

Network Working Group  
Request for Comments: 3499  
Category: Informational

S. Ginoza  
ISI  
December 2003

## Request for Comments Summary

RFC Numbers 3400-3499

### Status of This Memo

This RFC is a slightly annotated list of the 100 RFCs from RFC 3400 through RFC 3499. 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 (2003). 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 -----
3499	Ginoza		Request for Comments Summary

This memo.

3498      Kuhfeld                      Mar 2003                      Definitions of Managed Objects  
for Synchronous Optical  
Network (SONET) Linear  
Automatic Protection Switching  
(APS) Architectures

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP based internets. In particular, it defines objects for managing networks using Synchronous Optical Network (SONET) linear Automatic Protection Switching (APS) architectures. [STANDARDS TRACK]

3497      Gharai                        Mar 2003                      RTP Payload Format for  
Society of Motion Picture and  
Television Engineers (SMPTE)  
292M Video

This memo specifies an RTP payload format for encapsulating uncompressed High Definition Television (HDTV) as defined by the Society of Motion Picture and Television Engineers (SMPTE) standard, SMPTE 292M. SMPTE is the main standardizing body in the motion imaging industry and the SMPTE 292M standard defines a bit-serial digital interface for local area HDTV transport. [STANDARDS TRACK]

3496      Malis                            Mar 2003                      Protocol Extension for Support  
of Asynchronous Transfer Mode  
(ATM) Service Class-aware  
Multiprotocol Label Switching  
(MPLS) Traffic Engineering

This document specifies a Resource ReSerVation Protocol-Traffic Engineering (RSVP-TE) signaling extension for support of Asynchronous Transfer Mode (ATM) Service Class-aware Multiprotocol Label Switching (MPLS) Traffic Engineering. This memo provides information for the Internet community.

3495      Beser                      Mar 2003                      Dynamic Host Configuration  
   Protocol (DHCP) Option  
   for CableLabs Client  
   Configuration

This document defines a Dynamic Host Configuration Protocol (DHCP) option that will be used to configure various devices deployed within CableLabs architectures. Specifically, the document describes DHCP option content that will be used to configure one class of CableLabs client device: a PacketCable Media Terminal Adapter (MTA). The option content defined within this document will be extended as future CableLabs client devices are developed. [STANDARDS TRACK]

3494      Zeilenga                    Mar 2003                    Lightweight Directory Access  
   Protocol version 2 (LDAPv2)  
   to Historic Status

This document recommends the retirement of version 2 of the Lightweight Directory Access Protocol (LDAPv2) and other dependent specifications, and discusses the reasons for doing so. This document recommends RFC 1777, 1778, 1779, 1781, and 2559 (as well as documents they superseded) be moved to Historic status. This memo provides information for the Internet community.

3493      Gilligan                      Mar 2003                      Basic Socket Interface  
   Extensions for IPv6

The de facto standard Application Program Interface (API) for TCP/IP applications is the "sockets" interface. Although this API was developed for Unix in the early 1980s it has also been implemented on a wide variety of non-Unix systems. TCP/IP applications written using the sockets API have in the past enjoyed a high degree of portability and we would like the same portability with IPv6 applications. But changes are required to the sockets API to support IPv6 and this memo describes these changes. These include a new socket address structure to carry IPv6 addresses, new address conversion functions, and some new socket options. These extensions are designed to provide access to the basic IPv6 features required by TCP and UDP applications, including multicasting, while introducing a minimum of change into the system and providing complete compatibility for existing IPv4 applications. Additional extensions for advanced IPv6 features (raw sockets and access to the IPv6 extension headers) are defined in another document. This memo provides information for the Internet community.

3492	Costello	Mar 2003	Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)
------	----------	----------	--

Punycode is a simple and efficient transfer encoding syntax designed for use with Internationalized Domain Names in Applications (IDNA). It uniquely and reversibly transforms a Unicode string into an ASCII string. ASCII characters in the Unicode string are represented literally, and non-ASCII characters are represented by ASCII characters that are allowed in host name labels (letters, digits, and hyphens). This document defines a general algorithm called Bootstring that allows a string of basic code points to uniquely represent any string of code points drawn from a larger set. Punycode is an instance of Bootstring that uses particular parameter values specified by this document, appropriate for IDNA. [STANDARDS TRACK]

3491	Hoffman	Mar 2003	Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)
------	---------	----------	---

This document describes how to prepare internationalized domain name (IDN) labels in order to increase the likelihood that name input and name comparison work in ways that make sense for typical users throughout the world. This profile of the stringprep protocol is used as part of a suite of on-the-wire protocols for internationalizing the Domain Name System (DNS). [STANDARDS TRACK]

3490	Faltstrom	Mar 2003	Internationalizing Domain Names in Applications (IDNA)
------	-----------	----------	--

Until now, there has been no standard method for domain names to use characters outside the ASCII repertoire. This document defines internationalized domain names (IDNs) and a mechanism called Internationalizing Domain Names in Applications (IDNA) for handling them in a standard fashion. IDNs use characters drawn from a large repertoire (Unicode), but IDNA allows the non-ASCII characters to be represented using only the ASCII characters already allowed in so-called host names today. This backward-compatible representation is required in existing protocols like DNS, so that IDNs can be introduced with no changes to the existing infrastructure. IDNA is only meant for processing domain names, not free text. [STANDARDS TRACK]

3489      Rosenberg      Mar 2003      STUN - Simple Traversal of  
User Datagram Protocol (UDP)  
Through Network Address  
Translators (NATs)

Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) is a lightweight protocol that allows applications to discover the presence and types of NATs and firewalls between them and the public Internet. It also provides the ability for applications to determine the public Internet Protocol (IP) addresses allocated to them by the NAT. STUN works with many existing NATs, and does not require any special behavior from them. As a result, it allows a wide variety of applications to work through existing NAT infrastructure. [STANDARDS TRACK]

3488      Wu      Feb 2003      Cisco Systems Router-port  
Group Management Protocol  
(RGMP)

This document describes the Router-port Group Management Protocol (RGMP). This protocol was developed by Cisco Systems and is used between multicast routers and switches to restrict multicast packet forwarding in switches to those routers where the packets may be needed.

RGMP is designed for backbone switched networks where multiple, high speed routers are interconnected. This memo provides information for the Internet community.

3487      Schulzrinne      Feb 2003      Requirements for Resource  
Priority Mechanisms for the  
Session Initiation Protocol  
(SIP)

This document summarizes requirements for prioritizing access to circuit-switched network, end system and proxy resources for emergency preparedness communications using the Session Initiation Protocol (SIP). This memo provides information for the Internet community.

3486      Camarillo      Feb 2003      Compressing the Session  
Initiation Protocol (SIP)

This document describes a mechanism to signal that compression is desired for one or more Session Initiation Protocol (SIP) messages. It also states when it is appropriate to send compressed SIP messages to a SIP entity. [STANDARDS TRACK]

3485      Garcia-Martin      Feb 2003      The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)

The Session Initiation Protocol (SIP) is a text-based protocol for initiating and managing communication sessions. The protocol can be compressed by using Signaling Compression (SigComp). Similarly, the Session Description Protocol (SDP) is a text-based protocol intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. This memo defines the SIP/SDP-specific static dictionary that SigComp may use in order to achieve higher efficiency. The dictionary is compression algorithm independent. [STANDARDS TRACK]

3484      Draves                      Feb 2003      Default Address Selection for Internet Protocol version 6 (IPv6)

This document describes two algorithms, for source address selection and for destination address selection. The algorithms specify default behavior for all Internet Protocol version 6 (IPv6) implementations. They do not override choices made by applications or upper-layer protocols, nor do they preclude the development of more advanced mechanisms for address selection. The two algorithms share a common context, including an optional mechanism for allowing administrators to provide policy that can override the default behavior. In dual stack implementations, the destination address selection algorithm can consider both IPv4 and IPv6 addresses - depending on the available source addresses, the algorithm might prefer IPv6 addresses over IPv4 addresses, or vice-versa.

All IPv6 nodes, including both hosts and routers, must implement default address selection as defined in this specification. [STANDARDS TRACK]

3483	Rawlins	Mar 2003	Framework for Policy Usage Feedback for Common Open Policy Service with Policy Provisioning (COPS-PR)
------	---------	----------	--

Common Open Policy Services (COPS) Protocol (RFC 2748), defines the capability of reporting information to the Policy Decision Point (PDP). The types of report information are success, failure and accounting of an installed state. This document focuses on the COPS Report Type of Accounting and the necessary framework for the monitoring and reporting of usage feedback for an installed state. This memo provides information for the Internet community.

3482	Foster	Feb 2003	Number Portability in the Global Switched Telephone Network (GSTN): An Overview
------	--------	----------	---

This document provides an overview of E.164 telephone number portability (NP) in the Global Switched Telephone Network (GSTN).

NP is a regulatory imperative seeking to liberalize local telephony service competition, by enabling end-users to retain telephone numbers while changing service providers. NP changes the fundamental nature of a dialed E.164 number from a hierarchical physical routing address to a virtual address, thereby requiring the transparent translation of the later to the former. In addition, there are various regulatory constraints that establish relevant parameters for NP implementation, most of which are not network technology specific. Consequently, the implementation of NP behavior consistent with applicable regulatory constraints, as well as the need for interoperation with the existing GSTN NP implementations, are relevant topics for numerous areas of IP telephony works-in-progress with the IETF. This memo provides information for the Internet community.

3481      Inamura, Ed.      Feb 2003      TCP over Second (2.5G)  
and Third (3G) Generation  
Wireless Networks

This document describes a profile for optimizing TCP to adapt so that it handles paths including second (2.5G) and third (3G) generation wireless networks. It describes the relevant characteristics of 2.5G and 3G networks, and specific features of example deployments of such networks. It then recommends TCP algorithm choices for nodes known to be starting or ending on such paths, and it also discusses open issues. The configuration options recommended in this document are commonly found in modern TCP stacks, and are widely available standards-track mechanisms that the community considers safe for use on the general Internet. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3480      Kompella      Feb 2003      Signalling Unnumbered Links in  
CR-LDP (Constraint-Routing  
Label Distribution Protocol)

Current signalling used by Multi-Protocol Label Switching Traffic Engineering (MPLS TE) does not provide support for unnumbered links. This document defines procedures and extensions to Constraint-Routing Label Distribution Protocol (CR-LDP), one of the MPLS TE signalling protocols that are needed in order to support unnumbered links.  
[STANDARDS TRACK]

3479      Farrel, Ed.      Feb 2003      Fault Tolerance for the Label  
Distribution Protocol (LDP)

Multiprotocol Label Switching (MPLS) systems will be used in core networks where system downtime must be kept to an absolute minimum. Many MPLS Label Switching Routers (LSRs) may, therefore, exploit Fault Tolerant (FT) hardware or software to provide high availability of the core networks.

The details of how FT is achieved for the various components of an FT LSR, including Label Distribution Protocol (LDP), the switching hardware and TCP, are implementation specific. This document identifies issues in the LDP specification in RFC 3036, "LDP Specification", that make it difficult to implement an FT LSR using the current LDP protocols, and defines enhancements to the LDP specification to ease such FT LSR implementations.



The issues and extensions described here are equally applicable to RFC 3212, "Constraint-Based LSP Setup Using LDP" (CR-LDP). [STANDARDS TRACK]

3478      Leelanivas      Feb 2003      Graceful Restart Mechanism for  
Label Distribution Protocol

This document describes a mechanism that helps to minimize the negative effects on MPLS traffic caused by Label Switching Router's (LSR's) control plane restart, specifically by the restart of its Label Distribution Protocol (LDP) component, on LSRs that are capable of preserving the MPLS forwarding component across the restart.

The mechanism described in this document is applicable to all LSRs, both those with the ability to preserve forwarding state during LDP restart and those without (although the latter needs to implement only a subset of the mechanism described in this document). Supporting (a subset of) the mechanism described here by the LSRs that can not preserve their MPLS forwarding state across the restart would not reduce the negative impact on MPLS traffic caused by their control plane restart, but it would minimize the impact if their neighbor(s) are capable of preserving the forwarding state across the restart of their control plane and implement the mechanism described here.

The mechanism makes minimalistic assumptions on what has to be preserved across restart - the mechanism assumes that only the actual MPLS forwarding state has to be preserved; the mechanism does not require any of the LDP-related states to be preserved across the restart.

The procedures described in this document apply to downstream unsolicited label distribution. Extending these procedures to downstream on demand label distribution is for further study.  
[STANDARDS TRACK]

3477      Kompella      Jan 2003      Signalling Unnumbered Links in  
Resource ReSerVation Protocol -  
Traffic Engineering (RSVP-TE)

Current signalling used by Multi-Protocol Label Switching Traffic Engineering (MPLS TE) does not provide support for unnumbered links. This document defines procedures and extensions to Resource ReSerVation Protocol (RSVP) for Label Switched Path (LSP) Tunnels (RSVP-TE), one of the MPLS TE signalling protocols, that are needed in order to support unnumbered links. [STANDARDS TRACK]

3476	Rajagopalan	Mar 2003	Documentation of IANA Assignments for Label Distribution Protocol (LDP), Resource ReSerVation Protocol (RSVP), and Resource ReSerVation Protocol-Traffic Engineering (RSVP-TE) Extensions for Optical UNI Signaling
------	-------------	----------	---

The Optical Interworking Forum (OIF) has defined extensions to the Label Distribution Protocol (LDP) and the Resource ReSerVation Protocol (RSVP) for optical User Network Interface (UNI) signaling. These extensions consist of a set of new data objects and error codes. This document describes these extensions. This memo provides information for the Internet community.

3475	Aboul-Magd	Mar 2003	Documentation of IANA assignments for Constraint-Based LSP setup using LDP (CR-LDP) Extensions for Automatic Switched Optical Network (ASON)
------	------------	----------	--

Automatic Switched Optical Network (ASON) is an architecture, specified by ITU-T Study Group 15, for the introduction of a control plane for optical networks. The ASON architecture specifies a set of reference points that defines the relationship between the ASON architectural entities. Signaling over interfaces defined in those reference points can make use of protocols that are defined by the IETF in the context of Generalized Multi-Protocol Label Switching (GMPLS) work. This document describes Constraint-Based LSP setup using LDP (CR-LDP) extensions for signaling over the interfaces defined in the ASON reference points. The purpose of the document is to request that the IANA assigns code points necessary for the CR-LDP extensions. The protocol specifications for the use of the CR-LDP extensions are found in ITU-T documents. This memo provides information for the Internet community.

3474	Lin	Mar 2003	Documentation of IANA assignments for Generalized MultiProtocol Label Switching (GMPLS) Resource Reservation Protocol - Traffic Engineering (RSVP-TE) Usage and Extensions for Automatically Switched Optical Network (ASON)
------	-----	----------	--

The Generalized MultiProtocol Label Switching (GMPLS) suite of protocol specifications has been defined to provide support for different technologies as well as different applications. These include support for requesting TDM connections based on Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH) as well as Optical Transport Networks (OTNs).

This document concentrates on the signaling aspects of the GMPLS suite of protocols, specifically GMPLS signaling using Resource Reservation Protocol - Traffic Engineering (RSVP-TE). It proposes additional extensions to these signaling protocols to support the capabilities of an ASON network.

This document proposes appropriate extensions towards the resolution of additional requirements identified and communicated by the ITU-T Study Group 15 in support of ITU's ASON standardization effort. This memo provides information for the Internet community.

3473	Berger	Jan 2003	Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions
------	--------	----------	---

This document describes extensions to Multi-Protocol Label Switching (MPLS) Resource ReserVation Protocol - Traffic Engineering (RSVP-TE) signaling required to support Generalized MPLS. Generalized MPLS extends the MPLS control plane to encompass time-division (e.g., Synchronous Optical Network and Synchronous Digital Hierarchy, SONET/SDH), wavelength (optical lambdas) and spatial switching (e.g., incoming port or fiber to outgoing port or fiber). This document presents a RSVP-TE specific description of the extensions. A generic functional description can be found in separate documents. [STANDARDS TRACK]

3472      Ashwood-Smith      Jan 2003      Generalized Multi-Protocol  
Label Switching (GMPLS)  
Signaling Constraint-based  
Routed Label Distribution  
Protocol (CR-LDP) Extensions

This document describes extensions to Multi-Protocol Label Switching (MPLS) Constraint-based Routed Label Distribution Protocol (CR-LDP) signaling required to support Generalized MPLS. Generalized MPLS extends the MPLS control plane to encompass time-division (e.g., Synchronous Optical Network and Synchronous Digital Hierarchy, SONET/SDH), wavelength (optical lambdas) and spatial switching (e.g., incoming port or fiber to outgoing port or fiber). This document presents a CR-LDP specific description of the extensions. A generic functional description can be found in separate documents. [STANDARDS TRACK]

3471      Berger                  Jan 2003      Generalized Multi-Protocol  
Label Switching (GMPLS)  
Signaling Functional  
Description

This document describes extensions to Multi-Protocol Label Switching (MPLS) signaling required to support Generalized MPLS. Generalized MPLS extends the MPLS control plane to encompass time-division (e.g., Synchronous Optical Network and Synchronous Digital Hierarchy, SONET/SDH), wavelength (optical lambdas) and spatial switching (e.g., incoming port or fiber to outgoing port or fiber). This document presents a functional description of the extensions. Protocol specific formats and mechanisms, and technology specific details are specified in separate documents. [STANDARDS TRACK]

3470      Hollenbeck              Jan 2003      Guidelines for the Use  
of Extensible Markup  
Language (XML)  
within IETF Protocols

The Extensible Markup Language (XML) is a framework for structuring data. While it evolved from Standard Generalized Markup Language (SGML) -- a markup language primarily focused on structuring documents -- XML has evolved to be a widely-used mechanism for representing structured data.

There are a wide variety of Internet protocols being developed; many have need for a representation for structured data relevant to their application. There has been much interest in the use of XML as a representation method. This document describes basic XML concepts, analyzes various alternatives in the use of XML, and provides guidelines for the use of XML within IETF standards-track protocols. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3469      Sharma, Ed.      Feb 2003      Framework for Multi-Protocol  
Label Switching (MPLS)-based  
Recovery

Multi-protocol label switching (MPLS) integrates the label swapping forwarding paradigm with network layer routing. To deliver reliable service, MPLS requires a set of procedures to provide protection of the traffic carried on different paths. This requires that the label switching routers (LSRs) support fault detection, fault notification, and fault recovery mechanisms, and that MPLS signaling support the configuration of recovery. With these objectives in mind, this document specifies a framework for MPLS based recovery. Restart issues are not included in this framework. This memo provides information for the Internet community.

3468      Andersson      Feb 2003      The Multiprotocol Label  
Switching (MPLS) Working Group  
decision on MPLS signaling  
protocols

This document documents the consensus reached by the Multiprotocol Label Switching (MPLS) Working Group within the IETF to focus its efforts on "Resource Reservation Protocol (RSVP)-TE: Extensions to RSVP for Label-Switched Paths (LSP) Tunnels" (RFC 3209) as the MPLS signalling protocol for traffic engineering applications and to undertake no new efforts relating to "Constraint-Based LSP Setup using Label Distribution Protocol (LDP)" (RFC 3212). The recommendations of section 6 have been accepted by the IESG. This memo provides information for the Internet community.

3467	Klensin	Feb 2003	Role of the Domain Name System (DNS)
------	---------	----------	---

This document reviews the original function and purpose of the domain name system (DNS). It contrasts that history with some of the purposes for which the DNS has recently been applied and some of the newer demands being placed upon it or suggested for it. A framework for an alternative to placing these additional stresses on the DNS is then outlined. This document and that framework are not a proposed solution, only a strong suggestion that the time has come to begin thinking more broadly about the problems we are encountering and possible approaches to solving them. This memo provides information for the Internet community.

3466	Day	Feb 2003	A Model for Content Internetworking (CDI)
------	-----	----------	--

Content (distribution) internetworking (CDI) is the technology for interconnecting content networks, sometimes previously called "content peering" or "CDN peering". A common vocabulary helps the process of discussing such interconnection and interoperation. This document introduces content networks and content internetworking, and defines elements for such a common vocabulary. This memo provides information for the Internet community.

3465	Allman	Feb 2003	TCP Congestion Control with Appropriate Byte Counting (ABC)
------	--------	----------	---

This document proposes a small modification to the way TCP increases its congestion window. Rather than the traditional method of increasing the congestion window by a constant amount for each arriving acknowledgment, the document suggests basing the increase on the number of previously unacknowledged bytes each ACK covers. This change improves the performance of TCP, as well as closes a security hole TCP receivers can use to induce the sender into increasing the sending rate too rapidly. This memo defines an Experimental Protocol for the Internet community.

3464	Moore	Jan 2003	An Extensible Message Format for Delivery Status Notifications
------	-------	----------	--

This memo defines a Multipurpose Internet Mail Extensions (MIME) content-type that may be used by a message transfer agent (MTA) or electronic mail gateway to report the result of an attempt to deliver a message to one or more recipients. This content-type is intended as a machine-processable replacement for the various types of delivery status notifications currently used in Internet electronic mail.

Because many messages are sent between the Internet and other messaging systems (such as X.400 or the so-called "Local Area Network (LAN)-based" systems), the Delivery Status Notification (DSN) protocol is designed to be useful in a multi-protocol messaging environment. To this end, the protocol described in this memo provides for the carriage of "foreign" addresses and error codes, in addition to those normally used in Internet mail. Additional attributes may also be defined to support "tunneling" of foreign notifications through Internet mail. [STANDARDS TRACK]

3463	Vaudreuil	Jan 2003	Enhanced Mail System Status Codes
------	-----------	----------	-----------------------------------

This document defines a set of extended status codes for use within the mail system for delivery status reports, tracking, and improved diagnostics. In combination with other information provided in the Delivery Status Notification (DSN) delivery report, these codes facilitate media and language independent rendering of message delivery status. [STANDARDS TRACK]

3462	Vaudreuil	Jan 2003	The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages
------	-----------	----------	---

The Multipart/Report Multipurpose Internet Mail Extensions (MIME) content-type is a general "family" or "container" type for electronic mail reports of any kind. Although this memo defines only the use of the Multipart/Report content-type with respect to delivery status reports, mail processing programs will benefit if a single content-type is used to for all kinds of reports.

This document is part of a four document set describing the delivery status report service. This collection includes the Simple Mail Transfer Protocol (SMTP) extensions to request delivery status reports, a MIME content for the reporting of delivery reports, an enumeration of extended status codes, and a multipart container for the delivery report, the original message, and a human-friendly summary of the failure. [STANDARDS TRACK]

3461	Moore	Jan 2003	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)
------	-------	----------	--

This memo defines an extension to the Simple Mail Transfer Protocol (SMTP) service, which allows an SMTP client to specify (a) that Delivery Status Notifications (DSNs) should be generated under certain conditions, (b) whether such notifications should return the contents of the message, and (c) additional information, to be returned with a DSN, that allows the sender to identify both the recipient(s) for which the DSN was issued, and the transaction in which the original message was sent. [STANDARDS TRACK]

3460	Moore	Jan 2003	Policy Core Information Model (PCIM) Extensions
------	-------	----------	--

This document specifies a number of changes to the Policy Core Information Model (PCIM, RFC 3060). Two types of changes are included. First, several completely new elements are introduced, for example, classes for header filtering, that extend PCIM into areas that it did not previously cover. Second, there are cases where elements of PCIM (for example, policy rule priorities) are deprecated, and replacement elements are defined (in this case, priorities tied to associations that refer to policy rules). Both types of changes are done in such a way that, to the extent possible, interoperability with implementations of the original PCIM model is preserved. This document updates RFC 3060. [STANDARDS TRACK]

3459	Burger	Jan 2003	Critical Content Multi-purpose Internet Mail Extensions (MIME) Parameter
------	--------	----------	--

This document describes the use of a mechanism for identifying body parts that a sender deems critical in a multi-part Internet mail message. The mechanism described is a parameter to Content-Disposition, as described by RFC 3204.



By knowing what parts of a message the sender deems critical, a content gateway can intelligently handle multi-part messages when providing gateway services to systems of lesser capability. Critical content can help a content gateway to decide what parts to forward. It can indicate how hard a gateway should try to deliver a body part. It can help the gateway to pick body parts that are safe to silently delete when a system of lesser capability receives a message. In addition, critical content can help the gateway choose the notification strategy for the receiving system. Likewise, if the sender expects the destination to do some processing on a body part, critical content allows the sender to mark body parts that the receiver must process. [STANDARDS TRACK]

3458      Burger                      Jan 2003                      Message Context for Internet Mail

This memo describes a new RFC 2822 message header, "Message-Context". This header provides information about the context and presentation characteristics of a message.

A receiving user agent (UA) may use this information as a hint to optimally present the message. [STANDARDS TRACK]

3457      Kelly                          Jan 2003                      Requirements for IPsec Remote Access Scenarios

IPsec offers much promise as a secure remote access mechanism. However, there are a number of differing remote access scenarios, each having some shared and some unique requirements. A thorough understanding of these requirements is necessary in order to effectively evaluate the suitability of a specific set of mechanisms for any particular remote access scenario. This document enumerates the requirements for a number of common remote access scenarios. This memo provides information for the Internet community.

3456      Patel                      Jan 2003                      Dynamic Host Configuration  
Protocol (DHCPv4)  
Configuration of IPsec Tunnel  
Mode

This memo explores the requirements for host configuration in IPsec tunnel mode, and describes how the Dynamic Host Configuration Protocol (DHCPv4) may be leveraged for configuration. In many remote access scenarios, a mechanism for making the remote host appear to be present on the local corporate network is quite useful. This may be accomplished by assigning the host a "virtual" address from the corporate network, and then tunneling traffic via IPsec from the host's ISP-assigned address to the corporate security gateway. In IPv4, DHCP provides for such remote host configuration. [STANDARDS TRACK]

3455      Garcia-Martin      Jan 2003                      Private Header (P-Header)  
Extensions to the Session  
Initiation Protocol (SIP) for  
the 3rd-Generation Partnership  
Project (3GPP)

This document describes a set of private Session Initiation Protocol (SIP) headers (P-headers) used by the 3rd-Generation Partnership Project (3GPP), along with their applicability, which is limited to particular environments. The P-headers are for a variety of purposes within the networks that the partners use, including charging and information about the networks a call traverses. This memo provides information for the Internet community.

3454      Hoffman                      Dec 2002                      Preparation of  
Internationalized Strings  
("stringprep")

This document describes a framework for preparing Unicode text strings in order to increase the likelihood that string input and string comparison work in ways that make sense for typical users throughout the world. The stringprep protocol is useful for protocol identifier values, company and personal names, internationalized domain names, and other text strings.

This document does not specify how protocols should prepare text strings. Protocols must create profiles of stringprep in order to fully specify the processing options. [STANDARDS TRACK]

3453	Luby	Dec 2002	The Use of Forward Error Correction (FEC) in Reliable Multicast
------	------	----------	---

This memo describes the use of Forward Error Correction (FEC) codes to efficiently provide and/or augment reliability for one-to-many reliable data transport using IP multicast. One of the key properties of FEC codes in this context is the ability to use the same packets containing FEC data to simultaneously repair different packet loss patterns at multiple receivers. Different classes of FEC codes and some of their basic properties are described and terminology relevant to implementing FEC in a reliable multicast protocol is introduced. Examples are provided of possible abstract formats for packets carrying FEC. This memo provides information for the Internet community.

3452	Luby	Dec 2002	Forward Error Correction (FEC) Building Block
------	------	----------	---

This document generally describes how to use Forward Error Correction (FEC) codes to efficiently provide and/or augment reliability for data transport. The primary focus of this document is the application of FEC codes to one-to-many reliable data transport using IP multicast. This document describes what information is needed to identify a specific FEC code, what information needs to be communicated out-of-band to use the FEC code, and what information is needed in data packets to identify the encoding symbols they carry. The procedures for specifying FEC codes and registering them with the Internet Assigned Numbers Authority (IANA) are also described. This document should be read in conjunction with and uses the terminology of the companion document titled, "The Use of Forward Error Correction (FEC) in Reliable Multicast". This memo defines an Experimental Protocol for the Internet community.

3451	Luby	Dec 2002	Layered Coding Transport (LCT) Building Block
------	------	----------	---

Layered Coding Transport (LCT) provides transport level support for reliable content delivery and stream delivery protocols. LCT is specifically designed to support protocols using IP multicast, but also provides support to protocols that use unicast. LCT is compatible with congestion control that provides multiple rate delivery to receivers and is also compatible with coding techniques that provide reliable delivery of content. This memo defines an Experimental Protocol for the Internet community.

3450	Luby	Dec 2002	Asynchronous Layered Coding (ALC) Protocol Instantiation
------	------	----------	---

This document describes the Asynchronous Layered Coding (ALC) protocol, a massively scalable reliable content delivery protocol. Asynchronous Layered Coding combines the Layered Coding Transport (LCT) building block, a multiple rate congestion control building block and the Forward Error Correction (FEC) building block to provide congestion controlled reliable asynchronous delivery of content to an unlimited number of concurrent receivers from a single sender. This memo defines an Experimental Protocol for the Internet community.

3449	Balakrishnan	Dec 2002	TCP Performance Implications of Network Path Asymmetry
------	--------------	----------	---

This document describes TCP performance problems that arise because of asymmetric effects. These problems arise in several access networks, including bandwidth-asymmetric networks and packet radio subnetworks, for different underlying reasons. However, the end result on TCP performance is the same in both cases: performance often degrades significantly because of imperfection and variability in the ACK feedback from the receiver to the sender.

The document details several mitigations to these effects, which have either been proposed or evaluated in the literature, or are currently deployed in networks. These solutions use a combination of local link-layer techniques, subnetwork, and end-to-end mechanisms, consisting of: (i) techniques to manage the channel used for the upstream bottleneck link carrying the ACKs, typically using header compression or reducing the frequency of TCP ACKs, (ii) techniques to handle this reduced ACK frequency to retain the TCP sender's acknowledgment-triggered self-clocking and (iii) techniques to schedule the data and ACK packets in the reverse direction to improve performance in the presence of two-way traffic. Each technique is described, together with known issues, and recommendations for use. A summary of the recommendations is provided at the end of the document. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3448	Handley	Jan 2003	TCP Friendly Rate Control (TFRC): Protocol Specification
------	---------	----------	---

This document specifies TCP-Friendly Rate Control (TFRC). TFRC is a congestion control mechanism for unicast flows operating in a best-effort Internet environment. It is reasonably fair when competing for bandwidth with TCP flows, but has a much lower variation of throughput over time compared with TCP, making it more suitable for applications such as telephony or streaming media where a relatively smooth sending rate is of importance. [STANDARDS TRACK]

3447	Jonsson	Feb 2003	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
------	---------	----------	---

This memo represents a republication of PKCS #1 v2.1 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process. The body of this document is taken directly from the PKCS #1 v2.1 document, with certain corrections made during the publication process. This memo provides information for the Internet community.

3446	Kim	Jan 2003	Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
------	-----	----------	--

This document describes a mechanism to allow for an arbitrary number of Rendezvous Points (RPs) per group in a single shared-tree Protocol Independent Multicast-Sparse Mode (PIM-SM) domain. This memo provides information for the Internet community.

3445      Massey                      Dec 2002                      Limiting the Scope of the KEY  
Resource Record (RR)

This document limits the Domain Name System (DNS) KEY Resource Record (RR) to only keys used by the Domain Name System Security Extensions (DNSSEC). The original KEY RR used sub-typing to store both DNSSEC keys and arbitrary application keys. Storing both DNSSEC and application keys with the same record type is a mistake. This document removes application keys from the KEY record by redefining the Protocol Octet field in the KEY RR Data. As a result of removing application keys, all but one of the flags in the KEY record become unnecessary and are redefined. Three existing application key sub-types are changed to reserved, but the format of the KEY record is not changed. This document updates RFC 2535. [STANDARDS TRACK]

3444      Pras                          Jan 2003                      On the Difference between  
Information Models and Data  
Models

There has been ongoing confusion about the differences between Information Models and Data Models for defining managed objects in network management. This document explains the differences between these terms by analyzing how existing network management model specifications (from the IETF and other bodies such as the International Telecommunication Union (ITU) or the Distributed Management Task Force (DMTF)) fit into the universe of Information Models and Data Models.

This memo documents the main results of the 8th workshop of the Network Management Research Group (NMRG) of the Internet Research Task Force (IRTF) hosted by the University of Texas at Austin. This memo provides information for the Internet community.

3443      Agarwal                      Jan 2003                      Time To Live (TTL) Processing  
in Multi-Protocol Label  
Switching (MPLS) Networks

This document describes Time To Live (TTL) processing in hierarchical Multi-Protocol Label Switching (MPLS) networks and is motivated by the need to formalize a TTL-transparent mode of operation for an MPLS label-switched path. It updates RFC 3032, "MPLS Label Stack Encoding". TTL processing in both Pipe and Uniform Model hierarchical tunnels are specified with examples for both "push" and "pop" cases. The document also complements RFC 3270, "MPLS Support of Differentiated Services" and ties together the terminology introduced in that document with TTL processing in hierarchical MPLS networks. [STANDARDS TRACK]

3442	Lemon	Dec 2002	The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4
------	-------	----------	---

This document defines a new Dynamic Host Configuration Protocol (DHCP) option which is passed from the DHCP Server to the DHCP Client to configure a list of static routes in the client. The network destinations in these routes are classless - each routing table entry includes a subnet mask. [STANDARDS TRACK]

3441	Kumar	Jan 03	Asynchronous Transfer Mode (ATM) Package for the Media Gateway Control Protocol (MGCP)
------	-------	--------	---

This document describes an Asynchronous Transfer Mode (ATM) package for the Media Gateway Control Protocol (MGCP). This package includes new Local Connection Options, ATM-specific events and signals, and ATM connection parameters. Also included is a description of codec and profile negotiation. It extends the MGCP that is currently being deployed in a number of products. Implementers should be aware of developments in the IETF Megaco Working Group and ITU SG16, which are currently working on a potential successor to this protocol. This memo provides information for the Internet community.

3440	Ly	Dec 2002	Definitions of Extension Managed Objects for Asymmetric Digital Subscriber Lines
------	----	----------	--

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 additional managed objects used for managing Asymmetric Digital Subscriber Line (ADSL) interfaces not covered by the ADSL Line MIB (RFC 2662). [STANDARDS TRACK]

3439      Bush                      Dec 2002              Some Internet Architectural  
Guidelines and Philosophy

This document extends RFC 1958 by outlining some of the philosophical guidelines to which architects and designers of Internet backbone networks should adhere. We describe the Simplicity Principle, which states that complexity is the primary mechanism that impedes efficient scaling, and discuss its implications on the architecture, design and engineering issues found in large scale Internet backbones. This memo provides information for the Internet community.

3438      Townsley                  Dec 2002              Layer Two Tunneling Protocol  
(L2TP) Internet Assigned  
Numbers Authority (IANA)  
Considerations Update

This document describes updates to the Internet Assigned Numbers Authority (IANA) considerations for the Layer Two Tunneling Protocol (L2TP). This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3437      Palter                      Dec 2002              Layer-Two Tunneling Protocol  
Extensions for PPP Link  
Control Protocol Negotiation

This document defines extensions to the Layer Two Tunneling Protocol (L2TP) for enhanced support of link-specific Point to Point Protocol (PPP) options. PPP endpoints typically have direct access to the common physical media connecting them and thus have detailed knowledge about the media that is in use. When the L2TP is used, the two PPP peers are no longer directly connected over the same physical media. Instead, L2TP inserts a virtual connection over some or all of the PPP connection by tunneling PPP frames over a packet switched network such as IP. Under some conditions, an L2TP endpoint may need to negotiate PPP Link Control Protocol (LCP) options at a location which may not have access to all of the media information necessary for proper participation in the LCP negotiation. This document provides a mechanism for communicating desired LCP options between L2TP endpoints in advance of PPP LCP negotiation at the far end of an L2TP tunnel, as well as a mechanism for communicating the negotiated LCP options back to where the native PPP link resides. [STANDARDS TRACK]



3436	Jungmaier	Dec 2002	Transport Layer Security over Stream Control Transmission Protocol
------	-----------	----------	--

This document describes the usage of the Transport Layer Security (TLS) protocol, as defined in RFC 2246, over the Stream Control Transmission Protocol (SCTP), as defined in RFC 2960 and RFC 3309.

The user of TLS can take advantage of the features provided by SCTP, namely the support of multiple streams to avoid head of line blocking and the support of multi-homing to provide network level fault tolerance.

Additionally, discussions of extensions of SCTP are also supported, meaning especially the support of dynamic reconfiguration of IP-addresses. [STANDARDS TRACK]

3435	Andreasen	Jan 03	Media Gateway Control Protocol (MGCP) Version 1.0
------	-----------	--------	---

This document describes an application programming interface and a corresponding protocol (MGCP) which is used between elements of a decomposed multimedia gateway. The decomposed multimedia gateway consists of a Call Agent, which contains the call control "intelligence", and a media gateway which contains the media functions, e.g., conversion from TDM voice to Voice over IP.

Media gateways contain endpoints on which the Call Agent can create, modify and delete connections in order to establish and control media sessions with other multimedia endpoints. Also, the Call Agent can instruct the endpoints to detect certain events and generate signals. The endpoints automatically communicate changes in service state to the Call Agent. Furthermore, the Call Agent can audit endpoints as well as the connections on endpoints.

The basic and general MGCP protocol is defined in this document, however most media gateways will need to implement one or more MGCP packages, which define extensions to the protocol suitable for use with specific types of media gateways. Such packages are defined in separate documents. This memo provides information for the Internet community.

3434      Bierman              Dec 2002              Remote Monitoring MIB  
Extensions for High Capacity  
Alarms

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 managed objects for extending the alarm thresholding capabilities found in the Remote Monitoring (RMON) MIB (RFC 2819), to provide similar threshold monitoring of objects based on the Counter64 data type. [STANDARDS TRACK]

3433      Bierman              Dec 2002              Entity Sensor Management  
Information Base

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 managed objects for extending the Entity MIB (RFC 2737) to provide generalized access to information related to physical sensors, which are often found in networking equipment (such as chassis temperature, fan RPM, power supply voltage). [STANDARDS TRACK]

3432      Raisanen              Nov 2002              Network performance  
measurement with periodic  
streams

This memo describes a periodic sampling method and relevant metrics for assessing the performance of IP networks. First, the memo motivates periodic sampling and addresses the question of its value as an alternative to the Poisson sampling described in RFC 2330. The benefits include applicability to active and passive measurements, simulation of constant bit rate (CBR) traffic (typical of multimedia communication, or nearly CBR, as found with voice activity detection), and several instances in which analysis can be simplified. The sampling method avoids predictability by mandating random start times and finite length tests. Following descriptions of the sampling method and sample metric parameters, measurement methods and errors are discussed. Finally, we give additional information on periodic measurements, including security considerations. [STANDARDS TRACK]

3431 Segmuller Dec 2002 Sieve Extension: Relational Tests

This document describes the RELATIONAL extension to the Sieve mail filtering language defined in RFC 3028. This extension extends existing conditional tests in Sieve to allow relational operators. In addition to testing their content, it also allows for testing of the number of entities in header and envelope fields. [STANDARDS TRACK]

3430 Schoenwaelder Dec 2002 Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping

This memo defines a transport mapping for using the Simple Network Management Protocol (SNMP) over TCP. The transport mapping can be used with any version of SNMP. This document extends the transport mappings defined in STD 62, RFC 3417. This memo defines an Experimental Protocol for the Internet community.

3429 Ohta Nov 2002 Assignment of the 'OAM Alert Label' for Multiprotocol Label Switching Architecture (MPLS) Operation and Maintenance (OAM) Functions

This document describes the assignment of one of the reserved label values defined in RFC 3032 (MPLS label stack encoding) to the 'Operation and Maintenance (OAM) Alert Label' that is used by user-plane Multiprotocol Label Switching Architecture (MPLS) OAM functions for identification of MPLS OAM packets. This memo provides information for the Internet community.

3428 Campbell Dec 2002 Session Initiation Protocol (SIP) Extension for Instant Messaging

Instant Messaging (IM) refers to the transfer of messages between users in near real-time. These messages are usually, but not required to be, short. IMs are often used in a conversational mode, that is, the transfer of messages back and forth is fast enough for participants to maintain an interactive conversation.

This document proposes the MESSAGE method, an extension to the Session Initiation Protocol (SIP) that allows the transfer of Instant Messages. Since the MESSAGE request is an extension to SIP, it inherits all the request routing and security features of that protocol. MESSAGE requests carry the content in the form of MIME body parts. MESSAGE requests do not themselves initiate a SIP dialog; under normal usage each Instant Message stands alone, much like pager messages. MESSAGE requests may be sent in the context of a dialog initiated by some other SIP request. [STANDARDS TRACK]

3427      Mankin                      Dec 2002                      Change Process for the Session  
Initiation Protocol (SIP)

This memo documents a process intended to apply architectural discipline to the future development of the Session Initiation Protocol (SIP). There have been concerns with regards to new SIP proposals. Specifically, that the addition of new SIP features can be damaging towards security and/or greatly increase the complexity of the protocol. The Transport Area directors, along with the SIP and Session Initiation Proposal Investigation (SIPPING) working group chairs, have provided suggestions for SIP modifications and extensions. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3426      Floyd                      Nov 2002                      General Architectural and  
Policy Considerations

This document suggests general architectural and policy questions that the IETF community has to address when working on new standards and protocols. We note that this document contains questions to be addressed, as opposed to guidelines or architectural principles to be followed. This memo provides information for the Internet community.

3425      Lawrence                      Nov 2002                      Obsoleting IQUERY

The IQUERY method of performing inverse DNS lookups, specified in RFC 1035, has not been generally implemented and has usually been operationally disabled where it has been implemented. Both reflect a general view in the community that the concept was unwise and that the widely-used alternate approach of using pointer (PTR) queries and reverse-mapping records is preferable. Consequently, this document deprecates the IQUERY operation, declaring it entirely obsolete. This document updates RFC 1035. [STANDARDS TRACK]

3424	Daigle	Nov 2002	IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation
------	--------	----------	---

As a result of the nature of Network Address Translation (NAT) Middleboxes, communicating endpoints that are separated by one or more NATs do not know how to refer to themselves using addresses that are valid in the addressing realms of their (current and future) peers. Various proposals have been made for "UNilateral Self-Address Fixing (UNSAF)" processes. These are processes whereby some originating endpoint attempts to determine or fix the address (and port) by which it is known to another endpoint - e.g., to be able to use address data in the protocol exchange, or to advertise a public address from which it will receive connections.

This document outlines the reasons for which these proposals can be considered at best as short term fixes to specific problems and the specific issues to be carefully evaluated before creating an UNSAF proposal. This memo provides information for the Internet community.

3423	Zhang	Nov 2002	XACCT's Common Reliable Accounting for Network Element (CRANE) Protocol Specification Version 1.0
------	-------	----------	--

This document defines the Common Reliable Accounting for Network Element (CRANE) protocol that enables efficient and reliable delivery of any data, mainly accounting data from Network Elements to any systems, such as mediation systems and Business Support Systems (BSS)/ Operations Support Systems (OSS). The protocol is developed to address the critical needs for exporting high volume of accounting data from NE's with efficient use of network, storage, and processing resources.

This document specifies the architecture of the protocol and the message format, which MUST be supported by all CRANE protocol implementations. This memo provides information for the Internet community.

3422      Okamoto                      Nov 2002                      Forwarding Media Access  
Control (MAC) Frames over  
Multiple Access Protocol over  
Synchronous Optical  
Network/Synchronous Digital  
Hierarchy (MAPOS)

This memo describes a method for forwarding media access control (MAC) frames over Multiple Access Protocol over Synchronous Optical Network/Synchronous Digital Hierarchy (MAPOS), thus providing a way to unify MAPOS network environment and MAC-based Local Area Network (LAN) environment. This memo provides information for the Internet community.

3421      Zhao                              Nov 2002                      Select and Sort Extensions for  
the Service Location Protocol  
(SLP)

This document defines two extensions (Select and Sort) for the Service Location Protocol (SLP). These extensions allow a User Agent (UA) to request that the Uniform Resource Locator (URL) entries in a Service Reply (SrvRply) be limited to the specified number, or be sorted according to the specified sort key list. Using these two extensions together can facilitate discovering the best match, such as finding a service that has the maximum speed or the minimum load. This memo defines an Experimental Protocol for the Internet community.

3420      Sparks                              Nov 2002                      Internet Media Type  
message/sipfrag

This document registers the message/sipfrag Multipurpose Internet Mail Extensions (MIME) media type. This type is similar to message/sip, but allows certain subsets of well formed Session Initiation Protocol (SIP) messages to be represented instead of requiring a complete SIP message. In addition to end-to-end security uses, message/sipfrag is used with the REFER method to convey information about the status of a referenced request. [STANDARDS TRACK]

3419      Daniele              Dec 2002              Textual Conventions for  
   Transport Addresses

This document introduces a Management Information Base (MIB) module that defines textual conventions to represent commonly used transport-layer addressing information. The definitions are compatible with the concept of TAddress/TDomain pairs introduced by the Structure of Management Information version 2 (SMIv2) and support the Internet transport protocols over IPv4 and IPv6. [STANDARDS TRACK]

3418      Presuhn              Dec 2002              Management Information Base  
   (MIB) for the Simple Network  
   Management Protocol (SNMP)

This document defines managed objects which describe the behavior of a Simple Network Management Protocol (SNMP) entity. This document obsoletes RFC 1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2). [STANDARDS TRACK]

3417      Presuhn              Dec 2002              Transport Mappings for  
   the Simple Network Management  
   Protocol (SNMP)

This document defines the transport of Simple Network Management Protocol (SNMP) messages over various protocols. This document obsoletes RFC 1906. [STANDARDS TRACK]

3416      Presuhn              Dec 2002              Version 2 of the Protocol  
   Operations for the Simple  
   Network Management Protocol  
   (SNMP)

This document defines version 2 of the protocol operations for the Simple Network Management Protocol (SNMP). It defines the syntax and elements of procedure for sending, receiving, and processing SNMP PDUs. This document obsoletes RFC 1905. [STANDARDS TRACK]

3415	Wijnen	Dec 2002	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
------	--------	----------	--

This document describes the View-based Access Control Model (VACM) for use in the Simple Network Management Protocol (SNMP) architecture. It defines the Elements of Procedure for controlling access to management information. This document also includes a Management Information Base (MIB) for remotely managing the configuration parameters for the View-based Access Control Model. This document obsoletes RFC 2575. [STANDARDS TRACK]

3414	Blumenthal	Dec 2002	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
------	------------	----------	--

This document describes the User-based Security Model (USM) for Simple Network Management Protocol (SNMP) version 3 for use in the SNMP architecture. It defines the Elements of Procedure for providing SNMP message level security. This document also includes a Management Information Base (MIB) for remotely monitoring/managing the configuration parameters for this Security Model. This document obsoletes RFC 2574. [STANDARDS TRACK]

3413	Levi	Dec 2002	Simple Network Management Protocol (SNMP) Applications
------	------	----------	--

This document describes five types of Simple Network Management Protocol (SNMP) applications which make use of an SNMP engine as described in STD 62, RFC 3411. The types of application described are Command Generators, Command Responders, Notification Originators, Notification Receivers, and Proxy Forwarders.

This document also defines Management Information Base (MIB) modules for specifying targets of management operations, for notification filtering, and for proxy forwarding. This document obsoletes RFC 2573. [STANDARDS TRACK]



3412	Case	Dec 2002	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
------	------	----------	---

This document describes the Message Processing and Dispatching for Simple Network Management Protocol (SNMP) messages within the SNMP architecture. It defines the procedures for dispatching potentially multiple versions of SNMP messages to the proper SNMP Message Processing Models, and for dispatching PDUs to SNMP applications. This document also describes one Message Processing Model - the SNMPv3 Message Processing Model. This document obsoletes RFC 2572. [STANDARDS TRACK]

3411	Harrington	Dec 2002	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
------	------------	----------	---

This document describes an architecture for describing Simple Network Management Protocol (SNMP) Management Frameworks. The architecture is designed to be modular to allow the evolution of the SNMP protocol standards over time. The major portions of the architecture are an SNMP engine containing a Message Processing Subsystem, a Security Subsystem and an Access Control Subsystem, and possibly multiple SNMP applications which provide specific functional processing of management data. This document obsoletes RFC 2571. [STANDARDS TRACK]

3410	Case	Dec 2002	Introduction and Applicability Statements for Internet Standard Management Framework
------	------	----------	--

The purpose of this document is to provide an overview of the third version of the Internet-Standard Management Framework, termed the SNMP version 3 Framework (SNMPv3). This Framework is derived from and builds upon both the original Internet-Standard Management Framework (SNMPv1) and the second Internet-Standard Management Framework (SNMPv2).

The architecture is designed to be modular to allow the evolution of the Framework over time.

The document explains why using SNMPv3 instead of SNMPv1 or SNMPv2 is strongly recommended. The document also recommends that RFCs 1157, 1441, 1901, 1909 and 1910 be retired by moving them to Historic status. This document obsoletes RFC 2570. This memo provides information for the Internet community.

3409	Svanbro	Dec 2002	Lower Layer Guidelines for Robust RTP/UDP/IP Header Compression
------	---------	----------	---

This document describes lower layer guidelines for robust header compression (ROHC) and the requirements ROHC puts on lower layers. The purpose of this document is to support the incorporation of robust header compression algorithms, as specified in the ROHC working group, into different systems such as those specified by Third Generation Partnership Project (3GPP), 3GPP Project 2 (3GPP2), European Technical Standards Institute (ETSI), etc. This document covers only lower layer guidelines for compression of RTP/UDP/IP and UDP/IP headers as specified in [RFC3095]. Both general guidelines and guidelines specific for cellular systems are discussed in this document. This memo provides information for the Internet community.

3408	Liu	Dec 2002	Zero-byte Support for Bidirectional Reliable Mode (R-mode) in Extended Link-Layer Assisted ROHC Header Compression (ROHC) Profile
------	-----	----------	---

This document defines an additional mode of the link-layer assisted ROHC profile, also known as the zero-byte profile, beyond the two defined in RFC 3242. Zero-byte header compression exists in order to prevent the single-octet ROHC header from pushing a packet voice stream into the next higher fixed packet size for the radio. It is usable in certain widely deployed older air interfaces. This document adds the zero-byte operation for ROHC Bidirectional Reliable mode (R-mode) to the ones specified for Unidirectional (U-mode) and Bidirectional Optimistic (O-mode) modes of header compression in RFC 3242. [STANDARDS TRACK]

3407	Andreasen	Oct 2002	Session Description Protocol (SDP) Simple Capability Declaration
------	-----------	----------	--

This document defines a set of Session Description Protocol (SDP) attributes that enables SDP to provide a minimal and backwards compatible capability declaration mechanism. Such capability declarations can be used as input to a subsequent session negotiation, which is done by means outside the scope of this document. This provides a simple and limited solution to the general capability negotiation problem being addressed by the next generation of SDP, also known as SDPng. [STANDARDS TRACK]

3406	Daigle	Oct 2002	Uniform Resource Names (URN) Namespace Definition Mechanisms
------	--------	----------	--

This document lays out general definitions of and mechanisms for establishing Uniform Resource Names (URN) "namespaces". The URN WG has defined a syntax for URNs in RFC 2141, as well as some proposed mechanisms for their resolution and use in Internet applications in RFC 3401 and RFC 3405. The whole rests on the concept of individual "namespaces" within the URN structure. Apart from proof-of-concept namespaces, the use of existing identifiers in URNs has been discussed in RFC 2288. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3405	Mealling	Oct 2002	Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures
------	----------	----------	--

This document is fifth in a series that is completely specified in "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS" (RFC 3401). It is very important to note that it is impossible to read and understand any document in this series without reading the others. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3404	Mealling	Oct 2002	Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application
------	----------	----------	--

This document describes a specification for taking Uniform Resource Identifiers (URI) and locating an authoritative server for information about that URI. The method used to locate that authoritative server is the Dynamic Delegation Discovery System.

This document is part of a series that is specified in "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS" (RFC 3401). It is very important to note that it is impossible to read and understand any document in this series without reading the others.  
[STANDARDS TRACK]

3403	Mealling	Oct 2002	Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database
------	----------	----------	--

This document describes a Dynamic Delegation Discovery System (DDDS) Database using the Domain Name System (DNS) as a distributed database of Rules. The Keys are domain-names and the Rules are encoded using the Naming Authority Pointer (NAPTR) Resource Record (RR).

Since this document obsoletes RFC 2915, it is the official specification for the NAPTR DNS Resource Record. It is also part of a series that is completely specified in "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS" (RFC 3401). It is very important to note that it is impossible to read and understand any document in this series without reading the others. [STANDARDS TRACK]

3402	Mealling	Oct 2002	Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm
------	----------	----------	--

This document describes the Dynamic Delegation Discovery System (DDDS) algorithm for applying dynamically retrieved string transformation rules to an application-unique string. Well-formed transformation rules will reflect the delegation of management of information associated with the string. This document is also part of a series that is completely specified in "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS" (RFC 3401). It is very important to note that it is impossible to read and understand any document in this series without reading the others. [STANDARDS TRACK]

3401	Mealling	Oct 2002	Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS
------	----------	----------	---

This document specifies the exact documents that make up the complete Dynamic Delegation Discovery System (DDDS). DDDS is an abstract algorithm for applying dynamically retrieved string transformation rules to an application-unique string. This document along with RFC 3402, RFC 3403 and RFC 3404 obsolete RFC 2168 and RFC 2915, as well as updates RFC 2276. This memo provides information for the Internet community.

3400

Never Issued

RFC 3400 was never issued.

#### Security Considerations

Security issues are not discussed in this memo.

#### Author's Address

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

Phone: (310) 822-1511  
EMail: ginoza@isi.edu

## Full Copyright Statement

Copyright (C) The Internet Society (2003). 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.

