Network Working Group	D. Harrington
Internet-Draft	HuaweiSymantec
Intended status: Informational	March 03, 2009
Expires: September 4, 2009	

Survey of IETF Network Management Standards
draft-ietf-opsawg-survey-management-00

Status of This Memo

Copyright Notice

Abstract

This document provides a survey of existing IETF standards-track network management protocols and data models. The purpose of this document is to help protocol designers, implementers, and users to select appropriate standard management protocols and data models to address relevant management needs.

Table of Contents

1. Introduction
    1.1. Terminology
2. Protocols
    2.1. SNMP
    2.2. SYSLOG
    2.3. IPFIX
    2.4. PSAMP
    2.5. NETCONF
    2.6. COPS-PR
    2.7. RADIUS
    2.8. Diameter
    2.9. EPP
    2.10. VCCV
    2.11. ACAP
    2.12. XCAP
3. Draft and Standard Level Data Models
    3.1. Fault Management
    3.2. Configuration Management
    3.3. Accounting Management
    3.4. Performance Management
    3.5. Security Management
4. Proposed Standard Data Models
    4.1. Fault Management
    4.2. Configuration Management
    4.3. Accounting Management
    4.4. Performance Management
    4.5. Security Management
5. IANA Considerations
6. Security Considerations
7. Acknowledgements
8. Informative References
Appendix A. Open Issues
Appendix B. Change Log

TOC

1. Introduction

This document provides a survey of existing IETF standards-track network management protocols and data models. The purpose of this document is to help protocol designers, implementers, and users to select appropriate standard management protocols and data models to address relevant management needs.
Guidelines for Considering Operations and Management of New Protocols and Extensions (Harrington, D., “Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions,” September 2009.) [I-D.ietf-opsawg-operations-and-management] recommends working groups consider operations and management needs, and then select appropriate management protocols and data models. This document is designed to ease this process by surveying the IETF standards-track network management protocols and management data models available at the time of this document's publication.
Section 2 discusses IETF standards-track management protocols and their uses. Section 3 discusses Draft and Full Standard data models, such as MIB modules, that have been designed to address specific sets of issues.Section 4 describes Proposed Standard management data models that have been designed to address specific sets of issues.

1.1. Terminology

TOC

This document deliberately does not use the (capitalized) key words described in RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119]. RFC 2119 states the keywords must only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions). For example, they must not be used to try to impose a particular method on implementers where the method is not required for interoperability. This document is a survey of existing IETF network management technologies. This document does not describe requirements, so the key words from RFC2119 have no place here.

> CLI: Command Line Interface
>
> Data model: A mapping of the contents of an information model into a form that is specific to a particular type of data store or repository.
>
> Information model: An abstraction and representation of the entities in a managed environment, their properties, attributes and operations, and the way that they relate to each other. It is independent of any specific repository, software usage, protocol, or platform.

- [DISCUSS] markers indicate a lack of consensus on what should be written.

- [TODO] markers indicate the editor has a reasonable understanding of what needs to be (re-)written. Contributions of text would be welcome.

- Note to RFC Editor - All [DISCUSS] or [TODO] marks should be resolved before RFC publication. If any still exist, including in the Terminology section, then please return the document to the editor for resolution.

---

2. Protocols

TOC

This Section reviews which protocols the IETF has to offer for management and discusses for which applications they were designed and/or already successfully deployed. These are protocols that have reached Proposed Standard status or higher within the IETF. [DISCUSS: Juergen: I like to perhaps see even stronger guidelines]
The Overview of the 2002 IAB Network Management Workshop (Schoenwaelder, J., “Overview of the 2002 IAB Network Management Workshop,” May 2003.) [RFC3535] documented strengths and weaknesses of some IETF management protocols. In choosing existing protocol solutions to meet the management requirements, it is recommended that these strengths and weaknesses be considered. Some of the recommendations from the 2002 IAB workshop have become outdated, some have been standardized, and some are being worked on in the IETF.
Some Area Directors have formed directorates composed of experienced members of the IETF and the technical community. The details of the role for each group differ from area to area, but the primary intent is that these groups assist the Area Director(s) with the review of specifications, and serve as technical advisors when needed. At the time of this writing, the OPS Area has directorates focused on Address Management, Operations, DNS, and MIB modules. Other areas have directorates that might apply as well. Protocol designers should consider asking for help from the IETF directorates knowledgeable in available existing solutions.

2.1. SNMP

TOC

SNMP is widely used for monitoring fault and performance data. Some operators use SNMP for configuration in various environments/

technologies while others find SNMP an inappropriate choice for configuration in their environments.

SNMPv1 (Case, J., Fedor, M., Schoffstall, M., and J. Davin, “Simple Network Management Protocol (SNMP),” May 1990.) [RFC1157] is a Full Standard that the IETF has declared Historic and it is NOT RECOMMENDED due to its lack of security features. SNMPv2c (Case, J., McCloghrie, K., McCloghrie, K., Rose, M., and S. Waldbusser, “Introduction to Community-based SNMPv2,” January 1996.) [RFC1901] is an Experimental specification (not a standard of any kind) that the IETF has declared Historic and it is NOT RECOMMENDED due to its lack of security features. SNMPv3 is a Full Standard that is RECOMMENDED due to its security features, including support for authentication, encryption, timeliness and integrity checking, and fine-grained data access controls. An overview of the SNMPv3 document set is in [RFC3410] (Case, J., Mundy, R., Partain, D., and B. Stewart, “Introduction and Applicability Statements for Internet-Standard Management Framework,” December 2002.).

SNMP utilizes the Management Information Base, a virtual information store of modules of managed objects. MIB module support is uneven across vendors, and even within devices. The lack of standard MIB module support for all functionality in a device forces operators to use other protocols such as a command line interface (CLI) to do configuration of some aspects of their managed devices. Many operators have found it easier to use one protocol for all configuration than to split the task across multiple protocols.

SNMP is good at determining the operational state of specific functionality, but not necessarily for the complete operational state of a managed device.

SNMP is good for statistics gathering for specific functionality. The wide-spread use of counters in standard MIB modules permits the interoperable comparison of statistics across devices from different vendors. Counters have been especially useful in monitoring bytes and packets going in and out over various protocol interfaces. SNMP is often used to poll a device for sysUpTime, which serves to report the time since the last reinitialization of the device, to check for operational liveness, and to detect discontinuities in some counters.

SNMP traps and informs can alert an operator or an application when some aspect of a protocol fails or encounters an error condition, and the contents of a notification can be used to guide subsequent SNMP polling to gather additional information about an event.

Standards exist to use SNMP over multiple network protocols, including UDP, Ethernet, Appletalk, OSI, and others..

TOC

2.2. SYSLOG

The SYSLOG protocol [I-D.ietf-syslog-protocol] (Gerhards, R., “The syslog Protocol,” September 2007.) allows a machine to send system log messages across networks to event message collectors. The protocol is simply designed to transport these event messages. No acknowledgement of the receipt is made. One of the fundamental tenets of the SYSLOG protocol and process is its simplicity. No stringent coordination is required between the transmitters and the receivers. Indeed, the transmission of SYSLOG messages may be started on a device without a receiver being configured, or even actually physically present. Conversely, many devices will most likely be able to receive messages without explicit configuration or definitions. This simplicity has greatly aided the acceptance and deployment of SYSLOG.

Since each process, application and operating system was written somewhat independently, there has been little uniformity to the message format or content of SYSLOG messages.

The IETF has developed a new Proposed Standard version of the protocol that allows the use of any number of transport protocols including reliable transports and secure transports. The IETF has also standardized the application of message security for SYSLOG messages using TLS, and has defined a mechanism to digitally sign log data to ensure its integrity as log data is moved across the network and/or copied to different data stores.

The IETF has standardized a new message header format, including timestamp, hostname, application, and message ID, to improve filtering, interoperability and correlation between compliant implementations.

SYSLOG message content has traditionally been unstructured natural language text. This content is human-friendly, but difficult for applications to parse and correlate across vendors, or correlate with other event reporting such as SNMP traps. The IETF syslog protocol includes structured data elements to aid application-parsing. The structured data element design allows vendors to define their own structured data elements to supplement standardized elements.

The IETF has standardized MIB Textual-Conventions for facility and severity labels and codes to encourage consistency between syslog and MIB representations of these event properties.

IETF working groups are encouraged to standardize structured data elements, extensible human-friendly text, and consistent facility/severity values for SYSLOG to report events specific to their protocol.

2.3. IPFIX

TOC

There are several applications such as usage-based accounting, traffic profiling, traffic engineering, intrusion detection, and QoS monitoring, that require flow-based traffic measurements.

IPFIX [RFC5101] (Claise, B., “Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information,” January 2008.) is a Proposed Standard approach for transmitting IP traffic flow information over the network from an exporting process to an information collecting process.
IPFIX defines a common representation of flow data and a standard means of communicating the data over a number of transport protocols.

2.4. PSAMP

TOC

Several applications require sampling packets from specific data flows, or across multiple data flows, and reporting information about the packets. Measurement-based network management is a prime example. The PSAMP standard includes support for packet sampling in IPv4, IPv6, and MPLS-based networks.
PSAMP standardizes sampling, selection, metering, and reporting strategies for different purposes.
To simplify the solution, the IPFIX protocol is used for exporting the reports to collector applications.
[TODO: this is in IESG review to become a PS. update as needed]

2.5. NETCONF

TOC

The NETCONF protocol [RFC4741] (Enns, R., “NETCONF Configuration Protocol,” December 2006.) is a Proposed Standard that provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages.
The NETCONF protocol operations are realized on top of a simple Remote Procedure Call (RPC) layer.
A key aspect of NETCONF is that it allows the functionality of the management protocol to closely mirror the native command line interface of the device. This reduces implementation costs and allows timely access to new features. In addition, applications can access both the syntactic and semantic content of the device's native user interface.
The contents of both the request and the response can be fully described in XML DTDs or XML schemas, or both, allowing both parties to recognize the syntax constraints imposed on the exchange. As of this writing, no standard has been developed for data content specification.

TOC

2.6. COPS-PR

COPS-PR and the Structure of Policy Provisioning Information (SPPI) have been approved as Proposed Standards. COPS-PR [RFC3084] (Chan, K., Seligson, J., Durham, D., Gai, S., McCloghrie, K., Herzog, S., Reichmeyer, F., Yavatkar, R., and A. Smith, “COPS Usage for Policy Provisioning (COPS-PR),” March 2001.) uses the Common Open Policy Service (COPS) protocol for support of policy provisioning. The COPS-PR specification is independent of the type of policy being provisioned (QoS, Security, etc.) but focuses on the mechanisms and conventions used to communicate provisioned information between policy-decision-points (PDPs) and policy enforcement points (PEPs). COPS-PR does not make any assumptions about the policy data model being communicated, but describes the message formats and objects that carry the modeled policy data. Policy data is modeled using Policy Information Base modules (PIB modules).

COPS-PR has not had wide deployment, and operators have stated that its use of binary encoding (BER) for management data makes it difficult to develop automated scripts for simple configuration management tasks in most text-based scripting languages. In an IAB Workshop on Network Management [RFC3535] (Schoenwaelder, J., “Overview of the 2002 IAB Network Management Workshop,” May 2003.), the consensus of operators and protocol developers indicated a lack of interest in PIB modules for use with COPS-PR.

As a result, the IESG has not approved any policy models (PIB modules) as an IETF standard, and the use of COPS-PR is not recommended.

2.7. RADIUS

TOC

RADIUS [RFC2865] (Rigney, C., Willens, S., Rubens, A., and W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” June 2000.), the remote Authentication Dial In User Service, is a Draft Standard that describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.

This protocol is widely implemented and used. RADIUS is widely used in environments, such as enterprise networks, where a single administrative authority manages the network, and protects the privacy of user information.

2.8. Diameter

TOC

DIAMETER [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.) is a Proposed

Standard that provides an Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility. DIAMETER is also intended to work in local Authentication, Authorization, Accounting situations and in roaming situations.
Diameter is designed to resolve a number of known problems with RADIUS. Diameter supports server failover, transmission-level security, reliable transport over TCP, agents for proxy and redirect and relay, server-initiated messages, auditability, capability negotiation, peer discovery and configuration, and roaming support. Diameter also provides a larger attribute space than RADIUS.
Diameter features make it especially appropriate for environments where the providers of services are in different administrative domains than the maintainer (protector) of confidential user information.

2.9. EPP

TOC

The Extensible Provision Protocol [RFC4930] (Hollenbeck, S., “Extensible Provisioning Protocol (EPP),” May 2007.) is a Draft Standard that describes an application layer client-server protocol for the provisioning and management of objects stored in a shared central repository. EPP permits multiple service providers to perform object provisioning operations using a shared central object repository, and addresses the requirements for a generic registry registrar protocol.

2.10. VCCV

TOC

VCCV is a Proposed Standard protocol that provides a control channel associated with a Pseudowire. It is used for operations and management functions such as connectivity verification over the control channel. VCCV applies to all supported access circuit and transport types currently defined for Pseudowires.

2.11. ACAP

TOC

The Application Configuration Access Protocol (ACAP) is designed to support remote storage and access of program option, configuration and preference information. The data store model is designed to allow a client relatively simple access to interesting data, to allow new information to be easily added without server re-configuration, and to promote the use of both standardized data and custom or proprietary data. Key features include "inheritance" which can be used to manage default values for configuration settings and access control lists which allow interesting personal information to be shared and group information to be restricted.

ACAP's primary purpose is to allow users access to their configuration data from multiple network-connected computers. Users can then sit down in front of any network-connected computer, run any ACAP-enabled application and have access to their own configuration data. Because it is hoped that many applications will become ACAP- enabled, client simplicity was preferred to server or protocol simplicity whenever reasonable.

2.12. XCAP

TOC

XCAP [RFC4825] (Rosenberg, J., “The Extensible Markup Language (XML) Configuration Access Protocol (XCAP),” May 2007.) is a Proposed Standard protocol that allows a client to read, write, and modify application configuration data stored in XML format on a server.

XCAP is a protocol that can be used to manipulate per-user data. XCAP is a set of conventions for mapping XML documents and document components into HTTP URIs, rules for how the modification of one resource affects another, data validation constraints, and authorization policies associated with access to those resources. Because of this structure, normal HTTP primitives can be used to manipulate the data. XCAP is meant to support the configuration needs for a multiplicity of applications, rather than just a single one.

XCAP was not designed as a general purpose XML search protocol, XML database update protocol, nor a general purpose, XML-based configuration protocol for network elements.

---

3. Draft and Standard Level Data Models

TOC

[DISCUSS: JS: The weakest part of the document is IMHO section 6. It is not clear to me what David's intention were here; sometimes he gives general advise while at other places he kind of surveys data models and such things. I am also not sure all the stuff listed there is actually useful to list; for example, has anybody ever deployed the technology which came out of the snmpconf working group? So we need to be more selective and probably also organize our pointers based on the protocol layer people are working on (transmission specific MIB modules are kind of widely used, people managing application servers usually do not use much of SNMP; the IETF application management MIBs we have produced have not gained large deployments as far as I can tell).]

[DISCUSS: David: Some MIB modules may not be deployed because few people know about them and have never tried them. Others may have been tried and been found to be inadequate. We have very little feedback concerning which ones are useful and which are widely deployed, which have been found useful by operators, and which have been found to be junk. ;-) I hesitate to make recommendations that people should avoid a MIB module unless there is real evidence that it is unsuitable for its designed task. Even then, I hesitate because maybe the MIB would be found useful in a different environment that is just emerging. Maybe the IETF needs to perform a de-crufting operation for data models, similar to that done for protocols a few years ago. But I think that would require feedback from LOTS of operators and application developers - and these tend to be scarce in the IETF.]

The purpose of this section is to inform protocol designers about solutions for which information or data models have been standardized in the IETF, so they can reuse existing solutions or apply the information model to new solutions.

This section discusses management data models that have reached at least Draft Standard status in the IETF. IETF specifications must have "multiple, independent, and interoperable implementations" before they can be advanced to Draft Standard status. Management data models have a slightly different interpretation for interoperability. This is discussed in detail in BCP 27: Advancement of MIB specifications on the IETF Standards Track (O'Dell, M., Alvestrand, H., Wijnen, B., and S. Bradner, “Advancement of MIB specifications on the IETF Standards Track,” October 1998.) [RFC2438] discusses special considerations about the advancement process for management data models. Most IETF management data models never advance beyond Proposed Standard. T his section will focus on those data models that have reached at least Draft status. This is supplemented by a chapter that lists additional data models that are Proposed Standard status.

[TODO] discuss specific MIB modules, SDEs, XML schemas that are designed to solve generic problems. This might cover things like Textual Conventions, RFC3415 Target tables, SYSLOG SDEs defined in -protocol-, SYSLOG -sign-, IPFIX IEs, etc.

3.1. Fault Management

TOC

RFC 3418 [RFC3418] (Presuhn, R., “Management Information Base (MIB) for the Simple Network Management Protocol (SNMP),” December 2002.), part of STD 62 SNMP, contains objects in the system group that are often polled to determine if a device is still operating, and sysUpTime can be used to detect if a system has rebooted, and counters have been reinitialized.

RFC3413 [RFC3413] (Levi, D., Meyer, P., and B. Stewart, “Simple Network Management Protocol (SNMP) Applications,” December 2002.), part of STD 62 SNMP, includes objects designed for managing notifications, including tables for addressing, retry parameters, security, lists of targets for notifications, and user customization filters.

An RMON monitor [RFC2819] (Waldbusser, S., “Remote Network Monitoring Management Information Base,” May 2000.) can be configured to recognize conditions, most notably error conditions, and continuously to check for them. When one of these conditions occurs, the event may be logged, and management stations may be notified in a number of ways. See further discussion of RMON under Performance Management.

TOC

3.2. Configuration Management

It is expected that standard XML-based data models will be developed for use with NETCONF, and working groups might identify specific NETCONF data models that would be applicable to the new protocol. At the time of this writing, no such standard data models exist.

For monitoring network configuration, such as physical and logical network topologies, existing MIB modules already exist that provide some of the desired capabilities. New MIB modules might be developed for the target functionality to allow operators to monitor and modify the operational parameters, such as timer granularity, event reporting thresholds, target addresses, and so on.

RFC 3418 [RFC3418] (Presuhn, R., “Management Information Base (MIB) for the Simple Network Management Protocol (SNMP),” December 2002.), part of STD 62 SNMPv3, contains objects in the system group that are often polled to determine if a device is still operating, and sysUpTime can be used to detect if a system has rebooted and caused potential discontinuity in counters. Other objects in the system MIB are useful for identifying the type of device, the location of the device, the person responsible for the device, etc.

RFC3413 [RFC3413] (Levi, D., Meyer, P., and B. Stewart, “Simple Network Management Protocol (SNMP) Applications,” December 2002.), part of STD 62 SNMPv3, includes objects designed for configuring notification destinations, and for configuring proxy-forwarding SNMP agents, which can be used to forward messages through firewalls and NAT devices.

RFC2863 [RFC2863] (McCloghrie, K. and F. Kastenholz, “The Interfaces Group MIB,” June 2000.), the Interfaces MIB is used for managing Network Interfaces. This includes the 'interfaces' group of MIB-II and discusses the experience gained from the definition of numerous media-specific MIB modules for use in conjunction with the 'interfaces' group for managing various sub-layers beneath the internetwork-layer.

TOC

3.3. Accounting Management

TODO: RADIUS Accounting MIBs are PS; are there any DS data models for accounting?]

3.4. Performance Management

TOC

MIB modules typically contain counters to determine the frequency and rate of an occurrence.

RFC2819, STD 59 RMON, defines objects for managing remote network monitoring devices. An organization may employ many remote management probes, one per network segment, to manage its internet. These devices may be used for a network management service provider to access a client network, often geographically remote. Most of the objects in the RMON MIB module are suitable for the management of any type of network, and there are some which are specific to managing Ethernet networks.

RMON allows a probe to be configured to perform diagnostics and to collect statistics continuously, even when communication with the management station may not be possible or efficient. The alarm group periodically takes statistical samples from variables in the probe and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.

The RMON host group discovers hosts on the network by keeping a list of source and destination MAC Addresses seen in good packets promiscuously received from the network, and contains statistics associated with each host. The hostTopN group is used to prepare reports that describe the hosts that top a list ordered by one of their statistics. The available statistics are samples of one of their base statistics over an interval specified by the management station. Thus, these statistics are rate based. The management station also selects how many such hosts are reported.

The RMON matrix group stores statistics for conversations between sets of two addresses. The filter group allows packets to be matched by a filter equation. These matched packets form a data stream that may be captured or may generate events. The Packet Capture group allows packets to be captured after they flow through a channel. The event group controls the generation and notification of events from this device.

The RMON-2 MIB [RFC4502] (Waldbusser, S., “Remote Network Monitoring Management Information Base Version 2,” May 2006.) extends RMON by providing RMON analysis up to the application layer. The SMON MIB [RFC2613] (Waterman, R., Lahaye, B., Romascanu, D., and S. Waldbusser, “Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0,” June 1999.) extends RMON by providing RMON analysis for switched networks.

3.5. Security Management

TOC

Working groups should consider existing data models that would be relevant to monitoring and managing the security of the new protocol. The IETF has no standard data models for managing security protocols such as TLS and SSH.

4. Proposed Standard Data Models

TOC

4.1. Fault Management

TOC

The IETF SYSLOG protocol [I-D.ietf-syslog-protocol] (Gerhards, R., “The syslog Protocol,” September 2007.) is a Proposed Standard that includes a mechanism for defining structured data elements (SDEs). The SYSLOG protocol document defines an initial set of SDEs that relate to content time quality, content origin, and meta-information about the message, such as language. Proprietary SDEs can be used to supplement the IETF-defined SDEs.

DISMAN-EVENT-MIB in RFC 2981 and DISMAN-EXPRESSION-MIB in RFC 2982 provide a superset of the capabilities of the RMON alarm and event groups. These modules provide mechanisms for thresholding and reporting anomalous events to management applications.

The ALARM MIB in RFC 3877 and the Alarm Reporting Control MIB in RFC 3878 specify mechanisms for expressing state transition models for persistent problem states. There is also a mechanism specified to correlate a notification with subsequent state transition notifications about the same entity/object.

Other MIB modules that may be applied to Fault Management include:

> NOTIFICATION-LOG-MIB in RFC 3014
>
> ENTITY-STATE-MIB in RFC 4268
>
> ENTITY-SENSOR-MIB in RFC 4268

4.2. Configuration Management

TOC

The Entity MIB [RFC4133] (Bierman, A. and K. McCloghrie, “Entity MIB (Version 3),” August 2005.) is used for managing multiple logical and physical entities managed by a single SNMP agent. This module provides a useful mechanism for identifying the entities comprising a system. There are also event notifications defined for configuration changes that may be useful to management applications.

RFC3159 [RFC3159] (McCloghrie, K., Fine, M., Seligson, J., Chan, K., Hahn, S., Sahita, R., Smith, A., and F. Reichmeyer, “Structure of Policy Provisioning Information (SPPI),” August 2001.) discusses the Structure of Policy Provisioning Information, an extension to the SMI standard for purposes of policy-based provisioning, for use with the COPS-PR protocol defined in RFC3084 [RFC3084] (Chan, K., Seligson, J., Durham, D., Gai, S., McCloghrie, K., Herzog, S., Reichmeyer, F., Yavatkar, R., and A. Smith, “COPS Usage for Policy Provisioning (COPS-PR),” March 2001.). RFC3317 [RFC3317] (Chan, K., Sahita, R., Hahn, S., and K. McCloghrie, “Differentiated Services Quality of Service Policy Information Base,” March 2003.) defines a DiffServ QoS PIB. At the time of this writing, there are no standards-track PIBs. During the IAB Workshop on Network Management, the workshop had rough consensus from the protocol developers that the IETF should not spend resources on SPPI PIB definitions, and the operators had rough consensus that they do not care about SPPI PIBs.

The Policy Based Management MIB [RFC4011] (Waldbusser, S., Saperia, J., and T. Hongal, “Policy Based Management MIB,” March 2005.) defines objects that enable policy-based monitoring and management of SNMP infrastructures, a scripting language, and a script execution environment.

RFC3165 [RFC3165] (Levi, D. and J. Schoenwaelder, “Definitions of Managed Objects for the Delegation of Management Scripts,” August 2001.) supports the use of user-written scripts to delegate management functionality.

Proposed Standard RFC4011 [RFC4011] (Waldbusser, S., Saperia, J., and T. Hongal, “Policy Based Management MIB,” March 2005.) defines objects that enable policy-based monitoring using SNMP, using a scripting language, and a script execution environment.

Few vendors have implemented MIB modules that support scripting. Some vendors consider running user-developed scripts within the managed device as a violation of support agreements.

[TODO] Informational RFC3317 defines a DiffServ QoS PIB, and Informational RFC3571 defines policy classes for monitoring and reporting policy usage feedback, as well as policy classes for controlling reporting intervals, suspension, resumption and solicitation. At the time of this writing, there are no standards-track PIBs During the IAB Workshop on Network Management, the workshop had rough consensus from the protocol developers that the IETF should not spend resources on SPPI PIB definitions, and the operators had rough consensus that they do not care about SPPI PIBs.

TOC

4.3. Accounting Management

DIAMETER [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.) accounting might be collected for services, and working groups might document some of the RADIUS/DIAMETER attributes that could be used. [TODO: what data models?]
RADIUS Authentication Client MIB [RFC4668] (Nelson, D., “RADIUS Authentication Client MIB for IPv6,” August 2006.) and RADIUS Authentication Server MIB [RFC4669] (Nelson, D., “RADIUS Authentication Server MIB for IPv6,” August 2006.) allow the gathering of accounting data.
[TODO] The IPFIX protocol [RFC5101] (Claise, B., “Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information,” January 2008.) can collect information related to IP flows, and existing Information Elements (IEs) may be appropriate to report flows of the new protocol. New IPFIX Information Elements might be useful for collecting flow information useful only in consideration of the new protocol. As of this writing, no IEs have reached Proposed Standard status yet, but a base set of IEs has been submitted to IESG for advancement. These include IEs for Identifying the scope of reporting, Metering and Export Process configuration, IP and Transport and Sub-IP header fields, Packet and Flow properties, timestamps, and counters.

TOC

4.4. Performance Management

RAQMON [RFC4710] (Siddiqui, A., Romascanu, D., and E. Golovinsky, “Real-time Application Quality-of-Service Monitoring (RAQMON) Framework,” October 2006.) describes Real-Time Application Quality of Service Monitoring.
The IPPM WG has defined metrics for accurately measuring and reporting the quality, performance, and reliability of Internet data delivery services. The metrics include connectivity, one-way delay and loss, round-trip delay and loss, delay variation, loss patterns, packet reordering, bulk transport capacity, and link bandwidth capacity.
[TODO: detail the RFCs - 4737, 3393, 2681, 2680, 2679, 2678]
SIP Package for Voice Quality Reporting [I-D.ietf-sipping-rtcp-summary] (Pendleton, A., Clark, A., Johnston, A., and H. Sinnreich, “Session Initiation Protocol Event Package for Voice Quality Reporting,” March 2010.) defines a SIP event package that enables the collection and reporting of metrics that measure the quality for Voice over Internet Protocol (VoIP) sessions.

TOC

4.5. Security Management

---

5. IANA Considerations

TOC

This document does not introduce any new codepoints or name spaces for registration with IANA. Note to RFC Editor: this section may be removed on publication as an RFC.

---

6. Security Considerations

TOC

This document introduces no new security concerns.

---

7. Acknowledgements

TOC

---

8. Informative References

TOC

[I-D.ietf-opsawg-operations-and-management]	Harrington, D., "Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions," draft-ietf-opsawg-operations-and-management-09 (work in progress), September 2009 (TXT).
[I-D.ietf-sipping-rtcp-summary]	Pendleton, A., Clark, A., Johnston, A., and H. Sinnreich, "Session Initiation Protocol Event Package for Voice Quality Reporting," draft-ietf-sipping-rtcp-summary-10 (work in progress), March 2010 (TXT).
[I-D.ietf-syslog-protocol]	Gerhards, R., "The syslog Protocol," draft-ietf-syslog-protocol-23 (work in progress), September 2007 (TXT).
[RFC1157]	Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol (SNMP)," STD 15, RFC 1157, May 1990 (TXT).
[RFC1901]	Case, J., McCloghrie, K., McCloghrie, K., Rose, M., and S. Waldbusser, "Introduction to Community-based SNMPv2," RFC 1901, January 1996 (TXT).
[RFC2119]	

	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2438]	O'Dell, M., Alvestrand, H., Wijnen, B., and S. Bradner, “Advancement of MIB specifications on the IETF Standards Track,” BCP 27, RFC 2438, October 1998 (TXT, HTML, XML).
[RFC2613]	Waterman, R., Lahaye, B., Romascanu, D., and S. Waldbusser, “Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0,” RFC 2613, June 1999 (TXT).
[RFC2819]	Waldbusser, S., “Remote Network Monitoring Management Information Base,” STD 59, RFC 2819, May 2000 (TXT).
[RFC2863]	McCloghrie, K. and F. Kastenholz, “The Interfaces Group MIB,” RFC 2863, June 2000 (TXT).
[RFC2865]	Rigney, C., Willens, S., Rubens, A., and W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” RFC 2865, June 2000 (TXT).
[RFC3084]	Chan, K., Seligson, J., Durham, D., Gai, S., McCloghrie, K., Herzog, S., Reichmeyer, F., Yavatkar, R., and A. Smith, “COPS Usage for Policy Provisioning (COPS-PR),” RFC 3084, March 2001 (TXT).
[RFC3159]	McCloghrie, K., Fine, M., Seligson, J., Chan, K., Hahn, S., Sahita, R., Smith, A., and F. Reichmeyer, “Structure of Policy Provisioning Information (SPPI),” RFC 3159, August 2001 (TXT).
[RFC3165]	Levi, D. and J. Schoenwaelder, “Definitions of Managed Objects for the Delegation of Management Scripts,” RFC 3165, August 2001 (TXT).
[RFC3317]	Chan, K., Sahita, R., Hahn, S., and K. McCloghrie, “Differentiated Services Quality of Service Policy Information Base,” RFC 3317, March 2003 (TXT).
[RFC3410]	Case, J., Mundy, R., Partain, D., and B. Stewart, “Introduction and Applicability Statements for Internet-Standard Management Framework,” RFC 3410, December 2002 (TXT).
[RFC3413]	Levi, D., Meyer, P., and B. Stewart, “Simple Network Management Protocol (SNMP) Applications,” STD 62, RFC 3413, December 2002 (TXT).
[RFC3418]	Presuhn, R., “Management Information Base (MIB) for the Simple Network Management Protocol (SNMP),” STD 62, RFC 3418, December 2002 (TXT).
[RFC3444]	Pras, A. and J. Schoenwaelder, “On the Difference between Information Models and Data Models,” RFC 3444, January 2003 (TXT).

[RFC3535]	Schoenwaelder, J., “Overview of the 2002 IAB Network Management Workshop,” RFC 3535, May 2003 (TXT).
[RFC3585]	Jason, J., Rafalow, L., and E. Vyncke, “IPsec Configuration Policy Information Model,” RFC 3585, August 2003 (TXT).
[RFC3588]	Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” RFC 3588, September 2003 (TXT).
[RFC3644]	Snir, Y., Ramberg, Y., Strassner, J., Cohen, R., and B. Moore, “Policy Quality of Service (QoS) Information Model,” RFC 3644, November 2003 (TXT).
[RFC3670]	Moore, B., Durham, D., Strassner, J., Westerinen, A., and W. Weiss, “Information Model for Describing Network Device QoS Datapath Mechanisms,” RFC 3670, January 2004 (TXT).
[RFC3805]	Bergman, R., Lewis, H., and I. McDonald, “Printer MIB v2,” RFC 3805, June 2004 (TXT).
[RFC4011]	Waldbusser, S., Saperia, J., and T. Hongal, “Policy Based Management MIB,” RFC 4011, March 2005 (TXT).
[RFC4133]	Bierman, A. and K. McCloghrie, “Entity MIB (Version 3),” RFC 4133, August 2005 (TXT).
[RFC4502]	Waldbusser, S., “Remote Network Monitoring Management Information Base Version 2,” RFC 4502, May 2006 (TXT).
[RFC4668]	Nelson, D., “RADIUS Authentication Client MIB for IPv6,” RFC 4668, August 2006 (TXT).
[RFC4669]	Nelson, D., “RADIUS Authentication Server MIB for IPv6,” RFC 4669, August 2006 (TXT).
[RFC4710]	Siddiqui, A., Romascanu, D., and E. Golovinsky, “Real-time Application Quality-of-Service Monitoring (RAQMON) Framework,” RFC 4710, October 2006 (TXT).
[RFC4741]	Enns, R., “NETCONF Configuration Protocol,” RFC 4741, December 2006 (TXT).
[RFC4825]	Rosenberg, J., “The Extensible Markup Language (XML) Configuration Access Protocol (XCAP),” RFC 4825, May 2007 (TXT).
[RFC4930]	Hollenbeck, S., “Extensible Provisioning Protocol (EPP),” RFC 4930, May 2007 (TXT).
[RFC5101]	Claise, B., “Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information,” RFC 5101, January 2008 (TXT).

Appendix A. Open Issues

TOC

> [TODO: need to verify all citations have references (in xref format)]
>
> Organize data models by layer?

Appendix B. Change Log

TOC

Changes from being part of opsawg-operations-and-management to being opsawg-survey-00

Author's Address

TOC

	David Harrington
	HuaweiSymantec
	1700 Alma Dr, Suite 100
	Plano, TX 75075
	USA
Phone:	+1 603 436 8634
Fax:	
EMail:	dharrington@huawei.com
URI:	