Definition of Managed Objects for Synthetic Sources for Performance Monitoring Algorithms

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes objects for configuring Synthetic Sources for Performance Monitoring (SSPM) algorithms.

Table of Contents

1. Introduction

    This memo defines a portion of the Management Information Base (MIB)
    for use with network management protocols in the Internet community.

    In particular, it defines a method of describing Synthetic Sources
    for Performance Monitoring (SSPM). This is useful within the Remote
    Monitoring (RMON) framework [RFC3577] for performance monitoring in
    the cases where it is desirable to inject packets into the network
    for the purpose of monitoring their performance with the other MIBs
    in that framework.

    This memo also includes a MIB module.

    The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
    "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
    document are to be interpreted as described in RFC 2119 [RFC2119].

2. The Internet-Standard Management Framework

    For a detailed overview of the documents that describe the current
    Internet-Standard Management Framework, please refer to section 7 of
    RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed
the Management Information Base or MIB. MIB objects are generally
accessed through the Simple Network Management Protocol (SNMP).
Objects in the MIB are defined using the mechanisms defined in the
Structure of Management Information (SMI). This memo specifies a MIB
module that is compliant to the SMIv2, which is described in STD 58,
RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580
[RFC2580].

3. Overview

This document defines a MIB module for the purpose of remotely
controlling synthetic sources (or 'active' probes) and sinks in order
to enhance remote performance monitoring capabilities within IP
networks and services. Much work within the IETF exists related to
performance monitoring. One interesting aspect of this body of work
is that it does not explicitly define an 'active' probe capability.
An active probe capability is complimentary to existing capabilities,
and this MIB module is developed to fill this void.

3.1. Terms

The following definitions apply throughout this document:

   o 'Performance monitoring' is the act of monitoring traffic for
     the purpose of evaluating a statistic of a metric related to the
     performance of the system. A performance monitoring system is
     comprised of a) traffic generators, b) measurement, c) data
     reduction, and d) reporting. The traffic generators may be
     natural sources, synthetic sources, or intrusive sources.

     o A 'synthetic source' is a device or an embedded software
     program that generates a data packet (or packets) and injects it
     (or them) onto the path to a corresponding probe or existing
     server solely in support of a performance monitoring function.
     A synthetic source may talk intrusively to existing application
     servers.

The design goals for this MIB module are:

   o Complementing the overall performance management architecture
     being defined within the RMONMIB WG; refer to the RMONMIB
     framework document [RFC3577]. This MIB module is defined within
     the context of the APM-MIB [RFC3729].

   o Extensibility: the MIB module should be easily extended to
     include a greater set of protocols and applications for
     performance monitoring purposes.

o Flexibility: the module should support both round-trip and one-
     way measurements.

   o Security: the control of the source and sink of traffic is
     handled by a management application, and communication is
     recommended via SNMPv3.

   This document is organized as follows. The next section discusses
   the relationship of this MIB module to others from the RMONMIB and
   Distributed Management (DISMAN) working groups. Then the structure
   of the MIB module is discussed. Finally, the MIB module definitions
   are given.

4. Relationship to Other MIB modules

   This MIB module is designed to be used in conjunction with the RMON
   MIB Working Group's two other MIB modules for application performance
   measurement: Application Performance Measurement MIB [RFC3729] and
   Transport Performance Metrics MIB [RFC4150]. These MIB modules
   define reporting capabilities for that framework. The intent of this
   MIB module is to define a method for injecting packets into the
   network utilizing probe capabilities defined in the base MIB modules
   and measured with the reporting MIB modules. Other reporting MIB
   modules may be used as well.

   Specifically, this MIB module uses the AppLocalIndex as defined in
   the APM-MIB to map measurement configuration information to
   definition and reporting structures defined in the APM-MIB.

5. Relationship to Other Work

   Much work has already been done within the IETF that has a direct
   bearing on the development of active performance probe definitions.
   This body of work has been addressed in various working groups over
   the years. In this section, we focus on the work of a) the IP
   Performance Metrics (IPPM) working group, b) the DISMAN working
   group, c) the RMON working group, d) the Application MIB (ApplMIB)
   working group, and e) the Realtime Traffic Flow Measurement (RTFM)
   working group.

5.1. IPPM

   The IPPM working group has defined in detail a set of performance
   metrics, sampling techniques, and associated statistics for
   transport-level or connectivity-level measurements. The IPPM
   framework document [RFC2330] discusses numerous issues concerning
   sampling techniques, clock accuracy, resolution and skew, wire time
   versus host time, error analysis, etc. Many of these are

considerations for configuration and implementation issues discussed
below. The IPPM working group has defined several metrics and their
associated statistics, including

     + a connectivity metric [RFC2678],

     + one-way delay metric [RFC2679],

     + one-way loss metric [RFC2680],

     + round-trip delay and loss metrics [RFC2681],

     + delay variation metric [RFC3393],

     + a streaming media metric [RFC3432],

     + a throughput metric [EBT] and [TBT], and

     + others are under development.

These (or a subset) could form the basis for a set of active,
connectivity-level, probe types designed for monitoring the quality
of transport services. A consideration of some of these metrics may
form a set of work activities and a set of early deliverables for a
group developing an active probe capability.

During the early development of the SSPM-MIB, it became apparent that
a one-way measurement protocol was required in order for the SSPM-MIB
to control a one-way measurement. This led to the current work with
the IPPM WG on the development of the One-Way Measurement Protocol
(OWDP) [ODP]. This work includes both the measurement protocol
itself, as well as the development of a separate control protocol.
This later control protocol is redundant with the current work on the
SSPM-MIB. The SSPM-MIB could be used as an alternative to the one-
way delay control protocol.

5.2. DISMAN

The DISMAN working group has defined a set of 'active' tools for
remote management. Of relevance to this document are:

     + the pingMIB [RFC2925],

     + the DNS Lookup MIB [RFC2925],

     + the tracerouteMIB [RFC2925],

+ the scriptMIB [RFC3165], and

+ the expressionMIB [RFC2982].

The pingMIB and tracerouteMIB define an active probe capability,
primarily for the remote determination of path and path connectivity.
There are some performance-related metrics collected from the
pingMIB, and one could conceivably use these measurements for the
evaluation of a limited set of performance statistics. But there is
a fundamental difference between determining connectivity and
determining the quality of that connectivity. However, in the
context of performance monitoring, a fault can be viewed as not
performing at all. Therefore, both should be monitored with the same
probes to reduce network traffic.

The DNS Lookup MIB also includes some probe-like capabilities and
performance time measurements for the DNS lookup. This could be used
to suggest details of a related session-level, active probe.

The scriptMIB allows a network management application to distribute
and manage scripts to remote devices. Conceivably, these scripts
could be designed to run a set of active probe monitors on remote
devices.

5.3. RMON

The RMON working group has developed an extensive, passive monitoring
capability defined in RFC 2819 [RFC2819] and RFC 2021 [RFC2021] as
well as additional MIB modules. Initially, the monitors collected
statistics at the MAC layer, but the capability has now been extended
to higher-layer statistics. Higher-layer statistics are identified
through the definition of a Protocol Directory [RFC2021]. See the
RMONMIB framework document [RFC3577] for an overview of the RMONMIB
capabilities.

Within this context, the development of an active traffic source for
performance monitoring fits well within the overall performance
monitoring architecture being defined within the RMON WG.

5.4. ApplMIB

The ApplMIB working group defined a series of MIB modules that
monitor various aspects of applications, processes, and services.

The System Application MIB [RFC2287] describes a basic set of managed
objects for fault, configuration, and performance management of
applications from a systems perspective. More specifically, the
managed objects it defines are restricted to information that can be

determined from the system itself and that does not require special instrumentation within the applications to make the information available.

The Application MIB [RFC2564] complements the System Application MIB, providing for the management of applications' common attributes, which could not typically be observed without the cooperation of the software being managed. There are attributes that provide information on application and communication performance.

The WWW MIB [RFC2594] describes a set of objects for managing networked services in the Internet Community, particularly World Wide Web (WWW) services. Performance attributes are available for the information about each WWW service, each type of request, each type of response, and top-accessed documents.

In the development of synthetic application-level probes, consideration should be given to the relationship of the application MIB modules to the measurements being performed through a synthetic application-level probe. Similar, cross-indexing issues arise within the context of the RMON monitoring and synthetic application-level active probes.

5.5. SNMPCONF

The Configuration Management with SNMP (SNMPCONF) working group has created the informational RFC 3512 [RFC3512], which outlines the most effective methods for using the SNMP Framework to accomplish configuration management. This work includes recommendations for device-specific as well as network-wide (Policy) configuration. The group is also chartered to write any MIB modules necessary to facilitate configuration management. Specifically, they will write a MIB module that describes a network entity's capabilities and capacities, which can be used by management entities making policy decisions at a network level or device-specific level.

Currently, the SNMPCONF working group is focused on the SNMP Configuration MIB for policy [RFC4011]. It is conceivable that one would want to monitor the performance of newly configured policies as they are implemented within networks. This would require correlation of the implemented policy and a related performance monitoring policy that would specify synthetic probe definitions. For synthetic probes, there would be a need for a configuration of a) a single probe, b) several probes, c) source and destination probes, and d) intermediate probes. In addition, it may be necessary to configure any or all of these combinations simultaneously. It is hoped that the work of SNMPCONF will suffice. The scripting language defined by the SNMP Configuration MIB could allow for active monitoring to be

activated and configured from a policy management script. Further,
the results of active monitoring could become arguments in further
policy decisions. This notion is reflected in the decision flow
outlined in Figure 1 below.

5.6. RTFM

The Realtime Traffic Flow Measurement (RTFM) working group is
concerned with issues relating to traffic flow measurements and usage
reporting for network traffic and Internet accounting. Various
documents exist that describe requirements [RFC1272], traffic flow
measurement architectures [RFC2722], and a traffic flow MIB
[RFC2720]. The work in this group is focused on passive measurements
of user traffic. As such, its work is related to the monitoring work
within the RMON WG. Fundamentally, their attention has not been
concerned with methods of active traffic generation.

5.7. Relationship to Other Work: Summary

In summary, the development of an active traffic generation
capability (primarily for the purpose of performance monitoring)
should draw upon various activities, both past and present, within
the IETF. Figure 1 shows the relationship of the various work
activities briefly touched upon in this section.

Horizontally, across the top of the figure are overall control
functions, which would coordinate the various aspects of the
performance monitoring systems. Vertically at the bottom of the
figure are the functions which comprise the minimum performance
monitoring capability; i.e., traffic generation, monitoring and
measurements, and data reduction. Traffic generation is addressed in
this MIB module. Monitoring and measurement is addressed in the
APM-MIB [RFC3729] and TPM-MIB [RFC4150] modules. Data reduction is
not yet addressed within the IETF. But data reduction could include
both spatial and temporal aggregations at different levels of
reduction. This is indicated in the figure by the arrow labeled
"Various levels and span".

```
                            +-------------------------------------+
                            |                                     |
                            V                                     |
              +-------------------------------------------+       |
      +-------| Application [script], [expr], [snmpconf], |---+   |
      |       |                [apmmib]                    |   |   |
      |       +-------------------------------------------+   |   |
      |                          |                            |   |
  +-------------------------------------------+               |   |
  |           Synchronization Control         |               |   |
  +-------------------------------------------+               |   |
      |                          |                            |   |
      V                          V                            V   |
  +----------------+   +---------------------+   +---------------------+
  | Traffic        |   |Monitoring Metrics   |   |Data Reduction       |
  | Generation     |   |Control [rmon],[ippm],|  |Control [applmib],   |
  | Control [sspm] |   |   [applmib]         |   |[wwwservmib],[expr]  |
  +----------------+   +---------------------+   +---------------------+
      |                          |                            |   |
      V                          V                            V   |
  +-------------------+   +---------------------+   +-------------------+
  |Traffic Generation |   |Monitoring Metrics   |   |Data Reduction     |
  | Instrumentation   |   |  Instrumentation    | +-->| Instrumentation  |
  +-------------------+   +---------------------+   +-------------------+
                                                   |                |   |
                            Various levels         |                |   |
                               and span         +--------------------   |
                                                                    |   |
                                                                    V   |
                                                           Reports ---+
```
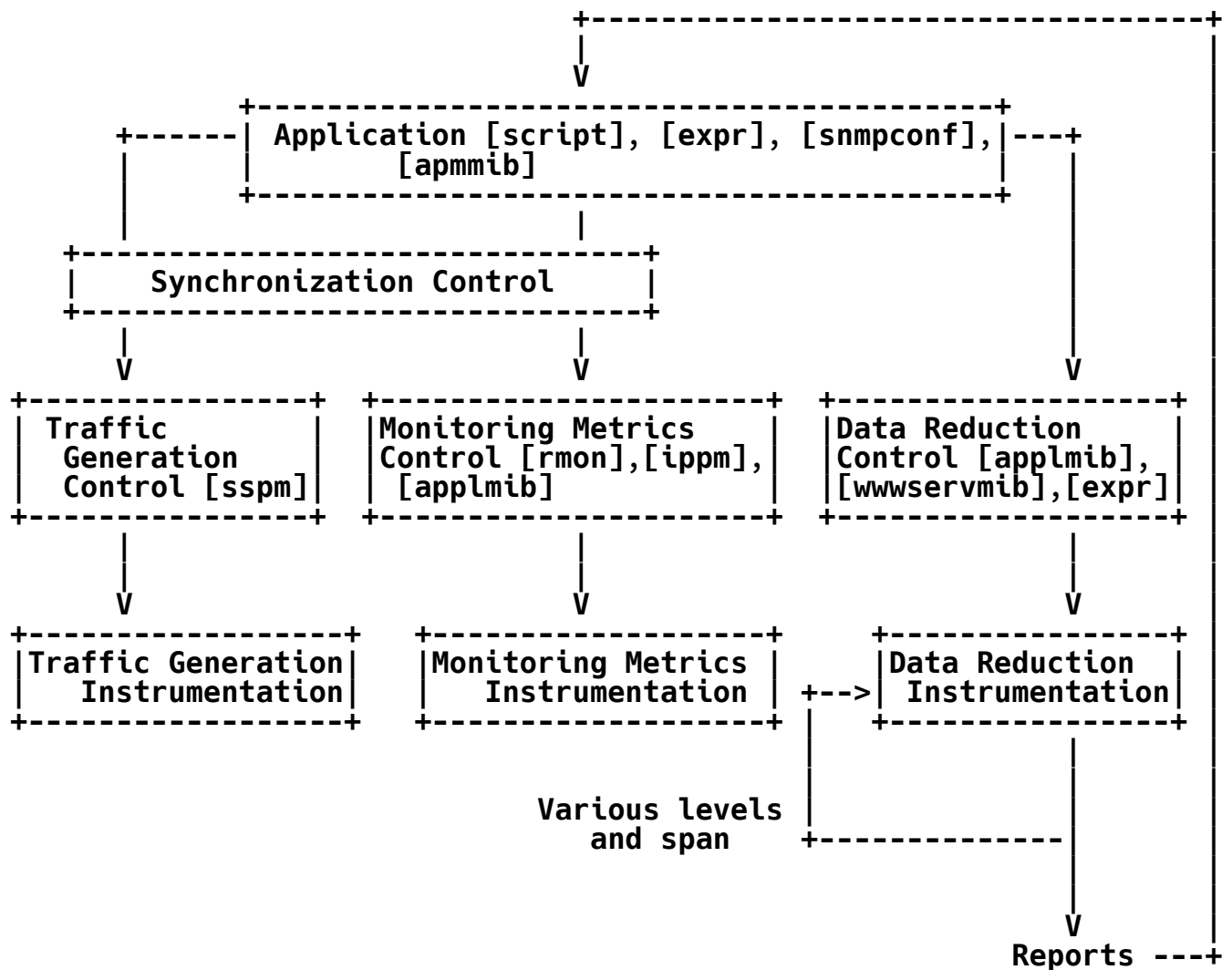
    Figure 1: Coverage for an overall performance monitoring system

6. MIB Structure

    This section presents the structure of the MIB module. The objects
    are arranged into the following groups:

        o general information

        o source configuration

        o sink configuration

6.1. General Information

   This section provides general information about the capabilities of
   the probe. Currently, this information is related to the resolution
   of the probe clock and its source.

6.2. Source Configuration

   The source is configured with a pair of tables. The first,
   sspmSourceProfileTable, defines a set of profiles for monitoring.
   These profiles are then used by the second table,
   sspmSourceControlTable, to instantiate a specific measurement. This
   MIB module takes an IP-centric view of the configuration of the
   measurement.

6.3. Sink Configuration

   Configures the sink for measurements. If the test is round-trip,
   then this table is on the same probe as the source configuration. If
   the test is one-way, then the table is on a different probe. The
   sspmSinkInstance is a unique identifier for the entry per probe.
   Additional attributes are provided for test type and test source to
   identify entries in the table uniquely.

7. Definitions

   SSPM-MIB DEFINITIONS ::= BEGIN

      IMPORTS

          MODULE-IDENTITY, OBJECT-TYPE,
          Counter32, Integer32, Unsigned32
                                 FROM SNMPv2-SMI --[RFC2578]

          TEXTUAL-CONVENTION, StorageType,
          TruthValue, RowStatus
                                 FROM SNMPv2-TC --[RFC2579]

          MODULE-COMPLIANCE, OBJECT-GROUP
                                 FROM SNMPv2-CONF --[RFC2578,
                                                  -- RFC2579,
                                                  -- RFC2580]
          OwnerString, rmon
                                 FROM RMON-MIB --[RFC2819]

          InetAddressType, InetAddress
                                 FROM INET-ADDRESS-MIB --[RFC3291]

```
        InterfaceIndexOrZero
                                  FROM IF-MIB  --[RFC2863]

        AppLocalIndex
                                  FROM APM-MIB  --[RFC3729]

        Utf8String
                                  FROM SYSAPPL-MIB;  --[RFC2287]

    sspmMIB MODULE-IDENTITY
        LAST-UPDATED "200507280000Z"  -- July 28, 2005
        ORGANIZATION "IETF RMON MIB working group"
        CONTACT-INFO
                 "          Carl W. Kalbfleisch
                  Consultant

             E-mail: ietf@kalbfleisch.us

             Working group mailing list: rmonmib@ietf.org
             To subscribe send email to rmonmib-request@ietf.org"
        DESCRIPTION
            "This SSPM MIB module is applicable to probes
             implementing Synthetic Source for Performance
             Monitoring functions.

             Copyright (C) The Internet Society (2005).  This version
             of this MIB module is part of RFC 4149; see the RFC
             itself for full legal notices."

            -- revision history

            REVISION     "200507280000Z"   -- July 28, 2005
            DESCRIPTION
                "The original version of this MIB module,
                 was published as RFC4149."
        ::= { rmon 28 }

 --
 -- Object Identifier Assignments
 --
 sspmMIBObjects       OBJECT IDENTIFIER ::= { sspmMIB 1 }
 sspmMIBNotifications OBJECT IDENTIFIER ::= { sspmMIB 2 }
 sspmMIBConformance   OBJECT IDENTIFIER ::= { sspmMIB 3 }

 --
 -- Textual Conventions
 --
```

```
    SspmMicroSeconds ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "d"
        STATUS current
        DESCRIPTION
          "A unit of time with resolution of MicroSeconds."
        SYNTAX Unsigned32

    SspmClockSource ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "d"
        STATUS current
        DESCRIPTION
            "An indication of the source of the clock as defined by the
             NTP specification RFC1305 [RFC1305] definition of stratum:

             Stratum (sys.stratum, peer.stratum, pkt.stratum): This is
             an integer indicating the stratum of the local clock,
             with values defined as follows:

             0       unspecified

             1       primary reference (e.g., calibrated atomic clock,
                     radio clock)

             2-255   secondary reference (via NTP)."
        REFERENCE
            "RFC1305."
        SYNTAX Integer32 (0..255)

    SspmClockMaxSkew ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "d"
        STATUS current
        -- UNITS "Seconds"
        DESCRIPTION
            "An indication of the accuracy of the clock as defined by
             RFC1305.  This variable indicates the maximum offset
             error due to skew of the local clock over the
             time interval 86400 seconds, in seconds."
        REFERENCE
            "RFC1305."
        SYNTAX Integer32 (1..65535)

    --
    -- sspmGeneral
    --
    sspmGeneral             OBJECT IDENTIFIER ::= { sspmMIBObjects 1 }
    sspmGeneralClockResolution OBJECT-TYPE
        SYNTAX       SspmMicroSeconds
        MAX-ACCESS   read-only
```

```
        STATUS      current
        -- UNITS        Microseconds
        DESCRIPTION
           "A read-only variable indicating the resolution
          of the measurements possible by this device."
        ::= { sspmGeneral 1 }

   sspmGeneralClockMaxSkew OBJECT-TYPE
        SYNTAX SspmClockMaxSkew
        MAX-ACCESS read-only
        STATUS current
        -- UNITS Seconds
        DESCRIPTION
           "A read-only variable indicating the maximum offset
            error due to skew of the local clock over the
            time interval 86400 seconds, in seconds."
        ::= { sspmGeneral 2 }



   sspmGeneralClockSource OBJECT-TYPE
        SYNTAX SspmClockSource
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
           "A read-only variable indicating the source of the clock.
            This is provided to allow a user to determine how accurate
            the timing mechanism is compared with other devices.  This
            is needed for the coordination of time values
            between probes for one-way measurements."
        ::= { sspmGeneral 3 }

   sspmGeneralMinFrequency OBJECT-TYPE
        SYNTAX      SspmMicroSeconds
        MAX-ACCESS read-only
        -- units   MicroSeconds
        STATUS      current
        DESCRIPTION
           "A read-only variable that indicates the devices'
            capability for the minimum supported
            sspmSourceFrequency.  If sspmSourceFrequency is
            set to a value lower than the value reported
            by this attribute, then the set of sspmSourceFrequency
            will fail with an inconsistent value error."
        ::= { sspmGeneral 4 }

   --
   -- sspmCapabilities
   --
```

```
   -- Describes the capabilities of the SSPM device.
   --
   sspmCapabilitiesTable OBJECT-TYPE
       SYNTAX       SEQUENCE OF SspmCapabilitiesEntry
       MAX-ACCESS   not-accessible
       STATUS       current
       DESCRIPTION
          "The table of SSPM capabilities."
       ::= { sspmGeneral 5 }

   sspmCapabilitiesEntry OBJECT-TYPE
       SYNTAX       SspmCapabilitiesEntry
       MAX-ACCESS   not-accessible
       STATUS       current
       DESCRIPTION
          "Details about a particular SSPM capability."
       INDEX { sspmCapabilitiesInstance }
       ::= { sspmCapabilitiesTable 1 }

   SspmCapabilitiesEntry ::= SEQUENCE {
       sspmCapabilitiesInstance AppLocalIndex
       }

   sspmCapabilitiesInstance OBJECT-TYPE
       SYNTAX       AppLocalIndex
       MAX-ACCESS   read-only
       STATUS       current
       DESCRIPTION
          "Indicates whether SSPM configuration of the corresponding
           AppLocalIndex is supported by this device.  Generally,
           entries in this table are only made by the device when the
           configuration of the measurement is available."
        ::= { sspmCapabilitiesEntry 1 }

   --
   -- sspmSource
   --
   -- Contains the details of the source of the
   -- Synthetic Sources for Performance Monitoring algorithms.
   -- This information is split into two tables.  The first defines
   -- profiles that can be applied to specific sources in the
   -- control table.
   --
   sspmSource             OBJECT IDENTIFIER ::= { sspmMIBObjects 2 }

   --
   -- sspmSourceProfileTable
   -- Defines template profiles for measurements.
```

```
    --
    sspmSourceProfileTable OBJECT-TYPE
        SYNTAX       SEQUENCE OF SspmSourceProfileEntry
        MAX-ACCESS   not-accessible
        STATUS       current
        DESCRIPTION
            "The table of SSPM Source Profiles configured."
        ::= { sspmSource 1 }

    sspmSourceProfileEntry OBJECT-TYPE
        SYNTAX       SspmSourceProfileEntry
        MAX-ACCESS   not-accessible
        STATUS       current
        DESCRIPTION
            "Details about a particular SSPM Source Profile
             configuration.  Entries must exist in this table
             in order to be referenced by rows in the
             sspmSourceControlTable."
        INDEX { sspmSourceProfileInstance }
        ::= { sspmSourceProfileTable 1 }

    SspmSourceProfileEntry ::= SEQUENCE {
        sspmSourceProfileInstance          Unsigned32,
        sspmSourceProfileType              AppLocalIndex,
        sspmSourceProfilePacketSize        Unsigned32,
        sspmSourceProfilePacketFillType    INTEGER,
        sspmSourceProfilePacketFillValue   OCTET STRING,
        sspmSourceProfileTOS               Integer32,
        sspmSourceProfileFlowLabel         Integer32,
        sspmSourceProfileLooseSrcRteFill   OCTET STRING,
        sspmSourceProfileLooseSrcRteLen    Integer32,
        sspmSourceProfileTTL               Integer32,
        sspmSourceProfileNoFrag            TruthValue,
        sspmSourceProfile8021Tagging       Integer32,
        sspmSourceProfileUsername          Utf8String,
        sspmSourceProfilePassword          Utf8String,
        sspmSourceProfileParameter         OCTET STRING,
        sspmSourceProfileOwner             OwnerString,
        sspmSourceProfileStorageType       StorageType,
        sspmSourceProfileStatus            RowStatus
    }

    sspmSourceProfileInstance OBJECT-TYPE
        SYNTAX       Unsigned32 (1..65535)
        MAX-ACCESS   not-accessible
        STATUS       current
        DESCRIPTION
            "An arbitrary index."
```

```
        ::= { sspmSourceProfileEntry 1 }

   sspmSourceProfileType OBJECT-TYPE
       SYNTAX       AppLocalIndex
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
           "The AppLocalIndex value that uniquely identifies the
            measurement per the APM-MIB.  In order to create a row
            in this table, there must be a corresponding row in the
            sspmCapabilitiesTable.

            When attempting to set this object, if no
            corresponding row exists in the sspmCapabilitiesTable,
            then the agent should return a 'badValue' error."
       ::= { sspmSourceProfileEntry 2}

   sspmSourceProfilePacketSize OBJECT-TYPE
       SYNTAX       Unsigned32
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
           "The size of packet to be transmitted in bytes.  The
            size accounts for all data within the IPv4 or IPv6
            payloads, excluding the IP headers, IP header options
            and link-level protocol headers.

            If the size is set smaller than the minimum allowed
            packet size or greater than the maximum allowed
            packet size, then the set should fail, and the agent
            should return a 'badValue' error."
       ::= { sspmSourceProfileEntry 3 }

   sspmSourceProfilePacketFillType OBJECT-TYPE
       SYNTAX       INTEGER {
                        random (1),
                        pattern (2),
                        url(3)
                    }
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
           "Indicates how the packet is filled.

            'random' indicates that the packet contains random
            data patterns.  This is probe and implementation
            dependent.
```

```
                        'pattern' indicates that the pattern defined in the
                        sspmSourceProfilePacketFillValue attribute is used to
                        fill the packet.

                        'url' indicates that the value of
                        sspmSourceProfilePacketFillValue should
                        contain a URL.  The contents of the document
                        at that URL are retrieved when sspmSourceStatus becomes
                        active and utilized in the packet.  If the attempt to
                        access that URL fails, then the row status is set to
                        'notReady', and the set should fail with
                        'inconsistentValue'.  This value must contain a
                        dereferencable URL of the type 'http:', 'https:', or
                        'ftp:' only."
                ::= { sspmSourceProfileEntry 4 }

        sspmSourceProfilePacketFillValue OBJECT-TYPE
                SYNTAX        OCTET STRING (SIZE(0..255))
                MAX-ACCESS  read-create
                STATUS        current
                DESCRIPTION
                        "The string value with which to fill the packet.  If
                        sspmSourceProfilePacketFillType is set to 'pattern',
                        then this pattern is repeated until the packet is
                        sspmSourcePacketSize in bytes.  Note that if the
                        length of the octet string specified for this
                        value does not divide evenly into the packet
                        size, then an incomplete last copy of this data
                        may be copied into the packet.  If the value of
                        sspmSourceProfilePacketFillType is set to 'random', then
                        this attribute is unused.  If the value of the
                        sspmSourceProfilePacketFillType is set to 'url', then
                        the URL specified in this attribute is retrieved
                        and used by the probe.  In the case of a URL, this value
                        must contain a dereferencable URL of the type
                        'http:', 'https:', or 'ftp:' only."
                ::= { sspmSourceProfileEntry 5 }

        sspmSourceProfileTOS OBJECT-TYPE
                SYNTAX        Integer32 (0..255)
                MAX-ACCESS  read-create
                STATUS        current
                DESCRIPTION
                        "Represents the TOS field in the IP packet header.  The
                        value of this object defaults to zero if not set."
                DEFVAL { 0 }
                ::= { sspmSourceProfileEntry 6 }
```

```
    sspmSourceProfileFlowLabel OBJECT-TYPE
        SYNTAX        Integer32 (0..1048575) -- 20-bit range (0 to 0xfffff)
        MAX-ACCESS    read-create
        STATUS        current
        DESCRIPTION
            "This object is used to specify the Flow Label in a IPv6
             packet (RFC 2460) to force special handling by the IPv6
             routers; e.g., non-default quality-of-service handling.

             This object is meaningful only when the object
             sspmSourceDestAddressType is IPv6(2).
             The value of this object defaults to zero if not set."
        DEFVAL { 0 }
        ::= { sspmSourceProfileEntry 7 }

    sspmSourceProfileLooseSrcRteFill OBJECT-TYPE
        SYNTAX        OCTET STRING (SIZE(0..240))
        MAX-ACCESS    read-create
        STATUS        current
        DESCRIPTION
            "In the event that the test should run over a
             specific route, the intent is to force the route using the
             Loose Source Route option in IPv4 [RFC791] and
             IPv6 [RFC2460].  This object contains a
             series of IP addresses along the path that would be
             put into the loose source route option in the IP header.

             The IPv4 addresses are to be listed as 32-bit
             address values, and the IPv6 addresses are to be
             listed as a string of 128-bit addresses.  The
             maximum length allowed within the IPv4 source route
             option is 63 addresses.  To simply account for
             IPv6 addresses as well, the maximum length of the
             octet string is 240.  This allows up to 60
             IPv4 addresses or up to 15 IPv6 addresses in the
             string."
        ::= { sspmSourceProfileEntry 8 }

    sspmSourceProfileLooseSrcRteLen OBJECT-TYPE
        SYNTAX        Integer32(0..240)
        MAX-ACCESS    read-create
        STATUS        current
        DESCRIPTION
            "In the event that the test should run over a
             specific route, the intent is to force the route.
             This attribute specifies the length of data to
             be copied from the sspmSourceProfileLooseSrcRteFill
             into the route data fields of the loose source route
```

```
        options in the IPv4 or IPv6 headers."
    ::= { sspmSourceProfileEntry 9 }

sspmSourceProfileTTL OBJECT-TYPE
    SYNTAX        Integer32(1..255)
    MAX-ACCESS  read-create
    STATUS        current
    DESCRIPTION
        "If non-zero, this specifies the value to place into
         the TTL field on transmission."
    ::= { sspmSourceProfileEntry 10 }

sspmSourceProfileNoFrag OBJECT-TYPE
    SYNTAX        TruthValue
    MAX-ACCESS  read-create
    STATUS        current
    DESCRIPTION
        "When true, the 'Don't Fragment Bit' should be set
         on the packet header."
    ::= { sspmSourceProfileEntry 11 }

sspmSourceProfile8021Tagging OBJECT-TYPE
    SYNTAX        Integer32 (-1..65535)
    MAX-ACCESS  read-create
    STATUS        current
    DESCRIPTION
        "IEEE 802.1Q tagging used in IEEE 802.1D bridged
        environments.

        A value of -1 indicates that the packets are untagged.

        A value of 0 to 65535 is the value of the tag to be
        inserted in the tagged packets.

        Note that according to IEEE 802.1Q, VLAN-ID tags with
        a value of 4095 shall not be transmitted on the wire.
        As the VLAN-ID is encoded in the 12 least significant
        bits on the tag, values that translate in a binary
        representation of all 1's in the last 12 bits
        SHALL NOT be configured.  In this case, the set should
        fail, and return an error-status of 'inconsistentValue'."
    ::= { sspmSourceProfileEntry 12 }

sspmSourceProfileUsername OBJECT-TYPE
    SYNTAX        Utf8String
    MAX-ACCESS  read-create
    STATUS        current
    DESCRIPTION
```

          "An optional username used by the application protocol."
        ::= { sspmSourceProfileEntry 13 }

    sspmSourceProfilePassword OBJECT-TYPE
        SYNTAX   Utf8String
        MAX-ACCESS   read-create
        STATUS   current
        DESCRIPTION
           "An optional password used by the application protocol."
        ::= { sspmSourceProfileEntry 14 }

    sspmSourceProfileParameter OBJECT-TYPE
        SYNTAX   OCTET STRING (SIZE(0..65535))
        MAX-ACCESS   read-create
        STATUS   current
        DESCRIPTION
            "An optional parameter used by the application protocol.
            For DNS, this would be the hostname or IP. For HTTP,
            this would be the URL. For nntp, this would be the
            news group. For TCP, this would be the port number.
            For SMTP, this would be the recipient (and could
            assume the message is predefined)."
        ::= { sspmSourceProfileEntry 15 }

    sspmSourceProfileOwner OBJECT-TYPE
        SYNTAX   OwnerString
        MAX-ACCESS   read-create
        STATUS   current
        DESCRIPTION
           "Name of the management station/application that
           set up the profile."
        ::= { sspmSourceProfileEntry 16 }

    sspmSourceProfileStorageType OBJECT-TYPE
        SYNTAX   StorageType
        MAX-ACCESS   read-create
        STATUS   current
        DESCRIPTION
           "The storage type of this sspmSourceProfileEntry. If the
           value of this object is 'permanent', no objects in this row
           need to be writable."
        ::= { sspmSourceProfileEntry 17 }

    sspmSourceProfileStatus OBJECT-TYPE
        SYNTAX   RowStatus
        MAX-ACCESS   read-create
        STATUS   current
        DESCRIPTION

```
            "Status of this profile.

             An entry may not exist in the active state unless all
             objects in the entry have an appropriate value.

             Once this object is set to active(1), no objects in the
             sspmSourceProfileTable can be changed."
         ::= { sspmSourceProfileEntry 18 }

   --
   -- sspmSourceControlTable
   -- Defines specific measurement instances based on template
   -- profiles in the sspmSourceProfileTable which must be
   -- pre-configured.
   --

   sspmSourceControlTable OBJECT-TYPE
       SYNTAX        SEQUENCE OF SspmSourceControlEntry
       MAX-ACCESS  not-accessible
       STATUS        current
       DESCRIPTION
           "The table of SSPM measurements configured."
       ::= { sspmSource 2 }

   sspmSourceControlEntry OBJECT-TYPE
       SYNTAX        SspmSourceControlEntry
       MAX-ACCESS  not-accessible
       STATUS        current
       DESCRIPTION
           "Details about a particular SSPM configuration."
       INDEX { sspmSourceControlInstance }
       ::= { sspmSourceControlTable 1 }

   SspmSourceControlEntry ::= SEQUENCE {
       sspmSourceControlInstance           Unsigned32,
       sspmSourceControlProfile            Integer32,
       sspmSourceControlSrc                InterfaceIndexOrZero,
       sspmSourceControlDestAddrType       InetAddressType,
       sspmSourceControlDestAddr           InetAddress,
       sspmSourceControlEnabled            TruthValue,
       sspmSourceControlTimeOut            SspmMicroSeconds,
       sspmSourceControlSamplingDist       INTEGER,
       sspmSourceControlFrequency          SspmMicroSeconds,
       sspmSourceControlFirstSeqNum        Unsigned32,
       sspmSourceControlLastSeqNum         Unsigned32,
       sspmSourceControlOwner              OwnerString,
       sspmSourceControlStorageType        StorageType,
       sspmSourceControlStatus             RowStatus
```

    }

    sspmSourceControlInstance OBJECT-TYPE
        SYNTAX   Unsigned32 (1..65535)
        MAX-ACCESS not-accessible
        STATUS   current
        DESCRIPTION
            "An arbitrary index."
         ::= { sspmSourceControlEntry 1 }

    sspmSourceControlProfile OBJECT-TYPE
        SYNTAX   Integer32 (1..65535)
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
            "A pointer to the profile (sspmSourceProfileEntry) that
             this control entry uses to define the test being
             performed."
         ::= { sspmSourceControlEntry 2 }

    sspmSourceControlSrc OBJECT-TYPE
        SYNTAX   InterfaceIndexOrZero
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
            "The ifIndex where the packet should originate from the
             probe (if it matters). A value of zero indicates that
             it does not matter and that the device decides."
         ::= { sspmSourceControlEntry 3 }

    sspmSourceControlDestAddrType OBJECT-TYPE
        SYNTAX   InetAddressType
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
            "The type of Internet address by which the destination
             is accessed."
         ::= { sspmSourceControlEntry 4 }

    sspmSourceControlDestAddr OBJECT-TYPE
        SYNTAX   InetAddress
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
            "The Internet address for the destination. The formatting
             of this object is controlled by the
             sspmSourceControlDestAddrType object above.

          When this object contains a DNS name, then the name is
          resolved to an address each time measurement is to be made.
          Further, the agent should not cache this address,
          but instead should perform the resolution prior to each
          measurement."
      ::= { sspmSourceControlEntry 5 }

   sspmSourceControlEnabled OBJECT-TYPE
       SYNTAX   TruthValue
       MAX-ACCESS read-create
       STATUS   current
       DESCRIPTION
          "When set to 'true', this test is enabled. When set to
           'false', it is disabled."
       ::= { sspmSourceControlEntry 6 }

   sspmSourceControlTimeOut OBJECT-TYPE
       SYNTAX   SspmMicroSeconds
       MAX-ACCESS read-create
       STATUS   current
       DESCRIPTION
          "Timeout value for the measurement response. If no
           response is received in the time specified, then
           the test fails."
       ::= { sspmSourceControlEntry 7 }

   sspmSourceControlSamplingDist OBJECT-TYPE
       SYNTAX   INTEGER {
                        deterministic(1),
                        poisson(2)
                   }
       MAX-ACCESS read-create
       STATUS   current
       DESCRIPTION
          "When this attribute is set to 'deterministic', then
           packets are generated at with a fixed inter-packet
           injection time specified by sspmSourceFrequency.

           When this attribute is set to 'Poisson', then packets
           are generated with inter-packet injection times sampled
           from an exponential distribution with the single
           distributional parameter determined by the inverse
           frequency)."
       ::= { sspmSourceControlEntry 8 }

   sspmSourceControlFrequency OBJECT-TYPE
       SYNTAX   SspmMicroSeconds
       MAX-ACCESS read-create

```
    STATUS         current
    DESCRIPTION
        "The inverse of this value is the rate at which packets
         are generated.  Refer to sspmSourceSamplingDistribution.
         If the value set is less than the value of
         sspmGeneralMinFrequency, then the set will fail with an
         error-status of 'inconsistentValue'."
    ::= { sspmSourceControlEntry 9 }

sspmSourceControlFirstSeqNum OBJECT-TYPE
    SYNTAX         Unsigned32
    MAX-ACCESS  read-create
    STATUS         current
    DESCRIPTION
        "The first sequence number of packets to be transmitted."
    ::= { sspmSourceControlEntry 10 }

sspmSourceControlLastSeqNum OBJECT-TYPE
    SYNTAX         Unsigned32
    MAX-ACCESS  read-only
    STATUS         current
    DESCRIPTION
        "The last sequence number transmitted.  This value is updated
         by the agent after packet generation."
    ::= { sspmSourceControlEntry 11 }

sspmSourceControlOwner OBJECT-TYPE
    SYNTAX         OwnerString
    MAX-ACCESS  read-create
    STATUS         current
    DESCRIPTION
        "Name of the management station/application that set
         up the test."
    ::= { sspmSourceControlEntry 12 }

sspmSourceControlStorageType OBJECT-TYPE
    SYNTAX         StorageType
    MAX-ACCESS  read-create
    STATUS         current
    DESCRIPTION
        "The storage type of this sspmSourceControlEntry.  If the
         value of this object is 'permanent', no objects in this row
         need to be writable."
    ::= { sspmSourceControlEntry 13 }

sspmSourceControlStatus OBJECT-TYPE
    SYNTAX         RowStatus
    MAX-ACCESS  read-create
```

```
        STATUS        current
        DESCRIPTION
            "Status of this source control entry.

            An entry may not exist in the active state unless all
            objects in the entry have an appropriate value.

            When this attribute has the value of
            'active', none of the read-write or read-create attributes
            in this table may be modified, with the exception of
            sspmSourceControlEnabled."
        ::= { sspmSourceControlEntry 14 }

 --
 -- sspmSinkTable
 --
 -- Contains attributes for configuration of Synthetic
 -- Sources for Performance Monitoring sinks, i.e.,
 -- sinks for receipt of one-way delay measurements.
 --
 sspmSink              OBJECT IDENTIFIER ::= { sspmMIBObjects 5 }

 sspmSinkTable OBJECT-TYPE
        SYNTAX        SEQUENCE OF SspmSinkEntry
        MAX-ACCESS  not-accessible
        STATUS        current
        DESCRIPTION
            "A table configuring the sink for measurements."
        ::= { sspmSink 1 }

 sspmSinkEntry OBJECT-TYPE
        SYNTAX        SspmSinkEntry
        MAX-ACCESS  not-accessible
        STATUS        current
        DESCRIPTION
            "The details of a particular sink entry.  If the measurement
             is a round-trip type, then the sink entry will be on the
             same probe as the corresponding sspmSourceEntry.  If the
             measurement is a one-way, type then the sink entry will be
             on a different probe."
        INDEX { sspmSinkInstance }
        ::= { sspmSinkTable 1}

 SspmSinkEntry ::= SEQUENCE {
        sspmSinkInstance                    Unsigned32,
        sspmSinkType                        AppLocalIndex,
        sspmSinkSourceAddressType           InetAddressType,
        sspmSinkSourceAddress               InetAddress,
```

```
        sspmSinkExpectedRate                  SspmMicroSeconds,
        sspmSinkEnable                        TruthValue,
        sspmSinkExpectedFirstSequenceNum      Unsigned32,
        sspmSinkLastSequenceNumber            Unsigned32,
        sspmSinkLastSequenceInvalid           Counter32,
        sspmSinkStorageType                   StorageType,
        sspmSinkStatus                        RowStatus
    }

    sspmSinkInstance OBJECT-TYPE
        SYNTAX      Unsigned32 (1..65535)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "An index.  When the measurement is for a round-trip
             measurement, then this table entry is on the same probe as
             the corresponding sspmSourceEntry, and the value of this
             attribute should correspond to the value of
             sspmSourceInstance.  Management applications configuring
             sinks for one-way measurements could define some
             scheme whereby the sspmSinkInstance is unique across
             all probes.  Note that the unique key to this entry is
             also constructed with sspmSinkType,
             sspmSinkSourceAddressType, and sspmSinkSourceAddress.
             To make the implementation simpler, those other
             attributes are not included in the index but uniqueness
             is still needed to receive all the packets."
         ::= { sspmSinkEntry 1 }

    sspmSinkType OBJECT-TYPE
        SYNTAX      AppLocalIndex
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The AppLocalIndex value that uniquely identifies the
             measurement per the APM-MIB.  In order to create a row
             in this table, there must be a corresponding row in the
             sspmCapabilitiesTable.  If there is no corresponding
             row in the sspmCapabilitiestable, then the agent will
             return an error-status of 'inconsistentValue'."
         ::= { sspmSinkEntry 2}

    sspmSinkSourceAddressType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The type of Internet address of the source."
```

```
        ::= { sspmSinkEntry 3 }

    sspmSinkSourceAddress OBJECT-TYPE
        SYNTAX       InetAddress
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
            "The Internet address of the source.  The formatting
            of this object is controlled by the sspmSinkSourceAddressType
            object above.

            This object should be set only to a valid device address
            that has been administratively configured into the
            device.  If a set attempts to set this object to an
            address that does not belong (i.e., is not administratively
            configured into the device), the set should fail, and the
            agent should return a error-status of 'inconsistentValue'."
        ::= { sspmSinkEntry 4 }

    sspmSinkExpectedRate OBJECT-TYPE
        SYNTAX       SspmMicroSeconds
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
            "The expected rate at which packets will arrive."
        ::= { sspmSinkEntry 5 }

    sspmSinkEnable OBJECT-TYPE
        SYNTAX       TruthValue
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
            "Indicates if the sink is enabled or not."
        ::= { sspmSinkEntry 6 }

    sspmSinkExpectedFirstSequenceNum OBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
            "The expected first sequence number of packets.
             This is used by the sink to determine if packets
             were lost at the initiation of the test."
        ::= { sspmSinkEntry 7 }

    sspmSinkLastSequenceNumber OBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESS   read-only
```

```
        STATUS        current
        DESCRIPTION
            "The last sequence number received."
        ::= { sspmSinkEntry 8 }

    sspmSinkLastSequenceInvalid OBJECT-TYPE
        SYNTAX        Counter32
        MAX-ACCESS  read-only
        STATUS        current
        DESCRIPTION
            "The number of packets that arrived whose
             sequence number was not one plus the value of
             sspmSinkLastSequenceNumber."
        ::= { sspmSinkEntry 9 }

    sspmSinkStorageType OBJECT-TYPE
        SYNTAX        StorageType
        MAX-ACCESS  read-create
        STATUS        current
        DESCRIPTION
            "The storage type of this sspmSinkEntry.  If the value
             of this object is 'permanent', no objects in this row
             need to be writable."
        ::= { sspmSinkEntry 10 }

    sspmSinkStatus OBJECT-TYPE
        SYNTAX         RowStatus
        MAX-ACCESS  read-create
        STATUS        current
        DESCRIPTION
            "Status of this conceptual row.
             An entry may not exist in the active state unless all
             objects in the entry have an appropriate value.

             Once this object is set to active(1), no objects with
             MAX-ACCESS of read-create in the sspmSinkTable can
             be changed."
        ::= { sspmSinkEntry 11 }

    --
    -- Notifications
    --


    --
    -- Conformance information
    --
    sspmCompliances OBJECT IDENTIFIER ::= { sspmMIBConformance 1 }
    sspmGroups       OBJECT IDENTIFIER ::= { sspmMIBConformance 2 }
```

```
     -- Compliance Statements
     sspmGeneralCompliance MODULE-COMPLIANCE
       STATUS current
       DESCRIPTION
         "A general compliance that allows all things to be optional."
       MODULE -- this module

       MANDATORY-GROUPS { sspmGeneralGroup }

       GROUP sspmSourceGroup
       DESCRIPTION
         "The SSPM Source Group is optional."

       GROUP sspmSinkGroup
       DESCRIPTION
         "The SSPM Sink Group is optional."

       GROUP sspmUserPassGroup
       DESCRIPTION
         "The SSPM User Pass Group is optional."

       ::= { sspmCompliances 1 }

     --
     -- SSPM Source Compliance
     --
     sspmSourceFullCompliance MODULE-COMPLIANCE
       STATUS current
       DESCRIPTION
         "A source compliance.  Use this compliance when implementing
          a traffic-source-only device.  This is useful for implementing
          devices that probe other devices for intrusive application
          monitoring.  It is also useful for implementing the source
          of one-way tests used with a sink-only device."
       MODULE -- this module

       MANDATORY-GROUPS { sspmGeneralGroup, sspmSourceGroup }

       GROUP sspmUserPassGroup
       DESCRIPTION
         "The SSPM User Pass Group is optional."
       ::= { sspmCompliances 2 }

     --
     -- SSPM Sink Compliance
     --
     sspmSinkFullCompliance MODULE-COMPLIANCE
       STATUS current
```

        DESCRIPTION
          "A sink-only compliance. Use this compliance when implementing a
           sink-only device. This is useful for devices to receive one-way
           measurements."
        MODULE -- this module

        MANDATORY-GROUPS { sspmGeneralGroup, sspmSinkGroup }

      ::= { sspmCompliances 3 }

    --
    -- Groups
    --
    sspmGeneralGroup OBJECT-GROUP
        OBJECTS {
        sspmGeneralClockResolution,
        sspmGeneralClockMaxSkew,
        sspmGeneralClockSource,
        sspmGeneralMinFrequency,
        sspmCapabilitiesInstance
        }
        STATUS   current
        DESCRIPTION
            "The objects in the SSPM General Group."
        ::= { sspmGroups 1 }

    sspmSourceGroup OBJECT-GROUP
        OBJECTS {
        sspmSourceProfileType,
        sspmSourceProfilePacketSize,
        sspmSourceProfilePacketFillType,
        sspmSourceProfilePacketFillValue,
        sspmSourceProfileTOS,
        sspmSourceProfileFlowLabel,
        sspmSourceProfileLooseSrcRteFill,
        sspmSourceProfileLooseSrcRteLen,
        sspmSourceProfileTTL,
        sspmSourceProfileNoFrag,
        sspmSourceProfile8021Tagging,
        sspmSourceProfileUsername,
        sspmSourceProfilePassword,
        sspmSourceProfileParameter,
        sspmSourceProfileOwner,
        sspmSourceProfileStorageType,
        sspmSourceProfileStatus,
        sspmSourceControlProfile,
        sspmSourceControlSrc,
        sspmSourceControlDestAddrType,

```
        sspmSourceControlDestAddr,
        sspmSourceControlEnabled,
        sspmSourceControlTimeOut,
        sspmSourceControlSamplingDist,
        sspmSourceControlFrequency,
        sspmSourceControlFirstSeqNum,
        sspmSourceControlLastSeqNum,
        sspmSourceControlOwner,
        sspmSourceControlStorageType,
        sspmSourceControlStatus
        }
        STATUS       current
        DESCRIPTION
            "The objects in the SSPM Source Group."
        ::= { sspmGroups 2 }

    sspmUserPassGroup OBJECT-GROUP
        OBJECTS {
        sspmSourceProfileUsername,
        sspmSourceProfilePassword
        }
        STATUS       current
        DESCRIPTION
            "The objects in the SSPM Username and password group."
        ::= { sspmGroups 3 }

    sspmSinkGroup OBJECT-GROUP
        OBJECTS {
        sspmSinkType,
        sspmSinkSourceAddressType,
        sspmSinkSourceAddress,
        sspmSinkExpectedRate,
        sspmSinkEnable,
        sspmSinkExpectedFirstSequenceNum,
        sspmSinkLastSequenceNumber,
        sspmSinkLastSequenceInvalid,
        sspmSinkStorageType,
        sspmSinkStatus
        }
        STATUS       current
        DESCRIPTION
            "The objects in the SSPM Sink Group."
        ::= { sspmGroups 4 }

    END
```

8. Security Considerations

   This MIB module defines objects that allow packets to be injected
   into the network for the purpose of measuring some performance
   characteristics. As such, the MIB module may contain sensitive
   network and application data; e.g., user IDs and passwords. Further,
   if security is compromised, this MIB module could provide a source
   for denial-of-service, and potential other, attacks. These issues
   will be addressed within this section.

   There are a number of management objects defined in this MIB module
   that have a MAX-ACCESS clause of read-write and/or read-create. Such
   objects may be considered sensitive or vulnerable in some network
   environments. The support for SET operations in a non-secure
   environment without proper protection can have a negative effect on
   network operations. These are the tables and objects and their
   sensitivity/vulnerability:

      + The sspmSourceProfileTable contains objects that configure link-
         level, IP, and application-level data used within test suites.
         These objects with a MAX-ACCESS clause of read-write and/or
         read- create are:

           o sspmSourcePacketSize - configures the overall size of the
              test packets,

           o sspmSourceProfileTOS - sets the TOS field in the IPv4 and
              IPv6 headers,

           o sspmSourceProfileLooseSrcRteFill and
              sspmSourceProfileLooseSrcRteLen - give a list of IPv4 or IPv6
              addresses for the loose source route options in the IP
              headers,

           o sspmSourceProfileFlowLabel - sets the Flow Label in the IPv6
              header,

           o sspmSourceProfileTTL - sets the TTL field in the packet
              headers,

           o sspmSourceProfileNoFrag - sets the No Fragment bit in the
              packet headers,

           o sspmSourceProfile8021Tagging - sets the Tag field in the
              802.1 headers, and

       o sspmSourceProfileUsername and sspmSourceProfilePassword -
         these hold the ID and passwords specific to an application
         test profile.,

    + The sspmSourceControlTable contains objects that configure IP
      and application-level data used within a given test. These
      objects with a MAX-ACCESS clause of read-write and/or read-
      create are:

       o sspmSourceControlSrc - controls the source IP address used on
         the test packets,

       o sspmSourceControlDestAddr - holds the destination address for
         the specific test packet,

       o sspmSourceControlTimeout, sspmSourceControlSamplingDist, and
         sspmSourceControlFrequency - control the nature and frequency
         of the test packet injection onto the network, and

       o sspmSourceControlFirstSeqNum and sspmSourceControlLastSeqNum
         - set the first and last sequence numbers for the specific
         test.

    + The sspmSinkTable contains objects that configure the recipient
      of the test packets. As such, the objects in this table have no
      security issues related to them.

   Some attributes configure username and password information for some
   application-level protocols as indicated above. Access to these
   attributes may provide unauthorized use of resources. These
   attributes are: sspmSourceProfileUsername and
   sspmSourceProfilePassword.

   Some attributes configure the size and rate of traffic flows for the
   purpose of performance measurements. Access to these attributes may
   exacerbate the use of this MIB module in denial-of-service attacks.
   It is possible to define a maximum packet rate on the device and to
   indicate this rate through the sspmSourceFrequency object. This
   object reflects the maximum acceptable packet rate that a device
   supporting this MIB module is willing to generate. This places a
   bound on setting the test packet rate through the
   sspmSourceControlFrequency object. Other objects that control
   aspects of the test packets related to packet size and rate are
   sspmSourceControlTimeOut, sspmSourceControlSamplingDist and
   sspmSourceControlFrequency.

The objects sspmSourceControlSrc, sspmSourceControlDestAddr,
sspmSourceControlLooseSrcRteFill, and sspmSourceControlLooseSrcRteLen
control the setting of the source and destination addresses on the
packet headers and the routing of the packets. The device should not
allow the setting of source addresses on the test packets other than
those that are administratively configured onto the device. This is
controlled by using the syntax InterfaceIndexOrZero for the control
of the source address through the sspmSourceControlSrc object.

It is thus important to control even GET access to these objects and
possibly to even encrypt the values of these object when sending them
over the network via SNMP. Not all versions of SNMP provide features
for such a secure environment.

SNMP versions prior to SNMPv3 did not include adequate security.
Even if the network itself is secure (for example by using IPSec),
even then, there is no control as to who on the secure network is
allowed to access and GET/SET (read/change/create/delete) the objects
in this MIB module.

It is RECOMMENDED that implementers consider the security features as
provided by the SNMPv3 framework (see [RFC3410], section 8),
including full support for the SNMPv3 cryptographic mechanisms (for
authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT
RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to
enable cryptographic security. It is then a customer/operator
responsibility to ensure that the SNMP entity giving access to an
instance of this MIB module is properly configured to give access to
the objects only to those principals (users) that have legitimate
rights to indeed GET or SET (change/create/delete) them.

9. Acknowledgements

   This document was produced by the IETF Remote Network Monitoring
   Working Group. The editors gratefully acknowledge the comments of
   the following individuals: Andy Bierman, Lester D'Souza, Jim McQuaid,
   and Steven Waldbusser.

10. Normative References

   [RFC791]   Postel, J., "Internet Protocol", STD 5, RFC 791,
                 September 1981.

   [RFC1305]   Mills, D., "Network Time Protocol (Version 3)
                 Specification, Implementation and Analysis", RFC 1305,
                 March 1992.

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

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

   [RFC2460]   Deering, S. and R. Hinden, "Internet Protocol, Version 6
                (IPv6) Specification", RFC 2460, December 1998.

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

   [RFC2579]   McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J.,
                Rose, M., and S. Waldbusser, "Textual Conventions for
                SMIv2", STD 58, RFC 2579, April 1999.

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

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

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

   [RFC3291]   Daniele, M., Haberman, B., Routhier, S., and J.
                Schoenwaelder, "Textual Conventions for Internet Network
                Addresses ", RFC 3291, May 2002.

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

   [RFC3432]   Raisanen, V., Grotefeld, G., and A. Morton, "Network
                Performance Measurement with Periodic Streams", RFC 3432,
                November 2002.

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

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

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

11. Informative References

   [RFC1272]   Mills, C., Hirsch, G., and G. Ruth, "Internet Accounting
               Background", RFC 1272, November 1991.

   [RFC2021]   Waldbusser, S., "Remote Network Monitoring Management
               Information Base Version 2 using SMIv2", RFC 2021,
               January 1997.

   [RFC2722]   Browlee, N., Mills, C., and G. Ruth, "Traffic Flow
               Measurement: Architecture", RFC 2722, October 1999.

   [RFC2720]   Brownlee, N. "Traffic Flow Measurement: Meter MIB", RFC
               2720, October 1999.

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

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

   [RFC2594]   Hazewinkel, H., Kalbfleisch, C., and J. Schoenwaelder,
               "Definitions of Managed Objects for WWW Services", RFC
               2594, May 1999.

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

   [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.

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

   [RFC2819]   Waldbusser, S., "Remote Network Monitoring Management
               Information Base", STD 59, RFC 2819, February 1995.

   [RFC2925]   White, K., "Definitions of Managed Objects for Remote
                 Ping, Traceroute, and Lookup Operations", RFC 2925,
                 September 2000.

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

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

   [RFC3512]   MacFaden, M., Partain, D., Saperia, J., and W. Tackabury,
                 "Configuring Networks and Devices with Simple Network
                 Management Protocol (SNMP)", RFC 3512, April 2003.

   [EBT]   Mathis, M. and M. Allman, "Empirical Bulk Transfer
                 Capacity", Work in Progress, October 1999.

   [ODP]   Shalunov, S., Teitelbaum, B., and M. Zekauskas, "A One-
                 Way Delay Protocol for IP Performance Measurements", Work
                 in Progress, December 2000.

   [RFC4011]   Waldbusser, S., Saperia, J., and T. Hongal, "Policy Based
                 Management MIB", RFC 4011, March 2005.

   [TBT]   Mathis, M., "TReno Bulk transfer Capacity", Work in
                 Progress, February 1999.

Authors' Addresses

    Carl W. Kalbfleisch
    Consultant

    EMail: ietf@kalbfleisch.us

    Robert G. Cole
    Johns Hopkins University Applied Physics Laboratory
    MP2-170
    11100 Johns Hopkins Road
    Laurel, MD 20723-6099
    USA

    Tel: +1 443-778-6951
    EMail: robert.cole@jhuapl.edu

    Dan Romascanu
    Avaya
    Atidim Technology Park, Bldg. #3
    Tel Aviv, 61131
    Israel

    Tel: +972-3-645-8414
    EMail: dromasca@avaya.com

Full Copyright Statement

Intellectual Property

Acknowledgement