Network Working Group
Request for Comments: 3599
Category: Informational

S. Ginoza
ISI

December 2003

Request for Comments Summary

RFC Numbers 3500-3599

Status of This Memo

This RFC is a slightly annotated list of the 100 RFCs from RFC 3500 through RFC 3599. 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
3599	Ginoza		Request for Comments Summary

This memo.

3598	Murchison	Sep 2003	Sieve Email Filtering -- Subaddress Extension

On email systems that allow for "subaddressing" or "detailed addressing" (e.g., "ken+sieve@example.org"), it is sometimes desirable to make comparisons against these sub-parts of addresses. This document defines an extension to the Sieve mail filtering language that allows users to compare against the user and detail parts of an address. [STANDARDS TRACK]

3597 Gustafsson Sep 2003 Handling of Unknown DNS Resource Record (RR) Types

Extending the Domain Name System (DNS) with new Resource Record (RR) types currently requires changes to name server software. This document specifies the changes necessary to allow future DNS implementations to handle new RR types transparently. [STANDARDS TRACK]

3596 Thomson Oct 2003 DNS Extensions to Support IP Version 6

This document defines the changes that need to be made to the Domain Name System (DNS) to support hosts running IP version 6 (IPv6). The changes include a resource record type to store an IPv6 address, a domain to support lookups based on an IPv6 address, and updated definitions of existing query types that return Internet addresses as part of additional section processing. The extensions are designed to be compatible with existing applications and, in particular, DNS implementations themselves. [STANDARDS TRACK]

3595 Wijnen Sep 2003 Textual Conventions for IPv6 Flow Label

This MIB module defines textual conventions to represent the commonly used IPv6 Flow Label. 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]

3594 Duffy Sep 2003 PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option

This document defines a new sub-option for the DHCP CableLabs Client Configuration (CCC) Option. This new sub-option will be used to direct CableLabs Client Devices (CCDs) to invalidate security tickets stored in CCD non volatile memory (i.e., locally persisted security tickets). [STANDARDS TRACK]

3593 Tesink, Ed. Sep 2003 Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals

This document defines a set of Textual Conventions for MIB modules that make use of performance history data based on 15 minute intervals.

This memo replaces RFC 2493. Changes relative to RFC 2493 are summarized in the MIB module's REVISION clause. [STANDARDS TRACK]

3592 Tesink Sep 2003 Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type

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 Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) interfaces. This document is a companion to the documents that define Managed Objects for the DS1/E1/DS2/E2 and DS3/E3 Interface Types.

This memo replaces RFC 2558. Changes relative to RFC 2558 are summarized in the MIB module's REVISION clause. [STANDARDS TRACK]

3591 Lam Sep 2003 Definitions of Managed Objects for the Optical Interface Type

This memo defines a portion of the Management Information Base (MIB) for use with Simple Network Management Protocol (SNMP) in TCP/IP-based internets. In particular, it defines objects for managing Optical Interfaces associated with WavelengthDivision Multiplexing systems or characterized by the Optical Transport Network (OTN) in accordance with the OTN architecture defined in ITU-T Recommendation G.872.

The MIB module defined in this memo can be used for performance monitoring and/or configuration of such optical interface. [STANDARDS TRACK]

3590 Haberman Sep 2003 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol

It has come to light that there is an issue with the selection of a suitable IPv6 source address for Multicast Listener Discovery (MLD) messages when a node is performing stateless address autoconfiguration. This document is intended to clarify the rules on selecting an IPv6 address to use for MLD messages. [STANDARDS TRACK]

3589 Loughney Sep 2003 Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5

This document describes the IANA's allocation of a block of Diameter Command Codes for the Third Generation Partnership Project (3GPP) Release 5. This document does not pass judgment on the usage of these command codes. Further more, these command codes are for use for Release 5. For future releases, these codes cannot be reused, but must be allocated according to the Diameter Base specification. This memo provides information for the Internet community.

3588 Calhoun Sep 2003 Diameter Base Protocol

The Diameter base protocol is intended to provide an Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter is also intended to work in both local Authentication, Authorization & Accounting and roaming situations. This document specifies the message format, transport, error reporting, accounting and security services to be used by all Diameter applications. The Diameter base application needs to be supported by all Diameter implementations. [STANDARDS TRACK]

3587 Hinden Aug 2003 IPv6 Global Unicast Address Format

This document obsoletes RFC 2374, "An IPv6 Aggregatable Global Unicast Address Format". It defined an IPv6 address allocation structure that includes Top Level Aggregator (TLA) and Next Level Aggregator (NLA). This document makes RFC 2374 and the TLA/NLA structure historic. This memo provides information for the Internet community.

3586 Blaze Aug 2003 IP Security Policy (IPSP) Requirements

This document describes the problem space and solution requirements for developing an IP Security Policy (IPSP) configuration and management framework. The IPSP architecture provides a scalable, decentralized framework for managing, discovering and negotiating the host and network security policies that govern access, authorization, authentication, confidentiality, data integrity, and other IP Security properties. This document highlights such architectural components and presents their functional requirements. [STANDARDS TRACK]

3585 Jason Aug 2003 IPsec Configuration Policy Information Model

This document presents an object-oriented information model of IP Security (IPsec) policy designed to facilitate agreement about the content and semantics of IPsec policy, and enable derivations of task-specific representations of IPsec policy such as storage schema, distribution representations, and policy specification languages used to configure IPsec-enabled endpoints. The information model described in this document models the configuration parameters defined by IPSec. The information model also covers the parameters found by the Internet Key Exchange protocol (IKE). Other key exchange protocols could easily be added to the information model by a simple extension. Further extensions can further be added easily due to the object-oriented nature of the model.

This information model is based upon the core policy classes as defined in the Policy Core Information Model (PCIM) and in the Policy Core Information Model Extensions (PCIMe). [STANDARDS TRACK]

3584 Frye Aug 2003 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework

The purpose of this document is to describe coexistence between version 3 of the Internet-standard Network Management Framework, (SNMPv3), version 2 of the Internet-standard Network Management Framework (SNMPv2), and the original Internet-standard Network Management Framework (SNMPv1). This document also describes how to convert MIB modules from SMIv1 format to SMIv2 format. This document obsoletes RFC 2576. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3583 Chaskar, Ed. Sep 2003 Requirements of a Quality of Service (QoS) Solution for Mobile IP

Mobile IP ensures correct routing of packets to a mobile node as the mobile node changes its point of attachment to the Internet. However, it is also required to provide proper Quality of Service (QoS) forwarding treatment to the mobile node's packet stream at the intermediate nodes in the network, so that QoS-sensitive IP services can be supported over Mobile IP. This document describes requirements for an IP QoS mechanism for its satisfactory operation with Mobile IP. This memo provides information for the Internet community.

3582 Abley Aug 2003 Goals for IPv6 Site-Multihoming Architectures

This document outlines a set of goals for proposed new IPv6 site-multihoming architectures. It is recognised that this set of goals is ambitious and that some goals may conflict with others. The solution or solutions adopted may only be able to satisfy some of the goals presented here. This memo provides information for the Internet community.

3581 Rosenberg Aug 2003 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing

The Session Initiation Protocol (SIP) operates over UDP and TCP, among others. When used with UDP, responses to requests are returned to the source address the request came from, and to the port written into the topmost Via header field value of the request. This behavior is not desirable in many cases, most notably, when the client is behind a Network Address Translator (NAT). This extension defines a new parameter for the Via header field, called "rport", that allows a client to request that the server send the response back to the source IP address and port from which the request originated. [STANDARDS TRACK]

3580 Congdon Sep 2003 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines

This document provides suggestions on Remote Authentication Dial In User Service (RADIUS) usage by IEEE 802.1X Authenticators. The material in this document is also included within a non-normative Appendix within the IEEE 802.1X specification, and is being presented as an IETF RFC for informational purposes. This memo provides information for the Internet community.

3579 Aboba Sep 2003 RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)

This document defines Remote Authentication Dial In User Service (RADIUS) support for the Extensible Authentication Protocol (EAP), an authentication framework which supports multiple authentication mechanisms. In the proposed scheme, the Network Access Server (NAS) forwards EAP packets to and from the RADIUS server, encapsulated within EAP-Message attributes. This has the advantage of allowing the NAS to support any EAP authentication method, without the need for method-specific code, which resides on the RADIUS server. While EAP was originally developed for use with PPP, it is now also in use with IEEE 802. This memo provides information for the Internet community.

3578 Camarillo Aug 2003 Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signalling to the Session Initiation Protocol (SIP)

This document describes a way to map Integrated Services Digital Network User Part (ISUP) overlap signalling to Session Initiation Protocol (SIP). This mechanism might be implemented when using SIP in an environment where part of the call involves interworking with the Public Switched Telephone Network (PSTN). [STANDARDS TRACK]

3577 Waldbusser Aug 2003 Introduction to the Remote Monitoring (RMON) Family of MIB Modules

The Remote Monitoring (RMON) Framework consists of a number of interrelated documents. This memo describes these documents and how they relate to one another. This memo provides information for the Internet community.

3576 Chiba Jul 2003 Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

This document describes a currently deployed extension to the Remote Authentication Dial In User Service (RADIUS) protocol, allowing dynamic changes to a user session, as implemented by network access server products. This includes support for disconnecting users and changing authorizations applicable to a user session. This memo provides information for the Internet community.

3575 Aboba Jul 2003 IANA Considerations for RADIUS (Remote Authentication Dial In User Service)

This document describes the IANA considerations for the Remote Authentication Dial In User Service (RADIUS). [STANDARDS TRACK]

3574 Soininen, Ed. Aug 2003 Transition Scenarios for 3GPP Networks

This document describes different scenarios in Third Generation Partnership Project (3GPP) defined packet network, i.e., General Packet Radio Service (GPRS) that would need IP version 6 and IP version 4 transition. The focus of this document is on the scenarios where the User Equipment (UE) connects to nodes in other networks, e.g., in the Internet. GPRS network internal transition scenarios, i.e., between different GPRS elements in the network, are out of scope. The purpose of the document is to list the scenarios for further discussion and study. This memo provides information for the Internet community.

3573 Goyret Jul 2003 Signaling of Modem-On-Hold status in Layer 2 Tunneling Protocol (L2TP)

The Layer 2 Tunneling Protocol (L2TP) defines a mechanism for tunneling Point-to-Point Protocol (PPP) sessions. It is common for these PPP sessions to be established using modems connected over the public switched telephone network.

One of the standards governing modem operation defines procedures that enable a client modem to put the call on hold and later, re-establish the modem link with minimal delay and without having to redial. While the modem call is on hold, the client phone line can be used to place or receive other calls.

The L2TP base protocol does not provide any means to signal these events from the L2TP Access Controller (LAC), where the modem is physically connected, to the L2TP Network Server (LNS), where the PPP session is handled.

This document describes a method to let the LNS know when a client modem connected to a LAC has placed the call on hold. [STANDARDS TRACK]

3572 Ogura Jul 2003 Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over SONET/SDH)

Multiple Access Protocol over SONET/SDH (MAPOS) is a high-speed link-layer protocol that provides multiple access capability over a Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH).

This document specifies the frame format for encapsulating an IPv6 datagram in a MAPOS frame. It also specifies the method of forming IPv6 interface identifiers, the method of detecting duplicate addresses, and the format of the Source/Target Link-layer Addresses option field used in IPv6 Neighbor Discovery messages. This memo provides information for the Internet community.

3571 Rawlins Aug 2003 Framework Policy Information Base for Usage Feedback

This document describes a portion of the Policy Information Base (PIB) to control policy usage collection and reporting in a device.

The provisioning classes specified here allow a Policy Decision Point (PDP) to select which policy objects should collect usage information, what information should be collected and when it should be reported.

This PIB requires the presence of other PIBs (defined elsewhere) that provide the policy objects from which usage information is collected. This memo provides information for the Internet community.

3570 Rzewski Jul 2003 Content Internetworking (CDI) Scenarios

In describing content internetworking as a technology targeted for use in production networks, it is useful to provide examples of the sequence of events that may occur when two content networks decide to interconnect. The scenarios presented here seek to provide some concrete examples of what content internetworking is, and also to provide a basis for evaluating content internetworking proposals. This memo provides information for the Internet community.

3569 Bhattacharyya Jul 2003 An Overview of Source-Specific Multicast (SSM)

The purpose of this document is to provide an overview of Source-Specific Multicast (SSM) and issues related to its deployment. It discusses how the SSM service model addresses the challenges faced in inter-domain multicast deployment, changes needed to routing protocols and applications to deploy SSM and interoperability issues with current multicast service models. This memo provides information for the Internet community.

3568 Barbir Jul 2003 Known Content Network (CN) Request-Routing Mechanisms

This document presents a summary of Request-Routing techniques that are used to direct client requests to surrogates based on various policies and a possible set of metrics. The document covers techniques that were commonly used in the industry on or before December 2000. In this memo, the term Request-Routing represents techniques that is commonly called content routing or content redirection. In principle, Request-Routing techniques can be classified under: DNS Request-Routing, Transport-layer Request-Routing, and Application-layer Request-Routing. This memo provides information for the Internet community.

3567 Li Jul 2003 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication

This document describes the authentication of Intermediate System to Intermediate System (IS-IS) Protocol Data Units (PDUs) using the Hashed Message Authentication Codes - Message Digest 5 (HMAC-MD5) algorithm as found in RFC 2104. IS-IS is specified in International Standards Organization (ISO) 10589, with extensions to support Internet Protocol version 4 (IPv4) described in RFC 1195. The base specification includes an authentication mechanism that allows for multiple authentication algorithms. The base specification only specifies the algorithm for cleartext passwords.

This document proposes an extension to that specification that allows the use of the HMAC-MD5 authentication algorithm to be used in conjunction with the existing authentication mechanisms. This memo provides information for the Internet community.

3566 Frankel Sep 2003 The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec

A Message Authentication Code (MAC) is a key-dependent one way hash function. One popular way to construct a MAC algorithm is to use a block cipher in conjunction with the Cipher-Block-Chaining (CBC) mode of operation. The classic CBC-MAC algorithm, while secure for messages of a pre-selected fixed length, has been shown to be insecure across messages of varying lengths such as the type found in typical IP datagrams. This memo specifies the use of AES in CBC mode with a set of extensions to overcome this limitation. This new algorithm is named AES-XCBC-MAC-96. [STANDARDS TRACK]

3565 Schaad Jul 2003 Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)

This document specifies the conventions for using the Advanced Encryption Standard (AES) algorithm for encryption with the Cryptographic Message Syntax (CMS). [STANDARDS TRACK]

3564 Le Faucheur Jul 2003 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering

This document presents Service Provider requirements for support of Differentiated Services (Diff-Serv)-aware MPLS Traffic Engineering (DS-TE).

Its objective is to provide guidance for the definition, selection and specification of a technical solution addressing these requirements. Specification for this solution itself is outside the scope of this document.

A problem statement is first provided. Then, the document describes example applications scenarios identified by Service Providers where existing MPLS Traffic Engineering mechanisms fall short and Diff-Serv-aware Traffic Engineering can address the needs. The detailed requirements that need to be addressed by the technical solution are also reviewed. Finally, the document identifies the evaluation criteria that should be considered for selection and definition of the technical solution. This memo provides information for the Internet community.

3563 Zinin Jul 2003 Cooperative Agreement Between the ISOC/IETF and ISO/IEC Joint Technical Committee 1/Sub Committee 6 (JTC1/SC6) on IS-IS Routing Protocol Development

This document contains the text of the agreement signed between ISOC/IETF and ISO/IEC JTC1/SC6 regarding cooperative development of the IS-IS routing protocol. The agreement includes definitions of the related work scopes for the two organizations, request for creation and maintenance of an IS-IS registry by IANA, as well as collaboration guidelines. This memo provides information for the Internet community.

3562 Leech Jul 2003 Key Management Considerations for the TCP MD5 Signature Option

The TCP MD5 Signature Option (RFC 2385), used predominantly by BGP, has seen significant deployment in critical areas of Internet infrastructure. The security of this option relies heavily on the quality of the keying material used to compute the MD5 signature. This document addresses the security requirements of that keying material. This memo provides information for the Internet community.

3561 Perkins Jul 2003 Ad hoc On-Demand Distance Vector (AODV) Routing

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols. This memo defines an Experimental Protocol for the Internet community.

3560 Housley Jul 2003 Use of the RSAES-OAEP Key Transport Algorithm in the Cryptographic Message Syntax (CMS)

This document describes the conventions for using the RSAES-OAEP key transport algorithm with the Cryptographic Message Syntax (CMS). The CMS specifies the enveloped-data content type, which consists of an encrypted content and encrypted content-encryption keys for one or more recipients. The RSAES-OAEP key transport algorithm can be used to encrypt content-encryption keys for intended recipients. [STANDARDS TRACK]

3559 Thaler Jun 2003 Multicast Address Allocation MIB

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 managing multicast address allocation. [STANDARDS TRACK]

3558 Li Jul 2003 RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)

This document describes the RTP payload format for Enhanced Variable Rate Codec (EVRC) Speech and Selectable Mode Vocoder (SMV) Speech. Two sub-formats are specified for different application scenarios. A bundled/interleaved format is included to reduce the effect of packet loss on speech quality and amortize the overhead of the RTP header over more than one speech frame. A non-bundled format is also supported for conversational applications. [STANDARDS TRACK]

3557 Xie, Ed. Jul 2003 RTP Payload Format for European Telecommunications Standards Institute (ETSI) European Standard ES 201 108 Distributed Speech Recognition Encoding

This document specifies an RTP payload format for encapsulating European Telecommunications Standards Institute (ETSI) European Standard (ES) 201 108 front-end signal processing feature streams for distributed speech recognition (DSR) systems. [STANDARDS TRACK]

3556 Casner Jul 2003 Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth

This document defines an extension to the Session Description Protocol (SDP) to specify two additional modifiers for the bandwidth attribute. These modifiers may be used to specify the bandwidth allowed for RTP Control Protocol (RTCP) packets in a Real-time Transport Protocol (RTP) session. [STANDARDS TRACK]

3555 Casner Jul 2003 MIME Type Registration of RTP Payload Formats

This document defines the procedure to register RTP Payload Formats as audio, video or other MIME subtype names. This is useful in a text-based format or control protocol to identify the type of an RTP transmission. This document also registers all the RTP payload formats defined in the RTP Profile for Audio and Video Conferences as MIME subtypes. Some of these may also be used for transfer modes other than RTP. [STANDARDS TRACK]

3554 Bellovin Jul 2003 On the Use of Stream Control Transmission Protocol (SCTP) with IPsec

This document describes functional requirements for IPsec (RFC 2401) and Internet Key Exchange (IKE) (RFC 2409) to facilitate their use in securing SCTP (RFC 2960) traffic. [STANDARDS TRACK]

3553 Mealling Jun 2003 An IETF URN Sub-namespace for Registered Protocol Parameters

This document describes a new sub-delegation for the 'ietf' URN namespace for registered protocol items. The 'ietf' URN namespace is defined in RFC 2648 as a root for persistent URIs that refer to IETF-defined resources. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3552 Rescorla Jul 2003 Guidelines for Writing RFC Text on Security Considerations

All RFCs are required to have a Security Considerations section. Historically, such sections have been relatively weak. This document provides guidelines to RFC authors on how to write a good Security Considerations section. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

3551 Schulzrinne Jul 2003 RTP Profile for Audio and Video Conferences with Minimal Control

This document describes a profile called "RTP/AVP" for the use of the real-time transport protocol (RTP), version 2, and the associated control protocol, RTCP, within audio and video multiparticipant conferences with minimal control. It provides interpretations of generic fields within the RTP specification suitable for audio and video conferences. In particular, this document defines a set of default mappings from payload type numbers to encodings.

This document also describes how audio and video data may be carried within RTP. It defines a set of standard encodings and their names when used within RTP. The descriptions provide pointers to reference implementations and the detailed standards. This document is meant as an aid for implementors of audio, video and other real-time multimedia applications.

This memorandum obsoletes RFC 1890. It is mostly backwards-compatible except for functions removed because two interoperable implementations were not found. The additions to RFC 1890 codify existing practice in the use of payload formats under this profile and include new payload formats defined since RFC 1890 was published. [STANDARDS TRACK]

3550 Schulzrinne Jul 2003 RTP: A Transport Protocol for Real-Time Applications

This memorandum describes RTP, the real-time transport protocol. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.

Most of the text in this memorandum is identical to RFC 1889 which it obsoletes. There are no changes in the packet formats on the wire, only changes to the rules and algorithms governing how the protocol is used. The biggest change is an enhancement to the scalable timer algorithm for calculating when to send RTCP packets in order to minimize transmission in excess of the intended rate when many participants join a session simultaneously. [STANDARDS TRACK]

3549 Salim Jul 2003 Linux Netlink as an IP Services Protocol

This document describes Linux Netlink, which is used in Linux both as an intra-kernel messaging system as well as between kernel and user space. The focus of this document is to describe Netlink's functionality as a protocol between a Forwarding Engine Component (FEC) and a Control Plane Component (CPC), the two components that define an IP service. As a result of this focus, this document ignores other uses of Netlink, including its use as a intra-kernel messaging system, as an inter-process communication scheme (IPC), or as a configuration tool for other non-networking or non-IP network services (such as decnet, etc.).

This document is intended as informational in the context of prior art for the ForCES IETF working group. This memo provides information for the Internet community.

3548 Josefsson Jul 2003 The Base16, Base32, and Base64 Data Encodings

This document describes the commonly used base 64, base 32, and base 16 encoding schemes. It also discusses the use of line-feeds in encoded data, use of padding in encoded data, use of non-alphabet characters in encoded data, and use of different encoding alphabets. This memo provides information for the Internet community.

3547 Baugher Jul 2003 The Group Domain of Interpretation

This document presents an ISAMKP Domain of Interpretation (DOI) for group key management to support secure group communications. The GDOI manages group security associations, which are used by IPSEC and potentially other data security protocols running at the IP or application layers. These security associations protect one or more key-encrypting keys, traffic-encrypting keys, or data shared by group members. [STANDARDS TRACK]

3546 Blake-Wilson Jun 2003 Transport Layer Security (TLS) Extensions

This document describes extensions that may be used to add functionality to Transport Layer Security (TLS). It provides both generic extension mechanisms for the TLS handshake client and server hellos, and specific extensions using these generic mechanisms.

The extensions may be used by TLS clients and servers. The extensions are backwards compatible - communication is possible between TLS 1.0 clients that support the extensions and TLS 1.0 servers that do not support the extensions, and vice versa. [STANDARDS TRACK]

3545 Koren Jul 2003 Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering

This document describes a header compression scheme for point to point links with packet loss and long delays. It is based on Compressed Real-time Transport Protocol (CRTP), the IP/UDP/RTP header compression described in RFC 2508. CRTP does not perform well on such links: packet loss results in context corruption and due to the long delay, many more packets are discarded before the context is repaired. To correct the behavior of CRTP over such links, a few extensions to the protocol are specified here. The extensions aim to reduce context corruption by changing the way the compressor updates the context at the decompressor: updates are repeated and include updates to full and differential context parameters. With these extensions, CRTP performs well over links with packet loss, packet reordering and long delays. [STANDARDS TRACK]

3544 Koren Jul 2003 IP Header Compression over PPP

This document describes an option for negotiating the use of header compression on IP datagrams transmitted over the Point-to-Point Protocol (RFC 1661). It defines extensions to the PPP Control Protocols for IPv4 and IPv6 (RFC 1332, RFC 2472). Header compression may be applied to IPv4 and IPv6 datagrams in combination with TCP, UDP and RTP transport protocols as specified in RFC 2507, RFC 2508 and RFC 3545. [STANDARDS TRACK]

3543 Glass Aug 2003 Registration Revocation in Mobile IPv4

This document defines a Mobile IPv4 Registration Revocation mechanism whereby a mobility agent involved in providing Mobile IP services to a mobile node can notify the other mobility agent providing Mobile IP services to the same mobile node of the termination of this registration. The mechanism is also usable by a home agent to notify a co-located mobile node of the termination of its binding as well. Moreover, the mechanism provides for this notification to be acknowledged. A signaling mechanism already defined by the Mobile IPv4 protocol is leveraged as a way to inform a mobile node of the revocation of its binding. [STANDARDS TRACK]

3542 Stevens May 2003 Advanced Sockets Application Program Interface (API) for IPv6

This document provides sockets Application Program Interface (API) to support "advanced" IPv6 applications, as a supplement to a separate specification, RFC 3493. The expected applications include Ping, Traceroute, routing daemons and the like, which typically use raw sockets to access IPv6 or ICMPv6 header fields. This document proposes some portable interfaces for applications that use raw sockets under IPv6. There are other features of IPv6 that some applications will need to access: interface identification (specifying the outgoing interface and determining the incoming interface), IPv6 extension headers, and path Maximum Transmission Unit (MTU) information. This document provides API access to these features too. Additionally, some extended interfaces to libraries for the "r" commands are defined. The extension will provide better backward compatibility to existing implementations that are not IPv6-capable. This memo provides information for the Internet community.

3541 Walsh May 2003 A Uniform Resource Name (URN) Namespace for the Web3D Consortium (Web3D)

This document describes a Uniform Resource Name (URN) namespace for the Web3D Consortium (Web3D) for naming persistent resources such as technical documents and specifications, Virtual Reality Modeling Language (VRML) and Extensible 3D (X3D) files and resources, Extensible Markup Language (XML) Document Type Definitions (DTDs), XML Schemas, namespaces, style sheets, media assets, and other resources produced or managed by Web3D. This memo provides information for the Internet community.

3540 Spring Jun 2003 Robust Explicit Congestion Notification (ECN) Signaling with Nonces

This note describes the Explicit Congestion Notification (ECN)-nonce, an optional addition to ECN that protects against accidental or malicious concealment of marked packets from the TCP sender. It improves the robustness of congestion control by preventing receivers from exploiting ECN to gain an unfair share of network bandwidth. The ECN-nonce uses the two ECN-Capable Transport (ECT)codepoints in the ECN field of the IP header, and requires a flag in the TCP header. It is computationally efficient for both routers and hosts. This memo defines an Experimental Protocol for the Internet community.

3539 Aboba Jun 2003 Authentication, Authorization and Accounting (AAA) Transport Profile

This document discusses transport issues that arise within protocols for Authentication, Authorization and Accounting (AAA). It also provides recommendations on the use of transport by AAA protocols. This includes usage of standards-track RFCs as well as experimental proposals. [STANDARDS TRACK]

3538 Kawatsura Jun 2003 Secure Electronic Transaction (SET) Supplement for the v1.0 Internet Open Trading Protocol (IOTP)

This document describes detailed Input/Output parameters for the Internet Open Trading Protocol (IOTP) Payment Application Programming Interface (API). It also describes procedures in the Payment Bridge for the use of SET (SET Secure Electronic Transaction) as the payment protocol within Version 1.0 of the IOTP. This memo provides information for the Internet community.

3537	Schaad	May 2003	Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES) Key

This document defines two methods for wrapping an HMAC (Hashed Message Authentication Code) key. The first method defined uses a Triple DES (Data Encryption Standard) key to encrypt the HMAC key. The second method defined uses an AES (Advanced Encryption Standard) key to encrypt the HMAC key. One place that such an algorithm is used is for the Authenticated Data type in CMS (Cryptographic Message Syntax). [PROPOSED STANDARD]

3536	Hoffman	May 2003	Terminology Used in Internationalization in the IETF

This document provides a glossary of terms used in the IETF when discussing internationalization. The purpose is to help frame discussions of internationalization in the various areas of the IETF and to help introduce the main concepts to IETF participants. This memo provides information for the Internet community.

3535	Schoenwaelder	May 2003	Overview of the 2002 IAB Network Management Workshop

This document provides an overview of a workshop held by the Internet Architecture Board (IAB) on Network Management. The workshop was hosted by CNRI in Reston, VA, USA on June 4 thru June 6, 2002. The goal of the workshop was to continue the important dialog started between network operators and protocol developers, and to guide the IETFs focus on future work regarding network management. This report summarizes the discussions and lists the conclusions and recommendations to the Internet Engineering Task Force (IETF) community. This memo provides information for the Internet community.

3534 Walleij May 2003 The application/ogg Media Type

The Ogg Bitstream Format aims at becoming a general, freely-available standard for transporting multimedia content across computing platforms and networks. The intention of this document is to define the MIME media type application/ogg to refer to this kind of content when transported across the Internet. It is the intention of the Ogg Bitstream Format developers that it be usable without intellectual property concerns. [STANDARDS TRACK]

3533 Pfeiffer May 2003 The Ogg Encapsulation Format Version 0

This document describes the Ogg bitstream format version 0, which is a general, freely-available encapsulation format for media streams. It is able to encapsulate any kind and number of video and audio encoding formats as well as other data streams in a single bitstream. This memo provides information for the Internet community. This memo provides information for the Internet community.

3532 Anderson May 2003 Requirements for the Dynamic Partitioning of Switching Elements

This document identifies a set of requirements for the mechanisms used to dynamically reallocate the resources of a switching element (e.g., an ATM switch) to its partitions. These requirements are particularly critical in the case of an operator creating a switch partition and then leasing control of that partition to a third party. This memo provides information for the Internet community.

3531 Blanchet Apr 2003 A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block

This document proposes a method to manage the assignment of bits of an IPv6 address block or range. When an organisation needs to make an address plan for its subnets or when an ISP needs to make an address plan for its customers, this method enables the organisation to postpone the final decision on the number of bits to partition in the address space they have. It does it by keeping the bits around the borders of the partition to be free as long as possible. This scheme is applicable to any bits addressing scheme using bits with partitions in the space, but its first intended use is for IPv6. It is a generalization of RFC 1219 and can be used for IPv6 assignments. This memo provides information for the Internet community.

3530 Shepler Apr 2003 Network File System (NFS) version 4 Protocol

The Network File System (NFS) version 4 is a distributed filesystem protocol which owes heritage to NFS protocol version 2, RFC 1094, and version 3, RFC 1813. Unlike earlier versions, the NFS version 4 protocol supports traditional file access while integrating support for file locking and the mount protocol. In addition, support for strong security (and its negotiation), compound operations, client caching, and internationalization have been added. Of course, attention has been applied to making NFS version 4 operate well in an Internet environment.

This document replaces RFC 3010 as the definition of the NFS version 4 protocol. [STANDARDS TRACK]

3529 Harold Apr 2003 XML-RPC is an Extensible

Markup Language-Remote Procedure Calling protocol that works over the Internet. It defines an XML format for messages that are transfered between clients and servers using HTTP. An XML-RPC message encodes either a procedure to be invoked by the server, along with the parameters to use in the invocation, or the result of an invocation. Procedure parameters and results can be scalars, numbers, strings, dates, etc.; they can also be complex record and list structures.

This document specifies a how to use the Blocks Extensible Exchange Protocol (BEEP) to transfer messages encoded in the XML-RPC format between clients and servers. This memo defines an Experimental Protocol for the Internet community.

3528 Zhao Apr 2003 Mesh-enhanced Service Location Protocol (mSLP)

This document describes the Mesh-enhanced Service Location Protocol (mSLP). mSLP enhances the Service Location Protocol (SLP) with a scope-based fully-meshed peering Directory Agent (DA) architecture. Peer DAs exchange new service registrations in shared scopes via anti-entropy and direct forwarding. mSLP improves the reliability and consistency of SLP DA services, and simplifies Service Agent (SA) registrations in systems with multiple DAs. mSLP is backward compatible with SLPv2 and can be deployed incrementally. This memo defines an Experimental Protocol for the Internet community.

3527 Kinnear Apr 2003 Link Selection sub-option for the Relay Agent Information Option for DHCPv4

This document describes the link selection sub-option of the relay-agent-information option for the Dynamic Host Configuration Protocol (DHCPv4). The giaddr specifies an IP address which determines both a subnet, and thereby a link on which a Dynamic Host Configuration Protocol (DHCP) client resides as well as an IP address that can be used to communicate with the relay agent. The subnet-selection option allows the functions of the giaddr to be split so that when one entity is performing as a DHCP proxy, it can specify the subnet/link from which to allocate an IP address, which is different from the IP address with which it desires to communicate with the DHCP server. Analogous situations exist where the relay agent needs to specify the subnet/link on which a DHCP client resides, which is different from an IP address that can be used to communicate with the relay agent. [STANDARDS TRACK]

3526 Kivinen May 2003 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)

This document defines new Modular Exponential (MODP) Groups for the Internet Key Exchange (IKE) protocol. It documents the well known and used 1536 bit group 5, and also defines new 2048, 3072, 4096, 6144, and 8192 bit Diffie-Hellman groups numbered starting at 14. The selection of the primes for theses groups follows the criteria established by Richard Schroeppel. [STANDARDS TRACK]

3525 Groves Jun 2003 Gateway Control Protocol Version 1

This document defines the protocol used between elements of a physically decomposed multimedia gateway, i.e., a Media Gateway and a Media Gateway Controller. The protocol presented in this document meets the requirements for a media gateway control protocol as presented in RFC 2805.

This document replaces RFC 3015. It is the result of continued cooperation between the IETF Megaco Working Group and ITU-T Study Group 16. It incorporates the original text of RFC 3015, modified by corrections and clarifications discussed on the Megaco E-mail list and incorporated into the Study Group 16 Implementor's Guide for Recommendation H.248. The present version of this document underwent ITU-T Last Call as Recommendation H.248 Amendment 1. Because of ITU-T renumbering, it was published by the ITU-T as Recommendation H.248.1 (03/2002), Gateway Control Protocol Version 1.

Users of this specification are advised to consult the H.248 Sub-series Implementors' Guide at http://www.itu.int/itudoc/itu-t/com16/implgd for additional corrections and clarifications. [STANDARDS TRACK]

3524 Camarillo Apr 2003 Mapping of Media Streams to Resource Reservation Flows

This document defines an extension to the Session Description Protocol (SDP) grouping framework. It allows requesting a group of media streams to be mapped into a single resource reservation flow. The SDP syntax needed is defined, as well as a new "semantics" attribute called Single Reservation Flow (SRF). [STANDARDS TRACK]

3523 Polk Apr 2003 Internet Emergency Preparedness (IEPREP) Telephony Topology Terminology

This document defines the topology naming conventions that are to be used in reference to Internet Emergency Preparedness (IEPREP) phone calls. These naming conventions should be used to focus the IEPREP Working Group during discussions and when writing requirements, gap analysis and other solutions documents. This memo provides information for the Internet community.

3522 Ludwig Apr 2003 The Eifel Detection Algorithm for TCP

The Eifel detection algorithm allows a TCP sender to detect a posteriori whether it has entered loss recovery unnecessarily. It requires that the TCP Timestamps option defined in RFC 1323 be enabled for a connection. The Eifel detection algorithm makes use of the fact that the TCP Timestamps option eliminates the retransmission ambiguity in TCP. Based on the timestamp of the first acceptable ACK that arrives during loss recovery, it decides whether loss recovery was entered unnecessarily. The Eifel detection algorithm provides a basis for future TCP enhancements. This includes response algorithms to back out of loss recovery by restoring a TCP sender's congestion control state. This memo defines an Experimental Protocol for the Internet community.

3521 Hamer Apr 2003 Framework for Session Set-up with Media Authorization

Establishing multimedia streams must take into account requirements for end-to-end QoS, authorization of network resource usage and accurate accounting for resources used. During session set up, policies may be enforced to ensure that the media streams being requested lie within the bounds of the service profile established for the requesting host. Similarly, when a host requests resources to provide a certain QoS for a packet flow, policies may be enforced to ensure that the required resources lie within the bounds of the resource profile established for the requesting host.

To prevent fraud and to ensure accurate billing, this document describes various scenarios and mechanisms that provide the linkage required to verify that the resources being used to provide a requested QoS are in-line with the media streams requested (and authorized) for the session. This memo provides information for the Internet community.

3520 Hamer Apr 2003 Session Authorization Policy Element

This document describes the representation of a session authorization policy element for supporting policy-based per-session authorization and admission control. The goal of session authorization is to allow the exchange of information between network elements in order to authorize the use of resources for a service and to co-ordinate actions between the signaling and transport planes. This document describes how a process on a system authorizes the reservation of resources by a host and then provides that host with a session authorization policy element which can be inserted into a resource reservation protocol (e.g., the Resource ReSerVation Protocol (RSVP) PATH message) to facilitate proper and secure reservation of those resources within the network. We describe the encoding of session authorization information as a policy element conforming to the format of a Policy Data object (RFC 2750) and provide details relating to operations, processing rules and error scenarios. [STANDARDS TRACK]

3519 Levkowetz May 2003 Mobile IP Traversal of Network Address Translation (NAT) Devices

Mobile IP’s datagram tunnelling is incompatible with Network Address Translation (NAT). This document presents extensions to the Mobile IP protocol and a tunnelling method which permits mobile nodes using Mobile IP to operate in private address networks which are separated from the public internet by NAT devices. The NAT traversal is based on using the Mobile IP Home Agent UDP port for encapsulated data traffic. [STANDARDS TRACK]

3518 Higashiyama Apr 2003 Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP)

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP defines an extensible Link Control Protocol (LCP) and proposes a family of Network Control Protocols (NCP) for establishing and configuring different network-layer protocols.

This document defines the NCP for establishing and configuring Remote Bridging for PPP links.

This document obsoletes RFC 2878, which was based on the IEEE 802.1D-1993 MAC Bridge. This document extends that specification by improving support for bridge control packets. [STANDARDS TRACK]

3517 Blanton Apr 2003 A Conservative Selective Acknowledgment (SACK)-based Loss Recovery Algorithm for TCP

This document presents a conservative loss recovery algorithm for TCP that is based on the use of the selective acknowledgment (SACK) TCP option. The algorithm presented in this document conforms to the spirit of the current congestion control specification (RFC 2581), but allows TCP senders to recover more effectively when multiple segments are lost from a single flight of data. [STANDARDS TRACK]

3516 Nerenberg Apr 2003 IMAP4 Binary Content Extension

This memo defines the Binary extension to the Internet Message Access Protocol (IMAP4). It provides a mechanism for IMAP4 clients and servers to exchange message body data without using a MIME content-transfer-encoding. [STANDARDS TRACK]

3515 Sparks Apr 2003 The Session Initiation Protocol (SIP) Refer Method

This document defines the REFER method. This Session Initiation Protocol (SIP) extension requests that the recipient REFER to a resource provided in the request. It provides a mechanism allowing the party sending the REFER to be notified of the outcome of the referenced request. This can be used to enable many applications, including call transfer.

In addition to the REFER method, this document defines the refer event package and the Refer-To request header. [STANDARDS TRACK]

3514 Bellovin 1 Apr 2003 The Security Flag in the IPv4 Header

Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. We define a security flag in the IPv4 header as a means of distinguishing the two cases. This memo provides information for the Internet community.

3513 Hinden Apr 2003 Internet Protocol Version 6 (IPv6) Addressing Architecture

This specification defines the addressing architecture of the IP Version 6 (IPv6) protocol. The document includes the IPv6 addressing model, text representations of IPv6 addresses, definition of IPv6 unicast addresses, anycast addresses, and multicast addresses, and an IPv6 node's required addresses. [STANDARDS TRACK]

3512 MacFaden Apr 2003 Configuring Networks and Devices with Simple Network Management Protocol (SNMP)

This document is written for readers interested in the Internet Standard Management Framework and its protocol, the Simple Network Management Protocol (SNMP). In particular, it offers guidance in the effective use of SNMP for configuration management. This information is relevant to vendors that build network elements, management application developers, and those that acquire and deploy this technology in their networks. This memo provides information for the Internet community.

3511 Hickman Apr 2003 Benchmarking Methodology for Firewall Performance

This document discusses and defines a number of tests that may be used to describe the performance characteristics of firewalls. In addition to defining the tests, this document also describes specific formats for reporting the results of the tests.

This document is a product of the Benchmarking Methodology Working Group (BMWG) of the Internet Engineering Task Force (IETF). This memo provides information for the Internet community.

3510 Herriot Apr 2003 Internet Printing Protocol/1.1: IPP URL Scheme

This memo defines the "ipp" URL (Uniform Resource Locator) scheme. This memo updates IPP/1.1: Encoding and Transport (RFC 2910), by expanding and clarifying Section 5, "IPP URL Scheme", of RFC 2910. An "ipp" URL is used to specify the network location of a print service that supports the IPP Protocol (RFC 2910), or of a network resource (for example, a print job) managed by such a print service. [STANDARDS TRACK]

3509 Zinin Apr 2003 Alternative Implementations of OSPF Area Border Routers

Open Shortest Path First (OSPF) is a link-state intra-domain routing protocol used for routing in IP networks. Though the definition of the Area Border Router (ABR) in the OSPF specification does not require a router with multiple attached areas to have a backbone connection, it is actually necessary to provide successful routing to the inter-area and external destinations. If this requirement is not met, all traffic destined for the areas not connected to such an ABR or out of the OSPF domain, is dropped. This document describes alternative ABR behaviors implemented in Cisco and IBM routers. This memo provides information for the Internet community.

3508 Levin Apr 2003 H.323 Uniform Resource Locator (URL) Scheme Registration

ITU-T Recommendation H.323 version 4 introduced an H.323-specific Uniform Resource Locator (URL). This document reproduces the H323-URL definition found in H.323, and is published as an RFC for ease of access and registration with the Internet Assigned Numbers Authority (IANA). This memo provides information for the Internet community.

3507 Elson Apr 2003 Internet Content Adaptation Protocol (ICAP)

ICAP, the Internet Content Adaption Protocol, is a protocol aimed at providing simple object-based content vectoring for HTTP services. ICAP is, in essence, a lightweight protocol for executing a "remote procedure call" on HTTP messages. It allows ICAP clients to pass HTTP messages to ICAP servers for some sort of transformation or other processing ("adaptation"). The server executes its transformation service on messages and sends back responses to the client, usually with modified messages. Typically, the adapted messages are either HTTP requests or HTTP responses. This memo provides information for the Internet community.

3506 Fujimura Mar 2003 Requirements and Design for Voucher Trading System (VTS)

Crediting loyalty points and collecting digital coupons or gift certificates are common functions in purchasing and trading transactions. These activities can be generalized using the concept of a "voucher", which is a digital representation of the right to claim goods or services. This document presents a Voucher Trading System (VTS) that circulates vouchers securely and its terminology; it lists design principles and requirements for VTS and the Generic Voucher Language (GVL), with which diverse types of vouchers can be described. This memo provides information for the Internet community.

3505 Eastlake Mar 2003 Electronic Commerce Modeling Language (ECML): Version 2 Requirements

This document lists the design principles, scope, and requirements for the Electronic Commerce Modeling Language (ECML) version 2 specification. It includes requirements as they relate to Extensible Markup Language (XML) syntax, data model, format, and payment processing. This memo provides information for the Internet community.

3504 Eastlake Mar 2003 Internet Open Trading Protocol (IOTP) Version 1, Errata

Since the publication of the RFCs specifying Version 1.0 of the Internet Open Trading Protocol (IOTP), some errors have been noted. This informational document lists these errors and provides corrections for them. This memo provides information for the Internet community.

3503 Melnikov Mar 2003 Message Disposition Notification (MDN) profile for Internet Message Access Protocol (IMAP)

The Message Disposition Notification (MDN) facility defined in RFC 2298 provides a means by which a message can request that message processing by the recipient be acknowledged as well as a format to be used for such acknowledgements. However, it doesn’t describe how multiple Mail User Agents (MUAs) should handle the generation of MDNs in an Internet Message Access Protocol (IMAP4) environment.

This document describes how to handle MDNs in such an environment and provides guidelines for implementers of IMAP4 that want to add MDN support to their products. [STANDARDS TRACK]

3502 Crispin Mar 2003 Internet Message Access Protocol (IMAP) - MULTIAPPEND Extension

This document describes the multiappending extension to the Internet Message Access Protocol (IMAP) (RFC 3501). This extension provides substantial performance improvements for IMAP clients which upload multiple messages at a time to a mailbox on the server.

A server which supports this extension indicates this with a capability name of "MULTIAPPEND". [STANDARDS TRACK]

3501 Crispin Mar 2003 INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1

The Internet Message Access Protocol, Version 4rev1 (IMAP4rev1) allows a client to access and manipulate electronic mail messages on a server. IMAP4rev1 permits manipulation of mailboxes (remote message folders) in a way that is functionally equivalent to local folders. IMAP4rev1 also provides the capability for an offline client to resynchronize with the server.

IMAP4rev1 includes operations for creating, deleting, and renaming mailboxes, checking for new messages, permanently removing messages, setting and clearing flags, RFC 2822 and RFC 2045 parsing, searching, and selective fetching of message attributes, texts, and portions thereof. Messages in IMAP4rev1 are accessed by the use of numbers. These numbers are either message sequence numbers or unique identifiers.

IMAP4rev1 supports a single server. A mechanism for accessing configuration information to support multiple IMAP4rev1 servers is discussed in RFC 2244.

IMAP4rev1 does not specify a means of posting mail; this function is handled by a mail transfer protocol such as RFC 2821. [STANDARDS TRACK]

3500 Never Issued

RFC 3500 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.