Network Working Group
Request for Comments: 3083
Category: Informational

R. Woundy
Cisco Systems

March 2001

Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines a basic set of managed objects for SNMP-based (Simple Network Management Protocol) management of the Baseline Privacy Interface (BPI), which provides data privacy for DOCSIS 1.0 (Data-Over-Cable Service Interface Specifications) compliant Cable Modems and Cable Modem Termination Systems. This MIB is defined as an extension to the DOCSIS Radio Frequency Interface MIB, RFC 2670.

This memo specifies a MIB module in a manner that is compliant to the SMIv2 (Structure of Management Information Version 2). The set of objects is consistent with the SNMP framework and existing SNMP standards.

CableLabs requires the implementation of this MIB in DOCSIS 1.0 cable modems that implement the Baseline Privacy Interface, as a prerequisite for DOCSIS 1.0 certification.

Table of Contents

1. The SNMP Management Framework

The SNMP Management Framework presently consists of five major components:

- An overall architecture, described in RFC 2571 [1].

- Mechanisms for describing and naming objects and events for the purpose of management. The first version of this Structure of Management Information (SMI) is called SMIv1 and described in STD 16, RFC 1155 [2], STD 16, RFC 1212 [3] and RFC 1215 [4]. The second version, called SMIv2, is described in STD 58, RFC 2578 [5], RFC 2579 [6] and RFC 2580 [7].

- Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in STD 15, RFC 1157 [8]. A second version of the SNMP

message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in RFC 1901 [9] and RFC 1906 [10]. The third version of the message protocol is called SNMPv3 and described in RFC 1906 [10], RFC 2572 [11] and RFC 2574 [12].

- o Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in STD 15, RFC 1157 [8]. A second set of protocol operations and associated PDU formats is described in RFC 1905 [13].

- o A set of fundamental applications described in RFC 2573 [14] and the view-based access control mechanism described in RFC 2575 [15].

A more detailed introduction to the current SNMP Management Framework can be found in RFC 2570 [24].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the mechanisms defined in the SMI.

This memo specifies a MIB module that is compliant to the SMIv2. A MIB conforming to the SMIv1 can be produced through the appropriate translations. The resulting translated MIB must be semantically equivalent, except where objects or events are omitted because no translation is possible (use of Counter64). Some machine readable information in SMIv2 will be converted into textual descriptions in SMIv1 during the translation process. However, this loss of machine readable information is not considered to change the semantics of the MIB.

2. Glossary

The terms in this document are derived either from normal cable system usage, or from the documents associated with the Data Over Cable Service Interface Specification process.

2.1. Authorization key

A key used to derive a key encryption key (used to encrypt TEKs), and to derive message authentication keys. When the CMTS communicates the authorization key to the CM, it encrypts the authorization key using the RSA public key of the CM [22].

2.2. BPI - Baseline Privacy Interface

A term referring to the DOCSIS specification [18] for enabling simple data privacy in the DOCSIS 1.0 system. Management of the BPI is the focus of this document.

2.3. BPI+ - Baseline Privacy Plus Interface

A term referring to the DOCSIS specification [21] for enabling CM authentication and data privacy in the DOCSIS 1.1 system. Management of the BPI+ is not addressed in this document.

2.4. CATV

Originally "Community Antenna Television", now used to refer to any cable or hybrid fiber and cable system used to deliver video signals to a community.

2.5. CM - Cable Modem

A CM acts as a "slave" station in a DOCSIS compliant cable data system.

2.6. CMTS - Cable Modem Termination System

A generic term covering a cable bridge or cable router in a head-end. A CMTS acts as the master station in a DOCSIS compliant cable data system. It is the only station that transmits downstream, and it controls the scheduling of upstream transmissions by its associated CMs.

2.7. DOCSIS

"Data-Over-Cable Service Interface Specifications". A term referring to the ITU-T J.112 Annex B standard for cable modem systems [19].

2.8. Downstream

The direction from the head-end towards the subscriber.

2.9. Head-end

The origination point in most cable systems of the subscriber video signals. Generally also the location of the CMTS equipment.

2.10. MAC Packet

A DOCSIS PDU.

2.11. MCNS

"Multimedia Cable Network System". Generally replaced in usage by DOCSIS.

2.12. RF

Radio Frequency.

2.13 SID

Service ID. The SID identifies a particular upstream bandwidth allocation and class-of-service management for DOCSIS, and identifies a particular bidirectional security association for BPI.

2.14. TEK - Traffic Encryption Key

Traffic Encryption Key, which is used for DES encryption of upstream and downstream traffic. When the CMTS communicates the TEK to the CM, it encrypts the TEK using the key encryption key derived from the authorization key.

2.15. Upstream

The direction from the subscriber towards the head-end.

3. Overview

This MIB provides a set of objects required for the management of the Baseline Privacy Interface for DOCSIS compliant Cable Modems (CMs) and Cable Modem Termination Systems (CMTSs). This MIB specification is derived from the DOCSIS Baseline Privacy Interface specification [18], which is an extension to the DOCSIS Radio Frequency Interface specification [19].

Please note that this MIB specification is not sufficient for the management of the DOCSIS Baseline Privacy Plus Interface specification [21]. The working group expects to issue a MIB for the management of BPI+ at a later time.

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 [23].

3.1. Structure of the MIB

This MIB consists of one group of CM-only objects (docsBpiCmGroup), and one group of CMTS-only objects (docsBpiCmtsGroup).

The CM-only objects are organized into two tables:

- The docsBpiCmBaseTable contains objects for managing basic Baseline Privacy parameters and counters, and for managing the Authorization finite state machine.

- The docsBpiCmTEKTable contains objects for managing the Traffic Encryption Key (TEK) finite state machine per SID.

The CMTS-only objects are organized into four sub-groups:

- The docsBpiCmtsBaseTable contains objects for managing basic Baseline Privacy parameters and counters.

- The docsBpiCmtsAuthTable contains objects for managing the Authorization association information per cable modem.

- The docsBpiCmtsTEKTable contains objects for managing the TEK association information per SID.

- The docsBpiMulticastControl consists of two tables. The docsBpiIpMulticastMapTable controls the mapping of downstream IP multicast data traffic to downstream multicast SID values. The docsBpiMulticastAuthTable controls which CMs are authorized to receive downstream traffic transmitted over particular multicast SIDs; a CM will receive TEKs corresponding to the multicast SIDs for which it is authorized. The combination of these two tables will limit the distribution of downstream IP multicast data traffic to authorized CMs.

3.2. Management requirements

The Baseline Privacy Interface specification is documented in [18], and is an extension to the Radio Frequency Interface specification documented in [19]. In addition to the explicit requirements in this specification, the CM and CMTS enabled for Baseline Privacy MUST support all applicable DOCSIS and IETF requirements and MIB objects. Specifications that identify relevant requirements and MIB objects include the IETF Radio Frequency MIB [16], the IETF Cable Device MIB [17], and the DOCSIS OSSI Specification [20].

The explicit management requirements of the Baseline Privacy Interface, which motivate the development of the MIB in this document, are detailed below:

- The CM and CMTS MUST support viewing relevant RSA public keys, for future subscriber authentication applications.

- The Baseline Privacy management interface needs to support operator configuration of Authorization and TEK Finite State Machine (FSM) parameters, for performance tuning and security incident handling. The CMTS MUST support viewing (and configuring if possible) all FSM-related parameters, including baseline privacy status (enabled or disabled), key lifetimes, key grace times, and state timeout values. The CM MUST support viewing these parameters where possible.

- The management interface needs to support operator analysis and override of FSM behavior, for fault management, subscriber service de-provisioning, and security incident handling. The CM MUST support viewing the current FSM states. The CM and CMTS MUST support viewing message error codes and message error strings, and counters for invalid KEK and TEK events, for key expirations and renewals, and for duplicate messages. The CM and CMTS MUST support viewing current authorization key sequence numbers and key expiration times for failure diagnosis.

- The management interface needs to support dynamic control of the distribution of IP multicast data traffic. This control includes forwarding IP multicast traffic to the correct multicast group (SID), and managing the membership lists of each multicast group (SID). The CMTS MUST support configuring and viewing all IP multicast forwarding state, and all multicast group memberships, within the MAC domains of the CMTS.

3.3. Textual convention

CableLabs has required the implementation of prior versions of this MIB in DOCSIS 1.0 cable modems that implement the Baseline Privacy Interface, as a prerequisite for DOCSIS 1.0 certification.

The Baseline Privacy Interface MIB contains eight MIB objects defined with the (now obsolete) DisplayString textual convention, and one MIB object defined with the (now undesirable) IpAddress textual convention.

In the judgment of the working group, it is preferable to keep these less-than-desirable textual conventions, in order to maintain backward compatibility and interoperability with DOCSIS 1.0 cable modems that implemented previous versions of this MIB.

4. Definitions

```
DOCS-BPI-MIB DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY, OBJECT-TYPE,
Integer32, Counter32, IpAddress
FROM SNMPv2-SMI
DisplayString, MacAddress, RowStatus, TruthValue, DateAndTime
FROM SNMPv2-TC
OBJECT-GROUP, MODULE-COMPLIANCE
FROM SNMPv2-CONF
ifIndex
FROM IF-MIB
docsIfMib, docsIfCmServiceId, docsIfCmtsServiceId
FROM DOCS-IF-MIB
;

docsBpiMIB      MODULE-IDENTITY
LAST-UPDATED "200103130000Z"
ORGANIZATION "IETF IPCDN Working Group"
CONTACT-INFO "Rich Woundy
              Postal: Cisco Systems
                      250 Apollo Drive
                      Chelmsford, MA 01824 U.S.A.
              Tel: +1 978 244 8000
              E-mail: rwoundy@cisco.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
                         Andrew Valentine, a.valentine@eu.hns.com"
DESCRIPTION
"This is the MIB Module for the DOCSIS Baseline Privacy Interface
(BPI) at cable modems (CMs) and cable modem termination systems
(CMTSs). CableLabs requires the implementation of this MIB in
DOCSIS 1.0 cable modems that implement the Baseline Privacy
Interface, as a prerequisite for DOCSIS 1.0 certification."

REVISION "200103130000Z"
DESCRIPTION
"Version published as RFC 3083."

REVISION "200011031930Z"
DESCRIPTION
"Modified by Richard Woundy to fix problems identified by the MIB
```

```
doctor. I marked docsBpiCmtsDefaultAuthGraceTime and
docsBpiCmtsDefaultTEKGraceTime as obsolete objects, to prevent OID
reassignment. Several object descriptions were also corrected."

REVISION "200002161930Z"
DESCRIPTION
"Initial version.
CableLabs requires the implementation of this MIB in certified DOCSIS
1.0 cable modems implementing the Baseline Privacy Interface, per
DOCSIS 1.0 engineering change notice oss-n-99027."
::= { docsIfMib 5 }

docsBpiMIBObjects  OBJECT IDENTIFIER ::= { docsBpiMIB 1 }

-- Cable Modem Group

docsBpiCmObjects OBJECT IDENTIFIER ::= { docsBpiMIBObjects 1 }

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

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

docsBpiCmBaseEntry      OBJECT-TYPE
SYNTAX                  DocsBpiCmBaseEntry
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 }
::= { docsBpiCmBaseTable 1 }

DocsBpiCmBaseEntry ::= SEQUENCE {
docsBpiCmPrivacyEnable                  TruthValue,
docsBpiCmPublicKey                      OCTET STRING,
docsBpiCmAuthState                      INTEGER,
docsBpiCmAuthKeySequenceNumber          Integer32,
docsBpiCmAuthExpires                    DateAndTime,
```

```
docsBpiCmAuthReset                      TruthValue,
docsBpiCmAuthGraceTime                  Integer32,
docsBpiCmTEKGraceTime                   Integer32,
docsBpiCmAuthWaitTimeout                Integer32,
docsBpiCmReauthWaitTimeout              Integer32,
docsBpiCmOpWaitTimeout                  Integer32,
docsBpiCmRekeyWaitTimeout               Integer32,
docsBpiCmAuthRejectWaitTimeout          Integer32,
docsBpiCmAuthRequests                   Counter32,
docsBpiCmAuthReplies                    Counter32,
docsBpiCmAuthRejects                    Counter32,
docsBpiCmAuthInvalids                   Counter32,
docsBpiCmAuthRejectErrorCode            INTEGER,
docsBpiCmAuthRejectErrorString          DisplayString,
docsBpiCmAuthInvalidErrorCode           INTEGER,
docsBpiCmAuthInvalidErrorString         DisplayString
}

docsBpiCmPrivacyEnable  OBJECT-TYPE
SYNTAX                  TruthValue
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"This object identifies whether this CM is provisioned to run
Baseline Privacy. This is analogous to the presence (or absence)
of the Baseline Privacy Configuration Setting option. The status
of each individual SID with respect to Baseline Privacy is
captured in the docsBpiCmTEKPrivacyEnable object."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.1.1."
::= { docsBpiCmBaseEntry 1 }

docsBpiCmPublicKey      OBJECT-TYPE
SYNTAX                  OCTET STRING (SIZE (74 | 106 | 140 | 270))
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) [22],
corresponding to the public key of the CM. The 74, 106, 140, and
270 byte key encoding lengths correspond to 512 bit, 768 bit, 1024
bit, and 2048 public moduli respectively."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.2.4."
::= { docsBpiCmBaseEntry 2 }

docsBpiCmAuthState      OBJECT-TYPE
SYNTAX                  INTEGER {
```

```
                                authWait(2),
                                authorized(3),
                                reauthWait(4),
                                authRejectWait(5)
                            }
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 Interface Specification, Section 4.1.2.1."
::= { docsBpiCmBaseEntry 3 }

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

docsBpiCmAuthExpires    OBJECT-TYPE
SYNTAX                  DateAndTime
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the actual clock time when the current
authorization for this FSM expires. If the CM does not have an active
authorization, then the value is of the expiration date and time of
the last active authorization."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.2
and 4.2.2.9."
::= { docsBpiCmBaseEntry 5 }

docsBpiCmAuthReset      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."
REFERENCE
```

```
"DOCSIS Baseline Privacy Interface Specification, Section 4.1.2.3.4."
::= { docsBpiCmBaseEntry 6 }

docsBpiCmAuthGraceTime  OBJECT-TYPE
SYNTAX                  Integer32 (1..1800)
UNITS                   "seconds"
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the grace time for an authorization key.
A CM is expected to start trying to get a new authorization key
beginning AuthGraceTime seconds before the authorization key actually
expires."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.1.1.1.3."
::= { docsBpiCmBaseEntry 7 }

docsBpiCmTEKGraceTime   OBJECT-TYPE
SYNTAX                  Integer32 (1..1800)
UNITS                   "seconds"
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the grace time for a TEK.  A CM is
expected to start trying to get a new TEK beginning TEKGraceTime
seconds before the TEK actually expires."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.1.1.1.6."
::= { docsBpiCmBaseEntry 8 }

docsBpiCmAuthWaitTimeout        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."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.1.1.1.1."
::= { docsBpiCmBaseEntry 9 }

docsBpiCmReauthWaitTimeout      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 Interface Specification, Appendix A.1.1.1.2."
::= { docsBpiCmBaseEntry 10 }

docsBpiCmOpWaitTimeout  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 Interface Specification, Appendix A.1.1.1.4."
::= { docsBpiCmBaseEntry 11 }

docsBpiCmRekeyWaitTimeout       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 Interface Specification, Appendix A.1.1.1.5."
::= { docsBpiCmBaseEntry 12 }

docsBpiCmAuthRejectWaitTimeout  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 Interface Specification, Appendix A.1.1.1.7."
::= { docsBpiCmBaseEntry 13 }

docsBpiCmAuthRequests   OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CM has
transmitted an Authorization Request message."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.1."
::= { docsBpiCmBaseEntry 14 }
```

```
docsBpiCmAuthReplies    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 Reply message."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.2."
::= { docsBpiCmBaseEntry 15 }

docsBpiCmAuthRejects    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 Reject message."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.3."
::= { docsBpiCmBaseEntry 16 }

docsBpiCmAuthInvalids   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."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.7."
::= { docsBpiCmBaseEntry 17 }

docsBpiCmAuthRejectErrorCode    OBJECT-TYPE
SYNTAX                          INTEGER {
                                        none(1),
                                        unknown(2),
                                        unauthorizedCm(3),
                                        unauthorizedSid(4)
                                }
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the enumerated description of the
Error-Code in most recent Authorization Reject message received by
the CM.  This has 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 Interface Specification, Sections 4.2.1.3
and 4.2.2.16."
::= { docsBpiCmBaseEntry 18 }

docsBpiCmAuthRejectErrorString  OBJECT-TYPE
SYNTAX                          DisplayString (SIZE (0..128))
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the Display-String in 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 Interface Specification, Sections 4.2.1.3
and 4.2.2.6."
::= { docsBpiCmBaseEntry 19 }

docsBpiCmAuthInvalidErrorCode   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 most recent Authorization Invalid message received by
the CM.  This has 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 Interface Specification, Sections 4.2.1.7
and 4.2.2.16."
::= { docsBpiCmBaseEntry 20 }

docsBpiCmAuthInvalidErrorString OBJECT-TYPE
SYNTAX                          DisplayString (SIZE (0..128))
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the Display-String in 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 Interface Specification, Sections 4.2.1.7
and 4.2.2.6."
::= { docsBpiCmBaseEntry 21 }

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

docsBpiCmTEKTable       OBJECT-TYPE
SYNTAX                  SEQUENCE OF     DocsBpiCmTEKEntry
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 SID per CM MAC interface."
::= { docsBpiCmObjects 2 }

docsBpiCmTEKEntry       OBJECT-TYPE
SYNTAX                  DocsBpiCmTEKEntry
MAX-ACCESS              not-accessible
STATUS                  current
DESCRIPTION
"Each entry contains objects describing the TEK association attributes
of one SID. The CM MUST create one entry per unicast SID, regardless
of whether the SID was obtained from a Registration Response message,
or from an Authorization Reply message."
INDEX                   { ifIndex, docsIfCmServiceId }
::= { docsBpiCmTEKTable 1 }

DocsBpiCmTEKEntry ::= SEQUENCE {
docsBpiCmTEKPrivacyEnable               TruthValue,
docsBpiCmTEKState                       INTEGER,
docsBpiCmTEKExpiresOld                  DateAndTime,
docsBpiCmTEKExpiresNew                  DateAndTime,
docsBpiCmTEKKeyRequests                 Counter32,
docsBpiCmTEKKeyReplies                  Counter32,
docsBpiCmTEKKeyRejects                  Counter32,
docsBpiCmTEKInvalids                    Counter32,
docsBpiCmTEKAuthPends                   Counter32,
docsBpiCmTEKKeyRejectErrorCode          INTEGER,
docsBpiCmTEKKeyRejectErrorString        DisplayString,
docsBpiCmTEKInvalidErrorCode            INTEGER,
docsBpiCmTEKInvalidErrorString          DisplayString
}
```

```
docsBpiCmTEKPrivacyEnable       OBJECT-TYPE
SYNTAX                          TruthValue
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"This object identifies whether this SID is provisioned to run
Baseline Privacy. This is analogous to enabling Baseline Privacy on
a provisioned SID using the Class-of-Service Privacy Enable option.
Baseline Privacy is not effectively enabled for any SID unless
Baseline Privacy is enabled for the CM, which is managed via the
docsBpiCmPrivacyEnable object."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.1.2."
::= { docsBpiCmTEKEntry 1 }

docsBpiCmTEKState       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 FSM is in its initial state."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.1.3.1."
::= { docsBpiCmTEKEntry 2 }

docsBpiCmTEKExpiresOld  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 Interface Specification, Sections 4.2.1.5 and
4.2.2.9."
::= { docsBpiCmTEKEntry 3 }

docsBpiCmTEKExpiresNew  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 Interface Specification, Sections 4.2.1.5 and
4.2.2.9."
::= { docsBpiCmTEKEntry 4 }

docsBpiCmTEKKeyRequests OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CM has transmitted
a Key Request message."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.4."
::= { docsBpiCmTEKEntry 5 }

docsBpiCmTEKKeyReplies  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
a Key Reply message, including a message whose authentication failed."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.5."
::= { docsBpiCmTEKEntry 6 }

docsBpiCmTEKKeyRejects  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
a Key Reject message, including a message whose authentication failed."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.6."
::= { docsBpiCmTEKEntry 7 }

docsBpiCmTEKInvalids    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
a TEK Invalid message, including a message whose authentication failed."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.8."
::= { docsBpiCmTEKEntry 8 }

docsBpiCmTEKAuthPends   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."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.1.3.3.3."
::= { docsBpiCmTEKEntry 9 }

docsBpiCmTEKKeyRejectErrorCode  OBJECT-TYPE
SYNTAX                          INTEGER {
                                        none(1),
                                        unknown(2),
                                        unauthorizedSid(4)
                                }
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the enumerated description of the
Error-Code in most recent Key Reject message received by the CM. This
has value unknown(2) if the last Error-Code value was 0, and none(1)
if no Key Reject message has been received since reboot."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.1.2.6
and 4.2.2.16."
::= { docsBpiCmTEKEntry 10 }

docsBpiCmTEKKeyRejectErrorString        OBJECT-TYPE
SYNTAX                                  DisplayString (SIZE (0..128))
MAX-ACCESS                              read-only
STATUS                                  current
DESCRIPTION
"The value of this object is the Display-String in most recent Key
Reject message received by the CM. This is a zero length string if no
Key Reject message has been received since reboot."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.1.2.6
and 4.2.2.6."
::= { docsBpiCmTEKEntry 11 }
```

```
docsBpiCmTEKInvalidErrorCode    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 most recent TEK Invalid message received by the CM.
This has value unknown(2) if the last Error-Code value was 0, and
none(1) if no TEK Invalid message has been received since reboot."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.1.2.8
and 4.2.2.16."
::= { docsBpiCmTEKEntry 12 }

docsBpiCmTEKInvalidErrorString  OBJECT-TYPE
SYNTAX                          DisplayString (SIZE (0..128))
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the Display-String in most recent TEK
Invalid message received by the CM. This is a zero length string if
no TEK Invalid message has been received since reboot."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.1.2.8
and 4.2.2.6."
::= { docsBpiCmTEKEntry 13 }

-- Cable Modem Termination System Group

docsBpiCmtsObjects OBJECT IDENTIFIER ::= { docsBpiMIBObjects 2 }

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

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

```
docsBpiCmtsBaseEntry    OBJECT-TYPE
SYNTAX                  DocsBpiCmtsBaseEntry
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 }
::= { docsBpiCmtsBaseTable 1 }

DocsBpiCmtsBaseEntry ::= SEQUENCE {
docsBpiCmtsDefaultAuthLifetime  Integer32,
docsBpiCmtsDefaultTEKLifetime   Integer32,
docsBpiCmtsDefaultAuthGraceTime Integer32,
docsBpiCmtsDefaultTEKGraceTime  Integer32,
docsBpiCmtsAuthRequests         Counter32,
docsBpiCmtsAuthReplies          Counter32,
docsBpiCmtsAuthRejects          Counter32,
docsBpiCmtsAuthInvalids         Counter32
}

docsBpiCmtsDefaultAuthLifetime  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, the
CMTS assigns to a new authorization key."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.2."
::= { docsBpiCmtsBaseEntry 1 }

docsBpiCmtsDefaultTEKLifetime   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, the
CMTS assigns to a new Traffic Encryption Key (TEK)."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.2."
::= { docsBpiCmtsBaseEntry 2 }

-- Note: the following two objects have been obsoleted from this MIB.
```

```
docsBpiCmtsDefaultAuthGraceTime OBJECT-TYPE
SYNTAX                          Integer32 (1..1800)
UNITS                           "seconds"
MAX-ACCESS                      read-write
STATUS                          obsolete
DESCRIPTION
"This object was obsoleted because the provisioning system, not the CMTS,
manages the authorization key grace time for DOCSIS CMs."
::= { docsBpiCmtsBaseEntry 3 }

docsBpiCmtsDefaultTEKGraceTime  OBJECT-TYPE
SYNTAX                          Integer32 (1..1800)
UNITS                           "seconds"
MAX-ACCESS                      read-write
STATUS                          obsolete
DESCRIPTION
"This object was obsoleted because the provisioning system, not the CMTS,
manages the Traffic Encryption Key (TEK) grace time for DOCSIS CMs."
::= { docsBpiCmtsBaseEntry 4 }

docsBpiCmtsAuthRequests OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CMTS has
received an Authorization Request message from any CM."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.1."
::= { docsBpiCmtsBaseEntry 5 }

docsBpiCmtsAuthReplies  OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CMTS has
transmitted an Authorization Reply message to any CM."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.2."
::= { docsBpiCmtsBaseEntry 6 }

docsBpiCmtsAuthRejects  OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CMTS has
```

```
transmitted an Authorization Reject message to any CM."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.3."
::= { docsBpiCmtsBaseEntry 7 }

docsBpiCmtsAuthInvalids OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CMTS has
transmitted an Authorization Invalid message to any CM."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.7."
::= { docsBpiCmtsBaseEntry 8 }

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

docsBpiCmtsAuthTable    OBJECT-TYPE
SYNTAX                  SEQUENCE OF     DocsBpiCmtsAuthEntry
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 on each CMTS MAC interface."
::= { docsBpiCmtsObjects 2 }

docsBpiCmtsAuthEntry    OBJECT-TYPE
SYNTAX                  DocsBpiCmtsAuthEntry
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 before the CM authorization
permanently expires."
INDEX                   { ifIndex, docsBpiCmtsAuthCmMacAddress }
::= { docsBpiCmtsAuthTable 1 }

DocsBpiCmtsAuthEntry ::= SEQUENCE {
docsBpiCmtsAuthCmMacAddress             MacAddress,
docsBpiCmtsAuthCmPublicKey              OCTET STRING,
docsBpiCmtsAuthCmKeySequenceNumber      Integer32,
docsBpiCmtsAuthCmExpires                DateAndTime,
```

```
docsBpiCmtsAuthCmLifetime               Integer32,
docsBpiCmtsAuthCmGraceTime              Integer32,
docsBpiCmtsAuthCmReset                  INTEGER,
docsBpiCmtsAuthCmRequests               Counter32,
docsBpiCmtsAuthCmReplies                Counter32,
docsBpiCmtsAuthCmRejects                Counter32,
docsBpiCmtsAuthCmInvalids               Counter32,
docsBpiCmtsAuthRejectErrorCode          INTEGER,
docsBpiCmtsAuthRejectErrorString        DisplayString,
docsBpiCmtsAuthInvalidErrorCode         INTEGER,
docsBpiCmtsAuthInvalidErrorString       DisplayString
}

docsBpiCmtsAuthCmMacAddress     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."
::= { docsBpiCmtsAuthEntry 1 }

docsBpiCmtsAuthCmPublicKey      OBJECT-TYPE
SYNTAX                          OCTET STRING
                                (SIZE (0 | 74 | 106 | 140 | 270))
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) [22],
corresponding to the public key of the CM. The 74, 106, 140, and
270 byte key encoding lengths correspond to 512 bit, 768 bit, 1024
bit, and 2048 public moduli respectively. This is a zero-length
string if the CMTS does not retain the public key."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.2.4."
::= { docsBpiCmtsAuthEntry 2 }

docsBpiCmtsAuthCmKeySequenceNumber      OBJECT-TYPE
SYNTAX                                  Integer32 (0..15)
MAX-ACCESS                              read-only
STATUS                                  current
DESCRIPTION
"The value of this object is the authorization key sequence number
for this CM."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.2
and 4.2.2.10."
```

```
::= { docsBpiCmtsAuthEntry 3 }

docsBpiCmtsAuthCmExpires        OBJECT-TYPE
SYNTAX                          DateAndTime
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the actual clock time when the current
authorization for this CM expires. If this CM does not have an
active authorization, then the value is of the expiration date and
time of the last active authorization."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.2
and 4.2.2.9."
::= { docsBpiCmtsAuthEntry 4 }

docsBpiCmtsAuthCmLifetime       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, the CMTS
assigns to an authorization key for this CM."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.2
and Appendix A.2."
::= { docsBpiCmtsAuthEntry 5 }

docsBpiCmtsAuthCmGraceTime      OBJECT-TYPE
SYNTAX                          Integer32 (1..1800)
UNITS                           "seconds"
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the grace time for the authorization key
in seconds.  The CM is expected to start trying to get a new
authorization key beginning AuthGraceTime seconds before the
authorization key actually expires."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.1.1.1.3."
::= { docsBpiCmtsAuthEntry 6 }

docsBpiCmtsAuthCmReset  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, but not to transmit an
    Authorization Invalid message nor to invalidate unicast TEKs.  Setting
    this object to sendAuthInvalid(3) causes the CMTS to invalidate the
    current CM authorization key, and to transmit an Authorization Invalid
    message to the CM, but not to invalidate unicast TEKs.  Setting this
    object to invalidateTeks(4) causes the CMTS to invalidate the current
    CM authorization key, to transmit an Authorization Invalid message to
    the CM, and to invalidate all unicast TEKs associated with this CM
    authorization. Reading this object returns the most-recently-set value
    of this object, or returns noResetRequested(1) if the object has not
    been set since the last CMTS reboot."
    REFERENCE
    "DOCSIS Baseline Privacy Interface Specification, Sections 4.1.2.3.4,
    4.1.2.3.5, and 4.1.3.3.5."
    ::= { docsBpiCmtsAuthEntry 7 }

    docsBpiCmtsAuthCmRequests       OBJECT-TYPE
    SYNTAX                          Counter32
    MAX-ACCESS                      read-only
    STATUS                          current
    DESCRIPTION
    "The value of this object is the count of times the CMTS has
    received an Authorization Request message from this CM."
    REFERENCE
    "DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.1."
    ::= { docsBpiCmtsAuthEntry 8 }

    docsBpiCmtsAuthCmReplies        OBJECT-TYPE
    SYNTAX                          Counter32
    MAX-ACCESS                      read-only
    STATUS                          current
    DESCRIPTION
    "The value of this object is the count of times the CMTS has
    transmitted an Authorization Reply message to this CM."
    REFERENCE
    "DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.2."
    ::= { docsBpiCmtsAuthEntry 9 }

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

```
DESCRIPTION
"The value of this object is the count of times the CMTS has
transmitted an Authorization Reject message to this CM."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.3."
::= { docsBpiCmtsAuthEntry 10 }

docsBpiCmtsAuthCmInvalids       OBJECT-TYPE
SYNTAX                          Counter32
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the count of times the CMTS has
transmitted an Authorization Invalid message to this CM."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.7."
::= { docsBpiCmtsAuthEntry 11 }

docsBpiCmtsAuthRejectErrorCode  OBJECT-TYPE
SYNTAX                  INTEGER {
                                none(1),
                                unknown(2),
                                unauthorizedCm(3),
                                unauthorizedSid(4)
                        }
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the enumerated description of the
Error-Code in most recent Authorization Reject message transmitted to
the CM.  This has 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."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.3
and 4.2.2.16."
::= { docsBpiCmtsAuthEntry 12 }

docsBpiCmtsAuthRejectErrorString        OBJECT-TYPE
SYNTAX                                  DisplayString (SIZE (0..128))
MAX-ACCESS                              read-only
STATUS                                  current
DESCRIPTION
"The value of this object is the Display-String in 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."
REFERENCE
```

```
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.3
and 4.2.2.6."
::= { docsBpiCmtsAuthEntry 13 }

docsBpiCmtsAuthInvalidErrorCode 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 most recent Authorization Invalid message transmitted
to the CM.  This has 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."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.7
and 4.2.2.16."
::= { docsBpiCmtsAuthEntry 14 }

docsBpiCmtsAuthInvalidErrorString       OBJECT-TYPE
SYNTAX                                  DisplayString (SIZE (0..128))
MAX-ACCESS                              read-only
STATUS                                  current
DESCRIPTION
"The value of this object is the Display-String in 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."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.7
and 4.2.2.6."
::= { docsBpiCmtsAuthEntry 15 }

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

docsBpiCmtsTEKTable     OBJECT-TYPE
SYNTAX                  SEQUENCE OF     DocsBpiCmtsTEKEntry
MAX-ACCESS              not-accessible
STATUS                  current
```

```
DESCRIPTION
"This table describes the attributes of each CM Traffic Encryption
Key (TEK) association. The CMTS maintains one TEK association per BPI
SID on each CMTS MAC interface."
::= { docsBpiCmtsObjects 3 }

docsBpiCmtsTEKEntry     OBJECT-TYPE
SYNTAX                  DocsBpiCmtsTEKEntry
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 SID per MAC interface, based on the receipt of an
Key Request message, and MUST not delete the entry before the CM
authorization for the SID permanently expires."
INDEX                   { ifIndex, docsIfCmtsServiceId }
::= { docsBpiCmtsTEKTable 1 }

DocsBpiCmtsTEKEntry ::= SEQUENCE {
docsBpiCmtsTEKLifetime                  Integer32,
docsBpiCmtsTEKGraceTime                 Integer32,
docsBpiCmtsTEKExpiresOld                DateAndTime,
docsBpiCmtsTEKExpiresNew                DateAndTime,
docsBpiCmtsTEKReset                     TruthValue,
docsBpiCmtsKeyRequests                  Counter32,
docsBpiCmtsKeyReplies                   Counter32,
docsBpiCmtsKeyRejects                   Counter32,
docsBpiCmtsTEKInvalids                  Counter32,
docsBpiCmtsKeyRejectErrorCode           INTEGER,
docsBpiCmtsKeyRejectErrorString         DisplayString,
docsBpiCmtsTEKInvalidErrorCode          INTEGER,
docsBpiCmtsTEKInvalidErrorString        DisplayString
}

docsBpiCmtsTEKLifetime  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, the CMTS assigns
to keys for this TEK association."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.5
and Appendix A.2."
::= { docsBpiCmtsTEKEntry 1 }
```

```
docsBpiCmtsTEKGraceTime OBJECT-TYPE
SYNTAX                  Integer32 (1..1800)
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 get a new TEK beginning
TEKGraceTime seconds before the TEK actually expires."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Appendix A.1.1.1.6."
::= { docsBpiCmtsTEKEntry 2 }

docsBpiCmtsTEKExpiresOld        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 Interface Specification, Sections 4.2.1.5
and 4.2.2.9."
::= { docsBpiCmtsTEKEntry 3 }

docsBpiCmtsTEKExpiresNew        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 Interface Specification, Sections 4.2.1.5
and 4.2.2.9."
::= { docsBpiCmtsTEKEntry 4 }

docsBpiCmtsTEKReset     OBJECT-TYPE
SYNTAX                  TruthValue
MAX-ACCESS              read-write
STATUS                  current
DESCRIPTION
"Setting this object to TRUE causes the CMTS to invalidate the current
active TEK(s) (plural due to key transition periods), and to generate
a new TEK for the associated SID; the CMTS MAY also generate an
unsolicited TEK Invalid message, to optimize the TEK synchronization
```

```
between the CMTS and the CM. Reading this object always returns
FALSE."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.1.3.3.5."
::= { docsBpiCmtsTEKEntry 5 }

docsBpiCmtsKeyRequests  OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CMTS has
received a Key Request message."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.4."
::= { docsBpiCmtsTEKEntry 6 }

docsBpiCmtsKeyReplies   OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CMTS has
transmitted a Key Reply message."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.5."
::= { docsBpiCmtsTEKEntry 7 }

docsBpiCmtsKeyRejects   OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CMTS has
transmitted a Key Reject message."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.6."
::= { docsBpiCmtsTEKEntry 8 }

docsBpiCmtsTEKInvalids  OBJECT-TYPE
SYNTAX                  Counter32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION
"The value of this object is the count of times the CMTS has
transmitted a TEK Invalid message."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Section 4.2.1.8."
```

```
::= { docsBpiCmtsTEKEntry 9 }

docsBpiCmtsKeyRejectErrorCode   OBJECT-TYPE
SYNTAX                          INTEGER {
                                        none(1),
                                        unknown(2),
                                        unauthorizedSid(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 BPI SID. This has value unknown(2) if the last
Error-Code value was 0, and none(1) if no Key Reject message has been
received since reboot."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.6
and 4.2.2.16."
::= { docsBpiCmtsTEKEntry 10 }

docsBpiCmtsKeyRejectErrorString OBJECT-TYPE
SYNTAX                          DisplayString (SIZE (0..128))
MAX-ACCESS                      read-only
STATUS                          current
DESCRIPTION
"The value of this object is the Display-String in the most recent
Key Reject message sent in response to a Key Request for this BPI
SID.  This is a zero length string if no Key Reject message has been
received since reboot."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.6
and 4.2.2.6."
::= { docsBpiCmtsTEKEntry 11 }

docsBpiCmtsTEKInvalidErrorCode  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 BPI SID.  This has value unknown(2) if the last Error-Code
value was 0, and none(1) if no TEK Invalid message has been received
```

```
since reboot."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.8
and 4.2.2.16."
::= { docsBpiCmtsTEKEntry 12 }

docsBpiCmtsTEKInvalidErrorString        OBJECT-TYPE
SYNTAX                                  DisplayString (SIZE (0..128))
MAX-ACCESS                              read-only
STATUS                                  current
DESCRIPTION
"The value of this object is the Display-String in the most recent TEK
Invalid message sent in association with this BPI SID.  This is a zero
length string if no TEK Invalid message has been received since reboot."
REFERENCE
"DOCSIS Baseline Privacy Interface Specification, Sections 4.2.1.8
and 4.2.2.6."
::= { docsBpiCmtsTEKEntry 13 }

--
-- The CMTS Multicast Control Group
--

docsBpiMulticastControl OBJECT IDENTIFIER ::= { docsBpiCmtsObjects 4 }

--
-- The CMTS IP Multicast Mapping Table, indexed by IP multicast
-- address and prefix, and by ifindex
--

docsBpiIpMulticastMapTable      OBJECT-TYPE
SYNTAX                          SEQUENCE OF DocsBpiIpMulticastMapEntry
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
"This table describes the mapping of IP multicast address prefixes to
multicast SIDs on each CMTS MAC interface."
::= { docsBpiMulticastControl 1 }

docsBpiIpMulticastMapEntry      OBJECT-TYPE
SYNTAX                          DocsBpiIpMulticastMapEntry
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
"Each entry contains objects describing the mapping of one IP
multicast address prefix to one multicast SID on one CMTS MAC
interface. The CMTS uses the mapping when forwarding downstream IP
multicast traffic."
```

```
INDEX                           { ifIndex, docsBpiIpMulticastAddress,
                                  docsBpiIpMulticastPrefixLength }
::= { docsBpiIpMulticastMapTable 1 }

DocsBpiIpMulticastMapEntry ::= SEQUENCE {
docsBpiIpMulticastAddress       IpAddress,
docsBpiIpMulticastPrefixLength  Integer32,
docsBpiIpMulticastServiceId     Integer32,
docsBpiIpMulticastMapControl    RowStatus
}

docsBpiIpMulticastAddress       OBJECT-TYPE
SYNTAX                          IpAddress
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
"This object represents the IP multicast address (prefix) to be
mapped by this row, in conjunction with
docsBpiIpMulticastPrefixLength."
::= { docsBpiIpMulticastMapEntry 1 }

docsBpiIpMulticastPrefixLength  OBJECT-TYPE
SYNTAX                          Integer32 (0..32)
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
"This object represents the IP multicast address prefix length
for this row. The value of this object represents the length in
bits of docsBpiIpMulticastAddress for multicast address
comparisons, using big-endian ordering. An IP multicast address
matches this row if the (docsBpiIpMulticastPrefixLength) most
significant bits of the IP multicast address and of the
(docsBpiIpMulticastAddress) are identical.
This object is similar in usage to an IP address mask. The value
0 corresponds to IP address mask 0.0.0.0, the value 1 corresponds
to IP address mask 128.0.0.0, the value 8 corresponds to IP
address mask 255.0.0.0, and the value 32 corresponds to IP
address mask 255.255.255.255."
::= { docsBpiIpMulticastMapEntry 2 }

docsBpiIpMulticastServiceId     OBJECT-TYPE
SYNTAX                          Integer32 (8192..16368)
MAX-ACCESS                      read-create
STATUS                          current
DESCRIPTION
"This object represents the multicast SID to be used in this
IP multicast address prefix mapping entry."
-- DEFVAL is an unused multicast SID value chosen by CMTS.
```

```
::= { docsBpiIpMulticastMapEntry 3 }

docsBpiIpMulticastMapControl    OBJECT-TYPE
SYNTAX                          RowStatus
MAX-ACCESS                      read-create
STATUS                          current
DESCRIPTION
"This object controls and reflects the IP multicast address prefix
mapping entry. There is no restriction on the ability to change values
in this row while the row is active."
::= { docsBpiIpMulticastMapEntry 4 }

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

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

docsBpiMulticastAuthEntry       OBJECT-TYPE
SYNTAX                          DocsBpiMulticastAuthEntry
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
"Each entry contains objects describing the key authorization of one
cable modem for one multicast SID for one CMTS MAC interface."
INDEX                           { ifIndex, docsBpiMulticastServiceId,
                                  docsBpiMulticastCmMacAddress }
::= { docsBpiMulticastAuthTable 1 }

DocsBpiMulticastAuthEntry ::= SEQUENCE {
docsBpiMulticastServiceId       Integer32,
docsBpiMulticastCmMacAddress    MacAddress,
docsBpiMulticastAuthControl     RowStatus
}

docsBpiMulticastServiceId       OBJECT-TYPE
SYNTAX                          Integer32 (8192..16368)
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
```

```
"This object represents the multicast SID for authorization."
::= { docsBpiMulticastAuthEntry 1 }

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

docsBpiMulticastAuthControl     OBJECT-TYPE
SYNTAX                          RowStatus
MAX-ACCESS                      read-create
STATUS                          current
DESCRIPTION
"This object controls and reflects the CM authorization for each
multicast SID. There is no restriction on the ability to change
values in this row while the row is active."
::= { docsBpiMulticastAuthEntry 3 }

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

docsBpiNotification     OBJECT IDENTIFIER ::= { docsBpiMIB 2 }
docsBpiConformance      OBJECT IDENTIFIER ::= { docsBpiMIB 3 }
docsBpiCompliances      OBJECT IDENTIFIER ::= { docsBpiConformance 1 }
docsBpiGroups           OBJECT IDENTIFIER ::= { docsBpiConformance 2 }

docsBpiBasicCompliance MODULE-COMPLIANCE
STATUS          current
DESCRIPTION
"This is the compliance statement for devices which implement the
DOCSIS Baseline Privacy Interface."

MODULE  -- docsBpiMIB

-- conditionally mandatory group
GROUP   docsBpiCmGroup
DESCRIPTION
"This group is implemented only in CMs, not in CMTSs."

-- conditionally mandatory group
GROUP   docsBpiCmtsGroup
DESCRIPTION
```

```
"This group is implemented only in CMTSs, not in CMs."

-- relaxation on mandatory range (unnecessary since object is read-only)
-- OBJECT       docsBpiCmAuthGraceTime
-- SYNTAX       Integer32 (300..1800)
-- DESCRIPTION
-- "The refined range corresponds to the minimum and maximum values in
-- operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range (unnecessary since object is read-only)
-- OBJECT       docsBpiCmTEKGraceTime
-- SYNTAX       Integer32 (300..1800)
-- DESCRIPTION
-- "The refined range corresponds to the minimum and maximum values in
-- operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range
OBJECT  docsBpiCmtsDefaultAuthLifetime
SYNTAX  Integer32 (86400..6048000)
DESCRIPTION
"The refined range corresponds to the minimum and maximum values in
operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range
OBJECT  docsBpiCmtsDefaultTEKLifetime
SYNTAX  Integer32 (1800..604800)
DESCRIPTION
"The refined range corresponds to the minimum and maximum values in
operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range (object removed from MIB)
-- OBJECT       docsBpiCmtsDefaultAuthGraceTime
-- SYNTAX       INTEGER (300..1800)
-- DESCRIPTION
-- "The refined range corresponds to the minimum and maximum values in
-- operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range  (object removed from MIB)
-- OBJECT       docsBpiCmtsDefaultTEKGraceTime
-- SYNTAX       INTEGER (300..1800)
-- DESCRIPTION
-- "The refined range corresponds to the minimum and maximum values in
-- operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range
OBJECT  docsBpiCmtsAuthCmLifetime
SYNTAX  Integer32 (86400..6048000)
DESCRIPTION
```

```
"The refined range corresponds to the minimum and maximum values in
operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range (unnecessary since object is read-only)
-- OBJECT       docsBpiCmtsAuthCmGraceTime
-- SYNTAX       Integer32 (300..1800)
-- DESCRIPTION
-- "The refined range corresponds to the minimum and maximum values in
-- operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range
OBJECT  docsBpiCmtsTEKLifetime
SYNTAX  Integer32 (1800..604800)
DESCRIPTION
"The refined range corresponds to the minimum and maximum values in
operational networks, according to Appendix A.2 in [18]."

-- relaxation on mandatory range (unnecessary since object is read-only)
-- OBJECT       docsBpiCmtsTEKGraceTime
-- SYNTAX       Integer32 (300..1800)
-- DESCRIPTION
-- "The refined range corresponds to the minimum and maximum values in
-- operational networks, according to Appendix A.2 in [18]."

::= { docsBpiCompliances 1 }

docsBpiCmGroup  OBJECT-GROUP
OBJECTS {
docsBpiCmPrivacyEnable,
docsBpiCmPublicKey,
docsBpiCmAuthState,
docsBpiCmAuthKeySequenceNumber,
docsBpiCmAuthExpires,
docsBpiCmAuthReset,
docsBpiCmAuthGraceTime,
docsBpiCmTEKGraceTime,
docsBpiCmAuthWaitTimeout,
docsBpiCmReauthWaitTimeout,
docsBpiCmOpWaitTimeout,
docsBpiCmRekeyWaitTimeout,
docsBpiCmAuthRejectWaitTimeout,
docsBpiCmAuthRequests,
docsBpiCmAuthReplies,
docsBpiCmAuthRejects,
docsBpiCmAuthInvalids,
docsBpiCmAuthRejectErrorCode,
docsBpiCmAuthRejectErrorString,
docsBpiCmAuthInvalidErrorCode,
```

```
docsBpiCmAuthInvalidErrorString,
docsBpiCmTEKPrivacyEnable,
docsBpiCmTEKState,
docsBpiCmTEKExpiresOld,
docsBpiCmTEKExpiresNew,
docsBpiCmTEKKeyRequests,
docsBpiCmTEKKeyReplies,
docsBpiCmTEKKeyRejects,
docsBpiCmTEKInvalids,
docsBpiCmTEKAuthPends,
docsBpiCmTEKKeyRejectErrorCode,
docsBpiCmTEKKeyRejectErrorString,
docsBpiCmTEKInvalidErrorCode,
docsBpiCmTEKInvalidErrorString
}
STATUS                  current
DESCRIPTION
"This collection of objects provides CM BPI status and control."
::= { docsBpiGroups 1 }

docsBpiCmtsGroup        OBJECT-GROUP
OBJECTS {
docsBpiCmtsDefaultAuthLifetime,
docsBpiCmtsDefaultTEKLifetime,
docsBpiCmtsAuthRequests,
docsBpiCmtsAuthReplies,
docsBpiCmtsAuthRejects,
docsBpiCmtsAuthInvalids,
docsBpiCmtsAuthCmPublicKey,
docsBpiCmtsAuthCmKeySequenceNumber,
docsBpiCmtsAuthCmExpires,
docsBpiCmtsAuthCmLifetime,
docsBpiCmtsAuthCmGraceTime,
docsBpiCmtsAuthCmReset,
docsBpiCmtsAuthCmRequests,
docsBpiCmtsAuthCmReplies,
docsBpiCmtsAuthCmRejects,
docsBpiCmtsAuthCmInvalids,
docsBpiCmtsAuthRejectErrorCode,
docsBpiCmtsAuthRejectErrorString,
docsBpiCmtsAuthInvalidErrorCode,
docsBpiCmtsAuthInvalidErrorString,
docsBpiCmtsTEKLifetime,
docsBpiCmtsTEKGraceTime,
docsBpiCmtsTEKExpiresOld,
docsBpiCmtsTEKExpiresNew,
docsBpiCmtsTEKReset,
docsBpiCmtsKeyRequests,
```

```
docsBpiCmtsKeyReplies,
docsBpiCmtsKeyRejects,
docsBpiCmtsTEKInvalids,
docsBpiCmtsKeyRejectErrorCode,
docsBpiCmtsKeyRejectErrorString,
docsBpiCmtsTEKInvalidErrorCode,
docsBpiCmtsTEKInvalidErrorString,
docsBpiIpMulticastServiceId,
docsBpiIpMulticastMapControl,
docsBpiMulticastAuthControl
}
STATUS          current
DESCRIPTION
"This collection of objects provides CMTS BPI status and control."
::= { docsBpiGroups 2 }

docsBpiObsoleteObjectsGroup     OBJECT-GROUP
OBJECTS {
docsBpiCmtsDefaultAuthGraceTime,
docsBpiCmtsDefaultTEKGraceTime
}
STATUS          obsolete
DESCRIPTION
"This is a collection of obsolete BPI objects."
::= { docsBpiGroups 3 }

END
```

5. Acknowledgments

This document was produced by the IPCDN Working Group. Much of the content of this MIB was conceived by Chet Birger and Mike StJohns. Kazuyoshi Ozawa and Bob Himlin provided many useful technical corrections.

6. References

[1] Harrington, D., Presuhn, R. and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", RFC 2571, April 1999.

[2] Rose, M. and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based Internets", STD 16, RFC 1155, May 1990.

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

[4] Rose, M., "A Convention for Defining Traps for use with the SNMP", RFC 1215, March 1991.

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

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

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

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

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

[10] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1906, January 1996.

[11] Case, J., Harrington D., Presuhn R. and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 2572, April 1999.

[12] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 2574, April 1999.

[13] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1905, January 1996.

[14] Levi, D., Meyer, P. and B. Stewart, "SNMP Applications", RFC 2573, April 1999.

[15] Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", RFC 2575, April 1999.

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

[17] St. Johns, M., editor, "DOCSIS Cable Device MIB, Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems", RFC 2669, August 1999.

[18] "Data-Over-Cable Service Interface Specifications: Baseline Privacy Interface Specification SP-BPI-I02-990319", DOCSIS, March 1999, http://www.cablemodem.com/.

[19] "Data-Over-Cable Service Interface Specifications: Cable Modem Radio Frequency Interface Specification SP-RFI-I05-991105", DOCSIS, November 1999, http://www.cablemodem.com/.

[20] "Data-Over-Cable Service Interface Specifications: Operations Support System Interface Specification RF Interface SP-OSSI-RF-I02-990113", DOCSIS, January 1999, http://www.cablemodem.com/.

[21] "Data-Over-Cable Service Interface Specifications: Baseline Privacy Plus Interface Specification SP-BPI+-I05-000714", DOCSIS, July 2000, http://www.cablemodem.com/.

[22] RSA Laboratories, "The Public-Key Cryptography Standards", RSA Data Security Inc., Redwood City, CA.

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

[24] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", RFC 2570, April 1999.

7. Security Considerations

The Baseline Privacy Interface provides data encryption for DOCSIS data-over-cable services. Baseline Privacy-capable cable modems have RSA private/public key pairs installed by manufacturers. The public key is used to encrypt an Authorization key, and the Authorization key is used to encrypt one or more Traffic Encryption Keys (TEKs). The TEKs are used to encrypt both upstream and downstream data traffic. Please refer to [18] to obtain further information on the Baseline Privacy specification.

In particular, the Baseline Privacy Interface does not provide an authentication service. CMTS implementors are encouraged not to rely on the MAC address of the CM for service authorization -- in particular, for the docsBpiMulticastAuthTable in this MIB. The Baseline Privacy Plus Interface does provide a CM authentication service, and the working group expects to issue a MIB for the management of BPI+ at a later time.

This MIB specification contains a number of read-write objects, that should be protected from unauthorized modification to prevent denial of service and theft of service attacks: in particular, objects that reset state machines (ex. docsBpiCmAuthReset), change key lifetimes (ex. docsBpiCmtsDefaultAuthLifetime), change rekeying grace times (ex. docsBpiCmtsDefaultAuthGraceTime), and control multicast traffic (ex. most objects in the docsBpiMulticastControl group).

The desired means to protect these objects from unwarranted access is to implement the security features as provided by the SNMPv3 framework. Specifically, the use of the User-based Security Model [12] and the View-based Access Control Model [15] is recommended.

Weaker methods to protect CMs from unauthorized access include using the docsDevNmAccessTable from the Cable Device MIB [17] to disallow configuration changes from unauthorized network management stations, and using the SNMP MIB Object and SNMP Write-Access Control configuration file options from the Radio Frequency Interface [19] to set MIB object values and disable SNMP SET operations at cable modem boot time. Note that these mechanisms may be vulnerable to an unauthorized network management station "spoofing" the source address of a legitimate network management station.

8. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

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

9. Author's Address

Richard Woundy
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
U.S.A.

Phone: +1 978 244 8000
EMail: rwoundy@cisco.com

10. Full Copyright Statement

Acknowledgement

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