Network Working Group
Request for Comments: 4036
Category: Standards Track

W. Sawyer

April 2005

Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modem Termination Systems for Subscriber Management

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 Data-over-Cable Service Interface Specification (DOCSIS)-compliant Cable Modem Termination Systems. These managed objects facilitate protection of the cable network from misuse by subscribers. The Differentiated Services MIB (RFC 3289) provides the filtering functions needed here, making use of classification items defined in this specification.

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].

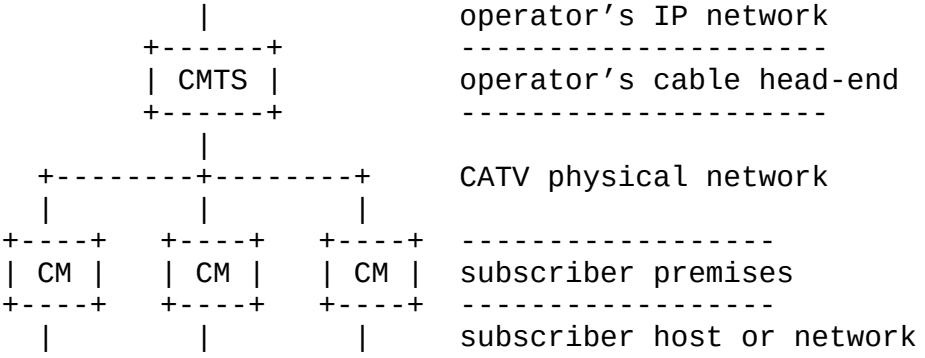
2. Conventions

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].

3. Overview

This MIB module provides a set of objects required for the management of DOCSIS Cable Modem Termination Systems (CMTS). The specification is derived in part from the operational model described in the DOCSIS Radio Frequency Interface Specification [ITU-T-J122]. These managed objects facilitate protection of the cable network from misuse by subscribers. This misuse might include, for example, address spoofing, service spoofing, or operation of unauthorized services.

The following figure illustrates the operational and physical deployment relationships between elements in a cable modem network. This MIB module resides at the CMTS, which is the first point in the public data network at which the cable operator controls physical access. The CMTS (possibly assisted by other IP service devices) acts as a network edge, separating the physical outside-plant cable television network from the operator's IP network.



This MIB module controls IP packet forwarding to and from each cable modem, at the CMTS. Different modems may be accorded different treatment.

Much of this module duplicates capabilities found in the DOCSIS Cable Device MIB [RFC2669]. Although it is expected that the Cable Device MIB will be used to prevent unwanted traffic from entering the cable network, it is also possible that a malicious user might tamper with cable modem software, disabling its filtering policies. This MIB provides a more secure mechanism, as physical access to the CMTS is controlled by the network operator.

In particular, this MIB provides two capabilities: first, to limit the IP addresses behind a modem, and second, to provide address and protocol filtering to and from a modem. The first duplicates the capabilities of the docsDevCpe group [RFC2669]. This provides for either learned or provisioned subscriber premises host IP addresses behind a cable modem.

The address and protocol filtering capability is similar to that performed by the cable modem itself. It differs in several respects because it is intended to control subscriber traffic at the CMTS, rather than at the individual CM. First, the MIB structure must be indexed appropriately at the CMTS to indicate which cable modem subscriber is intended. Second, rather than maintaining a separate list of filters for each modem at the CMTS, it is assumed that large numbers of modems will share filtering characteristics. Therefore, modems are grouped so as to share common filter lists.

The filtering capability is implemented using the Classification, Counting, and Drop facilities of the Differentiated Services MIB [RFC3289]. In order to provide different filtering for various classes of subscribers, this MIB defines the docsSubMgtFilterGroupTable, which specifies which filters apply to each subscriber packet. This table is used by RFC 3289 as a first pass of classification, and also to choose a second pass of classification using the diffServMultiFieldClfrTable:

```
diffServDataPathStart --> diffServClfrEntry(1)
diffServClfrElementSpecific(1) --> docsSubMgtFilterGroupIndex
diffServClfrElementNext(1) --> diffServClfrEntry(2)
diffServClfrElementSpecific(2)--> diffServMultiFieldClfrEntry
diffServClfrElementNext(2) --> difServActionEntry (count or algDrop)
```

Because it is assumed that large numbers of modems will share filtering characteristics, DOCSIS signaling defines filter groups according to which cable modems share common filter lists. The operator creates references to these groups in the diffServClfrElementSpecific(1) entries above.

3.1. Structure of the MIB

This MIB is structured in four tables:

- The docsSubMgtCpeControlTable controls the acceptance of subscriber host addresses behind a cable modem.
- The docsSubMgtCpeIpTable monitors the subscriber host addresses that the CMTS believes exist behind the cable modem.
- The docsSubMgtCmFilterTable binds a cable modem to a set of filters in diffServMultiFieldClfrTable.
- The docsSubMgtFilterGroupTable provides the OIDs by which the diffServClfrElementTable selects a filter group.

The docsSubMgtCpeControlTable and docsSubMgtCmFilterTable AUGMENT the docsIfCmtsCmStatusTable from [RFC2670]. Similarly, docsSubMgtCpeIpTable expands this table (an additional index is used). As such, each entry in these tables is bound to a registered cable modem, as perceived by the CMTS.

3.1.1. docsSubMgtFilterGroupTable

The docsSubMgtFilterGroupTable links the filter group (signaled by DOCSIS as a small integer) to the diffServClfrElementEntry for the first pass of filter classification. diffServClfrElementSpecific

requires a RowPointer. Thus, this table exists to provide referenced objects for diffServClfrElementSpecific. The classification method is as follows:

- Use the DOCSIS filter group, as inferred from the sending or receiving modem, as the classification criterion.
- Use docsSubMgtFilterGroupIndex as the value to match.

An entry exists in this Table if a reference to it exists in diffServClfrElementSpecific.

As such, contrary to common practice, the index for the table is read-only and is both the Entry's index and its only value.

3.1.2. IPv4 Compliance

Please note that the compliance statements in this version of the MIB module require support only for IPv4 addresses. That is because the current version of the DOCSIS protocols (1.0, 1.1, and 2.0) are not IPv6 capable. Although support for IPv6 will require changes to the DOCSIS protocols, it is expected that the only changes to the MIB module itself will be the addition of new compliance statements that mandate support for IPv6 addresses. All IP addresses that appear in this document conform to the textual conventions specified in [RFC4001].

3.2. Management Requirements

The DOCSIS cable modem provisioning model [ITU-T-J122] requires that cable modems use TFTP to acquire a list of parameters. The modem then passes many of these parameters to the CMTS in the DOCSIS Registration message. The parameter values are digitally signed by the creator of the TFTP contents, and the signature is verified by the CMTS. In general, then, the CMTS itself need not be configured with the attributes of its cable modems. It will acquire these values through the Registration process that is secured by the digital signature.

Cable modem subscriber management, as described here, modifies this process slightly to reduce data and to ease administrative control. Filtering criteria, for example, are maintained through SNMP at the CMTS, and the modem registration merely signals the index values for the rows that apply to that modem.

3.2.1. Interaction with DOCSIS Provisioning for CPE Address Control

The CMTS creates rows in docsSubMgtCpeControlTable for each modem as a result of the DOCSIS registration process. The DOCSIS registration attributes may include items semantically equivalent to those in the docsDevCpe section of the DOCSIS Cable Device MIB [RFC2669]:

- docsDevCpeEnroll
- docsDevCpeIpMax
- docsDevCpeIp

Successful DOCSIS registration will have the effect of setting the corresponding fields in the docsSubMgtCpeControlTable and the docsSubMgtCpeIpTable. If they are not present at modem registration, the CMTS shall apply the following:

- docsSubMgtCpeControlActive <-- docsSubMgtCpeActiveDefault
- docsSubMgtCpeControlMaxCpeIp <-- docsSubMgtCpeMaxIpDefault
- docsSubMgtCpeControlLearnable <-- docsSubMgtCpeLearnableDefault

Rows in docsSubMgtCpeIpTable are created through any of three ways: DOCSIS registration (as described above), learning by the CMTS, or some unspecified administrative mechanism on the CMTS. The docsDevCpeIpMax table bound applies only to the first two.

The CMTS may learn addresses simply by snooping source IP addresses from traffic originating from each cable modem. Other learning mechanisms (for example, ARP snooping) may be used. The learning mechanism is not defined by this document.

3.2.2. Interaction with DOCSIS Provisioning for Filtering

Rows in docsSubMgtCmFilterTable are created by the CMTS for each modem as a result of the DOCSIS registration process. The DOCSIS registration attributes may include four indices (see section C.1.1.18.3 of [ITU-T-J122]):

- One identifying the upstream (ingress with respect to the CMTS interface) filter group for packets originating from the cable modem (i.e., those packets whose source MAC address matches that of the cable modem).

- One identifying the upstream filter group for packets originating from subscribers attached to the cable modem (i.e., those packets whose source MAC address does not match that of the cable modem).

- One identifying the downstream (egress with respect to the CMTS interface) filter group for packets destined to the cable modem (i.e., those packets whose destination MAC address matches that of the cable modem).

- One identifying the downstream filter group for packets destined to subscribers attached to the cable modem (i.e., those packets whose destination MAC address does not match that of the cable modem).

Successful registration will have the effect of setting docsSubMgtCmFilterCmDownstream, docsSubMgtCmFilterCmUpstream, docsSubMgtCmFilterSubDownstream, and docsSubMgtCmFilterSubUpstream, for that modem (just as if they were set through the SNMP protocol). If the DOCSIS attributes are not present, the four values are set to zero. The effect will be to use the default entry (diffServClfrElementSpecific=zeroDotZero) specified in the diffServClfrElementTable. Note that omission of the DOCSIS-signaled values results in application of the default filtering entry, not in omission of filtering.

3.2.3. Distinguishing Modem from Subscriber Traffic

All traffic originating from or destined to a subscriber site is potentially suspect and subject to suppression by the network operator. This is true even if the traffic is ostensibly sourced or sunk by the cable modem itself, rather than by the subscriber hosts behind the modem. To provide more nuanced administrative control, this document allows separate filter policies for modems and hosts. For example, modem policies may limit modems to server subnet - only access while allowing a different scope to subscribers.

The CMTS chooses the filter set to apply based solely on the MAC address (source MAC upstream, destination MAC downstream). If the MAC address matches that of the modem, then the docsSubMgtCmFilterCmUp/Downstream pair is used; otherwise, the docsSubMgtCmFilterSubUp/Downstream pair is applied.

If the CM acts as a router rather than as a DOCSIS bridging forwarder, then the network operator will only use the docsSubMgtCmFilterCmUp/Downstream pair.

3.3. Relationship to the Differentiated Services MIB [RFC3289]

DOCSIS CMTSes rely on the classification, counting, and drop facilities of the Differentiated Services MIB to screen subscriber packets for IP, TCP, and UDP characteristics. It is expected that

any implementation of this MIB also includes at least the following from RFC 3289:

- diffServDataPathTable
- diffServClfrTable
- diffServClfrElementTable
- diffServMultiFieldClfrTable
- diffServActionTable
- diffServCountActTable
- diffServAlgDropTable (diffServAlgDropType=alwaysDrop)

The corresponding "next-free" objects are also required.

The use of other facilities from RFC 3289 is not precluded but is beyond the scope of this specification.

3.3.1. Using the Filter Group to Extend Packet Classification

The base capability of RFC 3289 assumes that all packets on the same direction of the same interface will be classified by the same criteria. Filter Groups, which are introduced in this document, expand on RFC 3289 to allow various subscribers to receive different classification (filtering) treatment. One way to view filter groups is as sub-interfaces within the physical DOCSIS channel. Another way to view them is as values of a field logically prepended to the packet prior to classification:

[filter group][DOCSIS MAC header][IP header]...

Of course this 'logical' field has no existence outside of the CMTS.

The diffServClfrTable and diffServClfrElementTable are then used twice: the first classifiers select among filter groups, using OIDs from docsSubMgtFilterGroupTable. The 'next' action on matching a filter group is to select a diffServClfrEntry that now classifies on IP/TCP/UDP criteria (the diffServMultiFieldClfrTable). The 'next' action on this second match may be a 'count' (and accept), a 'drop', or some other feature from RFC 3289.

3.3.2. Interface Usage

For the purposes of DOCSIS subscriber management, only the DOCSIS MAC cable interface(s) are used. The interface appears as the index to diffServDataPathEntry, which is the starting point for diffserv MIB table traversal.

The use of the diffserv MIB for other purposes, both on the DOCSIS MAC interfaces and on other network interfaces, is not precluded by this document.

3.4. Filtering and the Tiny Fragment Attack

It is recommended that the implementers prevent the "tiny fragment" and "overlapping fragment" attacks for the TCP filtering tables in this MIB, as discussed in RFC 1858 [RFC1858] and RFC 3128 [RFC3128].

Prevention of these attacks can be implemented with the following rules, when filtering is enabled:

- Admit all packets with fragment offset >= 2.
- Discard all packets with fragment offset = 1, or with fragment offset = 0 AND fragment payload length < 16.
- Apply filtering rules to all packets with fragment offset = 0.

4. Definitions

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

IMPORTS
        MODULE-IDENTITY,
        OBJECT-TYPE,
        Integer32,
        mib-2
                FROM SNMPv2-SMI
        RowStatus,
        TruthValue,
        TimeStamp,
        StorageType
                FROM SNMPv2-TC
        OBJECT-GROUP,
        MODULE-COMPLIANCE
                FROM SNMPv2-CONF
        InetAddressType,
        InetAddress
                FROM INET-ADDRESS-MIB
        docsIfCmtsCmStatusIndex,
        docsIfCmtsCmStatusEntry
                FROM DOCS-IF-MIB  -- RFC2670
        diffServMIBDataPathGroup,
        diffServMIBClfrGroup,
        diffServMIBClfrElementGroup,
        diffServMIBMultiFieldClfrGroup,
```

```
            diffServMIBActionGroup,
            diffServMIBAlgDropGroup,
            diffServMIBCounterGroup,
            diffServDataPathStatus,
            diffServClfrStatus,
            diffServClfrElementStatus,
            diffServMultiFieldClfrAddrType,
            diffServMultiFieldClfrSrcAddr,
            diffServMultiFieldClfrDstAddr,
            diffServAlgDropStatus,
            diffServDataPathStorage,
            diffServClfrStorage,
            diffServClfrElementStorage,
            diffServMultiFieldClfrStorage,
            diffServActionStorage,
            diffServCountActStorage,
            diffServAlgDropStorage,
            diffServAlgDropType
                    FROM DIFFSERV-MIB  -- RFC3289
        ;

    docsSubMgt MODULE-IDENTITY
        LAST-UPDATED    "200503290000Z" -- March 29, 2005
        ORGANIZATION    "IETF IP over Cable Data Network (IPCDN) Working
                         Group"
        CONTACT-INFO
            "        Wilson Sawyer
             Postal: 50 Kelly Brook Lane
                     East Hampstead, NH 03826
                     U.S.A.

             Phone:  +1 603 382 7080
             E-mail: wsawyer@ieee.org

             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, Richard_Woundy@cable.comcast.com
                        Jean-Francois Mule, jf.mule@cablelabs.com"
        DESCRIPTION
            "This is the CMTS centric subscriber management MIB for
        DOCSIS-compliant CMTS.  It provides the objects to allow a Cable
        Modem Termination operator to control the IP addresses and
        protocols associated with subscribers' cable modems.
```

```
        Copyright (C) The Internet Society (2005).  This version of this
        MIB module is part of RFC 4036; see the RFC itself for full legal
        notices."
        REVISION "200503290000Z" -- March 29, 2005
        DESCRIPTION
           "Initial version, published as RFC 4036.  Note that the
           compliance statements in this version apply only to
           implementations that support DOCSIS 1.0/1.1/2.0, which
           are not IPv6-capable."
        ::= { mib-2 125 }

    docsSubMgtObjects OBJECT IDENTIFIER ::= { docsSubMgt 1 }

    docsSubMgtCpeControlTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF DocsSubMgtCpeControlEntry
        MAX-ACCESS not-accessible
        STATUS  current
        DESCRIPTION
            "This table AUGMENTs the docsIfCmtsCmStatusTable, adding
        four WRITEable objects, as well as a read-only object, all of
        which reflect the state of subscriber management on a particular
        CM."
        ::= { docsSubMgtObjects 1 }

    docsSubMgtCpeControlEntry OBJECT-TYPE
        SYNTAX  DocsSubMgtCpeControlEntry
        MAX-ACCESS not-accessible
        STATUS  current
        DESCRIPTION
            "A row in the docsSubMgtCpeControlTable.  All values are set
        at successful modem registration, either from the system default,
        or from objects included in the DOCSIS registration request sent
        upstream to the CMTS from the CM.  The contents of this entry are
        meaningless unless the corresponding docsIfCmtsCmStatusValue (see
        reference) is registrationComplete(6).  The persistence of this
        row is determined solely by the lifespan of the corresponding
        docsIfCmtsCmStatusEntry (normally StorageType=volatile)."

        REFERENCE
            "RFC 2670"
        AUGMENTS { docsIfCmtsCmStatusEntry }
        ::= {docsSubMgtCpeControlTable 1 }

    DocsSubMgtCpeControlEntry ::= SEQUENCE
        {
        docsSubMgtCpeControlMaxCpeIp        Integer32,
        docsSubMgtCpeControlActive          TruthValue,
        docsSubMgtCpeControlLearnable       TruthValue,
```

```
        docsSubMgtCpeControlReset           TruthValue,
        docsSubMgtCpeControlLastReset       TimeStamp
        }

    docsSubMgtCpeControlMaxCpeIp OBJECT-TYPE
        SYNTAX  Integer32(0..2147483647)
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "The number of simultaneous IP addresses permitted behind
        the CM.  If this is set to zero, all CPE traffic from the CM is
        dropped.  If the provisioning object corresponding to
        docsSubMgtCpeIpTable includes more CPE IP address entries for
        this modem than the value of this object, then this object is
        set to the count of the number of rows in docsSubMgtCpeIpTable
        that have the same docsIfCmtsCmStatusIndex value.  (For example,
        if the CM has 5 IP addresses specified for it, this value is 5.)
        This limit applies to learned and DOCSIS-provisioned entries
        but not to entries added through some administrative
        process at the CMTS.  If not set through DOCSIS provisioning,
        this object defaults to docsSubMgtCpeMaxIpDefault.  Note that
        this object is only meaningful if docsSubMgtCpeControlActive
        is true."
        ::= { docsSubMgtCpeControlEntry 1 }

    docsSubMgtCpeControlActive OBJECT-TYPE
        SYNTAX  TruthValue
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "Controls the application of subscriber management to
        this cable modem.  If this is set to true, CMTS-based CPE
        control is active, and all the actions required by the various
        filter tables and controls apply at the CMTS.  If this is set
        to false, no subscriber management filtering is done at the
        CMTS (but other filters may apply).  If not set through DOCSIS
        provisioning, this object defaults to
        docsSubMgtCpeActiveDefault."
        ::= { docsSubMgtCpeControlEntry 2 }

    docsSubMgtCpeControlLearnable OBJECT-TYPE
        SYNTAX  TruthValue
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "Controls whether the CMTS may learn (and pass traffic
        for) CPE IP addresses associated with a cable modem.  If this is
        set to true, the CMTS may learn up to docsSubMgtMaxCpeIp
```

```
        addresses (less any DOCSIS-provisioned entries) related to this
        CM.  Those IP addresses are added (by internal process) to the
        docsSubMgtCpeIpTable.  The nature of the learning mechanism is
        not specified here.

        If not set through DOCSIS provisioning, this object defaults to
        docsSubMgtCpeLearnableDefault.  Note that this object is only
        meaningful if docsSubMgtCpeControlActive is true."
        ::= { docsSubMgtCpeControlEntry 3 }

    docsSubMgtCpeControlReset OBJECT-TYPE
        SYNTAX  TruthValue
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "This object always returns false on read.  If this object is
        set to true, the rows with 'learned' addresses in
        docsSubMgtCpeIpTable for this CM are deleted from that table."
        ::= { docsSubMgtCpeControlEntry 4 }

    docsSubMgtCpeControlLastReset OBJECT-TYPE
        SYNTAX  TimeStamp
        MAX-ACCESS read-only
        STATUS  current
        DESCRIPTION
            "The value of sysUpTime when docsSubMgtCpeControlReset was
        last set true.  Zero if never reset."
        DEFVAL { 0 }
        ::= { docsSubMgtCpeControlEntry 5 }

    docsSubMgtCpeMaxIpDefault OBJECT-TYPE
        SYNTAX  Integer32(0..2147483647)
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "The default value for docsSubMgtCpeControlMaxCpeIp if not
        signaled in the DOCSIS Registration request.  This value should
        be treated as nonvolatile; if set, its value should persist
        across device resets."
        DEFVAL { 16 }
        ::= { docsSubMgtObjects 2 }

    docsSubMgtCpeActiveDefault OBJECT-TYPE
        SYNTAX  TruthValue
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "The default value for docsSubMgtCpeControlActive if not
```

```
        signaled in the DOCSIS Registration request.  This value should
        be treated as nonvolatile; if set, its value should persist
        across device resets."
        DEFVAL { false }
        ::= { docsSubMgtObjects 3 }

    docsSubMgtCpeLearnableDefault OBJECT-TYPE
        SYNTAX  TruthValue
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "The default value for docsSubMgtCpeControlLearnable if not
        signaled in the DOCSIS Registration request.  This value should
        be treated as nonvolatile; if set, its value should persist
        across device resets."
        DEFVAL { true }
        ::= { docsSubMgtObjects 4 }

    docsSubMgtCpeIpTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF DocsSubMgtCpeIpEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table of CPE IP addresses known on a per-CM basis."
        ::= { docsSubMgtObjects 5 }

    docsSubMgtCpeIpEntry OBJECT-TYPE
        SYNTAX      DocsSubMgtCpeIpEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "An entry in the docsSubMgtCpeIpTable.  The first index is
        the specific modem we're referring to, and the second index is
        the specific CPE IP entry."
        INDEX   { docsIfCmtsCmStatusIndex,
                  docsSubMgtCpeIpIndex }
        ::= {docsSubMgtCpeIpTable 1 }

    DocsSubMgtCpeIpEntry ::= SEQUENCE
        {
        docsSubMgtCpeIpIndex        Integer32,
        docsSubMgtCpeIpAddressType  InetAddressType,
        docsSubMgtCpeIpAddr         InetAddress,
        docsSubMgtCpeIpLearned      TruthValue
        }

    docsSubMgtCpeIpIndex OBJECT-TYPE
        SYNTAX      Integer32(1..2147483647)
```

```
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "The index of this CPE IP address relative to the indexed CM.
        An entry is created either through the included CPE IP addresses
        in the provisioning object, or via learning.

        If docsSubMgtCpeControlActive is true and a CMTS receives
        an IP packet from a CM that contains a source IP address that
        does not match one of the docsSubMgtCpeIpAddr entries for this
        CM, one of two things occurs.  If the number of entries is less
        than docsSubMgtCpeControlMaxCpeIp, the source address is added to
        the table and the packet is forwarded.  If the number of entries
        equals the docsSubMgtCpeControlMaxCpeIp, then the packet is
        dropped."
        ::= { docsSubMgtCpeIpEntry 1 }

    docsSubMgtCpeIpAddressType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The type of internet address of docsSubMgtCpeIpAddr."
        ::= { docsSubMgtCpeIpEntry 2 }

    docsSubMgtCpeIpAddr OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The IP address either set from provisioning or learned via
        address gleaning or other forwarding means.  See
        docsSubMgtCpeIpIndex for the mechanism.

        The type of this address is determined by the value of
        docsSubMgtCpeIpAddressType."
        ::= { docsSubMgtCpeIpEntry 3 }

    docsSubMgtCpeIpLearned OBJECT-TYPE
        SYNTAX  TruthValue
        MAX-ACCESS read-only
        STATUS  current
        DESCRIPTION
            "If true, this entry was learned from IP packets sent
        upstream rather than from the provisioning objects."
        ::= { docsSubMgtCpeIpEntry 4 }

    docsSubMgtCmFilterTable OBJECT-TYPE
```

```
        SYNTAX  SEQUENCE OF DocsSubMgtCmFilterEntry
        MAX-ACCESS not-accessible
        STATUS  current
        DESCRIPTION
            "Binds filter groups to modems, identifying for each modem
        the upstream and downstream filter groups that apply to packets
        for that modem.  Normally, this table reflects the filter group
        values signaled by DOCSIS Registration, although values may be
        overridden by management action.

        For each of the columns in this table, zero is a distinguished
        value, indicating that the default filtering action is to be
        taken rather than that associated with a filter group number.
        Zero is used if the filter group is not signaled by DOCSIS
        registration."
        ::= { docsSubMgtObjects 6 }

    docsSubMgtCmFilterEntry OBJECT-TYPE
        SYNTAX  DocsSubMgtCmFilterEntry
        MAX-ACCESS not-accessible
        STATUS  current
        DESCRIPTION
            "Binds a filter group to each direction of traffic for a
        modem.  The filters in this entry apply if
        docsSubMgtCpeControlActive is true.

        The contents of this entry are meaningless unless the
        corresponding docsIfCmtsCmStatusValue (see reference) is
        registrationComplete(6).  The persistence of this row is
        determined solely by the lifespan of the corresponding
        docsIfCmtsCmStatusEntry (normally StorageType=volatile)."
        REFERENCE
            "RFC 2670"
        AUGMENTS { docsIfCmtsCmStatusEntry }
        ::= {docsSubMgtCmFilterTable 1 }

    DocsSubMgtCmFilterEntry ::= SEQUENCE
        {
        docsSubMgtCmFilterSubDownstream        Integer32,
        docsSubMgtCmFilterSubUpstream          Integer32,
        docsSubMgtCmFilterCmDownstream         Integer32,
        docsSubMgtCmFilterCmUpstream           Integer32
    }

    docsSubMgtCmFilterSubDownstream OBJECT-TYPE
        SYNTAX  Integer32(0..65535)
        MAX-ACCESS read-write
        STATUS  current
```

```
        DESCRIPTION
            "The filter group applied to traffic destined for subscribers
        attached to the referenced CM.  Upon row creation, this is set
        either to zero (use default classification, the
        diffServClfrElementSpecific=zeroDotZero row of
        diffServClfrElementTable) or to the value in the provisioning
        object sent upstream from the CM to the CMTS during registration.
        The value of this object is the same as that of the filter group
        index appearing as docsSubMgtFilterGroupIndex."
        ::= { docsSubMgtCmFilterEntry 1 }

    docsSubMgtCmFilterSubUpstream OBJECT-TYPE
        SYNTAX  Integer32(0..65535)
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "The filter group applied to traffic originating from
        subscribers attached to the referenced CM.  Upon row creation
        this is set to either zero (use default classification, the
        diffServClfrElementSpecific=zeroDotZero row of
        diffServClfrElementTable), or to the value in the provisioning
        object sent upstream from the CM to the CMTS.  The value of this
        object is the same as that of the filter group index appearing as
        docsSubMgtFilterGroupIndex."
        ::= { docsSubMgtCmFilterEntry 2 }

    docsSubMgtCmFilterCmDownstream OBJECT-TYPE
        SYNTAX  Integer32(0..65535)
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "The filter group applied to traffic destined for the
        referenced CM itself.  Upon row creation this is set either to
        zero (use default classification, the
        diffServClfrElementSpecific=zeroDotZero row of
        diffServClfrElementTable), or to the value in the provisioning
        object sent upstream from the CM to the CMTS during registration.
        The value of this object is the same as that of the filter group
        index appearing as docsSubMgtFilterGroupIndex."
        ::= { docsSubMgtCmFilterEntry 3 }

    docsSubMgtCmFilterCmUpstream OBJECT-TYPE
        SYNTAX  Integer32(0..65535)
        MAX-ACCESS read-write
        STATUS  current
        DESCRIPTION
            "The filter group applied to traffic originating from the
        referenced CM itself.  This is set upon row creation to either
```

```
        zero (use default classification, the
        diffServClfrElementSpecific=zeroDotZero row of
        diffServClfrElementTable), or to the value in the provisioning
        object sent upstream from the CM to the CMTS during registration.
        The value of this object is the same as the filter group index
        appearing as docsSubMgtFilterGroupIndex."
        ::= { docsSubMgtCmFilterEntry 4 }

    docsSubMgtFilterGroupTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF DocsSubMgtFilterGroupEntry
        MAX-ACCESS not-accessible
        STATUS  current
        DESCRIPTION
            "Provides a collection of referenceable entries to which
        diffServClfrElementSpecific refers.  This table provides filter
        group indices that can be compared with those signaled during
        DOCSIS registration.  A packet matches an entry from this table
        if the packet originated from or is destined to a cable modem
        that registered this index as one of its four filter groups
        (see docsSubMgtCmFilterTable), and if the packet direction and
        MAC address select the use of this index among the four."
        ::= { docsSubMgtObjects 7 }

    docsSubMgtFilterGroupEntry OBJECT-TYPE
        SYNTAX  DocsSubMgtFilterGroupEntry
        MAX-ACCESS not-accessible
        STATUS  current
        DESCRIPTION
            "An entry only exists if needed by the
        diffServClfrElementEntry.  A packet matches this entry if the
        packet's cable modem registered this index as one of its four
        filter groups (see docsSubMgtCmFilterTable) and if the packet
        direction and MAC address select the use of this index among
        the four."
        INDEX { docsSubMgtFilterGroupIndex }
        ::= { docsSubMgtFilterGroupTable 1 }

    DocsSubMgtFilterGroupEntry ::= SEQUENCE
        {
        docsSubMgtFilterGroupIndex    Integer32
        }

    docsSubMgtFilterGroupIndex OBJECT-TYPE
        SYNTAX  Integer32(1..65535)
        MAX-ACCESS read-only
        STATUS  current
        DESCRIPTION
            "The filter group index, from the set signaled at DOCSIS
```

```
        Registration.  Provides a referenceable entry to which
        diffServClfrElementSpecific points.  A packet matches this
        classifier entry if the packet's cable modem registered this
        index value as one of its four filter groups, and if the packet
        direction and MAC address select the use of this index among
        the four.  Because this is the only field in this table, it is
        read-only, contrary to the usual SMI custom of making indices
        not-accessible.

        Note that although zero may be signaled (or defaulted) at DOCSIS
        Registration to indicate a default filtering group, no such entry
        appears in this table, as diffServClfrElementSpecific will
        use a zeroDotZero pointer for that classification."
        ::= { docsSubMgtFilterGroupEntry 1 }

    docsSubMgtConformance OBJECT IDENTIFIER ::= { docsSubMgt 2 }
    docsSubMgtCompliances OBJECT IDENTIFIER ::=
                                            { docsSubMgtConformance 1 }
    docsSubMgtGroups OBJECT IDENTIFIER      ::=
                                            { docsSubMgtConformance 2 }

    docsSubMgtBasicCompliance MODULE-COMPLIANCE
        STATUS      current
        DESCRIPTION
            "The compliance statement for CMTS devices that implement
        CMTS centric subscriber management.

        This compliance statement applies to implementations that
        support DOCSIS 1.0/1.1/2.0, which are not IPv6 capable."


    MODULE DIFFSERV-MIB -- RFC3289
      MANDATORY-GROUPS {
               diffServMIBDataPathGroup,
               diffServMIBClfrGroup,
               diffServMIBClfrElementGroup,
               diffServMIBMultiFieldClfrGroup,
               diffServMIBActionGroup,
               diffServMIBAlgDropGroup,
               diffServMIBCounterGroup
               }

    OBJECT diffServDataPathStatus  -- same as RFC3289
        SYNTAX RowStatus { active(1) }
        WRITE-SYNTAX RowStatus { createAndGo(4), destroy(6) }
        DESCRIPTION
            "Support for createAndWait and notInService is not required."
```

```
   OBJECT diffServClfrStatus  -- same as RFC3289
       SYNTAX RowStatus { active(1) }
       WRITE-SYNTAX RowStatus { createAndGo(4), destroy(6) }
       DESCRIPTION
           "Support for createAndWait and notInService is not required."

   OBJECT diffServClfrElementStatus  -- same as RFC3289
       SYNTAX RowStatus { active(1) }
       WRITE-SYNTAX RowStatus { createAndGo(4), destroy(6) }
       DESCRIPTION
           "Support for createAndWait and notInService is not required."

   OBJECT diffServMultiFieldClfrAddrType
       SYNTAX  InetAddressType { ipv4(1) }
       DESCRIPTION
           "An implementation is only required to support IPv4
       addresses."

   OBJECT diffServMultiFieldClfrSrcAddr
       SYNTAX  InetAddress (SIZE(4))
       DESCRIPTION
           "An implementation is only required to support IPv4
       addresses."

   OBJECT diffServMultiFieldClfrDstAddr
       SYNTAX  InetAddress (SIZE(4))
       DESCRIPTION
           "An implementation is only required to support IPv4
       addresses."

   OBJECT diffServAlgDropStatus  -- same as RFC3289
       SYNTAX RowStatus { active(1) }
       WRITE-SYNTAX RowStatus { createAndGo(4), destroy(6) }
       DESCRIPTION
           "Support for createAndWait and notInService is not required."

   OBJECT diffServDataPathStorage
       SYNTAX StorageType { nonVolatile(3) }
       DESCRIPTION
           "An implementation is only required to support nonvolatile
       storage."

   OBJECT diffServClfrStorage
       SYNTAX StorageType { nonVolatile(3) }
       DESCRIPTION
           "An implementation is only required to support nonvolatile
       storage."
```

```
   OBJECT diffServClfrElementStorage
       SYNTAX StorageType { nonVolatile(3) }
       DESCRIPTION
           "An implementation is only required to support nonvolatile
       storage."

   OBJECT diffServMultiFieldClfrStorage
       SYNTAX StorageType { nonVolatile(3) }
       DESCRIPTION
           "An implementation is only required to support nonvolatile
       storage."

   OBJECT diffServActionStorage
       SYNTAX StorageType { nonVolatile(3) }
       DESCRIPTION
           "An implementation is only required to support nonvolatile
       storage."

   OBJECT diffServCountActStorage
       SYNTAX StorageType { nonVolatile(3) }
       DESCRIPTION
           "An implementation is only required to support nonvolatile
       storage."

   OBJECT diffServAlgDropStorage
       SYNTAX StorageType { nonVolatile(3) }
       DESCRIPTION
           "An implementation is only required to support nonvolatile
       storage."

   OBJECT diffServAlgDropType
       SYNTAX  INTEGER { alwaysDrop(5) }
       DESCRIPTION
           "For DOCSIS subscriber management, this object is
       only used to provide packet filtering.  Implementations
       need not support other values of this enumeration."

   MODULE -- This module i.e., DOCS-IETF-SUBMGT-MIB

   MANDATORY-GROUPS {
           docsSubMgtGroup
           }

   OBJECT docsSubMgtCpeControlMaxCpeIp
       SYNTAX Integer32(0..16)
       DESCRIPTION
           "An implementation is only required to support up to
       sixteen addresses per modem."
```

```
   OBJECT docsSubMgtCpeMaxIpDefault
       SYNTAX Integer32(0..16)
       DESCRIPTION
           "An implementation is only required to support up to
       sixteen addresses per modem."

   OBJECT docsSubMgtCpeIpAddressType
       SYNTAX InetAddressType { ipv4(1) }
       DESCRIPTION
           "An implementation is only required to support IPv4
       addresses."

   OBJECT docsSubMgtCpeIpAddr
       SYNTAX  InetAddress (SIZE(4))
       DESCRIPTION
           "An implementation is only required to support IPv4
       addresses."

   OBJECT docsSubMgtCmFilterSubDownstream
       SYNTAX  Integer32(0..30)
       DESCRIPTION
           "An implementation is only required to support thirty
       filter groups."

   OBJECT docsSubMgtCmFilterSubUpstream
       SYNTAX  Integer32(0..30)
       DESCRIPTION
           "An implementation is only required to support thirty
       filter groups."

   OBJECT docsSubMgtCmFilterCmDownstream
       SYNTAX  Integer32(0..30)
       DESCRIPTION
           "An implementation is only required to support thirty
       filter groups."

   OBJECT docsSubMgtCmFilterCmUpstream
       SYNTAX  Integer32(0..30)
       DESCRIPTION
           "An implementation is only required to support thirty
       filter groups."

           ::= { docsSubMgtCompliances 1 }

   docsSubMgtGroup OBJECT-GROUP
           OBJECTS {
               docsSubMgtCpeControlMaxCpeIp,
               docsSubMgtCpeControlActive,
```

```
                docsSubMgtCpeControlLearnable,
                docsSubMgtCpeControlReset,
                docsSubMgtCpeControlLastReset,
                docsSubMgtCpeMaxIpDefault,
                docsSubMgtCpeActiveDefault,
                docsSubMgtCpeLearnableDefault,
                docsSubMgtCpeIpAddressType,
                docsSubMgtCpeIpAddr,
                docsSubMgtCpeIpLearned,
                docsSubMgtCmFilterSubDownstream,
                docsSubMgtCmFilterSubUpstream,
                docsSubMgtCmFilterCmDownstream,
                docsSubMgtCmFilterCmUpstream,
                docsSubMgtFilterGroupIndex
                }
                STATUS      current
                DESCRIPTION
                    "The objects used to manage host-based cable modems
                via a set of CMTS enforced controls."
                ::= {  docsSubMgtGroups 1 }

   END
```

5. Acknowledgements

This document is based on work by Michael St. Johns, then at Excite@Home. Thanks to Guenter Roeck and Julie McGray for reviewing earlier versions. Thanks to Bert Wijnen, Mike Heard, and Harrie Hazewinkel for extensive later review. Thanks to the working group chairs, Richard Woundy and Jean-Francois Mule, for their extensive support.

6. IANA Considerations

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

Descriptor	OBJECT IDENTIFIER value
docsSubMgt	{ mib-2 125}

7. 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.

[ITU-T-J122] Second-Generation Transmission Systems for Interactive Cable Television Services, J.122, ITU-T, December, 2002.

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

[RFC3289] Baker, F., Chan, K., and A. Smith, "Management Information Base for the Differentiated Services Architecture", RFC 3289, May 2002.

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

8. Informative References

[RFC1858] Ziemba, G., Reed, D., and P. Traina, "Security Considerations for IP Fragment Filtering", RFC 1858, October 1995.

[RFC2669] St. Johns, M., "DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems", RFC 2669, August 1999.

[RFC3128] Miller, I., "Protection Against a Variant of the Tiny Fragment Attack (RFC 1858)", RFC 3128, June 2001.

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

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

9. Security Considerations

This MIB is intended to limit certain kinds of network behavior by subscriber hosts attached to cable modems, including, for example, IP spoofing. These limitations may be compromised, however, if the cable modem's identity or registration process is spoofed. The DOCSIS RFI and privacy specifications [ITU-T-J122] and [DOCSBPI] define a number of mechanisms for assuring modem identity.

For network filtering of TCP traffic to be effective, implementors MUST follow the recommendations in section 3.4.

There are a number of management objects defined in this MIB that have a MAX-ACCESS clause of read-write and/or read-create. These 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.

Unauthorized SETs to this MIB can permit two major security problems with public cable network operation: IP address spoofing, and defeat of operator-defined packet filtering.

The following objects, if SET maliciously, would evade controls on address spoofing:

- docsSubMgtCpeControlMaxCpeIp
- docsSubMgtCpeControlActive
- docsSubMgtCpeControlLearnable
- docsSubMgtCpeControlReset
- docsSubMgtCpeMaxIpDefault
- docsSubMgtCpeActiveDefault
- docsSubMgtCpeLearnableDefault

The following objects could also permit packet filtering to be defeated:

- docsSubMgtCmFilterSubDownstream
- docsSubMgtCmFilterSubUpstream
- docsSubMgtCmFilterCmDownstream
- docsSubMgtCmFilterCmUpstream

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 access to these objects and possibly even to encrypt the values of these objects when they are sent over the network via SNMP. The most sensitive is docsSubMgtCpeIpAddr within docsSubMgtCpeIpTable. Although docsSubMgtCpeIpTable is intended to control address spoofing, it includes information about the current subscriber address pool. This information may in itself be valuable to would-be spoofers.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec), 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) who have legitimate rights to GET or SET (change/create/delete) them.

Author's Address

Wilson Sawyer
50 Kelly Brook Lane
East Hampstead NH 03826

Phone: +1 603 382 7080
EMail: wsawyer@ieee.org

Full Copyright Statement

Intellectual Property

Acknowledgement

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