



**Society of Cable  
Telecommunication  
Engineers**

---

**ENGINEERING COMMITTEE  
HFC Management Subcommittee**

---

**AMERICAN NATIONAL STANDARD**

**ANSI/SCTE 95 2009**

**HMS Inside Plant  
HMTS Theory of Operation**

## NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability and ultimately the long term reliability of broadband communication facilities. These documents shall not in any way preclude any member or nonmember of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members, whether used domestically or internationally.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the Standards. Such adopting party assumes all risks associated with adoption of these Standards or Recommended Practices, and accepts full responsibility for any damage and/or claims arising from the adoption of such Standards or Recommended Practices.

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this standard have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2009

140 Philips Road

Exton, PA 19341

# CONTENTS

<b>SCOPE</b> .....	<b>1</b>
<b>COPYRIGHT</b> .....	<b>1</b>
<b>NORMATIVE REFERENCE</b> .....	<b>1</b>
<b>INFORMATIVE REFERENCE</b> .....	<b>1</b>
<b>TERMS AND DEFINITIONS</b> .....	<b>2</b>
<b>1 Introduction</b> .....	<b>3</b>
<b>2 HMTS Overview</b> .....	<b>3</b>
2.1 HMTS Scope .....	4
2.2 HMTS SNMP Support: v1, v2c, or v3 .....	4
<b>3 HMTS Internal Clock Synchronization with External Systems</b> .....	<b>4</b>
<b>4 HMTS Communication Port Support</b> .....	<b>5</b>
4.1 Separation of RX and TX RF ports .....	5
4.2 HMTS support for RF channel definition .....	5
4.3 Optional: Return Path Multicast Addressing.....	5
<b>5 HMS Media Access Control (MAC) Support</b> .....	<b>6</b>
5.1 HMS MAC configuration.....	6
5.2 Hybrid HMS Alarm Discovery Contention Mode .....	6
5.3 Periodic HMS Traffic.....	6
5.4 Broadcast HMS Discovery (REG) Contention Mode .....	6
5.5 Broadcast HMS Alarm Discovery Contention Mode.....	6
5.6 Broadcast HMS Alarm Discovery Contention Mode Operation.....	7
<b>6 External HMS Transponder Addressing</b> .....	<b>7</b>
6.1 IP Address Assignment Methods .....	8
6.2 HMTS Network Address Table.....	8
6.3 Direct IP Address Validation .....	9
6.4 Broadcast/Multicast Addressing .....	9
<b>7 Ethernet Packet Support</b> .....	<b>9</b>
7.1 ICMP Support .....	9
7.2 SNMP over HMS Serial.....	9
<b>8 External SNMP Request Processing</b> .....	<b>10</b>
<b>9 HMTS Event Notifications</b> .....	<b>10</b>
9.1 HMTS Generated Event Notifications .....	10
9.2 HMTS gathering of HMS transponder TRAPS .....	10
9.3 HMTS Forwarding of Event Notifications.....	10
<b>10 HMS Registration Server</b> .....	<b>10</b>
<b>11 HMS Transponder Status-monitoring</b> .....	<b>11</b>
11.1 HMTS Internal Device Table .....	11
11.2 Automatic HMS Transponder Discovery .....	11
11.3 Automatic HMTS Device Table Configuration.....	11
11.4 HMS Transponder Alarm Discovery Methods.....	11
11.5 HMS Transponder Status-monitoring Control .....	12
11.6 Periodic NO-COMMS status checking of HMS transponders .....	12
11.7 HMTS Transponder Return Path Level Alarms .....	12
<b>12 MIBs Supported by the HMTS</b> .....	<b>12</b>
12.1 SCTE 83-3: SCTE-HMS-HMTS-MIB (HMS120).....	12
12.2 SCTE 84-1: SCTE-HMS-HE-COMMON-MIB (HMS111).....	12
12.3 SCTE 38-1: SCTE-HMS-PROPERTY-MIB (HMS026) .....	13

12.4	SCTE 38-11: SCTE-HMS-HEADENDIDENT-MIB (HMS114).....	13
12.5	SCTE 37: SCTE-HMS-ROOTS (HMS072).....	13
12.6	SCTE 36: SCTE-ROOTS (HMS028).....	13
12.7	SNMPv2-MIB (RFC 3418) .....	13
12.8	ENTITY-MIB (RFC 2737).....	13
12.9	SNMP-NOTIFICATION-MIB (RFC 2573).....	13
12.10	SNMP-TARGET-MIB (RFC 2573) .....	13
12.11	SNMP-USER-BASED-SM-MIB (RFC 2574, SNMPv3 only) .....	13
12.12	SNMP-VIEW-BASED-ACM-MIB (RFC 2575, SNMPv3 only).....	13
12.13	SNMP-COMMUNITY-MIB (RFC 2576, SNMPv3 only).....	14

## **SCOPE**

This document contains information about the background of the Hybrid Management Termination System (HMTS). This document is a companion document for the HMTS MIB, and does not replace the MIB. Although this document has been written to be consistent with the HMTS MIB, in case there would be any conflicts between these two documents, the MIB is the reference.

## **COPYRIGHT**

The copyright owner for this document is the SCTE.

## **NORMATIVE REFERENCE**

- 1) IETF RFC 2573 SNMP-NOTIFICATION-MIB.
- 2) IETF RFC 2573 SNMP-TARGET-MIB.
- 3) IETF RFC 2578 SNMPv2-SMI.
- 4) IETF RFC 2579 SNMPv2-TC.
- 5) IETF RFC 2580 SNMPv2-CONF.
- 6) IETF RFC 2737 ENTITY-MIB.
- 7) IETF RFC 3418 SNMPv2-MIB.
- 8) ANSI/SCTE 25-2 200 Hybrid Fiber/Coax Outside Plant Status Monitoring- MAC Layer.
- 9) ANSI/SCTE 36 SCTE-ROOT Management Information Base (MIB) Definitions.
- 10) ANSI/SCTE 37 Hybrid Fiber/Coax Outside Plant Status Monitoring SCTE-HMS-ROOTS Management Information Base (MIB) Definition.
- 11) ANSI/SCTE 38-1 Hybrid Fiber/Coax Outside Plant Status Monitoring SCTE-HMS-PROPERTY-MIB Management Information Base (MIB) Definition.
- 12) ANSI/SCTE 38-11 Hybrid Management Sub-layer Management Information Base (MIB) Part 11: SCTE-HMS-HEADENDIDENT-MIB.
- 13) ANSI/SCTE 84-1 HMS Common Inside Plant Management Information Base (MIB) Part 1: SCTE-HMS-HE-COMMON-MIB.

## **INFORMATIVE REFERENCE**

None.

## TERMS AND DEFINITIONS

This document defines the following terms:

**Management Information Base (MIB)** - the specification of information in a manner that allows standard access through a network management protocol.

**HMTS:** Hybrid Management Termination System.

**HMS:** Hybrid Management System.

**EMS:** Element Management System.

**NO-COMMS:** A condition that exists when the HMTS cannot establish round trip communication with a HMS device.

**XP:** Abbreviation for transponder.

**IP:** Internet Protocol.

**TCP:** Transmission Control Protocol.

**SNMP:** Simple Network Management Protocol.

**ICMP:** Internet Control Message Protocol.

**MAC:** Media Access Control. Basically a data packet definition that provides for end to end transmission of data between two network elements.

**Broadcast Address:** A MAC specific address value that all devices will recognize and process requests to, but not reply to.

**Multicast Address:** A MAC specific address value that can be configured into multiple devices such that a group is created. Use of a multicast address will cause all members of the group to act upon the request, but none of the members will reply. This differs from the broadcast address only in that all devices are pre-configured with the broadcast address.

**Unicast Address:** A MAC specific unique address that is used to identify what device is to process a message and return a reply.

**Round Robin:** A method of processing a list of items which consists of starting with the first entry in the list and walking through the entire list in sequence, wrapping back to the first item in the list.

**Forward Path / Return Path:** bi-directional communication requires a forward (from HMTS to HMS device) and return (from HMS device to HMTS) path (communication connection) regardless of the type of port in use.

## 1 Introduction

A Hybrid Management Termination System (HMTS) provides a gateway from external element managers to the outside plant status-monitoring equipment. The termination system converts Ethernet IP requests from external element managers into requests that can be transmitted over the HMS network. The termination system also converts messages from the HMS network into Ethernet IP messages that can be understood by external element managers.

The following types categorize hybrid management termination systems:

Type 1: An SNMP based termination system that supports the HMTS and standard HMS transponder MIBs, but continues to support only proprietary protocols on the outside plant status-monitoring network.

Type 2: An SNMP based termination system that supports the HMTS and standard HMS transponder MIBs as well as the HMS standards for communication (PHY and MAC) with the transponders. Thus a type 2 HMTS is fully compliant with HMTS and HMS MIBs and HMS PHY and MAC on the RF/serial communication channels. Type 2 HMTS systems may also support Type 1 interfaces so long as they are compatible with the HMS PHY or use dedicated RF channels for non-compatible PHY channels. The HMTS MIB may support proprietary MIBs that extend the functionality defined.

It is important to note that these definitions do not limit any vendor to specific termination system architectures. The HMTS shall be considered a logical representation of one or more physical components.

This document provides a functional overview of the HMTS and is to be read before reviewing the HMTS MIB, which is a separate document.

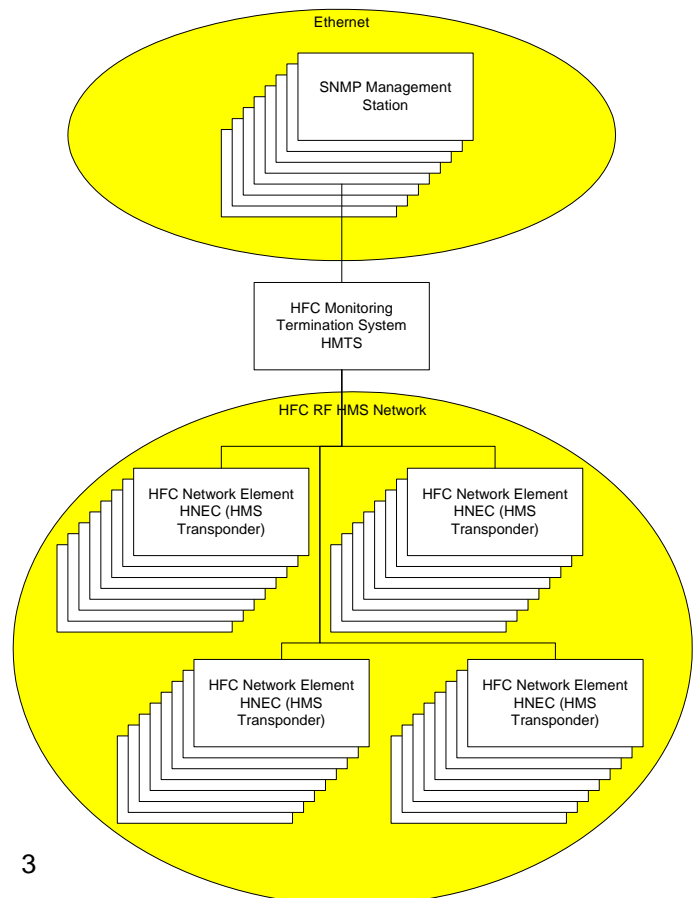
## 2 HMTS Overview

The HMTS is effectively a gateway between the outside plant status-monitoring equipment and a standard Ethernet network. This is the main feature of the HMTS and allows external SNMP based management systems to communicate with HMS transponders using standard SNMP requests. In addition to providing this SNMP gateway, the HMTS also provides these secondary features:

- Retrieval and forwarding of HMS traps generated by monitored transponders.
- Support for periodic broadcasting of HMS time of day and channel definition PDU messages.
- Periodic status monitoring of each HMS transponder.
- HMS Transponder registration server including assignment of IP address.
- Broadcast / multicast SNMP delivery via HMS MAC.

The HMTS shall proxy ICMP support for all transponders with a valid IP address.

Please note that because an HMTS is an SNMP gateway, it supports downloading transponder firmware (via the download MIB).



## 2.1 HMTS Scope

The HMTS is designed to support only those devices that use the HMS MAC to exchange data between the device (transponder) and the termination system. The HMS MAC may be implemented on any type of port defined by the HMTS standard.

## 2.2 HMTS SNMP Support: v1, v2c, or v3

The three SNMP versions that are used most frequently are SNMPv1, SNMPv2c and SNMPv3. While SNMPv1 and SNMPv2c support community strings, SNMPv3 does not but it has an extensive security model.

Although the HMTS MIB is written in the SMIV2 syntax, an HMTS is not required to support SNMPv2c operations and SNMPv2c notifications. An HMTS can use SNMPv1 or SNMPv3 as well, or any combination of SNMPv1, SNMPv2c and SNMPv3. An HMTS e.g. could only support SNMPv1 operations and deliver SNMPv1 traps.

Next to the HMTS SNMP agent itself, there are also the SNMPv1 agents in the transponders. An HMTS can support translation of the SNMPv1 transponder traffic to SNMPv2c or SNMPv3.

Notes:

- If the HMTS agent supports **SNMPv1**, then the agent should support RFC1213-MIB (RFC 1213, a.k.a. MIB-II) instead of SNMPv2-MIB (RFC 3418, only applies to SNMPv2 and SNMPv3).
- If the HMTS is a proxy, and it supports **SNMPv2c** or **SNMPv3**, then the `snmpTargetParamsMPModel` column in the SNMP-TARGET-MIB controls whether transponder traps should be sent unmodified using SNMPv1, or whether these traps should be translated into SNMPv2c or SNMPv3.
- If the HMTS is of the proxy type and if the HMTS supports **SNMPv3**, the addressing information stored in the community string for SNMPv1 or SNMPv2, must now be stored in the context field of an SNMPv3 PDU. If the SNMP-PROXY-MIB is implemented on an HMTS, it should be kept consistent with the information in the device table. See also RFC 2273 for more information.
- When the HMTS agent supports **SNMPv3**, then three additional MIBs should be supported: the SNMP-VIEW-BASED-ACM-MIB (RFC 2265), the SNMP-USER-BASED-SM-MIB (RFC 2574) and the SNMP-COMMUNITY-MIB. The SNMP-COMMUNITY-MIB is defined in RFC 2576, titled *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.

Examples of possible HMTS implementations are:

- The HMTS agent supports SNMPv1, and all communication to transponders happens in SNMPv1.
- The HMTS is a proxy, its agent supports SNMPv2c, and translates all transponder communication between SNMPv1 and SNMPv2c.
- The HMTS is a gateway, its agent supports SNMPv2c, and all communication to transponders happens in SNMPv1.
- The HMTS is a gateway, its agent supports SNMPv3, and transponder communication happens in SNMPv1.
- The HMTS is a gateway, its agent supports SNMPv3, and translates all transponder operations between SNMPv1 and SNMPv3.
- The HMTS is a proxy, its agent supports SNMPv3, and translates all transponder operations between SNMPv1 and SNMPv3.

## 3 HMTS Internal Clock Synchronization with External Systems

The HMTS must periodically set the time of day in all HMS transponders. This is done to ensure that SNMP traps are generated with the correct timestamp. For this to be of use, the HMTS will support setting of its own internal clock through an SNMP MIB and will optionally support time sync through use of a network timeserver.

## 4 HMTS Communication Port Support

By definition in the HMTS MIB, there can be three types of ports supported by the HMTS. Support for more than one of the following serial ports is not a requirement of the HMTS standard. These port types are:

- RF port: supported using the HMS physical standard (SCTE 25-1).
- RS-485 port: supported using the physical standard recommended by HMS070.
- RS-232 port: supported using the physical standard recommended by HMS070.

### 4.1 Separation of RX and TX RF ports

The design of the HMTS MIB is one where the operations of the transmitter and ports are considered independent of each other. This does not mean that the HMTS must physically have separate transmitter and receiver cards, only that they be treated as separate MIB entities with the ability to associate one or more receivers with a single transmitter. RF and RS-485 ports both share a common port definition through use of a media type flag. There is no restriction on the use of return path switches on RF receivers except that each return path port must then appear as a separate RF receiver in the receiver port table. The naming convention used for each port must be able to handle the use of this switch. The HMTS MIB does not limit the number of receivers or transmitters in any vendor implementation.

An important aspect of the separation of receiver and transmitter is that the receiver should be able to properly respond to a HMS TALKRQST regardless of when it is received. This modeless operation allows for a looser implementation of the HMS contention mode, allowing a HMTS to catch requests that may be slightly out of sync with the clock of the HMTS.

### 4.2 HMTS support for RF channel definition

The HMTS allows the user to define RF forward and return path channels. This is done using one return path frequency value per RF receiver and two forward path frequency values per RF transmitter. Two forward path frequencies are necessary, as the HMTS needs to be able to command transponders to switch frequencies while still being tuned to the old forward path frequency. The HMTS provides the user with two methods to control how forward channel switching occurs. The first is the manual method, in which the external management system will take control of setting both the transponder forward channel and the HMTS forward channel values separately<sup>1</sup>. The second automatic method is optional, but places control of switching the HMTS forward channel under control of the HMTS whenever the transponder forward channel definition is changed. Exactly how this automatic method is implemented will be left up to each vendor. The end result will be that when the user sets the transponder forward channel value, the HMTS will take actions to cause the transponders to switch to the new channel definition and then finally cause the HMTS forward channel value to be changed to the new value.

Recommended actions:

Whenever the forward port transponder frequency is changed, the HMTS should immediately send the HMS channel definition PDU multiple times while obeying the HMS MAC broadcast delay limitation.

The HMTS must be aware that since each transmitter can have more than one receiver. Each receiver may also have it's own return path frequency. Thus multiple HMS channel definition PDU messages may need to be sent (one for each unique return path frequency) whenever the forward path frequency is changed.

### 4.3 Optional: Return Path Multicast Addressing

The broadcast/multicast table can be used to define a multicast address that is to be associated with all HMS transponders on a single return path. This return path feature provides a method of addressing a specific subgroup of transponders based upon the return path they are attached to. It is the responsibility of the HMTS to ensure that each transponder's common MIB be updated (during the registration process) to reflect the multicast address assigned to a return path. Note: this is an optional HMTS feature - an HMTS that implements the HMTS MIB is not required to implement also return path multicast addressing.

---

<sup>1</sup> It is important that any forward channel frequency change be completed within the time frame that the target transponders are expecting to see the HMS channel definition PDU. Failure to have caused the HMTS to change to the new forward channel within this time can end up with transponders going into a channel search mode.

## **5 HMS Media Access Control (MAC) Support**

The HMTS is the single point of access for HMS MAC networks and the design of the HMS MAC allows the user to perform some tuning to optimize its operation within a specific installation. All communication between the HMTS and any HMS network device must use the HMS MAC regardless of the type of port in use. The HMS MAC also defines the methods used to send SNMP/IP requests to HMS devices and how asynchronous messages (TRAPS) are to be discovered and retrieved by the HMTS.

### **5.1 HMS MAC configuration**

SCTE 25-2 (formerly HMS004) defines the MAC that is used for all transport level communication to the HMS transponder. But SCTE 25-2 also defines values for timeouts and fallback calculations that must be observed by both the transponder and the HMTS. The HMTS MIB provides the user with the ability to tune how the HMTS will use the HMS MAC interface.

### **5.2 Hybrid HMS Alarm Discovery Contention Mode**

Hybrid HMS alarm discovery contention mode is basically a way to break HMS contention mode up into smaller groups of transponders and then periodically checking each group of transponders for alarms using multicast addresses. HMS broadcast contention mode starts to run into collision problems as the number of devices trying to talk increase in size. This hybrid contention mode allows the user to break a large network into smaller groups and provide control over the sequence that the various groups are checked. Hybrid contention mode is a table of multicast MAC addresses that are to be checked on a regular basis. These contention groups can overlap or can be chained or even mixed. Each chain is treated as a round robin action list with no limitation as to how many times a multicast address appears in the group. Each entry in the table can use a different mode of continuity and duration from each of the other entries. Thus it is possible to create a very flexible schedule of contention periods that can be tailored to the specifics of each multicast address group. Want to create a group that is always in contention mode with continuous continuity? This can be done for those devices that rarely report an alarm (like a fire monitor) while still ensuring that the trap is quickly discovered. Meanwhile other multicast groups can be checked using other parameters.

### **5.3 Periodic HMS Traffic**

The HMS MAC document defines two types of messages that must be broadcast on a periodic basis. The first of these is the channel definition PDU that is used to tell all HMS transponder what the frequencies of the forward and return paths are. The second periodic housekeeping message is used to set the time of day, which in itself means that the HMTS must have a method of keeping it's own internal clock in synchronization with the external system. The HMTS must support both of these periodic housekeeping tasks.

### **5.4 Broadcast HMS Discovery (REG) Contention Mode**

Discovery of HMS transponders using HMS contention mode is an optional feature of a HMTS, and can only use the HMS broadcast MAC address to perform this function. The user is provided with control over how registration contention mode will function.

### **5.5 Broadcast HMS Alarm Discovery Contention Mode**

HMS contention mode is an optional feature of the HMTS. When implemented the HMTS is the master of the HMS contention mode. It controls what devices are placed into contention and how long each contention mode lasts. The user has a set of contention mode parameters that provide control of how the HMTS performs this function. By default the HMTS provides the capability to control global contention mode operations though the use of the HMS broadcast MAC address.

## 5.6 Broadcast HMS Alarm Discovery Contention Mode Operation

The `hmtsOperatingMode` parameter provides the ability to define how the HMTS will handle TALK\_REQ messages discovered during the contention period. Once contention mode is enabled the user can also specify how the HMTS will handle HMS NE SNMP requests while contention mode is turned on. The following `hmtsTrapContinuity` settings are available<sup>2</sup>:

- **Immediate:** This setting will cause the HMTS to cancel the contention operating mode (by sending a CONTMODE=OFF PDU) so that the new SNMP request can be handled quickly without concern for collisions that may occur in the *continuous* mode below. This mode does effect the discovery of alarms from the transponders as the contention period is cut short.
- **Queued:** This setting will cause the new SNMP request to be postponed until the current contention-operating mode has expired. This ensures that the request will be handled without concern for collisions that may occur in the *continuous* mode below, but will delay the SNMP request for some time period. While this mode does not change the alarm discovery process, it may cause SNMP requests to be retried by external SNMP management systems.
- **Continuous:** This setting will cause the SNMP trap retrieval request to be sent while the contention mode of operation is still active. This mode of operation can suffer from return path collisions should the response to the SNMP request be transmitted at the same time that one or more transponders decide to send a TALK\_REQ PDU. The HMTS will have to handle retransmission of these SNMP requests due to timeout (possibly caused by a collision). This mode of contention operation allows the quick processing of new SNMP requests while allowing the normal alarm discovery time period to continue, but at the expense of possible collisions. This collision overhead may or may not be less than the overhead of the other modes outlined above.

## 6 External HMS Transponder Addressing

The HMTS supports at least one of two methods of external<sup>3</sup> HMS transponder addressing. A HMTS may support one or both of the following methods.

**Direct IP addressing.** This addressing method assigns a standard IP address to each HMS transponder. This allows external SNMP management systems to view the HMTS as a simple gateway between two different networks. In this mode of operation, the HMTS must monitor Ethernet traffic for any active HMS transponder's IP address and route the SNMP request onto the RF network wrapped in a HMS MAC. Use of Direct IP addressing also means that the HMTS must support pinging of the transponder address.

**Community String Proxy Addressing.** This addressing method requires that all SNMP requests contain the IP address of the HMTS, and that the community string of that SNMP request contains the unique name for the HMS transponder that the request is to be forwarded to. The suggested unique name of each transponder is the unique HMS MAC address of each transponder. But the HMTS MIB does not restrict the user to this value. To support this mode of addressing, the HMTS must use the internal device table to look up the unique name contained in the community string of the SNMP request. When that unique name has been found, the HMTS will forward the request out onto the HMS RF network using the HMS MAC address associated with that community string unique name.

These address methods allow external systems to refer to HMS transponders using an address scheme other than the MAC address used by the HMTS to communicate over the serial HMS MAC channel. The HMTS must intercept messages for a transponder (sent to the external address), locate the transponder's MAC address, and then encapsulate requests with a HMS MAC for forwarding to the transponder. The HMTS MIB provides IP and/or Community String lookup tables that provide for translation between either of the external address methods to the internal HMS MAC address used by the HMTS. If a transponder appears in either of these tables then it can be addressed using that external addressing scheme and thus available for use by external systems.

---

<sup>2</sup> Note: Support for all the various `hmtsTrapContinuity` settings are optional. The HMTS vendor need only implement at least one of the settings.

<sup>3</sup> The only way to address any HMS MAC device is through the use of its unique MAC address. Direct IP and SNMP community string proxy addressing is provided to allow external systems to send requests to the HMS transponder using SNMP based requests. SNMP community string proxy addressing is not support for non-SNMP IP requests.

## 6.1 IP Address Assignment Methods

The HMTS will support at least one of the following four IP address assignment methods if the HMTS supports Direct IP Addressing. These methods are:

- **Manual XP:** Use the IP address that the transponder is already configured with. This IP address is discovered when the transponder sends a HMS REG\_REQ PDU in response to a HMS TALK PDU. If this IP address is valid (contained in the `hmtsNetAddrTable`) and not a duplicate of an existing device table entry, then the device will be made active and may be used by external systems<sup>4</sup>. If the device supplied IP address is invalid or duplicate of an existing device table entry the device communication status will reflect an error and the device will not be addressable by an external system. The user must manually edit the device table entry for the device to correct the error, which will also cause the external address in the device to be changed<sup>5</sup>.
- **Manual HMTS** or manual IP address assignment: This method causes the device to be entered into the device table automatically upon discovery, but will not have an IP address assigned until the user changes the device table entry manually. The IP address assigned by the user must be valid (contained in the `hmtsNetAddrTable`). Changing the device `hmtsDevIPAddr` will cause the HMTS to update the `commonNetworkAddress` value in the device and make the device available for use by external systems.
- **Automatic:** The user manually defines the `hmtsNetAddrTable` through the HMTS MIB. This table provides a list of available IP address ranges that the HMTS can assign to transponders. During HMS contention mode registration, any new transponder discovered will first have its current `commonNetworkAddress` (supplied in the HMS REG\_REQ PDU) checked against the IP address table. If that address is contained in that table and not already in use, then the address supplied by the transponder will be used. If the address is not in the table, or is already in use by another transponder, then the HMTS will allocate an IP address from the table and assign it to the new transponder during the registration process. Once the IP address is assigned, the device can be used by external systems.
- **DHCP Proxy Client:** This method causes the HMTS to act as a DHCP proxy for each transponder in the device table. Thus new transponders are assigned an IP address by the HMTS asking the DHCP server to assign an address for the HMS NE MAC address. The HMTS must also ensure that all IP address leases are renewed when the lease period is one half expired. So long as the device has an IP address assigned by the DHCP server, that device will be available for use by external systems. *NOTE: in this mode of operation, the contents of the `hmtsNetAddrTable` are ignored.*

## 6.2 HMTS Network Address Table

The HMTS has to know something about the configuration of the network that it works within in order to provide the gateway functionality that is its core purpose. How much information is needed depends upon the method used to assign IP address values to transponders (assuming that Direct IP addressing is used). In all modes of IP address assignment except for *client*, this network address table (`hmtsNetAddrTable`) must be configured before the first IP address can be assigned to any transponder. In *client* IP address assignment mode, the HMTS shall maintain this table for the user using the IP address assignments provided by the DHCP server.

---

<sup>4</sup> [If the IP on the transponder was valid then the Record should become active. Otherwise the Manager can not talk to the Device.](#)

<sup>5</sup> The HMTS is considered the owner of the `commonNetworkAddress` value in the transponder. If the HMTS device table for a device has its `hmtsDevIPAddr` changed to a valid address, then the HMTS is responsible for ensuring that the IP address contained in transponder traps contains the proper IP address. The easiest way for this to occur is for the HMTS to change the `commonNetworkAddress` in the transponder to reflect the current value of `hmtsDevIPAddr` in the device table.

### 6.3 Direct IP Address Validation

The `hmtsNetAddrTable` contains a list of all IP address values that the HMTS shall consider valid for HMS transponders under its control. In general, this table is used to validate that any IP address assigned to a transponder is valid (must exist in one of the table entries). Whenever an entry in this table is added/changed, the contents of the HMTS device table will be checked to ensure that the current IP values are still valid. If no, then the device communication status will be changed to *invIP*, and a trap will be generated.

In *Automatic* address assignment mode, the `hmtsNetAddrTable` is also used to determine the next available IP address that can be assigned to a newly discovered transponder.

Recommended Action: In Automatic address assignment mode, the HMTS should reset any device that has had its previous IP address become invalid. This will cause the transponder to restart the registration process and be assigned a new IP address.

### 6.4 Broadcast/Multicast Addressing

Regardless of the type of transponder addressing supported (Direct IP or SNMP Community String Proxy) the HMTS must support the ability for a SNMP command to be addressed to a HMS broadcast or multicast address. This broadcast/multicast address table defines what HMS MAC address is to be associated with an IP address or unique SNMP community string. It is the responsibility of an external system to set up the multicast address tables in each transponder for general multicast address values.

## 7 Ethernet Packet Support

The HMTS provides a gateway between external element management systems attached to the Ethernet network and the HMS transponders attached to the HMS network.

### 7.1 ICMP Support

Since the HMS transponders are not true IP devices, they do not have support for the ICMP protocol. Yet ICMP is an important tool in many external management systems. Thus the HMTS must provide an ICMP proxy for all transponders that currently have an IP address assigned and do not have a communication error currently active.

### 7.2 SNMP over HMS Serial

The HMS MAC was designed to encapsulate the SNMP request without including the IP control information. Thus all SNMP traffic to any transponder will be sent to the transponder using the HMS MAC “SNMP over serial” protocol. Responses to the SNMP request will be returned using the same HMS MAC “SNMP over serial” protocol bit. The SNMP response will be extracted from the HMS MAC message and return to the originator of the SNMP request.

SNMP message traffic between a transponder and external Ethernet systems is bi-directional, but the HMS MAC “SNMP over serial” protocol was designed only to support SNMP transfer between the HMTS and transponder<sup>6</sup>. The HMTS is capable of routing external SNMP requests to a target transponder, and then routing the SNMP response from that transponder back to the originator of the SNMP request. But the HMTS cannot perform this routing in the other direction. Thus using the “SNMP over serial” protocol bit does not allow a transponder to issue SNMP requests to external systems.

---

<sup>6</sup> The HMS MAC allows transfer between two points in a multipoint slave/master network. There is no destination address on data sent from the transponder to the HMTS as the HMTS is the only destination.

## 8 External SNMP Request Processing

When a request is received from an external system for delivery to a transponder, the HMTS will need to merge that request into the normal status-monitoring functions that it is performing. Normally the HMTS will simply send the external request as soon as the return path for the addressed transponder is clear. But HMS contention mode (both alarm discovery and registration) will effect how the HMTS handles the external request. The HMTS must include at least one of the following (support for more than one selection is optional) configuration options:

- **Immediate:** If an external request is received while in contention mode, the HMTS will leave the contention mode active and send the request to the target transponder. This may result in a return path collision that must be properly handled.
- **Queued:** If an external request is received while in contention mode, the HMTS will queue that request until the current contention mode period expires.
- **Interrupt:** If an external request is received while in contention mode, the HMTS will immediately cancel the contention mode and then send the request to the target transponder.

## 9 HMTS Event Notifications

Since the HMTS is the gateway between the HMS network and the Ethernet network, it must provide the ability to forward events from transponders to Ethernet based systems. In addition, those events generated by the HMTS itself must also be forwarded to these external Ethernet based systems.

### 9.1 HMTS Generated Event Notifications

The HMTS is a SNMP managed device that is capable of generating SNMP notifications for issues that are specific to the operation of the HMTS system and for issues specific to HMS NE devices that are being monitored by the HMTS (NO-COMMS and return signal level events). These notifications are:

- Alarms that are discovered by the HMTS are maintained in the HMTS currentAlarmTable (as defined in SCTE 38-1 (formerly known as HMS026)). Entries into this table are reported using a heCommonAlarmEvent (as defined in SCTE 84-1 (formerly known as HMS111)).
- The SNMPv2-MIB notifications coldStart, warmStart, linkUp, linkDown<sup>7</sup>, authenticationFailure and egpNeighborLoss<sup>8</sup> are to be supported by HMTS. Note: since EGP support is only required for systems that implement EGP, an egpNeighborLoss trap should only be sent if EGP is implemented by the HMTS.
- Changes to ENTITY MIB entries are handled with a entConfigChange notification.
- The events generated by the HMTS shall be forwarded to external Ethernet based systems.

### 9.2 HMTS gathering of HMS transponder TRAPS

The HMTS provides the ability to gather traps from the HMS transponders that it is in communication with. The HMTS shall provide the ability to forward these traps to external Ethernet based systems.

### 9.3 HMTS Forwarding of Event Notifications

The HMTS supports forwarding of event notifications through the use of the SNMP-NOTIFICATION-MIB and the SNMP-TARGET-MIB. This allows an external system to register to receive notifications that are generated by the HMTS or by the HMS transponders. The HMTS is not required to support the filtering capability of the SNMP-NOTIFICATION-MIB.

## 10 HMS Registration Server

While the HMTS is required to automatically discover HMS transponders on the HMS network, it is not required to automatically register what is found. Automatic registration is dependent upon the external address method used. So long as the HMTS can select a proper external address, it can automatically register a new device. A HMS transponder will not report alarms until it is properly registered.

---

<sup>7</sup> linkUp and linkDown are defined in RFC 1573.

<sup>8</sup> egpNeighborLoss is defined in RFC 1213.

## **11 HMS Transponder Status-monitoring**

Not to be confused with forwarding of HMS Transponder traps, this function requires that the HMTS periodically test the communication between itself and each HMS transponder and when necessary generate HMTS SNMP traps on behalf of any transponder that can not be communicated with. Optionally HMTS systems may be able to monitor the return path signal level that is being received during a reply from each HMS transponders. In this case, the HMTS will generate SNMP traps when the signal level is not nominal. Status-monitoring also controls the retrieval of HMS transponder generated traps for delivery to external Ethernet based systems.

### **11.1HMTS Internal Device Table**

In order to support the periodic status checking of HMS transponders, the HMTS maintains a device table that is indexed by the HMS MAC address of each HMS NE. This device table is also needed for both direct IP and SNMP community string proxy addressing. The device table also allows the HMTS to provide optional management counters that can be used by external SNMP management systems to track the performance of their HMS transponders. Parts of the device table are non-volatile so that the HMTS will remember the configuration between power sessions. The device table is under the direct control of the HMTS (this allows the HMTS to provide automatic device discovery) and can be managed by external management systems through SNMP requests that are addressed to the HMTS itself.

While the HMTS is expected to discover all new HMS transponders, and automatically create device table entries, it is also possible for the user to manually create/edit/delete device table entries.

Recommended Action: If a transponder is deleted from the device table, the HMTS should cause that device to be reset so that it will go back through the registration process. This may cause the device to be re-discovered and thus added back into the device table, but it also ensures that we do not have registered transponders in the network that do not appear in the HMTS device table.

### **11.2Automatic HMS Transponder Discovery**

An HMTS is required to automatically discover HMS transponders. The vendor is not required to support the HMS contention mode in order to support this capability, through the use of the HMS registration contention mode is one possible way to perform this function.

### **11.3Automatic HMTS Device Table Configuration**

When a HMTS that discovers a previously unknown transponder (it's MAC address does not exist in the HMTS device table), the HMTS will automatically create a new device table entry. The new device will be marked as *active* so long as the device meets the requirements detailed in the HMTS MIB. Even though the device is active in the HMTS device table, this does not mean that an external system can communicate with the device, it does mean that the HMTS can communicate with the device. In order for an external system to be able to communicate with the device, an external address must have been assigned to the device.

### **11.4HMS Transponder Alarm Discovery Methods**

The HMS MAC specification defines two methods of alarm discovery. The HMTS is required to support at least one of the following methods:

**Polling.** This consists of active communication with each transponder on a cyclic basis to check for the existence of alarms that need to be retrieved. Due to the cyclic nature of polling, the time it takes to gather all alarms from all devices depends upon the number of devices that must be polled and the frequency of alarm generation on each of these devices. The number of external management system requests being processed also directly affects alarm gathering. In polling mode, all communication must be originated by the HMTS.

Contention Mode. Contention mode changes the master/slave relationship between the HMTS and the HMS transponders. Rather than cyclic polling of each device, the HMTS commands a group (through the use of MAC broadcast or multicast addresses) of HMS transponders to enter contention mode for some period of time. During this time period, the HMTS becomes the slave looking for talk requests from any of the transponders in contention mode. In this mode, return path collisions will occur; as it is possible that more than one transponder will have an alarm to be reported. The HMS MAC specifies how the HMTS and HMS transponders will handle this condition. During contention mode, any transponder placed into that mode with an alarm to report will issue a request to the HMTS asking that the alarm be retrieved. The user is presented with various options on how to handle the interaction between the HMTS and HMS transponder in the handling of these requests to retrieve alarms. Like polling, contention mode is interrupted by external management requests. But unlike polling, contention mode does not have to talk to those transponders that do not have alarms to report. But contention mode does suffer when the number of devices placed into contention mode (with alarms) causes a high probability of return path collisions. The HMTS provides methods to control not only the parameters that control how HMS transponders operate in contention mode, but also how to group transponders that are placed into contention mode.

### **11.5 HMS Transponder Status-monitoring Control**

The user can turn off the transponder status-monitoring functionality of the HMTS. This effectively disables unicast communication between the HMTS and all transponders. This does not disable the periodic time of day of channel description messages that the HMTS must normally broadcast to all transponders<sup>9</sup>.

### **11.6 Periodic NO-COMMS status checking of HMS transponders**

A secondary function of the HMTS is to provide periodic NO-COMMS status checking. If the HMTS is configured to gather alarms from transponders through active polling, this NO-COMMS condition will be discovered due to the cyclic communication with each device. If the HMTS is configured to gather alarms through the use of HMS contention mode, discovery of a NO-COMMS condition requires that the HMTS periodically communicate with each device (essentially a infrequent polling function) that it has not had recent communication with. The issue is that in contention mode, a device that does not generate alarms will not normally communicate with the HMTS. Thus the HMTS must periodically poll devices with no alarms to determine if their communication channel is still operational. The user is provided with control as to how frequently this NO-COMMS checking will occur.

### **11.7 HMTS Transponder Return Path Level Alarms**

An optional feature of the HMTS is the ability to monitor the return path signal level from each transponder. The user is able to set limits that will generate alarms when the level is too low or too high. This trap will identify the transponder that generated the alarm as well as the receiver port that the transponder is attached to.

## **12 MIBs Supported by the HMTS**

### **12.1 SCTE 83-3: SCTE-HMS-HMTS-MIB (HMS120)**

This MIB is known as the HMTS MIB. The HMTS requires that the standard MIBs listed below are also be supported.

### **12.2 SCTE 84-1: SCTE-HMS-HE-COMMON-MIB (HMS111)**

The HMTS is a head end device and as such is expected to support the SCTE-HMS-HE-COMMON-MIB. This MIB pulls in support for analog properties, discrete properties, and the current alarm table from SCTE-HMS-PROPERTY-MIB (SCTE 38-1 or HMS026). In addition, the SCTE-HMS-HE-COMMON-MIB also requires support of the ENTITY-MIB (RFC 2737). This MIB also pulls in support for the ENTITY-MIB, SNMP-NOTIFICATION-MIB and the SNMPv2-MIB.

---

<sup>9</sup> Disabling the broadcast of the HMS MAC channel definition PDU can cause some HMS transponders to go into a channel search pattern.

### **12.3 SCTE 38-1: SCTE-HMS-PROPERTY-MIB (HMS026)**

A HMTS is required to support the analogAlarmsGroup, discreteAlarmsGroup and currentAlarmsGroup groups of this MIB. These groups are used to support the configuration and generation of events within the HMTS.

### **12.4 SCTE 38-11: SCTE-HMS-HEADENDIDENT-MIB (HMS114)**

This MIB defines the branches of the HMS Headend Equipment MIBs.

### **12.5 SCTE 37: SCTE-HMS-ROOTS (HMS072)**

This MIB defines the branches HMS Subcommittee defined MIBs.

### **12.6 SCTE 36: SCTE-ROOTS (HMS028)**

This MIB defines the branches of the SCTE Subcommittees.

### **12.7 SNMPv2-MIB (RFC 3418)**

A HMTS is required to support the systemGroup group of the SNMPv2 MIB which provides identification of the HMTS as well as what MIBs are currently active on the HMTS. This MIB also defines coldStart and authenticationFailure notifications. Support of this MIB does not require the HMTS to be a SNMPv2 device. Support for this MIB calls in the following additional MIBs: SNMPv2-SMI (RFC 2578), SNMPv2-TC (RFC 2579), and SNMPv2-CONF (RFC 2580).

### **12.8 ENTITY-MIB (RFC 2737)**

At this time, the HMTS will appear as a single entry in the ENTITY-MIB. The entityPhysicalGroup, entityPhysical2Group, entityGeneralGroup and entityNotificationsGroup shall be supported to be HMTS compliant. A future version of the MIB may support sub-definitions for the communication channels but that is not currently planned.

### **12.9 SNMP-NOTIFICATION-MIB (RFC 2573)**

The standard method for external systems to request to receive traps/notifications is through the use of the SNMP-NOTIFICATION-MIB. The snmpNotifyGroup group of this MIB shall be supported to be HMTS compliant.

### **12.10 SNMP-TARGET-MIB (RFC 2573)**

The HMTS provides the ability forward traps/notifications to external systems through the use of the SNMP-NOTIFY-MIB, which requires that the HMTS also support the snmpTargetBasicGroup group of the SNMP-TARGET-MIB.

### **12.11 SNMP-USER-BASED-SM-MIB (RFC 2574, SNMPv3 only)**

RFC 2574 defines the User-based Security Model (USM), providing for both Authenticated and Private (encrypted) SNMP messages. This MIB only applies to SNMPv3.

### **12.12 SNMP-VIEW-BASED-ACM-MIB (RFC 2575, SNMPv3 only)**

RFC 2575 defines the View-based Access Control Model (VACM), providing the ability to limit access to different MIB objects on a per-user basis. This MIB only applies to SNMPv3.

### **12.13 SNMP-COMMUNITY-MIB (RFC 2576, SNMPv3 only)**

RFC 2576, titled Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework. This MIB provides the following functionality:

- snmpCommunityTable allows to configure how to translate a SNMPv1/SNMPv2c community string to SNMPv3 security information.
- snmpTargetAddrExtTable allows configuration of a maximum SNMP message size per notification target.

In case the HMTS translates SNMP PDU's, SNMP traps and/or SNMP notifications between SNMP versions, it is highly recommended that this MIB is implemented on the HMTS.