Network Working Group
Request for Comments: 4131
Category: Standards Track

S. Green
Consultant
K. Ozawa
Toshiba
E. Cardona, Ed.
CableLabs
A. Katsnelson
September 2005

Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus

Status of This Memo

Copyright Notice

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines a set of managed objects for Simple Network Management Protocol (SNMP) based management of the Baseline Privacy Plus features of DOCSIS 1.1 and DOCSIS 2.0 (Data-over-Cable Service Interface Specification) compliant Cable Modems and Cable Modem Termination Systems.

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].

2. Overview

This MIB module (BPI+ MIB) provides a set of objects required for the management of the Baseline Privacy Interface Plus features of DOCSIS 1.1 and DOCSIS 2.0 Cable Modem (CM) and Cable Modem Termination System (CMTS). The specification is derived from the operational model described in the DOCSIS Baseline Privacy Interface Plus Specification [DOCSIS].

DOCSIS Baseline Privacy Plus is composed of four distinct functional and manageable areas:

- Key exchange and data encryption
- Cable modem authentication
- Multicast encryption
- Authentication of downloaded software images

This MIB module is an extension of the DOCSIS 1.0 Baseline Privacy MIB module [RFC3083] (BPI MIB), which is derived from the Operational model described in the DOCSIS Baseline Privacy Interface Specification [DOCSIS-1.0]. The original Baseline Privacy MIB structure has mostly been preserved in the Baseline Privacy Plus MIB. Please note that the referenced DOCSIS specifications only require that Cable Modems process IPv4 customer traffic. Design choices in this MIB module reflect those requirements. Future versions of the DOCSIS specifications are expected to require support for IPv6 as well.

Conventions Used in This Document

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].

2.1. Structure of the MIB

This MIB module is structured into several tables and objects.

2.1.1. Cable Modem

- The docsBpi2CmBaseTable contains authorization key exchange information for one CM MAC interface.
- The docsBpi2CmTEKTable contains traffic key exchange and data encryption information for a particular security association ID of the cable modem.
- Multicast Encryption information is maintained under Docsbpi2CmMulticastObjects. There is currently one multicast table object that manages IP multicast encryption, docsBpi2CmIpMulticastMapTable.
- Digital certificates used for cable modem authentication are accessible via docsBpi2CmDeviceCertTable.
- Cryptographic suite capabilities for a CM MAC are maintained in the docsBpi2CmCryptoSuiteTable.

2.1.2. Cable Modem Termination System

- The docsBpi2CmtsBaseTable contains default settings and summary counters for the cable modem termination system.
- The DocsBpi2CmtsAuthTable contains Authorization Key Exchange information for each CM MAC interface, as well as data from CM certificates used in cable modem authentication.
- The docsBpi2CmtsTEKTable contains traffic key exchange and data encryption information for a particular security association ID.
- Multicast Encryption information is maintained under Docsbpi2CmtsMulticastObjects. There are currently two multicast table objects. The Table docsBpi2CmtsIpMulticastMapTable is

specifically designed for IP multicast encryption, whereas docsBpi2CmtsMulticastAuthTable is meant to manage all multicast security associations.

In particular, the table docsBpi2CmtsIpMulticastMapTable defines the object docsBpi2CmtsIpMulticastMask, which could be a non-contiguous netmask; this is why the object syntax is based on the INET-ADDRESS-MIB MIB Module [RFC4001] Textual Convention InetAddress instead of InetAddressPrefixLength.

This is to facilitate the assignment of same DOCSIS Security Association ID (SAID) to one or more IPv6 multicast group IDs matching one or more IPv6 multicast scope types within an entry in this table. For example, multicast scopes labeled "unassigned" [RFC3513] may be allocated by administrators to a particular SAID, regardless of their multicast scope; such mapping transient multicast group 'Y' to SAID 'z' for ANY multicast scope. The non-contiguous netmask will be FF10:Y. See [RFC3513] for details on IPv6 multicast addressing.

- DocsBpi2CmtsCertObjects contains 2 manageable tables: one for provisioned cable modem certificates and one for certification authority certificates.

2.1.3. Common

- The docsBpi2CodeDownloadControl objects manage the authenticated software download process for a given device.

2.2. Relationship of BPI+ and BPI MIB Modules

This section describes the relationship between the BPI+ MIB module defined in this document and the BPI MIB module defined in RFC 3083 [RFC3083]. The BPI+ protocol interface is an enhancement to the BPI protocol, and it is a distinct protocol from BPI. The associated BPI+ managed objects should be considered separate from the BPI MIB objects defined in RFC 3083.

DOCSIS 1.1 and 2.0 systems implement both the BPI+ and BPI protocols to be backward compatible with 1.0 systems. For more information regarding the interoperability between BPI and BPI+ compliant systems, refer to appendix C of the DOCSIS BPI+ specification [DOCSIS]. For MIB modules requirements, refer to section 4.6.1, Figure 9, of the DOCSIS 1.1 OSSI specification [DOCSIS-1.1] and to section 7.6.1, Tables 7-9, of the DOCSIS 2.0 OSSI specification [DOCSIS-2.0].

2.3. BPI+ MIB Module Relationship with the Interfaces Group MIB

The BPI+ MIB module is the management framework of Baseline Privacy Plus Interface Specification [DOCSIS], which provides the MAC layer (Media Access Control) security services of DOCSIS through the Baseline Privacy Key Management (BPKM) protocol. The BPI+ MIB module objects are organized as extensions of the Radio Frequency (RF) Interface Management [RFC2670].

The MIB table structures of this MIB Module are extensions of the DOCSIS CATV (Community Antenna Television) MAC layer interface (DocsCableMaclayer by [IANA]). In particular, the provisions of the Interface Group MIB [RFC2863] for counter discontinuities and system re-initialization apply to CM and CMTS to validate the difference between two consecutive counter polls.

All BPI+ MIB module counters are 32 bits and are based on the minimum time to wrap up considerations of [RFC2863] and their possible frequency occurrence as BPI+ FSM (Finite State Machine) event counters. See [DOCSIS] for BPI+ FSM parameter guidelines.

3. Definitions

```
DOCS-IETF-BPI2-MIB DEFINITIONS ::= BEGIN

IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE,
        Integer32,
        Unsigned32,
        Counter32,
        mib-2
             FROM SNMPv2-SMI           -- [RFC2578]
        SnmpAdminString
             FROM SNMP-FRAMEWORK-MIB   -- [RFC3411]
        TEXTUAL-CONVENTION,
        MacAddress,
        RowStatus,
        TruthValue,
        DateAndTime,
        StorageType
             FROM SNMPv2-TC            -- [RFC2579]
        OBJECT-GROUP,
        MODULE-COMPLIANCE
             FROM SNMPv2-CONF          -- [RFC2580]
        ifIndex
             FROM IF-MIB               -- [RFC2863]
        InetAddressType,
        InetAddress
```

```
            FROM INET-ADDRESS-MIB;    -- [RFC4001]

      docsBpi2MIB    MODULE-IDENTITY
           LAST-UPDATED "200507200000Z" -- July 20, 2005
           ORGANIZATION "IETF IP over Cable Data Network (IPCDN)
                         Working Group"
           CONTACT-INFO "----------------------------------------
                        Stuart M. Green
                        E-mail: rubbersoul3@yahoo.com
                        ----------------------------------------
                        Kaz Ozawa
                        Automotive Systems Development Center
                        TOSHIBA CORPORATION
                        1-1, Shibaura 1-Chome
                        Minato-ku, Tokyo 105-8001
                        Japan
                        Phone: +81-3-3457-8569
                        Fax: +81-3-5444-9325
                        E-mail: Kazuyoshi.Ozawa@toshiba.co.jp
                        ----------------------------------------
                        Alexander Katsnelson
                        Postal:
                        Tel:    +1-303-680-3924
                        E-mail: katsnelson6@peoplepc.com
                        ----------------------------------------
                        Eduardo Cardona
                        Postal:
                        Cable Television Laboratories, Inc.
                        858 Coal Creek Circle
                        Louisville, CO 80027- 9750
                        U.S.A.
                        Tel:    +1 303 661 9100
                        Fax:    +1 303 661 9199
                        E-mail: e.cardona@cablelabs.com
                        ----------------------------------------

                     IETF IPCDN Working Group
                     General Discussion: ipcdn@ietf.org
                     Subscribe: http://www.ietf.org/mailman/listinfo/ipcdn.
                     Archive: ftp://ftp.ietf.org/ietf-mail-archive/ipcdn.
                     Co-chairs: Richard Woundy, rwoundy@cisco.com
                                Jean-Francois Mule, jfm@cablelabs.com"
           DESCRIPTION
               "This is the MIB module for the DOCSIS Baseline
                Privacy Plus Interface (BPI+) at cable modems (CMs)
                and cable modem termination systems (CMTSs).

                Copyright (C) The Internet Society (2005).  This
```

```
                version of this MIB module is part of RFC 4131; see
                the RFC itself for full legal notices."

            REVISION        "200507200000Z"  -- July 20, 2005
            DESCRIPTION
                "Initial version of the IETF BPI+ MIB module.
                 This version published as RFC 4131."
               ::= { mib-2 126 }

      -- Textual conventions

   DocsX509ASN1DEREncodedCertificate ::= TEXTUAL-CONVENTION
            STATUS    current
            DESCRIPTION
                "An X509 digital certificate encoded as an ASN.1 DER
            object."
            SYNTAX    OCTET STRING (SIZE (0..4096))

   DocsSAId ::= TEXTUAL-CONVENTION
            DISPLAY-HINT "d"
            STATUS    current
            DESCRIPTION
                 "Security Association identifier (SAID)."
            REFERENCE
                  "DOCSIS Baseline Privacy Plus Interface
            specification, Section 2.1.3, BPI+ Security
            Associations"
            SYNTAX    Integer32 (1..16383)

   DocsSAIdOrZero ::= TEXTUAL-CONVENTION
            DISPLAY-HINT "d"
            STATUS    current
            DESCRIPTION
                 "Security Association identifier (SAID).  The value
            zero indicates that the SAID is yet to be determined."
            REFERENCE
                  "DOCSIS Baseline Privacy Plus Interface
            specification, Section 2.1.3, BPI+ Security
                  Associations"
            SYNTAX    Unsigned32 (0 | 1..16383)

   DocsBpkmSAType ::= TEXTUAL-CONVENTION
            STATUS    current
            DESCRIPTION
                 "The type of security association (SA).
            The values of the named-numbers are associated
            with the BPKM SA-Type attributes:
            'primary' corresponds to code '1', 'static' to code '2',
```

```
            and 'dynamic' to code '3'.
            The 'none' value must only be used if the SA type has yet
            to be determined."
            REFERENCE
                  "DOCSIS Baseline Privacy Plus Interface
            specification, Section 4.2.2.24"
            SYNTAX    INTEGER {
                           none(0),
                           primary(1),
                           static(2),
                           dynamic(3)
                      }

   DocsBpkmDataEncryptAlg ::= TEXTUAL-CONVENTION
            STATUS    current
            DESCRIPTION
                "The list of data encryption algorithms defined for
            the DOCSIS interface in the BPKM cryptographic-suite
            parameter.  The value 'none' indicates that the SAID
            being referenced has no data encryption."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.2.20."
            SYNTAX    INTEGER {
                           none(0),
                           des56CbcMode(1),
                           des40CbcMode(2),
                           t3Des128CbcMode(3),
                           aes128CbcMode(4),
                           aes256CbcMode(5)
                      }

   DocsBpkmDataAuthentAlg ::= TEXTUAL-CONVENTION
            STATUS    current
            DESCRIPTION
                "The list of data integrity algorithms defined for the
            DOCSIS interface in the BPKM cryptographic-suite parameter.
            The value 'none' indicates that no data integrity is used for
            the SAID being referenced."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.2.20."
            SYNTAX    INTEGER {
                           none(0),
                           hmacSha196(1)
                      }

      docsBpi2MIBObjects  OBJECT IDENTIFIER ::= { docsBpi2MIB 1 }
```

```
-- Cable Modem Group

docsBpi2CmObjects OBJECT IDENTIFIER ::= { docsBpi2MIBObjects 1 }

--
-- The BPI+ base and authorization table for CMs,
-- indexed by ifIndex
--

docsBpi2CmBaseTable OBJECT-TYPE
     SYNTAX              SEQUENCE OF    DocsBpi2CmBaseEntry
     MAX-ACCESS          not-accessible
     STATUS              current
     DESCRIPTION
          "This table describes the basic and authorization-
     related Baseline Privacy Plus attributes of each CM MAC
     interface."
     ::= { docsBpi2CmObjects 1 }

docsBpi2CmBaseEntry OBJECT-TYPE
     SYNTAX              DocsBpi2CmBaseEntry
     MAX-ACCESS          not-accessible
     STATUS              current
     DESCRIPTION
          "Each entry contains objects describing attributes of
     one CM MAC interface.  An entry in this table exists for
     each ifEntry with an ifType of docsCableMaclayer(127)."
     INDEX               { ifIndex }
     ::= { docsBpi2CmBaseTable 1 }

DocsBpi2CmBaseEntry ::= SEQUENCE {
     docsBpi2CmPrivacyEnable             TruthValue,
     docsBpi2CmPublicKey                 OCTET STRING,
     docsBpi2CmAuthState                 INTEGER,
     docsBpi2CmAuthKeySequenceNumber     Integer32,
     docsBpi2CmAuthExpiresOld            DateAndTime,
     docsBpi2CmAuthExpiresNew            DateAndTime,
     docsBpi2CmAuthReset                 TruthValue,
     docsBpi2CmAuthGraceTime             Integer32,
     docsBpi2CmTEKGraceTime              Integer32,
     docsBpi2CmAuthWaitTimeout           Integer32,
     docsBpi2CmReauthWaitTimeout         Integer32,
     docsBpi2CmOpWaitTimeout             Integer32,
     docsBpi2CmRekeyWaitTimeout          Integer32,
     docsBpi2CmAuthRejectWaitTimeout     Integer32,
     docsBpi2CmSAMapWaitTimeout          Integer32,
     docsBpi2CmSAMapMaxRetries           Integer32,
     docsBpi2CmAuthentInfos              Counter32,
```

```
          docsBpi2CmAuthRequests              Counter32,
          docsBpi2CmAuthReplies               Counter32,
          docsBpi2CmAuthRejects               Counter32,
          docsBpi2CmAuthInvalids              Counter32,
          docsBpi2CmAuthRejectErrorCode       INTEGER,
          docsBpi2CmAuthRejectErrorString     SnmpAdminString,
          docsBpi2CmAuthInvalidErrorCode      INTEGER,
          docsBpi2CmAuthInvalidErrorString    SnmpAdminString
          }

     docsBpi2CmPrivacyEnable  OBJECT-TYPE
          SYNTAX              TruthValue
          MAX-ACCESS          read-only
          STATUS              current
          DESCRIPTION
               "This object identifies whether this CM is
          provisioned to run Baseline Privacy Plus."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Appendix A.1.1."
          ::= { docsBpi2CmBaseEntry 1 }

     docsBpi2CmPublicKey     OBJECT-TYPE
          SYNTAX             OCTET STRING (SIZE (0..524))
          MAX-ACCESS         read-only
          STATUS             current
          DESCRIPTION
               "The value of this object is a DER-encoded
          RSAPublicKey ASN.1 type string, as defined in the RSA
          Encryption Standard (PKCS #1), corresponding to the
          public key of the CM."

          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.4."
          ::= { docsBpi2CmBaseEntry 2 }

     docsBpi2CmAuthState OBJECT-TYPE
          SYNTAX         INTEGER   {
                         start(1),
                         authWait(2),
                         authorized(3),
                         reauthWait(4),
                         authRejectWait(5),
                         silent(6)
                       }
          MAX-ACCESS     read-only
          STATUS         current
```

```
            DESCRIPTION
                 "The value of this object is the state of the CM
            authorization FSM.  The start state indicates that FSM is
            in its initial state."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.1.2.1."
            ::= { docsBpi2CmBaseEntry 3 }

       docsBpi2CmAuthKeySequenceNumber    OBJECT-TYPE
            SYNTAX              Integer32 (0..15)
            MAX-ACCESS          read-only
            STATUS              current
            DESCRIPTION
                 "The value of this object is the most recent
            authorization key sequence number for this FSM."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.2 and 4.2.2.10."
            ::= { docsBpi2CmBaseEntry 4 }

       docsBpi2CmAuthExpiresOld OBJECT-TYPE
            SYNTAX              DateAndTime
            MAX-ACCESS          read-only
            STATUS              current
            DESCRIPTION
                 "The value of this object is the actual clock time for
            expiration of the immediate predecessor of the most recent
            authorization key for this FSM.  If this FSM has only one
            authorization key, then the value is the time of activation
            of this FSM."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.2 and 4.2.2.9."
            ::= { docsBpi2CmBaseEntry 5 }

       docsBpi2CmAuthExpiresNew OBJECT-TYPE
            SYNTAX              DateAndTime
            MAX-ACCESS          read-only
            STATUS              current
            DESCRIPTION
                 "The value of this object is the actual clock time for
            expiration of the most recent authorization key for this
            FSM."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.2 and 4.2.2.9."
            ::= { docsBpi2CmBaseEntry 6 }
```

```
docsBpi2CmAuthReset OBJECT-TYPE
     SYNTAX         TruthValue
     MAX-ACCESS     read-write
     STATUS         current
     DESCRIPTION
          "Setting this object to 'true' generates a Reauthorize
     event in the authorization FSM.  Reading this object always
     returns FALSE.

     This object is for testing purposes only, and therefore it
     is not required to be associated with a last reset
     object."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Section 4.1.2.3.4."
     ::= { docsBpi2CmBaseEntry 7 }

docsBpi2CmAuthGraceTime  OBJECT-TYPE
     SYNTAX         Integer32 (1..6047999)
     UNITS          "seconds"
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the grace time for an
     authorization key in seconds.  A CM is expected to start
     trying to get a new authorization key beginning
     AuthGraceTime seconds before the most recent authorization
     key actually expires."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Appendix A.1.1.1.3."
     ::= { docsBpi2CmBaseEntry 8 }

docsBpi2CmTEKGraceTime   OBJECT-TYPE
     SYNTAX         Integer32 (1..302399)
     UNITS          "seconds"
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the grace time for
     the TEK in seconds.  The CM is expected to start trying to
     acquire a new TEK beginning TEK GraceTime seconds before
     the expiration of the most recent TEK."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Appendix A.1.1.1.6."
     ::= { docsBpi2CmBaseEntry 9 }
```

```
docsBpi2CmAuthWaitTimeout     OBJECT-TYPE
     SYNTAX         Integer32 (1..30)
     UNITS          "seconds"
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the Authorize Wait
     Timeout in seconds."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Appendix A.1.1.1.1."
     ::= { docsBpi2CmBaseEntry 10 }

docsBpi2CmReauthWaitTimeout   OBJECT-TYPE
     SYNTAX         Integer32 (1..30)
     UNITS          "seconds"
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the Reauthorize Wait
     Timeout in seconds."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Appendix A.1.1.1.2."
     ::= { docsBpi2CmBaseEntry 11 }

docsBpi2CmOpWaitTimeout  OBJECT-TYPE
     SYNTAX         Integer32 (1..10)
     UNITS          "seconds"
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the Operational Wait
     Timeout in seconds."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Appendix A.1.1.1.4."
     ::= { docsBpi2CmBaseEntry 12 }

docsBpi2CmRekeyWaitTimeout    OBJECT-TYPE
     SYNTAX         Integer32 (1..10)
     UNITS          "seconds"
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the Rekey Wait Timeout
     in seconds."
     REFERENCE
```

```
            "DOCSIS Baseline Privacy Plus Interface Specification,
        Appendix A.1.1.1.5."
        ::= { docsBpi2CmBaseEntry 13 }

    docsBpi2CmAuthRejectWaitTimeout    OBJECT-TYPE
        SYNTAX         Integer32 (1..600)
        UNITS          "seconds"
        MAX-ACCESS     read-only
        STATUS         current
        DESCRIPTION
            "The value of this object is the Authorization Reject
        Wait Timeout in seconds."
        REFERENCE
            "DOCSIS Baseline Privacy Plus Interface Specification,
        Appendix A.1.1.1.7."
        ::= { docsBpi2CmBaseEntry 14 }

    docsBpi2CmSAMapWaitTimeout    OBJECT-TYPE
        SYNTAX         Integer32 (1..10)
        UNITS          "seconds"
        MAX-ACCESS     read-only
        STATUS         current
        DESCRIPTION
            "The value of this object is the retransmission
        interval, in seconds, of SA Map Requests from the MAP Wait
        state."
        REFERENCE
            "DOCSIS Baseline Privacy Plus Interface Specification,
        Appendix A.1.1.1.8."
        ::= { docsBpi2CmBaseEntry 15 }

    docsBpi2CmSAMapMaxRetries     OBJECT-TYPE
        SYNTAX         Integer32 (0..10)
        UNITS          "count"
        MAX-ACCESS     read-only
        STATUS         current
        DESCRIPTION
            "The value of this object is the maximum number of
        Map Request retries allowed."
        REFERENCE
            "DOCSIS Baseline Privacy Plus Interface Specification,
        Appendix A.1.1.1.9."
        ::= { docsBpi2CmBaseEntry 16 }

    docsBpi2CmAuthentInfos   OBJECT-TYPE
        SYNTAX         Counter32
        MAX-ACCESS     read-only
        STATUS         current
```

```
            DESCRIPTION
                 "The value of this object is the number of times
            the CM has transmitted an Authentication Information
            message.  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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.9."
            ::= { docsBpi2CmBaseEntry 17 }

       docsBpi2CmAuthRequests   OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the CM
            has transmitted an Authorization Request message.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.1."
            ::= { docsBpi2CmBaseEntry 18 }

       docsBpi2CmAuthReplies    OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the CM
            has received an Authorization Reply message.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.2."
            ::= { docsBpi2CmBaseEntry 19 }

       docsBpi2CmAuthRejects    OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
```

```
          DESCRIPTION
               "The value of this object is the number of times the CM
          has received an Authorization Reject message.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.3."
          ::= { docsBpi2CmBaseEntry 20 }

     docsBpi2CmAuthInvalids   OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the count of times the CM
          has received an Authorization Invalid message.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.7."
          ::= { docsBpi2CmBaseEntry 21 }

     docsBpi2CmAuthRejectErrorCode OBJECT-TYPE
          SYNTAX         INTEGER {
                                 none(1),
                                 unknown(2),
                                 unauthorizedCm(3),
                                 unauthorizedSaid(4),
                                 permanentAuthorizationFailure(8),
                                 timeOfDayNotAcquired(11)
                                 }
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the enumerated
          description of the Error-Code in the most recent
          Authorization Reject message received by the CM.  This has
          the value unknown(2) if the last Error-Code value was 0 and
          none(1) if no Authorization Reject message has been received
          since reboot."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
```

```
          Sections 4.2.1.3 and 4.2.2.15."
          ::= { docsBpi2CmBaseEntry 22 }

     docsBpi2CmAuthRejectErrorString    OBJECT-TYPE
          SYNTAX         SnmpAdminString (SIZE (0..128))
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the text string in the
          most recent Authorization Reject message received by the
          CM.  This is a zero length string if no Authorization
          Reject message has been received since reboot."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.3 and 4.2.2.6."
          ::= { docsBpi2CmBaseEntry 23 }

     docsBpi2CmAuthInvalidErrorCode     OBJECT-TYPE
          SYNTAX         INTEGER {
                                 none(1),
                                 unknown(2),
                                 unauthorizedCm(3),
                                 unsolicited(5),
                                 invalidKeySequence(6),
                                 keyRequestAuthenticationFailure(7)
                                 }
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the enumerated
          description of the Error-Code in the most recent
          Authorization Invalid message received by the CM.  This has
          the value unknown(2) if the last Error-Code value was 0 and
          none(1) if no Authorization Invalid message has been received
          since reboot."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.7 and 4.2.2.15."
          ::= { docsBpi2CmBaseEntry 24 }

     docsBpi2CmAuthInvalidErrorString   OBJECT-TYPE
          SYNTAX         SnmpAdminString (SIZE (0..128))
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the text string in the
          most recent Authorization Invalid message received by the
          CM.  This is a zero length string if no Authorization
```

```
            Invalid message has been received since reboot."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.7 and 4.2.2.6."
            ::= { docsBpi2CmBaseEntry 25 }

      --
      -- The CM TEK Table, indexed by ifIndex and SAID
      --

      docsBpi2CmTEKTable  OBJECT-TYPE
            SYNTAX         SEQUENCE OF    DocsBpi2CmTEKEntry
            MAX-ACCESS     not-accessible
            STATUS         current
            DESCRIPTION
                 "This table describes the attributes of each CM
            Traffic Encryption Key (TEK) association.  The CM maintains
            (no more than) one TEK association per SAID per CM MAC
            interface."
            ::= { docsBpi2CmObjects 2 }

      docsBpi2CmTEKEntry  OBJECT-TYPE
            SYNTAX         DocsBpi2CmTEKEntry
            MAX-ACCESS     not-accessible
            STATUS         current
            DESCRIPTION
                 "Each entry contains objects describing the TEK
            association attributes of one SAID.  The CM MUST create one
            entry per SAID, regardless of whether the SAID was obtained
            from a Registration Response message, from an Authorization
            Reply message, or from any dynamic SAID establishment
            mechanisms."
            INDEX     { ifIndex, docsBpi2CmTEKSAId }
            ::= { docsBpi2CmTEKTable 1 }

      DocsBpi2CmTEKEntry ::= SEQUENCE {
            docsBpi2CmTEKSAId                  DocsSAId,
            docsBpi2CmTEKSAType                DocsBpkmSAType,
            docsBpi2CmTEKDataEncryptAlg        DocsBpkmDataEncryptAlg,
            docsBpi2CmTEKDataAuthentAlg        DocsBpkmDataAuthentAlg,
            docsBpi2CmTEKState                 INTEGER,
            docsBpi2CmTEKKeySequenceNumber     Integer32,
            docsBpi2CmTEKExpiresOld            DateAndTime,
            docsBpi2CmTEKExpiresNew            DateAndTime,
            docsBpi2CmTEKKeyRequests           Counter32,
            docsBpi2CmTEKKeyReplies            Counter32,
            docsBpi2CmTEKKeyRejects            Counter32,
            docsBpi2CmTEKInvalids              Counter32,
```

```
          docsBpi2CmTEKAuthPends             Counter32,
          docsBpi2CmTEKKeyRejectErrorCode    INTEGER,
          docsBpi2CmTEKKeyRejectErrorString  SnmpAdminString,
          docsBpi2CmTEKInvalidErrorCode      INTEGER,
          docsBpi2CmTEKInvalidErrorString    SnmpAdminString
          }

     docsBpi2CmTEKSAId   OBJECT-TYPE
          SYNTAX         DocsSAId
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "The value of this object is the DOCSIS Security
          Association ID (SAID)."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.12."
          ::= { docsBpi2CmTEKEntry 1 }

     docsBpi2CmTEKSAType OBJECT-TYPE
          SYNTAX         DocsBpkmSAType
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the type of security
          association."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 2.1.3."
          ::= { docsBpi2CmTEKEntry 2 }

     docsBpi2CmTEKDataEncryptAlg   OBJECT-TYPE
          SYNTAX    DocsBpkmDataEncryptAlg
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the data encryption
          algorithm for this SAID."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.20."
          ::= { docsBpi2CmTEKEntry 3 }

     docsBpi2CmTEKDataAuthentAlg   OBJECT-TYPE
          SYNTAX    DocsBpkmDataAuthentAlg
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
```

```
            "The value of this object is the data authentication
          algorithm for this SAID."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.20."
          ::= { docsBpi2CmTEKEntry 4 }

     docsBpi2CmTEKState  OBJECT-TYPE
          SYNTAX         INTEGER {
                                 start(1),
                                 opWait(2),
                                 opReauthWait(3),
                                 operational(4),
                                 rekeyWait(5),
                                 rekeyReauthWait(6)
                                 }
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the state of the
          indicated TEK FSM.  The start(1) state indicates that the
          FSM is in its initial state."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.1.3.1."
          ::= { docsBpi2CmTEKEntry 5 }

     docsBpi2CmTEKKeySequenceNumber     OBJECT-TYPE
          SYNTAX              Integer32 (0..15)
          MAX-ACCESS          read-only
          STATUS              current
          DESCRIPTION
               "The value of this object is the most recent TEK
          key sequence number for this TEK FSM."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.2.10 and 4.2.2.13."
          ::= { docsBpi2CmTEKEntry 6 }

     docsBpi2CmTEKExpiresOld  OBJECT-TYPE
          SYNTAX         DateAndTime
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the actual clock time for
          expiration of the immediate predecessor of the most recent
          TEK for this FSM.  If this FSM has only one TEK, then the
          value is the time of activation of this FSM."
```

```
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.5 and 4.2.2.9."
            ::= { docsBpi2CmTEKEntry 7 }

      docsBpi2CmTEKExpiresNew  OBJECT-TYPE
            SYNTAX         DateAndTime
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the actual clock time for
            expiration of the most recent TEK for this FSM."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.5 and 4.2.2.9."
            ::= { docsBpi2CmTEKEntry 8 }

      docsBpi2CmTEKKeyRequests OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the CM
            has transmitted a Key Request message.
            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
            ifCounterDiscontinuityTime."

            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.4."
            ::= { docsBpi2CmTEKEntry 9 }

      docsBpi2CmTEKKeyReplies  OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the CM
            has received a Key Reply message, including a message whose
            authentication failed.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
```

```
          Section 4.2.1.5."
          ::= { docsBpi2CmTEKEntry 10 }

     docsBpi2CmTEKKeyRejects  OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the number of times the CM
          has received a Key Reject message, including a message
          whose authentication failed.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.6."
          ::= { docsBpi2CmTEKEntry 11 }

     docsBpi2CmTEKInvalids    OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the number of times the CM
          has received a TEK Invalid message, including a message
          whose authentication failed.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.8."
          ::= { docsBpi2CmTEKEntry 12 }

     docsBpi2CmTEKAuthPends   OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the count of times an
          Authorization Pending (Auth Pend) event occurred in this
          FSM.
          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
```

```
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.1.3.3.3."
            ::= { docsBpi2CmTEKEntry 13 }

      docsBpi2CmTEKKeyRejectErrorCode    OBJECT-TYPE
            SYNTAX         INTEGER {
                                   none(1),
                                   unknown(2),
                                   unauthorizedSaid(4)
                                   }
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the enumerated
            description of the Error-Code in the most recent Key Reject
            message received by the CM.  This has the value unknown(2) if
            the last Error-Code value was 0 and none(1) if no Key
            Reject message has been received since registration."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.1.2.6 and 4.2.2.15."
            ::= { docsBpi2CmTEKEntry 14 }

      docsBpi2CmTEKKeyRejectErrorString  OBJECT-TYPE
            SYNTAX         SnmpAdminString (SIZE (0..128))
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the text string in the
            most recent Key Reject message received by the CM.  This is
            a zero length string if no Key Reject message has been
            received since registration."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.1.2.6 and 4.2.2.6."
            ::= { docsBpi2CmTEKEntry 15 }

      docsBpi2CmTEKInvalidErrorCode OBJECT-TYPE
            SYNTAX         INTEGER {
                                   none(1),
                                   unknown(2),
                                   invalidKeySequence(6)
                                   }
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
```

```
            "The value of this object is the enumerated
          description of the Error-Code in the most recent TEK Invalid
          message received by the CM.  This has the value unknown(2) if
          the last Error-Code value was 0 and none(1) if no TEK
          Invalid message has been received since registration."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.1.2.8 and 4.2.2.15."
          ::= { docsBpi2CmTEKEntry 16 }

     docsBpi2CmTEKInvalidErrorString    OBJECT-TYPE
          SYNTAX         SnmpAdminString (SIZE (0..128))
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the text string in the
          most recent TEK Invalid message received by the CM.  This is
          a zero length string if no TEK Invalid message has been
          received since registration."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.1.2.8 and 4.2.2.6."
          ::= { docsBpi2CmTEKEntry 17 }

     --
     -- The CM Multicast Objects Group
     --

     docsBpi2CmMulticastObjects OBJECT IDENTIFIER
          ::= { docsBpi2CmObjects 3 }

     --
     -- The CM Dynamic IP Multicast Mapping Table, indexed by
     -- docsBpi2CmIpMulticastIndex and by ifIndex
     --

     docsBpi2CmIpMulticastMapTable OBJECT-TYPE
          SYNTAX         SEQUENCE OF DocsBpi2CmIpMulticastMapEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "This table maps multicast IP addresses to SAIDs per
          CM MAC Interface.
          It is intended to map multicast IP addresses associated
          with SA MAP Request messages."
          ::= { docsBpi2CmMulticastObjects 1 }

     docsBpi2CmIpMulticastMapEntry OBJECT-TYPE
```

```
          SYNTAX         DocsBpi2CmIpMulticastMapEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "Each entry contains objects describing the mapping of
          one multicast IP address to one SAID, as well as
          associated state, message counters, and error information.

          An entry may be removed from this table upon the reception
          of an SA Map Reject."
          INDEX     { ifIndex, docsBpi2CmIpMulticastIndex }
          ::= { docsBpi2CmIpMulticastMapTable 1 }

     DocsBpi2CmIpMulticastMapEntry ::= SEQUENCE {
          docsBpi2CmIpMulticastIndex               Unsigned32,
          docsBpi2CmIpMulticastAddressType         InetAddressType,
          docsBpi2CmIpMulticastAddress             InetAddress,
          docsBpi2CmIpMulticastSAId                DocsSAIdOrZero,
          docsBpi2CmIpMulticastSAMapState          INTEGER,
          docsBpi2CmIpMulticastSAMapRequests       Counter32,
          docsBpi2CmIpMulticastSAMapReplies        Counter32,
          docsBpi2CmIpMulticastSAMapRejects        Counter32,
          docsBpi2CmIpMulticastSAMapRejectErrorCode INTEGER,
          docsBpi2CmIpMulticastSAMapRejectErrorString SnmpAdminString
          }

     docsBpi2CmIpMulticastIndex         OBJECT-TYPE
          SYNTAX         Unsigned32 (1..4294967295)
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "The index of this row."
          ::= { docsBpi2CmIpMulticastMapEntry 1 }

     docsBpi2CmIpMulticastAddressType   OBJECT-TYPE
          SYNTAX         InetAddressType
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The type of Internet address for
          docsBpi2CmIpMulticastAddress."
          ::= { docsBpi2CmIpMulticastMapEntry 2 }

     docsBpi2CmIpMulticastAddress  OBJECT-TYPE
          SYNTAX         InetAddress
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
```

```
            "This object represents the IP multicast address
          to be mapped.  The type of this address is determined by
          the value of the docsBpi2CmIpMulticastAddressType object."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 5.4."
          ::= { docsBpi2CmIpMulticastMapEntry 3 }

     docsBpi2CmIpMulticastSAId          OBJECT-TYPE
          SYNTAX         DocsSAIdOrZero
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "This object represents the SAID to which the IP
          multicast address has been mapped.  If no SA Map Reply has
          been received for the IP address, this object should have
          the value 0."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.12."
          ::= { docsBpi2CmIpMulticastMapEntry 4 }

     docsBpi2CmIpMulticastSAMapState         OBJECT-TYPE
          SYNTAX         INTEGER {
                                 start(1),
                                 mapWait(2),
                                 mapped(3)
                         }
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the state of the SA
          Mapping FSM for this IP."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 5.3.1."
          ::= { docsBpi2CmIpMulticastMapEntry 5 }

     docsBpi2CmIpMulticastSAMapRequests OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the number of times the
          CM has transmitted an SA Map Request message for this IP.
          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
```

```
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.10."
            ::= { docsBpi2CmIpMulticastMapEntry 6 }

      docsBpi2CmIpMulticastSAMapReplies  OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the
            CM has received an SA Map Reply message for this IP.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.11."
            ::= { docsBpi2CmIpMulticastMapEntry 7 }

      docsBpi2CmIpMulticastSAMapRejects  OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the
            CM has received an SA MAP Reject message for this IP.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.12."
            ::= { docsBpi2CmIpMulticastMapEntry 8 }

      docsBpi2CmIpMulticastSAMapRejectErrorCode    OBJECT-TYPE
            SYNTAX         INTEGER {
                           none(1),
                           unknown(2),
                           noAuthForRequestedDSFlow(9),
                           dsFlowNotMappedToSA(10)
                           }
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
```

```
            "The value of this object is the enumerated
          description of the Error-Code in the most recent SA Map
          Reject message sent in response to an SA Map Request for
          This IP.  It has the value none(1) if no SA MAP Reject
          message has been received since entry creation."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.12 and 4.2.2.15."
          ::= { docsBpi2CmIpMulticastMapEntry 9 }

     docsBpi2CmIpMulticastSAMapRejectErrorString  OBJECT-TYPE
          SYNTAX         SnmpAdminString (SIZE (0..128))
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the text string in
          the most recent SA Map Reject message sent in response to
          an SA Map Request for this IP.  It is a zero length string
          if no SA Map Reject message has been received since entry
          creation."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.12 and 4.2.2.6."
          ::= { docsBpi2CmIpMulticastMapEntry 10 }

     --
     -- CM Cert Objects
     --

     docsBpi2CmCertObjects OBJECT IDENTIFIER
          ::= { docsBpi2CmObjects 4 }

     --
     -- CM Device Cert Table
     --

     docsBpi2CmDeviceCertTable  OBJECT-TYPE
          SYNTAX                SEQUENCE OF DocsBpi2CmDeviceCertEntry
          MAX-ACCESS            not-accessible
          STATUS                current
          DESCRIPTION
               "This table describes the Baseline Privacy Plus
          device certificates for each CM MAC interface."
          ::= { docsBpi2CmCertObjects 1 }

     docsBpi2CmDeviceCertEntry  OBJECT-TYPE
          SYNTAX              DocsBpi2CmDeviceCertEntry
          MAX-ACCESS          not-accessible
```

```
          STATUS              current
          DESCRIPTION
               "Each entry contains the device certificates of
          one CM MAC interface.  An entry in this table exists for
          each ifEntry with an ifType of docsCableMaclayer(127)."
          INDEX               { ifIndex }
          ::= { docsBpi2CmDeviceCertTable 1 }

     DocsBpi2CmDeviceCertEntry ::= SEQUENCE {
          docsBpi2CmDeviceCmCert
                                DocsX509ASN1DEREncodedCertificate,
          docsBpi2CmDeviceManufCert
                                DocsX509ASN1DEREncodedCertificate
          }

     docsBpi2CmDeviceCmCert   OBJECT-TYPE
          SYNTAX        DocsX509ASN1DEREncodedCertificate
          MAX-ACCESS         read-write
          STATUS              current
          DESCRIPTION
               "The X509 DER-encoded cable modem certificate.
          Note:  This object can be set only when the value is the
          zero-length OCTET STRING; otherwise, an error of
          'inconsistentValue' is returned.  Once the object
          contains the certificate, its access MUST be read-only
          and persists after re-initialization of the
          managed system."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.1."
          ::= { docsBpi2CmDeviceCertEntry 1 }

     docsBpi2CmDeviceManufCert     OBJECT-TYPE
          SYNTAX         DocsX509ASN1DEREncodedCertificate
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The X509 DER-encoded manufacturer certificate that
          signed the cable modem certificate."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.1."
          ::= { docsBpi2CmDeviceCertEntry 2 }

     --
     -- CM Crypto Suite Table
     --
```

```
docsBpi2CmCryptoSuiteTable    OBJECT-TYPE
     SYNTAX         SEQUENCE OF    DocsBpi2CmCryptoSuiteEntry
     MAX-ACCESS     not-accessible
     STATUS         current
     DESCRIPTION
          "This table describes the Baseline Privacy Plus
     cryptographic suite capabilities for each CM MAC
     interface."
     ::= { docsBpi2CmObjects 5 }

docsBpi2CmCryptoSuiteEntry    OBJECT-TYPE
     SYNTAX         DocsBpi2CmCryptoSuiteEntry
     MAX-ACCESS     not-accessible
     STATUS         current
     DESCRIPTION
          "Each entry contains a cryptographic suite pair
     that this CM MAC supports."
     INDEX     { ifIndex, docsBpi2CmCryptoSuiteIndex }
     ::= { docsBpi2CmCryptoSuiteTable 1 }

DocsBpi2CmCryptoSuiteEntry ::= SEQUENCE {
     docsBpi2CmCryptoSuiteIndex              Unsigned32,
     docsBpi2CmCryptoSuiteDataEncryptAlg
                                  DocsBpkmDataEncryptAlg,
     docsBpi2CmCryptoSuiteDataAuthentAlg
                                  DocsBpkmDataAuthentAlg
     }

docsBpi2CmCryptoSuiteIndex OBJECT-TYPE
     SYNTAX         Unsigned32 (1..1000)
     MAX-ACCESS     not-accessible
     STATUS         current
     DESCRIPTION
          "The index for a cryptographic suite row."
     ::= { docsBpi2CmCryptoSuiteEntry 1 }

docsBpi2CmCryptoSuiteDataEncryptAlg     OBJECT-TYPE
     SYNTAX    DocsBpkmDataEncryptAlg
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the data encryption
     algorithm for this cryptographic suite capability."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Section 4.2.2.20."
     ::= { docsBpi2CmCryptoSuiteEntry 2 }
```

```
      docsBpi2CmCryptoSuiteDataAuthentAlg     OBJECT-TYPE
           SYNTAX    DocsBpkmDataAuthentAlg
           MAX-ACCESS     read-only
           STATUS         current
           DESCRIPTION
                "The value of this object is the data authentication
           algorithm for this cryptographic suite capability."
           REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
           Section 4.2.2.20."
           ::= { docsBpi2CmCryptoSuiteEntry 3 }

      -- Cable Modem Termination System Group

   docsBpi2CmtsObjects OBJECT IDENTIFIER ::= { docsBpi2MIBObjects 2 }

      --
      -- SPECIAL NOTE:  For the following CMTS tables, when a CM is
      -- running in BPI mode, replace SAID (Security Association ID)
      -- with SID (Service ID).  The CMTS is required to map SAIDs and
      -- SIDs to one contiguous space.
      --

      --
      -- The BPI+ base table for CMTSs, indexed by ifIndex
      --

      docsBpi2CmtsBaseTable    OBJECT-TYPE
           SYNTAX              SEQUENCE OF    DocsBpi2CmtsBaseEntry
           MAX-ACCESS          not-accessible
           STATUS              current
           DESCRIPTION
                "This table describes the basic Baseline Privacy
           attributes of each CMTS MAC interface."
           ::= { docsBpi2CmtsObjects 1 }

      docsBpi2CmtsBaseEntry    OBJECT-TYPE
           SYNTAX              DocsBpi2CmtsBaseEntry
           MAX-ACCESS          not-accessible
           STATUS              current
           DESCRIPTION
                "Each entry contains objects describing attributes of
           one CMTS MAC interface.  An entry in this table exists for
           each ifEntry with an ifType of docsCableMaclayer(127)."
           INDEX     { ifIndex }
           ::= { docsBpi2CmtsBaseTable 1 }

      DocsBpi2CmtsBaseEntry ::= SEQUENCE {
```

```
        docsBpi2CmtsDefaultAuthLifetime             Integer32,
        docsBpi2CmtsDefaultTEKLifetime              Integer32,
        docsBpi2CmtsDefaultSelfSignedManufCertTrust  INTEGER,
            docsBpi2CmtsCheckCertValidityPeriods        TruthValue,
            docsBpi2CmtsAuthentInfos                    Counter32,
            docsBpi2CmtsAuthRequests                    Counter32,
            docsBpi2CmtsAuthReplies                     Counter32,
            docsBpi2CmtsAuthRejects                     Counter32,
            docsBpi2CmtsAuthInvalids                    Counter32,
            docsBpi2CmtsSAMapRequests                   Counter32,
            docsBpi2CmtsSAMapReplies                    Counter32,
            docsBpi2CmtsSAMapRejects                    Counter32
            }

    docsBpi2CmtsDefaultAuthLifetime    OBJECT-TYPE
        SYNTAX         Integer32 (1..6048000)
        UNITS          "seconds"
        MAX-ACCESS     read-write
        STATUS         current
        DESCRIPTION
             "The value of this object is the default lifetime, in
        seconds, that the CMTS assigns to a new authorization key.
        This object value persists after re-initialization of the
        managed system."
        REFERENCE
             "DOCSIS Baseline Privacy Plus Interface Specification,
        Appendix A.2."
        DEFVAL { 604800 }
        ::= { docsBpi2CmtsBaseEntry 1 }

    docsBpi2CmtsDefaultTEKLifetime     OBJECT-TYPE
        SYNTAX         Integer32 (1..604800)
        UNITS          "seconds"
        MAX-ACCESS     read-write
        STATUS         current
        DESCRIPTION
             "The value of this object is the default lifetime, in
        seconds, that the CMTS assigns to a new Traffic Encryption
        Key (TEK).
        This object value persists after re-initialization of the
        managed system."
        REFERENCE
             "DOCSIS Baseline Privacy Plus Interface Specification,
        Appendix A.2."
        DEFVAL { 43200 }
        ::= { docsBpi2CmtsBaseEntry 2 }

    docsBpi2CmtsDefaultSelfSignedManufCertTrust  OBJECT-TYPE
```

```
          SYNTAX    INTEGER {
                    trusted (1),
                    untrusted (2)
                    }
          MAX-ACCESS     read-write
          STATUS         current
          DESCRIPTION
               "This object determines the default trust of
          self-signed manufacturer certificate entries, contained
          in docsBpi2CmtsCACertTable, and created after this
          object is set.
          This object need not persist after re-initialization
          of the managed system."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.4.1"
          ::= { docsBpi2CmtsBaseEntry 3 }

     docsBpi2CmtsCheckCertValidityPeriods    OBJECT-TYPE
          SYNTAX         TruthValue
          MAX-ACCESS     read-write
          STATUS         current
          DESCRIPTION
               "Setting this object to 'true' causes all chained and
          root certificates in the chain to have their validity
          periods checked against the current time of day, when
          the CMTS receives an Authorization Request from the
          CM.
          A 'false' setting causes all certificates in the chain
          not to have their validity periods checked against the
          current time of day.
          This object need not persist after re-initialization
          of the managed system."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.4.2"
          ::= { docsBpi2CmtsBaseEntry 4 }

     docsBpi2CmtsAuthentInfos OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the number of times the
          CMTS has received an Authentication Information message
          from any CM.
          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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.9."
            ::= { docsBpi2CmtsBaseEntry 5 }

      docsBpi2CmtsAuthRequests OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                    "The value of this object is the number of times the
            CMTS has received an Authorization Request message from any
            CM.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.1."
            ::= { docsBpi2CmtsBaseEntry 6 }

      docsBpi2CmtsAuthReplies  OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                   "The value of this object is the number of times the
            CMTS has transmitted an Authorization Reply message to any
            CM.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.2."
            ::= { docsBpi2CmtsBaseEntry 7 }

      docsBpi2CmtsAuthRejects  OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                    "The value of this object is the number of times the
            CMTS has transmitted an Authorization Reject message to any
```

```
          CM.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.3."
          ::= { docsBpi2CmtsBaseEntry 8 }

     docsBpi2CmtsAuthInvalids OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
                   "The value of this object is the number of times
          the CMTS has transmitted an Authorization Invalid message
          to any CM.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.7."
          ::= { docsBpi2CmtsBaseEntry 9 }

     docsBpi2CmtsSAMapRequests     OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the number of times the
          CMTS has received an SA Map Request message from any CM.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.10."
          ::= { docsBpi2CmtsBaseEntry 10 }

     docsBpi2CmtsSAMapReplies OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
```

```
            "The value of this object is the number of times the
          CMTS has transmitted an SA Map Reply message to any CM.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.11."
          ::= { docsBpi2CmtsBaseEntry 11 }

     docsBpi2CmtsSAMapRejects OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the number of times the
          CMTS has transmitted an SA Map Reject message to any CM.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.12."
          ::= { docsBpi2CmtsBaseEntry 12 }

     --
     -- The CMTS Authorization Table, indexed by ifIndex and CM MAC
     -- address
     --

     docsBpi2CmtsAuthTable    OBJECT-TYPE
          SYNTAX         SEQUENCE OF    DocsBpi2CmtsAuthEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "This table describes the attributes of each CM
          authorization association.  The CMTS maintains one
          authorization association with each Baseline Privacy-
          enabled CM, registered on each CMTS MAC interface,
          regardless of whether the CM is authorized or rejected."
          ::= { docsBpi2CmtsObjects 2 }

     docsBpi2CmtsAuthEntry    OBJECT-TYPE
          SYNTAX              DocsBpi2CmtsAuthEntry
          MAX-ACCESS          not-accessible
          STATUS              current
```

```
          DESCRIPTION
               "Each entry contains objects describing attributes of
          one authorization association.  The CMTS MUST create one
          entry per CM per MAC interface, based on the receipt of an
          Authorization Request message, and MUST not delete the
          entry until the CM loses registration."
          INDEX     { ifIndex, docsBpi2CmtsAuthCmMacAddress }
          ::= { docsBpi2CmtsAuthTable 1 }

     DocsBpi2CmtsAuthEntry ::= SEQUENCE {
          docsBpi2CmtsAuthCmMacAddress        MacAddress,
          docsBpi2CmtsAuthCmBpiVersion        INTEGER,
          docsBpi2CmtsAuthCmPublicKey         OCTET STRING,
          docsBpi2CmtsAuthCmKeySequenceNumber Integer32,
          docsBpi2CmtsAuthCmExpiresOld        DateAndTime,
          docsBpi2CmtsAuthCmExpiresNew        DateAndTime,
          docsBpi2CmtsAuthCmLifetime          Integer32,
          docsBpi2CmtsAuthCmReset             INTEGER,
          docsBpi2CmtsAuthCmInfos             Counter32,
          docsBpi2CmtsAuthCmRequests          Counter32,
          docsBpi2CmtsAuthCmReplies           Counter32,
          docsBpi2CmtsAuthCmRejects           Counter32,
          docsBpi2CmtsAuthCmInvalids          Counter32,
          docsBpi2CmtsAuthRejectErrorCode     INTEGER,
          docsBpi2CmtsAuthRejectErrorString   SnmpAdminString,
          docsBpi2CmtsAuthInvalidErrorCode    INTEGER,
          docsBpi2CmtsAuthInvalidErrorString  SnmpAdminString,
          docsBpi2CmtsAuthPrimarySAId         DocsSAIdOrZero,
          docsBpi2CmtsAuthBpkmCmCertValid     INTEGER,
          docsBpi2CmtsAuthBpkmCmCert
                               DocsX509ASN1DEREncodedCertificate,
          docsBpi2CmtsAuthCACertIndexPtr      Unsigned32
          }

     docsBpi2CmtsAuthCmMacAddress  OBJECT-TYPE
          SYNTAX         MacAddress
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "The value of this object is the physical address of
          the CM to which the authorization association applies."
          ::= { docsBpi2CmtsAuthEntry 1 }

     docsBpi2CmtsAuthCmBpiVersion  OBJECT-TYPE
          SYNTAX         INTEGER {
                           bpi (0),
                           bpiPlus (1)
                            }
```

```
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the version of Baseline
            Privacy for which this CM has registered.  The value
            'bpiplus' represents the value of BPI-Version Attribute of
            the Baseline Privacy Key Management BPKM attribute
            BPI-Version (1).  The value 'bpi' is used to represent the
            CM registered using DOCSIS 1.0 Baseline Privacy."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.2.22; ANSI/SCTE 22-2 2002(formerly DSS 02-03)
            Data-Over-Cable Service Interface Specification DOCSIS 1.0
            Baseline Privacy Interface (BPI)"
            ::= { docsBpi2CmtsAuthEntry 2 }

       docsBpi2CmtsAuthCmPublicKey   OBJECT-TYPE
            SYNTAX         OCTET STRING (SIZE (0..524))
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is a DER-encoded
            RSAPublicKey ASN.1 type string, as defined in the RSA
            Encryption Standard (PKCS #1), corresponding to the
            public key of the CM.  This is the zero-length OCTET
            STRING if the CMTS does not retain the public key."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.2.4."
            ::= { docsBpi2CmtsAuthEntry 3 }

       docsBpi2CmtsAuthCmKeySequenceNumber     OBJECT-TYPE
            SYNTAX         Integer32 (0..15)
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the most recent
            authorization key sequence number for this CM."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.2 and 4.2.2.10."
            ::= { docsBpi2CmtsAuthEntry 4 }

       docsBpi2CmtsAuthCmExpiresOld  OBJECT-TYPE
            SYNTAX         DateAndTime
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
```

```
            "The value of this object is the actual clock time
          for expiration of the immediate predecessor of the most
          recent authorization key for this FSM.  If this FSM has only
          one authorization key, then the value is the time of
          activation of this FSM.
          Note: This object has no meaning for CMs running in BPI
          mode; therefore, this object is not instantiated for entries
          associated to those CMs."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.2 and 4.2.2.9."
          ::= { docsBpi2CmtsAuthEntry 5 }

     docsBpi2CmtsAuthCmExpiresNew  OBJECT-TYPE
          SYNTAX         DateAndTime
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
                    "The value of this object is the actual clock
          time for expiration of the most recent authorization key
          for this FSM."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.2 and 4.2.2.9."
          ::= { docsBpi2CmtsAuthEntry 6 }

     docsBpi2CmtsAuthCmLifetime    OBJECT-TYPE
          SYNTAX         Integer32 (1..6048000)
          UNITS          "seconds"
          MAX-ACCESS     read-write
          STATUS         current
          DESCRIPTION
               "The value of this object is the lifetime, in seconds,
          that the CMTS assigns to an authorization key for this CM."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.2 and Appendix A.2."
          ::= { docsBpi2CmtsAuthEntry 7 }

     docsBpi2CmtsAuthCmReset  OBJECT-TYPE
          SYNTAX    INTEGER   {
                              noResetRequested(1),
                              invalidateAuth(2),
                              sendAuthInvalid(3),
                              invalidateTeks(4)
                              }
          MAX-ACCESS     read-write
          STATUS         current
```

```
            DESCRIPTION
                 "Setting this object to invalidateAuth(2) causes the
            CMTS to invalidate the current CM authorization key(s), but
            not to transmit an Authorization Invalid message nor to
            invalidate the primary SAID's TEKs.  Setting this object to
            sendAuthInvalid(3) causes the CMTS to invalidate the
            current CM authorization key(s), and to transmit an
            Authorization Invalid message to the CM, but not to
            invalidate the primary SAID's TEKs.  Setting this object to
            invalidateTeks(4) causes the CMTS to invalidate the current
            CM authorization key(s), to transmit an Authorization
            Invalid message to the CM, and to invalidate the TEKs
            associated with this CM's primary SAID.
            For BPI mode, substitute all of the CM's unicast
            TEKs for the primary SAID's TEKs in the previous
            paragraph.
            Reading this object returns the most recently set
            value of this object or, if the object has not been set
            since entry creation, returns noResetRequested(1)."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.1.2.3.4, 4.1.2.3.5, and 4.1.3.3.5."
            ::= { docsBpi2CmtsAuthEntry 8 }

       docsBpi2CmtsAuthCmInfos       OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the
            CMTS has received an Authentication Information message
            from this CM.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.9."
            ::= { docsBpi2CmtsAuthEntry 9 }

       docsBpi2CmtsAuthCmRequests    OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the
            CMTS has received an Authorization Request message from
```

```
          this CM.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.1."
          ::= { docsBpi2CmtsAuthEntry 10 }

     docsBpi2CmtsAuthCmReplies     OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the number of times the
          CMTS has transmitted an Authorization Reply message to this
          CM.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.2."
          ::= { docsBpi2CmtsAuthEntry 11 }

     docsBpi2CmtsAuthCmRejects     OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the number of times the
          CMTS has transmitted an Authorization Reject message to
          this CM.
          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
          ifCounterDiscontinuityTime."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.3."
          ::= { docsBpi2CmtsAuthEntry 12 }

     docsBpi2CmtsAuthCmInvalids    OBJECT-TYPE
          SYNTAX         Counter32
          MAX-ACCESS     read-only
          STATUS         current
```

```
            DESCRIPTION
                 "The value of this object is the number of times the
            CMTS has transmitted an Authorization Invalid message to
            this CM.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.7."
            ::= { docsBpi2CmtsAuthEntry 13 }

        docsBpi2CmtsAuthRejectErrorCode    OBJECT-TYPE
            SYNTAX         INTEGER {
                                   none(1),
                                   unknown(2),
                                   unauthorizedCm(3),
                                   unauthorizedSaid(4),
                                   permanentAuthorizationFailure(8),
                                   timeOfDayNotAcquired(11)
                                   }
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the enumerated
            description of the Error-Code in the most recent
            Authorization Reject message transmitted to the CM.  This has
            the value unknown(2) if the last Error-Code value was 0 and
            none(1) if no Authorization Reject message has been
            transmitted to the CM since entry creation."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.3 and 4.2.2.15."
            ::= { docsBpi2CmtsAuthEntry 14 }

        docsBpi2CmtsAuthRejectErrorString  OBJECT-TYPE
            SYNTAX         SnmpAdminString (SIZE (0..128))
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the text string in the
            most recent Authorization Reject message transmitted to the
            CM.  This is a zero length string if no Authorization
            Reject message has been transmitted to the CM since entry
            creation."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
```

```
          Sections 4.2.1.3 and 4.2.2.6."
          ::= { docsBpi2CmtsAuthEntry 15 }

     docsBpi2CmtsAuthInvalidErrorCode   OBJECT-TYPE
          SYNTAX         INTEGER {
                                 none(1),
                                 unknown(2),
                                 unauthorizedCm(3),
                                 unsolicited(5),
                                 invalidKeySequence(6),
                                 keyRequestAuthenticationFailure(7)
                                 }
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the enumerated
          description of the Error-Code in the most recent
          Authorization Invalid message transmitted to the CM.  This
          has the value unknown(2) if the last Error-Code value was 0
          and none(1) if no Authorization Invalid message has been
          transmitted to the CM since entry creation."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.7 and 4.2.2.15."
          ::= { docsBpi2CmtsAuthEntry 16 }

     docsBpi2CmtsAuthInvalidErrorString OBJECT-TYPE
          SYNTAX         SnmpAdminString (SIZE (0..128))
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the text string in the
          most recent Authorization Invalid message transmitted to
          the CM.  This is a zero length string if no Authorization
          Invalid message has been transmitted to the CM since entry
          creation."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.7 and 4.2.2.6."
          ::= { docsBpi2CmtsAuthEntry 17 }

     docsBpi2CmtsAuthPrimarySAId   OBJECT-TYPE
          SYNTAX         DocsSAIdOrZero
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the Primary Security
          Association identifier.  For BPI mode, the value must be
```

```
          any unicast SID."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 2.1.3."
          ::= { docsBpi2CmtsAuthEntry 18 }

     docsBpi2CmtsAuthBpkmCmCertValid         OBJECT-TYPE
          SYNTAX    INTEGER {
                            unknown (0),
                            validCmChained (1),
                            validCmTrusted (2),
                            invalidCmUntrusted (3),
                            invalidCAUntrusted (4),
                            invalidCmOther (5),
                            invalidCAOther (6)
                            }
          MAX-ACCESS     read-only
          STATUS    current
          DESCRIPTION
               "Contains the reason why a CM's certificate is deemed
          valid or invalid.
          Return unknown(0) if the CM is running BPI mode.
          ValidCmChained(1) means the certificate is valid
             because it chains to a valid certificate.
          ValidCmTrusted(2) means the certificate is valid
             because it has been provisioned (in the
             docsBpi2CmtsProvisionedCmCert table) to be trusted.
          InvalidCmUntrusted(3) means the certificate is invalid
             because it has been provisioned (in the
             docsBpi2CmtsProvisionedCmCert table) to be untrusted.
          InvalidCAUntrusted(4) means the certificate is invalid
             because it chains to an untrusted certificate.
          InvalidCmOther(5) and InvalidCAOther(6) refer to
             errors in parsing, validity periods, etc., which are
             attributable to the CM certificate or its chain,
             respectively; additional information may be found
             in docsBpi2AuthRejectErrorString for these types
             of errors."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.4.2."
          ::= { docsBpi2CmtsAuthEntry 19 }

     docsBpi2CmtsAuthBpkmCmCert    OBJECT-TYPE
          SYNTAX         DocsX509ASN1DEREncodedCertificate
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
```

```
            "The X509 CM Certificate sent as part of a BPKM
          Authorization Request.
          Note: The zero-length OCTET STRING must be returned if the
          Entire certificate is not retained in the CMTS."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.2."
          ::= { docsBpi2CmtsAuthEntry 20 }

     docsBpi2CmtsAuthCACertIndexPtr    OBJECT-TYPE
          SYNTAX         Unsigned32 (0..4294967295)
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "A row index into docsBpi2CmtsCACertTable.
                Returns the index in docsBpi2CmtsCACertTable to which
                CA certificate this CM is chained to.  A value of
                0 means it could not be found or not applicable."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.2."
          ::= { docsBpi2CmtsAuthEntry 21 }

     --
     -- The CMTS TEK Table, indexed by ifIndex and SAID
     --

     docsBpi2CmtsTEKTable     OBJECT-TYPE
          SYNTAX         SEQUENCE OF    DocsBpi2CmtsTEKEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "This table describes the attributes of each
          Traffic Encryption Key (TEK) association.  The CMTS
          Maintains one TEK association per SAID on each CMTS MAC
          interface."
          ::= { docsBpi2CmtsObjects 3 }

     docsBpi2CmtsTEKEntry     OBJECT-TYPE
          SYNTAX         DocsBpi2CmtsTEKEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "Each entry contains objects describing attributes of
          one TEK association on a particular CMTS MAC interface.  The
          CMTS MUST create one entry per SAID per MAC interface,
          based on the receipt of a Key Request message, and MUST not
          delete the entry before the CM authorization for the SAID
```

```
          permanently expires."
          INDEX     { ifIndex, docsBpi2CmtsTEKSAId }
          ::= { docsBpi2CmtsTEKTable 1 }

     DocsBpi2CmtsTEKEntry ::= SEQUENCE {
          docsBpi2CmtsTEKSAId                DocsSAId,
          docsBpi2CmtsTEKSAType              DocsBpkmSAType,
          docsBpi2CmtsTEKDataEncryptAlg      DocsBpkmDataEncryptAlg,
          docsBpi2CmtsTEKDataAuthentAlg      DocsBpkmDataAuthentAlg,
          docsBpi2CmtsTEKLifetime            Integer32,
          docsBpi2CmtsTEKKeySequenceNumber   Integer32,
          docsBpi2CmtsTEKExpiresOld          DateAndTime,
          docsBpi2CmtsTEKExpiresNew          DateAndTime,
          docsBpi2CmtsTEKReset               TruthValue,
          docsBpi2CmtsKeyRequests            Counter32,
          docsBpi2CmtsKeyReplies             Counter32,
          docsBpi2CmtsKeyRejects             Counter32,
          docsBpi2CmtsTEKInvalids            Counter32,
          docsBpi2CmtsKeyRejectErrorCode     INTEGER,
          docsBpi2CmtsKeyRejectErrorString   SnmpAdminString,
          docsBpi2CmtsTEKInvalidErrorCode    INTEGER,
          docsBpi2CmtsTEKInvalidErrorString  SnmpAdminString
     }

     docsBpi2CmtsTEKSAId OBJECT-TYPE
          SYNTAX         DocsSAId
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "The value of this object is the DOCSIS Security
          Association ID (SAID)."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.12."
          ::= { docsBpi2CmtsTEKEntry 1 }

     docsBpi2CmtsTEKSAType    OBJECT-TYPE
          SYNTAX         DocsBpkmSAType
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the type of security
          association.  'dynamic' does not apply to CMs running in
          BPI mode.  Unicast BPI TEKs must utilize the 'primary'
          encoding, and multicast BPI TEKs must utilize the 'static'
          encoding."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
```

```
          Section 2.1.3."
          ::= { docsBpi2CmtsTEKEntry 2 }

     docsBpi2CmtsTEKDataEncryptAlg OBJECT-TYPE
          SYNTAX    DocsBpkmDataEncryptAlg
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the data encryption
          algorithm for this SAID."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.20."
          ::= { docsBpi2CmtsTEKEntry 3 }

     docsBpi2CmtsTEKDataAuthentAlg OBJECT-TYPE
          SYNTAX    DocsBpkmDataAuthentAlg
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the data authentication
          algorithm for this SAID."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.20."
          ::= { docsBpi2CmtsTEKEntry 4 }

     docsBpi2CmtsTEKLifetime  OBJECT-TYPE
          SYNTAX         Integer32 (1..604800)
          UNITS          "seconds"
          MAX-ACCESS     read-write
          STATUS         current
          DESCRIPTION
               "The value of this object is the lifetime, in
          seconds, that the CMTS assigns to keys for this TEK
          association."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.1.5 and Appendix A.2."
          ::= { docsBpi2CmtsTEKEntry 5 }


     docsBpi2CmtsTEKKeySequenceNumber   OBJECT-TYPE
          SYNTAX              Integer32 (0..15)
          MAX-ACCESS          read-only
          STATUS              current
          DESCRIPTION
               "The value of this object is the most recent TEK
```

```
            key sequence number for this SAID."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.2.10 and 4.2.2.13."
            ::= { docsBpi2CmtsTEKEntry 6 }

      docsBpi2CmtsTEKExpiresOld     OBJECT-TYPE
            SYNTAX         DateAndTime
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the actual clock time
            for expiration of the immediate predecessor of the most
            recent TEK for this FSM.  If this FSM has only one TEK, then
            the value is the time of activation of this FSM."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.5 and 4.2.2.9."
            ::= { docsBpi2CmtsTEKEntry 7 }

      docsBpi2CmtsTEKExpiresNew     OBJECT-TYPE
            SYNTAX         DateAndTime
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the actual clock time
            for expiration of the most recent TEK for this FSM."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.5 and 4.2.2.9."
            ::= { docsBpi2CmtsTEKEntry 8 }

      docsBpi2CmtsTEKReset     OBJECT-TYPE
            SYNTAX         TruthValue
            MAX-ACCESS     read-write
            STATUS         current
            DESCRIPTION
                 "Setting this object to 'true' causes the CMTS to
            invalidate all currently active TEKs and to generate new
            TEKs for the associated SAID; the CMTS MAY also generate
            unsolicited TEK Invalid messages, to optimize the TEK
            synchronization between the CMTS and the CM(s).  Reading
            this object always returns FALSE."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.1.3.3.5."
            ::= { docsBpi2CmtsTEKEntry 9 }
```

```
docsBpi2CmtsKeyRequests  OBJECT-TYPE
     SYNTAX         Counter32
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the number of times the
     CMTS has received a Key Request message.
     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
     ifCounterDiscontinuityTime."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Section 4.2.1.4."
     ::= { docsBpi2CmtsTEKEntry 10 }

docsBpi2CmtsKeyReplies   OBJECT-TYPE
     SYNTAX         Counter32
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the number of times the
     CMTS has transmitted a Key Reply message.
     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
     ifCounterDiscontinuityTime."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Section 4.2.1.5."
     ::= { docsBpi2CmtsTEKEntry 11 }

docsBpi2CmtsKeyRejects   OBJECT-TYPE
     SYNTAX         Counter32
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the number of times the
     CMTS has transmitted a Key Reject message.
     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
     ifCounterDiscontinuityTime."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Section 4.2.1.6."
     ::= { docsBpi2CmtsTEKEntry 12 }
```

```
docsBpi2CmtsTEKInvalids  OBJECT-TYPE
     SYNTAX         Counter32
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the number of times the
     CMTS has transmitted a TEK Invalid message.
     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
     ifCounterDiscontinuityTime."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Section 4.2.1.8."
     ::= { docsBpi2CmtsTEKEntry 13 }

docsBpi2CmtsKeyRejectErrorCode     OBJECT-TYPE
     SYNTAX         INTEGER {
                            none(1),
                            unknown(2),
                            unauthorizedSaid(4)
                            }
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the enumerated
     description of the Error-Code in the most recent Key Reject
     message sent in response to a Key Request for this SAID.
     This has the value unknown(2) if the last Error-Code value
     was 0 and none(1) if no Key Reject message has been
     received since registration."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Sections 4.2.1.6 and 4.2.2.15."
     ::= { docsBpi2CmtsTEKEntry 14 }

docsBpi2CmtsKeyRejectErrorString   OBJECT-TYPE
     SYNTAX         SnmpAdminString (SIZE (0..128))
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The value of this object is the text string in
     the most recent Key Reject message sent in response to a
     Key Request for this SAID.  This is a zero length string if
     no Key Reject message has been received since
     registration."
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
```

```
          Sections 4.2.1.6 and 4.2.2.6."
          ::= { docsBpi2CmtsTEKEntry 15 }

     docsBpi2CmtsTEKInvalidErrorCode    OBJECT-TYPE
          SYNTAX         INTEGER {
                                 none(1),
                                 unknown(2),
                                 invalidKeySequence(6)
                                 }
          MAX-ACCESS          read-only
          STATUS              current
          DESCRIPTION
               "The value of this object is the enumerated
          description of the Error-Code in the most recent TEK
          Invalid message sent in association with this SAID.  This
          has the value unknown(2) if the last Error-Code value was 0
          and none(1) if no TEK Invalid message has been received
          since registration."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.8 and 4.2.2.15."
          ::= { docsBpi2CmtsTEKEntry 16 }

     docsBpi2CmtsTEKInvalidErrorString  OBJECT-TYPE
          SYNTAX         SnmpAdminString (SIZE (0..128))
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The value of this object is the text string in
          the most recent TEK Invalid message sent in association
          with this SAID.  This is a zero length string if no TEK
          Invalid message has been received since registration."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Sections 4.2.1.8 and 4.2.2.6."
          ::= { docsBpi2CmtsTEKEntry 17 }

     --
     -- The CMTS Multicast Objects Group
     --

     docsBpi2CmtsMulticastObjects OBJECT IDENTIFIER
          ::= { docsBpi2CmtsObjects 4 }

     --
     -- The CMTS IP Multicast Mapping Table, indexed by
     -- docsBpi2CmtsIpMulticastIndex, and by ifIndex
     --
```

```
docsBpi2CmtsIpMulticastMapTable         OBJECT-TYPE
     SYNTAX         SEQUENCE OF DocsBpi2CmtsIpMulticastMapEntry
     MAX-ACCESS     not-accessible
     STATUS         current
     DESCRIPTION
          "This table maps multicast IP addresses to SAIDs.
     If a multicast IP address is mapped by multiple rows
     in the table, the row with the lowest
     docsBpi2CmtsIpMulticastIndex must be utilized for the
     mapping."
     ::= { docsBpi2CmtsMulticastObjects 1 }

docsBpi2CmtsIpMulticastMapEntry         OBJECT-TYPE
     SYNTAX         DocsBpi2CmtsIpMulticastMapEntry
     MAX-ACCESS     not-accessible
     STATUS         current
     DESCRIPTION
          "Each entry contains objects describing the mapping of
     a set of multicast IP address and the mask to one SAID
     associated to a CMTS MAC Interface, as well as associated
     message counters and error information."
     INDEX     { ifIndex, docsBpi2CmtsIpMulticastIndex }
     ::= { docsBpi2CmtsIpMulticastMapTable 1 }

DocsBpi2CmtsIpMulticastMapEntry ::= SEQUENCE {
     docsBpi2CmtsIpMulticastIndex            Unsigned32,
     docsBpi2CmtsIpMulticastAddressType      InetAddressType,
     docsBpi2CmtsIpMulticastAddress          InetAddress,
     docsBpi2CmtsIpMulticastMask             InetAddress,
     docsBpi2CmtsIpMulticastSAId             DocsSAIdOrZero,
     docsBpi2CmtsIpMulticastSAType           DocsBpkmSAType,
     docsBpi2CmtsIpMulticastDataEncryptAlg
                                     DocsBpkmDataEncryptAlg,
     docsBpi2CmtsIpMulticastDataAuthentAlg
                                     DocsBpkmDataAuthentAlg,
     docsBpi2CmtsIpMulticastSAMapRequests    Counter32,
     docsBpi2CmtsIpMulticastSAMapReplies     Counter32,
     docsBpi2CmtsIpMulticastSAMapRejects     Counter32,
     docsBpi2CmtsIpMulticastSAMapRejectErrorCode
                                                INTEGER,
     docsBpi2CmtsIpMulticastSAMapRejectErrorString
                                                SnmpAdminString,
     docsBpi2CmtsIpMulticastMapControl          RowStatus,
     docsBpi2CmtsIpMulticastMapStorageType      StorageType
     }

docsBpi2CmtsIpMulticastIndex       OBJECT-TYPE
     SYNTAX         Unsigned32 (1..4294967295)
```

```
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "The index of this row.  Conceptual rows having the
          value 'permanent' need not allow write-access to any
          columnar objects in the row."
          ::= { docsBpi2CmtsIpMulticastMapEntry 1 }

     docsBpi2CmtsIpMulticastAddressType OBJECT-TYPE
          SYNTAX         InetAddressType
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "The type of Internet address for
          docsBpi2CmtsIpMulticastAddress
          and docsBpi2CmtsIpMulticastMask."
          DEFVAL { ipv4 }
          ::= { docsBpi2CmtsIpMulticastMapEntry 2 }

     docsBpi2CmtsIpMulticastAddress          OBJECT-TYPE
          SYNTAX         InetAddress
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "This object represents the IP multicast address
          to be mapped, in conjunction with
          docsBpi2CmtsIpMulticastMask.  The type of this address is
          determined by the value of the object
          docsBpi2CmtsIpMulticastAddressType."
          ::= { docsBpi2CmtsIpMulticastMapEntry 3 }

     docsBpi2CmtsIpMulticastMask        OBJECT-TYPE
          SYNTAX         InetAddress
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "This object represents the IP multicast address mask
          for this row.
          An IP multicast address matches this row if the logical
          AND of the address with docsBpi2CmtsIpMulticastMask is
          identical to the logical AND of
          docsBpi2CmtsIpMulticastAddr with
          docsBpi2CmtsIpMulticastMask.  The type of this address is
          determined by the value of the object
          docsBpi2CmtsIpMulticastAddressType.
          Note: For IPv6, this object need not represent a
          contiguous netmask; e.g., to associate a SAID to a
          multicast group matching 'any' multicast scope.  The TC
```

```
          InetAddressPrefixLength is not used, as it only
          represents contiguous netmask."
          ::= { docsBpi2CmtsIpMulticastMapEntry 4 }

     docsBpi2CmtsIpMulticastSAId        OBJECT-TYPE
          SYNTAX         DocsSAIdOrZero
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "This object represents the multicast SAID to be
          used in this IP multicast address mapping entry."
          ::= { docsBpi2CmtsIpMulticastMapEntry 5 }

     docsBpi2CmtsIpMulticastSAType OBJECT-TYPE
          SYNTAX         DocsBpkmSAType
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "The value of this object is the type of security
          association.  'dynamic' does not apply to CMs running in
          BPI mode.  Unicast BPI TEKs must utilize the 'primary'
          encoding, and multicast BPI TEKs must utilize the 'static'
          encoding.  By default, SNMP created entries set this object
          to 'static' if not set at row creation."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 2.1.3."
          ::= { docsBpi2CmtsIpMulticastMapEntry 6 }

     docsBpi2CmtsIpMulticastDataEncryptAlg   OBJECT-TYPE
          SYNTAX    DocsBpkmDataEncryptAlg
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "The value of this object is the data encryption
          algorithm for this IP."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 4.2.2.20."
          DEFVAL { des56CbcMode }
          ::= { docsBpi2CmtsIpMulticastMapEntry 7 }

     docsBpi2CmtsIpMulticastDataAuthentAlg   OBJECT-TYPE
          SYNTAX    DocsBpkmDataAuthentAlg
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "The value of this object is the data authentication
```

```
            algorithm for this IP."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.2.20."
            DEFVAL { none }
            ::= { docsBpi2CmtsIpMulticastMapEntry 8 }

       docsBpi2CmtsIpMulticastSAMapRequests    OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the
            CMTS has received an SA Map Request message for this IP.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.10."
            ::= { docsBpi2CmtsIpMulticastMapEntry 9 }

       docsBpi2CmtsIpMulticastSAMapReplies     OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the
            CMTS has transmitted an SA Map Reply message for this IP.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.11."
            ::= { docsBpi2CmtsIpMulticastMapEntry 10 }

       docsBpi2CmtsIpMulticastSAMapRejects     OBJECT-TYPE
            SYNTAX         Counter32
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the number of times the
            CMTS has transmitted an SA Map Reject message for this IP.
            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
            ifCounterDiscontinuityTime."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Section 4.2.1.12."
            ::= { docsBpi2CmtsIpMulticastMapEntry 11 }

      docsBpi2CmtsIpMulticastSAMapRejectErrorCode  OBJECT-TYPE
            SYNTAX         INTEGER {
                                   none(1),
                                   unknown(2),
                                   noAuthForRequestedDSFlow(9),
                                   dsFlowNotMappedToSA(10)
                                   }
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the enumerated
            description of the Error-Code in the most recent SA Map
            Reject message sent in response to an SA Map Request for
            this IP.  It has the value unknown(2) if the last Error-Code
            Value was 0 and none(1) if no SA MAP Reject message has
            been received since entry creation."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.12 and 4.2.2.15."
            ::= { docsBpi2CmtsIpMulticastMapEntry 12 }

      docsBpi2CmtsIpMulticastSAMapRejectErrorString     OBJECT-TYPE
            SYNTAX         SnmpAdminString (SIZE (0..128))
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                 "The value of this object is the text string in
            the most recent SA Map Reject message sent in response to
            an SA Map Request for this IP.  It is a zero length string
            if no SA Map Reject message has been received since entry
            creation."
            REFERENCE
                 "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections 4.2.1.12 and 4.2.2.6."
            ::= { docsBpi2CmtsIpMulticastMapEntry 13 }

      docsBpi2CmtsIpMulticastMapControl  OBJECT-TYPE
            SYNTAX         RowStatus
            MAX-ACCESS     read-create
            STATUS         current
            DESCRIPTION
```

```
            "This object controls and reflects the IP multicast
          address mapping entry.  There is no restriction on the
          ability to change values in this row while the row is
          active.
          A created row can be set to active only after the
          Corresponding instances of docsBpi2CmtsIpMulticastAddress,
          docsBpi2CmtsIpMulticastMask, docsBpi2CmtsIpMulticastSAId,
          and docsBpi2CmtsIpMulticastSAType have all been set."
          ::= { docsBpi2CmtsIpMulticastMapEntry 14 }

      docsBpi2CmtsIpMulticastMapStorageType     OBJECT-TYPE
          SYNTAX         StorageType
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The storage type for this conceptual row.
          Conceptual rows having the value 'permanent' need not allow
          write-access to any columnar objects in the row."
          ::= { docsBpi2CmtsIpMulticastMapEntry 15 }

      --
      -- The CMTS Multicast SAID Authorization Table,
      -- indexed by ifIndex by
      -- multicast SAID by CM MAC address
      --

      docsBpi2CmtsMulticastAuthTable          OBJECT-TYPE
          SYNTAX         SEQUENCE OF DocsBpi2CmtsMulticastAuthEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "This table describes the multicast SAID
          authorization for each CM on each CMTS MAC interface."
          ::= { docsBpi2CmtsMulticastObjects 2 }

      docsBpi2CmtsMulticastAuthEntry          OBJECT-TYPE
          SYNTAX         DocsBpi2CmtsMulticastAuthEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "Each entry contains objects describing the key
          authorization of one cable modem for one multicast SAID
          for one CMTS MAC interface.
          Row entries persist after re-initialization of
          the managed system."
          INDEX     { ifIndex, docsBpi2CmtsMulticastAuthSAId,
                      docsBpi2CmtsMulticastAuthCmMacAddress }
          ::= { docsBpi2CmtsMulticastAuthTable 1 }
```

```
DocsBpi2CmtsMulticastAuthEntry ::= SEQUENCE
     {
     docsBpi2CmtsMulticastAuthSAId                DocsSAId,
     docsBpi2CmtsMulticastAuthCmMacAddress        MacAddress,
     docsBpi2CmtsMulticastAuthControl             RowStatus
     }

docsBpi2CmtsMulticastAuthSAId OBJECT-TYPE
     SYNTAX         DocsSAId
     MAX-ACCESS     not-accessible
     STATUS         current
     DESCRIPTION
          "This object represents the multicast SAID for
     authorization."
     ::= { docsBpi2CmtsMulticastAuthEntry 1 }

docsBpi2CmtsMulticastAuthCmMacAddress   OBJECT-TYPE
     SYNTAX         MacAddress
     MAX-ACCESS     not-accessible
     STATUS         current
     DESCRIPTION
          "This object represents the MAC address of the CM
     to which the multicast SAID authorization applies."
     ::= { docsBpi2CmtsMulticastAuthEntry 2 }

docsBpi2CmtsMulticastAuthControl   OBJECT-TYPE
     SYNTAX         RowStatus
     MAX-ACCESS     read-create
     STATUS         current
     DESCRIPTION
          "The status of this conceptual row for the
     authorization of multicast SAIDs to CMs."
     ::= { docsBpi2CmtsMulticastAuthEntry 3 }

--
-- CMTS Cert Objects
--

docsBpi2CmtsCertObjects OBJECT IDENTIFIER
     ::= { docsBpi2CmtsObjects 5 }

--
-- CMTS Provisioned CM Cert Table
--

docsBpi2CmtsProvisionedCmCertTable OBJECT-TYPE
     SYNTAX         SEQUENCE OF
                     DocsBpi2CmtsProvisionedCmCertEntry
```

```
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "A table of CM certificate trust entries provisioned
          to the CMTS.  The trust object for a certificate in this
          table has an overriding effect on the validity object of a
          certificate in the authorization table, as long as the
          entire contents of the two certificates are identical."
          ::= { docsBpi2CmtsCertObjects 1 }

     docsBpi2CmtsProvisionedCmCertEntry OBJECT-TYPE
          SYNTAX         DocsBpi2CmtsProvisionedCmCertEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "An entry in the CMTS's provisioned CM certificate
          table.  Row entries persist after re-initialization of
          the managed system."
          REFERENCE
               "Data-Over-Cable Service Interface Specifications:
          Operations Support System Interface Specification
          SP-OSSIv2.0-I05-040407, Section 6.2.14"
          INDEX { docsBpi2CmtsProvisionedCmCertMacAddress }
          ::= { docsBpi2CmtsProvisionedCmCertTable 1 }

     DocsBpi2CmtsProvisionedCmCertEntry ::= SEQUENCE
          {
          docsBpi2CmtsProvisionedCmCertMacAddress MacAddress,
          docsBpi2CmtsProvisionedCmCertTrust      INTEGER,
          docsBpi2CmtsProvisionedCmCertSource     INTEGER,
          docsBpi2CmtsProvisionedCmCertStatus     RowStatus,
          docsBpi2CmtsProvisionedCmCert
                                    DocsX509ASN1DEREncodedCertificate
          }

     docsBpi2CmtsProvisionedCmCertMacAddress OBJECT-TYPE
          SYNTAX         MacAddress
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "The index of this row."
          ::= { docsBpi2CmtsProvisionedCmCertEntry 1 }

     docsBpi2CmtsProvisionedCmCertTrust      OBJECT-TYPE
          SYNTAX    INTEGER {
                              trusted(1),
                              untrusted(2)
                              }
```

```
          MAX-ACCESS     read-create
          STATUS    current
          DESCRIPTION
               "Trust state for the provisioned CM certificate entry.
          Note: Setting this object need only override the validity
          of CM certificates sent in future authorization requests;
          instantaneous effect need not occur."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.4.1."
          DEFVAL { untrusted }
          ::= { docsBpi2CmtsProvisionedCmCertEntry 2 }

     docsBpi2CmtsProvisionedCmCertSource     OBJECT-TYPE
          SYNTAX    INTEGER {
                            snmp(1),
                            configurationFile(2),
                            externalDatabase(3),
                            other(4)
                            }
          MAX-ACCESS read-only
          STATUS  current
          DESCRIPTION
               "This object indicates how the certificate reached the
          CMTS.  Other(4) means that it originated from a source not
          identified above."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.4.1."
          ::= { docsBpi2CmtsProvisionedCmCertEntry 3 }

     docsBpi2CmtsProvisionedCmCertStatus OBJECT-TYPE
          SYNTAX  RowStatus
          MAX-ACCESS read-create
          STATUS  current
          DESCRIPTION
               "The status of this conceptual row.  Values in this row
          cannot be changed while the row is 'active'."
          ::= { docsBpi2CmtsProvisionedCmCertEntry 4 }

     docsBpi2CmtsProvisionedCmCert OBJECT-TYPE
          SYNTAX         DocsX509ASN1DEREncodedCertificate
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "An X509 DER-encoded Certificate Authority
          certificate.
          Note: The zero-length OCTET STRING must be returned, on
```

```
          reads, if the entire certificate is not retained in the
          CMTS."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.2."
          ::= { docsBpi2CmtsProvisionedCmCertEntry 5 }

     --
     -- CMTS CA Cert Table
     --

     docsBpi2CmtsCACertTable OBJECT-TYPE
          SYNTAX         SEQUENCE OF DocsBpi2CmtsCACertEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "The table of known Certificate Authority certificates
          acquired by this device."
          ::= { docsBpi2CmtsCertObjects 2 }

     docsBpi2CmtsCACertEntry OBJECT-TYPE
          SYNTAX         DocsBpi2CmtsCACertEntry
          MAX-ACCESS     not-accessible
          STATUS         current
          DESCRIPTION
               "A row in the Certificate Authority certificate
          table.  Row entries with the trust status 'trusted',
          'untrusted', or 'root' persist after re-initialization
           of the managed system."
          REFERENCE
               "Data-Over-Cable Service Interface Specifications:
          Operations Support System Interface Specification
          SP-OSSIv2.0-I05-040407, Section 6.2.14"
          INDEX   { docsBpi2CmtsCACertIndex }
          ::= {docsBpi2CmtsCACertTable 1 }

     DocsBpi2CmtsCACertEntry ::= SEQUENCE {
          docsBpi2CmtsCACertIndex            Unsigned32,
          docsBpi2CmtsCACertSubject          SnmpAdminString,
          docsBpi2CmtsCACertIssuer           SnmpAdminString,
          docsBpi2CmtsCACertSerialNumber     OCTET STRING,
          docsBpi2CmtsCACertTrust            INTEGER,
          docsBpi2CmtsCACertSource           INTEGER,
          docsBpi2CmtsCACertStatus           RowStatus,
          docsBpi2CmtsCACert
                                  DocsX509ASN1DEREncodedCertificate,
          docsBpi2CmtsCACertThumbprint       OCTET STRING
     }
```

```
docsBpi2CmtsCACertIndex OBJECT-TYPE
     SYNTAX         Unsigned32 (1.. 4294967295)
     MAX-ACCESS     not-accessible
     STATUS         current
     DESCRIPTION
          "The index for this row."
     ::= { docsBpi2CmtsCACertEntry 1 }

docsBpi2CmtsCACertSubject OBJECT-TYPE
     SYNTAX         SnmpAdminString
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The subject name exactly as it is encoded in the
     X509 certificate.
     The organizationName portion of the certificate's subject
     name must be present.  All other fields are optional.  Any
     optional field present must be prepended with <CR>
     (carriage return, U+000D) <LF> (line feed, U+000A).
     Ordering of fields present must conform to the following:

     organizationName <CR> <LF>
     countryName <CR> <LF>
     stateOrProvinceName <CR> <LF>
     localityName <CR> <LF>
     organizationalUnitName <CR> <LF>
     organizationalUnitName=<Manufacturing Location> <CR> <LF>
     commonName"
     REFERENCE
          "DOCSIS Baseline Privacy Plus Interface Specification,
     Section 9.2.4"
     ::= { docsBpi2CmtsCACertEntry 2 }

docsBpi2CmtsCACertIssuer OBJECT-TYPE
     SYNTAX         SnmpAdminString
     MAX-ACCESS     read-only
     STATUS         current
     DESCRIPTION
          "The issuer name exactly as it is encoded in the
     X509 certificate.
     The commonName portion of the certificate's issuer
     name must be present.  All other fields are optional.  Any
     optional field present must be prepended with <CR>
     (carriage return, U+000D) <LF> (line feed, U+000A).
     Ordering of fields present must conform to the following:

     CommonName <CR><LF>
     countryName <CR><LF>
```

```
          stateOrProvinceName <CR><LF>
          localityName <CR><LF>
          organizationName <CR><LF>
          organizationalUnitName <CR><LF>
          organizationalUnitName=<Manufacturing Location>"
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.2.4"
          ::= { docsBpi2CmtsCACertEntry 3 }

     docsBpi2CmtsCACertSerialNumber OBJECT-TYPE
          SYNTAX         OCTET STRING (SIZE (1..32))
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "This CA certificate's serial number, represented as
          an octet string."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.2.2"
          ::= { docsBpi2CmtsCACertEntry 4 }

     docsBpi2CmtsCACertTrust OBJECT-TYPE
          SYNTAX    INTEGER {
                            trusted (1),
                            untrusted (2),
                            chained (3),
                            root (4)
                            }
          MAX-ACCESS     read-create
          STATUS    current
          DESCRIPTION
               "This object controls the trust status of this
          certificate.  Root certificates must be given root(4)
          trust; manufacturer certificates must not be given root(4)
          trust.  Trust on root certificates must not change.
          Note: Setting this object need only affect the validity of
          CM certificates sent in future authorization requests;
          instantaneous effect need not occur."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.4.1"
          DEFVAL { chained }
          ::= { docsBpi2CmtsCACertEntry 5 }

     docsBpi2CmtsCACertSource OBJECT-TYPE
          SYNTAX    INTEGER {
                    snmp (1),
```

```
                    configurationFile (2),
                    externalDatabase (3),
                    other (4),
                    authentInfo (5),
                    compiledIntoCode (6)
                    }
          MAX-ACCESS     read-only
          STATUS    current
          DESCRIPTION
               "This object indicates how the certificate reached
          the CMTS.  Other(4) means that it originated from a source
          not identified above."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.4.1"
          ::= { docsBpi2CmtsCACertEntry 6 }

     docsBpi2CmtsCACertStatus OBJECT-TYPE
          SYNTAX         RowStatus
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "The status of this conceptual row.  An attempt
          to set writable columnar values while this row is active
          behaves as follows:
          - Sets to the object docsBpi2CmtsCACertTrust are allowed.
          - Sets to the object docsBpi2CmtsCACert will return an
            error of 'inconsistentValue'.
          A newly created entry cannot be set to active until the
          value of docsBpi2CmtsCACert is being set."
          ::= { docsBpi2CmtsCACertEntry 7 }

     docsBpi2CmtsCACert  OBJECT-TYPE
          SYNTAX         DocsX509ASN1DEREncodedCertificate
          MAX-ACCESS     read-create
          STATUS         current
          DESCRIPTION
               "An X509 DER-encoded Certificate Authority
          certificate.
          To help identify certificates, either this object or
          docsBpi2CmtsCACertThumbprint must be returned by a CMTS for
          self-signed CA certificates.

          Note: The zero-length OCTET STRING must be returned, on
          reads, if the entire certificate is not retained in the
          CMTS."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
```

```
          Section 9.2."
          ::= { docsBpi2CmtsCACertEntry 8 }

     docsBpi2CmtsCACertThumbprint OBJECT-TYPE
          SYNTAX         OCTET STRING (SIZE (20))
          MAX-ACCESS     read-only
          STATUS         current
          DESCRIPTION
               "The SHA-1 hash of a CA certificate.
          To help identify certificates, either this object or
          docsBpi2CmtsCACert must be returned by a CMTS for
          self-signed CA certificates.

          Note: The zero-length OCTET STRING must be returned, on
          reads, if the CA certificate thumb print is not retained
          in the CMTS."
          REFERENCE
               "DOCSIS Baseline Privacy Plus Interface Specification,
          Section 9.4.3"
          ::= { docsBpi2CmtsCACertEntry 9 }

     --
     -- Authenticated Software Download Objects
     --

     --
     -- Note: the authenticated software download objects are a
     -- CM requirement only.
     --

     docsBpi2CodeDownloadControl OBJECT IDENTIFIER
          ::= { docsBpi2MIBObjects 4 }

     docsBpi2CodeDownloadStatusCode     OBJECT-TYPE
          SYNTAX    INTEGER {
                            configFileCvcVerified (1),
                            configFileCvcRejected (2),
                            snmpCvcVerified (3),
                            snmpCvcRejected (4),
                            codeFileVerified (5),
                            codeFileRejected (6),
                            other (7)
                            }
          MAX-ACCESS     read-only
          STATUS    current
          DESCRIPTION
              "The value indicates the result of the latest config
          file CVC verification, SNMP CVC verification, or code file
```

```
            verification."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Sections D.3.3.2 and D.3.5.1."
            ::= { docsBpi2CodeDownloadControl 1 }

        docsBpi2CodeDownloadStatusString   OBJECT-TYPE
            SYNTAX         SnmpAdminString
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                "The value of this object indicates the additional
            information to the status code.  The value will include
            the error code and error description, which will be defined
            separately."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Section D.3.7"
            ::= { docsBpi2CodeDownloadControl 2 }

        docsBpi2CodeMfgOrgName   OBJECT-TYPE
            SYNTAX         SnmpAdminString
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                "The value of this object is the device manufacturer's
            organizationName."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Section D.3.2.2."
            ::= { docsBpi2CodeDownloadControl 3 }

        docsBpi2CodeMfgCodeAccessStart     OBJECT-TYPE
            SYNTAX         DateAndTime  (SIZE(11))
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                "The value of this object is the device manufacturer's
            current codeAccessStart value.  This value will always
            refer to Greenwich Mean Time (GMT), and the value
            format must contain TimeZone information (fields 8-10)."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Section D.3.2.2."
            ::= { docsBpi2CodeDownloadControl 4 }

        docsBpi2CodeMfgCvcAccessStart OBJECT-TYPE
            SYNTAX         DateAndTime (SIZE(11))
```

```
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                "The value of this object is the device manufacturer's
            current cvcAccessStart value.  This value will always
            refer to Greenwich Mean Time (GMT), and the value
            format must contain TimeZone information (fields 8-10)."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Section D.3.2.2."
            ::= { docsBpi2CodeDownloadControl 5 }

        docsBpi2CodeCoSignerOrgName   OBJECT-TYPE
            SYNTAX         SnmpAdminString
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                "The value of this object is the co-signer's
            organizationName.  The value is a zero length string if
            the co-signer is not specified."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Section D.3.2.2."
            ::= { docsBpi2CodeDownloadControl 6 }

        docsBpi2CodeCoSignerCodeAccessStart     OBJECT-TYPE
            SYNTAX         DateAndTime (SIZE(11))
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                "The value of this object is the co-signer's current
            codeAccessStart value.  This value will always refer to
            Greenwich Mean Time (GMT), and the value format must contain
            TimeZone information (fields 8-10).
            If docsBpi2CodeCoSignerOrgName is a zero
            length string, the value of this object is meaningless."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Section D.3.2.2."
            ::= { docsBpi2CodeDownloadControl 7 }

        docsBpi2CodeCoSignerCvcAccessStart OBJECT-TYPE
            SYNTAX         DateAndTime (SIZE(11))
            MAX-ACCESS     read-only
            STATUS         current
            DESCRIPTION
                "The value of this object is the co-signer's current
            cvcAccessStart value.  This value will always refer to
```

```
            Greenwich Mean Time (GMT), and the value format must contain
            TimeZone information (fields 8-10).
            If docsBpi2CodeCoSignerOrgName is a zero
            length string, the value of this object is meaningless."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Section D.3.2.2."
            ::= { docsBpi2CodeDownloadControl 8 }

        docsBpi2CodeCvcUpdate    OBJECT-TYPE
            SYNTAX         DocsX509ASN1DEREncodedCertificate
            MAX-ACCESS     read-write
            STATUS         current
            DESCRIPTION
                "Setting a CVC to this object triggers the device
            to verify the CVC and update the cvcAccessStart values.
            The content of this object is then discarded.
            If the device is not enabled to upgrade codefiles, or if
            the CVC verification fails, the CVC will be rejected.
            Reading this object always returns the zero-length OCTET
            STRING."
            REFERENCE
                "DOCSIS Baseline Privacy Plus Interface Specification,
            Section D.3.3.2.2."
            ::= { docsBpi2CodeDownloadControl 9 }

        --
        -- The BPI+ MIB Conformance Statements (with a placeholder for
        -- notifications)
        --

        docsBpi2Notification     OBJECT IDENTIFIER
            ::= { docsBpi2MIB 0 }
        docsBpi2Conformance OBJECT IDENTIFIER
            ::= { docsBpi2MIB 2 }
        docsBpi2Compliances OBJECT IDENTIFIER
            ::= { docsBpi2Conformance 1 }
        docsBpi2Groups      OBJECT IDENTIFIER
            ::= { docsBpi2Conformance 2 }


        docsBpi2CmCompliance MODULE-COMPLIANCE
            STATUS         current
            DESCRIPTION
                 "This is the compliance statement for CMs that
            implement the DOCSIS Baseline Privacy Interface Plus."

            MODULE  -- docsBpi2MIB
```

```
          -- unconditionally mandatory group
          MANDATORY-GROUPS {
                 docsBpi2CmGroup,
                 docsBpi2CodeDownloadGroup
          }

     -- constrain on Encryption algorithms
     OBJECT docsBpi2CmTEKDataEncryptAlg
          SYNTAX    DocsBpkmDataEncryptAlg {
                                 none(0),
                                 des56CbcMode(1),
                                 des40CbcMode(2)
                    }
          DESCRIPTION
               "It is compliant to support des56CbcMode(1) and
          des40CbcMode(2) for data encryption algorithms."

     -- constrain on Integrity algorithms
     OBJECT docsBpi2CmTEKDataAuthentAlg
          SYNTAX    DocsBpkmDataAuthentAlg {
                                 none(0)
                    }
          DESCRIPTION
               "It is compliant to not support data message
          authentication algorithms."

     -- constrain on IP addressing
     OBJECT    docsBpi2CmIpMulticastAddressType
          SYNTAX InetAddressType { ipv4(1) }
          DESCRIPTION
               "An implementation is only required to support IPv4
          addresses.  Support for other address types may be defined
          in future versions of this MIB module."

     -- constrain on IP addressing
     OBJECT    docsBpi2CmIpMulticastAddress
          SYNTAX  InetAddress (SIZE(4))
          DESCRIPTION
               "An implementation is only required to support IPv4
          addresses Other address types support may be defined in
          future versions of this MIB module."

     -- constrain on Encryption algorithms
     OBJECT docsBpi2CmCryptoSuiteDataEncryptAlg
          SYNTAX    DocsBpkmDataEncryptAlg {
                                 none(0),
                                 des56CbcMode(1),
                                 des40CbcMode(2)
```

```
                    }
          DESCRIPTION
               "It is compliant to only support des56CbcMode(1)
          and des40CbcMode(2) for data encryption algorithms."

     -- constrain on Integrity algorithms
     OBJECT docsBpi2CmCryptoSuiteDataAuthentAlg
          SYNTAX    DocsBpkmDataAuthentAlg {
                              none(0)
                    }
          DESCRIPTION
               "It is compliant to not support data message
          authentication algorithms."

     ::= { docsBpi2Compliances 1 }


     docsBpi2CmtsCompliance MODULE-COMPLIANCE
          STATUS         current
          DESCRIPTION
               "This is the compliance statement for CMTSs that
          implement the DOCSIS Baseline Privacy Interface Plus."

          MODULE  -- docsBpi2MIB
          -- unconditionally mandatory group
          MANDATORY-GROUPS {
                 docsBpi2CmtsGroup
          }

     -- unconditionally optional group
     GROUP     docsBpi2CodeDownloadGroup
          DESCRIPTION
               "This group is optional for CMTSes.  The implementation
          decision of this group is left to the vendor"

     -- constrain on mandatory range

     OBJECT    docsBpi2CmtsDefaultAuthLifetime
          SYNTAX    Integer32 (86400..6048000)
          DESCRIPTION
               "The refined range corresponds to the minimum and
          maximum values in operational networks."

     -- constrain on mandatory range

     OBJECT    docsBpi2CmtsDefaultTEKLifetime
          SYNTAX    Integer32 (1800..604800)
          DESCRIPTION
```

```
                "The refined range corresponds to the minimum and
            maximum values in operational networks."

        -- constrain on mandatory range

        OBJECT    docsBpi2CmtsAuthCmLifetime
             SYNTAX    Integer32 (86400..6048000)
             DESCRIPTION
                 "The refined range corresponds to the minimum and
            maximum values in operational networks."

        -- constrain on Encryption algorithms

    OBJECT   docsBpi2CmtsTEKDataEncryptAlg
            SYNTAX    DocsBpkmDataEncryptAlg {
                                none(0),
                                des56CbcMode(1),
                                des40CbcMode(2)
                      }
            DESCRIPTION
                 "It is compliant to only support des56CbcMode(1)
            and des40CbcMode(2) for data encryption."

        -- constrain on Integrity algorithms

    OBJECT docsBpi2CmtsTEKDataAuthentAlg
            SYNTAX    DocsBpkmDataAuthentAlg {
                                none(0)
                      }
            DESCRIPTION
                 "It is compliant to not support data message
            authentication algorithms."

        -- constrain on mandatory range

        OBJECT    docsBpi2CmtsTEKLifetime
             SYNTAX    Integer32 (1800..604800)
             DESCRIPTION
                 "The refined range corresponds to the minimum and
            maximum values in operational networks."

        -- constrain on access
        -- constrain on IP Addressing

        OBJECT    docsBpi2CmtsIpMulticastAddressType
             SYNTAX      InetAddressType { ipv4(1) }
             MIN-ACCESS  read-only
             DESCRIPTION
```

```
            "Write access is not required.
         An implementation is only required to support IPv4
         addresses.  Support for other address types may be defined
         in future versions of this MIB module."

      OBJECT    docsBpi2CmtsIpMulticastAddress
         SYNTAX  InetAddress (SIZE(4))
         MIN-ACCESS  read-only
         DESCRIPTION
            "Write access is not required.
         An implementation is only required to support IPv4
         addresses.  Support for other address types may be defined
         in future versions of this MIB module."

      OBJECT    docsBpi2CmtsIpMulticastMask
         SYNTAX  InetAddress (SIZE(4))
         MIN-ACCESS  read-only
         DESCRIPTION
            "Write access is not required.
         An implementation is only required to support IPv4
         addresses.  Support for other address types may be defined
         in future versions of this MIB module."

      -- constrain on access

      OBJECT    docsBpi2CmtsIpMulticastSAId
         MIN-ACCESS  read-only
         DESCRIPTION
            "Write access is not required."

      OBJECT    docsBpi2CmtsIpMulticastSAType
         MIN-ACCESS  read-only
         DESCRIPTION
            "Write access is not required."

      -- constrain on access
      -- constrain on Encryption algorithms

      OBJECT    docsBpi2CmtsIpMulticastDataEncryptAlg
         SYNTAX    DocsBpkmDataEncryptAlg {
                                 none(0),
                                 des56CbcMode(1),
                                 des40CbcMode(2)
                   }
         MIN-ACCESS  read-only
         DESCRIPTION
            "Write access is not required.
         It is compliant to only support des56CbcMode(1)
```

```
          and des40CbcMode(2) for data encryption"

      -- constrain on access
      -- constrain on Integrity algorithms

      OBJECT    docsBpi2CmtsIpMulticastDataAuthentAlg
           SYNTAX    DocsBpkmDataAuthentAlg {
                                 none(0)
                     }
           MIN-ACCESS  read-only
           DESCRIPTION
               "Write access is not required.
           It is compliant to not support data message
           authentication algorithms."

      -- constrain on access

      OBJECT    docsBpi2CmtsMulticastAuthControl
           MIN-ACCESS  read-only
           DESCRIPTION
          "Write access is not required."

           ::= { docsBpi2Compliances 2 }

      docsBpi2CmGroup     OBJECT-GROUP
           OBJECTS   {
                docsBpi2CmPrivacyEnable,
                docsBpi2CmPublicKey,
                docsBpi2CmAuthState,
                docsBpi2CmAuthKeySequenceNumber,
                docsBpi2CmAuthExpiresOld,
                docsBpi2CmAuthExpiresNew,
                docsBpi2CmAuthReset,
                docsBpi2CmAuthGraceTime,
                docsBpi2CmTEKGraceTime,
                docsBpi2CmAuthWaitTimeout,
                docsBpi2CmReauthWaitTimeout,
                docsBpi2CmOpWaitTimeout,
                docsBpi2CmRekeyWaitTimeout,
                docsBpi2CmAuthRejectWaitTimeout,
                docsBpi2CmSAMapWaitTimeout,
                docsBpi2CmSAMapMaxRetries,
                docsBpi2CmAuthentInfos,
                docsBpi2CmAuthRequests,
                docsBpi2CmAuthReplies,
                docsBpi2CmAuthRejects,
                docsBpi2CmAuthInvalids,
                docsBpi2CmAuthRejectErrorCode,
```

```
                docsBpi2CmAuthRejectErrorString,
                docsBpi2CmAuthInvalidErrorCode,
                docsBpi2CmAuthInvalidErrorString,
                docsBpi2CmTEKSAType,
                docsBpi2CmTEKDataEncryptAlg,
                docsBpi2CmTEKDataAuthentAlg,
                docsBpi2CmTEKState,
                docsBpi2CmTEKKeySequenceNumber,
                docsBpi2CmTEKExpiresOld,
                docsBpi2CmTEKExpiresNew,
                docsBpi2CmTEKKeyRequests,
                docsBpi2CmTEKKeyReplies,
                docsBpi2CmTEKKeyRejects,
                docsBpi2CmTEKInvalids,
                docsBpi2CmTEKAuthPends,
                docsBpi2CmTEKKeyRejectErrorCode,
                docsBpi2CmTEKKeyRejectErrorString,
                docsBpi2CmTEKInvalidErrorCode,
                docsBpi2CmTEKInvalidErrorString,
                docsBpi2CmIpMulticastAddressType,
                docsBpi2CmIpMulticastAddress,
                docsBpi2CmIpMulticastSAId,
                docsBpi2CmIpMulticastSAMapState,
                docsBpi2CmIpMulticastSAMapRequests,
                docsBpi2CmIpMulticastSAMapReplies,
                docsBpi2CmIpMulticastSAMapRejects,
                docsBpi2CmIpMulticastSAMapRejectErrorCode,
                docsBpi2CmIpMulticastSAMapRejectErrorString,
                docsBpi2CmDeviceCmCert,
                docsBpi2CmDeviceManufCert,
                docsBpi2CmCryptoSuiteDataEncryptAlg,
                docsBpi2CmCryptoSuiteDataAuthentAlg
                }
        STATUS          current
        DESCRIPTION
                "This collection of objects provides CM BPI+ status
        and control."
    ::= { docsBpi2Groups 1 }

    docsBpi2CmtsGroup   OBJECT-GROUP
        OBJECTS {
                docsBpi2CmtsDefaultAuthLifetime,
                docsBpi2CmtsDefaultTEKLifetime,
                docsBpi2CmtsDefaultSelfSignedManufCertTrust,
                docsBpi2CmtsCheckCertValidityPeriods,
                docsBpi2CmtsAuthentInfos,
                docsBpi2CmtsAuthRequests,
                docsBpi2CmtsAuthReplies,
```

```
                docsBpi2CmtsAuthRejects,
                docsBpi2CmtsAuthInvalids,
                docsBpi2CmtsSAMapRequests,
                docsBpi2CmtsSAMapReplies,
                docsBpi2CmtsSAMapRejects,
                docsBpi2CmtsAuthCmBpiVersion,
                docsBpi2CmtsAuthCmPublicKey,
                docsBpi2CmtsAuthCmKeySequenceNumber,
                docsBpi2CmtsAuthCmExpiresOld,
                docsBpi2CmtsAuthCmExpiresNew,
                docsBpi2CmtsAuthCmLifetime,
                docsBpi2CmtsAuthCmReset,
                docsBpi2CmtsAuthCmInfos,
                docsBpi2CmtsAuthCmRequests,
                docsBpi2CmtsAuthCmReplies,
                docsBpi2CmtsAuthCmRejects,
                docsBpi2CmtsAuthCmInvalids,
                docsBpi2CmtsAuthRejectErrorCode,
                docsBpi2CmtsAuthRejectErrorString,
                docsBpi2CmtsAuthInvalidErrorCode,
                docsBpi2CmtsAuthInvalidErrorString,
                docsBpi2CmtsAuthPrimarySAId,
                docsBpi2CmtsAuthBpkmCmCertValid,
                docsBpi2CmtsAuthBpkmCmCert,
                docsBpi2CmtsAuthCACertIndexPtr,
                docsBpi2CmtsTEKSAType,
                docsBpi2CmtsTEKDataEncryptAlg,
                docsBpi2CmtsTEKDataAuthentAlg,
                docsBpi2CmtsTEKLifetime,
                docsBpi2CmtsTEKKeySequenceNumber,
                docsBpi2CmtsTEKExpiresOld,
                docsBpi2CmtsTEKExpiresNew,
                docsBpi2CmtsTEKReset,
                docsBpi2CmtsKeyRequests,
                docsBpi2CmtsKeyReplies,
                docsBpi2CmtsKeyRejects,
                docsBpi2CmtsTEKInvalids,
                docsBpi2CmtsKeyRejectErrorCode,
                docsBpi2CmtsKeyRejectErrorString,
                docsBpi2CmtsTEKInvalidErrorCode,
                docsBpi2CmtsTEKInvalidErrorString,
                docsBpi2CmtsIpMulticastAddressType,
                docsBpi2CmtsIpMulticastAddress,
                docsBpi2CmtsIpMulticastMask,
                docsBpi2CmtsIpMulticastSAId,
                docsBpi2CmtsIpMulticastSAType,
                docsBpi2CmtsIpMulticastDataEncryptAlg,
                docsBpi2CmtsIpMulticastDataAuthentAlg,
```

```
            docsBpi2CmtsIpMulticastSAMapRequests,
            docsBpi2CmtsIpMulticastSAMapReplies,
            docsBpi2CmtsIpMulticastSAMapRejects,
            docsBpi2CmtsIpMulticastSAMapRejectErrorCode,
            docsBpi2CmtsIpMulticastSAMapRejectErrorString,
            docsBpi2CmtsIpMulticastMapControl,
            docsBpi2CmtsIpMulticastMapStorageType,
            docsBpi2CmtsMulticastAuthControl,
            docsBpi2CmtsProvisionedCmCertTrust,
            docsBpi2CmtsProvisionedCmCertSource,
            docsBpi2CmtsProvisionedCmCertStatus,
            docsBpi2CmtsProvisionedCmCert,
            docsBpi2CmtsCACertSubject,
            docsBpi2CmtsCACertIssuer,
            docsBpi2CmtsCACertSerialNumber,
            docsBpi2CmtsCACertTrust,
            docsBpi2CmtsCACertSource,
            docsBpi2CmtsCACertStatus,
            docsBpi2CmtsCACert,
            docsBpi2CmtsCACertThumbprint
            }
        STATUS         current
        DESCRIPTION
            "This collection of objects provides CMTS BPI+ status
        and control."
    ::= { docsBpi2Groups 2 }

    docsBpi2CodeDownloadGroup OBJECT-GROUP
            OBJECTS {
            docsBpi2CodeDownloadStatusCode,
            docsBpi2CodeDownloadStatusString,
            docsBpi2CodeMfgOrgName,
            docsBpi2CodeMfgCodeAccessStart,
            docsBpi2CodeMfgCvcAccessStart,
            docsBpi2CodeCoSignerOrgName,
            docsBpi2CodeCoSignerCodeAccessStart,
            docsBpi2CodeCoSignerCvcAccessStart,
            docsBpi2CodeCvcUpdate
            }
        STATUS         current
        DESCRIPTION
            "This collection of objects provides authenticated
        software download support."
    ::= { docsBpi2Groups 3 }

    END
```

4. Acknowledgements

Kaz Ozawa: Authenticated Software Download objects and general suggestions.

Rich Woundy: BPI MIB and general MIB expertise.

Mike St. Johns: BPI MIB and first version of BPI+ MIB.

Bert Wijnen: Extensive comments in MIB syntax and accuracy.

Thanks to Mike Sabin and Manson Wong for reviewing early BPI+ MIB drafts and to Jean-Francois Mule for contributing to the last versions.

5. Normative References

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

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

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

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

[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 J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC 4001, February 2005.

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

[RFC2670] St. Johns, M., "Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces", RFC 2670, August 1999.

[DOCSIS] "Data-Over-Cable Service Interface Specifications: Baseline Privacy Plus Interface Specification SP-BPI+-I11-040407", DOCSIS, April 2004, available at http://www.cablemodem.com. http://www.cablelabs.com/specifications/archives.

6. Informative References

[RFC3083] Woundy, R., "Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems", RFC 3083, March 2001.

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

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[DOCSIS-1.0] "Data-Over-Cable Service Interface Specifications: DOCSIS 1.0 Baseline Privacy Interface (BPI) ANSI/SCTE 22-2 2202, Available at http://www.scte.org.

[DOCSIS-1.1] "Data-Over-Cable Service Interface Specifications: Operations Support System Interface Specification SP-OSSIv1.1-I07-030730", DOCSIS 1.1 July 2003, available at http://www.cablemodem.com. http://www.cablelabs.com/specifications/archives.

[DOCSIS-2.0] "Data-Over-Cable Service Interface Specifications: Operations Support System Interface Specification SP-OSSIv2.0-I05-040407", DOCSIS 2.0 April 2004, http://www.cablemodem.com. http://www.cablelabs.com/specifications/archives.

[IANA] "Protocol Numbers and Assignment Services", IANA, http://www.iana.org/assignments/ianaiftype-mib.

7. Security Considerations

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:

- The following objects, if SNMP SET maliciously, could constitute denial of service or theft of service attacks or compromise the intended data privacy of users:

Objects related to the Baseline Privacy Key Management (BPKM)

docsBpi2CmAuthReset,
docsBpi2CmtsAuthCmReset,
docsBpi2CmtsTEKReset:
: These objects are used for initiating a re-key process. A malicious massive SET attack may cause CMTS processing overload and may compromise the service.

docsBpi2CmtsDefaultAuthLifetime,
docsBpi2CmtsDefaultTEKLifetime,
docsBpi2CmtsAuthCmLifetime,
docsBpi2CmtsTEKLifetime:
: To minimize the risk of malicious or unintended short periods of time when key updates may lead to degradation or denial of service, implementers are encouraged to follow these objects' range constraints, as defined in the docsBpi2CmtsCompliance MODULE-COMPLIANCE clause for operational deployments.

docsBpi2CmtsDefaultSelfSignedManufCertTrust:
: A malicious SET in a self-signed certificate as reject message, which may constitute denial of service. This object is designed for testing purposes; therefore, it is not RECOMMENDED for use in commercial deployments [DOCSIS]. Administrators can make use of View-based Access Control (VACM) introduced in section 7.9 of [RFC3410] to restrict write access to this object.

docsBpi2CmtsCheckCertValidityPeriods:
: A malicious SET in this object that enables the period validity and a wrong clock time in the CMTS could cause denial of service, as CM authorization requests will be rejected.

For more details in the validation of CM certificates, refer to section 9 of [DOCSIS] .

Objects related to the CM only:

Objects in docsBpi2CmDeviceCertTable

docsBpi2CmDeviceCmCert:
This object is not harmful, considering that a CM received a Certificate during the manufacturing process. Therefore, the object access becomes read-only. See the object DESCRIPTION clause in section 3 for details.

Objects for Secure Software Download in table docsBpi2CodeDownloadControl:

docsBpi2CodeCvcUpdate:
A malicious SET on this object may not constitute a risk, since the CM holds the DOCSIS root key to verify the CVC authenticity. The operator, if configured, could receive a notification for event occurrences, which may lead to detecting the source of the attack. Moreover, [DOCSIS] recommends that CMs CVC be regularly updated to minimize the risk of potential code-signing keys being compromised (e.g., by configuration file).

Objects related to the CMTS only:

Objects in docsBpi2CmtsProvisionedCmCertTable and docsBpi2CmtsCACertTable containing CM Certificates and Certificate Authority information, respectively:

docsBpi2CmtsProvisionedCmCertTrust,
docsBpi2CmtsProvisionedCmCertStatus,
docsBpi2CmtsProvisionedCmCert,
docsBpi2CmtsCACertStatus,
docsBpi2CmtsCACert:
A malicious SET on these objects may constitute a denial of service attack that will be experienced after the CMs perform authorization requests. It does not affect CMs in the authorized state.

Objects in multicast tables docsBpi2CmtsIpMulticastMapTable and docsBpi2CmtsMulticastAuthTable:

docsBpi2CmtsIpMulticastAddressType,
docsBpi2CmtsIpMulticastAddress,
docsBpi2CmtsIpMulticastMaskType,

docsBpi2CmtsIpMulticastMask,
docsBpi2CmtsIpMulticastSAId,
docsBpi2CmtsIpMulticastSAType:
Malicious SET on these objects may cause misconfiguration, causing interruption of the users' active multicast applications.

docsBpi2CmtsIpMulticastDataEncryptAlg,
docsBpi2CmtsIpMulticastDataAuthentAlg:
Malicious SETs on these objects may create service misconfiguration, causing service interruption or theft of service if encryption algorithms are removed for the multicast groups.

docsBpi2CmtsIpMulticastMapControl,
docsBpi2CmtsMulticastAuthControl:
Malicious SETs on these objects may remove and/or disable customers and/or multicast groups, causing service disruption. This may also constitute theft of service by authorizing non-subscribed users to multicast groups or by adding other multicast groups in the forward path.

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:

Objects in docsBpi2CmBaseTable, docsBpi2CmTEKTable, docsBpi2CmtsBaseTable, docsBpi2CmtsAuthTable, docsBpi2CmtsTEKTable, docsBpi2CmtsProvisionedCmCertTable, and docsBpi2CmtsCACertTable:
If this information is accessible, attackers may use it to distinguish users configured to work without data encryption (e.g., docsBpi2CmPrivacyEnable) and to know current Baseline Privacy parameters in the network.

Objects in docsBpi2CmIpMulticastMapTable and docsBpi2CmtsMulticastAuthTable:
In addition to the vulnerabilities around BPI plus multicast objects described in the previous part, the read-only objects of this table may help attackers monitor the status of the intrusion.

Objects in docsBpi2CodeDownloadControl:
In addition to the vulnerability of the read-write object docsBpi2CodeCvcUpdate, attackers may be able to monitor the status of a denial of service using Secure Software Download.

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

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

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

BPI+ Encryption Algorithms:

The BPI+ Traffic Encryption Keys (TEK) defined in the DOCSIS BPI+ specification [DOCSIS] use 40-bit or 56-bit DES for encryption (DES CBC mode). Currently, there is no mechanism or algorithm defined for data integrity.

Due to the DES cryptographic weaknesses, future revisions of the DOCSIS BPI+ specification should introduce more advanced encryption algorithms, as proposed in the DocsBpkmDataEncryptAlg textual convention, to overcome the progress in cheaper and faster hardware or software decryption tools. Future revisions of the DOCSIS BPI+ specification [DOCSIS] should also adopt authentication algorithms, as described in the DocsBpkmDataAuthentAlg textual convention.

It is important to note that frequent key changes do not necessarily help in mitigating or reducing the risks of a DES attack. Indeed, the traffic encryption keys, which are configured on a per cable modem basis and per BPI+ multicast group, can be utilized to decrypt old traffic, even when they are no longer in active use.

Note that, not exempt to the same recommendations above, the CM BPI+ authorization protocol uses triple DES encryption, which offers improved robustness in comparison to DES for CM authorization and TEK re-key management.

8. IANA Considerations

The MIB module in this document uses the following IANA-assigned OBJECT IDENTIFIER value, recorded in the SMI Numbers registry:

Descriptor	OBJECT IDENTIFIER Value
docsBpi2MIB	{ mib-2 126 }

Authors' Addresses

Stuart M. Green

EMail: rubbersoul3@yahoo.com

Kaz Ozawa
Automotive Systems Development Center
TOSHIBA CORPORATION
1-1, Shibaura 1-Chome
Minato-ku, Tokyo 105-8001
Japan

Phone: +81-3-3457-8569
Fax: +81-3-5444-9325
EMail: Kazuyoshi.Ozawa@toshiba.co.jp

Alexander Katsnelson

Phone: +1-303-680-3924
EMail: katsnelson6@peoplepc.com

Eduardo Cardona
Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville, CO 80027- 9750
U.S.A.

Phone: +1 303 661 9100
EMail: e.cardona@cablelabs.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.