              Toll Quality Voice - 32 kbit/s  
   ADPCM MIME Sub-type Registration

This document describes the registration of the MIME sub-type audio/32KADPCM for toll quality audio. [STANDARDS-TRACK]

2421      Vaudreuil              Sep 1998              Voice Profile for Internet  
   Mail - version 2

This document profiles Internet mail for voice messaging. [STANDARDS-TRACK]

2420      Kummert                  Sep 1998              The PPP Triple-DES Encryption  
   Protocol (3DESE)

This document provides specific details for the use of the Triple-DES standard (3DES) for encrypting PPP encapsulated packets. [STANDARDS-TRACK]

2419      Sklower                   Sep 1998              The PPP DES Encryption  
   Protocol, Version 2 (DESE-bis)

This document provides specific details for the use of the DES standard for encrypting PPP encapsulated packets. [STANDARDS-TRACK]

2418      Bradner                   Sep 1998              IETF Working Group  
   Guidelines and Procedures

This document describes the guidelines and procedures for formation and operation of IETF working groups. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

2417      Chung                      Sep 1998              Definitions of Managed Objects  
for Multicast over UNI 3.0/3.1  
based ATM Networks

This memo specifies a MIB module in a manner that is both compliant to the SNMPv2 SMI, and semantically identical to the peer SNMPv1 definitions. [STANDARDS-TRACK]

2416      Shepard                    Sep 1998              When TCP Starts Up With Four  
Packets Into Only Three Buffers

This memo is to document a simple experiment. The experiment showed that in the case of a TCP receiver behind a 9600 bps modem link at the edge of a fast Internet where there are only 3 buffers before the modem (and the fourth packet of a four-packet start will surely be dropped), no significant degradation in performance is experienced by a TCP sending with a four-packet start when compared with a normal slow start (which starts with just one packet). This memo provides information for the Internet community.

2415      Poduri                      Sep 1998              Simulation Studies of  
Increased Initial TCP Window Size

This document covers some simulation studies of the effects of increasing the initial window size of TCP. This memo provides information for the Internet community.

2414      Allman                        Sep 1998              Increasing TCP's Initial Window

This document specifies an increase in the permitted initial window for TCP from one segment to roughly 4K bytes. This memo defines an Experimental Protocol for the Internet community.

2413      Weibel                          Sep 1998              Dublin Core Metadata for  
Resource Discovery

This is the first of a set of Informational RFCs describing the Dublin Core. Its purpose is to introduce the Dublin Core and to describe the consensus reached on the semantics of each of the 15 elements. This memo provides information for the Internet community.

2412 Orman Nov 1998 The OAKLEY Key Determination Protocol

This document describes a protocol, named OAKLEY, by which two authenticated parties can agree on secure and secret keying material. The basic mechanism is the Diffie-Hellman key exchange algorithm. This memo provides information for the Internet community.

2411 Thayer Nov 1998 IP Security Document Roadmap

This document is intended to provide guidelines for the development of collateral specifications describing the use of new encryption and authentication algorithms with the ESP protocol, described in and new authentication algorithms used with the AH protocol. This memo provides information for the Internet community.

2410 Glenn Nov 1998 The NULL Encryption Algorithm and Its Use With IPsec

This memo defines the NULL encryption algorithm and its use with the IPsec Encapsulating Security Payload (ESP). [STANDARDS-TRACK]

2409 Harkins Nov 1998 The Internet Key Exchange (IKE)

This memo describes a hybrid protocol. The purpose is to negotiate, and provide authenticated keying material for, security associations in a protected manner. [STANDARDS-TRACK]

2408 Maughan Nov 1998 Internet Security Association and Key Management Protocol (ISAKMP)

This memo describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. [STANDARDS-TRACK]

2407 Piper Nov 1998 The Internet IP Security Domain of Interpretation for ISAKMP

This document defines the Internet IP Security DOI (IPSEC DOI), which instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations. [STANDARDS-TRACK]

2406      Kent                      Nov 1998              IP Encapsulating Security  
   Payload (ESP)

The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. [STANDARDS-TRACK]

2405      Madson                    Nov 1998              The ESP DES-CBC Cipher  
   Algorithm With Explicit IV

This document describes the use of the DES Cipher algorithm in Cipher Block Chaining Mode, with an explicit IV, as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP). [STANDARDS-TRACK]

2404      Madson                    Nov 1998              The Use of HMAC-SHA-1-96  
   within ESP and AH

This memo describes the use of the HMAC algorithm in conjunction with the SHA-1 algorithm as an authentication mechanism within the revised IPSEC Encapsulating Security Payload and the revised IPSEC Authentication Header. [STANDARDS-TRACK]

2403      Madson                    Nov 1998              The Use of HMAC-MD5-96 within  
   ESP and AH

This memo describes the use of the HMAC algorithm in conjunction with the MD5 algorithm as an authentication mechanism within the revised IPSEC Encapsulating Security Payload and the revised IPSEC Authentication Header. [STANDARDS-TRACK]

2402      Kent                      Nov 1998              IP Authentication Header

The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "authentication"), and to provide protection against replays. [STANDARDS-TRACK]

2401      Kent                      Nov 1998              Security Architecture for the  
Internet Protocol

This memo specifies the base architecture for IPsec compliant systems.  
[STANDARDS-TRACK]

2400      IAB                      Sep 1998              INTERNET OFFICIAL PROTOCOL  
STANDARDS

This memo describes the state of standardization of protocols used in  
the Internet as determined by the Internet Architecture Board (IAB).  
This memo is an Internet Standard. [STANDARDS-TRACK]

#### Security Considerations

This memo does not affect the technical security of the Internet, but  
it does cite some security specifications.

#### Author's Address

Alegre Ramos  
University of Southern California  
Information Sciences Institute  
4676 Admiralty Way  
Marina del Rey, CA 90292

Phone: (310) 822-1511

EMail: ramos@isi.edu

## Full Copyright Statement

Copyright (C) The Internet Society (1999). 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 implementation 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.

## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

