IP over Cable Data Network (IPCDN)
Internet Draft
Document: <draft-ietf-ipcdn-igmp-mib-04.txt>
Category: Informational

Howard Abramson
ADC Telecommunications

July 2002

Application of the IGMP MIB, RFC 2933, and Cable Device MIB, RFC 2669, to DOCSIS 1.1 Devices

Status of this Memo

Abstract

This memo describes the application of a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes the application of the managed objects specified in RFC 2933, [20], and proposes a new object for the Cable Device MIB, RFC 2669 [25], for SNMP-based management of DOCSIS 1.1 IGMPv2 compliant interfaces.

This memo is a product of the IPCDN working group within the Internet Engineering Task Force. Comments are solicited and should be addressed to the working group's mailing list at ipcdn@ietf.org and/or the author.

Table of Contents

1. The SNMP Management Framework

The SNMP Management Framework presently consists of five major components:

- o An overall architecture, described in RFC 2571 [3].
- o 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 [4], STD 16, RFC 1212 [5] and RFC 1215 [6]. The second version, called SMIv2, is described in STD 58, RFC 2578 [7], STD 58, RFC 2579 [8] and STD 58, RFC 2580 [9].
- o Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in STD 15, RFC 1157 [10]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in RFC 1901 [11] and RFC 1906 [12]. The third version of the message protocol is called SNMPv3 and described in RFC 1906 [12], RFC 2572 [13] and RFC 2574 [14].
- o Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in STD 15, RFC 1157 [10]. A second set of protocol operations and associated PDU formats is described in RFC 1905 [15].
- o A set of fundamental applications described in RFC 2573 [16] and the view-based access control mechanism described in RFC 2575 [17].

A more detailed introduction to the current SNMP Management Framework can be found in RFC 2570 [26].

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 following non-ietf terms are derived either from normal cable system usage, or from the documents associated with the Data Over Cable Service Interface Specification process.

CATV - Originally 'Community Antenna Television', refers to cable or HFC (see below) system used to deliver video signals to a community.

CM, Cable Modem - A CM acts as a 'slave' station in a DOCSIS compliant cable data system.

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.

CMCI - or Subscriber side, refers to the Cable Modem Customer Interface that connects to CPE on the CM.

CPE - Customer Premise Equipment, non-Cable Modem IP Hosts attached to the Cable Modem.

DOCSIS - 'Data Over Cable Interface Specification'. A term referring to the ITU-T J.112 Annex B standard for cable modem systems, [23]

Downstream - From the head-end towards the subscriber.

Head-end - The origination point in most cable systems of the subscriber video signals. Generally this is also the location of the CMTS equipment.

HFC - Hybrid-Fiber-Coax, refers to physical wire(s) connecting the CMTS and CM.

MAC Packet - A DOCSIS PDU.

NSI - Network-Side-Interface, refers to interface(s) on the CMTS that are typically connected to the Internet.

RF - Radio Frequency.

Upstream - From the subscriber towards the head-end.

2.1 Conventions used in this document

The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in this document are to be interpreted as described in RFC-2119, [2].

3. Overview

The DOCSIS Multicast CM and CMTS interconnect specification can be modeled (or described) by 'splitting' the traditional Internet Group Management Protocol (IGMP), [22], interfaces into Host and Querier side interfaces. That is, to provide basic DOCSIS 1.1 Multicast capabilities, all NSI-facing interfaces (NSI on the CMTS and HFC-side on CM) need only present an IGMP Host interface to the external multicast network. All Subscriber-facing interfaces (HFC-side on CMTS and CPE-side on CM) need only present a Querier interface to CPE. This is in contrast to a Multicast Router model where each interface has both Host and Querier capabilities.

It is expected that the root of each Multicast session tree originate from the NSI interface(s). Although not strictly prohibited by the RFI, a more symmetrical model, where the root of a Multicast group may be on the HFC/Subscriber-side, is discouraged. In either case, Querying MUST only be in the downstream direction (initiated by an NSI Querier or the CMTS itself). Host Membership Reporting is expected to be in the upstream direction (from CPE or active IGMP CM devices). The IGMPv2 MIB provides an excellent and standard means for managing multicast within such a network.

3.1 IGMP Capabilities: Active and Passive Mode

There are two basic modes of IGMP capability defined by the DOCSIS 1.1 RFI specification that are applicable to a DOCSIS 1.1 device.

- Passive IGMP Devices - The first mode is a passive operation in which the device selectively forwards IGMP based upon the known state of multicast session activity on the subscriber side (an example of this is described in Appendix L of [23]). In passive mode, the device derives its IGMP timers based on the rules specified in section 3.3.1 of the RFI.

- Active IGMP Devices - The second mode is an active operation in which the device terminates and initiates IGMP based upon the known state of multicast session activity on the subscriber side. One example of the latter, active, mode is commonly referred to as an IGMP-Proxy implementation (as described in [21]). A more complete example of an active IGMP device is that of a Multicast Router.

Passive IGMP devices do not initiate IGMP PDUs (i.e., report or

queries). Passive devices rely on an (upstream) device to transmit IGMP Queries and a (downstream) device to transmit IGMP Membership Reports and Leaves to manage session activity, e.g., a Multicast Router and Multicast Host, respectively. In contrast, an active IGMP

device initiates IGMP PDUs (queries and/or reports) to manage session activity.

Although a specific implementation is not imposed, a DOCSIS 1.1 device MUST meet the requirements stated in section 3.3.1 of [23] and MUST support the IDMR IGMP MIB, [20], and the Cable Device MIB, [25], as described herein. As specified in the DOCSIS 1.1 RFI, active CMs are explicitly prohibited from transmitting IGMP Queries upstream onto the HFC. However, an active CMTS may transmit IGMP Queries on any of its interfaces.

3.2 IGMP Timers

The IGMP standard, [22], defines several timers that are applicable to the management of Multicast session activity on a given interface. Timers for DOCSIS 1.1 passive IGMP devices are derived based on the requirements specified in section 3.3.1 of [23]. As such, MIB objects that apply to these timers must be considered read only values. IGMP timers in active devices should be considered values that may be managed within the device.

4. DOCSIS 1.1 Interfaces and the IGMP MIB

DOCSIS 1.1 devices, CM and CMTS, MUST support the IDMR IGMP MIB (RFC-2933), [20]. As such, the following sections describe the application of RFC-2933 to DOCSIS 1.1 devices.

The IDMR IGMP MIB is organized into two distinct tables, the interface and cache tables. The IGMP Interface Table contains entries for each interface that supports IGMP on a device. For DOCSIS 1.1 this includes the NSI and HFC for the CMTS and the HFC and CMCI on the CM. The IGMP Cache Table contains one row for each IP Multicast Group for which there are active members on a given interface. Active membership MUST only exist on the CMCI of a Cable Modem. However, active membership MAY exist on both the NSI and HFC side interfaces of the CMTS. This is because a CMTS may be implemented as a Multicast Router on which other network side devices are actively participating in a multicast session.

Support of the IDMR IGMP MIB by DOCSIS 1.1 devices is presented in terms of IGMP capabilities, the device type (CM or CMTS), and the interface on which IGMP is supported. This is followed by a set of new IGMP MIB conformance, compliance and group statements for DOCSIS 1.1 devices.

4.1 DOCSIS 1.1 CM Support for the IGMP MIB

There are two types of interfaces applicable to IGMP on a DOCSIS 1.1 CM. These are the HFC-Side and CMCI-Side interfaces, respectively. Application of the IGMP MIB to DOCSIS 1.1 CMs is presented in terms of passive and active CM operation and these two interface types.

4.1.1 igmpInterfaceTable - igmpInterfaceEntry

4.1.1.1 igmpInterfaceIfIndex

The ifIndex value of the interface for which IGMP is enabled.

All Modes / Both sides: same for passive and active modes.

HFC-side: not-accessible. ifIndex of docsCableMaclayer(127), CATV MAC Layer
CMCI-side: not-accessible. ifIndex of CMCI-Side interface.

4.1.1.2 igmpInterfaceQueryInterval

The frequency at which IGMP Host-Query packets are transmitted on this interface.

Passive Mode

HFC-side: n/a, read-only. The CM MUST not transmit queries upstream. Return a value of zero.
CMCI-side: read only . This value is derived based on the interval of queries received from an upstream querier.

Active Mode

HFC-side: n/a, read-only. The CM MUST not transmit queries upstream. Return a value of zero.
CMCI-side: read-create. Min = 0; Max = (2^32 - 1); Default = 125

4.1.1.3 igmpInterfaceStatus

The activation of a row enables IGMP on the interface. The destruction of a row disables IGMP on the interface.

All Modes / Both sides: MUST be enabled on both interfaces for all DOCSIS 1.1 CM interfaces.

4.1.1.4 igmpInterfaceVersion

The version of IGMP which is running on this interface.

All Modes / Both sides: MUST be version 2 for all DOCSIS 1.1 CM interfaces.

4.1.1.5 igmpInterfaceQuerier

The address of the IGMP Querier on the IP subnet to which this interface is attached.

Passive Mode

HFC-side: read-only. MUST be the address of an upstream device for both active and passive CMs.
CMCI-side: read-only. Same as HFC-side value.

Active Mode

HFC-side: read-only. MUST be the address of an upstream device for both active and passive CMs.
CMCI-side: read-only. Active CMs may report it as the HFC-side value. However, active CMs that participate in IGMP Querier negotiation on the CMCI may report it as a different CPE.

4.1.1.6 igmpInterfaceQueryMaxResponseTime

The maximum query response time advertised in IGMPv2 queries on this interface.

Passive Mode

HFC-side: n/a, read-only. return a value of zero.
CMCI-side: read-only. This value is derived from observation of queries received from an upstream querier

Active Mode

HFC-side: n/a, read-only. return a value of zero.
CMCI-side: read-create. Min = 0; Max = 255; Default = 100.

4.1.1.7 igmpInterfaceQuerierUpTime

The time since igmpInterfaceQuerier was last changed.

Passive Mode

HFC-side: read-only.
CMC-side: n/a, read-only. Return a value of zero.

```
   Active Mode
   -----------
   HFC-side:  read-only.
   CMCI-side: read-only.
```

4.1.1.8 igmpInterfaceQuerierExpiryTime

The amount of time remaining before the other querier present timer expires. If the local system is the querier, the value of this object is zero.

Passive Mode

Both Sides: n/a, read-only. The CM is never the querier, return 0.

Active Mode

HFC-side: n/a, read-only. Return 0.
CMCI-side: read-only. The CM may only be the querier on the CMCI.

4.1.1.9 igmpInterfaceVersion1QuerierTimer

The time remaining until the host assumes that there are no IGMPv1 routers present on the interface. While this is non-zero, the host will reply to all queries with version 1 membership reports.

Passive Mode

HFC-side: n/a read-only. Return a value of zero.
CMCI-side: n/a read-only. Return a value of zero.

Active Mode

HFC-side: read-only.
CMCI-side: read-only.

4.1.1.10 igmpInterfaceWrongVersionQueries

The number of queries received whose IGMP version does not match igmpInterfaceVersion, over the lifetime of the row entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Although, DOCSIS 1.1 requires that all CM and CMTS devices support IGMPv2, it is possible for an upstream querier to be an IGMPv1 querier.

All Modes / Both sides - read-only. The number of non-v2 queries received on this interface.

4.1.1.11 igmpInterfaceJoins

The number of times a group membership has been added on this interface; that is, the number of times an entry for this interface

has been added to the Cache Table. This object gives an indication of the amount of IGMP activity over the lifetime of the row entry.

All HFC-side - n/a, read-only. Always return a value of zero (see CMCI-side).

All CMCI-side - read-only. Group membership is defined to only exist on the CMCI.

4.1.1.12 igmpInterfaceProxyIfIndex

Some devices implement a form of IGMP proxy whereby memberships learned on the interface represented by this row, cause IGMP Host Membership Reports to be sent on the interface whose ifIndex value is given by this object. Such a device would implement the igmpV2RouterMIBGroup only on its router interfaces (those interfaces with non-zero igmpInterfaceProxyIfIndex). Typically, the value of this object is 0, indicating that no proxy is being done.

Passive Mode

Both side: read-only. Always return a value of zero.

Active Mode

HFC-side: read-only. Always return a value of zero.
CMCI-side: read-only. Always return ifIndex for HFC-side interface.

4.1.1.13 igmpInterfaceGroups

The current number of entries for this interface in the Cache Table (number of active sessions Proxied or Active on this Interface).

All HFC-side - n/a, read-only. Always return a value of zero (see CMCI-side).

All CMCI-side - read-only. Group membership is defined to only exist on the CMCI.

4.1.1.14 igmpInterfaceRobustness

The robustness variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness variable may be increased. IGMP is robust to (robustness variable-1) packet losses.

Passive Mode

In passive mode, the device does not initiate IGMP PDUs.

HFC-side: read-write. Return default value of two.

CMCI-side: read-write. Return default value of two.

Active Mode

Both sides: read-create. Min = 1; Max = (2^32 - 1); Default = 2

Note, on the HFC-side, the Robustness variable is applicable to the number of Unsolicited Membership Reports transmitted upstream by the CM. Although RFC 2236 does not explicitly state that the robustness variable be used for this purpose, it is implied by the following statement.

> "To cover the possibility of the initial Membership Report being lost or damaged, it is recommended that it be repeated once or twice after short delays [Unsolicited Report Interval]. (A simple way to accomplish this is to send the initial Version 2 Membership Report and then act as if a Group-Specific Query was received for that group, and set a timer appropriately), [22]."

The Query Response Interval is derived from the last Max Response Time received (or 10 seconds if none), and the number of retransmissions is equal to the Robustness variable.

4.1.1.15 igmpInterfaceLastMemberQueryIntvl

The last member query interval is the max response time inserted into group specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

Passive Mode

HFC-side: n/a, read-only. return a value of zero.
CMCI-side: read-only. This value is derived from observation of queries received from an upstream querier

Active Mode

HFC-side: n/a, read-only. return a value of zero.
CMCI-side: read-create. Min = 0; Max = 255; Default = 100.

4.1.2 **igmpCacheTable -** igmpCacheEntry

4.1.2.1 **igmpCacheAddress**

The IP multicast group address for which this entry contains information.

All Modes / Both sides: Not-accessible (index). Report the address of active IP Multicast on the CMCI interface.

4.1.2.2 **igmpCacheIfIndex**

The interface for which this entry contains information for an IP multicast group address.

All Modes / CMCI side: Not-accessible (index). MUST only apply to CMCI interface (e.g., membership is only active on subscriber side of CM).

4.1.2.3 **igmpCacheSelf**

An indication of whether the local system is a member of this group address on this interface.

Passive Mode / Both sides: read-only. MUST be set to FALSE. The CM is not a member of any group.

Active Mode / Both sides: read-create. Implementation specific. If the CM is configured to be a member of the group, then membership reports are sent with the CMs IP Address but MUST ONLY be sent in proxy for active sessions on the CMCI (e.g., the CM MUST NOT be a member of a multicast group that is not active on the CMCI). If the CM is not configured to be a member, then the source IP Address of membership reports MUST be set to the current value of the igmpCacheLastReporter address.

4.1.2.4 **igmpCacheLastReporter**

The IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, this object has the value of 0.0.0.0.

All Modes / CMCI side: MUST only apply to last reporter on CMCI interface (e.g., membership only active on subscriber side of CM).

4.1.2.5 igmpCacheUpTime

The time elapsed since this entry was created.

All Modes / CMCI side: read-only. MUST only apply to duration of membership on CMCI interface (e.g., membership is only active on subscriber side of CM).

4.1.2.6 igmpCacheExpiryTime

The minimum amount of time remaining before this entry will be aged out.

All Modes / Both sides - read-only. MUST only apply to duration of membership on CMCI interface (e.g., membership is only active on subscriber side of CM).

4.1.2.7 igmpCacheStatus

The status of this entry.

All Modes / CMCI side - read-create. MUST only apply to membership on CMCI interface (e.g., membership is only active on subscriber side of CM). Deletion of a row results in preventing downstream forwarding to this IP Multicast group address on this interface. Deletion of a row does not prevent recreation of the row by subsequent IGMP Membership Reporting. The agent can refuse to remove the row, but this is implementation dependent.

4.1.2.8 igmpCacheVersion1HostTimer

The time remaining until the local querier will assume that there are no longer any IGMP version 1 members on this IP subnet attached to this interface. Upon hearing any IGMPv1 membership report, this value is reset to the group membership timer. While this time remaining is non-zero, the local querier ignores any IGMPv2 leave messages for this group that it receives on this interface.

Passive Mode

Both side: n/a, read-only. Return a value of zero.

Active Mode

HFC-side: n/a, read-only. Return a value of zero.
CMCI-side: read-only.

4.2 DOCSIS 1.1 CMTS Support for the IGMP MIB

There are two types of interfaces applicable to IGMP on a DOCSIS 1.1 CMTS. These are the HFC-Side and NSI-Side interfaces, respectively. Application of the IGMP MIB to a DOCSIS 1.1 CMTS is presented in terms of passive and active CMTS operation and these two interface types. In contrast to a CM, the CMTS is likely to have several NSI-side interfaces and several HFC-side (subscriber-side) interfaces.

It is important to note that an active IGMP capable CMTS may be implemented as a proxy, router, or hybrid device. As such, the CMTS may be capable of querying on both its NSI and HFC side interfaces and may manage membership for devices on its NSI interfaces (e.g., as a multicast router). This is different than an active CM, which MUST NOT query on its HFC side interface (e.g., it may only query on its CMCI). This capability is accounted for in the application of the IGMP MIB to the CMTS.

4.2.1 **igmpInterfaceTable-** igmpInterfaceEntry

4.2.1.1 **igmpInterfaceIfIndex**

The ifIndex value of the interface for which IGMP is enabled.

All Modes

This is the same for passive and active modes.

NSI-side: not-accessible. ifIndex of applicable network side interface(s).
HFC-side: not-accessible. ifIndex of docsCableMaclayer(127), CATV MAC Layer interface.

4.2.1.2 **igmpInterfaceQueryInterval**

The frequency at which IGMP Host-Query packets are transmitted on this interface.

Passive Mode

NSI-side: n/a, read-only. Return a value of zero.
HFC-side: read only . This value is derived based on the interval of queries received from a Network Side querier.

Active Mode

NSI-side: read-create. Min = 0; Max = (2^32 - 1); Default = 125
HFC-side: read-create. Min = 0; Max = (2^32 - 1); Default = 125

4.2.1.3 igmpInterfaceStatus

All Modes / All Interfaces: the activation of a row enables IGMP on the interface. The destruction of a row disables IGMP on the interface.

4.2.1.4 igmpInterfaceVersion

The version of IGMP which is running on this interface. MUST be version 2 for all DOCSIS 1.1 CMTS interfaces.

4.2.1.5 igmpInterfaceQuerier

The address of the IGMP Querier on the IP subnet to which this interface is attached.

Passive Mode

NSI-side: read-only. This is the address of a network side device.
HFC-side: read-only. Same as NSI-side value.

Active Mode

NSI-side: read-only.
HFC-side: read-only. Active CMTSs MUST report this as an IP Address assigned to the CMTS' HFC-side interface. That is, queries MUST not originate from CMs or CPE.

4.2.1.6 igmpInterfaceQueryMaxResponseTime

The maximum query response time advertised in IGMPv2 queries on this interface.

Passive Mode

NSI-side: n/a, read-only. return a value of zero.
HFC-side: read-only. This value is derived from observation of queries received from a network side querier.

Active Mode

NSI-side: read-create. Min = 0; Max = 255; Default = 100.
HFC-side: read-create. Min = 0; Max = 255; Default = 100.

4.2.1.7 igmpInterfaceQuerierUpTime

The time since igmpInterfaceQuerier was last changed.

Passive Mode

NSI-side: read-only.
HFC-side: n/a, read-only. Return a value of zero.

Active Mode

```
-----------
NSI-side:  read-only.
HFC-side:  read-only.
```

4.2.1.8 igmpInterfaceQuerierExpiryTime

The amount of time remaining before the other querier present timer expires. If the local system is the querier, the value of this object is zero.

```
Passive Mode
------------
All interfaces: n/a, read-only. The CMTS is not a querier, return 0.

Active Mode
-----------
NSI-side:  read-only.
HFC-side:  read-only. The CMTS MUST be the only querier on the HFC.
```

4.2.1.9 igmpInterfaceVersion1QuerierTimer

The time remaining until the host assumes that there are no IGMPv1 routers present on the interface. While this is non-zero, the host will reply to all queries with version 1 membership reports.

```
Passive Mode
------------
NSI-side:  n/a read-only. Return a value of zero.
HFC-side:  n/a read-only. Return a value of zero.

Active Mode
-----------
NSI-side:  read-only.
HFC-side:  read-only.
```

4.2.1.10 igmpInterfaceWrongVersionQueries

The number of queries received whose IGMP version does not match igmpInterfaceVersion, over the lifetime of the row entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Although, DOCSIS 1.1 requires that all CMTS and CMTSTS devices support IGMPv2, it is possible for a network side querier to be an IGMPv1 querier.

All Modes / All interfaces: read-only. The number of non-v2 queries received on this interface.

4.2.1.11 igmpInterfaceJoins

The number of times a group membership has been added on this interface; that is, the number of times an entry for this interface has been added to the Cache Table. This object gives an indication of the amount of IGMP activity over the lifetime of the row entry.

Passive Mode

NSI-side: n/a read-only. Return a value of zero.
HFC-side: n/a read-only. Return a value of zero.

Active Mode

NSI-side: read-only.
HFC-side: read-only.

4.2.1.12 igmpInterfaceProxyIfIndex

Some devices implement a form of IGMP proxy whereby memberships learned on the interface represented by this row, cause IGMP Host Membership Reports to be sent on the interface whose ifIndex value is given by this object. Such a device would implement the igmpV2RouterMIBGroup only on its router interfaces (those interfaces with non-zero igmpInterfaceProxyIfIndex). Typically, the value of this object is 0, indicating that no proxy is being done.

Passive Mode

All Interfaces: read-only. Always return a value of zero.

Active Mode

NSI-side: read-only.
HFC-side: read-only. Always return an ifIndex for a NSI-side interface.

4.2.1.13 igmpInterfaceGroups

The current number of entries for this interface in the Cache Table.

Passive Mode

NSI-side: n/a read-only. Return a value of zero.
HFC-side: n/a read-only. Group membership of HFC-side devices.

Active Mode

NSI-side: read-only.
HFC-side: read-only.

4.2.1.14 igmpInterfaceRobustness

The robustness variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness

variable may be increased. IGMP is robust to (robustness variable-1) packet losses.

Passive Mode

In passive mode, the device does not initiate IGMP PDUs.

HFC-side: read-write. Return default value of two.
CMCI-side: read-write. Return default value of two.

Active Mode

All interfaces: read-create. Min = 1; Max = (2^32 - 1); Default = 2

4.2.1.15 igmpInterfaceLastMemberQueryIntvl

The last member query interval is the max response time inserted into group specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

Passive Mode

NSI-side: n/a, read-only. return a value of zero.
HFC-side: read-only. This value is derived from observation of queries received from a network side querier.

Active Mode

NSI-side: read-create. Min = 0; Max = 255; Default = 100.
HFC-side: read-create. Min = 0; Max = 255; Default = 100.

4.2.2 igmpCacheTable - igmpCacheEntry

4.2.2.1 igmpCacheAddress

The IP multicast group address for which this entry contains information.

All Modes / All Interfaces: Not-accessible (index). Report the address of active IP Multicast on the interface.

4.2.2.2 igmpCacheIfIndex

The interface for which this entry contains information for an IP multicast group address.

Passive Mode / HFC Side: Not-accessible (index). MUST only apply to HFC side interface (e.g., membership is only active on subscriber side of CMTS).

```
   Active Mode
   -----------
   NSI-side:  not-accessible
   HFC-side:  not-accessible
```

4.2.2.3 igmpCacheSelf

An indication of whether the local system is a member of this group address on this interface.

Passive Mode / All Interfaces: read-only. MUST be set to FALSE. The CMTS is not a member of any group.

Active Mode

NSI-side: read-create. Implementation specific (i.e., may apply to RIPv2 or OSPF)
HFC-side: read-create. Default is FALSE. The device is typically not a member of any group on the HFC.

4.2.2.4 igmpCacheLastReporter

The IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, this object has the value of 0.0.0.0.

Passive Mode / HFC Side: MUST only apply to last reporter on HFC-side interface (e.g., membership is only active on subscriber side of CMTS).

Active Mode

NSI-side: read-only
HFC-side: read-only

4.2.2.5 igmpCacheUpTime

The time elapsed since this entry was created.

Passive Mode / HFC-side: MUST only apply to duration of membership on HFC-side interface (e.g., membership is only active on subscriber side of CMTS).

Active Mode

NSI-side: read-only
HFC-side: read-only

4.2.2.6 igmpCacheExpiryTime

The minimum amount of time remaining before this entry will be aged out.

Passive Mode / HFC-side: MUST only apply to duration of membership on HFC-side interface (e.g., membership is only active on subscriber side of CMTS).

Active Mode

NSI-side: read-only
HFC-side: read-only

4.2.2.7 igmpCacheStatus

The status of this entry. Deletion of a row results in preventing forwarding to this IP Multicast group address on this interface. Deletion of a row does not prevent recreation of the row by subsequent IGMP Membership Reporting or Multicast Routing updates. The agent can refuse to remove the row, but this is implementation dependent.

Passive Mode / HFC-side: read-create MUST only apply to membership on HFC-side interface (e.g., membership is only active on subscriber side of CMTS).

Active Mode

NSI-side: read-create
HFC-side: read-create

4.2.2.8 igmpCacheVersion1HostTimer

The time remaining until the local querier will assume that there are no longer any IGMP version 1 members on this IP subnet attached to this interface. Upon hearing any IGMPv1 membership report, this value is reset to the group membership timer. While this time remaining is non-zero, the local querier ignores any IGMPv2 leave messages for this group that it receives on this interface.

Passive Mode / All interfaces: n/a, read-only. Return a value of zero.

Active Mode

NSI-side: read-only.
HFC-side: read-only.

4.3 IGMP MIB Compliance and MIB Object Groupings

This section presents a proposed set of MIB compliance and MIB Groups that are applicable to the description as set forth in this document.

4.3.1 DOCSIS 1.1. IGMP MIB Compliance Statements

4.3.1.1 docsIgmpV2PassiveDeviceCompliance

```
docsIgmpV2PassiveDeviceCompliance MODULE-COMPLIANCE
     STATUS current
     DESCRIPTION
     "The compliance statement for DOCSIS Devices passively running
      IGMPv2 and implementing the IGMP MIB."
     MODULE - this module
     MANDATORY-GROUPS { igmpBaseMIBGroup,
                        igmpRouterMIBGroup,
                        igmpV2RouterMIBGroup
                      }
     OBJECT igmpInterfaceStatus
     MIN-ACCESS read-only
     DESCRIPTION
     "Write access is not required. "
     OBJECT igmpCacheStatus
     MIN-ACCESS read-only
     DESCRIPTION
     "Write access is not required."
     ::= {docsIgmpMIBCompliances 1}
```

4.3.1.2 docsIgmpV2ActiveDeviceCompliance

```
docsIgmpV2ActiveCmCompliance MODULE-COMPLIANCE
     STATUS current
     DESCRIPTION
     "The compliance statement for DOCSIS Devices actively running
      IGMPv2 and implementing the IGMP MIB."
     MODULE - this module
     MANDATORY-GROUPS { igmpBaseMIBGroup,
                        igmpV2HostMIBGroup,
                        igmpRouterMIBGroup,
                        igmpV2RouterMIBGroup
                      }
     OBJECT igmpInterfaceStatus
     MIN-ACCESS read-only
     DESCRIPTION
     "Write access is not required."
     OBJECT igmpCacheStatus
```

```
        MIN-ACCESS read-only
        DESCRIPTION
        "Write access is not required."
        ::= {docsIgmpMIBCompliances 2}
```

4.3.2 MIB Groups

See IGMP MIB for a description of the objects included in each group.

4.3.2.1 igmpV2HostMIBGroup

Active Devices only (optional, see notes for igmpCacheSelf).

4.3.2.1 igmpV2RouterMIBGroup

Active and Passive Devices

4.3.2.2 igmpBaseMIBGroup

Active and Passive Devices

4.3.2.3 igmpV2RouterMIBGroup

Active and Passive Devices

4.3.2.4 igmpRouterMIBGroup

Active and Passive Devices

4.3.2.5 igmpV2HostOptMIBGroup

Active and Passive Devices

4.3.2.6 igmpV2ProxyMIBGroup

Active Devices only.

5. DOCSIS 1.1 IGMP Mode Control and Cable Device MIB Support

The default mode of a DOCSIS 1.1 CM MUST be to support passive IGMP operation. The default mode of a DOCSIS 1.1 CMTS SHOULD be to support passive IGMP operation. No objects in the IDMR IGMP MIB provide a consistent way to control this mode for a DOCSIS 1.1 device. One option considered was to overload the context of the igmpInterfaceProxyIfIndex such that setting this object constitutes active mode and clearing the object constitutes passive mode. The problem is that this precludes implementation of a DOCSIS 1.1 device as a multicast router. Another option was to overload the context of the igmpInterfaceQueryInterval such that setting this object constitutes active mode and clearing this object constitutes passive mode. However, this precludes setting the query interval to zero.

The, unambiguous, solution to controlling DOCSIS 1.1 IGMP mode is to define a new object. The following object is proposed as a new entry to the docsDevBaseGroup in the Cable Device MIB, [25]. This object is shown as read-write for devices that support both modes. For devices that only support the required passive mode, this object is specified to be read-only.

```
docsDevIgmpModeControl OBJECT-TYPE
    SYNTAX          INTEGER {passive(1), active(2)}
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION    "This object controls the mode of operation that
                    the CM/CMTS will operate in. In passive mode,
                    the device forwards IGMP between interfaces
                    based on knowledge of Multicast Session activity
                    on the subscriber side interface and the rules
                    defined in section 3.3.1 of the RFI. In active
                    mode, the device terminates and initiates IGMP
                    through its interfaces based on the knowledge of
                    Multicast Session activity on the subscriber
                    side interface."
    DEFVAL          { 1 } -- passive
    ::= { docsDevBase 6 }

docsDevBaseGroup OBJECT-GROUP
        OBJECTS {
             docsDevRole,
             docsDevDateTime,
             docsDevResetNow,
             docsDevSerialNumber,
             docsDevSTPControl,
             docsDevIgmpModeControl
```

```
            }
            STATUS      current
            DESCRIPTION
                "A collection of objects providing device status and
                 control."
```

```
          ::= { docsDevGroups 1 }

   docsDevBasicComplianceV2 MODULE-COMPLIANCE
          STATUS  current
          DESCRIPTION
          "The compliance statement for MCNS Cable Modems and
          Cable Modem Termination Systems."

   OBJECT docsDevIgmpModeControl
       MIN-ACCESS read-only
       DESCRIPTION
           "It is compliant to implement this object as read-only.
            Devices need only support passive(1) mode."
       ::= { docsDevCompliances 1 }
```

6. Security Considerations

This MIB relates to a system which will provide metropolitan public internet access to multicast services. The security considerations discussed in RFC 2933, [20], apply here as well.

There are a number of management objects defined in this MIB that have a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations.

SNMPv1 by itself is not a secure environment. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB.

It is recommended that the implementers consider the security features as provided by the SNMPv3 framework. Specifically, the use of the User-based Security Model RFC 2574 [14] and the View-based Access Control Model RFC 2575 [17] is recommended.

It is then a customer/user responsibility to ensure that the SNMP entity giving access to an instance of this MIB, is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

6.1 Additional DOCSIS IGMP Security Considerations

Although it is beyond the scope of this MIB application note, the security of IGMP and IP Multicasting in a DOCSIS network is worth further discussion. For example, improper transmission of IGMP PDUs may result in unauthorized access to multicast services, and may present 'denial-of-service' potential on the HFC (e.g., mischievous users could simply flood the upstream with IGMP for sessions they are not authorized to receive; the result being cluttering the downstream with unauthorized and undesired multicast traffic).

Early discussions on IGMP within the IPCDN and DOCSIS communities centered on conditional and timed multicast session activity. More recent discussions have focused on a tighter coupling between the Baseline Privacy Plus protocol, [24], and IGMP to resolve these issues. Tying these protocols too tightly together may present problems and complexity that is unwarranted during the early stages of multicast deployments in DOCSIS networks. It is important to note

that a DOCSIS CM will never forward unauthorized and encrypted data from the HFC to the CMCI as it will fail on the downstream Security Association as defined by the BPI+ protocol. It is expected that 'non-destructive' users will give up trying to receive unauthorized

sessions (e.g., stop sending membership reports for sessions not received). This will result in timing-out the session through normal IGMP mechanisms (e.g., no one left sending MRs for this group). Preventing denial-of-service is, perhaps, the greater security concern for IGMP in a DOCSIS network. One approach is to establish controls on the CMTS that consult BPI+ Authorization tables before accepting IGMP Membership Reports from a given CM.

6.1.1 Proposed Security Rules for DOCSIS IGMP

The following set of rules have been proposed to provide better security for IGMP/IP Multicast in DOCSIS networks. The reader is referred to the RFC 2236, [22], and the BPI+ specification, [24].

NOTE: forwarding of IGMP, presented below, MUST be subject to permit rules at the IP and IEEE802.2 MAC Layer.

- The CM MUST NOT forward IGMP PDUs (Membership Reports, Leaves, etc.) upstream for Multicast Sessions that have been SA-MAP Reply Rejected for authorization (e.g., this does not apply to SA-MAP reject for unencrypted sessions).

Discussion: this requires that the CM apply the following order to forwarding of IGMP PDUs upstream.

> If the IGMP PDU is for a Session that is new to the CMCI-LAN, then the CM MUST NOT forward the PDU for this Session until such time as a BPI+ SA-MAP Reply, with the requested SA mapping, or a SA-Map Reject 'not mapped to a SA' is received. Said another way, the CM MUST NOT forward IGMP for Sessions that result in a SA-MAP Reject not authorized for SA. The CM MUST continue to treat all subsequent IGMP Membership Reports for this session as being new and MUST result in a SA-MAP Request for this traffic flow (Session).

- The CM MUST consider all Multicast Sessions, associated with a given SA, inactive on the CMCI-LAN as soon as the TEK state machine terminates for these sessions. That is, once the TEK state machine terminates (either by a Key Reject or Authorization Invalid), Multicast data for Sessions associated with this SA MUST NOT be forwarded from the HFC to the CMCI AND the CM MUST consider subsequent MRs for these Sessions as being new (as described above).

- The CMTS SHOULD NOT process an IGMP PDU sent from/through a CM

if the MR is for a Session that is associated with Multicast Addresses that has a SA (is encrypted) and is not authorized for the CM (based on the HFC-side CM mac address).

Discussion: this requires that the CMTS consult the BPI+ docsBpi2CmIpMulticastMapTable (IP Multicast Address to SAID) table and the docsBpi2CmtsMulticastAuthTable (CMTS Multicast SAID Authorization) table before processing IGMP messages (MR or Leave; Queries are explicitly prohibited on the upstream). The following rules apply.

If the IGMP is for a Multicast address that has an SA and the CM from which this IGMP PDU was sent is authorized for this SA, then process the IGMP (i.e., MRs are reflected on downstream, and the NSI multicast filters are removed to send downstream data, etc.)

If the IGMP is for a Multicast address that does not have an SA, then process the IGMP.

If the IGMP is for a Multicast address that has an SA and the CM from which this IGMP PDU was sent is not authorized for this SA, then the IGMP PDU SHOULD be silently discarded.

- The CMTS MAY stop forwarding Multicast data downstream for Sessions that have an SA and for which there is no TEK state machine running.

7. References

[1] Bradner, S., "The Internet Standards Process - Revision-3", BCP 9, RFC 2026, October 1996.

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

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

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

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

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

[7] McCloghrie, K., Perkins, D. and J. Schoenwaelder,

"Structure of Management Information for Version 2
(SMIv2)", STD 58, RFC2578, April 1999.

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

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

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

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

[12] 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.

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

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

[15] 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.

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

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

[18] Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 2272, January 1998.

[19] Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 2274, January 1998.

[20] McCloghrie, K., Farinacci, D., Thaler, D., "Internet
Group Management Protocol MIB", RFC 2933, October 2000.

[21] Fenner, W., "IGMP-based Multicast Forwarding ('IGMP Proxying')", internet draft in progress.

[22] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[23] "Data Over Cable Service Interface Specifications - Radio Frequency Interface Specification SP-RFIv1.1-I07-010829", DOCSIS, August 2001, available at http://www.cablemodem.com/.

[24] "Data Over Cable Service Interface Specifications - Baseline Privacy Plus Interface Specification SP-BPI+-I07-010829", DOCSIS, August 2001, available at http://www.cablemodem.com/.

[25] St. Johns, M., "DOCSIS Cable Device MIB", RFC 2669, August 1999.

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

8. Acknowledgments

The author would like to acknowledge the following individuals for contributions to this document. This includes Paul Gray, Greg Nakanishi, Pak Siripunkaw, Mike St. Johns, David Thaler, Rich Woundy, and Greg White.

9. Author's Address

Howard D. Abramson
ADC Telecommunications
8 Technology Drive
Westborough, MA 01581
Phone: 508.870.2615
Email: howard_abramson@adc.com

10. 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 implementers 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.

11. Full Copyright Statement

Acknowledgement

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