Cisco Lawful Intercept Control MIB
draft-baker-slem-mib-00

Status of this Memo

Copyright Notice

Abstract

   Ths document describes an SNMP V3 MIB for controlling the Lawful
   Intercept architecture described in the associated document.
   Any comments on this document should be sent to:
     li-comment@external.cisco.com

Table of Contents

1. Introduction

   For a detailed overview of the documents that describe the current
   Internet-Standard Management Framework, please refer to section 7 of
   RFC 3410 [5].

   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 [1], STD 58, RFC 2579 [2], and STD 58, RFC 2580 [3].

2. Theory of Operations

The essential information described in the Lawful Intercept MIB is
the relationship between the Mediation Device and the Intercept
Access Point, and the data which is diverted into that connection.

2.1 Mediation Device Sessions

The Mediation Device, or MD, is, simply, the device which serves as a
formal interface between the parties imposing the intercept and the
network in which the intercept occurs. It is operated by a trusted
administration, by definition, and has the responsibilities of

o Configuring Intercept Access Points (IAP, usually routers and
   switches) to intercept data to it,

o Accepting that data,

o Selecting a subset of the data to report to the appropriate
   authority, and

o Delivering the data to the authority.

Each such session represents a separate and identifiable data stream,
such as the traffic to and from a particular subscriber. If there are
multiple intercepts in place for multiple agencies but requesting the
same data, it is preferable that the Mediation Device program the
Intercept Access Point to intercept the data once, and have the
Mediation Device deliver separate copied to the various agencies.
However, it is imaginable that the data streams would be sufficiently
different that it is simpler to understand them as separate intercept
orders.

A note on transports is in order. There are a number of ways to
convey information from an intercepting device to the Mediation
Device. One could simply dump Ethernet traffic onto a dedicated
Ethernet port, encapsulate in UDP, encapsulate in UDP per the
PacketCable specification, encapsulate in TCP or some other "normal"
transport, or something else. One that Cisco has looked at closely is
the use of the Nack-Oriented Retransmission feature of RTP, being
discussed in the IETF. When standardized, this has the relatively
nice attributes of being able to reliably deliver an intercepted data
stream to a Mediation Device without many of the overheads or
start-up issues of a TCP session.

The key attributes of a session between a Mediation Device and an
Intercept Access Point are:

   Content ID: An identifier for the MD<->IAP Session.

   Destination Address Type: The type of address for the MD (IPv4 or
      IPv6).

   Destination Address: The address of the MD.

   Destination Port: The UDP port number to which data is sent.

   Source Interface: The interface (hardware and address) the IAP will
      use to transmit the data.

   RTCP Port: If RTP NOR is used (future), the port number used for RTCP
      messages

   DSCP: The DSCP that intercept data will carry.

   Data Stream Type: If RTP NOR is used (future), the data type for
      data.

   Retransmission Stream Type: If RTP NOR is used (future), the data
      type for retransmissions.

   Time-out: The interval after which a session is dropped if
      communication to the MD is lost.

   Transport: The transport protocol used for intercepted data.

   Notification Enable: Whether notifications are in use for this
      session.

   Status: Controls to activate and de-activate sessions with the
      Mediation Device.

2.2 Intercepted Data Streams

   The data stream intercepted to the MD on a particular IAP must be
   specified. Depending on the relevant law and warrant, it may be
   necessary to intercept all data on a specified interface, all IP or
   Ethernet data to or from a specified address, or something as
   specific as a single voice out of a teleconference. The tables which
   describe this data are referred to as "stream tables". In this MIB,
   we show a stream table for IP traffic and a stream table for Ethernet
   traffic; other stream tables are possible as well. The key elements
   of every stream table are:

Content ID: The Content ID of the Session with the MD that this data
    stream is associated with.

Index: An enumeration of the data stream itself (there might be
    several).

N-Tuple: Parameters that permit selection of the data stream
    according to the relevant architecture.

Intercept Enable: It may be appropriate to enable and disable
    interception of a given data stream.

Intercepted packet counter: Counts packets intercepted in this data
    stream.

Intercepted Packet Drops: Counts packets that matched the criterion
    but could not be intercepted.

Status: Controls to activate and de-activate streams.

[3](#). The Management Information Base

```
-- *****************************************************************
-- CISCO-TAP-MIB.my:  Cisco intercept ("tap") MIB
--
-- December 2001, Fred Baker
-- July 2002, Edward Pham
--
-- Copyright (c) 2001-2002 by Cisco Systems, Inc.
-- All rights reserved.
--
-- *****************************************************************
-- $Log:
--
-- *****************************************************************
-- $Endlog$
--

CISCO-TAP-MIB DEFINITIONS ::= BEGIN

IMPORTS
        MODULE-IDENTITY,
        OBJECT-TYPE,
        NOTIFICATION-TYPE,
        Integer32,
        Unsigned32
                FROM SNMPv2-SMI
        MODULE-COMPLIANCE,
        OBJECT-GROUP,
        NOTIFICATION-GROUP
                FROM SNMPv2-CONF
        InetAddressType,
        InetAddress,
        InetAddressPrefixLength,
        InetPortNumber
                FROM INET-ADDRESS-MIB
        RowStatus,
        TruthValue,
        DateAndTime,
        MacAddress
                FROM SNMPv2-TC
        SnmpAdminString
                FROM SNMP-FRAMEWORK-MIB
        InterfaceIndexOrZero
                FROM IF-MIB
        Dscp
                FROM CISCO-QOS-PIB-MIB
```

```
            ciscoMgmt
                   FROM CISCO-SMI;

   cTapMIB MODULE-IDENTITY
           LAST-UPDATED  "200207250000Z"
           ORGANIZATION  "Cisco Systems, Inc."
           CONTACT-INFO
                  "       Cisco Systems
                          Customer Service

                  Postal:170 W. Tasman Drive
                          San Jose, CA  95134
                          USA

                     Tel:+1 800 553-NETS

                  E-mail:li-comment@cisco.com"
           DESCRIPTION
                  "This module manages Cisco's intercept feature."
           REVISION        "200207250000Z"
           DESCRIPTION
                  "Initial version of this MIB module."
           ::= { ciscoMgmt 252 }

   cTapMIBNotifications OBJECT IDENTIFIER ::= { cTapMIB 0 }
   cTapMIBObjects        OBJECT IDENTIFIER ::= { cTapMIB 1 }
   cTapMIBConformance    OBJECT IDENTIFIER ::= { cTapMIB 2 }

   cTapMediationGroup    OBJECT IDENTIFIER ::= { cTapMIBObjects 1 }
   cTapStreamGroup       OBJECT IDENTIFIER ::= { cTapMIBObjects 2 }
   cTapDebugGroup        OBJECT IDENTIFIER ::= { cTapMIBObjects 3 }

   -- cTapMediationNewIndex is defined to allow a network manager
   -- to create a new Mediation Table entry and its corresponding
   -- Stream Table entries without necessarily knowing what other
   -- entries might exist.

   cTapMediationNewIndex OBJECT-TYPE
       SYNTAX     Integer32 (1..2147483647)
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "This object contains a value which may be used as an index
          value for a new cTapMediationEntry. Whenever read, the agent
          will change the value to a new non-conflicting value.  This is
          to reduce the probability of errors during creation of new
          cTapMediationTable entries."
       ::= { cTapMediationGroup 1 }
```

```
   -- The Tap Mediation Table lists the applications, by address and
   -- port number, to which traffic may be intercepted. These may be
   -- on the same or different Mediation Devices.

   cTapMediationTable OBJECT-TYPE
       SYNTAX     SEQUENCE OF CTapMediationEntry
       MAX-ACCESS not-accessible
       STATUS     current
       DESCRIPTION
          "This table lists the Mediation Devices with which the
          intercepting device communicates. These may be on the same or
          different Mediation Devices.

          This table is written by the Mediation Device, and is always
          volatile. This is because intercepts may disappear during a
          restart of the intercepting equipment."
       ::= { cTapMediationGroup 2 }

   cTapMediationEntry OBJECT-TYPE
       SYNTAX     CTapMediationEntry
       MAX-ACCESS not-accessible
       STATUS     current
       DESCRIPTION
          "The entry describes a single session maintained with an
          application on a Mediation Device."
       INDEX     { cTapMediationContentId }
       ::= { cTapMediationTable 1 }

   CTapMediationEntry ::= SEQUENCE {
           cTapMediationContentId          Integer32,
           cTapMediationDestAddressType    InetAddressType,
           cTapMediationDestAddress        InetAddress,
           cTapMediationDestPort           InetPortNumber,
           cTapMediationSrcInterface       InterfaceIndexOrZero,
           cTapMediationRtcpPort           InetPortNumber,
           cTapMediationDscp               Dscp,
           cTapMediationDataType           Integer32,
           cTapMediationRetransmitType     Integer32,
           cTapMediationTimeout            DateAndTime,
           cTapMediationTransport          INTEGER,
           cTapMediationNotificationEnable TruthValue,
           cTapMediationStatus             RowStatus
   }

   cTapMediationContentId OBJECT-TYPE
       SYNTAX     Integer32 (1..2147483647)
       MAX-ACCESS not-accessible
       STATUS     current
```

        DESCRIPTION
            "cTapMediationContentId is a session identifier, from the
            intercept application's perspective, and a content identifier
            from the Mediation Device's perspective. The Mediation Device
            is responsible for making sure these are unique, although the
            SNMP RowStatus row creation process will help by not allowing
            it to create conflicting entries. Before creating a new entry,
            a value for this variable may be obtained by reading
            cTapMediationNewIndex to reduce the probability of a value
            collision."
        ::= { cTapMediationEntry 1 }

    cTapMediationDestAddressType OBJECT-TYPE
        SYNTAX   InetAddressType
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
            "The type of cTapMediationDestAddress."
        ::= { cTapMediationEntry 2 }

    cTapMediationDestAddress OBJECT-TYPE
        SYNTAX   InetAddress
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
            "The IP Address of the Mediation Device's network interface
            to which to direct intercepted traffic."
        ::= { cTapMediationEntry 3 }

    cTapMediationDestPort OBJECT-TYPE
        SYNTAX   InetPortNumber
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
            "The port number on the Mediation Device's network interface
            to which to direct intercepted traffic."
        ::= { cTapMediationEntry 4 }

    cTapMediationSrcInterface OBJECT-TYPE
        SYNTAX   InterfaceIndexOrZero
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
            "The interface on the intercepting device from which to
            transmit intercepted data. If zero, any interface may be used
            according to normal IP practice."
        ::= { cTapMediationEntry 5 }

```
cTapMediationRtcpPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS read-only
    STATUS      current
    DESCRIPTION
       "The port number on the intercepting device to which the
       Mediation Devices directs RTCP Receiver Reports and Nacks.
       This object is only relevant when the value of
       cTapMediationTransport is 'rtpNack'.

       This port is assigned by the intercepting device, rather than
       by the Mediation Device or manager application.  The value of
       this MIB object has no effect before activating the
       cTapMediationEntry."
    ::= { cTapMediationEntry 6 }

cTapMediationDscp OBJECT-TYPE
    SYNTAX      Dscp
    MAX-ACCESS read-create
    STATUS      current
    DESCRIPTION
       "The Differentiated Services Code Point the intercepting
       device applies to the IP packets encapsulating the
       intercepted traffic."
    DEFVAL { 34 }          -- by default, AF41, code 100010
    ::= { cTapMediationEntry 7 }

cTapMediationDataType OBJECT-TYPE
    SYNTAX      Integer32 (0..127)
    MAX-ACCESS read-create
    STATUS      current
    DESCRIPTION
       "If RTP with Ack/Nack resilience is selected as a transport,
       the mediation process requires an RTP payload type for data
       transmissions, and a second RTP payload type for
       retransmissions.  This is the RTP payload type for
       transmissions.

       This object is only effective when the value of
       cTapMediationTransport is 'rtpNack'."
    DEFVAL { 0 }
    ::= { cTapMediationEntry 8 }

cTapMediationRetransmitType OBJECT-TYPE
    SYNTAX      Integer32 (0..127)
    MAX-ACCESS read-create
    STATUS      current
    DESCRIPTION
```

             "If RTP with Ack/Nack resilience is selected as a transport,
             the mediation process requires an RTP payload type for data
             transmissions, and a second RTP payload type for
             retransmissions. This is the RTP payload type for
             retransmissions.

             This object is only effective when the value of
             cTapMediationTransport is 'rtpNack'."
         DEFVAL { 0 }
         ::= { cTapMediationEntry 9 }

    cTapMediationTimeout OBJECT-TYPE
         SYNTAX   DateAndTime
         MAX-ACCESS read-create
         STATUS   current
         DESCRIPTION
             "The time at which this row and all related Stream Table rows
             should be automatically removed, and the intercept function
             cease. Since the initiating network manager may be the only
             device able to manage a specific intercept or know of its
             existence, this acts as a fail-safe for the failure or removal
             of the network manager. The object is only effective when the
             value of cTapMediationStatus is 'active'."
         ::= { cTapMediationEntry 10 }

    cTapMediationTransport OBJECT-TYPE
         SYNTAX   INTEGER {
                              udp(1),
                              rtpNack(2),
                              tcp(3),
                              sctp(4)
                     }
         MAX-ACCESS read-create
         STATUS   current
         DESCRIPTION
             "The protocol used in transferring intercepted data to the
             Mediation Device. The following protocols may be supported:
                     udp: PacketCable udp format
                     rtpNack: RTP with Nack resilience
                     tcp: TCP with head of line blocking
                     sctp: SCTP with head of line blocking "
         ::= { cTapMediationEntry 11 }

    cTapMediationNotificationEnable OBJECT-TYPE
         SYNTAX   TruthValue
         MAX-ACCESS read-create
         STATUS   current
         DESCRIPTION

```
             "This variable controls the generation of any notifications or
              informs by the MIB agent for this table entry."
          DEFVAL { true }
          ::= { cTapMediationEntry 12 }

     cTapMediationStatus OBJECT-TYPE
          SYNTAX      RowStatus
          MAX-ACCESS read-create
          STATUS      current
          DESCRIPTION
            "The status of this conceptual row. This object is used to
             manage creation, modification and deletion of rows in this
             table.

             cTapMediationTimeout may be modified at any time (even while the
             row is active). But when the row is active, the other writable
             objects may not be modified without setting its value to
             'notInService'.

             The entry may not be deleted or deactivated by setting its
             value to 'destroy' or 'notInService' if there is any associated
             entry in cTapStreamIpTable, or other such tables when such are
             defined."
          ::= { cTapMediationEntry 13 }

     --
     -- cTapMediationCapabilities
     --

     cTapMediationCapabilities  OBJECT-TYPE
          SYNTAX      BITS {
                               ipV4SrcInterface(0),
                               ipV6SrcInterface(1),
                               udp(2),
                               rtpNack(3),
                               tcp(4),
                               sctp(5)
                           }
          MAX-ACCESS read-only
          STATUS      current
          DESCRIPTION
              "This object displays the device capabilities with respect to
               certain fields in Mediation Device table. This may be dependent
               on hardware capabilities, software capabilities.
               The following values may be supported:
                   ipV4SrcInterface:  SNMP ifIndex Value may be used to select
                                      the interface (denoted by
                                      cTapMediationSrcInterface) on the
```

                                    intercepting device from which to
                                    transmit intercepted data to an IPv4
                                    address Mediation Device.

                ipV6SrcInterface: SNMP ifIndex Value may be used to select
                                    the interface (denoted by
                                    cTapMediationSrcInterface) on the
                                    intercepting device from which to
                                    transmit intercepted data to an IPv6
                                    address Mediation Device.

                udp: UDP may be used as transport protocol
                                    (denoted by cTapMediationTransport) in
                                    transferring intercepted data to the
                                    Mediation Device.

                rtcpNack: RTP with Nack resilience may be used
                                    as transport protocol (denoted by
                                    cTapMediationTransport) in transferring
                                    intercepted data to the Mediation
                                    Device.

                tcp: TCP may be used as transport protocol
                                    (denoted by cTapMediationTransport) in
                                    transferring intercepted data to the
                                    Mediation Device.

                sctp: SCTP may be used as transport protocol
                                    (denoted by cTapMediationTransport) in
                                    transferring intercepted data to the
                                    Mediation Device."
          ::= { cTapMediationGroup 3 }
    --
    -- the stream tables
    --
    -- In the initial version of the MIB, only IPv4 and IPv6 intercept is
    -- defined. It is expected that in the future other types of intercepts
    -- may be required; these will be defined in tables like the
    -- cTapStreamIpTable with appropriate attributes. Such tables, when
    -- defined, will be used by the Mediation Entry in exactly the same way
    -- that the cTapStreamIpTable is used.
    --
    -- Such Tables all belong in cTapStreamGroup.
    --

    cTapStreamCapabilities OBJECT-TYPE
         SYNTAX   BITS {
                          tapEnable(0),

```
                              interface(1),
                              ipV4(2),
                              ipV6(3),
                              l4Port(4),
                              dscp(5),
                              dstMacAddr(6),
                              srcMacAddr(7),
                              ethernetPid(8),
                              dstLlcSap(9),
                              srcLlcSap(10)
                       }
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
            "This object displays what types of intercept streams can be
            configured on this type of device. This may be dependent on
            hardware capabilities, software capabilities. The following
            fields may be supported:
                interface:   SNMP ifIndex Value may be used to select
                             interception of all data crossing an
                             interface or set of interfaces.
                tapEnable:   set if table entries with
                             cTapStreamIpInterceptEnable set to 'false'
                             are used to pre-screen packets for intercept;
                             otherwise these entries are ignored.
                ipV4:        IPv4 Address or prefix may be used to select
                             traffic to be intercepted.
                ipV6:        IPv6 Address or prefix may be used to select
                             traffic to be intercepted.
                l4Port:      TCP/UDP Ports may be used to select traffic
                             to be intercepted.
                dscp:        DSCP may be used to select traffic to be
                             intercepted.
                dstMacAddr:  Destination MAC Address may be used to select
                             traffic to be intercepted.
                srcMacAddr:  Source MAC Address may be used to select
                             traffic to be intercepted.
                ethernetPid: Ethernet Protocol Identifier may be used to
                             select traffic to be intercepted.
                dstLlcSap:   IEEE 802.2 Destination SAP may be used to
                             select traffic to be intercepted.
                srcLlcSap:   IEEE 802.2 Source SAP may be used to select
                             traffic to be intercepted."
        ::= { cTapStreamGroup 1 }
    --
    -- The 'access list' for intercepting data at the IP network
    -- layer
    --
```

```
    cTapStreamIpTable OBJECT-TYPE
        SYNTAX        SEQUENCE OF CTapStreamIpEntry
        MAX-ACCESS not-accessible
        STATUS        current
        DESCRIPTION
           "The Intercept Stream IP Table lists the IPv4 and IPv6 streams
           to be intercepted.  The same data stream may be required by
           multiple taps, and one might assume that often the intercepted
           stream is a small subset of the traffic that could be
           intercepted.

           This essentially provides options for packet selection, only
           some of which might be used. For example, if all traffic to or
           from a given interface is to be intercepted, one would
           configure an entry which lists the interface, and wild-card
           everything else.  If all traffic to or from a given IP Address
           is to be intercepted, one would configure two such entries
           listing the IP Address as source and destination respectively,
           and wild-card everything else.  If a particular voice on a
           teleconference is to be intercepted, on the other hand, one
           would extract the multicast (destination) IP address, the
           source IP Address, the protocol (UDP), and the source and
           destination ports from the call control exchange and list all
           necessary information.

           The first index indicates which Mediation Device the
           intercepted traffic will be diverted to. The second index
           permits multiple classifiers to be used together, such as
           having an IP address as source or destination. "
        ::= { cTapStreamGroup 2 }

    cTapStreamIpEntry OBJECT-TYPE
        SYNTAX     CTapStreamIpEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
           "A stream entry indicates a single data stream to be
           intercepted to a Mediation Device. Many selected data
           streams may go to the same application interface, and many
           application interfaces are supported."
        INDEX { cTapMediationContentId, cTapStreamIpIndex }
        ::= { cTapStreamIpTable 1 }

    CTapStreamIpEntry ::= SEQUENCE {
           cTapStreamIpIndex                 Integer32,
           cTapStreamIpInterface             Integer32,
           cTapStreamIpAddrType              InetAddressType,
           cTapStreamIpDestinationAddress    InetAddress,
```

```
        cTapStreamIpDestinationLength      InetAddressPrefixLength,
        cTapStreamIpSourceAddress          InetAddress,
        cTapStreamIpSourceLength           InetAddressPrefixLength,
        cTapStreamIpTosByte                Integer32,
        cTapStreamIpTosByteMask            Integer32,
        cTapStreamIpFlowId                 Integer32,
        cTapStreamIpProtocol               Integer32,
        cTapStreamIpDestL4PortMin          InetPortNumber,
        cTapStreamIpDestL4PortMax          InetPortNumber,
        cTapStreamIpSourceL4PortMin        InetPortNumber,
        cTapStreamIpSourceL4PortMax        InetPortNumber,
        cTapStreamIpInterceptEnable        TruthValue,
        cTapStreamIpInterceptedPackets     Counter32,
        cTapStreamIpInterceptDrops         Counter32,
        cTapStreamIpStatus                 RowStatus
    }

cTapStreamIpIndex OBJECT-TYPE
     SYNTAX     Integer32 (1..2147483647)
     MAX-ACCESS not-accessible
     STATUS     current
     DESCRIPTION
        "The index of the stream itself."
     ::= { cTapStreamIpEntry 1 }

cTapStreamIpInterface OBJECT-TYPE
     SYNTAX     Integer32 (-1 | 0 | 1..2147483647)
     MAX-ACCESS read-create
     STATUS     current
     DESCRIPTION
        "The ifIndex value of the interface over which traffic to be
        intercepted is received or transmitted. The interface may be
        physical or virtual. If this is the only parameter specified,
        and it is other than -1 or 0, all traffic on the selected
        interface will be chosen.

        If the value is zero, matching traffic may be received or
        transmitted on any interface.  Additional selection parameters
        must be selected to limit the scope of traffic intercepted.
        This is most useful on non-routing platforms or on intercepts
        placed elsewhere than a subscriber interface.

        If the value is -1, one or both of
        cTapStreamIpDestinationAddress and cTapStreamIpSourceAddress
        must be specified with prefix length greater than zero.
        Matching traffic on the interface pointed to by ipRouteIfIndex
        or ipCidrRouteIfIndex values associated with those values is
        intercepted, whichever is specified to be more focused than a
```

```
            default route.  If routing changes, either by operator action
            or by routing protocol events, the interface will change with
            it. This is primarily intended for use on subscriber interfaces
            and other places where routing is guaranteed to be
            symmetrical.

            In both of these cases, it is possible to have the same packet
            selected for intersection on both its ingress and egress
            interface.  Nonetheless, only one instance of the packet is
            sent to the Mediation Device.

            This value must be set when creating a stream entry, either to
            select an interface, to select all interfaces, or to select the
            interface that routing chooses. Some platforms may not
            implement the entire range of options."
        REFERENCE  "RFC 1213, RFC 2096"
        ::= { cTapStreamIpEntry 2 }

    cTapStreamIpAddrType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
            "The type of address, used in packet selection."
        DEFVAL      { ipv4 }
        ::= { cTapStreamIpEntry 3 }

    cTapStreamIpDestinationAddress OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
            "The Destination address or prefix used in packet selection.
            This address will be of the type specified in
            cTapStreamIpAddrType."
        DEFVAL      { '00000000'H } -- 0.0.0.0
        ::= { cTapStreamIpEntry 4 }

    cTapStreamIpDestinationLength OBJECT-TYPE
        SYNTAX      InetAddressPrefixLength
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
            "The length of the Destination Prefix. A value of zero causes
            all addresses to match.  This prefix length will be consistent
            with the type specified in cTapStreamIpAddrType."
        DEFVAL { 0 } -- by default, any destination address
        ::= { cTapStreamIpEntry 5 }
```

    cTapStreamIpSourceAddress OBJECT-TYPE
        SYNTAX   InetAddress
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
           "The Source Address used in packet selection. This address will
           be of the type specified in cTapStreamIpAddrType."
        DEFVAL   { '00000000'H } -- 0.0.0.0
        ::= { cTapStreamIpEntry 6 }

    cTapStreamIpSourceLength OBJECT-TYPE
        SYNTAX   InetAddressPrefixLength
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
           "The length of the Source Prefix. A value of zero causes all
           addresses to match. This prefix length will be consistent with
           the type specified in cTapStreamIpAddrType."
        DEFVAL { 0 } -- by default, any source address
        ::= { cTapStreamIpEntry 7 }

    cTapStreamIpTosByte OBJECT-TYPE
        SYNTAX   Integer32 (0..255)
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
           "The value of the TOS byte, when masked with
           cTapStreamIpTosByteMask, of traffic to be intercepted.
           If cTapStreamIpTosByte & (~cTapStreamIpTosByteMask) != 0,
           configuration is rejected."
        DEFVAL { 0 }
        ::= { cTapStreamIpEntry 8 }

    cTapStreamIpTosByteMask OBJECT-TYPE
        SYNTAX   Integer32 (0..255)
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
           "The value of the TOS byte in an IPv4 or IPv6 header is ANDed
           with cTapStreamIpTosByteMask and compared with
           cTapStreamIpTosByte.

           If the values are equal, the comparison is equal. If the mask
           is zero and the TosByte value is zero, the result is to always
           accept."
        DEFVAL { 0 } -- by default, any DSCP or other TOS byte value
        ::= { cTapStreamIpEntry 9 }

```
     cTapStreamIpFlowId OBJECT-TYPE
         SYNTAX      Integer32 (-1 | 0..1048575)
         MAX-ACCESS read-create
         STATUS      current
         DESCRIPTION
            "The flow identifier in an IPv6 header. -1 indicates that the
            Flow Id is unused."
         DEFVAL { -1 } -- by default, any flow identifier value
         ::= { cTapStreamIpEntry 10 }

     cTapStreamIpProtocol OBJECT-TYPE
         SYNTAX      Integer32 (-1 | 0..255)
         MAX-ACCESS read-create
         STATUS      current
         DESCRIPTION
            "The IP protocol to match against the IPv4 protocol number or
            the IPv6 Next- Header number in the packet. -1 means 'any IP
            protocol'."
         DEFVAL { -1 } -- by default, any IP protocol
         ::= { cTapStreamIpEntry 11 }

     cTapStreamIpDestL4PortMin OBJECT-TYPE
         SYNTAX      InetPortNumber
         MAX-ACCESS read-create
         STATUS      current
         DESCRIPTION
            "The minimum value that the layer-4 destination port number in
            the packet must have in order to match.  This value must be
            equal to or less than the value specified for this entry in
            cTapStreamIpDestL4PortMax.

            If both cTapStreamIpDestL4PortMin and cTapStreamIpDestL4PortMax
            are at their default values, the port number is effectively
            unused."
         DEFVAL { 0 } -- by default, any transport layer port number
         ::= { cTapStreamIpEntry 12 }

     cTapStreamIpDestL4PortMax OBJECT-TYPE
         SYNTAX      InetPortNumber
         MAX-ACCESS read-create
         STATUS      current
         DESCRIPTION
            "The maximum value that the layer-4 destination port number in
            the packet must have in order to match this classifier entry.
            This value must be equal to or greater than the value specified
            for this entry in cTapStreamIpDestL4PortMin.

            If both cTapStreamIpDestL4PortMin and cTapStreamIpDestL4PortMax
```

          are at their default values, the port number is effectively
          unused."
      DEFVAL { 65535 } -- by default, any transport layer port number
      ::= { cTapStreamIpEntry 13 }

  cTapStreamIpSourceL4PortMin OBJECT-TYPE
      SYNTAX   InetPortNumber
      MAX-ACCESS read-create
      STATUS   current
      DESCRIPTION
         "The minimum value that the layer-4 destination port number in
         the packet must have in order to match. This value must be
         equal to or less than the value specified for this entry in
         cTapStreamIpSourceL4PortMax.

         If both cTapStreamIpSourceL4PortMin and
         cTapStreamIpSourceL4PortMax are at their default values, the
         port number is effectively unused."
      DEFVAL { 0 } -- by default, any transport layer port number
      ::= { cTapStreamIpEntry 14 }

  cTapStreamIpSourceL4PortMax OBJECT-TYPE
      SYNTAX   InetPortNumber
      MAX-ACCESS read-create
      STATUS   current
      DESCRIPTION
         "The maximum value that the layer-4 destination port number in
         the packet must have in order to match this classifier entry.
         This value must be equal to or greater than the value specified
         for this entry in cTapStreamIpSourceL4PortMin.

         If both cTapStreamIpSourceL4PortMin and
         cTapStreamIpSourceL4PortMax are at their default values, the
         port number is effectively unused."
      DEFVAL { 65535 } -- by default, any transport layer port number
      ::= { cTapStreamIpEntry 15 }

  cTapStreamIpInterceptEnable OBJECT-TYPE
      SYNTAX   TruthValue
      MAX-ACCESS read-create
      STATUS   current
      DESCRIPTION
         "If 'true', the tap should intercept matching traffic.
         If 'false', this entry is used to pre-screen packets for
         intercept."
      DEFVAL { true }
      ::= { cTapStreamIpEntry 16 }

```
cTapStreamIpInterceptedPackets OBJECT-TYPE
    SYNTAX     Counter32
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
      "The number of packets matching this data stream specification
      that have been intercepted."
    ::= { cTapStreamIpEntry 17 }

cTapStreamIpInterceptDrops OBJECT-TYPE
    SYNTAX     Counter32
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
      "The number of packets matching this data stream specification
      that, having been intercepted, were dropped in the lawful
      intercept process."
    ::= { cTapStreamIpEntry 18 }

cTapStreamIpStatus OBJECT-TYPE
    SYNTAX     RowStatus
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
      "The status of this conceptual row. This object manages
      creation, modification, and deletion of rows in this table.
      cTapStreamIpInterceptEnable may be modified any time even the
      value of this entry rowStatus object is 'active'.  When other
      rows must be changed, cTapStreamIpStatus must be first set to
      'notInService'."
    ::= { cTapStreamIpEntry 19 }

--
-- The "access list" for intercepting data at the IEEE 802
-- link layer
--

cTapStream802Table OBJECT-TYPE
    SYNTAX      SEQUENCE OF CTapStream802Entry
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
      "The Intercept Stream 802 Table lists the IEEE 802 data streams
      to be intercepted.  The same data stream may be required by
      multiple taps, and one might assume that often the intercepted
      stream is a small subset of the traffic that could be
      intercepted.
```

          This essentially provides options for packet selection, only
          some of which might be used. For example, if all traffic to or
          from a given interface is to be intercepted, one would
          configure an entry which lists the interface, and wild-card
          everything else. If all traffic to or from a given MAC Address
          is to be intercepted, one would configure two such entries
          listing the MAC Address as source and destination respectively,
          and wild-card everything else.

          The first index indicates which Mediation Device the
          intercepted traffic will be diverted to. The second index
          permits multiple classifiers to be used together, such as
          having a MAC address as source or destination. "
      ::= { cTapStreamGroup 3 }

   cTapStream802Entry OBJECT-TYPE
       SYNTAX   CTapStream802Entry
       MAX-ACCESS not-accessible
       STATUS   current
       DESCRIPTION
          "A stream entry indicates a single data stream to be
          intercepted to a Mediation Device. Many selected data
          streams may go to the same application interface, and many
          application interfaces are supported."
       INDEX { cTapMediationContentId, cTapStream802Index }
       ::= { cTapStream802Table 1 }

   CTapStream802Entry ::= SEQUENCE {
          cTapStream802Index   Integer32,
          cTapStream802Fields   BITS,
          cTapStream802Interface   Integer32,
          cTapStream802DestinationAddress   MacAddress,
          cTapStream802SourceAddress   MacAddress,
          cTapStream802EthernetPid   Integer32,
          cTapStream802SourceLlcSap   Integer32,
          cTapStream802DestinationLlcSap   Integer32,
          cTapStream802InterceptEnable   TruthValue,
          cTapStream802InterceptedPackets   Counter32,
          cTapStream802InterceptDrops   Counter32,
          cTapStream802Status   RowStatus
   }

   cTapStream802Index OBJECT-TYPE
       SYNTAX   Integer32 (1..2147483647)
       MAX-ACCESS not-accessible
       STATUS   current
       DESCRIPTION
          "The index of the stream itself."

```
          ::= { cTapStream802Entry 1 }

   cTapStream802Fields  OBJECT-TYPE
        SYNTAX      BITS {
                            interface(0),
                            dstMacAddress(1),
                            srcMacAddress(2),
                            ethernetPid(3),
                            dstLlcSap(4),
                            srcLlcSap(5)
                        }
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
            "This object displays what attributes must be tested to
            identify traffic which requires interception. The packet
            matches if all flagged fields match.

                interface:      indicates that traffic on the stated
                                interface is to be intercepted
                dstMacAddress: indicates that traffic destined to a
                                given address should be intercepted
                srcMacAddress: indicates that traffic sourced from a
                                given address should be intercepted
                ethernetPid:   indicates that traffic with a stated
                                Ethernet Protocol Identifier should be
                                intercepted
                dstLlcSap:     indicates that traffic with an certain
                                802.2 LLC Destination SAP should be
                                intercepted
                srcLlcSap:     indicates that traffic with an certain
                                802.2 LLC Source SAP should be
                                intercepted

            At least one of the bits has to be set in order to activate an
            entry.  If the bit is not on, the corresponding MIB object
            value has no effect, and need not be specified when creating
            the entry."
        ::= { cTapStream802Entry 2 }

   cTapStream802Interface OBJECT-TYPE
        SYNTAX      Integer32 (-1 | 0 | 1..2147483647)
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
            "The ifIndex value of the interface over which traffic to be
            intercepted is received or transmitted. The interface may be
            physical or virtual. If this is the only parameter specified,
```

and it is other than -1 or 0, all traffic on the selected
interface will be chosen.

If the value is zero, matching traffic may be received or
transmitted on any interface. Additional selection parameters
must be selected to limit the scope of traffic intercepted.
This is most useful on non-routing platforms or on intercepts
placed elsewhere than a subscriber interface.

If the value is -1, one or both of
cTapStream802DestinationAddress and cTapStream802SourceAddress
must be specified. Matching traffic on the interface pointed
to by the dot1dTpFdbPort values associated with those values is
intercepted, whichever is specified. If dot1dTpFdbPort
changes, either by operator action or by protocol events, the
interface will change with it. This is primarily intended for
use on subscriber interfaces and other places where routing is
guaranteed to be symmetrical.

In both of these cases, it is possible to have the same packet
selected for intersection on both its ingress and egress
interface. Nonetheless, only one instance of the packet is
sent to the Mediation Device.

This value must be set when creating a stream entry, either to
select an interface, to select all interfaces, or to select the
interface that bridging learns. Some platforms may not
implement the entire range of options."
        REFERENCE "RFC 1493"
        ::= { cTapStream802Entry 3 }

    cTapStream802DestinationAddress OBJECT-TYPE
        SYNTAX   MacAddress
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
          "The Destination address used in packet selection."
        ::= { cTapStream802Entry 4 }

    cTapStream802SourceAddress OBJECT-TYPE
        SYNTAX   MacAddress
        MAX-ACCESS read-create
        STATUS   current
        DESCRIPTION
          "The Source Address used in packet selection."
        ::= { cTapStream802Entry 5 }

    cTapStream802EthernetPid OBJECT-TYPE

```
        SYNTAX      Integer32 (0..65535)
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
           "The value of the Ethernet Protocol Identifier, which may be
           found on Ethernet traffic or IEEE 802.2 SNAP traffic."
        ::= { cTapStream802Entry 6 }

    cTapStream802DestinationLlcSap OBJECT-TYPE
        SYNTAX      Integer32 (0..65535)
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
           "The value of the IEEE 802.2 Destination SAP."
        ::= { cTapStream802Entry 7 }

    cTapStream802SourceLlcSap OBJECT-TYPE
        SYNTAX      Integer32 (0..65535)
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
           "The value of the IEEE 802.2 Source SAP."
        ::= { cTapStream802Entry 8 }

    cTapStream802InterceptEnable OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
            "If 'true', the tap enables interception of matching traffic.
            If cTapStreamCapabilities flag tapEnable is zero, this may not
            be set to 'false'."
        DEFVAL { true }
        ::= { cTapStream802Entry 9 }

    cTapStream802InterceptedPackets OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS read-only
        STATUS      current
        DESCRIPTION
           "The number of packets matching this data stream specification
           that have been intercepted."
        ::= { cTapStream802Entry 10 }

    cTapStream802InterceptDrops OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS read-only
        STATUS      current
```

```
        DESCRIPTION
           "The number of packets matching this data stream specification
           that, having been intercepted, were dropped in the lawful
           intercept process."
        ::= { cTapStream802Entry 11 }

   cTapStream802Status OBJECT-TYPE
        SYNTAX      RowStatus
        MAX-ACCESS read-create
        STATUS      current
        DESCRIPTION
           "The status of this conceptual row. This object manages
           creation, modification, and deletion of rows in this table.
           cTapStream802InterceptEnable can be modified any time even the
           value of this entry rowStatus object is active.  When other
           rows must be changed, cTapStream802Status must be first set to
           'notInService'."
        ::= { cTapStream802Entry 12 }


   --
   -- The debug table
   --

   cTapDebugTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF CTapDebugEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
           "A table that contains Lawful Intercept debug information
           available on this device. This table is used to map an error
           code to a text message for further information."
        ::= { cTapDebugGroup 1 }

   cTapDebugEntry OBJECT-TYPE
        SYNTAX      CTapDebugEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
           "A list of the debug messages."
        INDEX { cTapDebugIndex }
        ::= { cTapDebugTable 1 }


   CTapDebugEntry ::= SEQUENCE {
           cTapDebugIndex      Unsigned32,
           cTapDebugMessage    SnmpAdminString
   }
```

```
   cTapDebugIndex OBJECT-TYPE
        SYNTAX        Unsigned32
        MAX-ACCESS    not-accessible
        STATUS        current
        DESCRIPTION
           "Indicates an error code."
        ::= { cTapDebugEntry 1 }

   cTapDebugMessage OBJECT-TYPE
        SYNTAX        SnmpAdminString
        MAX-ACCESS    read-only
        STATUS        current
        DESCRIPTION
           "A text string contains the description of an error code."
        ::= { cTapDebugEntry 2 }




   -- notifications

   cTapMIBActive    NOTIFICATION-TYPE
        STATUS     current
        DESCRIPTION
           "This Notification is sent when an intercepting router or
           switch is first capable of intercepting a packet corresponding
           to a configured data stream. If the configured data stream is
           an IP one, the value of the corresponding cTapStreamIpStatus
           is included in this notification. If the configured data stream
           is an IEEE 802 one, the value of the corresponding
           cTapStream802Status is included in this notification.

           This notification may be generated in conjunction with the
           intercept application, which is designed to expect the
           notification to be sent as reliably as possible, e.g., through
           the use of a finite number of retransmissions until
           acknowledged, as and when such mechanisms are available; for
           example, with SNMPv3, this would be an InformRequest.  Filter
           installation can take a long period of time, during which call
           progress may be delayed."
        ::= { cTapMIBNotifications 1 }

   cTapMediationTimedOut NOTIFICATION-TYPE
        OBJECTS    { cTapMediationStatus }
        STATUS     current
        DESCRIPTION
           "When an intercept is autonomously removed by an intercepting
           device, such as due to the time specified in
```

```
            cTapMediationTimeout arriving, the device notifies the manager
            of the action."
        ::= { cTapMIBNotifications 2 }

    cTapMediationDebug NOTIFICATION-TYPE
        OBJECTS    { cTapMediationContentId, cTapDebugIndex }
        STATUS     current
        DESCRIPTION
            "When there is intervention needed due to some events related
            to entries configured in cTapMediationTable, the device
            notifies the manager of the event.

            This notification may be generated in conjunction with the
            intercept application, which is designed to expect the
            notification to be sent as reliably as possible, e.g., through
            the use of a finite number of retransmissions until
            acknowledged, as and when such mechanisms are available; for
            example, with SNMPv3, this would be an InformRequest."
        ::= { cTapMIBNotifications 3 }

    cTapStreamIpDebug NOTIFICATION-TYPE
        OBJECTS    { cTapMediationContentId, cTapStreamIpIndex,
                     cTapDebugIndex }
        STATUS     current
        DESCRIPTION
            "When there is intervention needed due to some events related
            to entries configured in cTapStreamIpTable, the device
            notifies the manager of the event.

            This notification may be generated in conjunction with the
            intercept application, which is designed to expect the
            notification to be sent as reliably as possible, e.g., through
            the use of a finite number of retransmissions until
            acknowledged, as and when such mechanisms are available; for
            example, with SNMPv3, this would be an InformRequest."
        ::= { cTapMIBNotifications 4 }

    -- conformance information

    cTapMIBCompliances OBJECT IDENTIFIER ::= { cTapMIBConformance 1 }
    cTapMIBGroups      OBJECT IDENTIFIER ::= { cTapMIBConformance 2 }

    -- compliance statement

    cTapMIBCompliance MODULE-COMPLIANCE
        STATUS  current
        DESCRIPTION
            "The compliance statement for entities which implement the
```

```
             Cisco Intercept MIB"
         MODULE          -- this module
            MANDATORY-GROUPS {
                    cTapMediationComplianceGroup,
                    cTapStreamComplianceGroup,
                    cTapMediationCpbComplianceGroup,
                    cTapNotificationGroup
             }
         ::= { cTapMIBCompliances 1 }

    -- units of conformance

    cTapMediationComplianceGroup OBJECT-GROUP
         OBJECTS {
            cTapMediationNewIndex,
            cTapMediationDestAddressType,
            cTapMediationDestAddress,
            cTapMediationDestPort,
            cTapMediationSrcInterface,
            cTapMediationRtcpPort,
            cTapMediationDscp,
            cTapMediationDataType,
            cTapMediationRetransmitType,
            cTapMediationTimeout,
            cTapMediationTransport,
            cTapMediationNotificationEnable,
            cTapMediationStatus
         }
         STATUS     current
         DESCRIPTION
            "These objects are necessary for description of the data
            streams directed to a Mediation Device."
         ::= { cTapMIBGroups 1 }

    cTapStreamComplianceGroup OBJECT-GROUP
         OBJECTS {
            cTapStreamCapabilities
         }
         STATUS     current
         DESCRIPTION
            "These objects are necessary for a description of the packets
            to select for interception."
         ::= { cTapMIBGroups 2 }

    cTapStreamIpComplianceGroup OBJECT-GROUP
         OBJECTS {
            cTapStreamIpInterface,
            cTapStreamIpAddrType,
```

```
            cTapStreamIpDestinationAddress,
            cTapStreamIpDestinationLength,
            cTapStreamIpSourceAddress,
            cTapStreamIpSourceLength,
            cTapStreamIpTosByte,
            cTapStreamIpTosByteMask,
            cTapStreamIpFlowId,
            cTapStreamIpProtocol,
            cTapStreamIpDestL4PortMin,
            cTapStreamIpDestL4PortMax,
            cTapStreamIpSourceL4PortMin,
            cTapStreamIpSourceL4PortMax,
            cTapStreamIpInterceptEnable,
            cTapStreamIpInterceptedPackets,
            cTapStreamIpInterceptDrops,
            cTapStreamIpStatus
        }
        STATUS     current
        DESCRIPTION
           "These objects are necessary for a description of IPv4 and IPv6
           packets to select for interception."
        ::= { cTapMIBGroups 3 }

   cTapStream802ComplianceGroup OBJECT-GROUP
        OBJECTS {
            cTapStream802Fields,
            cTapStream802Interface,
            cTapStream802DestinationAddress,
            cTapStream802SourceAddress,
            cTapStream802EthernetPid,
            cTapStream802SourceLlcSap,
            cTapStream802DestinationLlcSap,
            cTapStream802InterceptEnable,
            cTapStream802InterceptedPackets,
            cTapStream802InterceptDrops,
            cTapStream802Status
        }
        STATUS     current
        DESCRIPTION
           "These objects are necessary for a description of IEEE 802
           packets to select for interception."
        ::= { cTapMIBGroups 4 }

   cTapNotificationGroup NOTIFICATION-GROUP
        NOTIFICATIONS {
            cTapMIBActive,
            cTapMediationTimedOut,
            cTapMediationDebug,
```

```
             cTapStreamIpDebug
        }
        STATUS     current
        DESCRIPTION
           "These notifications are used to present status from the
           intercepting device to the Mediation Device."
        ::= { cTapMIBGroups 5 }

   cTapMediationCpbComplianceGroup OBJECT-GROUP
        OBJECTS {
           cTapMediationCapabilities
        }
        STATUS     current
        DESCRIPTION
           "These objects are necessary for a description of the
           mediation device to select for Lawful Intercept."
        ::= { cTapMIBGroups 6 }

   cTapDebugComplianceGroup OBJECT-GROUP
        OBJECTS {
           cTapDebugMessage
        }
        STATUS     current
        DESCRIPTION
           "These objects are necessary for debug information."
        ::= { cTapMIBGroups 7 }

   END
```

[4]. **Security Considerations**

   Lawful Intercept can be viewed as the direct violation of the
   privacy, and therefore of the security, of the party under
   surveillance. This is a legal matter, not a technical one; the laws
   of a country and a warrant issued by a duly appointed authority in
   that country cause the feature to be deployed and to be used.

   The presence of the capability in a certain router or switch creates
   the possibility that it can be misused, either accidentally or on
   purpose. It may be misconfigured, causing unintended data to be
   intercepted, for example, or the target may come under a denial of
   service attack, resulting in an indirect denial of service attack on
   the Mediation Device. Intercepted data, if left in the clear, may
   betray information to an unintended party. As such, it is Cisco's
   position that appropriate security measures should be used by the
   agency deploying this feature. It should use appropriate
   configuration protocols, such as SNMPv3, and appropriate privacy
   management facilities, such as IPSEC ESP, on this data. It is also
   necessary to maintain close control of the visibility of the
   configuration, as this can have harmful effects both on the
   surveillance subject if leaked, and on the investigation if leaked to
   the subject.

   The considerations of RFC 2804 [4] are very important; it is for this
   reason that Cisco did not attempt to modify existing protocols, but
   created a separate feature for the interception of relevant
   information.

5. Acknowledgements

   The authors worked among a large team of contributors at Cisco, too
   many to name here. And they might not want us to...

Normative References

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

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

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

Informative References

   [4] IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, May 2000.

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

Author's Address

   Fred Baker
   Cisco Systems
   1121 Via Del Rey
   Santa Barbara, CA 93117
   US

   Phone: +1-408-526-4257
   Fax: +1-413-473-2403
   EMail: fred@cisco.com

Intellectual Property Statement

   The IETF takes no position regarding the validity or scope of any
   intellectual property 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; neither does it represent that it
   has made any effort to identify any such rights. Information on the
   IETF's procedures with respect to rights in standards-track and
   standards-related documentation can be found in BCP-11. Copies of
   claims of rights made available for publication 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 implementors or users of this specification can
   be obtained from the IETF Secretariat.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights which may cover technology that may be required to practice
   this standard. Please address the information to the IETF Executive
   Director.

Full Copyright Statement

   HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
   MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement