                An Overview of the IETF Network Management Standards

Abstract

   This document gives an overview of the IETF network management
   standards and summarizes existing and ongoing development of IETF
   Standards Track network management protocols and data models. The
   document refers to other overview documents, where they exist and
   classifies the standards for easy orientation. The purpose of this
   document is, on the one hand, to help system developers and users to
   select appropriate standard management protocols and data models to
   address relevant management needs. On the other hand, the document
   can be used as an overview and guideline by other Standard
   Development Organizations or bodies planning to use IETF management
   technologies and data models. This document does not cover
   Operations, Administration, and Maintenance (OAM) technologies on the
   data-path, e.g., OAM of tunnels, MPLS Transport Profile (MPLS-TP)
   OAM, and pseudowire as well as the corresponding management models.

Copyright Notice

Table of Contents

1. Introduction

1.1. Scope and Target Audience

   This document gives an overview of the IETF network management
   standards and summarizes existing and ongoing development of IETF
   Standards Track network management protocols and data models. The
   document refers to other overview documents where they exist and
   classifies the standards for easy orientation.

   The target audience of the document is, on the one hand, IETF working
   groups, which aim to select appropriate standard management protocols
   and data models to address their needs concerning network management.
   On the other hand, the document can be used as an overview and
   guideline by non-IETF Standards Development Organizations (SDOs)
   planning to use IETF management technologies and data models for the
   realization of management applications. The document can also be
   used to initiate a discussion between the bodies with the goal to
   gather new requirements and to detect possible gaps. Finally, this
   document is directed to all interested parties that seek to get an
   overview of the current set of the IETF network management protocols
   such as network administrators or newcomers to the IETF.

   Section 2 gives an overview of the IETF core network management
   standards with a special focus on Simple Network Management Protocol
   (SNMP), syslog, IP Flow Information eXport / Packet SAMPling (IPFIX/
   PSAMP), and Network Configuration (NETCONF). Section 3 discusses
   IETF management protocols and mechanisms with a specific focus, e.g.,
   IP address management or IP performance management. Section 4
   discusses IETF data models, such as MIB modules, IPFIX Information
   Elements, Syslog Structured Data Elements, and YANG modules designed
   to address a specific set of management issues and provides two
   complementary overviews for the network management data models
   standardized within the IETF. Section 4.1 focuses on a broader view
   of models classified into categories such as generic and
   infrastructure data models as well as data models matched to
   different layers. Whereas Section 4.2 structures the data models
   following the management application view and maps them to the
   network management tasks fault, configuration, accounting,
   performance, and security management.

   Appendix A guides the reader for the high-level selection of
   management standards. For this, the section classifies the protocols
   according to high-level criteria, such as push versus pull
   mechanisms, passive versus active monitoring, as well as categorizes
   the protocols concerning the network management task they address and
   their data model extensibility. If the reader is interested only in
   a subset of the IETF network management protocols and data models

described in this document, Appendix A can be used as a dispatcher to
the corresponding chapter. Appendix B gives an overview of the new
work on Energy Management in the IETF.

This document mainly refers to Proposed, Draft, or Internet Standard
documents from the IETF (see [RFCSEARCH]). Whenever valuable, Best
Current Practice (BCP) documents are referenced. In exceptional
cases, and if the document provides substantial guideline for
standard usage or fills an essential gap, Experimental and
Informational RFCs are noticed and ongoing work is mentioned.

Information on active and concluded IETF working groups (e.g., their
charters, published or currently active documents, and mail archives)
can be found at [IETF-WGS]).

Note that this document does not cover OAM technologies on the data-
path including MPLS forwarding plane and control plane protocols
(e.g., OAM of tunnels, MPLS-TP OAM, and pseudowire) as well as the
corresponding management models and MIB modules. For a list of
related work, see Section 1.2.

1.2. Related Work

"Internet Protocols for the Smart Grid" [RFC6272] gives an overview
and guidance on the key protocols of the Internet Protocol Suite. In
analogy to [RFC6272], this document gives an overview of the IETF
network management standards and their usage scenarios.

"Overview of the 2002 IAB Network Management Workshop" [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, even though some of the recommendations
from the 2002 IAB workshop have become outdated, some have been
standardized, and some are being worked on within the IETF.

"Guidelines for Considering Operations and Management of New
Protocols and Extensions" [RFC5706] recommends working groups
consider operations and management needs and then select appropriate
management protocols and data models. This document can be used to
ease surveying the IETF Standards Track network management protocols
and management data models.

"Multiprotocol Label Switching (MPLS) Management Overview" [RFC4221]
describes the management architecture for MPLS and indicates the
interrelationships between the different MIB modules used for MPLS

network management, where "Operations, Administration, and
Maintenance Framework for MPLS-Based Transport Networks" [RFC6371]
describes the OAM Framework for MPLS-based Transport Networks.

"An Overview of Operations, Administration, and Maintenance (OAM)
Mechanisms" [OAM-OVERVIEW] gives an overview of the OAM toolset for
detecting and reporting connection failures or measuring connection
performance parameters.

"An Overview of the OAM Tool Set for MPLS-based Transport Networks"
[OAM-ANALYSIS] provides an overview of the OAM toolset for MPLS-based
Transport Networks including a brief summary of MPLS-TP OAM
requirements and functions and of generic mechanisms created in the
MPLS data plane to allow the OAM packets run in-band and share their
fate with data packets. The protocol definitions for each MPLS-TP
OAM tool are listed in separate documents, which are referenced.

"MPLS-TP MIB-based Management Overview" [MPLSTP-MIB] describes the
MIB-based architecture for MPLS-TP, and indicates the
interrelationships between different existing MIB modules that can be
leveraged for MPLS-TP network management and identifies areas where
additional MIB modules are required.

Note that so far, the IETF has not developed specific technologies
for the management of sensor networks. IP-based sensors or
constrained devices in such an environment, i.e., with very limited
memory and CPU resources, can use, e.g., application-layer protocols
to do simple resource management and monitoring.

1.3. Terminology

This document does not describe standard requirements. Therefore,
key words from RFC 2119 [RFC2119] are not used in the document.

o 3GPP: 3rd Generation Partnership Project, a collaboration between
   groups of telecommunications associations, to prepare the third-
   generation (3G) mobile phone system specification.

o Agent: A software module that performs the network management
   functions requested by network management stations. An agent may
   be implemented in any network element that is to be managed, such
   as a host, bridge, or router. The 'management server' in NETCONF
   terminology.

o BCP: An IETF Best Current Practice document.

o CLI: Command Line Interface. A management interface that system
   administrators can use to interact with networking equipment.

o Data model: A mapping of the contents of an information model into
   a form that is specific to a particular type of datastore or
   repository (see [RFC3444]).

o Event: An occurrence of something in the "real world". Events can
   be indicated to managers through an event message or notification.

o IAB: Internet Architecture Board

o IANA: Internet Assigned Numbers Authority, an organization that
   oversees global IP address allocation, autonomous system number
   allocation, media types, and other IP-related code point
   allocations.

o Information model: An abstraction and representation of entities
   in a managed environment, their properties, attributes,
   operations, and the way they relate to each other, independent of
   any specific repository, protocol, or platform (see [RFC3444]).

o ITU-T: International Telecommunication Union - Telecommunication
   Standardization Sector

o Managed object: A management abstraction of a resource; a piece of
   management information in a MIB module. In the context of SNMP, a
   structured set of data variables that represent some resource to
   be managed or other aspect of a managed device.

o Manager: An entity that acts in a manager role, either a user or
   an application. The counterpart to an agent. A 'management
   client' in NETCONF terminology.

o Management Information Base (MIB): An information repository with
   a collection of related objects that represent the resources to be
   managed.

o MIB module: MIB modules usually contain object definitions, may
   contain definitions of event notifications, and sometimes include
   compliance statements in terms of appropriate object and event
   notification groups. A MIB that is provided by a management agent
   is typically composed of multiple instantiated MIB modules.

o Modeling language: A modeling language is any artificial language
   that can be used to express information or knowledge or systems in
   a structure that is defined by a consistent set of rules.
   Examples are Structure of Management Information Version 2 (SMIv2)
   [STD58], XML Schema Definition (XSD) [XSD-1], and YANG [RFC6020].

o Notification: An unsolicited message sent by an agent to a
   management station to notify it of an unusual event.

o OAM: Operations, Administration, and Maintenance

o PDU: Protocol Data Unit, a unit of data, which is specified in a
   protocol of a given layer consisting protocol-control information
   and possibly layer-specific data.

o Principal: An application, an individual, or a set of individuals
   acting in a particular role, on whose behalf access to a service
   or MIB is allowed.

o RELAX NG: REgular LAnguage for XML Next Generation, a schema
   language for XML [RELAX-NG].

o SDO: Standards Development Organization

o SMI: Structure of Managed Information, the notation and grammar
   for the managed information definition used to define MIB modules
   [STD58].

o STDnn: An Internet Standard published at IETF, also referred as
   Standard, e.g., [STD62].

o URI: Uniform Resource Identifier, a string of characters used to
   identify a name or a resource on the Internet [STD66]. Can be
   classified as locators (URLs), as names (URNs), or as both.

o XPATH: XML Path Language, a query language for selecting nodes
   from an XML document [XPATH].

2. Core Network Management Protocols

2.1. Simple Network Management Protocol (SNMP)

2.1.1. Architectural Principles of SNMP

The SNMPv3 Framework [RFC3410], builds upon both the original SNMPv1
and SNMPv2 Frameworks. The basic structure and components for the
SNMP Framework did not change between its versions and comprises the
following components:

o managed nodes, each with an SNMP entity providing remote access to
   management instrumentation (the agent),

o at least one SNMP entity with management applications (the
   manager), and

o a management protocol used to convey management information
   between the SNMP entities and management information.

During its evolution, the fundamental architecture of the SNMP
Management Framework remained consistent based on a modular
architecture, which consists of:

o a generic protocol definition independent of the data it is
   carrying,

o a protocol-independent data definition language,

o an information repository containing a data set of management
   information definitions (the Management Information Base, or MIB),
   and

o security and administration.

As such, the following standards build up the basis of the current
SNMP Management Framework:

o the SNMPv3 protocol [STD62],

o the modeling language SMIv2 [STD58], and

o the MIB modules for different management issues.

The SNMPv3 Framework extends the architectural principles of SNMPv1
and SNMPv2 by:

o building on these three basic architectural components, in some
   cases, incorporating them from the SNMPv2 Framework by reference,
   and

o by using the same layering principles in the definition of new
   capabilities in the security and administration portion of the
   architecture.

2.1.2. SNMP and Its Versions

   SNMP is based on three conceptual entities: Manager, Agent, and the
   Management Information Base (MIB). In any configuration, at least
   one manager node runs SNMP management software. Typically, network
   devices, such as bridges, routers, and servers, are equipped with an
   agent. The agent is responsible for providing access to a local MIB
   of objects that reflects the resources and activity at its node.

Following the manager-agent paradigm, an agent can generate
notifications and send them as unsolicited messages to the management
application.

SNMPv2 enhances this basic functionality with an Inform PDU, a bulk
transfer capability and other functional extensions like an
administrative model for access control, security extensions, and
Manager-to-Manager communication. SNMPv2 entities can have a dual
role as manager and agent. However, neither SNMPv1 nor SNMPv2 offers
sufficient security features. To address the security deficiencies
of SNMPv1/v2, SNMPv3 [STD62] has been issued.

"Coexistence between Version 1, Version 2, and Version 3 of the
Internet-standard Network Management Framework" [BCP074] gives an
overview of the relevant Standard documents on the three SNMP
versions. The BCP document furthermore describes how to convert MIB
modules from SMIv1 to SMIv2 format and how to translate notification
parameters. It also describes the mapping between the message
processing and security models.

SNMP utilizes the MIB, a virtual information store of modules of
managed objects. Generally, standard MIB modules support common
functionality in a device. Operators often define additional MIB
modules for their enterprise or use the Command Line Interface (CLI)
to configure non-standard data in managed devices and their
interfaces.

SNMPv2 Trap and Inform PDUs can alert an operator or an application
when some aspects of a protocol fail or encounter an error condition,
and the contents of a notification can be used to guide subsequent
SNMP polling to gather additional information about an event.

SNMP is widely used for the monitoring of fault and performance data
and with its stateless nature, SNMP also works well for status
polling and determining the operational state of specific
functionality. The widespread 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 basic parameter of
a device (e.g., sysUpTime, which reports the time since the last re-
initialization of the network management portion of the device) to
check for operational liveliness and to detect discontinuities in
counters. Some operators also use SNMP for configuration management
in their environment (e.g., for systems based on Data Over Cable
Service Interface Specification (DOCSIS) such as cable modems).

SNMPv1 [RFC1157] has been declared Historic and its use is not
recommended due to its lack of security features. "Introduction to
Community-based SNMPv2" [RFC1901] is an Experimental RFC, which has
been declared Historic, and its use is not recommended due to its
lack of security features.

Use of SNMPv3 [STD62] is recommended due to its security features,
including support for authentication, encryption, message timeliness
and integrity checking, and fine-grained data access controls. An
overview of the SNMPv3 document set is in [RFC3410].

Standards exist to use SNMP over diverse transport and link-layer
protocols, including Transmission Control Protocol (TCP) [STD07],
User Datagram Protocol (UDP) [STD06], Ethernet [RFC4789], and others
(see Section 2.1.5.1).

2.1.3. Structure of Managed Information (SMI)

   SNMP MIB modules are defined with the notation and grammar specified
   as the Structure of Managed Information (SMI). The SMI uses an
   adapted subset of Abstract Syntax Notation One (ASN.1) [ITU-X680].

   The SMI is divided into three parts: module definitions, object
   definitions, and notification definitions.

   o Module definitions are used when describing information modules.
      An ASN.1 macro, MODULE-IDENTITY, is used to concisely convey the
      semantics of an information module.

   o Object definitions are used when describing managed objects. An
      ASN.1 macro, OBJECT-TYPE, is used to concisely convey the syntax
      and semantics of a managed object.

   o Notification definitions are used when describing unsolicited
      transmissions of management information. An ASN.1 macro,
      NOTIFICATION-TYPE, is used to concisely convey the syntax and
      semantics of a notification.

   SMIv1 is specified in "Structure and Identification of Management
   Information for TCP/IP-based Internets" [RFC1155] and "Concise MIB
   Definitions" [RFC1212], both part of [STD16]. [RFC1215] specifies
   conventions for defining SNMP traps. Note that SMIv1 is outdated and
   its use is not recommended.

   SMIv2 is the new notation for managed information definitions and
   should be used to define MIB modules. SMIv2 is specified in the
   following RFCs. With the exception of BCP 74, they are all part of
   [STD58]:

   o [RFC2578] defines Version 2 of the Structure of Management
      Information (SMIv2),

   o [RFC2579] defines the textual conventions macro for defining new
      types and it provides a core set of generally useful textual
      convention definitions,

   o [RFC2580] defines conformance statements and requirements for
      defining agent and manager capabilities, and

   o [BCP074] defines the mapping rules for and the conversion of MIB
      modules between SMIv1 and SMIv2 formats.

2.1.4. SNMP Security and Access Control Models

2.1.4.1. Security Requirements on the SNMP Management Framework

   Several of the classical threats to network protocols are applicable
   to management problem space and therefore are applicable to any
   security model used in an SNMP Management Framework. This section
   lists primary and secondary threats, and threats that are of lesser
   importance (see [RFC3411] for the detailed description of the
   security threats).

   The primary threats against which SNMP Security Models can provide
   protection are, "modification of information" by an unauthorized
   entity, and "masquerade", i.e., the danger that management operations
   not authorized for some principal may be attempted by assuming the
   identity of another principal.

   Secondary threats against which SNMP Security Models can provide
   protection are "message stream modification", e.g., reordering,
   delay, or replay of messages, and "disclosure", i.e., the danger of
   eavesdropping on the exchanges between SNMP engines.

   There are two threats against which the SNMP Security Model does not
   protect, since they are deemed to be of lesser importance in this
   context: Denial of Service and Traffic Analysis (see [RFC3411]).

2.1.4.2. User-Based Security Model (USM)

   SNMPv3 [STD62] introduced the User-based Security Model (USM). USM
   is specified in [RFC3414] and provides authentication and privacy
   services for SNMP. Specifically, USM is designed to secure against
   the primary and secondary threats discussed in Section 2.1.4.1. USM
   does not secure against Denial of Service and attacks based on
   Traffic Analysis.

The USM supports following security services:

o Data integrity is the provision of the property that data has not
   been altered or destroyed in an unauthorized manner, nor have data
   sequences been altered to an extent greater than can occur non-
   maliciously.

o Data origin authentication is the provision of the property that
   the claimed identity of the user on whose behalf received data was
   originated is supported.

o Data confidentiality is the provision of the property that
   information is not made available or disclosed to unauthorized
   individuals, entities, or processes.

o Message timeliness and limited replay protection is the provision
   of the property that a message whose generation time is outside of
   a specified time window is not accepted.

   See [RFC3414] for a detailed description of SNMPv3 USM.

2.1.4.3. View-Based Access Control Model (VACM)

   SNMPv3 [STD62] introduced the View-based Access Control (VACM)
   facility. The VACM is defined in [RFC3415] and enables the
   configuration of agents to provide different levels of access to the
   agent's MIB. An agent entity can restrict access to a certain
   portion of its MIB, e.g., restrict some principals to view only
   performance-related statistics or disallow other principals to read
   those performance-related statistics. An agent entity can also
   restrict the access to monitoring (read-only) as opposed to
   monitoring and configuration (read-write) of a certain portion of its
   MIB, e.g., allowing only a single designated principal to update
   configuration parameters.

   VACM defines five elements that make up the Access Control Model:
   groups, security level, contexts, MIB views, and access policy.
   Access to a MIB module is controlled by means of a MIB view.

   See [RFC3415] for a detailed description of SNMPv3 VACM.

2.1.5. SNMP Transport Subsystem and Transport Models

   The User-based Security Model (USM) was designed to be independent of
   other existing security infrastructures to ensure it could function
   when third-party authentication services were not available. As a
   result, USM utilizes a separate user and key-management

infrastructure. Operators have reported that the deployment of a
separate user and key-management infrastructure in order to use
SNMPv3 is costly and hinders the deployment of SNMPv3.

SNMP Transport Subsystem [RFC5590] extends the original SNMP
architecture and Transport Model and enables the use of transport
protocols to provide message security unifying the administrative
security management for SNMP and other management interfaces.

Transport Models are tied into the SNMP Framework through the
Transport Subsystem. The Transport Security Model [RFC5591] has been
designed to work on top of lower-layer, secure Transport Models.

The SNMP Transport Model defines an alternative to existing standard
transport mappings described in [RFC3417], e.g., for SNMP over UDP,
in [RFC4789] for SNMP over IEEE 802 networks, and in the Experimental
RFC [RFC3430] defining SNMP over TCP.

2.1.5.1. SNMP Transport Security Model

The SNMP Transport Security Model [RFC5591] is an alternative to the
existing SNMPv1 and SNMPv2 Community-based Security Models [BCP074],
and the User-based Security Model [RFC3414], part of [STD62].

The Transport Security Model utilizes one or more lower-layer
security mechanisms to provide message-oriented security services.
These include authentication of the sender, encryption, timeliness
checking, and data integrity checking.

A secure Transport Model sets up an authenticated and possibly
encrypted session between the Transport Models of two SNMP engines.
After a transport-layer session is established, SNMP messages can be
sent through this session from one SNMP engine to the other. The new
Transport Model supports the sending of multiple SNMP messages
through the same session to amortize the costs of establishing a
security association.

The Secure Shell (SSH) Transport Model [RFC5592] and the Transport
Layer Security (TLS) Transport Model [RFC6353] are current examples
of Transport Security Models.

The SSH Transport Model makes use of the commonly deployed SSH
security and key-management infrastructure. Furthermore, [RFC5592]
defines MIB objects for monitoring and managing the SSH Transport
Model for SNMP.

The Transport Layer Security (TLS) Transport Model [RFC6353] uses
either the TLS protocol [RFC5246] or the Datagram Transport Layer
Security (DTLS) protocol [RFC6347]. The TLS and DTLS protocols
provide authentication and privacy services for SNMP applications.
The TLS Transport Model supports the sending of SNMP messages over
TLS and TCP and over DTLS and UDP. Furthermore, [RFC6353] defines
MIB objects for managing the TLS Transport Model for SNMP.

[RFC5608] describes the use of a Remote Authentication Dial-In User
Service (RADIUS) service by SNMP secure Transport Models for
authentication of users and authorization of services. Access
control authorization, i.e., how RADIUS attributes and messages are
applied to the specific application area of SNMP Access Control
Models, and VACM in particular has been specified in [RFC6065].

2.2. Syslog Protocol

Syslog is a mechanism for distribution of logging information
initially used on Unix systems (see [RFC3164] for BSD syslog). The
IETF Syslog Protocol [RFC5424] introduces a layered architecture
allowing the use of any number of transport protocols, including
reliable and secure transports, for transmission of syslog messages.

The Syslog protocol enables a machine to send system log messages
across networks to event message collectors. The protocol is simply
designed to transport and distribute these event messages. By
default, no acknowledgements of the receipt are made, except the
reliable delivery extensions specified in [RFC3195] are used. The
Syslog protocol and process does not require a stringent coordination
between the transport sender and the receiver. 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.

BSD syslog had little uniformity for the message format and the
content of syslog messages. The body of a BSD syslog message has
traditionally been unstructured text. This content is human
friendly, but difficult to parse for applications. With the Syslog
Protocol [RFC5424], 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.

The Syslog protocol [RFC5424] also introduces a mechanism for
defining Structured Data Elements (SDEs). The SDEs allow vendors to
define their own structured data elements to supplement standardized
elements. [RFC5675] defines a mapping from SNMP notifications to

syslog messages. [RFC5676] defines an SNMP MIB module to represent
syslog messages for the purpose of sending those syslog messages as
notifications to SNMP notification receivers. [RFC5674] defines the
way alarms are sent in syslog, which includes the mapping of ITU-
perceived severities onto syslog message fields and a number of
alarm-specific definitions from ITU-T X.733 [ITU-X733] and the IETF
Alarm MIB [RFC3877].

"Signed Syslog Messages" [RFC5848] defines a mechanism to add origin
authentication, message integrity, replay resistance, message
sequencing, and detection of missing messages to the transmitted
syslog messages to be used in conjunction with the Syslog protocol.

The Syslog protocol's layered architecture provides support for a
number of transport mappings. For interoperability purposes and
especially in managed networks, where the network path has been
explicitly provisioned for UDP syslog traffic, the Syslog protocol
can be used over UDP [RFC5426]. However, to support congestion
control and reliability, [RFC5426] strongly recommends the use of the
TLS transport.

Furthermore, the IETF defined the TLS Transport Mapping for syslog in
[RFC5425], which provides a secure connection for the transport of
syslog messages. [RFC5425] describes the security threats to syslog
and how TLS can be used to counter such threats. [RFC6012] defines
the Datagram Transport Layer Security (DTLS) Transport Mapping for
syslog, which can be used if a connectionless transport is desired.

For information on MIB modules related to syslog, see Section 4.2.1.

2.3. IP Flow Information eXport (IPFIX) and Packet SAMPling (PSAMP)
      Protocols

"Specification of the IP Flow Information Export (IPFIX) Protocol for
the Exchange of IP Traffic Flow Information" (the IPFIX Protocol)
[RFC5101] defines a push-based data export mechanism for transferring
IP flow information in a compact binary format from an Exporter to a
Collector.

"Architecture for IP Flow Information Export" (the IPFIX
Architecture) [RFC5470] defines the components involved in IP flow
measurement and reporting of information on IP flows, particularly, a
Metering Process generating Flow Records, an Exporting Process that
sends metered flow information using the IPFIX protocol, and a
Collecting Process that receives flow information as IPFIX Data
Records.

After listing the IPFIX requirements in [RFC3917], NetFlow Version 9
[RFC3954] was taken as the basis for the IPFIX protocol and the IPFIX
architecture.

IPFIX can run over different transport protocols. The IPFIX Protocol
[RFC5101] specifies Stream Control Transmission Protocol (SCTP)
[RFC4960] as the mandatory transport protocol to implement. Optional
alternatives are TCP [STD07] and UDP [STD06].

SCTP is used with its Partial Reliability extension (PR-SCTP)
specified in [RFC3758]. [RFC6526] specifies an extension to
[RFC5101], when using the PR-SCTP [RFC3758]. The extension offers
several advantages over IPFIX export, e.g., the ability to calculate
Data Record losses for PR-SCTP, immediate reuse of Template IDs
within an SCTP stream, reduced likelihood of Data Record loss, and
reduced demands on the Collecting Process.

IPFIX transmits IP flow information in Data Records containing IPFIX
Information Elements (IEs) defined by the IPFIX Information Model
[RFC5102]. IPFIX IEs are quantities with unit and semantics defined
by the Information Model. When transmitted over the IPFIX protocol,
only their values need to be carried in Data Records. This compact
encoding allows efficient transport of large numbers of measured flow
values. Remaining redundancy in Data Records can be further reduced
by the methods described in [RFC5473] (for further discussion on
IPFIX IEs, see Section 4).

The IPFIX Information Model is extensible. New IEs can be registered
at IANA (see "IPFIX Information Elements" in [IANA-PROT]). IPFIX
also supports the use of proprietary, i.e., enterprise-specific IEs.

The PSAMP protocol [RFC5476] extends the IPFIX protocol by means of
transferring information on individual packets. [RFC5475] specifies
a set of sampling and filtering techniques for IP packet selection,
based on the PSAMP Framework [RFC5474]. The PSAMP Information Model
[RFC5477] provides a set of basic IEs for reporting packet
information with the IPFIX/PSAMP protocol.

The IPFIX model of an IP traffic flow is unidirectional. [RFC5103]
adds means of reporting bidirectional flows to IPFIX, for example,
both directions of packet flows of a TCP connection.

When enterprise-specific IEs are transmitted with IPFIX, a Collector
receiving Data Records may not know the type of received data and
cannot choose the right format for storing the contained information.
[RFC5610] provides a means of exporting extended type information for
enterprise-specific Information Elements from an Exporter to a
Collector.

Collectors may store received flow information in files. The IPFIX
file format [RFC5655] can be used for storing IP flow information in
a way that facilitates exchange of traffic flow information between
different systems and applications.

In terms of IPFIX and PSAMP configurations, the Metering and
Exporting Processes are configured out of band. As the IPFIX
protocol is a push mechanism only, IPFIX cannot configure the
Exporter. The actual configuration of selection processes, caches,
Exporting Processes, and Collecting Processes of IPFIX- and PSAMP-
compliant monitoring devices is executed using the NETCONF protocol
[RFC6241] (see Section 2.4.1). The "Configuration Data Model for
IPFIX and PSAMP" (the IPFIX Configuration Data Model) [CONF-MODEL]
has been specified using Unified Modeling Language (UML) class
diagrams. The data model is formally defined using the YANG modeling
language [RFC6020] (see Section 2.4.2).

At the time of this writing, a framework for IPFIX flow mediation is
in preparation, which addresses the need for mediation of flow
information in IPFIX applications in large operator networks, e.g.,
for aggregating huge amounts of flow data and for anonymization of
flow information (see the problem statement in [RFC5982]).

The IPFIX Mediation Framework [RFC6183] defines the intermediate
device between Exporters and Collectors, which provides an IPFIX
mediation by receiving a record stream from, e.g., a Collecting
Process, hosting one or more Intermediate Processes to transform this
stream, and exporting the transformed record stream into IPFIX
messages via an Exporting Process.

Examples for mediation functions are flow aggregation, flow
selection, and anonymization of traffic information (see [RFC6235]).

Privacy, integrity, and authentication of the Exporter and Collector
are important security requirements for IPFIX [RFC3917].
Confidentiality, integrity, and authenticity of IPFIX data
transferred from an Exporting Process to a Collecting Process must be
ensured. The IPFIX and PSAMP protocols do not define any new
security mechanisms and rely on the security mechanism of the
underlying transport protocol, such as TLS [RFC5246] and DTLS
[RFC6347].

The primary goal of IPFIX is the reporting of the flow accounting for
flexible flow definitions and usage-based accounting. As described
in the IPFIX Applicability Statement [RFC5472], there are also other
applications such as traffic profiling, traffic engineering,
intrusion detection, and QoS monitoring, that require flow-based
traffic measurements and can be realized using IPFIX. Furthermore,

the IPFIX Applicability Statement explains the relation of IPFIX to
other framework and protocols such as PSAMP, RMON (Remote Network
Monitoring MIB, [Section 4.2.1](#)), and IPPM (IP Performance Metrics,
[Section 3.4](#))). Similar flow information could be also used for
security monitoring. The addition of Performance Metrics in the
IPFIX IANA registry [[IANA-IPFIX](#)], will extend the IPFIX use case to
performance management.

Note that even if the initial IPFIX focus has been around IP flow
information exchange, non-IP-related IEs are now specified in the
IPFIX IANA registration (e.g., MAC (Media Access Control) address,
MPLS (Multiprotocol Label Switching) labels, etc.). At the time of
this writing, there are requests to widen the focus of IPFIX and to
export non-IP related IEs (such as SIP monitoring IEs).

The IPFIX structured data [[RFC6313](#)] is an extension to the IPFIX
protocol, which supports hierarchical structured data and lists
(sequences) of Information Elements in Data Records. This extension
allows the definition of complex data structures such as variable-
length lists and specification of hierarchical containment
relationships between templates. Furthermore, the extension provides
the semantics to express the relationship among multiple list
elements in a structured Data Record.

For information on data models related to the management of the IPFIX
and PSAMP protocols, see Sections [4.2.1](#) and [4.2.2](#). For information
on IPFIX/PSAMP IEs, see [Section 4.2.3](#).

[2.4](#). Network Configuration

[2.4.1](#). Network Configuration Protocol (NETCONF)

The IAB workshop on Network Management [[RFC3535](#)] determined advanced
requirements for configuration management:

o robustness: Minimizing disruptions and maximizing stability,

o a task-oriented view,

o extensibility for new operations,

o standardized error handling,

o clear distinction between configuration data and operational
   state,

o distribution of configurations to devices under transactional
   constraints,

o single- and multi-system transactions and scalability in the
   number of transactions and managed devices,

o operations on selected subsets of management data,

o dumping and reloading a device configuration in a textual format
   in a standard manner across multiple vendors and device types,

o a human interface and a programmatic interface,

o a data modeling language with a human-friendly syntax,

o easy conflict detection and configuration validation, and

o secure transport, authentication, and robust access control.

The NETCONF protocol [RFC6241] provides mechanisms to install,
manipulate, and delete the configuration of network devices and aims
to address the configuration management requirements pointed out in
the IAB workshop. It uses an 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 and reliable
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.

The NETCONF working group developed the NETCONF Event Notifications
Mechanism as an optional capability, which provides an asynchronous
message notification delivery service for NETCONF [RFC5277]. The
NETCONF notification mechanism enables using general purpose
notification streams, where the originator of the notification stream
can be any managed device (e.g., SNMP notifications).

The NETCONF Partial Locking specification introduces fine-grained
locking of the configuration datastore to enhance NETCONF for fine-
grained transactions on parts of the datastore [RFC5717].

The NETCONF working group also defined the necessary data model to
monitor the NETCONF protocol [RFC6022], by using the modeling
language YANG [RFC6020] (see Section 2.4.2). The monitoring data
model includes information about NETCONF datastores, sessions, locks,
and statistics, which facilitate the management of a NETCONF server.

NETCONF connections are required to provide authentication, data
integrity, confidentiality, and replay protection. NETCONF depends
on the underlying transport protocol for this capability. For
example, connections can be encrypted in TLS or SSH, depending on the
underlying protocol.

   The NETCONF working group defined the SSH transport protocol as the
   mandatory transport binding [RFC6242]. Other optional transport
   bindings are TLS [RFC5539], Blocks Extensible Exchange Protocol
   (BEEP) over TLS [RFC4744], and Simple Object Access Protocol (SOAP)
   over HTTP over TLS [RFC4743].

   The NETCONF Access Control Model (NACM) [RFC6536] provides standard
   mechanisms to restrict protocol access to particular users with a
   pre-configured subset of operations and content.

2.4.2. YANG - NETCONF Data Modeling Language

   Following the guidelines of the IAB management workshop [RFC3535],
   the NETMOD working group developed a data modeling language defining
   the semantics of operational and configuration data, notifications,
   and operations [RFC6020]. The new data modeling language, called
   YANG, maps directly to XML-encoded content (on the wire) and will
   serve as the normative description of NETCONF data models.

   YANG has the following properties addressing specific requirements on
   a modeling language for configuration management:

   o YANG provides the means to define hierarchical data models. It
      supports reusable data types and groupings, i.e., a set of schema
      nodes that can be reused across module boundaries.

   o YANG supports the distinction between configuration and state
      data. In addition, it provides support for modeling event
      notifications and the specification of operations that extend the
      base NETCONF operations.

   o YANG allows the expression of constraints on data models by means
      of type restrictions and XML Path Language (XPATH) 1.0 [XPATH]
      expressions. XPATH expressions can also be used to make certain
      portions of a data model conditional.

   o YANG supports the integration of standard- and vendor-defined data
      models. YANG's augmentation mechanism allows the seamless
      augmentation of standard data models with proprietary extensions.

   o YANG data models can be partitioned into collections of features,
      allowing low-end devices only to implement the core features of a
      data model while high-end devices may choose to support all
      features. The supported features are announced via the NETCONF
      capability exchange to management applications.

o The syntax of the YANG language is compact and optimized for human
   readers. An associated XML-based syntax called the YANG
   Independent Notation (YIN) [RFC6020] is available to allow the
   processing of YANG data models with XML-based tools. The mapping
   rules for the translation of YANG data models into Document Schema
   Definition Languages (DSDL), of which RELAX NG is a major
   component, are defined in [RFC6110].

o Devices implementing standard data models can document deviations
   from the data model in separate YANG modules. Applications
   capable of discovering deviations can make allowances that would
   otherwise not be possible.

A collection of common data types for IETF-related standards is
provided in [RFC6021]. This standard data type library has been
derived to a large extend from common SMIv2 data types, generalizing
them to a less-constrained NETCONF Framework.

The document "An Architecture for Network Management using NETCONF
and YANG" describes how NETCONF and YANG can be used to build network
management applications that meet the needs of network operators
[RFC6244].

The Experimental RFC [RFC6095] specifies extensions for YANG,
introducing language abstractions such as class inheritance and
recursive data structures.

[RFC6087] gives guidelines for the use of YANG within the IETF and
other standardization organizations.

Work is underway to standardize a translation of SMIv2 data models
into YANG data models preserving investments into SNMP MIB modules,
which are widely available for monitoring purposes [SMI-YANG].

Several independent and open source implementations of the YANG data
modeling language and associated tools are available.

While YANG is a relatively recent data modeling language, some data
models have already been produced. The specification of the base
NETCONF protocol operations has been revised and uses YANG as the
normative modeling language to specify its operations [RFC6241]. The
IPFIX working group prepared the normative model for configuring and
monitoring IPFIX- and PSAMP-compliant monitoring devices using the
YANG modeling language [CONF-MODEL].

   At the time of this writing, the NETMOD working group is developing
   core system and interface data models. Following the example of the
   IPFIX configuration model, IETF working groups will prepare models
   for their specific needs.

   For information on data models developed using the YANG modeling
   language, see Sections 4.2.1 and 4.2.2.

3. Network Management Protocols and Mechanisms with Specific Focus

   This section reviews additional protocols the IETF offers for
   management and discusses for which applications they were designed
   and/or have already been successfully deployed. These are protocols
   that have mostly reached Proposed Standard status or higher within
   the IETF.

3.1. IP Address Management

3.1.1. Dynamic Host Configuration Protocol (DHCP)

   Dynamic Host Configuration Protocol (DHCP) [RFC2131] provides a
   framework for passing configuration information to hosts on a TCP/IP
   network and, as such, enables autoconfiguration in IP networks. In
   addition to IP address management, DHCP can also provide other
   configuration information, such as default routers, the IP addresses
   of recursive DNS servers, and the IP addresses of NTP servers. As
   described in [RFC6272], DHCP can be used for IPv4 and IPv6 Address
   Allocation and Assignment as well as for Service Discovery.

   There are two versions of DHCP: one for IPv4 (DHCPv4) [RFC2131] and
   one for IPv6 (DHCPv6) [RFC3315]. DHCPv4 was defined as an extension
   to BOOTP (Bootstrap Protocol) [RFC0951]. DHCPv6 was subsequently
   defined to accommodate new functions required by IPv6 such as
   assignment of multiple addresses to an interface and to address
   limitations in the design of DHCPv4 resulting from its origins in
   BOOTP. While both versions bear the same name and perform the same
   functionality, the details of DHCPv4 and DHCPv6 are sufficiently
   different that they can be considered separate protocols.

   In addition to the assignment of IP addresses and other configuration
   information, DHCP options like the Relay Agent Information option
   (DHCPv4) [RFC3046] and, the Interface-Id Option (DHCPv6) [RFC3315]
   are widely used by ISPs.

   DHCPv6 includes Prefix Delegation [RFC3633], which is used to
   provision a router with an IPv6 prefix for use in the subnetwork
   supported by the router.

   The following are examples of DHCP options that provide configuration
   information or access to specific servers. A complete list of DHCP
   options is available at [IANA-PROT].

   o "DNS Configuration options for Dynamic Host Configuration Protocol
      for IPV6 (DHCPv6)" [RFC3646] describes DHCPv6 options for passing
      a list of available DNS recursive name servers and a domain search
      list to a client.

   o "DHCP Options for Service Location Protocol" [RFC2610] describes
      DHCPv4 options and methods through which entities using the
      Service Location Protocol can find out the address of Directory
      Agents in order to transact messages and how the assignment of
      scope for configuration of Service Location Protocol (SLP) User
      and Service Agents can be achieved.

   o "Dynamic Host Configuration Protocol (DHCPv6) Options for Session
      Initiation Protocol (SIP) Servers" [RFC3319] specifies DHCPv6
      options that allow SIP clients to locate a local SIP server that
      is to be used for all outbound SIP requests, a so-called "outbound
      proxy server".

   o "Dynamic Host Configuration Protocol (DHCP) Options for Broadcast
      and Multicast Control Servers" [RFC4280] defines DHCPv6 options to
      discover the Broadcast and Multicast Service (BCMCS) controller in
      an IP network.

   Built directly on UDP and IP, DHCP itself has no security provisions.
   There are two different classes of potential security issues related
   to DHCP: unauthorized DHCP Servers and unauthorized DHCP Clients.
   The recommended solutions to these risks generally involve providing
   security at lower layers, e.g., careful control over physical access
   to the network, security techniques implemented at Layer 2 but also
   IPsec at Layer 3 can be used to provide authentication.

3.1.2. Ad Hoc Network Autoconfiguration

   Ad hoc nodes need to configure their network interfaces with locally
   unique addresses as well as globally routable IPv6 addresses, in
   order to communicate with devices on the Internet. The IETF AUTOCONF
   working group developed [RFC5889], which describes the addressing
   model for ad hoc networks and how nodes in these networks configure
   their addresses.

   The ad hoc nodes under consideration are expected to be able to
   support multi-hop communication by running MANET (Mobile Ad Hoc
   Network) routing protocols as developed by the IETF MANET working
   group.

From the IP layer perspective, an ad hoc network presents itself as a
Layer 3 multi-hop network formed over a collection of links. The
addressing model aims to avoid problems for parts of the system that
are ad hoc unaware, such as standard applications running on an ad
hoc node or regular Internet nodes attached to the ad hoc nodes.

3.2. IPv6 Network Operations

The IPv6 Operations (V6OPS) working group develops guidelines for the
operation of a shared IPv4/IPv6 Internet and provides operational
guidance on how to deploy IPv6 into existing IPv4-only networks, as
well as into new network installations.

o "Basic Transition Mechanisms for IPv6 Hosts and Routers" [RFC4213]
   specifies IPv4 compatibility mechanisms for dual-stack and
   configured tunneling that can be implemented by IPv6 hosts and
   routers. "Dual stack" implies providing complete implementations
   of both IPv4 and IPv6, and configured tunneling provides a means
   to carry IPv6 packets over unmodified IPv4 routing
   infrastructures.

o "Transition Scenarios for 3GPP Networks" [RFC3574] lists different
   scenarios in 3GPP defined packet network that would need IPv6 and
   IPv4 transition, where "Analysis on IPv6 Transition in Third
   Generation Partnership Project (3GPP) Networks" [RFC4215] does a
   more detailed analysis of the transition scenarios that may come
   up in the deployment phase of IPv6 in 3GPP packet networks.

o "Scenarios and Analysis for Introducing IPv6 into ISP Networks"
   [RFC4029] describes and analyzes different scenarios for the
   introduction of IPv6 into an ISP's existing IPv4 network. "IPv6
   Deployment Scenarios in 802.16 Networks" [RFC5181] provides a
   detailed description of IPv6 deployment, integration methods, and
   scenarios in wireless broadband access networks (802.16) in
   coexistence with deployed IPv4 services. [RFC4057] describes the
   scenarios for IPv6 deployment within enterprise networks.

o "Application Aspects of IPv6 Transition" [RFC4038] specifies
   scenarios and application aspects of IPv6 transition considering
   how to enable IPv6 support in applications running on IPv6 hosts,
   and giving guidance for the development of IP-version-independent
   applications.

o "IANA-Reserved IPv4 Prefix for Shared Address Space" [RFC6598]
   updates RFC 5735 and requested the allocation of an IPv4/10
   address block to be used as "Shared Carrier-Grade Network Address

      Translation (CGN) Space" by Service Providers to number the
      interfaces that connect CGN devices to Customer Premises Equipment
      (CPE).

3.3. Policy-Based Management

3.3.1. IETF Policy Framework

   The IETF specified a general policy framework [RFC2753] for managing,
   sharing, and reusing policies in a vendor-independent, interoperable,
   and scalable manner. [RFC3460] specifies the Policy Core Information
   Model (PCIM) as an object-oriented information model for representing
   policy information. PCIM has been developed jointly in the IETF
   Policy Framework (POLICY) working group and the Common Information
   Model (CIM) activity in the Distributed Management Task Force (DMTF).
   PCIM has been published as extensions to CIM [DMTF-CIM].

   The IETF Policy Framework is based on a policy-based admission
   control specifying two main architectural elements: the Policy
   Enforcement Point (PEP) and the Policy Decision Point (PDP). For the
   purpose of network management, policies allow an operator to specify
   how the network is to be configured and monitored by using a
   descriptive language. Furthermore, it allows the automation of a
   number of management tasks, according to the requirements set out in
   the policy module.

   The IETF Policy Framework has been accepted by the industry as a
   standard-based policy management approach and has been adopted by
   different SDOs, e.g., for 3GGP charging standards.

3.3.2. Use of Common Open Policy Service (COPS) for Policy Provisioning
        (COPS-PR)

   [RFC3159] defines the Structure of Policy Provisioning Information
   (SPPI), an extension to the SMIv2 modeling language used to write
   Policy Information Base (PIB) modules. COPS-PR [RFC3084] uses the
   Common Open Policy Service (COPS) protocol [RFC2748] for the
   provisioning of policy information. COPS provides a simple client/
   server model for supporting policy control over QoS signaling
   protocols. 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). Policy data is modeled using PIB modules.

   COPS-PR has not been widely deployed, and operators have stated that
   its use of binary encoding for management data makes it difficult to
   develop automated scripts for simple configuration management tasks

   in most text-based scripting languages. In the IAB Workshop on
   Network Management [RFC3535], the consensus of operators and protocol
   developers indicated a lack of interest in PIB modules for use with
   COPS-PR.

   As a result, even if COPS-PR and the Structure of Policy Provisioning
   Information (SPPI) were initially approved as Proposed Standards, the
   IESG has not approved any PIB modules as Proposed Standard, and the
   use of COPS-PR is not recommended.

3.4. IP Performance Metrics (IPPM)

   The IPPM working group has defined metrics for accurately measuring
   and reporting the quality, performance, and reliability of Internet
   data delivery. 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.

   These metrics are designed for use by network operators and their
   customers, and they provide unbiased quantitative measures of
   performance. The IPPM metrics have been developed inside an active
   measurement context, that is, the devices used to measure the metrics
   produce their own traffic. However, most of the metrics can be used
   inside a passive context as well. At the time of this writing, there
   is no work planned in the area of passive measurement.

   As a property, individual IPPM performance and reliability metrics
   need to be well defined and concrete: thus, implementable.
   Furthermore, the methodology used to implement a metric needs to be
   repeatable with consistent measurements.

   IPPMs have been adopted by different organizations, e.g., the Metro
   Ethernet Forum.

   Note that this document does not aim to cover OAM technologies on the
   data-path and, as such, the discussion of IPPM-based active versus
   passive monitoring as well as the data plane measurement and its
   diagnostics is rather incomplete. For a detailed overview and
   discussion of IETF OAM standards and IPPM measurement mechanisms, the
   reader is referred to the documents listed at the end of Section 1.2
   ("Related Work") but especially to [OAM-OVERVIEW].

The following are essential IPPM documents:

o "Framework for IP Performance Metrics" [RFC2330] defines a general
   framework for particular metrics developed by the IPPM working
   group, and it defines the fundamental concepts of 'metric' and
   'measurement methodology'. It also discusses the issue of
   measurement uncertainties and errors as well as introduces the
   notion of empirically defined metrics and how metrics can be
   composed.

o "A One-way Delay Metric for IPPM" [RFC2679] defines a metric for
   the one-way delay of packets across Internet paths. It builds on
   notions introduced in the IPPM Framework document.

o "A Round-trip Delay Metric for IPPM" [RFC2681] defines a metric
   for the round-trip delay of packets across network paths and
   closely follows the corresponding metric for one-way delay.

o "IP Packet Delay Variation Metric for IP Performance Metrics
   (IPPM)" [RFC3393] refers to a metric for variation in the delay of
   packets across network paths and is based on the difference in the
   one-way-delay of selected packets called "IP Packet Delay
   Variation (ipdv)".

o "A One-way Packet Loss Metric for IPPM" [RFC2680] defines a metric
   for one-way packet loss across Internet paths.

o "A One-Way Packet Duplication Metric" [RFC5560] defines a metric
   for the case where multiple copies of a packet are received, and
   it discusses methods to summarize the results of streams.

o "Packet Reordering Metrics" [RFC4737] defines metrics to evaluate
   whether a network has maintained packet order on a packet-by-
   packet basis and discusses the measurement issues, including the
   context information required for all metrics.

o "IPPM Metrics for Measuring Connectivity" [RFC2678] defines a
   series of metrics for connectivity between a pair of Internet
   hosts.

o "Framework for Metric Composition" [RFC5835] describes a detailed
   framework for composing and aggregating metrics.

o "Guidelines for Considering New Performance Metric Development"
   [BCP170] describes the framework and process for developing
   Performance Metrics of protocols and applications transported over
   IETF-specified protocols.

To measure these metrics, two protocols and a sampling method have
been standardized:

o "A One-way Active Measurement Protocol (OWAMP)" [RFC4656] measures
   unidirectional characteristics such as one-way delay and one-way
   loss between network devices and enables the interoperability of
   these measurements. OWAMP is discussed in more detail in
   [OAM-OVERVIEW].

o "A Two-Way Active Measurement Protocol (TWAMP)" [RFC5357] adds
   round-trip or two-way measurement capabilities to OWAMP. TWAMP is
   discussed in more detail in [OAM-OVERVIEW].

o "Network performance measurement with periodic streams" [RFC3432]
   describes a periodic sampling method and relevant metrics for
   assessing the performance of IP networks, as an alternative to the
   Poisson sampling method described in [RFC2330].

For information on MIB modules related to IP Performance Metrics see
Section 4.2.4.

3.5. Remote Authentication Dial-In User Service (RADIUS)

"Remote Authentication Dial In User Service (RADIUS)" [RFC2865]
describes a client/server protocol for carrying authentication,
authorization, and configuration information between a Network Access
Server (NAS), which desires to authenticate its links, and a shared
authentication server. The companion document "Radius Accounting"
[RFC2866] describes a protocol for carrying accounting information
between a NAS and a shared accounting server. [RFC2867] adds
required new RADIUS accounting attributes and new values designed to
support the provision of tunneling in dial-up networks.

The RADIUS protocol is widely used in environments like enterprise
networks, where a single administrative authority manages the network
and protects the privacy of user information. RADIUS is deployed in
the networks of fixed broadband access provider as well as cellular
broadband operators.

RADIUS uses attributes to carry the specific authentication,
authorization, information, and configuration details. RADIUS is
extensible with a known limitation of a maximum of 255 attribute
codes and 253 octets as attribute content length. RADIUS has Vendor-
Specific Attributes (VSAs), which have been used both for vendor-
specific purposes (as an addition to standardized attributes) as well
as to extend the limited attribute code space.

The RADIUS protocol uses a shared secret along with the MD5 hash
algorithm to secure passwords [RFC1321]. Based on the known threads,
additional protection like IPsec tunnels [RFC4301] are used to
further protect the RADIUS traffic. However, building and
administering large IPsec-protected networks may become a management
burden, especially when the IPsec-protected RADIUS infrastructure
should provide inter-provider connectivity. Moving towards TLS-based
security solutions [RFC5246] and establishing dynamic trust
relationships between RADIUS servers has become a trend. Since the
introduction of TCP transport for RADIUS [RFC6613], it became natural
to have TLS support for RADIUS. An ongoing work is "Transport Layer
Security (TLS) encryption for RADIUS" [RFC6614].

"RADIUS Attributes for Tunnel Protocol Support" [RFC2868] defines a
number of RADIUS attributes designed to support the compulsory
provision of tunneling in dial-up network access. Some applications
involve compulsory tunneling, i.e., the tunnel is created without any
action from the user and without allowing the user any choice in the
matter. In order to provide this functionality, specific RADIUS
attributes are needed to carry the tunneling information from the
RADIUS server to the tunnel end points. "Signalling Connection
Control Part User Adaptation Layer (SUA)" [RFC3868] defines the
necessary attributes, attribute values, and the required IANA
registries.

"RADIUS and IPv6" [RFC3162] specifies the operation of RADIUS over
IPv6 and the RADIUS attributes used to support the IPv6 network
access. "RADIUS Delegated-IPv6-Prefix Attribute" [RFC4818] describes
how to transport delegated IPv6 prefix information over RADIUS.

"RADIUS Attributes for Virtual LAN and Priority Support" [RFC4675]
defines additional attributes for dynamic Virtual LAN assignment and
prioritization, for use in provisioning of access to IEEE 802 local
area networks usable with RADIUS and diameter.

"Common Remote Authentication Dial In User Service (RADIUS)
Implementation Issues and Suggested Fixes" [RFC5080] describes common
issues seen in RADIUS implementations and suggests some fixes. Where
applicable, unclear statements and errors in previous RADIUS
specifications are clarified. People designing extensions to RADIUS
protocol for various deployment cases should get familiar with
"RADIUS Design Guidelines" [RFC6158] in order to avoid, e.g., known
interoperability challenges.

"RADIUS Extension for Digest Authentication" [RFC5090] defines an
extension to the RADIUS protocol to enable support of Digest
Authentication, for use with HTTP-style protocols like the Session
Initiation Protocol (SIP) and HTTP.

"Carrying Location Objects in RADIUS and DIAMETER" [RFC5580]
describes procedures for conveying access-network ownership and
location information based on civic and geospatial location formats
in RADIUS and diameter.

"Remote Authentication Dial-In User Service (RADIUS) Authorization
for Network Access Server (NAS) Management" [RFC5607] specifies
required RADIUS attributes and their values for authorizing a
management access to a NAS. Both local and remote management are
supported, with access rights and management privileges. Specific
provisions are made for remote management via Framed Management
protocols, such as SNMP and NETCONF, and for management access over a
secure transport protocol.

"RADIUS (Remote Authentication Dial In User Service) Support For
Extensible Authentication Protocol (EAP)" [RFC3579] describes how to
use RADIUS to convey an EAP [RFC3748] payload between the
authenticator and the EAP server using RADIUS. RFC 3579 is widely
implemented, for example, in WLAN and 802.1 X environments. "IEEE
802.1X Remote Authentication Dial In User Service (RADIUS) Usage
Guidelines" [RFC3580] describes how to use RADIUS with IEEE 802.1X
authenticators. In the context of 802.1X and EAP-based
authentication, the VSAs described in [RFC2458] have been widely
accepted by the industry. "RADIUS Extensions" [RFC2869] is another
important RFC related to EAP use. RFC 2869 describes additional
attributes for carrying AAA information between a NAS and a shared
accounting server using RADIUS. It also defines attributes to
encapsulate EAP message payload.

There are different MIB modules defined for multiple purposes to use
with RADIUS (see Sections 4.2.3 and 4.2.5).

3.6. Diameter Base Protocol (Diameter)

Diameter [RFC3588] 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 AAA and in
roaming scenarios. Diameter provides an upgrade path for RADIUS but
is not directly backwards compatible.

Diameter is designed to resolve a number of known problems with
RADIUS. Diameter supports server failover, reliable transport over
TCP and SCTP, well-documented functions for proxy, redirect and relay
agent functions, server-initiated messages, auditability, and
capability negotiation. Diameter also provides a larger attribute
space for Attribute-Value Pairs (AVPs) and identifiers 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.

Other notable differences to RADIUS are as follows:

o Network and Transport Layer Security (IPsec or TLS),

o Stateful and stateless models,

o Dynamic discovery of peers (using DNS Service Record (SRV) and
   Naming Authority Pointer (NAPTR)),

o Concept of an application that describes how a specific set of
   commands and Attribute-Value Pairs (AVPs) are treated by diameter
   nodes. Each application has an IANA-assigned unique identifier,

o Support of application layer acknowledgements, failover methods
   and state machines,

o Basic support for user-sessions and accounting,

o Better roaming support,

o Error notification, and

o Easy extensibility.

The Diameter protocol is designed to be extensible to support, e.g.,
proxies, brokers, mobility and roaming, Network Access Servers
(NASREQ), and Accounting and Resource Management. Diameter
applications extend the Diameter base protocol by adding new commands
and/or attributes. Each application is defined by a unique IANA-
assigned application identifier and can add new command codes and/or
new mandatory AVPs.

The Diameter application identifier space has been divided into
Standards Track and 'First Come First Served' vendor-specific
applications. The following are examples of Diameter applications
published at IETF:

o Diameter Base Protocol Application [RFC3588]: Required support
   from all Diameter implementations.

o Diameter Base Accounting Application [RFC3588]: A Diameter
   application using an accounting protocol based on a server-
   directed model with capabilities for real-time delivery of
   accounting information.

o Diameter Mobile IPv4 Application [RFC4004]: A Diameter application
   that allows a Diameter server to authenticate, authorize, and
   collect accounting information for Mobile IPv4 services rendered
   to a mobile node.

o Diameter Network Access Server Application (NASREQ, [RFC4005]): A
   Diameter application used for AAA services in the NAS environment.

o Diameter Extensible Authentication Protocol Application [RFC4072]:
   A Diameter application that carries EAP packets between a NAS and
   a back-end authentication server.

o Diameter Credit-Control Application [RFC4006]: A Diameter
   application that can be used to implement real-time credit-control
   for a variety of end-user services such as network access, Session
   Initiation Protocol (SIP) services, messaging services, and
   download services.

o Diameter Session Initiation Protocol Application [RFC4740]: A
   Diameter application designed to be used in conjunction with SIP
   and provides a Diameter client co-located with a SIP server, with
   the ability to request the authentication of users and
   authorization of SIP resources usage from a Diameter server.

o Diameter Quality-of-Service Application [RFC5866]: A Diameter
   application allowing network elements to interact with Diameter
   servers when allocating QoS resources in the network.

o Diameter Mobile IPv6 IKE (MIP6I) Application [RFC5778]: A Diameter
   application that enables the interaction between a Mobile IP home
   agent and a Diameter server and is used when the mobile node is
   authenticated and authorized using IKEv2 [RFC5996].

o Diameter Mobile IPv6 Auth (MIP6A) Application [RFC5778]: A
   Diameter application that enables the interaction between a Mobile
   IP home agent and a Diameter server and is used when the mobile
   node is authenticated and authorized using the Mobile IPv6
   Authentication Protocol [RFC4285].

The large majority of Diameter applications are vendor-specific and
mainly used in various SDOs outside the IETF. One example SDO using
diameter extensively is 3GPP (e.g., 3GPP 'IP Multimedia Subsystem'
(IMS) uses diameter-based interfaces (e.g., Cx) [3GPPIMS]).
Recently, during the standardization of the '3GPP Evolved Packet
Core' [3GPPEPC], diameter was chosen as the only AAA signaling
protocol.

One part of diameter's extensibility mechanism is an easy and
consistent way of creating new commands for the need of applications.
RFC 3588 proposed to define diameter command code allocations with a
new RFC. This policy decision caused undesired use and redefinition
of existing command codes within SDOs. Diverse RFCs have been
published as simple command code allocations for other SDO purposes
(see [RFC3589], [RFC5224], [RFC5431], and [RFC5516]). [RFC5719]
changed the command code policy and added a range for vendor-specific
command codes to be allocated on a 'First Come First Served' basis by
IANA.

The implementation and deployment experience of diameter has led to
the ongoing development of an update of the base protocol [DIAMETER],
which introduces TLS as the preferred security mechanism and
deprecates the in-band security negotiation for TLS.

Some Diameter protocol enhancements and clarifications that logically
fit better into [DIAMETER], are also needed on the existing
deployments based on RFC 3588. Therefore, protocol extensions
specifically usable in large inter-provider roaming network scenarios
are made available for RFC 3588. Two currently existing
specifications are mentioned below:

o "Clarifications on the Routing of Diameter Requests Based on the
   Username and the Realm" [RFC5729] defines the behavior required
   for Diameter agents to route requests when the User-Name AVP
   contains a NAI formatted with multiple realms. These multi-realm
   Network Access Identifiers are used in order to force the routing
   of request messages through a predefined list of mediating realms.

o "Diameter Straightforward-Naming Authority Pointer (S-NAPTR)
   Usage" [RFC6408] describes an improved DNS-based dynamic Diameter
   agent discovery mechanism without having to do diameter capability
   exchange beforehand with a number of agents.

There have been a growing number of Diameter Framework documents from
the IETF that basically are just a collection of AVPs for a specific
purpose or a system architecture with semantic AVP descriptions and a
logic for "imaginary" applications. From a standardization point of
view, this practice allows the development of larger system
architecture documents that do not need to reference AVPs or
application logic outside the IETF. Below are examples of a few
recent AVP and Framework documents:

   o "Diameter Mobile IPv6: Support for Network Access Server to
      Diameter Server Interaction" [RFC5447] describes the bootstrapping
      of the Mobile IPv6 framework and the support of interworking with
      existing AAA infrastructures by using the diameter NAS-to-home-AAA
      server interface.

   o "Traffic Classification and Quality of Service (QoS) Attributes
      for Diameter" [RFC5777] defines a number of Diameter AVPs for
      traffic classification with actions for filtering and QoS
      treatment.

   o "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local
      Mobility Anchor Interaction with Diameter Server" [RFC5779]
      defines AAA interactions between Proxy Mobile IPv6 (PMIPv6)
      entities (MAG and LMA) and a AAA server within a PMIPv6 Domain.

   For information on MIB modules related to diameter, see
   Section 4.2.5.

3.7. Control and Provisioning of Wireless Access Points (CAPWAP)

   Wireless LAN (WLAN) product architectures have evolved from single
   autonomous Access Points to systems consisting of a centralized
   Access Controller (AC) and Wireless Termination Points (WTPs). The
   general goal of centralized control architectures is to move access
   control, including user authentication and authorization, mobility
   management, and radio management from the single access point to a
   centralized controller, where an Access Point pulls the information
   from the AC.

   Based on "Architecture Taxonomy for Control and Provisioning of
   Wireless Access Points (CAPWAP)" [RFC4118], the CAPWAP working group
   developed the CAPWAP protocol [RFC5415] to facilitate control,
   management, and provisioning of WTPs specifying the services,
   functions, and resources relating to 802.11 WLAN Termination Points
   in order to allow for interoperable implementations of WTPs and ACs.
   The protocol defines the CAPWAP control plane, including the
   primitives to control data access. The protocol document also
   specifies how configuration management of WTPs can be done and
   defines CAPWAP operations responsible for debugging, gathering
   statistics, logging, and managing firmware as well as discusses
   operational and transport considerations.

   The CAPWAP protocol is prepared to be independent of Layer 2
   technologies, and meets the objectives in "Objectives for Control and
   Provisioning of Wireless Access Points (CAPWAP)" [RFC4564]. Separate

   binding extensions enable the use with additional wireless
   technologies. [RFC5416] defines the CAPWAP Protocol Binding for IEEE
   802.11.

   CAPWAP Control messages, and optionally CAPWAP Data messages, are
   secured using DTLS [RFC6347]. DTLS is used as a tightly integrated,
   secure wrapper for the CAPWAP protocol.

   For information on MIB modules related to CAPWAP, see Section 4.2.2.

3.8. Access Node Control Protocol (ANCP)

   The Access Node Control Protocol (ANCP) [RFC6320] realizes a control
   plane between a service-oriented Layer 3 edge device, the NAS and a
   Layer 2 Access Node (AN), e.g., Digital Subscriber Line Access Module
   (DSLAM). As such, ANCP operates in a multi-service reference
   architecture and communicates QoS-, service-, and subscriber-related
   configuration and operation information between a NAS and an AN.

   The main goal of this protocol is to configure and manage access
   equipment and allow them to report information to the NAS in order to
   enable and optimize configuration.

   The framework and requirements for an AN control mechanism and the
   use cases for ANCP are documented in [RFC5851].

   ANCP offers authentication and authorization between AN and NAS nodes
   and provides replay protection and data-origin authentication. The
   ANCP solution is also robust against Denial-of-Service (DoS) attacks.
   Furthermore, the ANCP solution is recommended to offer
   confidentiality protection. Security Threats and Security
   Requirements for ANCP are discussed in [RFC5713].

3.9. Application Configuration Access Protocol (ACAP)

   The Application Configuration Access Protocol (ACAP) [RFC2244] is
   designed to support remote storage and access of program option,
   configuration, and preference information. The datastore model is
   designed to allow a client relatively simple access to interesting
   data, to allow new information to be easily added without server
   reconfiguration, 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 that allow interesting personal information
   to be shared and group information to be restricted.

ACAP's primary purpose is to allow applications access to their
configuration data from multiple network-connected computers. Users
can then use any network-connected computer, run any ACAP-enabled
application, and have access to their own configuration data. To
enable wide usage client simplicity has been preferred to server or
protocol simplicity whenever reasonable.

The ACAP 'authenticate' command uses Simple Authentication and
Security Layer (SASL) [RFC4422] to provide basic authentication,
authorization, integrity, and privacy services. All ACAP
implementations are required to implement the CRAM-MD5 (Challenge-
Response Authentication Mechanism) [RFC2195] for authentication,
which can be disabled based on the site security policy.

3.10. XML Configuration Access Protocol (XCAP)

The Extensible Markup Language (XML) Configuration Access Protocol
(XCAP) [RFC4825] has been designed for and is commonly used with SIP-
based solutions, in particular, for instant messages, presence, and
SIP conferences. XCAP is a protocol that allows a client to read,
write, and modify application configuration data stored in XML format
on a server, where the main functionality is provided by so-called
"XCAP Application Usages".

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. Like ACAP, XCAP supports the configuration
needs for a multiplicity of applications.

All XCAP servers are required to implement HTTP Digest Authentication
[RFC2617]. Furthermore, XCAP servers are required to implement HTTP
over TLS (HTTPS) [RFC2818]. It is recommended that administrators
use an HTTPS URI as the XCAP root URI, so that the digest client
authentication occurs over TLS.

The following list summarizes important XCAP application usages:

o XCAP server capabilities [RFC4825] can be read by clients to
   determine which extensions, application usages, or namespaces a
   server supports.

o A resource lists application is any application that needs access
   to a list of resources, identified by a URI, to which operations,
   such as subscriptions, can be applied [RFC4826].

   o A Resource List Server (RLS) Services application is a SIP
      application, where a server receives SIP SUBSCRIBE requests for
      resources and generates subscriptions towards the resource list
      [RFC4826].

   o A Presence Rules application uses authorization policies, also
      known as authorization rules, to specify what presence information
      can be given to which watchers, and when [RFC4827].

   o A 'pidf-manipulation' application defines how XCAP is used to
      manipulate the contents of PIDF-based presence documents
      [RFC4827].

4. Network Management Data Models

   This section provides two complementary overviews for the network
   management data models standardized at IETF. The first subsection
   focuses on a broader view of models classified into categories such
   as generic and infrastructure data models as well as data models
   matched to different layers. The second subsection is structured
   following the management application view and focuses mainly on the
   data models for the network management tasks fault, configuration,
   accounting, performance, and security management (see [FCAPS]).

   Note that the IETF does not use the FCAPS view as an organizing
   principle for its data models. However, the FCAPS view is used
   widely outside of the IETF for the realization of management tasks
   and applications. Section 4.2 aims to address the FCAPS view to
   enable people outside of the IETF to understand the relevant data
   models in the IETF.

   The different data models covered in this section are MIB modules,
   IPFIX Information Elements, Syslog Structured Data Elements, and YANG
   modules. There are many technology-specific IETF data models, such
   as transmission and protocol MIBs, which are not mentioned in this
   document and can be found at [RFCSEARCH].

   This section gives an overview of management data models that have
   reached Draft or Proposed Standard status at the IETF. In
   exceptional cases, important Informational RFCs are referenced. The
   advancement process for management data models beyond Proposed
   Standard status, has been defined in [BCP027] with a more pragmatic
   approach and special considerations on data model specification
   interoperability. However, most IETF management data models never
   advanced beyond Proposed Standard.

4.1. IETF Network Management Data Models

   The data models defined by the IETF can be broadly classified into
   the following categories depicted in Figure 1.

```
   +----------+  +------------------------------+  +----------+
   |          |  | application-layer data models |  | network  |
   |  generic |  +------------------------------+  |management|
   |  infra-  |  |  transport-layer data models  |  |  infra-  |
   | structure|  +------------------------------+  | structure|
   |   data   |  |   network-layer data models   |  |   data   |
   |  models  |  +------------------------------+  |  models  |
   |          |  |    link-layer data models     |  |          |
   +----------+  +------------------------------+  +----------+
```
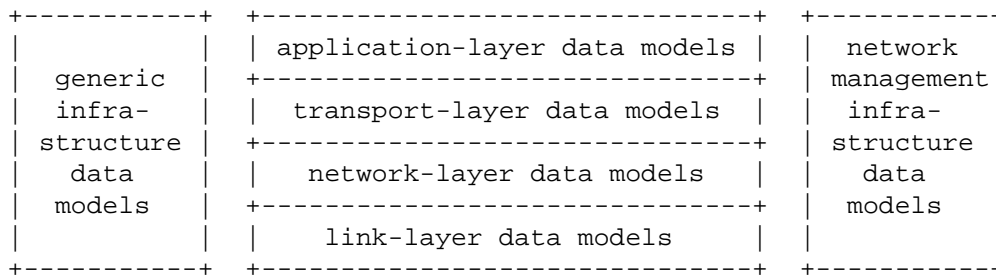
          Figure 1: Categories of Network Management Data Models

   Each of the categories is briefly described below. Note that the
   classification used here is intended to provide orientation and
   reflects how most data models have been developed in the IETF by the
   various working groups. This classification does not aim to classify
   correctly all data models that have been defined by the IETF so far.
   The network layering model in the middle of Figure 1 follows the
   four-layer model of the Internet as defined in [RFC1021].

   The network management object identifiers for use with IETF MIB
   modules defined in the IETF can be found under the IANA registry at
   [SMI-NUMBERS].

4.1.1. Generic Infrastructure Data Models

   Generic infrastructure data models provide core abstractions that
   many other data models are built upon. The most important example is
   the interfaces data model defined in the IF-MIB [RFC2863]. It
   provides the basic notion of network interfaces and allows expressing
   stacking/layering relationships between interfaces. The interfaces
   data model also provides basic monitoring objects that are widely
   used for performance and fault management.

   The second important infrastructure data model is defined in the
   Entity MIB [RFC4133]. It exports the containment hierarchy of the
   physical entities (slots, modules, ports) that make up a networking
   device and, as such, it is a key data model for inventory management.
   Physical entities can have pointers to other data models that provide
   more specific information about them (e.g., physical ports usually
   point to the related network interface). Entity MIB extensions exist
   for physical sensors such as temperature sensors embedded on line
   cards or sensors that report fan rotation speeds [RFC3433]. The

Entity State MIB [RFC4268] models states and alarms of physical
entities. Some vendors have extended the basic Entity MIB with
several proprietary data models.

4.1.2. Link-Layer Data Models

A number of data models exist in the form of MIB modules covering the
link layers IP runs over, such as Asymmetric Bit-Rate DSL (ADSL)
[RFC4706], Very high bit-rate Digital Subscriber Line (VDSL)
[RFC5650], GMPLS [RFC4803], ISDN [RFC2127], ATM [RFC2515] [RFC3606],
Cable Modems [RFC4546], or Ethernet [RFC4188] [RFC4318] [RFC4363].
These so-called transmission data models typically extend the generic
network interfaces data model with interface type specific
information. Most of the link-layer data models focus on monitoring
capabilities that can be used for performance and fault management
functions and, to some lesser extent, for accounting and security
management functions. Meanwhile, the IEEE has taken over the
responsibility to maintain and further develop data models for the
IEEE 802 family of protocols [RFC4663]. The cable modem industry
consortium DOCSIS is working with the IETF to publish data models for
cable modem networks as IETF Standards Track specifications.

4.1.3. Network-Layer Data Models

There are data models in the form of MIB modules covering IP/ICMP
[RFC4293] [RFC4292] network protocols and their extensions (e.g.,
Mobile IP), the core protocols of the Internet. In addition, there
are data models covering popular unicast routing protocols (OSPF
[RFC4750], IS-IS [RFC4444], BGP-4 [RFC4273]) and multicast routing
protocols (PIM [RFC5060]).

Detailed models also exist for performance measurements in the form
of IP Performance Metrics [RFC2330] (see Section 3.4).

The necessary data model infrastructure for configuration data models
covering network layers are currently being defined using NETCONF
[RFC6242] and YANG [RFC6020].

4.1.4. Transport-Layer Data Models

There are data models for the transport protocols TCP [RFC4022], UDP
[RFC4113], and SCTP [RFC3873]. For TCP, a data model providing
extended statistics is defined in [RFC4898].

4.1.5. Application-Layer Data Models

   Some data models have been developed for specific application
   protocols (e.g., SIP [RFC4780]). In addition, there are data models
   that provide a generic infrastructure for instrumenting applications
   in order to obtain data useful primarily for performance management
   and fault management [RFC2287] [RFC2564]. In general, however,
   generic application MIB modules have been less successful in gaining
   widespread deployment.

4.1.6. Network Management Infrastructure Data Models

   A number of data models are concerned with the network management
   system itself. This includes, in addition to a set of SNMP MIB
   modules for monitoring and configuring SNMP itself [RFC3410], some
   MIB modules providing generic functions such as the calculation of
   expressions over MIB objects, generic functions for thresholding and
   event generation, event notification logging functions, and data
   models to represent alarms [RFC2981] [RFC2982] [RFC3014] [RFC3877].

   In addition, there are data models that allow the execution of basic
   reachability and path discovery tests [RFC4560]. Another collection
   of MIB modules provides remote monitoring functions, ranging from the
   data link layer up to the application layer. This is known as the
   "RMON family of MIB modules" [RFC3577].

   The IPFIX Protocol [RFC5101] (Section 2.3) is used to export
   information about network flows collected at so-called Observation
   Points (typically, a network interface). The IEs [RFC5102] carried
   in IPFIX cover the majority of the network and transport layer header
   fields and a few link-layer-specific fields. Work is underway to
   further extend the standardized information that can be carried in
   IPFIX.

   The Syslog Protocol document [RFC5424] (Section 2.2) defines an
   initial set of Structured Data Elements (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.

4.2. Network Management Data Models - FCAPS View

   This subsection follows the management application view and aims to
   match the data models to network management tasks for fault,
   configuration, accounting, performance, and security management
   ([FCAPS]). As OAM is a general term that refers to a toolset, which
   can be used for fault detection, isolation, and performance
   measurement, aspects of FCAPS in the context of the data path, such

   as fault and performance management, are also discussed in "An
   Overview of Operations, Administration, and Maintenance (OAM)
   Mechanisms" [OAM-OVERVIEW].

   Some of the data models do not fit into one single FCAPS category per
   design but span multiple areas. For example, there are many
   technology-specific IETF data models, such as transmission and
   protocol MIBs, which cover multiple FCAPS categories, and therefore
   are not mentioned in this subsection and can be found at [RFCSEARCH].

4.2.1. Fault Management

   Fault management encloses a set of functions to detect, isolate,
   notify, and correct faults encountered in a network as well as to
   maintain and examine error logs. The data models below can be
   utilized to realize a fault management application.

   [RFC3418], part of SNMPv3 standard [STD62], is a MIB module
   containing 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 the network management portion of the system has
   restarted and counters have been re-initialized.

   [RFC3413], part of SNMPv3 standard [STD62], is a MIB module including
   objects designed for managing notifications, including tables for
   addressing, retry parameters, security, lists of targets for
   notifications, and user customization filters.

   The Interfaces Group MIB [RFC2863] builds on the old standard for MIB
   II [STD17] and is used as a primary MIB module for managing and
   monitoring the status of network interfaces. The Interfaces Group
   MIB defines a generic set of managed objects for network interfaces,
   and it provides the infrastructure for additional managed objects
   specific to particular types of network interfaces, such as Ethernet.

   [RFC4560] defines a MIB module for performing ping, traceroute, and
   lookup operations at a host. For troubleshooting purposes, it is
   useful to be able to initiate and retrieve the results of ping or
   traceroute operations when they are performed at a remote host.

   The RMON (Remote Network Monitoring) MIB [STD59] can be configured to
   recognize conditions on existing MIB variables (most notably error
   conditions) and continuously 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 (for further discussion on RMON,
   see Section 4.2.4).

DISMAN-EVENT-MIB in [RFC2981] and DISMAN-EXPRESSION-MIB in [RFC2982]
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 [RFC3877] and the Alarm Reporting Control MIB in
[RFC3878] specify mechanisms for expressing state transition models
for persistent problem states. Alarm MIB defines the following:

o a mechanism for expressing state transition models for persistent
   problem states,

o a mechanism to correlate a notification with subsequent state
   transition notifications about the same entity/object, and

o a generic alarm reporting mechanism (extends ITU-T work on X.733
   [ITU-X733]).

In particular, [RFC3878] defines objects for controlling the
reporting of alarm conditions and extends ITU-T work on M.3100
Amendment 3 [ITU-M3100].

Other MIB modules that may be applied to fault management with SNMP
include:

o NOTIFICATION-LOG-MIB [RFC3014] describes managed objects used for
   logging SNMP Notifications.

o ENTITY-STATE-MIB [RFC4268] describes extensions to the Entity MIB
   to provide information about the state of physical entities.

o ENTITY-SENSOR-MIB [RFC3433] describes managed objects for
   extending the Entity MIB to provide generalized access to
   information related to physical sensors, which are often found in
   networking equipment (such as chassis temperature, fan RPM, power
   supply voltage).

The Syslog protocol document [RFC5424] 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.

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 [RFC5427]. The intent
is that these textual conventions will be imported and used in MIB
modules that would otherwise define their own representations.

An IPFIX MIB module [RFC5815] has been defined for monitoring IPFIX
Meters, Exporters, and Collectors (see Section 2.3). The ongoing
work on the PSAMP MIB module extends the IPFIX MIB modules by managed
objects for monitoring PSAMP implementations [PSAMP-MIB].

The NETCONF working group defined the data model necessary to monitor
the NETCONF protocol [RFC6022] with the modeling language YANG. The
monitoring data model includes information about NETCONF datastores,
sessions, locks, and statistics, which facilitate the management of a
NETCONF server. The NETCONF monitoring document also defines methods
for NETCONF clients to discover the data models supported by a
NETCONF server and defines the operation <get-schema> to retrieve
them.

4.2.2. Configuration Management

Configuration management focuses on establishing and maintaining
consistency of a system and defines the functionality to configure
its functional and physical attributes as well as operational
information throughout its life. Configuration management includes
configuration of network devices, inventory management, and software
management. The data models below can be used to utilize
configuration management.

MIB modules for monitoring of network configuration (e.g., for
physical and logical network topologies) already exist and 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, etc.

[RFC3418], part of [STD62], contains objects in the system group
useful, e.g., for identifying the type of device and the location of
the device, the person responsible for the device. The SNMPv3
standard [STD62] furthermore includes objects designed for
configuring principals, access control rules, notification
destinations, and for configuring proxy-forwarding SNMP agents, which
can be used to forward messages through firewalls and NAT devices.

The Entity MIB [RFC4133] supports mainly inventory management and is
used for managing multiple logical and physical entities matched to a
single SNMP agent. This module provides a useful mechanism for
identifying the entities comprising a system and defines event
notifications for configuration changes that may be useful to
management applications.

[RFC3165] defines a set of managed objects that enable the delegation
of management scripts to distributed managers.

For configuring IPFIX and PSAMP devices, the IPFIX working group
developed the IPFIX Configuration Data Model [CONF-MODEL], by using
the YANG modeling language and in close collaboration with the NETMOD
working group (see Section 2.4.2). The model specifies the necessary
data for configuring and monitoring Selection Processes, caches,
Exporting Processes, and Collecting Processes of IPFIX- and PSAMP-
compliant monitoring devices.

At the time of this writing, the NETMOD working group is developing
core system and interface models in YANG.

The CAPWAP protocol exchanges message elements using the Type-Length-
Value (TLV) format. The base TLVs are specified in [RFC5415], while
the TLVs for IEEE 802.11 are specified in [RFC5416]. The CAPWAP Base
MIB [RFC5833] specifies managed objects for the modeling the CAPWAP
protocol and provides configuration and WTP status-monitoring aspects
of CAPWAP, where the CAPWAP Binding MIB [RFC5834] defines managed
objects for the modeling of the CAPWAP protocol for IEEE 802.11
wireless binding.
Note: RFC 5833 and RFC 5834 have been published as Informational RFCs
to provide the basis for future work on a SNMP management of the
CAPWAP protocol.

4.2.3. Accounting Management

Accounting management collects usage information of network
resources. Note that the IETF does not define any mechanisms related
to billing and charging. Many technology-specific MIBs (link layer,
network layer, transport layer, or application layer) contain
counters but are not primarily targeted for accounting and,
therefore, are not included in this section.

"RADIUS Accounting Client MIB for IPv6" [RFC4670] defines RADIUS
Accounting Client MIB objects that support version-neutral IP
addressing formats.

"RADIUS Accounting Server MIB for IPv6" [RFC4671] defines RADIUS
Accounting Server MIB objects that support version-neutral IP
addressing formats.

IPFIX/PSAMP Information Elements:

As expressed in Section 2.3, the IPFIX Architecture [RFC5470] defines
components involved in IP flow measurement and reporting of
information on IP flows. As such, IPFIX records provide fine-grained
measurement data for flexible and detailed usage reporting and enable
usage-based accounting.

The IPFIX Information Elements (IEs) have been initially defined in
the IPFIX Information Model [RFC5102] and registered with IANA
[IANA-IPFIX]. The IPFIX IEs are composed of two types:

o IEs related to identification of IP flows such as header
   information, derived packet properties, IGP and BGP next-hop IP
   address, BGP AS, etc., and

o IEs related to counter and timestamps, such as per-flow counters
   (e.g., octet count, packet count), flow start times, flow end
   times, and flow duration, etc.

The Information Elements specified in the IPFIX Information Model
[RFC5102] are used by the PSAMP protocol where applicable. PSAMP
Parameters defined in the PSAMP protocol specification are registered
at [IANA-PSAMP]. An additional set of PSAMP Information Elements for
reporting packet information with the IPFIX/PSAMP protocol such as
Sampling-related IEs are specified in the PSAMP Information Model
[RFC5477]. These IEs fulfill the requirements on reporting of
different sampling and filtering techniques specified in [RFC5475].

4.2.4. Performance Management

Performance management covers a set of functions that evaluate and
report the performance of network elements and the network, with the
goal to maintain the overall network performance at a defined level.
Performance management functionality includes monitoring and
measurement of network performance parameters, gathering statistical
information, maintaining and examining activity logs. The data
models below can be used for performance management tasks.

The RMON (Remote Network Monitoring) MIB [STD59] defines objects for
collecting data related to network performance and traffic from
remote monitoring devices. An organization may employ many remote
monitoring probes, one per network segment, to monitor its network.
These devices may be used by a network service provider to access a
(distant) client network. Most of the objects in the RMON MIB module
are suitable for the monitoring of any type of network, while some of
them are specific to the monitoring of Ethernet networks.

RMON allows a probe to be configured to perform diagnostics and to
collect network 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.

"Introduction to the Remote Monitoring (RMON) Family of MIB Modules"
[RFC3577] describes the documents associated with the RMON Framework
and how they relate to each other.

The RMON-2 MIB [RFC4502] extends RMON by providing RMON analysis up
to the application layer and defines performance data to monitor.
The SMON MIB [RFC2613] extends RMON by providing RMON analysis for
switched networks.

"Remote Monitoring MIB Extensions for High Capacity Alarms" [RFC3434]
describes managed objects for extending the alarm thresholding
capabilities found in the RMON MIB and provides similar threshold
monitoring of objects based on the Counter64 data type.

"Remote Network Monitoring Management Information Base for High
Capacity Networks" [RFC3273] defines objects for managing RMON
devices for use on high-speed networks.

"Remote Monitoring MIB Extensions for Interface Parameters
Monitoring" [RFC3144] describes an extension to the RMON MIB with a
method of sorting the interfaces of a monitored device according to
values of parameters specific to this interface.

[RFC4710] describes Real-Time Application Quality of Service
Monitoring (RAQMON), which is part of the RMON protocol family.
RAQMON supports end-to-end QoS monitoring for multiple concurrent
applications and does not relate to a specific application transport.
RAQMON is scalable and works well with encrypted payload and
signaling. RAQMON uses TCP to transport RAQMON PDUs.

[RFC4711] proposes an extension to the Remote Monitoring MIB [STD59]
and describes managed objects used for RAQMON. [RFC4712] specifies
two transport mappings for the RAQMON information model using TCP as
a native transport and SNMP to carry the RAQMON information from a
RAQMON Data Source (RDS) to a RAQMON Report Collector (RRC).

"Application Performance Measurement MIB" [RFC3729] uses the
architecture created in the RMON MIB and defines objects by providing
measurement and analysis of the application performance as
experienced by end-users. [RFC3729] enables the measurement of the
quality of service delivered to end-users by applications.

"Transport Performance Metrics MIB" [RFC4150] describes managed
objects used for monitoring selectable Performance Metrics and
statistics derived from the monitoring of network packets and sub-
application level transactions. The metrics can be defined through
reference to existing IETF, ITU, and other SDOs' documents.

The IPPM working group has defined "IP Performance Metrics (IPPM)
Metrics Registry" [RFC4148]. Note that with the publication of
[RFC6248], [RFC4148] and the corresponding IANA registry for IPPM
metrics have been declared Obsolete and shouldn't be used.

The IPPM working group defined the "Information Model and XML Data
Model for Traceroute Measurements" [RFC5388], which defines a common
information model dividing the IEs into two semantically separated
groups (configuration elements and results elements) with an
additional element to relate configuration elements and results
elements by means of a common unique identifier. Based on the
information model, an XML data model is provided to store the results
of traceroute measurements.

"Session Initiation Protocol Event Package for Voice Quality
Reporting" [RFC6035] defines a SIP event package that enables the
collection and reporting of metrics that measure the quality for
Voice over Internet Protocol (VoIP) sessions.

4.2.5. Security Management

Security management provides the set of functions to protect the
network and system from unauthorized access and includes functions
such as creating, deleting, and controlling security services and
mechanisms, key management, reporting security-relevant events, and
authorizing user access and privileges. Based on their support for
authentication and authorization, RADIUS and diameter are seen as
security management protocols. The data models below can be used to
utilize security management.

[RFC3414], part of [STD62], specifies the procedures for providing
SNMPv3 message-level security and includes a MIB module for remotely
monitoring and managing the configuration parameters for the USM.

[RFC3415], part of [STD62], describes the procedures for controlling
access to management information in the SNMPv3 architecture and
includes a MIB module, which defines managed objects to access
portions of an SNMP engine's Local Configuration Datastore (LCD). As
such, this MIB module enables remote management of the configuration
parameters of the VACM.

The NETCONF Access Control Model (NACM) [RFC6536] addresses the need
for access control mechanisms for the operation and content layers of
NETCONF, as defined in [RFC6241]. As such, the NACM proposes
standard mechanisms to restrict NETCONF protocol access for
particular users to a pre-configured subset of all available NETCONF
protocol operations and content within a particular server.

There are numerous MIB modules defined for multiple purposes to use
with RADIUS:

o "RADIUS Authentication Client MIB for IPv6" [RFC4668] defines
   RADIUS Authentication Client MIB objects that support version-
   neutral IP addressing formats and defines a set of extensions for
   RADIUS authentication client functions.

o "RADIUS Authentication Server MIB for IPv6" [RFC4669] defines
   RADIUS Authentication Server MIB objects that support version-
   neutral IP addressing formats and defines a set of extensions for
   RADIUS authentication server functions.

o "RADIUS Dynamic Authorization Client MIB" [RFC4672] defines the
   MIB module for entities implementing the client side of the
   Dynamic Authorization Extensions to RADIUS [RFC5176].

o "RADIUS Dynamic Authorization Server MIB" [RFC4673] defines the
   MIB module for entities implementing the server side of the
   Dynamic Authorization Extensions to RADIUS [RFC5176].

The MIB Module definitions in [RFC4668], [RFC4669], [RFC4672],
[RFC4673] are intended to be used only for RADIUS over UDP and do not
support RADIUS over TCP. There is also a recommendation that RADIUS
clients and servers implementing RADIUS over TCP should not reuse
earlier listed MIB modules to perform statistics counting for RADIUS-
over-TCP connections.

Currently, there are no standardized MIB modules for diameter
applications, which can be considered as a lack on the management
side of diameter nodes.

5. Security Considerations

   This document gives an overview of IETF network management standards
   and summarizes existing and ongoing development of IETF Standards
   Track network management protocols and data models. As such, it does
   not have any security implications in or of itself.

   For each specific technology discussed in the document a summary of
   its security usage has been given in corresponding chapters. In a
   few cases, e.g., for SNMP, a detailed description of developed
   security mechanisms has been provided.

   The attention of the reader is particularly drawn to the security
   discussion in following document sections:

   o SNMP Security and Access Control Models in Section 2.1.4.1,

   o User-based Security Model (USM) in Section 2.1.4.2,

   o View-based Access Control Model (VACM) in Section 2.1.4.3,

   o SNMP Transport Security Model in Section 2.1.5.1,

   o Secure syslog message delivery in Section 2.2,

   o Use of secure NETCONF message transport and the NETCONF Access
      Control Model (NACM) in Section 2.4.1,

   o Message authentication for Dynamic Host Configuration Protocol
      (DHCP) in Section 3.1.1,

   o Security for Remote Authentication Dial-In User Service (RADIUS)
      in conjunction with EAP and IEEE 802.1X authenticators in
      Section 3.5,

   o Built-in and transport security for the Diameter Base Protocol in
      Section 3.6,

   o Transport security for Control And Provisioning of Wireless Access
      Points (CAPWAP) in Section 3.7,

   o Built-in security for Access Node Control Protocol (ANCP) in
      Section 3.8,

   o Security for Application Configuration Access Protocol (ACAP) in
      Section 3.9,

   o Security for XML Configuration Access Protocol (XCAP) in
      Section 3.10, and

   o Data models for Security Management in Section 4.2.5.

   The authors would also like to refer to detailed security
   consideration sections for specific management standards described in
   this document, which contain comprehensive discussion of security
   implications of the particular management protocols and mechanisms.
   Among others, security consideration sections of following documents
   should be carefully read before implementing the technology.

   o For SNMP security in general, subsequent security consideration
      sections in [STD62], which includes RFCs 3411-3418,

   o Security considerations section in Section 8 of [BCP074] for the
      coexistence of SNMP versions 1, 2, and 3,

   o Security considerations for the SNMP Transport Security Model in
      Section 8 of [RFC5591],

   o Security considerations for the Secure Shell Transport Model for
      SNMP in Section 9 of [RFC5592],

   o Security considerations for the TLS Transport Model for SNMP in
      Section 9 of [RFC6353],

   o Security considerations for the TLS Transport Mapping for syslog
      in Section 6 of [RFC5425],

   o Security considerations for the IPFIX Protocol Specification in
      Section 11 of [RFC5101],

   o Security considerations for the NETCONF protocol in Section 9 of
      [RFC6241] and the SSH transport in Section 6 of [RFC6242],

   o Security considerations for the NETCONF Access Control Model
      (NACM) in Section 3.7 of [RFC6536],

   o Security considerations for DHCPv4 and DHCPv6 in Section 7 of
      [RFC2131] and Section 23. of [RFC3315],

   o Security considerations for RADIUS in Section 8 of [RFC2865],

   o Security considerations for diameter in Section 13 of [RFC3588],

   o Security considerations for the CAPWAP protocol in Section 12 of
      [RFC5415],

   o Security considerations for the ANCP protocol in Section 11 of
      [RFC6320], and

   o Security considerations for the XCAP protocol in Section 14 of
      [RFC4825].

6. Contributors

   Following persons made significant contributions to and reviewed this
   document:

   o Ralph Droms (Cisco) - revised the section on IP Address Management
      and DHCP.

   o Jouni Korhonen (Nokia Siemens Networks) - contributed the sections
      on RADIUS and diameter.

   o Al Morton (AT&T) - contributed to the section on IP Performance
      Metrics.

   o Juergen Quittek (NEC) - contributed the section on IPFIX/PSAMP.

   o Juergen Schoenwaelder (Jacobs University Bremen) - contributed the
      sections on IETF Network Management Data Models and YANG.

7. Acknowledgements

   The editor would like to thank Fred Baker, Alex Clemm, Miguel A.
   Garcia, Simon Leinen, Christopher Liljenstolpe, Tom Petch, Randy
   Presuhn, Dan Romascanu, Juergen Schoenwaelder, Tina Tsou, and Henk
   Uijterwaal for their valuable suggestions and comments in the OPSAWG
   sessions and on the mailing list.

   The editor would like to especially thank Dave Harrington, who
   created the document "Survey of IETF Network Management Standards" a
   few years ago, which has been used as a starting point and enhanced
   with a special focus on the description of the IETF network
   management standards and management data models.

8. Informative References

   [3GPPEPC]   3GPP, "Access to the 3GPP Evolved Packet Core (EPC)
                  via non-3GPP access networks", December 2010,
                  <http://www.3gpp.org/ftp/Specs/html-info/24302.htm>.

   [3GPPIMS]   3GPP, "Release 10, IP Multimedia Subsystem (IMS);
                  Stage 2", September 2010,
                  <http://www.3gpp.org/ftp/Specs/html-info/23228.htm>.

   [BCP027]   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.

   [BCP074]   Frye, R., Levi, D., Routhier, S., and B. Wijnen,
                  "Coexistence between Version 1, Version 2, and
                  Version 3 of the Internet-standard Network Management
                  Framework", BCP 74, RFC 3584, August 2003.

   [BCP170]   Clark, A. and B. Claise, "Guidelines for Considering
                  New Performance Metric Development", BCP 170,
                  RFC 6390, October 2011.

   [CONF-MODEL]   Muenz, G., Claise, B., and P. Aitken, "Configuration
                   Data Model for IPFIX and PSAMP", Work in Progress,
                   July 2011.

   [DIAMETER]   Fajardo, V., Arkko, J., Loughney, J., and G. Zorn,
                   "Diameter Base Protocol", Work in Progress,
                   April 2012.

   [DMTF-CIM]   DMTF, "Common Information Model Schema, Version
                   2.27.0", November 2010,
                   <http://www.dmtf.org/standards/cim>.

   [EMAN-WG]   IETF, "EMAN Working Group",
                   <http://datatracker.ietf.org/wg/eman>.

   [FCAPS]   International Telecommunication Union, "X.700:
                   Management Framework For Open Systems Interconnection
                   (OSI) For CCITT Applications", September 1992,
                   <http://www.itu.int/rec/T-REC-X.700-199209-I/en>.

   [IANA-AAA]   Internet Assigned Numbers Authority, "Authentication,
                   Authorization, and Accounting (AAA) Parameters",
                   February 2012,
                   <http://www.iana.org/assignments/aaa-parameters>.

   [IANA-IPFIX]   Internet Assigned Numbers Authority, "IP Flow
                   Information Export (IPFIX) Entities", May 2012,
                   <http://www.iana.org/assignments/ipfix>.

   [IANA-PROT]   Internet Assigned Numbers Authority, "Protocol
                   Registries", <http://www.iana.org/protocols/>.

   [IANA-PSAMP]   Internet Assigned Numbers Authority, "Packet Sampling
                   (PSAMP) Parameters", April 2009,
                   <http://www.iana.org/assignments/psamp-parameters>.

   [IETF-WGS]   IETF, "IETF Working Groups",
                   <http://datatracker.ietf.org/wg/>.

   [ITU-M3100]   International Telecommunication Union, "M.3100:
                   Generic network information model", January 2006,
                   <http://www.itu.int/rec/T-REC-M.3100-200504-I>.

   [ITU-X680]   International Telecommunication Union, "X.680:
                   Abstract Syntax Notation One (ASN.1): Specification
                   of basic notation", July 2002, <http://www.itu.int/
                   ITU-T/studygroups/com17/languages/X.680-0207.pdf>.

   [ITU-X733]   International Telecommunication Union, "X.733:
                    Systems Management: Alarm Reporting Function",
                    October 1992,
                    <http://www.itu.int/rec/T-REC-X.733-199202-I/en>.

   [MPLSTP-MIB]   King, D. and V. Mahalingam, "Multiprotocol Label
                    Switching Transport Profile (MPLS-TP) MIB-based
                    Management Overview", Work in Progress, April 2012.

   [OAM-ANALYSIS]   Sprecher, N. and L. Fang, "An Overview of the OAM
                    Tool Set for MPLS based Transport Networks", Work
                    in Progress, April 2012.

   [OAM-OVERVIEW]   Mizrahi, T., Sprecher, N., Bellagamba, E., and Y.
                    Weingarten, "An Overview of Operations,
                    Administration, and Maintenance (OAM) Mechanisms",
                    Work in Progress, March 2012.

   [PSAMP-MIB]   Dietz, T., Claise, B., and J. Quittek, "Definitions
                    of Managed Objects for Packet Sampling", Work
                    in Progress, October 2011.

   [RELAX-NG]   OASIS, "RELAX NG Specification, Committee
                    Specification 3 December 2001", December 2001, <http:
                    //www.oasis-open.org/committees/relax-ng/
                    spec-20011203.html>.

   [RFC0951]   Croft, B. and J. Gilmore, "Bootstrap Protocol",
                    RFC 951, September 1985.

   [RFC1021]   Partridge, C. and G. Trewitt, "High-level Entity
                    Management System (HEMS)", RFC 1021, October 1987.

   [RFC1155]   Rose, M. and K. McCloghrie, "Structure and
                    identification of management information for TCP/
                    IP-based internets", STD 16, RFC 1155, May 1990.

   [RFC1157]   Case, J., Fedor, M., Schoffstall, M., and J. Davin,
                    "Simple Network Management Protocol (SNMP)", STD 15,
                    RFC 1157, May 1990.

   [RFC1212]   Rose, M. and K. McCloghrie, "Concise MIB
                    definitions", STD 16, RFC 1212, March 1991.

   [RFC1215]   Rose, M., "Convention for defining traps for use with
                    the SNMP", RFC 1215, March 1991.

   [RFC1321]   Rivest, R., "The MD5 Message-Digest Algorithm",
                      RFC 1321, April 1992.

   [RFC1470]   Enger, R. and J. Reynolds, "FYI on a Network
                      Management Tool Catalog: Tools for Monitoring and
                      Debugging TCP/IP Internets and Interconnected
                      Devices", RFC 1470, June 1993.

   [RFC1901]   Case, J., McCloghrie, K., McCloghrie, K., Rose, M.,
                      and S. Waldbusser, "Introduction to Community-based
                      SNMPv2", RFC 1901, January 1996.

   [RFC2026]   Bradner, S., "The Internet Standards Process --
                      Revision 3", BCP 9, RFC 2026, October 1996.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
                      Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2127]   Roeck, G., "ISDN Management Information Base using
                      SMIv2", RFC 2127, March 1997.

   [RFC2131]   Droms, R., "Dynamic Host Configuration Protocol",
                      RFC 2131, March 1997.

   [RFC2195]   Klensin, J., Catoe, R., and P. Krumviede, "IMAP/POP
                      AUTHorize Extension for Simple Challenge/Response",
                      RFC 2195, September 1997.

   [RFC2244]   Newman, C. and J. Myers, "ACAP -- Application
                      Configuration Access Protocol", RFC 2244,
                      November 1997.

   [RFC2287]   Krupczak, C. and J. Saperia, "Definitions of System-
                      Level Managed Objects for Applications", RFC 2287,
                      February 1998.

   [RFC2330]   Paxson, V., Almes, G., Mahdavi, J., and M. Mathis,
                      "Framework for IP Performance Metrics", RFC 2330,
                      May 1998.

   [RFC2458]   Lu, H., Krishnaswamy, M., Conroy, L., Bellovin, S.,
                      Burg, F., DeSimone, A., Tewani, K., Davidson, P.,
                      Schulzrinne, H., and K. Vishwanathan, "Toward the
                      PSTN/Internet Inter-Networking --Pre-PINT
                      Implementations", RFC 2458, November 1998.

   [RFC2515]   Tesink, K., "Definitions of Managed Objects for ATM
                      Management", RFC 2515, February 1999.

   [RFC2564]   Kalbfleisch, C., Krupczak, C., Presuhn, R., and J.
                  Saperia, "Application Management MIB", RFC 2564,
                  May 1999.

   [RFC2578]   McCloghrie, K., Ed., Perkins, D., Ed., and J.
                  Schoenwaelder, Ed., "Structure of Management
                  Information Version 2 (SMIv2)", STD 58, RFC 2578,
                  April 1999.

   [RFC2579]   McCloghrie, K., Ed., Perkins, D., Ed., and J.
                  Schoenwaelder, Ed., "Textual Conventions for SMIv2",
                  STD 58, RFC 2579, April 1999.

   [RFC2580]   McCloghrie, K., Perkins, D., and J. Schoenwaelder,
                  "Conformance Statements for SMIv2", STD 58, RFC 2580,
                  April 1999.

   [RFC2610]   Perkins, C. and E. Guttman, "DHCP Options for Service
                  Location Protocol", RFC 2610, June 1999.

   [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.

   [RFC2617]   Franks, J., Hallam-Baker, P., Hostetler, J.,
                  Lawrence, S., Leach, P., Luotonen, A., and L.
                  Stewart, "HTTP Authentication: Basic and Digest
                  Access Authentication", RFC 2617, June 1999.

   [RFC2678]   Mahdavi, J. and V. Paxson, "IPPM Metrics for
                  Measuring Connectivity", RFC 2678, September 1999.

   [RFC2679]   Almes, G., Kalidindi, S., and M. Zekauskas, "A One-
                  way Delay Metric for IPPM", RFC 2679, September 1999.

   [RFC2680]   Almes, G., Kalidindi, S., and M. Zekauskas, "A One-
                  way Packet Loss Metric for IPPM", RFC 2680,
                  September 1999.

   [RFC2681]   Almes, G., Kalidindi, S., and M. Zekauskas, "A Round-
                  trip Delay Metric for IPPM", RFC 2681,
                  September 1999.

   [RFC2748]   Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan,
                  R., and A. Sastry, "The COPS (Common Open Policy
                  Service) Protocol", RFC 2748, January 2000.

   [RFC2753]   Yavatkar, R., Pendarakis, D., and R. Guerin, "A
                      Framework for Policy-based Admission Control",
                      RFC 2753, January 2000.

   [RFC2818]   Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

   [RFC2863]   McCloghrie, K. and F. Kastenholz, "The Interfaces
                      Group MIB", RFC 2863, June 2000.

   [RFC2865]   Rigney, C., Willens, S., Rubens, A., and W. Simpson,
                      "Remote Authentication Dial In User Service
                      (RADIUS)", RFC 2865, June 2000.

   [RFC2866]   Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

   [RFC2867]   Zorn, G., Aboba, B., and D. Mitton, "RADIUS
                      Accounting Modifications for Tunnel Protocol
                      Support", RFC 2867, June 2000.

   [RFC2868]   Zorn, G., Leifer, D., Rubens, A., Shriver, J.,
                      Holdrege, M., and I. Goyret, "RADIUS Attributes for
                      Tunnel Protocol Support", RFC 2868, June 2000.

   [RFC2869]   Rigney, C., Willats, W., and P. Calhoun, "RADIUS
                      Extensions", RFC 2869, June 2000.

   [RFC2981]   Kavasseri, R., "Event MIB", RFC 2981, October 2000.

   [RFC2982]   Kavasseri, R., "Distributed Management Expression
                      MIB", RFC 2982, October 2000.

   [RFC3014]   Kavasseri, R., "Notification Log MIB", RFC 3014,
                      November 2000.

   [RFC3046]   Patrick, M., "DHCP Relay Agent Information Option",
                      RFC 3046, January 2001.

   [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.

   [RFC3144]   Romascanu, D., "Remote Monitoring MIB Extensions for
                      Interface Parameters Monitoring", RFC 3144,
                      August 2001.

   [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.

   [RFC3162]   Aboba, B., Zorn, G., and D. Mitton, "RADIUS and
                  IPv6", RFC 3162, August 2001.

   [RFC3164]   Lonvick, C., "The BSD Syslog Protocol", RFC 3164,
                  August 2001.

   [RFC3165]   Levi, D. and J. Schoenwaelder, "Definitions of
                  Managed Objects for the Delegation of Management
                  Scripts", RFC 3165, August 2001.

   [RFC3195]   New, D. and M. Rose, "Reliable Delivery for syslog",
                  RFC 3195, November 2001.

   [RFC3273]   Waldbusser, S., "Remote Network Monitoring Management
                  Information Base for High Capacity Networks",
                  RFC 3273, July 2002.

   [RFC3315]   Droms, R., Bound, J., Volz, B., Lemon, T., Perkins,
                  C., and M. Carney, "Dynamic Host Configuration
                  Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

   [RFC3319]   Schulzrinne, H. and B. Volz, "Dynamic Host
                  Configuration Protocol (DHCPv6) Options for Session
                  Initiation Protocol (SIP) Servers", RFC 3319,
                  July 2003.

   [RFC3393]   Demichelis, C. and P. Chimento, "IP Packet Delay
                  Variation Metric for IP Performance Metrics (IPPM)",
                  RFC 3393, November 2002.

   [RFC3410]   Case, J., Mundy, R., Partain, D., and B. Stewart,
                  "Introduction and Applicability Statements for
                  Internet-Standard Management Framework", RFC 3410,
                  December 2002.

   [RFC3411]   Harrington, D., Presuhn, R., and B. Wijnen, "An
                  Architecture for Describing Simple Network Management
                  Protocol (SNMP) Management Frameworks", STD 62,
                  RFC 3411, December 2002.

   [RFC3413]   Levi, D., Meyer, P., and B. Stewart, "Simple Network
                  Management Protocol (SNMP) Applications", STD 62,
                  RFC 3413, December 2002.

   [RFC3414]   Blumenthal, U. and B. Wijnen, "User-based Security
                      Model (USM) for version 3 of the Simple Network
                      Management Protocol (SNMPv3)", STD 62, RFC 3414,
                      December 2002.

   [RFC3415]   Wijnen, B., Presuhn, R., and K. McCloghrie, "View-
                      based Access Control Model (VACM) for the Simple
                      Network Management Protocol (SNMP)", STD 62,
                      RFC 3415, December 2002.

   [RFC3417]   Presuhn, R., "Transport Mappings for the Simple
                      Network Management Protocol (SNMP)", STD 62,
                      RFC 3417, December 2002.

   [RFC3418]   Presuhn, R., "Management Information Base (MIB) for
                      the Simple Network Management Protocol (SNMP)",
                      STD 62, RFC 3418, December 2002.

   [RFC3430]   Schoenwaelder, J., "Simple Network Management
                      Protocol Over Transmission Control Protocol Transport
                      Mapping", RFC 3430, December 2002.

   [RFC3432]   Raisanen, V., Grotefeld, G., and A. Morton, "Network
                      performance measurement with periodic streams",
                      RFC 3432, November 2002.

   [RFC3433]   Bierman, A., Romascanu, D., and K. Norseth, "Entity
                      Sensor Management Information Base", RFC 3433,
                      December 2002.

   [RFC3434]   Bierman, A. and K. McCloghrie, "Remote Monitoring MIB
                      Extensions for High Capacity Alarms", RFC 3434,
                      December 2002.

   [RFC3444]   Pras, A. and J. Schoenwaelder, "On the Difference
                      between Information Models and Data Models",
                      RFC 3444, January 2003.

   [RFC3460]   Moore, B., "Policy Core Information Model (PCIM)
                      Extensions", RFC 3460, January 2003.

   [RFC3535]   Schoenwaelder, J., "Overview of the 2002 IAB Network
                      Management Workshop", RFC 3535, May 2003.

   [RFC3574]   Soininen, J., "Transition Scenarios for 3GPP
                      Networks", RFC 3574, August 2003.

   [RFC3577]   Waldbusser, S., Cole, R., Kalbfleisch, C., and D.
                    Romascanu, "Introduction to the Remote Monitoring
                    (RMON) Family of MIB Modules", RFC 3577, August 2003.

   [RFC3579]   Aboba, B. and P. Calhoun, "RADIUS (Remote
                    Authentication Dial In User Service) Support For
                    Extensible Authentication Protocol (EAP)", RFC 3579,
                    September 2003.

   [RFC3580]   Congdon, P., Aboba, B., Smith, A., Zorn, G., and J.
                    Roese, "IEEE 802.1X Remote Authentication Dial In
                    User Service (RADIUS) Usage Guidelines", RFC 3580,
                    September 2003.

   [RFC3588]   Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and
                    J. Arkko, "Diameter Base Protocol", RFC 3588,
                    September 2003.

   [RFC3589]   Loughney, J., "Diameter Command Codes for Third
                    Generation Partnership Project (3GPP) Release 5",
                    RFC 3589, September 2003.

   [RFC3606]   Ly, F., Noto, M., Smith, A., Spiegel, E., and K.
                    Tesink, "Definitions of Supplemental Managed Objects
                    for ATM Interface", RFC 3606, November 2003.

   [RFC3633]   Troan, O. and R. Droms, "IPv6 Prefix Options for
                    Dynamic Host Configuration Protocol (DHCP) version
                    6", RFC 3633, December 2003.

   [RFC3646]   Droms, R., "DNS Configuration options for Dynamic
                    Host Configuration Protocol for IPv6 (DHCPv6)",
                    RFC 3646, December 2003.

   [RFC3729]   Waldbusser, S., "Application Performance Measurement
                    MIB", RFC 3729, March 2004.

   [RFC3748]   Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J.,
                    and H. Levkowetz, "Extensible Authentication Protocol
                    (EAP)", RFC 3748, June 2004.

   [RFC3758]   Stewart, R., Ramalho, M., Xie, Q., Tuexen, M., and P.
                    Conrad, "Stream Control Transmission Protocol (SCTP)
                    Partial Reliability Extension", RFC 3758, May 2004.

   [RFC3868]   Loughney, J., Sidebottom, G., Coene, L., Verwimp, G.,
                Keller, J., and B. Bidulock, "Signalling Connection
                Control Part User Adaptation Layer (SUA)", RFC 3868,
                October 2004.

   [RFC3873]   Pastor, J. and M. Belinchon, "Stream Control
                Transmission Protocol (SCTP) Management Information
                Base (MIB)", RFC 3873, September 2004.

   [RFC3877]   Chisholm, S. and D. Romascanu, "Alarm Management
                Information Base (MIB)", RFC 3877, September 2004.

   [RFC3878]   Lam, H., Huynh, A., and D. Perkins, "Alarm Reporting
                Control Management Information Base (MIB)", RFC 3878,
                September 2004.

   [RFC3917]   Quittek, J., Zseby, T., Claise, B., and S. Zander,
                "Requirements for IP Flow Information Export
                (IPFIX)", RFC 3917, October 2004.

   [RFC3954]   Claise, B., "Cisco Systems NetFlow Services Export
                Version 9", RFC 3954, October 2004.

   [RFC4004]   Calhoun, P., Johansson, T., Perkins, C., Hiller, T.,
                and P. McCann, "Diameter Mobile IPv4 Application",
                RFC 4004, August 2005.

   [RFC4005]   Calhoun, P., Zorn, G., Spence, D., and D. Mitton,
                "Diameter Network Access Server Application",
                RFC 4005, August 2005.

   [RFC4006]   Hakala, H., Mattila, L., Koskinen, J-P., Stura, M.,
                and J. Loughney, "Diameter Credit-Control
                Application", RFC 4006, August 2005.

   [RFC4022]   Raghunarayan, R., "Management Information Base for
                the Transmission Control Protocol (TCP)", RFC 4022,
                March 2005.

   [RFC4029]   Lind, M., Ksinant, V., Park, S., Baudot, A., and P.
                Savola, "Scenarios and Analysis for Introducing IPv6
                into ISP Networks", RFC 4029, March 2005.

   [RFC4038]   Shin, M-K., Hong, Y-G., Hagino, J., Savola, P., and
                E. Castro, "Application Aspects of IPv6 Transition",
                RFC 4038, March 2005.

   [RFC4057]   Bound, J., "IPv6 Enterprise Network Scenarios",
                     RFC 4057, June 2005.

   [RFC4072]   Eronen, P., Hiller, T., and G. Zorn, "Diameter
                     Extensible Authentication Protocol (EAP)
                     Application", RFC 4072, August 2005.

   [RFC4113]   Fenner, B. and J. Flick, "Management Information Base
                     for the User Datagram Protocol (UDP)", RFC 4113,
                     June 2005.

   [RFC4118]   Yang, L., Zerfos, P., and E. Sadot, "Architecture
                     Taxonomy for Control and Provisioning of Wireless
                     Access Points (CAPWAP)", RFC 4118, June 2005.

   [RFC4133]   Bierman, A. and K. McCloghrie, "Entity MIB (Version
                     3)", RFC 4133, August 2005.

   [RFC4148]   Stephan, E., "IP Performance Metrics (IPPM) Metrics
                     Registry", BCP 108, RFC 4148, August 2005.

   [RFC4150]   Dietz, R. and R. Cole, "Transport Performance Metrics
                     MIB", RFC 4150, August 2005.

   [RFC4188]   Norseth, K. and E. Bell, "Definitions of Managed
                     Objects for Bridges", RFC 4188, September 2005.

   [RFC4213]   Nordmark, E. and R. Gilligan, "Basic Transition
                     Mechanisms for IPv6 Hosts and Routers", RFC 4213,
                     October 2005.

   [RFC4215]   Wiljakka, J., "Analysis on IPv6 Transition in Third
                     Generation Partnership Project (3GPP) Networks",
                     RFC 4215, October 2005.

   [RFC4221]   Nadeau, T., Srinivasan, C., and A. Farrel,
                     "Multiprotocol Label Switching (MPLS) Management
                     Overview", RFC 4221, November 2005.

   [RFC4268]   Chisholm, S. and D. Perkins, "Entity State MIB",
                     RFC 4268, November 2005.

   [RFC4273]   Haas, J. and S. Hares, "Definitions of Managed
                     Objects for BGP-4", RFC 4273, January 2006.

   [RFC4280]   Chowdhury, K., Yegani, P., and L. Madour, "Dynamic
                    Host Configuration Protocol (DHCP) Options for
                    Broadcast and Multicast Control Servers", RFC 4280,
                    November 2005.

   [RFC4285]   Patel, A., Leung, K., Khalil, M., Akhtar, H., and K.
                    Chowdhury, "Authentication Protocol for Mobile IPv6",
                    RFC 4285, January 2006.

   [RFC4292]   Haberman, B., "IP Forwarding Table MIB", RFC 4292,
                    April 2006.

   [RFC4293]   Routhier, S., "Management Information Base for the
                    Internet Protocol (IP)", RFC 4293, April 2006.

   [RFC4301]   Kent, S. and K. Seo, "Security Architecture for the
                    Internet Protocol", RFC 4301, December 2005.

   [RFC4318]   Levi, D. and D. Harrington, "Definitions of Managed
                    Objects for Bridges with Rapid Spanning Tree
                    Protocol", RFC 4318, December 2005.

   [RFC4363]   Levi, D. and D. Harrington, "Definitions of Managed
                    Objects for Bridges with Traffic Classes, Multicast
                    Filtering, and Virtual LAN Extensions", RFC 4363,
                    January 2006.

   [RFC4422]   Melnikov, A. and K. Zeilenga, "Simple Authentication
                    and Security Layer (SASL)", RFC 4422, June 2006.

   [RFC4444]   Parker, J., "Management Information Base for
                    Intermediate System to Intermediate System (IS-IS)",
                    RFC 4444, April 2006.

   [RFC4502]   Waldbusser, S., "Remote Network Monitoring Management
                    Information Base Version 2", RFC 4502, May 2006.

   [RFC4546]   Raftus, D. and E. Cardona, "Radio Frequency (RF)
                    Interface Management Information Base for Data over
                    Cable Service Interface Specifications (DOCSIS) 2.0
                    Compliant RF Interfaces", RFC 4546, June 2006.

   [RFC4560]   Quittek, J. and K. White, "Definitions of Managed
                    Objects for Remote Ping, Traceroute, and Lookup
                    Operations", RFC 4560, June 2006.

   [RFC4564]   Govindan, S., Cheng, H., Yao, ZH., Zhou, WH., and L.
                  Yang, "Objectives for Control and Provisioning of
                  Wireless Access Points (CAPWAP)", RFC 4564,
                  July 2006.

   [RFC4656]   Shalunov, S., Teitelbaum, B., Karp, A., Boote, J.,
                  and M. Zekauskas, "A One-way Active Measurement
                  Protocol (OWAMP)", RFC 4656, September 2006.

   [RFC4663]   Harrington, D., "Transferring MIB Work from IETF
                  Bridge MIB WG to IEEE 802.1 WG", RFC 4663,
                  September 2006.

   [RFC4668]   Nelson, D., "RADIUS Authentication Client MIB for
                  IPv6", RFC 4668, August 2006.

   [RFC4669]   Nelson, D., "RADIUS Authentication Server MIB for
                  IPv6", RFC 4669, August 2006.

   [RFC4670]   Nelson, D., "RADIUS Accounting Client MIB for IPv6",
                  RFC 4670, August 2006.

   [RFC4671]   Nelson, D., "RADIUS Accounting Server MIB for IPv6",
                  RFC 4671, August 2006.

   [RFC4672]   De Cnodder, S., Jonnala, N., and M. Chiba, "RADIUS
                  Dynamic Authorization Client MIB", RFC 4672,
                  September 2006.

   [RFC4673]   De Cnodder, S., Jonnala, N., and M. Chiba, "RADIUS
                  Dynamic Authorization Server MIB", RFC 4673,
                  September 2006.

   [RFC4675]   Congdon, P., Sanchez, M., and B. Aboba, "RADIUS
                  Attributes for Virtual LAN and Priority Support",
                  RFC 4675, September 2006.

   [RFC4706]   Morgenstern, M., Dodge, M., Baillie, S., and U.
                  Bonollo, "Definitions of Managed Objects for
                  Asymmetric Digital Subscriber Line 2 (ADSL2)",
                  RFC 4706, November 2006.

   [RFC4710]   Siddiqui, A., Romascanu, D., and E. Golovinsky,
                  "Real-time Application Quality-of-Service Monitoring
                  (RAQMON) Framework", RFC 4710, October 2006.

   [RFC4711]   Siddiqui, A., Romascanu, D., and E. Golovinsky,
                      "Real-time Application Quality-of-Service Monitoring
                      (RAQMON) MIB", RFC 4711, October 2006.

   [RFC4712]   Siddiqui, A., Romascanu, D., Golovinsky, E., Rahman,
                      M., and Y. Kim, "Transport Mappings for Real-time
                      Application Quality-of-Service Monitoring (RAQMON)
                      Protocol Data Unit (PDU)", RFC 4712, October 2006.

   [RFC4737]   Morton, A., Ciavattone, L., Ramachandran, G.,
                      Shalunov, S., and J. Perser, "Packet Reordering
                      Metrics", RFC 4737, November 2006.

   [RFC4740]   Garcia-Martin, M., Belinchon, M., Pallares-Lopez, M.,
                      Canales-Valenzuela, C., and K. Tammi, "Diameter
                      Session Initiation Protocol (SIP) Application",
                      RFC 4740, November 2006.

   [RFC4743]   Goddard, T., "Using NETCONF over the Simple Object
                      Access Protocol (SOAP)", RFC 4743, December 2006.

   [RFC4744]   Lear, E. and K. Crozier, "Using the NETCONF Protocol
                      over the Blocks Extensible Exchange Protocol (BEEP)",
                      RFC 4744, December 2006.

   [RFC4750]   Joyal, D., Galecki, P., Giacalone, S., Coltun, R.,
                      and F. Baker, "OSPF Version 2 Management Information
                      Base", RFC 4750, December 2006.

   [RFC4780]   Lingle, K., Mule, J-F., Maeng, J., and D. Walker,
                      "Management Information Base for the Session
                      Initiation Protocol (SIP)", RFC 4780, April 2007.

   [RFC4789]   Schoenwaelder, J. and T. Jeffree, "Simple Network
                      Management Protocol (SNMP) over IEEE 802 Networks",
                      RFC 4789, November 2006.

   [RFC4803]   Nadeau, T. and A. Farrel, "Generalized Multiprotocol
                      Label Switching (GMPLS) Label Switching Router (LSR)
                      Management Information Base", RFC 4803,
                      February 2007.

   [RFC4818]   Salowey, J. and R. Droms, "RADIUS Delegated-IPv6-
                      Prefix Attribute", RFC 4818, April 2007.

   [RFC4825]   Rosenberg, J., "The Extensible Markup Language (XML)
                      Configuration Access Protocol (XCAP)", RFC 4825,
                      May 2007.

   [RFC4826]   Rosenberg, J., "Extensible Markup Language (XML)
                      Formats for Representing Resource Lists", RFC 4826,
                      May 2007.

   [RFC4827]   Isomaki, M. and E. Leppanen, "An Extensible Markup
                      Language (XML) Configuration Access Protocol (XCAP)
                      Usage for Manipulating Presence Document Contents",
                      RFC 4827, May 2007.

   [RFC4898]   Mathis, M., Heffner, J., and R. Raghunarayan, "TCP
                      Extended Statistics MIB", RFC 4898, May 2007.

   [RFC4960]   Stewart, R., "Stream Control Transmission Protocol",
                      RFC 4960, September 2007.

   [RFC5060]   Sivaramu, R., Lingard, J., McWalter, D., Joshi, B.,
                      and A. Kessler, "Protocol Independent Multicast MIB",
                      RFC 5060, January 2008.

   [RFC5080]   Nelson, D. and A. DeKok, "Common Remote
                      Authentication Dial In User Service (RADIUS)
                      Implementation Issues and Suggested Fixes", RFC 5080,
                      December 2007.

   [RFC5085]   Nadeau, T. and C. Pignataro, "Pseudowire Virtual
                      Circuit Connectivity Verification (VCCV): A Control
                      Channel for Pseudowires", RFC 5085, December 2007.

   [RFC5090]   Sterman, B., Sadolevsky, D., Schwartz, D., Williams,
                      D., and W. Beck, "RADIUS Extension for Digest
                      Authentication", RFC 5090, February 2008.

   [RFC5101]   Claise, B., "Specification of the IP Flow Information
                      Export (IPFIX) Protocol for the Exchange of IP
                      Traffic Flow Information", RFC 5101, January 2008.

   [RFC5102]   Quittek, J., Bryant, S., Claise, B., Aitken, P., and
                      J. Meyer, "Information Model for IP Flow Information
                      Export", RFC 5102, January 2008.

   [RFC5103]   Trammell, B. and E. Boschi, "Bidirectional Flow
                      Export Using IP Flow Information Export (IPFIX)",
                      RFC 5103, January 2008.

   [RFC5176]   Chiba, M., Dommety, G., Eklund, M., Mitton, D., and
                      B. Aboba, "Dynamic Authorization Extensions to Remote
                      Authentication Dial In User Service (RADIUS)",
                      RFC 5176, January 2008.

   [RFC5181]   Shin, M-K., Han, Y-H., Kim, S-E., and D. Premec,
                      "IPv6 Deployment Scenarios in 802.16 Networks",
                      RFC 5181, May 2008.

   [RFC5224]   Brenner, M., "Diameter Policy Processing
                      Application", RFC 5224, March 2008.

   [RFC5246]   Dierks, T. and E. Rescorla, "The Transport Layer
                      Security (TLS) Protocol Version 1.2", RFC 5246,
                      August 2008.

   [RFC5277]   Chisholm, S. and H. Trevino, "NETCONF Event
                      Notifications", RFC 5277, July 2008.

   [RFC5357]   Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and
                      J. Babiarz, "A Two-Way Active Measurement Protocol
                      (TWAMP)", RFC 5357, October 2008.

   [RFC5388]   Niccolini, S., Tartarelli, S., Quittek, J., Dietz,
                      T., and M. Swany, "Information Model and XML Data
                      Model for Traceroute Measurements", RFC 5388,
                      December 2008.

   [RFC5415]   Calhoun, P., Montemurro, M., and D. Stanley, "Control
                      And Provisioning of Wireless Access Points (CAPWAP)
                      Protocol Specification", RFC 5415, March 2009.

   [RFC5416]   Calhoun, P., Montemurro, M., and D. Stanley, "Control
                      and Provisioning of Wireless Access Points (CAPWAP)
                      Protocol Binding for IEEE 802.11", RFC 5416,
                      March 2009.

   [RFC5424]   Gerhards, R., "The Syslog Protocol", RFC 5424,
                      March 2009.

   [RFC5425]   Miao, F., Ma, Y., and J. Salowey, "Transport Layer
                      Security (TLS) Transport Mapping for Syslog",
                      RFC 5425, March 2009.

   [RFC5426]   Okmianski, A., "Transmission of Syslog Messages over
                      UDP", RFC 5426, March 2009.

   [RFC5427]   Keeni, G., "Textual Conventions for Syslog
                      Management", RFC 5427, March 2009.

   [RFC5431]   Sun, D., "Diameter ITU-T Rw Policy Enforcement
                      Interface Application", RFC 5431, March 2009.

   [RFC5447]   Korhonen, J., Bournelle, J., Tschofenig, H., Perkins,
                 C., and K. Chowdhury, "Diameter Mobile IPv6: Support
                 for Network Access Server to Diameter Server
                 Interaction", RFC 5447, February 2009.

   [RFC5470]   Sadasivan, G., Brownlee, N., Claise, B., and J.
                 Quittek, "Architecture for IP Flow Information
                 Export", RFC 5470, March 2009.

   [RFC5472]   Zseby, T., Boschi, E., Brownlee, N., and B. Claise,
                 "IP Flow Information Export (IPFIX) Applicability",
                 RFC 5472, March 2009.

   [RFC5473]   Boschi, E., Mark, L., and B. Claise, "Reducing
                 Redundancy in IP Flow Information Export (IPFIX) and
                 Packet Sampling (PSAMP) Reports", RFC 5473,
                 March 2009.

   [RFC5474]   Duffield, N., Chiou, D., Claise, B., Greenberg, A.,
                 Grossglauser, M., and J. Rexford, "A Framework for
                 Packet Selection and Reporting", RFC 5474,
                 March 2009.

   [RFC5475]   Zseby, T., Molina, M., Duffield, N., Niccolini, S.,
                 and F. Raspall, "Sampling and Filtering Techniques
                 for IP Packet Selection", RFC 5475, March 2009.

   [RFC5476]   Claise, B., Johnson, A., and J. Quittek, "Packet
                 Sampling (PSAMP) Protocol Specifications", RFC 5476,
                 March 2009.

   [RFC5477]   Dietz, T., Claise, B., Aitken, P., Dressler, F., and
                 G. Carle, "Information Model for Packet Sampling
                 Exports", RFC 5477, March 2009.

   [RFC5516]   Jones, M. and L. Morand, "Diameter Command Code
                 Registration for the Third Generation Partnership
                 Project (3GPP) Evolved Packet System (EPS)",
                 RFC 5516, April 2009.

   [RFC5539]   Badra, M., "NETCONF over Transport Layer Security
                 (TLS)", RFC 5539, May 2009.

   [RFC5560]   Uijterwaal, H., "A One-Way Packet Duplication
                 Metric", RFC 5560, May 2009.

   [RFC5580]   Tschofenig, H., Adrangi, F., Jones, M., Lior, A., and
                 B. Aboba, "Carrying Location Objects in RADIUS and
                 Diameter", RFC 5580, August 2009.

   [RFC5590]   Harrington, D. and J. Schoenwaelder, "Transport
                 Subsystem for the Simple Network Management Protocol
                 (SNMP)", RFC 5590, June 2009.

   [RFC5591]   Harrington, D. and W. Hardaker, "Transport Security
                 Model for the Simple Network Management Protocol
                 (SNMP)", RFC 5591, June 2009.

   [RFC5592]   Harrington, D., Salowey, J., and W. Hardaker, "Secure
                 Shell Transport Model for the Simple Network
                 Management Protocol (SNMP)", RFC 5592, June 2009.

   [RFC5607]   Nelson, D. and G. Weber, "Remote Authentication
                 Dial-In User Service (RADIUS) Authorization for
                 Network Access Server (NAS) Management", RFC 5607,
                 July 2009.

   [RFC5608]   Narayan, K. and D. Nelson, "Remote Authentication
                 Dial-In User Service (RADIUS) Usage for Simple
                 Network Management Protocol (SNMP) Transport Models",
                 RFC 5608, August 2009.

   [RFC5610]   Boschi, E., Trammell, B., Mark, L., and T. Zseby,
                 "Exporting Type Information for IP Flow Information
                 Export (IPFIX) Information Elements", RFC 5610,
                 July 2009.

   [RFC5650]   Morgenstern, M., Baillie, S., and U. Bonollo,
                 "Definitions of Managed Objects for Very High Speed
                 Digital Subscriber Line 2 (VDSL2)", RFC 5650,
                 September 2009.

   [RFC5655]   Trammell, B., Boschi, E., Mark, L., Zseby, T., and A.
                 Wagner, "Specification of the IP Flow Information
                 Export (IPFIX) File Format", RFC 5655, October 2009.

   [RFC5674]   Chisholm, S. and R. Gerhards, "Alarms in Syslog",
                 RFC 5674, October 2009.

   [RFC5675]   Marinov, V. and J. Schoenwaelder, "Mapping Simple
                 Network Management Protocol (SNMP) Notifications to
                 SYSLOG Messages", RFC 5675, October 2009.

   [RFC5676]   Schoenwaelder, J., Clemm, A., and A. Karmakar,
                  "Definitions of Managed Objects for Mapping SYSLOG
                  Messages to Simple Network Management Protocol (SNMP)
                  Notifications", RFC 5676, October 2009.

   [RFC5706]   Harrington, D., "Guidelines for Considering
                  Operations and Management of New Protocols and
                  Protocol Extensions", RFC 5706, November 2009.

   [RFC5713]   Moustafa, H., Tschofenig, H., and S. De Cnodder,
                  "Security Threats and Security Requirements for the
                  Access Node Control Protocol (ANCP)", RFC 5713,
                  January 2010.

   [RFC5717]   Lengyel, B. and M. Bjorklund, "Partial Lock Remote
                  Procedure Call (RPC) for NETCONF", RFC 5717,
                  December 2009.

   [RFC5719]   Romascanu, D. and H. Tschofenig, "Updated IANA
                  Considerations for Diameter Command Code
                  Allocations", RFC 5719, January 2010.

   [RFC5729]   Korhonen, J., Jones, M., Morand, L., and T. Tsou,
                  "Clarifications on the Routing of Diameter Requests
                  Based on the Username and the Realm", RFC 5729,
                  December 2009.

   [RFC5777]   Korhonen, J., Tschofenig, H., Arumaithurai, M.,
                  Jones, M., and A. Lior, "Traffic Classification and
                  Quality of Service (QoS) Attributes for Diameter",
                  RFC 5777, February 2010.

   [RFC5778]   Korhonen, J., Tschofenig, H., Bournelle, J.,
                  Giaretta, G., and M. Nakhjiri, "Diameter Mobile IPv6:
                  Support for Home Agent to Diameter Server
                  Interaction", RFC 5778, February 2010.

   [RFC5779]   Korhonen, J., Bournelle, J., Chowdhury, K., Muhanna,
                  A., and U. Meyer, "Diameter Proxy Mobile IPv6: Mobile
                  Access Gateway and Local Mobility Anchor Interaction
                  with Diameter Server", RFC 5779, February 2010.

   [RFC5815]   Dietz, T., Kobayashi, A., Claise, B., and G. Muenz,
                  "Definitions of Managed Objects for IP Flow
                  Information Export", RFC 5815, April 2010.

   [RFC5833]   Shi, Y., Perkins, D., Elliott, C., and Y. Zhang,
                       "Control and Provisioning of Wireless Access Points
                       (CAPWAP) Protocol Base MIB", RFC 5833, May 2010.

   [RFC5834]   Shi, Y., Perkins, D., Elliott, C., and Y. Zhang,
                       "Control and Provisioning of Wireless Access Points
                       (CAPWAP) Protocol Binding MIB for IEEE 802.11",
                       RFC 5834, May 2010.

   [RFC5835]   Morton, A. and S. Van den Berghe, "Framework for
                       Metric Composition", RFC 5835, April 2010.

   [RFC5848]   Kelsey, J., Callas, J., and A. Clemm, "Signed Syslog
                       Messages", RFC 5848, May 2010.

   [RFC5851]   Ooghe, S., Voigt, N., Platnic, M., Haag, T., and S.
                       Wadhwa, "Framework and Requirements for an Access
                       Node Control Mechanism in Broadband Multi-Service
                       Networks", RFC 5851, May 2010.

   [RFC5866]   Sun, D., McCann, P., Tschofenig, H., Tsou, T., Doria,
                       A., and G. Zorn, "Diameter Quality-of-Service
                       Application", RFC 5866, May 2010.

   [RFC5880]   Katz, D. and D. Ward, "Bidirectional Forwarding
                       Detection (BFD)", RFC 5880, June 2010.

   [RFC5889]   Baccelli, E. and M. Townsley, "IP Addressing Model in
                       Ad Hoc Networks", RFC 5889, September 2010.

   [RFC5982]   Kobayashi, A. and B. Claise, "IP Flow Information
                       Export (IPFIX) Mediation: Problem Statement",
                       RFC 5982, August 2010.

   [RFC5996]   Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen,
                       "Internet Key Exchange Protocol Version 2 (IKEv2)",
                       RFC 5996, September 2010.

   [RFC6012]   Salowey, J., Petch, T., Gerhards, R., and H. Feng,
                       "Datagram Transport Layer Security (DTLS) Transport
                       Mapping for Syslog", RFC 6012, October 2010.

   [RFC6020]   Bjorklund, M., "YANG - A Data Modeling Language for
                       the Network Configuration Protocol (NETCONF)",
                       RFC 6020, October 2010.

   [RFC6021]   Schoenwaelder, J., "Common YANG Data Types",
                       RFC 6021, October 2010.

   [RFC6022]   Scott, M. and M. Bjorklund, "YANG Module for NETCONF
                    Monitoring", RFC 6022, October 2010.

   [RFC6035]   Pendleton, A., Clark, A., Johnston, A., and H.
                    Sinnreich, "Session Initiation Protocol Event Package
                    for Voice Quality Reporting", RFC 6035,
                    November 2010.

   [RFC6065]   Narayan, K., Nelson, D., and R. Presuhn, "Using
                    Authentication, Authorization, and Accounting
                    Services to Dynamically Provision View-Based Access
                    Control Model User-to-Group Mappings", RFC 6065,
                    December 2010.

   [RFC6087]   Bierman, A., "Guidelines for Authors and Reviewers of
                    YANG Data Model Documents", RFC 6087, January 2011.

   [RFC6095]   Linowski, B., Ersue, M., and S. Kuryla, "Extending
                    YANG with Language Abstractions", RFC 6095,
                    March 2011.

   [RFC6110]   Lhotka, L., "Mapping YANG to Document Schema
                    Definition Languages and Validating NETCONF Content",
                    RFC 6110, February 2011.

   [RFC6158]   DeKok, A. and G. Weber, "RADIUS Design Guidelines",
                    BCP 158, RFC 6158, March 2011.

   [RFC6183]   Kobayashi, A., Claise, B., Muenz, G., and K.
                    Ishibashi, "IP Flow Information Export (IPFIX)
                    Mediation: Framework", RFC 6183, April 2011.

   [RFC6235]   Boschi, E. and B. Trammell, "IP Flow Anonymization
                    Support", RFC 6235, May 2011.

   [RFC6241]   Enns, R., Bjorklund, M., Schoenwaelder, J., and A.
                    Bierman, "Network Configuration Protocol (NETCONF)",
                    RFC 6241, June 2011.

   [RFC6242]   Wasserman, M., "Using the NETCONF Protocol over
                    Secure Shell (SSH)", RFC 6242, June 2011.

   [RFC6244]   Shafer, P., "An Architecture for Network Management
                    Using NETCONF and YANG", RFC 6244, June 2011.

   [RFC6248]   Morton, A., "RFC 4148 and the IP Performance Metrics
                    (IPPM) Registry of Metrics Are Obsolete", RFC 6248,
                    April 2011.

   [RFC6272]   Baker, F. and D. Meyer, "Internet Protocols for the
                        Smart Grid", RFC 6272, June 2011.

   [RFC6313]   Claise, B., Dhandapani, G., Aitken, P., and S. Yates,
                        "Export of Structured Data in IP Flow Information
                        Export (IPFIX)", RFC 6313, July 2011.

   [RFC6320]   Wadhwa, S., Moisand, J., Haag, T., Voigt, N., and T.
                        Taylor, "Protocol for Access Node Control Mechanism
                        in Broadband Networks", RFC 6320, October 2011.

   [RFC6347]   Rescorla, E. and N. Modadugu, "Datagram Transport
                        Layer Security Version 1.2", RFC 6347, January 2012.

   [RFC6353]   Hardaker, W., "Transport Layer Security (TLS)
                        Transport Model for the Simple Network Management
                        Protocol (SNMP)", RFC 6353, July 2011.

   [RFC6371]   Busi, I. and D. Allan, "Operations, Administration,
                        and Maintenance Framework for MPLS-Based Transport
                        Networks", RFC 6371, September 2011.

   [RFC6408]   Jones, M., Korhonen, J., and L. Morand, "Diameter
                        Straightforward-Naming Authority Pointer (S-NAPTR)
                        Usage", RFC 6408, November 2011.

   [RFC6410]   Housley, R., Crocker, D., and E. Burger, "Reducing
                        the Standards Track to Two Maturity Levels", BCP 9,
                        RFC 6410, October 2011.

   [RFC6526]   Claise, B., Aitken, P., Johnson, A., and G. Muenz,
                        "IP Flow Information Export (IPFIX) Per Stream
                        Control Transmission Protocol (SCTP) Stream",
                        RFC 6526, March 2012.

   [RFC6536]   Bierman, A. and M. Bjorklund, "Network Configuration
                        Protocol (NETCONF) Access Control Model", RFC 6536,
                        March 2012.

   [RFC6598]   Weil, J., Kuarsingh, V., Donley, C., Liljenstolpe,
                        C., and M. Azinger, "IANA-Reserved IPv4 Prefix for
                        Shared Address Space", BCP 153, RFC 6598, April 2012.

   [RFC6613]   DeKok, A., "RADIUS over TCP", RFC 6613, May 2012.

   [RFC6614]   Winter, S., McCauley, M., Venaas, S., and K.
                        Wierenga, "Transport Layer Security (TLS) Encryption
                        for RADIUS", RFC 6614, May 2012.

   [RFCSEARCH]   RFC Editor, "RFC Index Search Engine",
                    <http://www.rfc-editor.org/rfcsearch.html>.

   [SMI-NUMBERS]   IANA, "Network Management Parameters - SMI OID List",
                    May 2012,
                    <http://www.iana.org/assignments/smi-numbers>.

   [SMI-YANG]   Schoenwaelder, J., "Translation of SMIv2 MIB Modules
                    to YANG Modules", Work in Progress, April 2012.

   [STD06]   Postel, J., "User Datagram Protocol", STD 6, RFC 768,
                    August 1980.

   [STD07]   Postel, J., "Transmission Control Protocol", STD 7,
                    RFC 793, September 1981.

   [STD16]   Rose, M. and K. McCloghrie, "Structure and
                    identification of management information for TCP/
                    IP-based internets", STD 16, RFC 1155, May 1990.

                    Rose, M. and K. McCloghrie, "Concise MIB
                    definitions", STD 16, RFC 1212, March 1991.

   [STD17]   McCloghrie, K. and M. Rose, "Management Information
                    Base for Network Management of TCP/IP-based
                    internets:MIB-II", STD 17, RFC 1213, March 1991.

   [STD58]   McCloghrie, K., Ed., Perkins, D., Ed., and J.
                    Schoenwaelder, Ed., "Structure of Management
                    Information Version 2 (SMIv2)", STD 58, RFC 2578,
                    April 1999.

                    McCloghrie, K., Ed., Perkins, D., Ed., and J.
                    Schoenwaelder, Ed., "Textual Conventions for SMIv2",
                    STD 58, RFC 2579, April 1999.

                    McCloghrie, K., Ed., Perkins, D., Ed., and J.
                    Schoenwaelder, Ed., "Conformance Statements for
                    SMIv2", STD 58, RFC 2580, April 1999.

   [STD59]   Waldbusser, S., "Remote Network Monitoring Management
                    Information Base", STD 59, RFC 2819, May 2000.

   [STD62]   Harrington, D., Presuhn, R., and B. Wijnen, "An
                    Architecture for Describing Simple Network Management
                    Protocol (SNMP) Management Frameworks", STD 62,
                    RFC 3411, December 2002.

                    Case, J., Harrington, D., Presuhn, R., and B. Wijnen,
                    "Message Processing and Dispatching for the Simple
                    Network Management Protocol (SNMP)", STD 62, RFC
                    3412, December 2002.

                    Levi, D., Meyer, P., and B. Stewart, "Simple Network
                    Management Protocol (SNMP) Applications", STD 62, RFC
                    3413, December 2002.

                    Blumenthal, U. and B. Wijnen, "User-based Security
                    Model (USM) for version 3 of the Simple Network
                    Management Protocol (SNMPv3)", STD 62, RFC 3414,
                    December 2002.

                    Wijnen, B., Presuhn, R., and K. McCloghrie, "View-
                    based Access Control Model (VACM) for the Simple
                    Network Management Protocol (SNMP)", STD 62, RFC
                    3415, December 2002.

                    Presuhn, R., Ed., "Version 2 of the Protocol
                    Operations for the Simple Network Management Protocol
                    (SNMP)", STD 62, RFC 3416, December 2002.

                    Presuhn, R., Ed., "Transport Mappings for the Simple
                    Network Management Protocol (SNMP)", STD 62, RFC
                    3417, December 2002.

                    Presuhn, R., Ed., "Management Information Base (MIB)
                    for the Simple Network Management Protocol (SNMP)",
                    STD 62, RFC 3418, December 2002.

   [STD66]   Berners-Lee, T., Fielding, R., and L. Masinter,
                    "Uniform Resource Identifier (URI): Generic Syntax",
                    STD 66, RFC 3986, January 2005.

   [XPATH]   World Wide Web Consortium, "XML Path Language (XPath)
                    Version 1.0", November 1999,
                    <http://www.w3.org/TR/1999/REC-xpath-19991116>.

   [XSD-1]   Beech, D., Thompson, H., Maloney, M., Mendelsohn, N.,
                  and World Wide Web Consortium Recommendation REC-
                  xmlschema-1-20041028, "XML Schema Part 1: Structures
                  Second Edition", October 2004,
                  <http://www.w3.org/TR/2004/REC-xmlschema-1-20041028>.

Appendix A. High-Level Classification of Management Protocols and Data
             Models

   The following subsections aim to guide the reader for the fast
   selection of the management standard in interest and can be used as a
   dispatcher to forward to the appropriate chapter. The subsections
   below classify the protocols on one hand according to high-level
   criteria such as push versus pull mechanism, and passive versus
   active monitoring. On the other hand, the protocols are categorized
   concerning the network management task they address or the data model
   extensibility they provide. Based on the reader's requirements, a
   reduced set of standard protocols and associated data models can be
   selected for further reading.

   As an example, someone outside of IETF typically would look for the
   TWAMP protocol in the Operations and Management Area working groups
   as it addresses performance management. However, the protocol TWAMP
   has been developed by the IPPM working group in the Transport Area.

   Note that not all protocols have been listed in all classification
   sections. Some of the protocols, especially the protocols with
   specific focus in Section 3 cannot be clearly classified. Note also
   that COPS and COPS-PR are not listed in the tables, as COPS-PR is not
   recommended to use (see Section 3.3).

A.1. Protocols Classified by Standards Maturity in the IETF

   This section classifies the management protocols according their
   standard maturity in the IETF. The IETF standard maturity levels
   Proposed, Draft, or Internet Standard, are defined in [RFC2026] (as
   amended by [RFC6410]). An Internet Standard is characterized by a
   high degree of technical maturity and by a generally held belief that
   the specified protocol or service provides significant benefit to the
   Internet community.

   The table below covers the standard maturity of the different
   protocols listed in this document. Note that only the main protocols
   (and not their extensions) are noted. An RFC search tool listing the
   current document status is available at [RFCSEARCH].

```
+------------------------------------------------+--------------------+
| Protocol                                       | Maturity Level     |
+------------------------------------------------+--------------------+
| SNMP [STD62][RFC3411] (Section 2.1)            | Internet Standard  |
|                                                |                    |
| Syslog [RFC5424] (Section 2.2)                 | Proposed Standard  |
|                                                |                    |
| IPFIX [RFC5101] (Section 2.3)                  | Proposed Standard  |
|                                                |                    |
| PSAMP [RFC5476] (Section 2.3)                  | Proposed Standard  |
|                                                |                    |
| NETCONF [RFC6241] (Section 2.4.1)              | Proposed Standard  |
|                                                |                    |
| DHCP for IPv4 [RFC2131] (Section 3.1.1)        | Draft Standard     |
|                                                |                    |
| DHCP for IPv6 [RFC3315] (Section 3.1.1)        | Proposed Standard  |
|                                                |                    |
| OWAMP [RFC4656] (Section 3.4)                  | Proposed Standard  |
|                                                |                    |
| TWAMP [RFC5357] (Section 3.4)                  | Proposed Standard  |
|                                                |                    |
| RADIUS [RFC2865] (Section 3.5)                 | Draft Standard     |
|                                                |                    |
| Diameter [RFC3588] (Section 3.6)               | Proposed Standard  |
|                                                |                    |
| CAPWAP [RFC5416] (Section 3.7)                 | Proposed Standard  |
|                                                |                    |
| ANCP [RFC6320] (Section 3.8)                   | Proposed Standard  |
|                                                |                    |
| Ad hoc network configuration [RFC5889]         | Informational      |
| (Section 3.1.2)                                |                    |
|                                                |                    |
| ACAP [RFC2244] (Section 3.9)                   | Proposed Standard  |
|                                                |                    |
| XCAP [RFC4825] (Section 3.10)                  | Proposed Standard  |
+------------------------------------------------+--------------------+
```

Table 1: Protocols Classified by Standard Maturity in the IETF

A.2. Protocols Matched to Management Tasks

   This subsection classifies the management protocols matching to the
   management tasks for fault, configuration, accounting, performance,
   and security management.

Fault Mgmt	Config. Mgmt	Accounting Mgmt	Performance Mgmt	Security Mgmt
SNMP notif. with trap operation (S. 2.1.1)	SNMP config. with set operation (S. 2.1.1)	SNMP monitoring with get operation (S. 2.1.1)	SNMP monitoring with get operation (S. 2.1.1)	
IPFIX (S. 2.3)	CAPWAP (S. 3.7)	IPFIX (S. 2.3)	IPFIX (S. 2.3)	
PSAMP (S. 2.3)	NETCONF (S. 2.4.1)	PSAMP (S. 2.3)	PSAMP (S. 2.3)	
Syslog (S. 2.2)	ANCP (S. 3.8)	RADIUS Accounting (S. 3.5)		RADIUS Authent.& Authoriz. (S. 3.5)
	AUTOCONF (S. 3.1.2)	Diameter Accounting (S. 3.6)		Diameter Authent.& Authoriz. (S. 3.6)
	ACAP (S. 3.9)			
	XCAP (S. 3.10)			
	DHCP (S. 3.1.1)			

                 Table 2: Protocols Matched to Management Tasks

   Note: Corresponding section numbers are given in parentheses.

A.3. Push versus Pull Mechanism

   A pull mechanism is characterized by the Network Management System
   (NMS) pulling the management information out of network elements,
   when needed. A push mechanism is characterized by the network
   elements pushing the management information to the NMS, either when
   the information is available or on a regular basis.

   Client/Server protocols, such as DHCP, ANCP, ACAP, and XCAP are not
   listed in Table 3.

   +-------------------------------+-------------------------------+
   | Protocols supporting the Pull | Protocols supporting the Push |
   | mechanism | mechanism |
   +-------------------------------+-------------------------------+
SNMP (except notifications)	SNMP notifications
(Section 2.1)	(Section 2.1)
NETCONF (except notifications)	NETCONF notifications
(Section 2.4.1)	(Section 2.4.1)
CAPWAP (Section 3.7)	Syslog (Section 2.2)
	IPFIX (Section 2.3)
	PSAMP (Section 2.3)
	RADIUS accounting
	(Section 3.5)
	Diameter accounting
	(Section 3.6)
   +-------------------------------+-------------------------------+

       Table 3: Protocol Classification by Push versus Pull Mechanism

A.4. Passive versus Active Monitoring

   Monitoring can be divided into two categories: passive and active
   monitoring. Passive monitoring can perform the network traffic
   monitoring, monitoring of a device, or the accounting of network
   resource consumption by users. Active monitoring, as used in this
   document, focuses mainly on active network monitoring and relies on
   the injection of specific traffic (also called "synthetic traffic"),
   which is then monitored. The monitoring focus is indicated in the
   table below as "network", "device", or "accounting".

   This classification excludes non-monitoring protocols, such as
   configuration protocols: Ad hoc network autoconfiguration, ANCP, and
   XCAP. Note that some of the active monitoring protocols, in the
   context of the data path, e.g., ICMP Ping and Traceroute [RFC1470],
   Bidirectional Forwarding Detection (BFD) [RFC5880], and PWE3 Virtual
   Circuit Connectivity Verification (VCCV) [RFC5085] are covered in
   [OAM-OVERVIEW].

```
+-------------------------------+-------------------------------+
| Protocols supporting passive  | Protocols supporting active   |
| monitoring                    | monitoring                    |
+-------------------------------+-------------------------------+
| IPFIX (network) (Section 2.3) | OWAMP (network) (Section 3.4) |
| PSAMP (network) (Section 2.3) | TWAMP (network) (Section 3.4) |
| SNMP (network and device)     |                               |
| (Section 2.1)                 |                               |
| NETCONF (device)              |                               |
| (Section 2.4.1)               |                               |
| RADIUS (accounting)           |                               |
| (Section 3.5)                 |                               |
| Diameter (accounting)         |                               |
| (Section 3.6)                 |                               |
| CAPWAP (device) (Section 3.7) |                               |
+-------------------------------+-------------------------------+
```

          Table 4: Protocols for Passive and Active Monitoring and Their
                              Monitoring Focus

   The application of SNMP to passive traffic monitoring (e.g., with
   RMON-MIB) or active monitoring (with IPPM MIB) depends on the MIB
   modules used. However, the SNMP protocol itself does not have
   operations, which support active monitoring. NETCONF can be used for
   passive monitoring, e.g., with the NETCONF Monitoring YANG module
   [RFC6022] for the monitoring of the NETCONF protocol. CAPWAP
   monitors the status of a Wireless Termination Point.

   RADIUS and diameter are considered passive monitoring protocols as
   they perform accounting, i.e., counting the number of packets/bytes
   for a specific user.

A.5. Supported Data Model Types and Their Extensibility

   The following table matches the protocols to the associated data
   model types. Furthermore, the table indicates how the data model can
   be extended based on the available content today and whether the
   protocol contains a built-in mechanism for proprietary extensions of
   the data model.

Protocol	Data Modeling	Data Model Extensions	Proprietary Data Modeling Extensions
SNMP (S. 2.1)	MIB modules defined with SMI (S. 2.1.3)	New MIB modules specified in new RFCs	Enterprise-specific MIB modules
Syslog (S. 2.2)	Structured Data Elements (SDEs) (S. 4.2.1)	With the procedure to add Structured Data ID in [RFC5424]	Enterprise-specific SDEs
IPFIX (S. 2.3)	IPFIX Information Elements, IPFIX IANA registry at [IANA-IPFIX] (S. 2.3)	With the procedure to add Information Elements specified in [RFC5102]	Enterprise-specific Information Elements [RFC5101]
PSAMP (S. 2.3)	PSAMP Information Elements, as an extension to IPFIX [IANA-IPFIX], and PSAMP IANA registry at [IANA-PSAMP] (S. 2.3)	With the procedure to add Information Elements specified in [RFC5102]	Enterprise-specific Information Elements [RFC5101]
NETCONF (S. 2.4.1)	YANG modules (S. 2.4.2)	New YANG modules specified in new RFCs following the guideline in [RFC6087]	Enterprise-specific YANG modules
IPPM OWAMP/ TWAMP (S. 3.4)	IPPM metrics (*) (S. 3.4)	New IPPM metrics (S. 3.4)	Not applicable

```
|             |              |                  |                  |
| RADIUS      | TLVs         | RADIUS-related   | Vendor-Specific  |
| (S. 3.5)    |              | registries at    | Attributes       |
|             |              | [IANA-AAA] and   | [RFC2865]        |
|             |              | [IANA-PROT]      |                  |
|             |              |                  |                  |
| Diameter    | AVPs         | Diameter-related | Vendor-Specific  |
| (S. 3.6)    |              | registry at      | Attributes       |
|             |              | [IANA-AAA]       | [RFC2865]        |
|             |              |                  |                  |
| CAPWAP      | TLVs         | New bindings     | Vendor-specific  |
| (S. 3.7)    |              | specified in new | TLVs             |
|             |              | RFCs             |                  |
+-------------+--------------+------------------+------------------+
```

              Table 5: Data Models and Their Extensibility

   (*): With the publication of [RFC6248], the latest IANA registry for
        IPFIX metrics has been declared Obsolete.

Appendix B. New Work Related to IETF Management Standards

B.1. Energy Management (EMAN)

   Energy management is becoming an additional requirement for network
   management systems due to several factors including the rising and
   fluctuating energy costs, the increased awareness of the ecological
   impact of operating networks and devices, and government regulation
   on energy consumption and production.

   The basic objective of energy management is operating communication
   networks and other equipment with a minimal amount of energy while
   still providing sufficient performance to meet service-level
   objectives. Today, most networking and network-attached devices
   neither monitor nor allow controlled energy usage as they are mainly
   instrumented for functions such as fault, configuration, accounting,
   performance, and security management. These devices are not
   instrumented to be aware of energy consumption. There are very few
   means specified in IETF documents for energy management, which
   includes the areas of power monitoring, energy monitoring, and power
   state control.

   A particular difference between energy management and other
   management tasks is that in some cases energy consumption of a device
   is not measured at the device itself but reported by a different
   place. For example, at a Power over Ethernet (PoE) sourcing device
   or at a smart power strip, where one device is effectively metering
   another remote device. This requires a clear definition of the

relationship between the reporting devices and identification of
remote devices for which monitoring information is provided. Similar
considerations will apply to power state control of remote devices,
for example, at a PoE sourcing device that switches on and off power
at its ports. Another example scenario for energy management is a
gateway to low resourced and lossy network devices in wireless a
building network. Here the energy management system talks directly
to the gateway but not necessarily to other devices in the building
network.

At the time of this writing, the EMAN working group is working on the
management of energy-aware devices, covered by the following items:

o The requirements for energy management, specifying energy
   management properties that will allow networks and devices to
   become energy aware. In addition to energy awareness
   requirements, the need for control functions will be discussed.
   Specifically, the need to monitor and control properties of
   devices that are remote to the reporting device should be
   discussed.

o The energy management framework, which will describe extensions to
   the current management framework, required for energy management.
   This includes: power and energy monitoring, power states, power
   state control, and potential power state transitions. The
   framework will focus on energy management for IP-based network
   equipment (routers, switches, PCs, IP cameras, phones and the
   like). Particularly, the relationships between reporting devices,
   remote devices, and monitoring probes (such as might be used in
   low-power and lossy networks) need to be elaborated. For the case
   of a device reporting on behalf of other devices and controlling
   those devices, the framework will address the issues of discovery
   and identification of remote devices.

o The Energy-aware Networks and Devices MIB document, for monitoring
   energy-aware networks and devices, will address devices
   identification, context information, and potential relationship
   between reporting devices, remote devices, and monitoring probes.

o The Power and Energy Monitoring MIB document will document
   defining managed objects for the monitoring of power states and
   energy consumption/production. The monitoring of power states
   includes the following: retrieving power states, properties of
   power states, current power state, power state transitions, and
   power state statistics. The managed objects will provide means of
   reporting detailed properties of the actual energy rate (power)
   and of accumulated energy. Further, they will provide information
   on electrical power quality.

   o The Battery MIB document will define managed objects for battery
      monitoring, which will provide means of reporting detailed
      properties of the actual charge, age, and state of a battery and
      of battery statistics.

   o The applicability statement will describe the variety of
      applications that can use the energy framework and associated MIB
      modules. Potential examples are building networks, home energy
      gateway, etc. Finally, the document will also discuss
      relationships of the framework to other architectures and
      frameworks (such as Smart Grid). The applicability statement will
      explain the relationship between the work in this WG and other
      existing standards, e.g., from the IEC, ANSI, DMTF, etc. Note
      that the EMAN WG will be looking into existing standards such as
      those from the IEC, ANSI, DMTF and others, and reuse existing work
      as much as possible.

   The documents of the EMAN working group can be found at [EMAN-WG].

Authors' Addresses

   Mehmet Ersue (editor)
   Nokia Siemens Networks
   St.-Martin-Strasse 53
   Munich 81541
   Germany

   EMail: mehmet.ersue@nsn.com

   Benoit Claise
   Cisco Systems, Inc.
   De Kleetlaan 6a b1
   Diegem 1831
   Belgium

   EMail: bclaise@cisco.com