Syslog Working Group
INTERNET-DRAFT
Intended Status: Proposed Standard
Expires: August 8, 2008

Glenn Mansfield Keeni
Cyber Solutions Inc.

February 9, 2008

Syslog Management Information Base
<draft-ietf-syslog-device-mib-17.txt>

Status of this Memo

This document is a product of the syslog Working Group. Comments should be addressed to the authors or the mailing list at syslog@ietf.org

Copyright Notice

Abstract

This memo defines a portion of the Management Information Base (MIB), the Syslog MIB, for use with network management protocols in the Internet community. In particular, the Syslog MIB will be used to monitor and control syslog applications.

Table of Contents

1. 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].

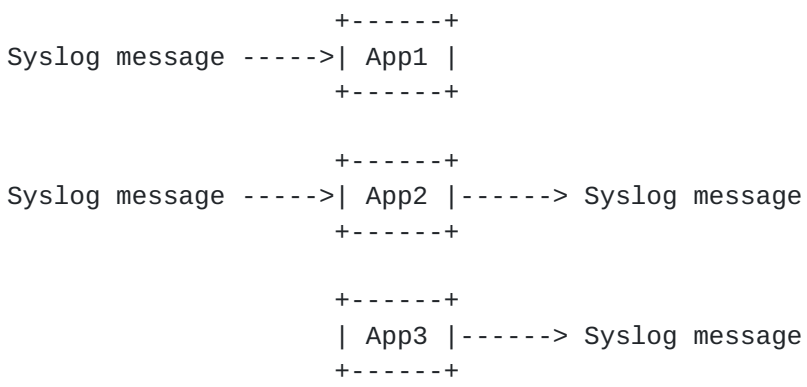
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. Background

Operating systems, processes and applications, collectively termed "facilities" in the following, generate messages indicating their own status or the occurrence of events. These messages are handled by what has come to be known as the syslog application[RFCPROT]. A syslog application sends and/or receives syslog messages. The reader is referred to [RFCPROT] for a description of the various roles of a syslog application viz. "sender", "receiver" and "relay". The discussion in this document in general applies to a generic syslog application. For special cases the specific role of the syslog application will be mentioned.

This document defines a set of managed objects (MOs) that can be used to monitor a group of syslog applications.

The SYSLOG-MIB can be used in conjunction with other MIB modules - in particular the Host Resources MIB[RFC2790]. The generic process related matters e.g. control and monitoring for status, resource usage etc. can be serviced by the corresponding entries in the Host Resources MIB.



App1: Syslog collector (syslog receiver)
App2: Syslog relay (syslog receiver, syslog sender)
App3: Syslog originator (syslog sender)

Fig.1 Syslog applications modeled by the SYSLOG-MIB

The syslog applications modeled by the SYSLOG-MIB are shown in Fig.1. A syslog receiver receives syslog messages. A syslog sender sends syslog messages to other syslog applications. A syslog relay forwards some of the received syslog messages to other syslog applications. A syslog receiver receives a syslog message and processes it. The processing will depend on the internal configuration and may involve relaying the message to one or more syslog applications. Note that a syslog application may have multiple roles. Multiple syslog applications may co-exist on the same host.

3. The MIB Design.

The purpose of the SYSLOG-MIB is to allow the monitoring of a group of syslog applications. This requires managed objects representing the following elements.

- o The configuration and status related details of each syslog application.
- o The statistics on syslog messages received, processed locally, relayed by each syslog application.

The MIB contains three subtrees.

- o The syslogNotifications subtree defines the set of notifications that will be used to asynchronously report

the change of status of a syslog application.

- o The syslogObjects subtree contains three subtrees.
  - The syslogControlTable subtree deals with the configuration and control information for a syslog application.
  - The syslogOperationsTable subtree deals with operations and statistical information about syslog messages sent and/or received by a syslog application.
- o The conformance subtree defines the compliance statements.

The SYSLOG-MIB module uses textual conventions defined in INET-ADDRESS-MIB[RFC4001] and SNMP-FRAMEWORK-MIB[RFC3411].

4. The Syslog MIB

```
   SYSLOG-MIB DEFINITIONS ::= BEGIN

   IMPORTS
       MODULE-IDENTITY, OBJECT-TYPE,
                 Unsigned32, Counter32, Integer32, mib-2,
                 NOTIFICATION-TYPE
                 FROM SNMPv2-SMI
       RowStatus, StorageType,
       TEXTUAL-CONVENTION, TimeStamp
                 FROM SNMPv2-TC
       InetAddressType, InetAddress, InetPortNumber
                 FROM INET-ADDRESS-MIB
       MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
                 FROM SNMPv2-CONF
       SyslogFacility, SyslogSeverity
                 FROM SYSLOG-TC-MIB
       SnmpAdminString
                 FROM SNMP-FRAMEWORK-MIB;

   syslogMIB  MODULE-IDENTITY
       LAST-UPDATED "200703040000Z"  --  4th March, 2007
       ORGANIZATION "IETF Syslog Working Group"
       CONTACT-INFO
       "                       Glenn Mansfield Keeni
                     Postal: Cyber Solutions Inc.
                             6-6-3, Minami Yoshinari
                             Aoba-ku, Sendai, Japan 989-3204.
                        Tel: +81-22-303-4012
                        Fax: +81-22-303-4015
                     E-mail: glenn@cysols.com

        Support Group E-mail: syslog@ietf.org
        "

       DESCRIPTION
           "The MIB module for monitoring syslog applications.

            A syslog application sends and/or receives syslog messages.
            The reader is referred to [RFCPROT] for a description of
            the various roles of a syslog application viz. ''sender'',
            ''receiver'' and ''relay''. The discussion in this
            document in general applies to a generic syslog application.
```

```
            For special cases the specific role of the syslog
            application will be mentioned.


            Copyright (C) The IETF Trust (2008). This version of
            this MIB module is part of RFC XXXX; see the RFC itself for
            full legal notices.
           "
      -- RFC Ed.: replace XXXX with the actual RFC number & remove this
      -- note


       REVISION "200703040000Z"  --   4th March, 2007
       DESCRIPTION
           "The initial version, published as RFC XXXX."

      -- RFC Ed.: replace XXXX with the actual RFC number & remove this
      -- note


       ::= { mib-2 YYYY }     -- Will be assigned by IANA

      -- IANA Reg.: Please assign a value for "YYYY" under the
      -- 'mib-2' subtree and record the assignment in the SMI
      -- Numbers registry.

      -- RFC Ed.: When the above assignment has been made, please
      --     remove the above note
      --     replace "YYYY" here with the assigned value and
      --     remove this note.



   -- ---------------------------------------------------------
   -- Textual Conventions
   -- ---------------------------------------------------------
```

```
   SyslogRoles ::=  TEXTUAL-CONVENTION
       STATUS  current
       DESCRIPTION
           "This textual convention enumerates the roles of a
            syslog application. Note that a syslog application can
            have multiple roles.
           "
       REFERENCE
           "The Syslog Protocol [RFCPROT] sec. 3.
           "
       SYNTAX      BITS
             {
               sender    (0),
               receiver  (1),
               relay     (2)
             }

   SyslogEncapsulation  ::=  TEXTUAL-CONVENTION
       STATUS  current
       DESCRIPTION
           "This textual convention enumerates the encapsulations
            of the syslog message that is used between syslog
            application endpoints.
           "
       REFERENCE
           "Transmission of syslog messages over UDP [RFCUDPX],
            TLS Transport Mapping for Syslog [RFCTLSX],
            Reliable Delivery for syslog [RFC3195].
           "
       SYNTAX  INTEGER
            {
              other           (1),
              none            (2),  -- [RFCUDPX] (no encapsulation)
              tls             (3),  -- [RFCTLSX]
              beep            (4)   -- [RFC3195]
            }

   -- syslogMIB - the main groups
   -- ------------------------------------------------------------

   syslogNotifications       OBJECT IDENTIFIER
                         ::= { syslogMIB 0 }

   syslogObjects             OBJECT IDENTIFIER
                         ::= { syslogMIB 1 }
```

```
   syslogConformance         OBJECT IDENTIFIER
                          ::= { syslogMIB 3 }


   -- ------------------------------------------------------------
   -- syslog application configuration info table
   -- ------------------------------------------------------------
   syslogControlTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF SyslogControlEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "A table containing the configuration parameters
            pertaining to the syslog applications serviced by an
            SNMP agent.
           "
       ::= { syslogObjects 1 }

   syslogControlEntry OBJECT-TYPE
       SYNTAX      SyslogControlEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The configuration parameters pertaining to a syslog
            application.
           "
       INDEX  { syslogControlIndex }
       ::= { syslogControlTable 1 }
```

```
   SyslogControlEntry ::=
       SEQUENCE {
           syslogControlIndex
                Unsigned32,
           syslogControlDescr
                SnmpAdminString,
           syslogControlRoles
                SyslogRoles,
           syslogControlBindAddrType
                InetAddressType,
           syslogControlBindAddr
                InetAddress,
           syslogControlBindPort
                InetPortNumber,
           syslogControlEncapsulation
                SyslogEncapsulation,
           syslogControlMaxMessageSize
                Unsigned32,
           syslogControlConfFileName
                SnmpAdminString,
           syslogControlStorageType
                StorageType,
           syslogControlRowStatus
                RowStatus
        }


   syslogControlIndex OBJECT-TYPE
       SYNTAX      Unsigned32 (1..2147483647)
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The Index that uniquely identifies the syslog
            application in the syslogControlTable.
            The value of the index for a syslog application may
            not be the same across system reboots. Users and
            applications will need to determine the index of a
            syslog application after system reboots.
           "
       ::= { syslogControlEntry 1 }
```

```
   syslogControlDescr OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "A user definable description of the syslog application.
            This description could be used by syslog management
            applications e.g. in reports or in user interfaces.
           "
       ::= { syslogControlEntry 2 }

   syslogControlRoles OBJECT-TYPE
       SYNTAX      SyslogRoles
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The roles of the syslog application.
           "
       ::= { syslogControlEntry 3 }


   syslogControlBindAddrType OBJECT-TYPE
       SYNTAX      InetAddressType
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The type of Internet address which follows
            in syslogControlBindAddr.
            If this syslog application is not a syslog receiver,
            the value of this object will be 'unknown' (0).
           "
       ::= { syslogControlEntry 4 }

   syslogControlBindAddr OBJECT-TYPE
       SYNTAX      InetAddress
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The specific address the syslog receiver will bind to.
            The format of the address is specified by the
            corresponding syslogControlBindAddrType object.
            If the address is specified in the DNS domain name format
            [syslogControlBindAddrType = 'dns'], the
            corresponding IPv4 or IPv6 address obtained at the time
            of the binding operation by the syslog application, will be
```

```
            used.
            If this syslog application is not a syslog receiver, the
            value of this object will be a zero-length string.
           "
       ::= { syslogControlEntry 5 }

   syslogControlBindPort OBJECT-TYPE
       SYNTAX      InetPortNumber
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The port number that this syslog receiver will bind to.

            If this syslog application is not a syslog receiver the
            value of this object will be zero.
           "
       ::= { syslogControlEntry 6 }

   syslogControlEncapsulation OBJECT-TYPE
       SYNTAX      SyslogEncapsulation
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The encapsulation that will be used for syslog messages
            by the syslog receiver.

            If this syslog application is not a syslog receiver the
            value of this object will be ''other''.
           "
       ::= { syslogControlEntry 7 }


   syslogControlMaxMessageSize OBJECT-TYPE
       SYNTAX      Unsigned32
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The maximum size of the syslog messages in bytes
            for this syslog application.

            A syslog receiver may reject or truncate messages larger
            than the specified maximum syslog message size.
           "
       REFERENCE
           "The Syslog Protocol [RFCPROT] sec. 6.1.
```

```
          "
      ::= { syslogControlEntry 8 }


   syslogControlConfFileName OBJECT-TYPE
       SYNTAX       SnmpAdminString
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
         "The fullpath name of the configuration file where the
          syslog application's message selection and corresponding
          action rules will be read from.
          If the syslog application does not support the specification
          of a configuration file, the value of this object will
          be a zero-length string.
         "
       DEFVAL { "/etc/syslog.conf" }
       ::= { syslogControlEntry 9 }

   syslogControlStorageType OBJECT-TYPE
       SYNTAX       StorageType
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
           "This object defines whether the parameters defined in
            this row are kept in volatile storage and lost upon
            reboot or are backed up by non-volatile or permanent
            storage.
            Conceptual rows having the value 'permanent' need not
            allow write-access to any columnar objects in the row.
           "
       DEFVAL      { nonVolatile }
       ::= { syslogControlEntry 11 }
```

```
   syslogControlRowStatus OBJECT-TYPE
       SYNTAX      RowStatus
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object is used to create, modify and delete rows in
            the syslogControlTable.
            The value of syslogControlDescr can be changed
            when this object is in state ''active'' or in
            ''notInService''.
            The other objects in a row can be modified only when the
            value of this object in the corresponding conceptual row
            is not ''active''. Thus to modify one or more of the
            objects in this conceptual row,
              a. change the row status to ''notInService'',
              b. change the values of the row
              c. change the row status to ''active''
            The syslogControlRowStatus may be changed to
            ''active'' if all the managed objects in the conceptual
            row with MAX-ACCESS read-create except
            syslogControlBindPort and
            syslogControlEncapsulation have been assigned valid
            values.
           "
       ::= { syslogControlEntry 12 }

   -- ------------------------------------------------------------
   -- syslogOperations
   -- ------------------------------------------------------------
   syslogOperationsTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF SyslogOperationsEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "A table containing operations information about
            the syslog applications serviced by an SNMP agent.
            This table complements the (configuration) information
            in syslogControlTable .
           "
       ::= { syslogObjects 2 }
```

```
   syslogOperationsEntry OBJECT-TYPE
       SYNTAX      SyslogOperationsEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The operations information pertaining to a syslog
            application.
           "
       AUGMENTS  { syslogControlEntry }
       ::= { syslogOperationsTable 1 }

   SyslogOperationsEntry ::=
       SEQUENCE {
           syslogOperationsMsgsReceived
                Counter32,
           syslogOperationsMsgsTransmitted
                Counter32,
           syslogOperationsMsgsRelayed
                Counter32,
           syslogOperationsMsgsDropped
                Counter32,
           syslogOperationsMsgsMalFormed
                Counter32,
           syslogOperationsMsgsDiscarded
                Counter32,
           syslogOperationsLastMsgRecdTime
                TimeStamp,
           syslogOperationsLastMsgTransmittedTime
                TimeStamp,
           syslogOperationsStartTime
                TimeStamp,
           syslogOperationsLastError
                SnmpAdminString,
           syslogOperationsLastErrorTime
                TimeStamp,
           syslogOperationsRunIndex
                Integer32,
           syslogOperationsCounterDiscontinuityTime
                TimeStamp,
           syslogOperationsStatus
                INTEGER
       }
```

```
   syslogOperationsMsgsReceived OBJECT-TYPE
       SYNTAX      Counter32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The number of messages received by the syslog
            receiver. This includes messages that were discarded.
            If this syslog application is not a syslog receiver the
            value of this object will be zero.
            Discontinuities in the value of this counter can
            occur at re-initialization of the management system,
            and at other times as indicated by the value of
            syslogOperationsCounterDiscontinuityTime.
           "
       ::= { syslogOperationsEntry 1 }

   syslogOperationsMsgsTransmitted OBJECT-TYPE
       SYNTAX      Counter32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The number of messages transmitted by the syslog
            sender. This does not include the messages that could
            not be queued for transmission by the syslog sender.
            If this syslog application is not a syslog sender the
            value of this object will be zero.
            Discontinuities in the value of this counter can
            occur at re-initialization of the management system,
            and at other times as indicated by the value of
            syslogOperationsCounterDiscontinuityTime.
           "
       ::= { syslogOperationsEntry 2 }

   syslogOperationsMsgsRelayed OBJECT-TYPE
       SYNTAX      Counter32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The number of messages relayed by the syslog
            relay to other syslog applications.
            If this syslog application is not a syslog relay the value
            of this object will be zero.
            Discontinuities in the value of this counter can
            occur at re-initialization of the management system,
            and at other times as indicated by the value of
```

```
            syslogOperationsCounterDiscontinuityTime.
           "
       REFERENCE
           "The Syslog Protocol [RFCPROT] sec. 3.
           "
       ::= { syslogOperationsEntry 3 }

   syslogOperationsMsgsDropped OBJECT-TYPE
       SYNTAX      Counter32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The number of messages that could not be queued
            for transmission by the syslog sender.
            If this syslog application is not a syslog sender the
            value of this object will be zero.
            Discontinuities in the value of this counter can
            occur at re-initialization of the management system,
            and at other times as indicated by the value of
            syslogOperationsCounterDiscontinuityTime.
           "
       ::= { syslogOperationsEntry 4 }

   syslogOperationsMsgsMalFormed OBJECT-TYPE
       SYNTAX      Counter32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The number of messages received by the syslog
            receiver which had malformed header.
            If this syslog application is not a syslog receiver,
            then this object will have a zero value.
            Discontinuities in the value of this counter can
            occur at re-initialization of the management system,
            and at other times as indicated by the value of
            syslogOperationsCounterDiscontinuityTime.
           "
       REFERENCE
           "The Syslog Protocol [RFCPROT] sec. 6.3.
           "
       ::= { syslogOperationsEntry 5 }
```

```
   syslogOperationsMsgsDiscarded OBJECT-TYPE
       SYNTAX      Counter32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The number of messages that were discarded by the
            syslog receiver. This will include messages that
            were discarded because the message size was greater
            than the system's maximum message size.
            If this syslog application is not a syslog receiver this
            object will have a zero value.
            Discontinuities in the value of this counter can
            occur at re-initialization of the management system,
            and at other times as indicated by the value of
            syslogOperationsCounterDiscontinuityTime.
           "
       REFERENCE
           "The Syslog Protocol [RFCPROT] sec. 6.1.
           "
       ::= { syslogOperationsEntry 6 }

   syslogOperationsLastMsgRecdTime OBJECT-TYPE
       SYNTAX      TimeStamp
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The value of sysUpTime when the last message was
            received by the syslog receiver.
            If this syslog application is not a syslog receiver or,
            if no messages have been received by this syslog
            application, since the last re-initialization of the
            local SNMP management subsystem, then this object
            will have a zero value.
           "
       ::= { syslogOperationsEntry 7 }

   syslogOperationsLastMsgTransmittedTime OBJECT-TYPE
       SYNTAX      TimeStamp
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The value of sysUpTime when the last message
            was transmitted by the syslog sender.
            If this syslog application is not a syslog sender or,
            if no messages have been transmitted by this syslog
```

```
            application, since the last re-initialization of the local
            management subsystem, then this object will have a
            zero value.
           "
       ::= { syslogOperationsEntry 8 }


   syslogOperationsStartTime OBJECT-TYPE
       SYNTAX      TimeStamp
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The value of sysUpTime when this syslog application was
            started.
           "
       ::= { syslogOperationsEntry 9 }

   syslogOperationsLastError OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "A description of the last error related to sending,
            receiving or processing a syslog message that was
            encountered by this syslog application.
            If no error has been encountered by this syslog
            application then the value of this object will be a
            zero-length string.
            If no error has been encountered by this syslog
            application since the last re-initialization of the
            local management subsystem then the value of this
            object will be a zero-length string.
           "
       ::= { syslogOperationsEntry 10 }

   syslogOperationsLastErrorTime OBJECT-TYPE
       SYNTAX      TimeStamp
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The value of sysUpTime when the last error was
            encountered.
            If no error has been encountered by this syslog
            application since the last re-initialization of the
            local management subsystem, then this object will
```

```
            have a zero value.
           "
       ::= { syslogOperationsEntry 11 }

   syslogOperationsRunIndex OBJECT-TYPE
       SYNTAX      Integer32 (0..2147483647)
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "If the Host resource MIB is instantiated on the
            host then this entry will have the value of the
            hrSWRunIndex of the corresponding entry in the
            hrSWRunTable.
            Note that the hrSWRunIndex is not persistent
            across system reboots or software restarts. The
            value of syslogOperationsRunIndex SHOULD
            reference the latest value of the hrSWRunIndex
            of the corresponding entry in the hrSWRunTable.

            The special value of zero indicates that the Host
            resource MIB is not instantiated.
           "
       ::= { syslogOperationsEntry 12 }


   syslogOperationsCounterDiscontinuityTime OBJECT-TYPE
       SYNTAX      TimeStamp
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
            "The value of sysUpTime on the most recent occasion
             at which any one or more of this syslog application's
             counters, viz., counters with OID prefix
             'syslogOperationsMsgsReceived' or
             'syslogOperationsMsgsTransmitted' or
             'syslogOperationsMsgsRelayed' or
             'syslogOperationsMsgsDropped' or
             'syslogOperationsMsgsMalFormed' or
             'syslogOperationsMsgsDiscarded' suffered a
             discontinuity.
             If no such discontinuities have occurred since the
             last re-initialization of the local management
             subsystem, then this object will have a zero value.
            "
       ::= { syslogOperationsEntry 13 }
```

```
   syslogOperationsStatus OBJECT-TYPE
       SYNTAX       INTEGER  {
                         unknown  (1),
                         started  (2),
                         suspended(3),
                         stopped  (4)
                       }
       MAX-ACCESS   read-only
       STATUS       current
       DESCRIPTION
           "The status of the syslog application.
           "
       DEFVAL      { unknown }
       ::= { syslogOperationsEntry 14 }

   syslogPriorityTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF SyslogPriorityEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "A table containing the relay configuration
            parameters pertaining to the syslog applications
            serviced by an SNMP agent.
           "
       ::= { syslogObjects 3 }

   syslogPriorityEntry OBJECT-TYPE
       SYNTAX      SyslogPriorityEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The relay configuration parameters pertaining to
            a syslog application.
           "
       INDEX  { syslogControlIndex,
                syslogPriorityFacility,
                syslogPrioritySeverity }
       ::= { syslogPriorityTable 1 }
```

```
   SyslogPriorityEntry ::=
       SEQUENCE {
           syslogPriorityFacility
                SyslogFacility,
           syslogPrioritySeverity
                SyslogSeverity,
           syslogPriorityDescr
                SnmpAdminString,
           syslogPriorityDestinationIndex
                Unsigned32,
           syslogPriorityStorageType
                StorageType,
           syslogPriorityRowStatus
                RowStatus
       }

   syslogPriorityFacility OBJECT-TYPE
       SYNTAX      SyslogFacility
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The facility value of this entry.
           "
       ::= { syslogPriorityEntry 1 }

   syslogPrioritySeverity OBJECT-TYPE
       SYNTAX      SyslogSeverity
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The severity value of this entry.
           "
       ::= { syslogPriorityEntry 2 }

   syslogPriorityDescr OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "A textual description of this priority entry.
           "
       ::= { syslogPriorityEntry 3 }
```

```
   syslogPriorityDestinationIndex OBJECT-TYPE
       SYNTAX      Unsigned32
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "On systems where the priority value in a syslog message
            indicates the destination to which a syslog message
            should be relayed, the value of this object will identify
            the row in syslogRelayTable that contains
            information about the relay destination to which
            messages which have the priority value represented by
            syslogPriorityFacility and syslogPrioritySeverity values
            of this row will be relayed.
            A value of 0 will indicate that there is no corresponding
            row in the syslogRelayTable table.
           "
       ::= { syslogPriorityEntry 4 }

   syslogPriorityStorageType OBJECT-TYPE
       SYNTAX       StorageType
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
           "This object defines whether the parameters defined in
            this row are kept in volatile storage and lost upon
            reboot or are backed up by non-volatile or permanent
            storage.
            Conceptual rows having the value 'permanent' need not
            allow write-access to any columnar objects in the row.
           "
       DEFVAL      { nonVolatile }
       ::= { syslogPriorityEntry 5 }
```

```
   syslogPriorityRowStatus OBJECT-TYPE
       SYNTAX      RowStatus
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object is used to create, modify and delete rows
            in the syslogPriorityTable.
            The value of syslogPriorityDescr can be changed
            when this object is in state ''active'' or in
            ''notInService''.
            The other objects in a row can be modified only when the
            value of this object in the corresponding conceptual row
            is not ''active''. Thus to modify one or more of the
            objects in this conceptual row,
              a. change the row status to ''notInService'',
              b. change the values of the row
              c. change the row status to ''active''
            The syslogPriorityRowStatus may be changed to
            ''active'' if all the managed objects in the conceptual
            row with MAX-ACCESS read-create have been assigned valid
            values.
           "
       ::= { syslogPriorityEntry 6 }


   syslogRelayTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF SyslogRelayEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "A table containing information for the relay
            destinations.
           "
       ::= { syslogObjects 4 }

   syslogRelayEntry OBJECT-TYPE
       SYNTAX      SyslogRelayEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The information pertaining to a syslog message
            relay destination.
           "
       INDEX  { syslogRelayIndex }
       ::= { syslogRelayTable 1 }
```

```
   SyslogRelayEntry ::=
       SEQUENCE {
           syslogRelayIndex
                Unsigned32,
           syslogRelayDescr
                SnmpAdminString,
           syslogRelayAddrType
                InetAddressType,
           syslogRelayAddr
                InetAddress,
           syslogRelayPort
                InetPortNumber,
           syslogRelayEncapsulation
                SyslogEncapsulation,
           syslogRelayMsgsRelayed
                Counter32,
           syslogRelayCounterDiscontinuityTime
                TimeStamp,
           syslogRelayStorageType
                StorageType,
           syslogRelayRowStatus
                RowStatus
       }


   syslogRelayIndex OBJECT-TYPE
       SYNTAX      Unsigned32 (1..2147483647)
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The Index that uniquely identifies the syslog
            relay in the syslogRelayTable.
            The value of the index for a syslog relay may
            not be the same across system reboots. Users and
            applications will need to determine the index of a
            syslog relay after system reboots.
           "
       ::= { syslogRelayEntry 1 }
```

```
   syslogRelayDescr OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "A user definable description of the syslog relay.
            This description could be used by syslog management
            applications e.g. in reports or in user interfaces.
           "
       ::= { syslogRelayEntry 2 }

   syslogRelayAddrType OBJECT-TYPE
       SYNTAX      InetAddressType
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The type of Internet address which follows
            in syslogRelayAddr.
           "
       ::= { syslogRelayEntry 3 }

   syslogRelayAddr OBJECT-TYPE
       SYNTAX      InetAddress
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The address of the syslog relay .
            The format of the address is specified by the
            corresponding syslogRelayAddrType object.
            If the address is specified in the DNS domain name format
            [syslogRelayAddrType = 'dns'], the
            corresponding IPv4 or IPv6 address obtained at the time
            of the relay operation by the syslog application, will be
            used.
           "
       ::= { syslogRelayEntry 4 }
```

```
   syslogRelayPort OBJECT-TYPE
       SYNTAX      InetPortNumber
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The port number of the syslog relay.
           "
       ::= { syslogRelayEntry 5 }

   syslogRelayEncapsulation OBJECT-TYPE
       SYNTAX      SyslogEncapsulation
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The encapsulation that will be used for syslog messages
            sent by the syslog sender to the relay destination.
           "
       ::= { syslogRelayEntry 6 }

   syslogRelayMsgsRelayed OBJECT-TYPE
       SYNTAX      Counter32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
           "The number of messages relayed by the syslog
            relay to this relay destination.
            Discontinuities in the value of this counter can
            occur at re-initialization of the management system,
            and at other times as indicated by the value of
            syslogRelayCounterDiscontinuityTime.
           "
       REFERENCE
           "The Syslog Protocol [RFCPROT] sec. 3.
           "
       ::= { syslogRelayEntry 7 }

   syslogRelayCounterDiscontinuityTime OBJECT-TYPE
       SYNTAX      TimeStamp
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
            "The value of sysUpTime on the most recent occasion
             at which counters with OID prefix
             'syslogRelayMsgsRelayed' suffered a
             discontinuity.
```

```
            If no such discontinuities have occurred since the
            last re-initialization of the local management
            subsystem, then this object will have a zero value.
           "
      ::= { syslogRelayEntry 8 }

   syslogRelayStorageType OBJECT-TYPE
       SYNTAX       StorageType
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
           "This object defines whether the parameters defined in
            this row are kept in volatile storage and lost upon
            reboot or are backed up by non-volatile or permanent
            storage.
            Conceptual rows having the value 'permanent' need not
            allow write-access to any columnar objects in the row.
           "
       DEFVAL      { nonVolatile }
       ::= { syslogRelayEntry 9 }

      syslogRelayRowStatus OBJECT-TYPE
          SYNTAX      RowStatus
          MAX-ACCESS  read-create
          STATUS      current
          DESCRIPTION
              "This object is used to create, modify and delete rows
               in the syslogRelayTable.
               The value of syslogRelayDescr can be changed
               when this object is in state ''active'' or in
               ''notInService''.
               The other objects in a row can be modified only when the
               value of this object in the corresponding conceptual row
               is not ''active''. Thus to modify one or more of the
               objects in this conceptual row,
                 a. change the row status to ''notInService'',
                 b. change the values of the row
                 c. change the row status to ''active''
               The syslogRelayRowStatus may be changed to
               ''active'' if all the managed objects in the conceptual
               row with MAX-ACCESS read-create have been assigned valid
               values.
              "
          ::= { syslogRelayEntry 10 }
```

```
   syslogStatusChanged NOTIFICATION-TYPE
       OBJECTS   {
                    syslogControlDescr,
                    syslogControlRoles,
                    syslogControlBindAddrType,
                    syslogControlBindAddr,
                    syslogControlBindPort,
                    syslogControlEncapsulation,
                    syslogControlConfFileName,
                    syslogOperationsStatus
                 }
       STATUS    current
       DESCRIPTION
               "This notification is sent when a syslog application
                changes state. For example when the syslog application
                starts [syslogOperationsStatus is ''started'' ]
                or the syslog application stops [syslogOperationsStatus
                is ''suspended'' or ''stopped''].
                The value of syslogOperationsStatus will be the
                new status of the syslog application after the change.
                The syslog application corresponding to the notification
                will be identified by the syslogOperationsIndex
                instance identifier of the objects in the notification.
               "
       ::= { syslogNotifications 1 }



   -- ---------------------------------------------------------------
   -- Conformance Information
   -- ---------------------------------------------------------------

   syslogGroups OBJECT IDENTIFIER
                            ::= { syslogConformance 1 }

   syslogCompliances OBJECT IDENTIFIER
                            ::= { syslogConformance 2 }
```

```
   -- ------------------------------------------------------------
   -- units of conformance
   -- ------------------------------------------------------------

   syslogOperationsGroup OBJECT-GROUP
       OBJECTS {
               --  syslogOperationsIndex,
                   syslogOperationsMsgsReceived,
                   syslogOperationsMsgsTransmitted,
                   syslogOperationsMsgsRelayed,
                   syslogOperationsMsgsDropped,
                   syslogOperationsMsgsMalFormed,
                   syslogOperationsMsgsDiscarded,
                   syslogOperationsLastMsgRecdTime,
                   syslogOperationsLastMsgTransmittedTime,
                   syslogOperationsStartTime,
                   syslogOperationsLastError,
                   syslogOperationsLastErrorTime,
                   syslogOperationsRunIndex,
                   syslogOperationsCounterDiscontinuityTime,
                   syslogOperationsStatus
               }
       STATUS  current
       DESCRIPTION
           "A collection of objects providing message related
            statistics."
       ::= { syslogGroups 1}
```

```
   syslogControlGroup OBJECT-GROUP
       OBJECTS {
                   syslogControlDescr,
                   syslogControlRoles,
                   syslogControlBindAddrType,
                   syslogControlBindAddr,
                   syslogControlEncapsulation,
                   syslogControlBindPort,
                   syslogControlMaxMessageSize,
                   syslogControlConfFileName,
                   syslogControlStorageType,
                   syslogControlRowStatus
               }
       STATUS  current
       DESCRIPTION
           "A collection of objects representing the run time parameters
            for the syslog applications.
           "
       ::= { syslogGroups 2}

   syslogPriorityGroup OBJECT-GROUP
       OBJECTS {
                   syslogPriorityDescr,
                   syslogPriorityDestinationIndex,
                   syslogPriorityStorageType,
                   syslogPriorityRowStatus
               }
       STATUS  current
       DESCRIPTION
           "A collection of objects representing the priority
            groupings of syslog messages.
           "
       ::= { syslogGroups 3}
```

```
   syslogRelayGroup OBJECT-GROUP
       OBJECTS {
                   syslogRelayDescr,
                   syslogRelayAddrType,
                   syslogRelayAddr,
                   syslogRelayPort,
                   syslogRelayEncapsulation,
                   syslogRelayMsgsRelayed,
                   syslogRelayCounterDiscontinuityTime,
                   syslogRelayStorageType,
                   syslogRelayRowStatus
               }
       STATUS  current
       DESCRIPTION
           "A collection of objects representing the relay
            destinations for syslog messages.
           "
       ::= { syslogGroups 4}


   syslogNotificationGroup NOTIFICATION-GROUP
       NOTIFICATIONS {
                   syslogStatusChanged
               }
       STATUS  current
       DESCRIPTION
           "A collection of notifications about the operational
            state of a syslog application.
           "
       ::= { syslogGroups 5}
```

```
   -- ------------------------------------------------------------
   -- compliance statements
   -- ------------------------------------------------------------

   syslogFullCompliance1 MODULE-COMPLIANCE
       STATUS  current
       DESCRIPTION
           "The compliance statement for SNMP entities which
            implement the SYSLOG-MIB with support for writable
            objects and notifications. Such an implementation can
            be both monitored and configured via SNMP. It can
            also send notifications about change in the
            operational status of the syslog application.
           "
       MODULE -- this module
       MANDATORY-GROUPS {
           syslogNotificationGroup,
           syslogOperationsGroup,
           syslogControlGroup,
           syslogPriorityGroup,
           syslogRelayGroup
       }

       ::= { syslogCompliances 1 }

   syslogFullCompliance2 MODULE-COMPLIANCE
       STATUS  current
       DESCRIPTION
           "The compliance statement for SNMP entities which
            implement the SYSLOG-MIB with support for writable
            objects. Such an implementation can
            be both monitored and configured via SNMP.
           "
       MODULE -- this module
       MANDATORY-GROUPS {
           syslogOperationsGroup,
           syslogControlGroup,
           syslogPriorityGroup,
           syslogRelayGroup
       }

       ::= { syslogCompliances 2 }

   syslogFullCompliance3 MODULE-COMPLIANCE
       STATUS  current
```

```
        DESCRIPTION
            "The compliance statement for SNMP entities which
             implement the SYSLOG-MIB with support for writable
             objects but without support for the objects in
             syslogPriorityGroup and syslogRelayGroup. Such an
             implementation can be both monitored and configured
             via SNMP.
            "
        MODULE -- this module
        MANDATORY-GROUPS {
            syslogOperationsGroup,
            syslogControlGroup
        }

        ::= { syslogCompliances 3 }

    syslogReadOnlyCompliance1 MODULE-COMPLIANCE
        STATUS  current
        DESCRIPTION
            "The compliance statement for SNMP entities which
             implement the syslog MIB without support
             for read-write (i.e. in read-only mode). It can
             also send notifications about change in the
             operational status of the syslog application.
            "
        MODULE -- this module
        MANDATORY-GROUPS {
            syslogNotificationGroup,
            syslogOperationsGroup,
            syslogControlGroup,
            syslogPriorityGroup,
            syslogRelayGroup
        }

        OBJECT  syslogControlDescr
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlRoles
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
```

```
        OBJECT  syslogControlBindAddrType
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlBindAddr
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlBindPort
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlEncapsulation
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlMaxMessageSize
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlConfFileName
        MIN-ACCESS   read-only
        DESCRIPTION
          "Write access is not required.
          "
        OBJECT  syslogControlStorageType
        MIN-ACCESS   read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlRowStatus
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "

        ::= { syslogCompliances 4 }
```

```
   syslogReadOnlyCompliance2 MODULE-COMPLIANCE
       STATUS  current
       DESCRIPTION
           "The compliance statement for SNMP entities which
            implement the syslog MIB without support
            for read-write (i.e. in read-only mode).
           "
       MODULE -- this module
       MANDATORY-GROUPS {
           syslogOperationsGroup,
           syslogControlGroup,
           syslogPriorityGroup,
           syslogRelayGroup
       }

       OBJECT  syslogControlDescr
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlRoles
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlBindAddrType
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlBindAddr
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlBindPort
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlEncapsulation
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
```

```
        OBJECT  syslogControlMaxMessageSize
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlConfFileName
        MIN-ACCESS   read-only
        DESCRIPTION
          "Write access is not required.
          "
        OBJECT  syslogControlStorageType
        MIN-ACCESS   read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlRowStatus
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogPriorityDescr
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogPriorityDestinationIndex
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogPriorityStorageType
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogPriorityRowStatus
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogRelayDescr
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
```

```
        OBJECT  syslogRelayAddrType
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogRelayAddr
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogRelayPort
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogRelayEncapsulation
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogRelayStorageType
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogRelayRowStatus
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        ::= { syslogCompliances 5 }
```

```
   syslogReadOnlyCompliance3 MODULE-COMPLIANCE
       STATUS  current
       DESCRIPTION
           "The compliance statement for SNMP entities which
            implement the syslog MIB without support
            for read-write (i.e. in read-only mode) and without
            support for the objects in syslogRelayGroup and
            syslogPriorityGroup.
           "
       MODULE -- this module
       MANDATORY-GROUPS {
           syslogOperationsGroup,
           syslogControlGroup
       }

       OBJECT  syslogControlDescr
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlRoles
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlBindAddrType
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlBindAddr
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlBindPort
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
       OBJECT  syslogControlEncapsulation
       MIN-ACCESS  read-only
       DESCRIPTION
           "Write access is not required.
           "
```

```
        OBJECT  syslogControlMaxMessageSize
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlConfFileName
        MIN-ACCESS   read-only
        DESCRIPTION
          "Write access is not required.
          "
        OBJECT  syslogControlStorageType
        MIN-ACCESS   read-only
        DESCRIPTION
            "Write access is not required.
            "
        OBJECT  syslogControlRowStatus
        MIN-ACCESS  read-only
        DESCRIPTION
            "Write access is not required.
            "
        ::= { syslogCompliances 6 }

    syslogNotificationCompliance MODULE-COMPLIANCE
        STATUS  current
        DESCRIPTION
            "The compliance statement for SNMP entities
             which implement the SYSLOG-MIB and support
             only notifications about change in the
             operational status of a syslog application.
            "
        MODULE -- this module
        MANDATORY-GROUPS {
            syslogNotificationGroup
        }

        ::= { syslogCompliances 7 }



    END
```

5. Security Considerations

Syslog plays a very important role in the computer and network security of an organization. SYSLOG-MIB defines several managed objects that may be used to monitor, configure and control syslog applications. As such improper manipulation of the objects represented by this MIB may lead to an attack on an important component of the computer and network security infrastructure. The objects in syslogControlTable, syslogPriorityTable and syslogRelayTable may be misconfigured to cause syslog messages to be diverted or lost.

There are a number of management objects defined in this MIB module with 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:

- syslogControlTable: The objects in this table describe the configuration of the syslog applications. It may be misconfigured to start up a very large number of syslog applications (processes) and deny the system of its resources.
- syslogControlBindAddr: This object may be misconfigured to bind syslog application to the wrong address. This will cause messages to be lost.
- syslogControlBindPort : This object may be misconfigured to bind syslog application to the wrong service (port). This will cause messages to be lost.
- syslogControlMaxMessageSize: This message may be misconfigured to set the wrong MaxMessageSize for the syslog application. It may cause syslog messages to be lost.
- syslogControlConfFileName: This object may be misconfigured to start the syslog application with the wrong (rogue) configuration.
- syslogControlStorageType: This object may be misconfigured to set the wrong storage type. That may cause confusion, operational errors and/or loss of information.
- syslogPriorityTable: The objects in this table link the priority value in a syslog message to the

entry in the syslogRelayTable corresponding to the syslog collector to which the syslog message should be relayed. The table may be misconfigured to redirect a syslog message to a potentially non-existent wrong destination and/or to redirect a large number of messages to a particular syslog collector.

- o syslogRelayTable: The rows in this table represent the relays to which syslog messages will be relayed, depending on the priority value in the respective syslog messages. The table may be misconfigured to redirect a syslog message to a potentially non-existent wrong destination and/or redirect a large number of messages to a particular syslog collector.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

- o syslogOperationsTable: Objects in this table carry sensitive information. The counters may reveal information about the deployment and effectiveness of the relevant security systems. The counters may be analyzed to tell whether the security systems are able to detect an event or not.

- o syslogOperationsLastError: This object may contain sensitive information e.g. user-id, password etc. depending on the implementation of the syslog application. It may reveal details about the syslog implementation itself, e.g. version, OS etc.

- o syslogPriorityTable: Objects in this table carry sensitive information. The objects reveal how the syslog messages are grouped, relayed and/or stored.

- o syslogRelayTable: Objects in this table carry sensitive information. The objects reveal the destination of syslog messages.

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 application 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.

6. IANA Considerations

The MIB modules in this document use the following IANA-assigned OBJECT IDENTIFIER values recorded in the SMI Numbers registry:

Descriptor	OBJECT IDENTIFIER value
syslogMIB	{ mib-2 YYYY }

IANA Reg.: Please assign a value under the 'mib-2' subtree for the 'syslogMIB' MODULE-IDENTITY and record the assignment in the SMI Numbers registry.

RFC Ed.: When the above assignments have been made, please
- remove the above note
- replace "YYYY" here with the assigned values and
- remove this note.

7. References

7.1 Normative References

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

[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

[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.

[RFC4001] Daniele, M., Haberman, B., Routhier, S., and Schoenwaelder, J., "Textual Conventions for Internet Network Addresses", RFC 4001, February 2005.

[RFCPROT] Gerhards, R., "The syslog Protocol", draft-ietf-syslog-protocol-21.txt, work in progress, June 2006.

[RFCUDPX] Okmianski, A., "Transmission of syslog messages over UDP", draft-ietf-syslog-transport-udp-09.txt work in progress, May 2006.

[RFCTLSX] Miao, F., and Yuzhi, M., "TLS Transport Mapping for Syslog", draft-ietf-syslog-transport-tls-10.txt, work in progress, December 2006.

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

7.2 Informative References

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

[RFC2790] Waldbusser, S., and Grillo, P., "Host Resources MIB", RFC 2790, March 2000.

Note: The strings "PROT", "UDPX" and "TLSX" in this document will be replaced by the RFC numbers assigned to the latest versions of
draft-ietf-syslog-protocol-*.txt,
draft-ietf-syslog-transport-udp-*.txt and
draft-ietf-syslog-transport-tls-*.txt,
respectively, and this note will be removed.

8. Acknowledgments

The initial draft of this document was authored by Bruno Pape.
The authors would like to thank Mark Ellison, David Harrington, Mike MacFaden, Dave T Perkins, Tom Petch, Juergen Schoenwaelder, Rohit M, Bert Wijnen and members of the WIDE-netman group for their comments and suggestions.

9. Author's Addresses

Glenn Mansfield Keeni
Cyber Solutions Inc.
6-6-3 Minami Yoshinari
Aoba-ku, Sendai 989-3204
Japan

Phone: +81-22-303-4012
EMail: glenn@cysols.com

10. Full Copyright Statement

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

APPENDIX

This section documents the development of the draft. It will be deleted when the draft becomes an RFC.

Revision History:
Changes from draft-ietf-syslog-device-mib-15.txt
to draft-ietf-syslog-device-mib-16.txt

1. **The definitions of the TEXTUAL-CONVENTIONS** SyslogFacility and SyslogSeverity are deleted. These are now imported from SYSLOG-TC-MIB
2. **Two tables**
   syslogPriorityTable and
   syslogRelayTable
   have been added.
3. **The compliance statements corresponding the new tables are added.**
4. **The Security considerations corresponding to the new yables are added.**

Changes from draft-ietf-syslog-device-mib-14.txt
to draft-ietf-syslog-device-mib-15.txt

1. **Revised syslogControlService to represent only a port number, and not a service name**
   Renamed syslogControlService to syslogControlBindPort
2. **Eliminated "entity" wording and used "syslog application".**
3. **The default objects are removed.**

```
+--syslogSystem(1)
|  +-- syslogDefaultService(1)
|  +-- syslogDefaultEncapsulation(2)
```

and the corresponding conformance group

```
+--syslogGroups(1)
|  +--syslogDefaultGroup(1)
```

4. **Descriptions of objects that had references to the default objects are revised.**

5. **The Textual Conventions for SyslogSeverity and SyslogFacility are put back. (This did not happen in -14.txt though it is** listed in the changes.)

6. **The references in the MIB module have been revised to make the MIB module references independent of the container** document.

7. Noted that the strings "PROT", "UDPX" and "TLSX" in this document will be replaced by the respective RFC numbers assigned to the corresponding documents.

Changes from draft-ietf-syslog-device-mib-13.txt
to draft-ietf-syslog-device-mib-14.txt

1. Changed the object hierarchy and naming from

```
   |
   +--syslogObjects(1)
   |  |
   |  +--syslogSystem(1)
   |  |
   |  +--syslogEntity(2)
   |     |
   |     +--syslogEntityControlTable(1)
   |     |
   |     +--syslogEntityOperationsTable(2)
```

to

```
   |
   +--syslogObjects(1)
   |  |
   |  +--syslogSystem(1)
   |  |
   |  +--syslogControlTable(2)
   |  |
   |  +--syslogOperationsTable(3)
   |
```

2. Removed the reference to UDP transport in section 2.
3. Put back SyslogSeverity and SyslogFacility TCs.
4. Revised the DESCRIPTION of syslogOperationsMsgsReceived
5. Added syslogOperationsMsgsTransmitted
6. Revised the DESCRIPTION of syslogOperationsLastMsgRecdTime
7. Renamed syslogOperationsReference to syslogOperationsRunIndex

Changes from draft-ietf-syslog-device-mib-12.txt
to draft-ietf-syslog-device-mib-13.txt

1. Removed reference to RFC3164.
2. Added TC SyslogEncapsulation

removed syslogDefaultTransportDomain,
syslogEntityControlTransportDomain
Added syslogDefaultEncapsulation,
syslogEntityControlEncapsulation

3. Modified the DESCRIPTION clauses for
syslogEntityControlMaxMessageSize,
syslogEntityOperationsMsgsReceived,
syslogEntityOperationsMsgsRelayed,
syslogEntityOperationsMsgsIllFormed,
syslogEntityOperationsMsgsIgnored,

4. Changed name
from syslogEntityOperationsMsgsIllFormed
to syslogEntityOperationsMsgsMalFormed

from syslogEntityOperationsMsgsIgnored
to syslogEntityOperationsMsgsDiscarded

5. Revised figure 1.

6. Added MO syslogEntityControlRoles

7. renamed syslogEntityControlStatus to
syslogEntityOperationsStatus
moved this object from
syslogEntityControlEntry to
syslogEntityOperationsEntry

8. Removed MOs syslogDefaultFacility
syslogDefaultSeverity

9. Removed TCs SyslogFacility
SyslogSeverity

10. Added the TC SyslogRoles

11. Added the MO syslogEntityControlRoles

12. Replaced references to "local time" by "value
of sysUpTime"
13. Revised the DESCRIPTION syslogEntityStatusChange

14. Revised the DESCRIPTION of the MOs to cover the
exception cases.

15. Revised the text to clear ambiguities about the role of the "syslog entity".
16. Editorial nits.

Changes from draft-ietf-syslog-device-mib-11.txt
to draft-ietf-syslog-device-mib-12.txt

1. Added text in introduction and in the DESCRIPTION of the MIB module to explain the terminology used in the document.
Ref. Comment 1.1, 1.2, 1.3, 1.4.
2. Changed "group" to "subtree" in Section 3 (The MIB Design).
Ref. Comment 1.5
3. Removed enumeration "other" from the enumeration for SyslogSeverity. This case does not arise.
Ref. Comment 1.6

4. Revised DESCRIPTION of syslogEntityControlStorageType
Ref. comment 2.3
5. Revised DESCRIPTION of syslogEntityStatusChanged
Ref. Comment 2.4
6. Updated the boilerplate for the Copyright notice.
Ref. Comment 2.7

7. Changed "should" to "SHOULD" in DESCRIPTION of syslogEntityOperationsReference
Ref. Comment 3.2
8. Changed RFCPROT to "[RFCPROT]" in REFERENCE of syslogDefaultTransportDomain

Changes from draft-ietf-syslog-device-mib-9.txt
to draft-ietf-syslog-device-mib-11.txt
[Note: The changes to the mib-9.txt and mib-10.txt are consolidated below.]
1. Namings changed:
Page-8.
changed the duplicate instances of auth and cron to
auth1, auth2, cron1, cron2
changed: SyslDevOpsEntry -> SyslogEntityOperationsEntry
syslEntOpsEntry -> syslogEntityOperationsEntry
SyslDevCtlEntry -> SyslogEntityControlEntry
syslEntCtlEntry -> syslogEntityControlEntry
syslEntOpsTable -> syslogEntityOperationsTable
syslogDevice -> syslogDevice
syslEntCtlProcDescr -> syslogEntityControlDescr
syslEntOpsLastMsgDeliveredTime ->

syslogEntityOperationsLastMsgTransmittedTime.
syslDevOpsGroup -> syslogEntityOperationsGroup

2. Added TRANSPORT-ADDRESS-MIB[RFC3419] to the text on section 3
(and 7.1 Normative References).

3. MIB.
Fixed MIB nits.

4. Added text about the expected persistency behaviour of the read-write objects in the corresponding DESCRIPTION clauses.
syslogDefaultTransport
syslogDefaultService
syslogDefaultFacility
syslogDefaultSeverity

5. Replaced
syslogDefaultTransport OBJECT-TYPE
SYNTAX TransportAddressType
and
syslEntCtlTransport OBJECT-TYPE
SYNTAX TransportAddressType
by
syslogDefaultTransportDomain OBJECT-TYPE
SYNTAX TransportDomain
syslogEntityControlTransportDomain OBJECT-TYPE
SYNTAX TransportDomain

6. Changed the ordering of
syslEntOpsTable ::= { syslogDevice 1 }
syslEntCtlTable ::= { syslogDevice 2 }
to
syslogEntityControlTable ::= { syslogEntity 1 }
syslogEntityOperationsTable ::= { syslogEntity 2 }

7. The tree structure is changed
from

```
syslogSystem              OBJECT IDENTIFIER
                ::= { syslogMIB 1 }

syslogDevice              OBJECT IDENTIFIER
                ::= { syslogMIB 2 }
```

to,

```
  syslogObjects             OBJECT IDENTIFIER
                    ::= { syslogMIB 1 }

  syslogSystem              OBJECT IDENTIFIER
                    ::= { syslogObjects 1 }

  syslogEntity              OBJECT IDENTIFIER
                    ::= { syslogObjects 2 }
```

8. **syslogEntityOperationsEntry AUGMENTS** { syslogEntityControlEntry }

9. **Added**
syslogEntityOperationsCounterDiscontinuityTime OBJECT-TYPE

to indicate whether
'syslogEntityOperationsMsgsReceived' or
'syslogEntityOperationsMsgsRelayed' or
'syslogEntityOperationsMsgsDropped' or
'syslogEntityOperationsMsgsIllFormed' or
'syslogEntityOperationsMsgsIgnored' suffered a
discontinuity.

Revised the DESCRIPTION of the above Objects.

10. **Changed all references of "syslog process", "syslog device" to** "syslog entity".

11. **Changed syntax of syslogEntityOperationsReference from**
syslEntOpsReference OBJECT-TYPE
SYNTAX Integer32
to
syslogEntityOperationsReference OBJECT-TYPE
SYNTAX Integer32 (0..2147483647)

12. **Revised the DESCRIPTION clauses of**
syslogEntityControlTable
syslogEntityOperationsReference
syslogEntityControlBindAddrType
syslogEntityControlBindAddr
syslogEntityControlTransportDomain
syslogEntityControlService
syslogEntityControlConfFileName
syslogEntityControlStatus
syslogEntityControlRowStatus
syslogEntityOperationsTable

syslogEntityControlTable
syslogEntityOperationsMsgsDropped
syslogEntityOperationsReference
syslogEntityControlEntry

13. **Added** DEFVAL { nonVolatile } to syslogEntityControlStorageType

14. **Merged the NOTIFICATIONs**
syslEntStarted
syslEntStopped
into syslogEntityStatusChanged

15. **Overhauled the syslogCompliance tree**

16. **idnits fixed.**

17. **IANA considerations section revised.**

17. **Labels and Captions in figure 1 are revised.**

18. **Revised DESCRIPTION clauses of**
SyslogSeverity
syslogDefaultFacility
syslogDefaultSeverity

19. **syslogDefaultMaxMessageSize is deleted**
revised the DESCRIPTION of syslogEntityControlMaxMessageSize

20. **editorial fixes**

The changes upto draft-ietf-syslog-device-mib-9.txt are documented below in the form of MIB Revision clauses.

```
    REVISION "200609040000Z"  --  9th September 2006
    DESCRIPTION
        "
        o The draft has been aligned with the current
          standards track documents syslog-protocol-17.txt
          and syslog-transport-udp-07.txt: the REFERNCE
          clauses have changed.
        o The TEXTUAL-CONVENTION SyslogTransport has been
          replaced by the TransportAddressType.
        o The TEXTUAL-CONVENTION SyslogFacility and
          SyslogSeverity have been aligned with
          syslog-protocol-17.txt
```

```
        o A paragraph has been added to list the related
          MIBs from which MOS and TEXTUAL-CONVENTIONs have
          been imported.
        o The target of this MIB is now called a syslog
          entity. [ Earlier it was referred to as a syslog
          device.] The prefix syslDev has been changed to
          syslEnt
        o The DEFVALS have been aligned with the reference
          documents.
        o The REFERENCE section has been updated.
        o The OID for syslogConformance has been changed
          from 4 to 3.
        "

    REVISION "200607250000Z"  -- 25th July 2006
    DESCRIPTION
        "the internet draft's version number has
         been changed (7->8).
        "

    REVISION "200511250000Z"  -- 25th November 2005
    DESCRIPTION
        "A near complete overhaul of the MIB and the document.
         The BSD-syslog flavor has been abandoned in favor of a
         more generic syslog-protocol document that is under
         preparation.
         TBD. The reference clauses need to be redone once the
              new syslog document is ready.

         List of authors changed. Original draft author Bruno
         Pape is acknowledged in the Acknowledgments section.

         Editorial nits fixed.
        "

    REVISION "200406160000Z"  -- Mon Feb       16 00:00 GMT 2004
    DESCRIPTION
        "Major change.
             The configuration parts have been removed.

         Updated the description clauses.

         Editorial nits fixed.
        "
```

```
    REVISION "200306250000Z"  -- Wed June      25 00:00 GMT 2003
    DESCRIPTION
        "Changed the type of
             syslogProcLastError            SnmpAdminString,
             from Integer32.

         DEFVAL { 0 ] is added to syslogAllowedHostsMaskLen

         MO name changed from
         syslogCtlSelectionHostname to syslogCtlSelectionHostName

         Updated the description clauses.

         Fixed nits pointed out in Bert's mails of 20030319 and
         revised the document wrt the guidelines in
         draft-ietf-ops-mib-review-guidelines-01.txt

         Editorial nits fixed.
        "

    REVISION "200303030000Z"  -- Mon March     03 00:00 GMT 2003
    DESCRIPTION
        "Fixing of nits in descriptions, addition of references,
         addition of the following MOs
             syslogProcMsgsIllFormed        Counter32,
             syslogProcStartTime            TimeStamp,
             syslogProcLastError            Integer32,
             syslogProcLastErrorTime        TimeStamp,
             syslDevCtlStorageType        StorageType,
             syslogCtlFwdActionSrcAddrType  InetAddressType,
             syslogCtlFwdActionSrcAddr      InetAddress,
         added enumeration ''suspended(2)'' to
             syslDevCtlStatus.
        "

    REVISION "200212252343Z"  -- Wed December  25 23:43 GMT 2002
    DESCRIPTION
        "Radical revision of the MIB structure and design."

    REVISION "200206061841Z"  -- Thu Jun  6 18:41 GMT 2002
    DESCRIPTION
        "The initial version of this MIB module."
```