Network Working Group
Request for Comments: 3299
Category: Informational

S. Ginoza
ISI

December 2003

Request for Comments Summary

RFC Numbers 3200-3299

Status of This Memo

This RFC is a slightly annotated list of the 100 RFCs from RFC 3200 through RFC 3299. 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

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
3299	Ginoza	Dec 2003	Request for Comments Summary

This memo.

3298 Faynberg Aug 2002 Service in the Public Switched Telephone Network/Intelligent Network (PSTN/IN) Requesting InTernet Service (SPIRITS) Protocol Requirements

This document describes the SPIRITS protocol requirements, based on the architecture presented in RFC 3136. (SPIRITS stands for "Service in the PSTN/IN Requesting InTernet Service".) The purpose of the protocol is to support services that originate in the Public Switched Telephone Network (PSTN) and necessitate the interactions between the PSTN and the Internet. Similarly, such services are called SPIRITS services. (Internet Call Waiting, Internet Caller-ID Delivery, and Internet Call Forwarding are examples of SPIRIT services, but the protocol is to define the building blocks from which many other services can be built.) On the PSTN side, the SPIRITS services are initiated from the Intelligent Network (IN) entities; the earlier IETF work on the PSTN/Internet Interworking (PINT) resulted in the protocol (RFC 2848) in support of the services initiated the other way around--from the Internet to PSTN.

To this end, this document lists general requirements for the SPIRITS protocol as well as those pertinent to IN, Wireless IN, and PINT building blocks. The document also presents the SPIRITS WG consensus on the choice of the SPIRITS signaling protocol. This memo provides information for the Internet community.

3297 Klyne Jul 2002 Content Negotiation for Messaging Services based on Email

This memo describes a content negotiation mechanism for facsimile, voice and other messaging services that use Internet email. [STANDARDS TRACK]

3296 Zeilenga Jul 2002 Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories

This document details schema and protocol elements for representing and managing named subordinate references in Lightweight Directory Access Protocol (LDAP) Directories. [STANDARDS TRACK]

3295 Sjostrand Jun 2002 Definitions of Managed Objects for the General Switch Management Protocol (GSMP)

This memo defines a portion of the Management Information Base (MIB) for the use with the network management protocols in the Internet community. In particular, it describes managed objects for the General Switch Management Protocol (GSMP). [STANDARDS TRACK]

3294 Doria Jun 2002 General Switch Management Protocol (GSMP) Applicability

This memo provides an overview of the GSMP (General Switch Management Protocol) and includes information relating to its deployment in a IP network in an MPLS environment. It does not discuss deployment in an ATM (Asynchronous Transfer Mode) network or in a raw ethernet configuration. This memo provides information for the Internet community.

3293 Doria Jun 2002 General Switch Management Protocol (GSMP) Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)

This memo specifies the encapsulation of GSMP (General Switch Management Protocol) packets in ATM (Asynchronous Transfer Mode), Ethernet and TCP (Transmission Control Protocol). [STANDARDS TRACK]

3292 Doria Jun 2002 General Switch Management Protocol (GSMP) V3

This document describes the General Switch Management Protocol Version 3 (GSMPv3). The GSMPv3 is an asymmetric protocol that allows one or more external switch controllers to establish and maintain the state of a label switch such as, an ATM, frame relay or MPLS switch. The GSMPv3 allows control of both unicast and multicast switch connection state as well as control of switch system resources and QoS features. [STANDARDS TRACK]

3291 Daniele May 2002 Textual Conventions for Internet Network Addresses

This MIB module defines textual conventions to represent commonly used Internet network layer addressing information. The intent is that these textual conventions (TCs) will be imported and used in MIB modules that would otherwise define their own representations. [STANDARDS TRACK]

3290 Bernet May 2002 An Informal Management Model for Diffserv Routers

This document proposes an informal management model of Differentiated Services (Diffserv) routers for use in their management and configuration. This model defines functional datapath elements (e.g., classifiers, meters, actions, marking, absolute dropping, counting, multiplexing), algorithmic droppers, queues and schedulers. It describes possible configuration parameters for these elements and how they might be interconnected to realize the range of traffic conditioning and per-hop behavior (PHB) functionalities described in the Diffserv Architecture. This memo provides information for the Internet community.

3289 Baker May 2002 Management Information Base for the Differentiated Services Architecture

This memo describes an SMIv2 (Structure of Management Information version 2) MIB for a device implementing the Differentiated Services Architecture. It may be used both for monitoring and configuration of a router or switch capable of Differentiated Services functionality. [STANDARDS TRACK]

3288 O'Tuathail Jun 2002 Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP)

This memo specifies a Simple Object Access Protocol (SOAP) binding to the Blocks Extensible Exchange Protocol core (BEEP). A SOAP binding describes how SOAP messages are transmitted in the network. [STANDARDS TRACK]

3287 Bierman Jul 2002 Remote Monitoring MIB Extensions for Differentiated Services

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 used for monitoring Differentiated Services (DS) Codepoint usage in packets which contain a DS field, utilizing the monitoring framework defined in the RMON-2 (Remote Network Monitoring Management Version 2) MIB. [STANDARDS TRACK]

3286 Ong May 2002 An Introduction to the Stream Control Transmission Protocol (SCTP)

This document provides a high level introduction to the capabilities supported by the Stream Control Transmission Protocol (SCTP). It is intended as a guide for potential users of SCTP as a general purpose transport protocol. This memo provides information for the Internet community.

3285 Gahrns May 2002 Using Microsoft Word to create Internet Drafts and RFCs

This document describes the steps to configure the Microsoft Word application to produce documents in Internet Draft and RFC format. This memo provides information for the Internet community.

3284 Korn Jun 2002 The VCDIFF Generic Differencing and Compression Data Format

This memo describes VCDIFF, a general, efficient and portable data format suitable for encoding compressed and/or differencing data so that they can be easily transported among computers. [STANDARDS TRACK]

3283 Mahoney Jun 2002 Guide to Internet Calendaring

This document describes the various Internet calendaring and scheduling standards and works in progress, and the relationships between them. Its intent is to provide a context for these documents, assist in their understanding, and potentially aid in the design of standards-based calendaring and scheduling systems. The standards addressed are RFC 2445 (iCalendar), RFC 2446 (iTIP), and RFC 2447 (iMIP). The work in progress addressed is "Calendar Access Protocol" (CAP). This document also describes issues and problems that are not solved by these protocols, and that could be targets for future work. This memo provides information for the Internet community.

3282 Alvestrand May 2002 Content Language Headers

This document defines a "Content-language:" header, for use in cases where one desires to indicate the language of something that has RFC 822-like headers, like MIME body parts or Web documents, and an "Accept-Language:" header for use in cases where one wishes to indicate one’s preferences with regard to language. [STANDARDS TRACK]

3281 Farrell Apr 2002 An Internet Attribute Certificate Profile for Authorization

This specification defines a profile for the use of X.509 Attribute Certificates in Internet Protocols. Attribute certificates may be used in a wide range of applications and environments covering a broad spectrum of interoperability goals and a broader spectrum of operational and assurance requirements. The goal of this document is to establish a common baseline for generic applications requiring broad interoperability as well as limited special purpose requirements. The profile places emphasis on attribute certificate support for Internet electronic mail, IPSec, and WWW security applications. [STANDARDS TRACK]

3280 Housley Apr 2002 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

This memo profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet. [STANDARDS TRACK]

3279	Polk	Apr 2002	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

This document specifies algorithm identifiers and ASN.1 encoding formats for digital signatures and subject public keys used in the Internet X.509 Public Key Infrastructure (PKI). Digital signatures are used to sign certificates and certificate revocation list (CRLs). Certificates include the public key of the named subject. [STANDARDS TRACK]

3278	Blake-Wilson	Apr 2002	Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)

This document describes how to use Elliptic Curve Cryptography (ECC) public-key algorithms in the Cryptographic Message Syntax (CMS). The ECC algorithms support the creation of digital signatures and the exchange of keys to encrypt or authenticate content. The definition of the algorithm processing is based on the ANSI X9.62 standard, developed by the ANSI X9F1 working group, the IEEE 1363 standard, and the SEC 1 standard. This memo provides information for the Internet community.

3277	McPherson	Apr 2002	Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance

This document describes a simple, interoperable mechanism that can be employed in Intermediate System to Intermediate System (IS-IS) networks in order to decrease the data loss associated with deterministic blackholing of packets during transient network conditions. The mechanism proposed here requires no IS-IS protocol changes and is completely interoperable with the existing IS-IS specification. This memo provides information for the Internet community.

3276	Ray	May 2002	Definitions of Managed Objects for High Bit-Rate DSL - 2nd generation (HDSL2) and Single-Pair High-Speed Digital Subscriber Line (SHDSL) Lines

This document defines a portion of the Management Information Base (MIB) module for use with network management protocols in the Internet community. In particular, it describes objects used for managing High Bit-Rate DSL - 2nd generation (HDSL2) and Single-Pair High-Speed Digital Subscriber Line (SHDSL) interfaces. [STANDARDS TRACK]

3275	Eastlake 3rd	Mar 2002	(Extensible Markup Language) XML-Signature Syntax and Processing

This document specifies XML (Extensible Markup Language) digital signature processing rules and syntax. [STANDARDS TRACK]

3274	Gutmann	Jun 2002	Compressed Data Content Type for Cryptographic Message Syntax (CMS)

This document defines a format for using compressed data as a Cryptographic Message Syntax (CMS) content type. Compressing data before transmission provides a number of advantages, including the elimination of data redundancy which could help an attacker, speeding up processing by reducing the amount of data to be processed by later steps (such as signing or encryption), and reducing overall message size. Although there have been proposals for adding compression at other levels (for example at the MIME or SSL level), these don’t address the problem of compression of CMS content unless the compression is supplied by an external means (for example by intermixing MIME and CMS). [STANDARDS TRACK]

3273 Waldbusser Jul 2002 Remote Network Monitoring Management Information Base for High Capacity Networks

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 remote network monitoring (RMON) devices for use on high speed networks. This document contains a MIB Module that defines these new objects and also contains definitions of some updated objects from the RMON-MIB in RFC 2819 and the RMON2-MIB in RFC 2021. [PROPOSED STANDARD]

3272 Awduche May 2002 Overview and Principles of Internet Traffic Engineering

This memo describes the principles of Traffic Engineering (TE) in the Internet. The document is intended to promote better understanding of the issues surrounding traffic engineering in IP networks, and to provide a common basis for the development of traffic engineering capabilities for the Internet. The principles, architectures, and methodologies for performance evaluation and performance optimization of operational IP networks are discussed throughout this document. This memo provides information for the Internet community.

3271 Cerf Apr 2002 The Internet is for Everyone

This document expresses the Internet Society’s ideology that the Internet really is for everyone. However, it will only be such if we make it so. This memo provides information for the Internet community.

3270 Le Faucheur May 2002 Multi-Protocol Label Switching (MPLS) Support of Differentiated Services

This document defines a flexible solution for support of Differentiated Services (Diff-Serv) over Multi-Protocol Label Switching (MPLS) networks. [STANDARDS TRACK]

3269 Kermode Apr 2002 Author Guidelines for Reliable Multicast Transport (RMT) Building Blocks and Protocol Instantiation documents

This document provides general guidelines to assist the authors of Reliable Multicast Transport (RMT) building block and protocol instantiation definitions. The purpose of these guidelines is to ensure that any building block and protocol instantiation definitions produced contain sufficient information to fully explain their operation and use. In addition these guidelines provide directions to specify modular and clearly defined RMT building blocks and protocol instantiations that can be refined and augmented to safely create new protocols for use in new scenarios for which any existing protocols were not designed. This memo provides information for the Internet community.

3268 Chown Jun 2002 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)

This document proposes several new ciphersuites. At present, the symmetric ciphers supported by Transport Layer Security (TLS) are RC2, RC4, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), and triple DES. The protocol would be enhanced by the addition of Advanced Encryption Standard (AES) ciphersuites. [STANDARDS TRACK]

3267 Sjoberg Jun 2002 Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs

This document specifies a real-time transport protocol (RTP) payload format to be used for Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) encoded speech signals. The payload format is designed to be able to interoperate with existing AMR and AMR-WB transport formats on non-IP networks. In addition, a file format is specified for transport of AMR and AMR-WB speech data in storage mode applications such as email. Two separate MIME type registrations are included, one for AMR and one for AMR-WB, specifying use of both the RTP payload format and the storage format. [STANDARDS TRACK]

3266 Olson Jun 2002 Support for IPv6 in Session Description Protocol (SDP)

This document describes the use of Internet Protocol Version 6 (IPv6) addresses in conjunction with the Session Description Protocol (SDP). Specifically, this document clarifies existing text in SDP with regards to the syntax of IPv6 addresses. [STANDARDS TRACK]

3265 Roach Jun 2002 Session Initiation Protocol (SIP)-Specific Event Notification

This document describes an extension to the Session Initiation Protocol (SIP). The purpose of this extension is to provide an extensible framework by which SIP nodes can request notification from remote nodes indicating that certain events have occurred. [STANDARDS TRACK]

3264 Rosenberg Jun 2002 An Offer/Answer Model with the Session Description Protocol (SDP)

This document defines a mechanism by which two entities can make use of the Session Description Protocol (SDP) to arrive at a common view of a multimedia session between them. In the model, one participant offers the other a description of the desired session from their perspective, and the other participant answers with the desired session from their perspective. This offer/answer model is most useful in unicast sessions where information from both participants is needed for the complete view of the session. The offer/answer model is used by protocols like the Session Initiation Protocol (SIP). [STANDARDS TRACK]

3263 Rosenberg Jun 2002 Session Initiation Protocol (SIP): Locating SIP Servers

The Session Initiation Protocol (SIP) uses DNS procedures to allow a client to resolve a SIP Uniform Resource Identifier (URI) into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS to allow a server to send a response to a backup client if the primary client has failed. This document describes those DNS procedures in detail. [STANDARDS TRACK]

3262 Rosenberg Jun 2002 Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

This document specifies an extension to the Session Initiation Protocol (SIP) providing reliable provisional response messages. This extension uses the option tag 100rel and defines the Provisional Response ACKnowledgement (PRACK) method. [STANDARDS TRACK]

3261 Rosenberg Jun 2002 SIP: Session Initiation Protocol

This document describes Session Initiation Protocol (SIP), an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. [STANDARDS TRACK]

3260 Grossman Apr 2002 New Terminology and Clarifications for Diffserv

This memo captures Diffserv working group agreements concerning new and improved terminology, and provides minor technical clarifications. It is intended to update RFC 2474, RFC 2475 and RFC 2597. When RFCs 2474 and 2597 advance on the standards track, and RFC 2475 is updated, it is intended that the revisions in this memo will be incorporated, and that this memo will be obsoleted by the new RFCs. This memo provides information for the Internet community.

3259 Ott Apr 2002 A Message Bus for Local Coordination

The local Message Bus (Mbus) is a light-weight message-oriented coordination protocol for group communication between application components. The Mbus provides automatic location of communication peers, subject based addressing, reliable message transfer and different types of communication schemes. The protocol is layered on top of IP multicast and is specified for IPv4 and IPv6. The IP multicast scope is limited to link-local multicast. This document specifies the Mbus protocol, i.e., message syntax, addressing and transport mechanisms. This memo provides information for the Internet community.

3258 Hardie Apr 2002 Distributing Authoritative Name Servers via Shared Unicast Addresses

This memo describes a set of practices intended to enable an authoritative name server operator to provide access to a single named server in multiple locations. The primary motivation for the development and deployment of these practices is to increase the distribution of Domain Name System (DNS) servers to previously under-served areas of the network topology and to reduce the latency for DNS query responses in those areas. This memo provides information for the Internet community.

3257 Coene Apr 2002 Stream Control Transmission Protocol Applicability Statement

This document describes the applicability of the Stream Control Transmission Protocol (SCTP). It also contrasts SCTP with the two dominant transport protocols, User Datagram Protocol (UDP) & Transmission Control Protocol (TCP), and gives some guidelines for when best to use SCTP and when not best to use SCTP. This memo provides information for the Internet community.

3256 Jones Apr 2002 The DOCSIS (Data-Over-Cable Service Interface Specifications) Device Class DHCP (Dynamic Host Configuration Protocol) Relay Agent Information Sub-option

This document proposes a new sub-option to the DHCP (Dynamic Host Configuration Protocol) Relay Agent Information Option. [STANDARDS TRACK]

3255	Jones	Apr 2002	Extending Point-to-Point Protocol (PPP) over Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH) with virtual concatenation, high order and low order payloads

This document describes an extension to the mapping of Point-to-Point Protocol (PPP) into Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH) to include the use of SONET/SDH SPE/VC virtual concatenation and the use of both high order and low order payloads. [STANDARDS TRACK]

3254	Alvestrand	Apr 2002	Definitions for talking about directories

When discussing systems for making information accessible through the Internet in standardized ways, it may be useful if the people who are discussing it have a common understanding of the terms they use. For example, a reference to this document would give one the power to agree that the DNS (Domain Name System) is a global lookup repository with perimeter integrity and loose, converging consistency. On the other hand, a LDAP (Lightweight Directory Access Protocol) directory server is a local, centralized repository with both lookup and search capability. This document discusses one group of such systems which is known under the term, "directories". This memo provides information for the Internet community.

3253	Clemm	Mar 2002	Versioning Extensions to WebDAV (Web Distributed Authoring and Versioning)

This document specifies a set of methods, headers, and resource types that define the WebDAV (Web Distributed Authoring and Versioning) versioning extensions to the HTTP/1.1 protocol. [STANDARDS TRACK]

3252	Kennedy	1 April 2002	Binary Lexical Octet Ad-hoc Transport

This document defines a reformulation of IP and two transport layer protocols (TCP and UDP) as XML applications. This memo provides information for the Internet community.

3251 Rajagopalan 1 April 2002 Electricity over IP

Mostly Pointless Lamp Switching (MPLampS) is an architecture for carrying electricity over IP (with an MPLS control plane). According to our marketing department, MPLampS has the potential to dramatically lower the price, ease the distribution and usage, and improve the manageability of delivering electricity. This document is motivated by such work as SONET/SDH over IP/MPLS (with apologies to the authors). Readers of the previous work have been observed scratching their heads and muttering, "What next?". This document answers that question. This memo provides information for the Internet community.

3250 McIntyre Sep 2002 Tag Image File Format Fax eXtended (TIFF-FX) - image/tiff-fx MIME Sub-type Registration

This document describes the registration of the MIME sub-type image/tiff-fx. The encodings are defined by File Format for Internet Fax and its extensions. [STANDARDS TRACK]

3249 Cancio Sep 2002 Implementers Guide for Facsimile Using Internet Mail

This document is intended for the implementers of software that use email to send to facsimiles using RFC 2305 and 2532. This is an informational document and its guidelines do not supersede the referenced documents. This memo provides information for the Internet community.

3248 Armitage Mar 2002 A Delay Bound alternative revision of RFC 2598

For historical interest, this document captures the EF Design Team's proposed solution, preferred by the original authors of RFC 2598 but not adopted by the working group in December 2000. The original definition of EF was based on comparison of forwarding on an unloaded network. This experimental Delay Bound (DB) PHB requires a bound on the delay of packets due to other traffic in the network. At the Pittsburgh IETF meeting in August 2000, the Differentiated Services working group faced serious questions regarding RFC 2598 - the group's standards track definition of the Expedited Forwarding (EF) Per Hop Behavior (PHB). An 'EF Design Team' volunteered to develop a re-expression of RFC 2598, bearing in mind the issues raised in the DiffServ group. At the San Diego IETF meeting in December 2000 the DiffServ working group decided to pursue an alternative re-expression of the EF PHB. This memo provides information for the Internet community.

3247 Charny Mar 2002 Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)

This document was written during the process of clarification of RFC2598 "An Expedited Forwarding PHB" that led to the publication of revised specification of EF "An Expedited Forwarding PHB". Its primary motivation is providing additional explanation to the revised EF definition and its properties. The document also provides additional implementation examples and gives some guidance for computation of the numerical parameters of the new definition for several well known schedulers and router architectures. This memo provides information for the Internet community.

3246 Davie Mar 2002 An Expedited Forwarding PHB (Per-Hop Behavior)

This document defines a PHB (per-hop behavior) called Expedited Forwarding (EF). The PHB is a basic building block in the Differentiated Services architecture. EF is intended to provide a building block for low delay, low jitter and low loss services by ensuring that the EF aggregate is served at a certain configured rate. This document obsoletes RFC 2598. [STANDARDS TRACK]

3245	Klensin, Ed.	Mar 2002	The History and Context of Telephone Number Mapping (ENUM) Operational Decisions: Informational Documents Contributed to ITU-T Study Group 2 (SG2)

RFC 2916 assigned responsibility for a number of administrative and operational details of Telephone Number Mapping (ENUM) to the IAB. It also anticipated that ITU would take responsibility for determining the legitimacy and appropriateness of applicants for delegation of "country code"-level subdomains of the top-level ENUM domain. Recently, three memos have been prepared for the ITU-T Study Group 2 (SG2) to explain the background of, and reasoning for, the relevant decisions. The IAB has also supplied a set of procedural instructions to the RIPE NCC for implementation of their part of the model. The content of the three memos is provided in this document for the information of the IETF community.

3244	Swift	Feb 2002	Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols

This memo specifies Microsoft’s Windows 2000 Kerberos change password and set password protocols. The Windows 2000 Kerberos change password protocol interoperates with the original Kerberos change password protocol. Change password is a request reply protocol that includes a KRB_PRIV message that contains the new password for the user. This memo provides information for the Internet community.

3243	Jonsson	Apr 2002	RObust Header Compression (ROHC): Requirements and Assumptions for 0-byte IP/UDP/RTP Compression

This document contains requirements for the 0-byte IP/UDP/RTP (Internet Protocol/User Datagram Protocol/Real-Time Transport Protocol) header compression scheme to be developed by the Robust Header Compression (ROHC) Working Group. It also includes the basic assumptions for the typical link layers over which 0-byte compression may be implemented, and assumptions about its usage in general.

3242 Jonsson Apr 2002 RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP

This document defines a ROHC (Robust Header Compression) profile for compression of IP/UDP/RTP (Internet Protocol/User Datagram Protocol/Real-Time Transport Protocol) packets, utilizing functionality provided by the lower layers to increase compression efficiency by completely eliminating the header for most packets during optimal operation. The profile is built as an extension to the ROHC RTP profile. It defines additional mechanisms needed in ROHC, states requirements on the assisting layer to guarantee transparency, and specifies general logic for compression and decompression making use of this header-free packet. [STANDARDS TRACK]

3241 Bormann Apr 2002 Robust Header Compression (ROHC) over PPP

This document describes an option for negotiating the use of robust header compression (ROHC) on IP datagrams transmitted over the Point-to-Point Protocol (PPP). It defines extensions to the PPP Control Protocols for IPv4 and IPv6. [STANDARDS TRACK]

3240 Clunie Feb 2002 Digital Imaging and Communications in Medicine (DICOM) - Application/dicom MIME Sub-type Registration

This document describes the registration of the MIME sub-type application/dicom (Digital Imaging and Communications in Medicine). The baseline encoding is defined by the DICOM Standards Committee in "Digital Imaging and Communications in Medicine". This memo provides information for the Internet community.

3239	Kugler	Feb 2002	Internet Printing Protocol (IPP): Requirements for Job, Printer, and Device Administrative Operations

This document specifies the requirements and uses cases for some optional administrative operations for use with the Internet Printing Protocol (IPP) version 1.0 and version 1.1. Some of these administrative operations operate on the IPP Job and Printer objects. The remaining operations operate on a new Device object that more closely models a single output device. This memo provides information for the Internet community.

3238	IAB	Jan 2002	IAB Architectural and Policy Considerations for Open Pluggable Edge Services

This document includes comments and recommendations by the IAB on some architectural and policy issues related to the chartering of Open Pluggable Edge Services (OPES) in the IETF. OPES are services that would be deployed at application-level intermediaries in the network, for example, at a web proxy cache between the origin server and the client. These intermediaries would transform or filter content, with the explicit consent of either the content provider or the end user. This memo provides information for the Internet community.

3237	Tuexen	Jan 2002	Requirements for Reliable Server Pooling

This document defines a basic set of requirements for reliable server pooling. This memo provides information for the Internet community.

3236	Baker	Feb 2002	The 'application/xhtml+xml' Media Type

This document defines the 'application/xhtml+xml' MIME media type for XHTML based markup languages; it is not intended to obsolete any previous IETF documents, in particular RFC 2854 which registers 'text/html'. This memo provides information for the Internet community.

3235 Senie Jan 2002 Network Address Translator (NAT)-Friendly Application Design Guidelines

This document discusses those things that application designers might wish to consider when designing new protocols. While many common Internet applications will operate cleanly in the presence of Network Address Translators, others suffer from a variety of problems when crossing these devices. Guidelines are presented herein to help ensure new protocols and applications will, to the extent possible, be compatible with NAT (Network Address Translation). This memo provides information for the Internet community.

3234 Carpenter Feb 2002 Middleboxes: Taxonomy and Issues

This document is intended as part of an IETF discussion about "middleboxes" - defined as any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host. This document establishes a catalogue or taxonomy of middleboxes, cites previous and current IETF work concerning middleboxes, and attempts to identify some preliminary conclusions. It does not, however, claim to be definitive. This memo provides information for the Internet community.

3233 Hoffman Feb 2002 Defining the IETF

This document gives a more concrete definition of "the IETF" as it understood today. Many RFCs refer to "the IETF". Many important IETF documents speak of the IETF as if it were an already-defined entity. However, no IETF document correctly defines what the IETF is. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3232 Reynolds Jan 2002 Assigned Numbers: RFC 1700 is Replaced by an On-line Database

This memo obsoletes RFC 1700 (STD 2) "Assigned Numbers", which contained an October 1994 snapshot of assigned Internet protocol parameters. This memo provides information for the Internet community.

3231 Levi Jan 2002 Definitions of Managed Objects for Scheduling Management Operations

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 a set of managed objects that are used to schedule management operations periodically or at specified dates and times. [STANDARDS TRACK]

3230 Mogul Jan 2002 Instance Digests in HTTP

HTTP/1.1 defines a Content-MD5 header that allows a server to include a digest of the response body. However, this is specifically defined to cover the body of the actual message, not the contents of the full file (which might be quite different, if the response is a Content-Range, or uses a delta encoding). Also, the Content-MD5 is limited to one specific digest algorithm; other algorithms, such as SHA-1 (Secure Hash Standard), may be more appropriate in some circumstances. Finally, HTTP/1.1 provides no explicit mechanism by which a client may request a digest. This document proposes HTTP extensions that solve these problems. [STANDARDS TRACK]

3229 Mogul Jan 2002 Delta encoding in HTTP

This document describes how delta encoding can be supported as a compatible extension to HTTP/1.1. [STANDARDS TRACK]

3228 Fenner Feb 2002 IANA Considerations for IPv4 Internet Group Management Protocol (IGMP)

This memo requests that the IANA create a registry for fields in the IGMP (Internet Group Management Protocol) protocol header, and provides guidance for the IANA to use in assigning parameters for those fields. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3227 Brezinski Feb 2002 Guidelines for Evidence Collection and Archiving

A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3226 Gudmundsson Dec 2001 DNSSEC and IPv6 A6 aware server/resolver message size requirements

This document mandates support for EDNS0 (Extension Mechanisms for DNS) in DNS entities claiming to support either DNS Security Extensions or A6 records. This requirement is necessary because these new features increase the size of DNS messages. If EDNS0 is not supported fall back to TCP will happen, having a detrimental impact on query latency and DNS server load. This document updates RFC 2535 and RFC 2874, by adding new requirements. [STANDARDS TRACK]

3225 Conrad Dec 2001 Indicating Resolver Support of DNSSEC

In order to deploy DNSSEC (Domain Name System Security Extensions) operationally, DNSSEC aware servers should only perform automatic inclusion of DNSSEC RRs when there is an explicit indication that the resolver can understand those RRs. This document proposes the use of a bit in the EDNS0 header to provide that explicit indication and describes the necessary protocol changes to implement that notification. [STANDARDS TRACK]

3224 Guttman Jan 2002 Vendor Extensions for Service Location Protocol, Version 2

This document specifies how the features of the Service Location Protocol, Version 2 allow for vendor extensibility safely, with no possibility of collisions. The specification introduces a new SLPv2 extension: The Vendor Opaque Extension. While proprietary protocol extensions are not encouraged by IETF standards, it is important that they not hinder interoperability of compliant implementations when they are undertaken. This document udpates RFC 2608, "The Service Location Protocol." [STANDARDS TRACK]

3223 Never Issued

RFC 3223 was never issued.

3222 Trotter Dec 2001 Terminology for Forwarding Information Base (FIB) based Router Performance

This document describes the terms to be used in a methodology that determines the IP packet forwarding performance of IP routers as a function of the forwarding information base installed within a router. The forwarding performance of an IP router may be dependent upon or may be linked to the composition and size of the forwarding information base installed within a router. This memo provides information for the Internet community.

3221 Huston Dec 2001 Commentary on Inter-Domain Routing in the Internet

This document examines the various longer term trends visible within the characteristics of the Internet’s BGP table and identifies a number of operational practices and protocol factors that contribute to these trends. The potential impacts of these practices and protocol properties on the scaling properties of the inter-domain routing space are examined. This memo provides information for the Internet community.

3220 Perkins Jan 2002 IP Mobility Support for IPv4

This document specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node. [STANDARDS TRACK]

3219 Rosenberg Jan 2002 Telephony Routing over IP (TRIP)

This document presents the Telephony Routing over IP (TRIP). TRIP is a policy driven inter-administrative domain protocol for advertising the reachability of telephony destinations between location servers, and for advertising attributes of the routes to those destinations. TRIP's operation is independent of any signaling protocol, hence TRIP can serve as the telephony routing protocol for any signaling protocol. [STANDARDS TRACK]

3218 Rescorla Jan 2002 Preventing the Million Message Attack on Cryptographic Message Syntax

This memo describes a strategy for resisting the Million Message Attack. This memo provides information for the Internet community.

3217 Housley Dec 2001 Triple-DES and RC2 Key Wrapping

This document specifies the algorithm for wrapping one Triple-DES key with another Triple-DES key and the algorithm for wrapping one RC2 key with another RC2 key. This memo provides information for the Internet community.

3216 Elliott Dec 2001 SMIng Objectives

This document describes the objectives for a new data definition language, suitable for the modeling of network management constructs, that can be directly mapped into SNMP and COPS-PR protocol operations. This memo provides information for the Internet community.

3215 Boscher Jan 2002 LDP State Machine

This document provides state machine tables for ATM (Asynchronous Transfer Mode) switch LSRs. In the current LDP specification, there is no state machine specified for processing LDP messages. We think that defining a common state machine is very important for interoperability between different LDP and CR-LDP implementations. This memo provides information for the Internet community.

3214 Ash Jan 2002 LSP Modification Using CR-LDP

This document presents an approach to modify the bandwidth and possibly other parameters of an established CR-LSP (Constraint-based Routed Label Switched Paths) using CR-LDP (Constraint-based Routed Label Distribution Protocol) without service interruption. [STANDARDS TRACK]

3213 Ash Jan 2002 Applicability Statement for CR-LDP

This document discusses the applicability of Constraint-Based LSP Setup using LDP. It discusses possible network applications, extensions to Label Distribution Protocol (LDP) required to implement constraint-based routing, guidelines for deployment and known limitations of the protocol. This document is a prerequisite to advancing CR-LDP on the standards track. This memo provides information for the Internet community.

3212 Jamoussi Jan 2002 Constraint-Based LSP Setup using LDP

This document specifies mechanisms and TLVs (Type/Length/Value) for support of CR-LSPs (constraint-based routed Label Switched Path) using LDP (Label Distribution Protocol). [STANDARDS TRACK]

3211 Gutmann Dec 2001 Password-based Encryption for CMS

This document provides a method of encrypting data using user-supplied passwords and, by extension, any form of variable-length keying material which is not necessarily an algorithm-specific fixed-format key. The Cryptographic Message Syntax data format does not currently contain any provisions for password-based data encryption. [STANDARDS TRACK]

3210 Awduche Dec 2001 Applicability Statement for Extensions to RSVP for LSP-Tunnels

This memo discusses the applicability of "Extensions to RSVP (Resource ReSerVation Protocol) for LSP Tunnels". It highlights the protocol's principles of operation and describes the network context for which it was designed. Guidelines for deployment are offered and known protocol limitations are indicated. This document is intended to accompany the submission of "Extensions to RSVP for LSP Tunnels" onto the Internet standards track. This memo provides information for the Internet community.

3209 Awduche Dec 2001 RSVP-TE: Extensions to RSVP for LSP Tunnels

This document describes the use of RSVP (Resource Reservation Protocol), including all the necessary extensions, to establish label-switched paths (LSPs) in MPLS (Multi-Protocol Label Switching). Since the flow along an LSP is completely identified by the label applied at the ingress node of the path, these paths may be treated as tunnels. A key application of LSP tunnels is traffic engineering with MPLS as specified in RFC 2702. [STANDARDS TRACK]

3208 Speakman Dec 2001 PGM Reliable Transport Protocol Specification

Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for applications that require ordered or unordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in the group either receives all data packets from transmissions and repairs, or is able to detect unrecoverable data packet loss. PGM is specifically intended as a workable solution for multicast applications with basic reliability requirements. Its central design goal is simplicity of operation with due regard for scalability and network efficiency. This memo defines an Experimental Protocol for the Internet community.

3207 Hoffman Feb 2002 SMTP Service Extension for Secure SMTP over Transport Layer Security

This document describes an extension to the SMTP (Simple Mail Transfer Protocol) service that allows an SMTP server and client to use TLS (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]

3206 Gellens Feb 2002 The SYS and AUTH POP Response Codes

This memo proposes two response codes: SYS and AUTH, which enable clients to unambiguously determine an optimal response to an authentication failure. In addition, a new capability (AUTH-RESP-CODE) is defined. [STANDARDS TRACK]

3205 Moore Feb 2002 On the use of HTTP as a Substrate

Recently there has been widespread interest in using Hypertext Transfer Protocol (HTTP) as a substrate for other applications-level protocols. This document recommends technical particulars of such use, including use of default ports, URL schemes, and HTTP security mechanisms. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3204 Zimmerer Dec 2001 MIME media types for ISUP and QSIG Objects

This document describes MIME types for application/ISUP and application/QSIG objects for use in SIP applications, according to the rules defined in RFC 2048. These types can be used to identify ISUP and QSIG objects within a SIP message such as INVITE or INFO, as might be implemented when using SIP in an environment where part of the call involves interworking to the PSTN. [STANDARDS TRACK]

3203 T'Joens Dec 2001 DHCP reconfigure extension

This document defines extensions to DHCP (Dynamic Host Configuration Protocol) to allow dynamic reconfiguration of a single host triggered by the DHCP server (e.g., a new IP address and/or local configuration parameters). [STANDARDS TRACK]

3202 Steinberger Jan 2002 Definitions of Managed Objects for Frame Relay Service Level Definitions

This memo defines an extension of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing the Frame Relay Service Level Definitions. [STANDARDS TRACK]

3201 Steinberger Jan 2002 Definitions of Managed Objects for Circuit to Interface Translation

This memo defines an extension of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing the insertion of interesting Circuit Interfaces into the ifTable. This is important for circuits that must be used within other MIB modules which require an ifEntry. It allows for integrated monitoring of circuits as well as routing to circuits using unaltered, pre-existing MIB modules. [STANDARDS TRACK]

3200 Never Issued

RFC 3200 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

Acknowledgement

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