BRITISH STANDARD

BS EN
60728-7-2:2005

Cable networks for television signals, sound signals and interactive services —

Part 7-2: Hybrid Fibre Coax Outside Plant Status Monitoring — Media access Control (MAC) Layer Specification

The European Standard EN 60728-7-2:2005 has the status of a British Standard

ICS 35.100.60; 33.160; 33.040

BSI
British Standards

National foreword

This British Standard is the official English language version of EN 60728-7-2:2005. It is identical with IEC 60728-7-2:2003.

The UK participation in its preparation was entrusted to Technical Committee EPL/100, Audio, video and multimedia systems and equipment, which has the responsibility to:

— aid enquirers to understand the text;

— present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;

— monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled "International Standards Correspondence Index", or by using the "Search" facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 45 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 22 March 2005

ISBN 0 580 45597 1

EUROPEAN STANDARD **EN 60728-7-2**

NORME EUROPÉENNE

EUROPÄISCHE NORM February 2005

ICS 35.100.60; 33.160; 33.040

English version

Cable networks for television signals, sound signals and interactive services Part 7-2: Hybrid Fibre Coax Outside Plant Status Monitoring – Media access Control (MAC) Layer Specification

(IEC 60728-7-2:2003)

Réseaux de distribution par câbles pour signaux de télévision, signaux de radiodiffusion sonore et services interactifs
Partie 7-2: Surveillance de l'état des installations extérieures des réseaux hybrides à fibre optique et câble coaxial - Spécification de la couche du contrôle d'accès au support
(CEI 60728-7-2:2003)

Kabelnetze für Fernsehsignale, Tonsignale und interaktive Dienste
Teil 7-2: Zustandsüberwachung Hybrid-Faser-Koax-Netze (HFC) – Festlegung Steuerungsschicht für Mediumzugriff (MAC)
(IEC 60728-7-2:2003)

This European Standard was approved by CENELEC on 2004-12-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in one official version (English). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 60728-7-2:2004 E

Foreword

The text of the International Standard IEC 60728-7-2:2003, prepared by technical area 5: Cable networks for television signals, sound signals and interactive services, of IEC TC 100, Audio, video and multimedia systems and equipment, was submitted to the formal vote and was approved by CENELEC as EN 60728-7-2 on 2004-12-01 without any modification.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop) 2005-12-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow) 2007-12-01

_____

Endorsement notice

The text of the International Standard IEC 60728-7-2:2003 was approved by CENELEC as a European Standard without any modification.

_____

CONTENTS

INTRODUCTION

Standards of the IEC 60728 series deal with cable networks for television signals, sound signals and interactive services including equipment, systems and installations for

- head-end reception, processing and distribution of television and sound signals and their associated data signals, and
- processing, interfacing and transmitting all kinds of signals for interactive services

using all applicable transmission media.

All kinds of networks like

- CATV-networks,
- MATV-networks and SMATV-networks,
- individual receiving networks,

and all kinds of equipment, systems and installations installed in such networks, are within this scope.

The extent of this standardization work is from the antennas, special signal source inputs to the head-end or other interface points to the network up to the system outlet or the terminal input, where no system outlet exists.

The standardization of any user terminals (i.e. tuners, receivers, decoders, multimedia terminals, etc.) as well as any coaxial and optical cables and accessories therefore is excluded.

CABLE NETWORKS FOR TELEVISION SIGNALS, SOUND SIGNALS AND INTERACTIVE SERVICES –

Part 7-2: Hybrid Fibre Coax Outside Plant status monitoring – Media Access Control (MAC) layer specification

1 Scope

This part of IEC 60728 specifies requirements for The Hybrid Fibre Coax (HFC) Outside Plant (OSP) Media Access Control (MAC) Layer. This standard is part of the series developed to support the design and implementation of interoperable management systems for evolving HFC cable networks. The HMS Media Access Control (MAC) layer specification describes the messaging and protocols implemented at the Data Link Layer (DLL), layer 2 in the 7 layer ISO-OSI reference model, that support reliable and efficient communications between HMS compliant transponders interfacing to managed OSP network elements (NEs) and a centralized head-end element (HE).

This standard describes the MAC layer protocols that must be implemented between all *Type 2* and *Type 3* compliant OSP transponders on the HFC plant and the controlling equipment in the head-end to support bandwidth management and reliable communications. Any exceptions to compliance with this standard will be specifically noted herein as necessary. Refer to Table 1 for a full definition of the type classifications.

Transponder type classifications referenced within the HMS series of standards are defined in Table 1.

Table 1 – Transponder type classifications

Type	Description	Application
Type 0	Refers to legacy transponder equipment, which is incapable of supporting the specifications	This transponder interfaces with legacy network equipment through proprietary means. This transponder could be managed through the same management applications as the other types through proxies or other means at the head-end.
Type 1	Refers to stand-alone transponder equipment (legacy or new), which can be upgraded to support the specifications	This transponder interfaces with legacy network equipment through proprietary means. Type 1 is a standards-compliant transponder (either manufactured to the standard or upgraded) that connects to legacy network equipment via a proprietary interface.
Type 2	Refers to a stand-alone, compliant transponder	This transponder interfaces with network equipment designed to support the electrical and physical specifications defined in the standards. It can be factory or field-installed. Its RF connection is independent of the monitored NE.
Type 3	Refers to a stand-alone or embedded, compliant transponder.	This transponder interfaces with network equipment designed to support the electrical specifications defined in the standards. It may or may not support the physical specifications defined in the standards. It can be factory-installed. It may or may not be field-installed. Its RF connection is through the monitored NE.

2 Normative references

None.

3 Terms, definitions and abbreviations

For the purposes of this document, the following definitions apply.

3.1 Terms and definitions

3.2
data link layer (DLL)
layer 2 in the Open System Interconnection (OSI) architecture; the layer that provides services to transfer data over the physical transmission link between open systems

3.3
forward spectrum
pass band of frequencies in HFC cable systems with a lower edge of between 48 MHz and 87,5 MHz, depending on the particular geographical area, and an upper edge that is typically in the range of 300 MHz to 860 MHz depending on implementation

3.4
full spectrum
combined forward and return spectrums in HFC cable systems and excludes any guard band

3.5
guard band
unused frequency band between the upper edge of the usable return spectrum and the lower edge of the usable forward spectrum in HFC cable systems

3.6
network element (NE)
active element in the outside plant (OSP) that is capable of receiving commands from a head-end element (HE) in the head-end and, as necessary, providing status information and alarms back to the HE

3.7
open system interconnection (OSI)
a framework of the International Organization for Standardization (ISO) standards for communication between multi-vendor systems that organizes the communication process into seven different categories that are placed in a layered sequence based on the relationship to the user. Each layer uses the layer immediately below it and provides services to the layer above. Layers 7 through 4 deal with end-to-end communication between the message source and destination, and layers 3 through 1 deal with network functions

3.8
organizationally unique identifier (OUI)
a 3-octet IEEE assigned identifier that can be used to generate universal LAN MAC addresses and protocol identifiers per ANSI/IEEE standard 802 for use in local and metropolitan area network applications

3.9
physical (PHY) layer
layer 1 in the open system interconnection (OSI) architecture; the layer that provides services to transmit bits or groups of bits over a transmission link between open systems and which entails electrical, mechanical and handshaking procedures

3.10
return spectrum
pass band of frequencies in HFC cable systems with a lower edge of 5 MHz and an upper edge that is typically in the range of 42 MHz to 65 MHz depending on the particular geographical area

3.11
transponder
device that interfaces to outside plant (OSP) NEs and relays status and alarm information to the HE. It can interface with an active NE via an arrangement of parallel analogue, parallel digital and serial ports

3.12 Abbreviated terms

CCITT	Comité Consultatif International de Télégraphie et Téléphonie (ITU – International Telecommunication Union)
CRC	Cyclic Redundancy Code
DLL	Data Link Layer
EMS	Element Management System
FCS	Frame Check Sequence
HE	Head-end Element
HEX	Hexadecimal
HFC	Hybrid Fibre Coax
HMS	Hybrid Management Sub-Layer (defined in the standard)
I/G	Individual / group address bit
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
LSB	Least Significant Bit
MAC	Media Access Control
MIB	Management Information Base
MSB	Most Significant Bit
NE	Network Element
OSI	Open System Interconnection
OSP	Outside Plant
OUI	Organizationally Unique Identifier
PDU	Protocol Data Unit
PHY	Physical
POSIX	Portable Operating System Interface
RF	Radio Frequency
RFC	Request for Comment
RSVD	Reserved
SNMP	Simple Network Management Protocol
TOD	Time-of-Day
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Data-gram Protocol

4 Reference architecture forward and return channel specifications

The reference architecture for the series of specifications is illustrated in Figure 1.

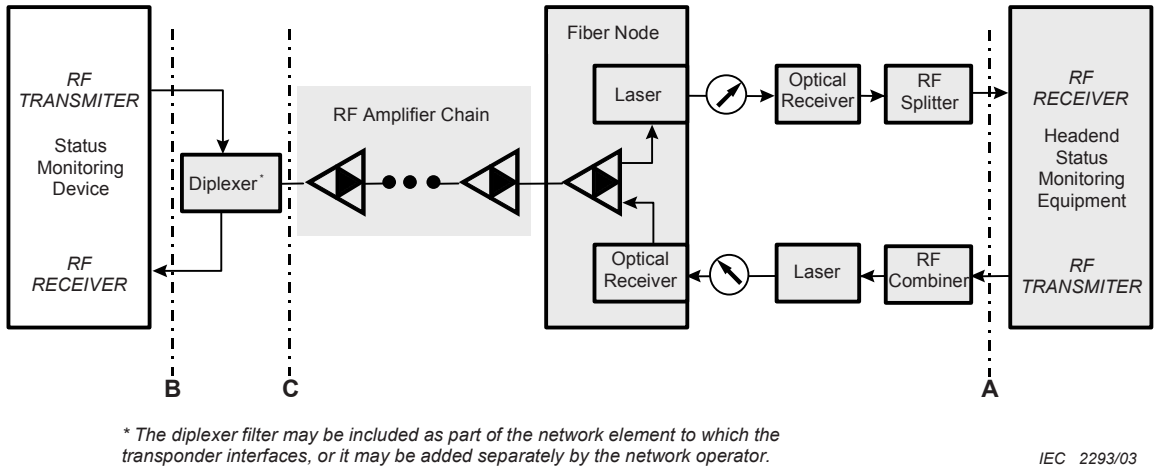


Figure 1 – Reference architecture diagram

All quantities relating to forward channel transmission or reverse channel reception are measured at point A in Figure 1. All quantities relating to forward channel reception or reverse channel transmission are measured at point B for two-port devices and point C for single-port devices as shown in Figure 1.

5 Media access control layer specification

5.1 Overview

This clause describes the MAC protocol. Some of the MAC protocol features include:

- support for transaction-based message exchange over the HFC forward and return RF channels. Transactions can be initiated by either the HE or the NE; support for transport of multiple network PDU types over the HFC forward and return RF channels including, but not limited to, IP over serial and SNMP over serial;
- extensions provided to support future transport of other network PDU types;
- efficient use of HFC forward and return RF spectrum through central HE management of NE transmission opportunities.

5.1.1 Definitions and conventions

5.1.1.1 Separate forward and return channels

The one-way communication channel from the HE to a managed OSP NE is referred to as the *forward* channel. The one-way communication channel from a managed OSP NE to the HE is referred to as the *return* channel. Both the forward and the return channels are placed on specific centre frequencies. The forward and return channels' centre frequencies are different. Since the NEs only listen to the forward channel, they cannot listen to return channel transmissions from other NEs. This channel separation is a result of the sub-band split between the forward and return portions of the typical HFC plant spectrum.

5.1.1.2 Single forward and return path channels per MAC layer domain

To keep management of carrier frequencies simple, each status monitoring system has a single forward channel and a single return channel. This does not preclude the use of multiple monitoring systems, each with its own individual forward and return RF channels.

A MAC layer domain consists of a single forward RF channel and a single return RF channel over which a single MAC layer bandwidth allocation and management protocol operates. It includes a centralized HE and multiple compliant transponders interfacing to managed OSP NEs. The centralized HE may support multiple HMS-based status monitoring systems, i.e. multiple MAC layer domains. Each OSP NE must only access a single forward channel and its associated single return channel, i.e. it must only operate within a single HMS MAC layer domain.

5.1.1.3 Network element (NE) term usage

The HMS MAC layer supports bandwidth management and reliable communications between a HE and multiple compliant transponders that interface to managed OSP NEs. Throughout this standard, the terms “compliant transponder”, “transponder”, and “NE” are used interchangeably when describing the MAC processes that support the exchange of data or other information between two or more entities at the DLL.

5.1.1.4 Packet

A packet is a unit of data exchanged between the HE and any of a number of managed OSP NEs at the DLL. Packets are strings of bytes that can be sent contiguously or be separated by periods of silence. Document *Outside Plant Status Monitoring – Physical (PHY) Layer Specification* describes specific byte transmission modes that must be implemented in both forward and return channels. A MAC packet consists of a MAC header, a variable-length payload, and a frame check sequence (see 5.3).

5.1.1.5 Most significant byte

Unless otherwise specified, it is assumed throughout this standard that the left-most entry in any numeric value is the most significant, i.e. for the address represented as 12-34-56-78-9A-BC the left-most entry ‘12’ is the most significant value.

5.1.1.6 Byte number representation

Throughout this standard, bits labelled ‘0’ are the least significant bits (LSBs) and bits labelled ‘7’ are the most significant bits (MSBs). The bits in a given byte will be described with bit 7 (MSB) at the left and bit 0 (LSB) at the right. This convention has been adopted for presentation purposes only and has no effect on the actual bit transmission order. Bit transmission order details are provided in 5.2 of this standard.

5.1.1.7 Reserved bits

A number of bits are indicated with the word “Reserved” or the abbreviation “RSVD” in the various MAC packets described in this standard. Any receiving NE must ignore these bits when implementing this version of the MAC protocol.

5.2 MAC packet transport

5.2.1 Byte transmission format

Bytes transmitted over both forward and return channels are ten bits in length. They contain one start bit, eight bits of data, and one stop bit. The start bit has the binary value ‘0’, and the stop bit has the binary value ‘1.’

5.2.2 Byte transmission order

Fields consisting of multiple bytes, i.e. a MAC address will have the most significant byte transmitted first. Any exceptions to this rule will be specifically noted in this standard as necessary.

5.2.3 Bit transmission order

The LSB of a single byte, bit 0, is always transmitted first following the start bit. The MSB of a single byte, bit 7, is always transmitted last followed by the stop bit. The transmission order is summarized in Figure 2.

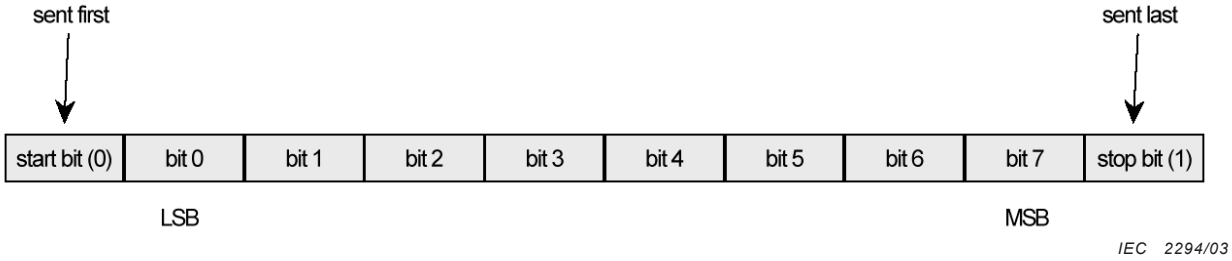


Figure 2 – Bit transmission order

NOTE In the NCTEA S-006, eleven bits data format is used as follows:
– start bit(0);
– LSB bit(0) ~ MSB bit(7);
– parity bit;
– stop bit(1).

5.2.4 Transmission timing

5.2.4.1 Forward channel packets

5.2.4.1.1 Timing

Forward channel packets shall be transmitted in such a manner that

a) no two bytes within a packet are separated by more than 3 ms, and

b) the entire packet must be transmitted within 120 % of the *shortest* time for that frame. The shortest time is defined as the time for transmission of the packet with no gaps between bytes.

5.2.4.2 Return channel packets

5.2.4.2.1 Front porch

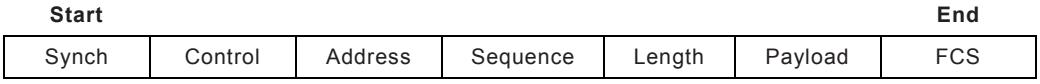
NE transmission of the first byte of a message shall begin within a window of two and five byte times after the transmitter power reaches 90 % of its final value. Until the first byte is transmitted, the frequency will rest on the ‘mark’ frequency. This is standard Universal Asynchronous Receiver/Transmitter (UART) transmission. The front porch ensures that the receiving UART can be cleared of all framing errors prior to the start of reception of valid data.

5.2.4.2.2 Timing

Return channel packets must be transmitted in such a manner that no two bytes within a packet are separated by more than 260 μs (1 byte time). All bits within a single byte shall be immediately contiguous; there shall be no gaps at bit boundaries within a byte.

5.3 MAC packet structure

MAC packets consist of a MAC header, a variable-length payload, and a two-byte frame check sequence. Packet structure and sizes are identical for both forward and return channel packets. MAC packet structure is illustrated in Figure 3.



IEC 2295/03

Figure 3 – MAC packet structure

All MAC packets must have the general format as described in Table 2.

Table 2 – Generic MAC packet structure

Field name	Length (bits)	Subclause
Synch	8	5.3.1
Control	8	5.3.2
Address	48	5.3.3
Sequence	8	5.3.4
Length	16	5.3.5
Payload	N	5.3.6
FCS	16	5.3.7

5.3.1 Synch

The synch field consists of a single byte and identifies the start of the MAC layer packet. It shall be set to 0xA5.

5.3.2 Control

The control field consists of a single byte and defines the type and format of the payload field. The bit definition of the control byte is shown in Figure 4. The control field also serves, in conjunction with the synch, length and FCS fields, as a packet delimiter as described in 5.4.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RSVD3	RSVD2	RSVD1	RSVD0	Protocol			

IEC 2296/03

Figure 4 – MAC header control byte – bit definition

5.3.2.1 Protocol (bits 3:0)

The four-bit protocol field indicates the type of protocol to be used to interpret the payload field of the MAC layer packet. In addition, the protocol field allows the message service handler to pass messages with alternative protocol values to other upper layer processes without having to unravel the entire message. The value represented by the protocol field shall be as assigned in Table 3.

Table 3 – Protocol field values

Description	Binary value
MAC management message	0000
SNMP over serial (see note below)	0001
IP over serial	0010
SNMP trap over serial	0011
Available for future use	0100 to 1111 [a]
NOTE This is SNMPv1 as defined by RFC 1157. However, the UDP and IP protocols are not used for this implementation. Thus, all references by RFC 1157 to UDP are not relevant. Subclause 3.2.4 of RFC 1157 explains how the SNMP mechanisms are suitable over different transport protocols. Clauses 4 and 4.1 of RFC 1157 explain this further. In fact, in 4.1, the RFC states: "Other transport services may be used to support the SNMP."	
[a] Protocol 0101 is not allowed to prevent accidental creation of a synch byte (0xA5).	

5.3.2.2 RSVDx (bits 7:4)

The bits identified as RSVD are reserved for future use. They must be set to 0.

5.3.3 Address

The Address field consists of six bytes. It is used to address devices on a unicast, multicast, or broadcast basis. The address field follows the IEEE Organizationally Unique Identifier (OUI) Std 802 usage for a Universal address. For clarity, this standard conforms to the address documentation suggested by the IEEE as follows:

a) each byte is represented as a two digit hexadecimal numeral (with no radix identification) using leading zeroes where the first (left-most) digit of the pair is the most significant.

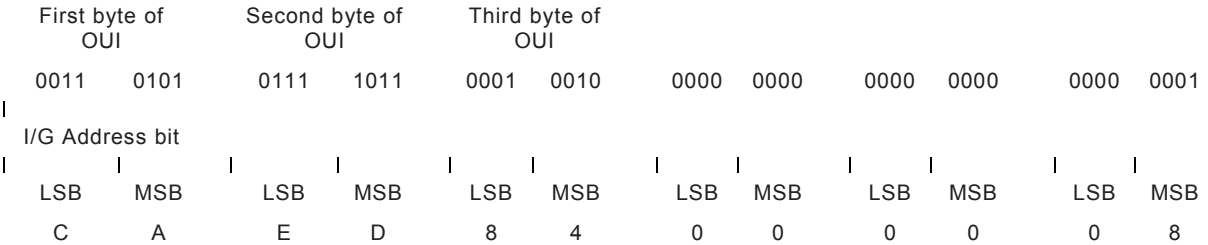
b) each byte is separated by hyphens, with the most significant byte in the left-most position.

An example address is 00-AA-BB-00-43-21.

A universal address is a sequence of six bytes. The first three take the values of the three bytes of the OUI in order. The last three bytes are administered by the assignee. The binary representation of an address is formed by taking each byte in order and expressing it as a sequence of eight bits, LSB to MSB, left to right. For example, the OUI AC-DE-48 could be used to generate the address

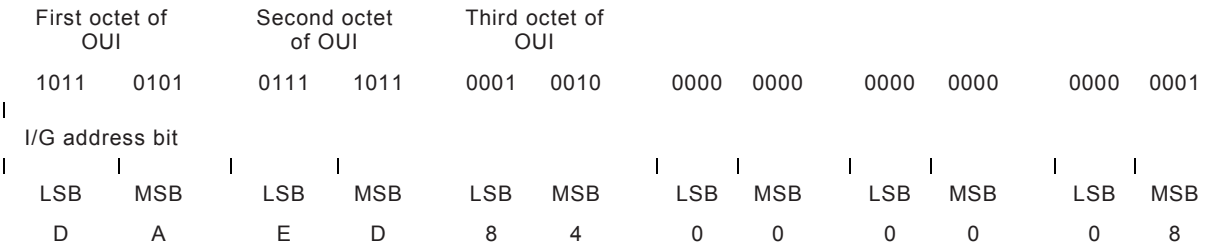
AC-DE-48-00-00-80

Whose binary representation is:



The first (left-most) bit in the binary representation of the MAC address is the I/G (Individual/Group) Address Bit. This bit is the LSB of the most significant byte. When set to 0 as shown above, it indicates an individual address. It may be set to 1 in an address allocated by the assignee to indicate that that address is a group address. For example, the same OUI above could be used to generate the group address.

AD-DE-48-00-00-80



The address shall be transmitted the most significant byte first and the least significant byte last.

5.3.3.1 Unicast

The Unicast address is the unique address assigned to a particular NE. An NE transmitting a message places its unicast address in the Address field, most significant byte first. This address is completely unique across all manufacturers. By definition, the I/G bit is set to 0.

Each vendor shall obtain an address prefix, or OUI, from the IEEE and assign a unique address using this prefix to each HMS-compliant transponder at time of manufacture. This is the Unicast address for that NE. This standard places no restriction on the number of OUIs a single manufacturer may obtain as the IEEE governs that. An OUI assignment allows the assignee to generate approximately 16 million addresses by varying the last three octets.

5.3.3.2 Broadcast

A message with a broadcast address is intended for all NEs that receive it. All NEs must support the broadcast address. The broadcast address is FF-FF-FF-FF-FF-FF.

5.3.3.3 Multicast

The multicast address follows the IEEE Standard 802 for indicating a group Address, i.e. the I/G address bit is set to 1.

A multicast address defines a group to which zero, one, or more than one NE has been assigned by a higher level management system. An NE maintains a list of multicast addresses to which it will respond. An NE is a member of a particular multicast group if at least one of its provisioned multicast addresses matches that particular multicast address. The assignment and usage of multicast addresses is out of the scope of this standard. However, examples might be fault isolation, frequency changes, and firmware downloads.

All NEs must support a minimum of four (4) multicast addresses not counting the broadcast address. This standard places no maximum limit on the number of multicast address groups an NE may support.

Multicast addresses are *not* assigned at manufacture. The network provider provisions multicast addresses into the NE. The method for this provisioning is out of the scope of this standard. To avoid accidental assignment to the wrong multicast address, all multicast addresses held at the NE shall default to the broadcast address prior to provisioning.

5.3.4 Sequence

The MAC protocol is transaction-based, i.e. every originating message from a “requestor” has a corresponding response from the “responder” regardless of which device originated the message. The sequence field consists of a single byte and defines a message sequence number to ensure message exchanges are synchronized. In order to handle possible loss of messages in either the forward or the return channel, and to avoid duplication of messages at

the application layer, all messages have a sequence number. The bit definition of the sequence byte is shown in Figure 5.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
SYN	MSGSEQ						

Figure 5 – MAC header sequence byte – bit definition

IEC 2297/03

5.3.4.1 MSGSEQ (Bits 6:0)

The 7-bit MSGSEQ field indicates the message sequence number. Sequence numbers are generated by either the HE or NE. Sequence number generation, modification and elicited behaviour must conform to the following rules:

a) HE-originated transactions will have bit 6 of the MSGSEQ field set to 1. Thus, the range for HE-generated sequence numbers is 0x40 through 0x7F with wraparound to 0x40;

b) the HE shall generate and track sequence numbers per unicast address;

c) HE-generated messages directed to broadcast or multicast addresses, i.e. where the I/G bit is set to 1, shall have a sequence number of 0 since this field is ignored by the NE for multicast and broadcast messages. Upon receiving a valid broadcast or multicast message from the HE, the NE shall not change the last received HE sequence number. The NE shall *always* process broadcast or multicast messages regardless of sequence number;

d) NE-originated transactions will have bit 6 of the MSGSEQ field set to 0. Thus, the range for the NE is 0x00 through 0x3F with wraparound to 0x00;

e) as a requestor, the NE can have only a single originating message requiring a response outstanding at any time (see 6.8). Thus, the NE only needs to track the sequence number for this single value;

f) the MSGSEQ field is incremented by the originator of the number. The sequence number shall be incremented only:

   1) when a response is received with a matching sequence number (excluding the SYN bit, see 5.3.4.2), or

   2) when a requestor's maximum allowed number of MAC layer transmission retries has been exceeded. The MSGSEQ shall not change if a message must be retransmitted at the MAC layer, which occurs only when a response or acknowledgement has not been received within a pre-determined timeout window, and the maximum allowed number of MAC layer transmission retries for this message has not been exceeded. See clause 6 of this standard for additional details on MAC protocol operation;

g) the responding entity shall save the sequence number of the last received message directed to its unicast address and perform one of the following:

   1) if the MSGSEQ field is different from the last one seen, the responder should process the message, form a response if one is required, and send it. The responding entity shall take the value of the sequence number in the MSGSEQ field from the request and place it in the MSGSEQ field of its response,

   2) if the MSGSEQ field is the same as the last one seen, the responder knows that its last response was not received and it should resend the response. The responder should *not* process the message again. It must simply resend the previously transmitted message. The responding entity shall take the value of the sequence number in the MSGSEQ field from the request and place it in the MSGSEQ field of its response;

h) if the responding entity has been reset, it shall process the first received message directed to its unicast address regardless of the value in the MSGSEQ field.

NOTE A possible implementation refinement to ensure subsequent message exchanges are synchronized is to initialize the "last sequence number" to an out-of-range value that a requestor cannot possibly support. This would guarantee that the first message from a responder after a reset always has a unique sequence number associated with it that forces the requestor to re-issue the original request thus ensuring message exchange re-synchronization.

5.3.4.2 SYN (Bit 7)

The following rules govern the selection of the SYN bit value and elicited behaviour:

a) after a device (HE or NE) is reset, it shall set the SYN bit to 1 in every packet it originates and sends to a given responder until the first correct response is received from that responder. When the SYN bit is set to 1 by a requestor, the responder is not to verify the MSGSEQ field in the message. The MSGSEQ field contained within the packet is to be used by the requestor as the last received value. This will synchronize the responder to the current requestor sequence number;

b) the SYN bit shall always be set to 0 when responding to a request. When the SYN bit is set to 0 by a requestor, the responder is to verify the MSGSEQ field in the packet.

Clause 6 of this standard provides additional information on the use of the sequence field. It also includes a sample message exchange for illustration purposes.

5.3.5 Length

The length field consists of two bytes and specifies the number of bytes in the payload field of the MAC layer packet. Although the *theoretical* maximum payload length is 65 535 bytes, the absolute maximum message length that may be transmitted (including all message overhead and synch byte padding) will be determined by the maximum duration of return channel transmissions before automatic RF transmission cut-off is invoked. An *Outside Plant Status Monitoring – Physical (PHY) Layer Specification* document requires that compliant transponders support automatic RF transmission cut-off on the return channel to shut down transponders that have failed with their transmitter ON.

An implementation of this protocol need not accept messages whose length exceeds 484 bytes. However, it is recommended that implementations support larger messages whenever feasible. Synch bytes inserted in the payload do *not* count towards the message length, see 5.4.3.

5.3.6 Payload

The payload field contains the data delivered to/from the higher layer protocols.

5.3.7 Frame check sequence (FCS)

The FCS field consists of two bytes. It is CCITT CRC-16 as documented in RFC 1662, appendices C.1 and C.2. The CRC calculation is performed over the entire packet, *excluding* the synch field, but *including* the control, address, sequence, length, and payload fields. Synch byte insertions for achieving transparent throughput of all data (see 5.4.3) are NOT included in the CRC calculation.The final value obtained from the CRC calculation is complemented and transmitted *least significant byte first.* The following example illustrates this convention (sample forward path message, all values in HEX):

A5 00 00 10 3F 00 43 21 49 00 01 02 1D 1C

The FCS for this message is calculated to be 0xE3E2. When complemented, the value is 0x1C1D. This is then transmitted least significant byte first (0x1D, 0x1C).

5.4 MAC packet delimiters

The synch, control, length and FCS fields are used to delimit a packet and indicate its integrity.

5.4.1 Packet start

Detection of a synch byte followed by a non-synch byte will identify the start of a packet. Characters received after the end of a packet (see 6.4) but prior to detection of a new synch byte and a non-synch byte combination shall be discarded.

5.4.2 Packet end

The exact location of the FCS and the end of the packet can be calculated from the length byte. The integrity of the packet is checked using the FCS. Packets with an invalid FCS shall be discarded. Packets with a valid FCS, but with invalid content will also be discarded.

5.4.3 Synch byte padding

In order to ensure message synchronization and obtain data transparency in the message, it is necessary to distinguish a true synch byte from any other byte in the payload that has the same value. To accomplish this, a transmitting device (NE or HE) will insert the synch byte *after* any data byte having a value of 0xA5. This rule shall apply to the address, sequence, length, payload, and FCS fields but *not* to the synch and control fields. This ensures that the synch byte and non-synch byte combination will never be found together in the remainder of the packet.

After detection of the start of a packet, the receiver of the packet will remove one synch byte from any two-byte sequence that contains back-to-back synch bytes [0xA5, 0xA5]. If a single synch byte is detected within the packet, the data up to that point shall be discarded and the receiver shall begin the packet delimitation process again, using the newly received 0xA5 as the start of packet indicator.

Synch bytes added for data transparency are *not* counted toward the length of the packet, and are *not* included in the FCS calculation for a packet by either the sender or the receiver.

5.5 MAC protocol data units (PDUs)

MAC PDUs are contained in the payload field of the message. MAC PDU structure is illustrated in Figure 6.

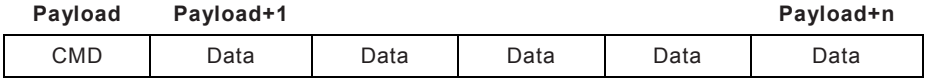


Figure 6 – MAC PDU structure

IEC 2298/03

The presence of the data fields depends on the PDU.

The PDUs defined for the MAC layer are listed in Table 4. Since all MAC layer messages are transaction-based, a list of possible transactions is shown in Table 5.

Table 4 – MAC PDUs

PDU Name	CMD	Subclause
NAK	0x00	5.5.1
ACK	0x01	5.5.2
STATRQST	0x02	5.5.3
STATRESP	0x03	5.5.4
TALKRQST	0x04	5.5.5
TALK	0x05	5.5.6
CONTMODE	0x06	5.5.7
REG_REQ	0x07	5.5.8
SET_ADDR	0x08	5.5.9
REG_END	0x09	5.5.10
CHNLDESC	0x0A	5.5.11
INVCMD	0x0B	5.5.12
TIME	0x0C	5.5.13

Table 5 – Possible MAC protocol transactions

Originator	PDU	Responder	Possible responses
HE	STATRQST	NE	STATRESP
HE	CONTMODE	NE	ACK or INVCMD
HE	TALK	NE	NAK REG_REQ INVCMD Non-MAC protocol message
HE	SET_ADDR	NE	ACK INVCMD
HE	REG_END	NE	ACK or INVCMD
HE	CHNLDESC	NE	ACK or INVCMD
HE	TIME	NE	ACK
NE	TALKRQST	HE	ACK

All of these MAC transactions can be processed by the NE before the NE is registered. The only message restriction at this time is that SNMP traps shall not be transmitted by the NE prior to registration completion as signalled by reception of a successful REG_END PDU from the HE (see 5.5.10). Additionally, there is no restriction on SNMP Get, GetNext, and Set requests.

5.5.1 NAK

The NAK PDU is a *possible* NE response to the HE TALK PDU. The NAK PDU has the format shown in Table 6. Description of the use of this message can be found in A.5.5.

Table 6 – NAK PDU format

Field	Size (bytes)	Value
CMD	1	0x00

5.5.2 ACK

The ACK PDU can be originated by the HE or the NE. The ACK PDU has the format shown in Table 7.

Table 7 – ACK PDU format

Field	Size (bytes)	Value
CMD	1	0x01

Only unicast addresses can be used with the ACK PDU. Additional details on the use of the ACK PDU can be found in A.5.5.

5.5.3 STATRQST

The STATRQST PDU is originated by the HE. The expected response is a STATRESP PDU. The STATRQST PDU has the format shown in Table 8.

Table 8 – STATRQST PDU format

Field	Size (bytes)	Value
CMD	1	0x02

Only unicast addresses can be used with the STATRQST PDU.

5.5.4 STATRESP

The STATRESP PDU is the NE response to a HE STATRQST PDU. The STATRESP PDU has the format shown in Table 9. The STATRESP PDU has a one-byte STATUS Data field associated with it. The STATUS Data field bit definition is shown in Figure 7

Table 9 – STATRESP PDU format

Field	Size (bytes)	Value
CMD	1	0x03
STATUS	1	See Figure 7

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RSVD3	RSVD2	RSVD1	MINOR	MAJOR	CNTCUR	CNTNRM	CHNLRQST

IEC 2299/03

Note that this STATUS byte is *identical* to the common NEStatus variable.

Figure 7 – STATRESP STATUS byte – Bit definition

5.5.4.1 CHNLRQST (bit 0)

The CHNLRQST bit indicates when the NE has unsolicited messages it wants to transmit to the HE. See Table 10 for the bit value definitions. See Figure 9 for the state diagram governing the actions and usage of contention.

Table 10 – CHNLRQST bit settings

Value	Meaning
0	NE has no unsolicited messages to transmit.
1	NE has unsolicited messages that will be transmitted when the return channel is allocated a transmit opportunity with a TALK PDU, as permitted by the registration state.

Until an NE is registered, only a REG_REQ PDU can be generated (see 5.5.8). After successful registration (REG_END with SUCCESS status, see 5.5.10), the CHNLRQST bit shall be set for any non-MAC messages that are to be transmitted (e.g. SNMP traps).

5.5.4.2 CNTNRM (bit 1)

The CNTNRM bit indicates the “normal” state of contention, as set by the last CONTMODE PDU message (see 5.5.7). See Table 11 for the bit value definitions.

Table 11 – CNTNRM bit settings

Value	Meaning
0	The “normal” mode of contention is OFF for this NE.
1	The “normal” mode of contention is ON for this NE.

5.5.4.3 CNTCUR (bit 2)

The CNTCUR bit indicates the “current” state of contention, as set by the last CONTMODE PDU message (see 5.5.7). See Table 12 for the bit value definitions.

Table 12 – CNTCUR bit settings

Value	Meaning
0	Contention is OFF for this NE.
1	Contention is ON for this NE.

5.5.4.4 MAJOR (bit 3)

The MAJOR bit indicates whether alarms with a major severity are present in the NE or in the equipment monitored by the NE. See Table 13 for the bit value definitions.

Table 13 – MAJOR bit settings

Value	Meaning
0	No alarms with MAJOR severity are present.
1	Alarms with MAJOR severity are present.

5.5.4.5 MINOR (bit 4)

The MINOR bit indicates whether alarms with a minor severity are present in the NE or in the equipment monitored by the NE. See Table 14 for the bit value definitions.

Table 14 – MINOR bit settings

Value	Meaning
0	No alarms with MINOR severity are present.
1	Alarms with MINOR severity are present.

5.5.4.6 RSVDx (bit 7:5)

The bits identified as RSVD are reserved for future use. They must be set to 0.

5.5.5 TALKRQST

The TALKRQST PDU is originated by an NE. The expected HE response is the ACK PDU. The TALKRQST PDU has the format shown in Table 15.

Table 15 – TALKRQST PDU format

Field	Size (bytes)	Value
CMD	1	0x04

The TALKRQST is transmitted by the NE *only* under the following conditions:

a) the NE *must* have unsolicited messages that it wants to transmit.

b) contention mode *must* be in the ON state for the NE (C_C = 1). See 5.5.7.

Once an ACK PDU response has been received, the TALKRQST PDU can be transmitted again in either of two cases:

a) the current contention mode of the NE has been toggled OFF then ON again using the CONTMODE PDU (effectively a new contention period, see 5.5.7). In this case, the TALKRQST PDU can be transmitted again since the CHNLRQST bit (bit 0 in status byte of the STATRESP PDU) is still set; or

b) the NE transmitted a NAK PDU in response to a TALK PDU, i.e. the last time the NE was given permission to transmit it had no more messages to send (see 5.5.6). In this case, the NE, which previously had no more messages to transmit, now has new outstanding messages and is permitted to generate a new TALKRQST PDU.

5.5.6 TALK

The TALK PDU is originated by the HE. The expected NE responses are:

a) NAK PDU (no more messages to transmit);

b) non-MAC protocol message (e.g. SNMP trap over serial);

c) REG_REQ PDU (NE requesting registration, see 5.5.8).

The TALK PDU has the format shown in Table 16. The TALK PDU has a one-byte ACKSEQ data field associated with it.

Table 16 – TALK PDU format

Field	Size (bytes)	Value
CMD	1	0x05
ACKSEQ	1	See text

The TALK PDU gives the addressed NE access to the return channel to transmit a single message. In typical usage, the HE issues a CONTMODE PDU to turn off contention mode, then issues the TALK PDU to give the clear return channel to the NE. See the transaction example illustrated in Table 19.

The ACKSEQ field of the TALK PDU contains the sequence number of a previous message that *this* packet is acknowledging. In the situation where the HE has no previous message to acknowledge, the ACKSEQ field shall be 0xFF.

If the message sequence number in the ACKSEQ data field of the TALK PDU does not match the expected number, the NE shall respond with the INVCMD PDU using the "invalid parameter" error code (see 5.5.12). The expected HE behaviour would then be to re-issue a TALK PDU. The ACKSEQ byte in the TALK PDU will have a sequence number of 0xFF to indicate that the HE lost track of the sequence numbers. This will cause the NE to retransmit its last response to the HE TALK PDU allowing the HE to resynchronize correctly.

5.5.7 CONTMODE

The CONTMODE PDU is originated by the HE. The CONTMODE PDU has the format shown in Table 17. The CONTMODE PDU has two data fields associated with it: the MODE field and the DURATION field both of which are one byte in length.

Table 17 – CONTMODE PDU format

Field	Size (bytes)	Value
CMD	1	0x06
MODE	1	See Table 18
DURATION	1	Time duration of C_C = 1

5.5.7.1 CONTMODE: MODE

The MODE field determines the contention state for the addressed NEs. The expected NE response to the CONTMODE PDU is an ACK PDU *only* if a unicast address is used and the MODE value is one of those in Table 18 (even if the MODE value is not applicable). An INVCMD PDU response shall be transmitted if a unicast address is used and the mode value is *not* one of those shown in Table 18.

Table 18 – CONTMODE: MODE settings

Value	Meaning
0 (OFF)	Contention is turned OFF for the addressed NEs. C_N = 0, C_C = 0. DURATION has no effect.
1 (ON)	Contention is turned ON for the addressed NEs. C_N = 1, C_C = 1. DURATION is meaningful.
2 (INH)	Contention is *inhibited* for the addressed NEs. C_N = unchanged, C_C = 0. DURATION has no effect.
3 (RES)	Contention is *restored* for the addressed NEs. C_N = unchanged, C_C = C_N. DURATION is meaningful for NEs with C_N = 1.

4 (REG)	Contention is *enabled* for non-registered NEs. C_N = 0, C_C = 1. DURATION is meaningful for these NEs. Contention is *inhibited* for all registered NEs. C_N = unchanged, C_C = 0. DURATION has no effect for these NEs.

C_C: Contention mode "current" – the setting of this flag controls whether or not contention is currently enabled or disabled for the NE. A value of 0 means that the NE is *not* permitted to send the TALKRQST PDU.

C_N: Contention mode "normal" – the setting is restored with the MODE value of 3. This flag is changed *only* with the OFF and ON MODE values.

Upon NE power up for the first time or NE reset, the state of these flags shall be

$$C_N = 0,\ C_C = 0$$

Figure 9 illustrates the applicable state machine diagrams and describes how these modes are to be used in the NE. If a MODE value is valid, but not applicable in a given state (as shown in the state diagram), it shall not be processed. However, if the NE was addressed using a unicast address it shall respond with an ACK PDU.

Table 19 illustrates the use of the CONTMODE PDU in the case of an NE with three messages to send. The value in parentheses for the TALK PDU is the value of the ACKSEQ field.

Table 19 – NE message retrieval example

HE	Message sequence number		To/from	NE	Message sequence number	MODE value
CONTMODE ON	00	->	*			1
		<-	A	TALKRQST	15	1
ACK	15	->	A			1
CONTMODE INH	00	->	*			0
TALK (0xFF)	43	->	A			0
		<-	A	SNMP trap 1	43	0
CONTMODE RES	00	->				1
		<-	A	TALKRQST [1]	16	1
ACK	16	->	A			1
TALK (0x43)	44	->	A			1
		<-	A	SNMP trap 2	44	1
TALK (0x44)	45	->	A			1
		<-	A	SNMP trap 3	45	1
TALK (0x45)	46	->	A			1
		<-	A	NAK	46	1
				New alarm occurs		1
		<-	A	TALKRQST [2]	17	1
ACK	17	->	A			

[1] Case 1: New contention window.

[2] Case 2: New alarms after a NAK, same contention window.

5.5.7.2 CONTMODE: DURATION

When a CONTMODE PDU is issued which changes the state of C_C to 1, the DURATION field specifies the number of seconds that this mode will be active. Specifically, the DURATION field has meaning for the ON, RES, and REG modes. This field has *no meaning* when the state of C_C will be set to 0. Note that if a RES mode is issued and C_C is set to 0, the DURATION field, though valid, has no effect. A value of 0 in the DURATION field indicates unlimited time.

If the duration timer is active, i.e. a previous CONTMODE PDU with MODE setting and DURATION value has started the timer, and a new CONTMODE PDU with a new MODE setting and DURATION field is received, the timer is restarted using the new DURATION field value.

The duration timer acts as a “master shutoff” meaning that once the DURATION period expires a state change to C_C = 0 occurs. This action is identical to using all MAC layer transmission retries (see Clause 6). When this occurs, the NE shall *not* transmit any further TALKRQST packets. Note that any CONTMODE PDU which explicitly sets C_C = 0 prior to the expiration of the DURATION period will have the same effect.

The DURATION field protects against the possibility of the HE transmitting a CONTMODE PDU setting C_C = 0 that is not received by the NE. In this case, the DURATION field and timer-activated shutoff action provides an NE-based failsafe backup mechanism to prevent unwanted transmissions.

5.5.8 REG_REQ

The REG_REQ PDU can be generated by an NE in response to the TALK PDU. The REG_REQ PDU has the format shown in Table 20. The REG_REQ PDU has a four-byte IP_ADDRESS data field associated with it.

Table 20 – REG_REQ PDU format

Field	Size (bytes)	Value
CMD	1	0x07
IP_ADDRESS	4	IP address programmed into the NE (IPv4 only)

The NE transmits the REG_REQ *only* after it “boots” (power-up, hard or soft reset, etc.) The NE uses this message to register it in the system. This message may be transmitted *only* when the contention state is non-REG (see Figure 9). Note that if a REG_END PDU is received when this message is waiting to be transmitted, it will cause the NE to cancel the transmission of this message (see 5.5.10). See clause A.7 for more details about the auto-registration process.

5.5.9 SET_ADDR

The SET_ADDR PDU is originated by the HE. The expected NE response is the ACK PDU. The SET_ADDR PDU has the format shown in Table 21. The SET_ADDR PDU has a four-byte IP_ADDRESS data field associated with it.

Table 21 – SET_ADDR PDU format

Field	Size (bytes)	Value
CMD	1	0x08
IP_ADDR	4	Appropriate

The HE transmits the SET_ADDR command to set the IP address of the NE. The value for IP_ADDR can be:

a) address 0.0.0.0 for an NE in a proxy system; or

b) a real IP address. How this IP address is determined or obtained by the HE is beyond the scope of this standard. This could be the IP address received with the REG_REQ PDU, i.e. the HE is setting the NE to the IP address already programmed into the NE; or

c) the IP address of the HE (only in a proxy system).

The following ranges of IP addresses are reserved and define sets of invalid IP addresses for the NEs:

a) 224.0.0.0 – 239.255.255.255. This address range is reserved for IP multicast addresses (class D); and

b) 240.0.0.0 – 255.255.255.255. This address range is reserved for future use (class E).

The IP address of the NE must not be set within any of the above ranges.

Only unicast MAC addresses may be used with this command. The NE must discard a SET_ADDR command if a MAC multicast address or the MAC broadcast address is used. The NE shall respond with an INVCMD PDU if any of the following occurs:

a) if the NE was unable to set its IP address as indicated, the NE shall respond with an INVCMD PDU with the “undefined error” value (see 5.5.12). Note that this does not imply anything about the validity of the IP address, but rather the ability of the NE to save the IP address in non-volatile memory; or

b) if the NE is commanded to set its IP address to an invalid IP address, the NE shall respond with an INVCMD PDU with the “invalid parameter” value (see 5.5.12).

5.5.10 REG_END

The REG_END PDU is originated by the HE. The expected NE response is the ACK PDU. The REG_END PDU has the format shown in Table 22. The REG_END PDU has two data fields associated with it: a one-byte STATUS field and a four-byte TOD field.

Table 22 – REG_END PDU format

Field	Size (bytes)	Value
CMD	1	0x09
STATUS	1	See Table 23
TOD	4	Time of day in POSIX format, most significant byte first

5.5.10.1 REG_END:STATUS

The REG_END PDU is transmitted by the HE upon completion of NE registration. The STATUS field indicates NE registration status. Defined STATUS field settings are shown in Table 23.

Table 23 – REG_END: STATUS settings

Value	Meaning
0	SUCCESS. Registration succeeded. The NE must continue its start-up sequence.

1	DENIED. Registration has been denied. The NE may optionally use the CHNLDESC PDU mechanism (see 5.5.11) to search for another channel, or it may request registration on this channel again.
2	FAILED. Registration failed. The NE must wait until the next registration opportunity (CONTMODE REG).
3	PENDING. Registration is pending. The NE has found the correct HE but the HE is not yet ready to process this NE. The NE must not send any further registration requests. The NE must not send any SNMP traps or perform alarm processing.

Receipt of the REG_END PDU with a STATUS value of 0 (SUCCESS) shall change the contention state to REG (see Table 18 and Figure 9). Additionally, if the NE has a pending REG_REQ PDU waiting to be transmitted, receipt of the REG_END will clear this pending request.

The NE shall be permitted to send SNMP traps and may perform alarm processing *only* upon receiving a STATUS of 0 (SUCCESS). If a REG_END PDU with STATUS of 3 (PENDING) is received by the NE, the NE must still wait for reception of a REG_END PDU message with STATUS of 0 (SUCCESS).

Upon reception of a REG_END PDU with a status of PENDING, the NE shall remain in that state for a maximum period of 1 h. At the end of that time, if the NE is still in that state, it shall return to the non-registered OFF state.

Upon reception of a REG_END PDU with a status of SUCCESS, the NE shall not recognize any further REG_END PDU commands. If a unicast address was used, the transponder shall respond with an INVCMD PDU with the “invalid parameter” error code (see 5.5.12).

5.5.10.2 REG_END: TOD

The TOD field shall contain the time in POSIX format (see A.2) with the most significant byte first. The NE is *required* to synchronize its internal time-of-day clock to this time. This field is always valid regardless of the value of the STATUS field.

5.5.11 CHNLDESC

The CHNLDESC PDU is originated by the HE. The expected NE response (unicast address only) is the ACK PDU. The CHNLDESC PDU has the format shown in Table 24. The CHNLDESC PDU has two Data fields associated with it: the FORWARD field and the RETURN field both of which are four bytes in length.

Table 24 – CHNLDESC PDU format

Field	Size (bytes)	Value
CMD	1	0x0A
FORWARD	4	Forward channel frequency in use for this channel (centre frequency in Hz)
RETURN	4	Return channel frequency in use for this channel (centre frequency in Hz)

The CHNLDESC is transmitted by the HE under *any* of the following conditions:

a) periodically, *at least* every 30 s, with a +5 s tolerance, using the broadcast address. This is used by the NE to automatically find the proper forward and return channels in use.

b) anytime forward or return channel frequencies are changed. In this case, it is *recommended* that the message be transmitted several times in sequence. There are no address restrictions in this mode. If a unicast address is used, the NE must send an ACK PDU in response.

The NE shall *always* process this PDU if it belongs to the addressed group. If either of the frequencies specified in the PDU are invalid for the NE, then

a) the NE shall *not* change either frequency; and
b) if a unicast address was used, the NE will reply with the INVCMD PDU using the “invalid parameter” error code (see 5.5.12).

The NE shall implement a failsafe mechanism to recover from loss of forward channel frequency due to a requested frequency change. The recovery method used shall be determined by the vendor. The method used to determine loss of forward frequency shall also be determined by the vendor.

5.5.12 INVCMD

The INVCMD PDU can be originated by the NE in response to a command from the HE. This message is transmitted *only* if a unicast address was used in the original message. The INVCMD PDU has the format shown in Table 25. The INVCMD PDU has a one-byte REASON data field associated with it.

Table 25 – INVCMD PDU format

Field	Size (bytes)	Value
CMD	1	0x0B
REASON	1	Reason code (see Table 26)

5.5.12.1 INVCMD: REASON

This message is transmitted by the NE with the REASON field indicating various error conditions. Defined REASON field codes are listed in Table 26.

Table 26 – INVCMD: REASON codes

Value	Meaning	Response to
0x00	Undefined error	CHNLDESC: unable to execute [1] SET_ADDR: unable to execute [1]
0x01	Invalid parameter	CHNLDESC: invalid frequencies CONTMODE: invalid MODE TALK: invalid ACKSEQ number REG_END: invalid STATUS SET_ADDR: invalid IP address

[1] Parameters are valid but the transponder cannot execute the command for other reasons (e.g. non-volatile write did not succeed)

5.5.13 TIME

The TIME PDU is originated by the HE at its discretion. The expected NE response is an ACK PDU *only* if a unicast address is used. The TIME PDU has the format shown in Table 27. The TIME PDU has a four-byte TOD data field associated with it.

Table 27 – TIME PDU format

Field	Size (bytes)	Value
CMD	1	0x0C
TOD	4	Time of day in POSIX format, most significant byte first

5.5.13.1 TIME: TOD

The TOD field shall contain the time in POSIX format (see Clause A.2) with the most significant byte first. The NE is *required* to synchronize its internal time-of-day clock to this time.

6 MAC protocol operation

This clause covers key operational characteristics to support the interaction between HMS-compliant transponders that interface to OSP NEs and a centralized HE. These procedures are critical to ensure interoperability among multiple NEs.

6.1 Non-volatile parameters

The parameters listed in Table 28 *must* be stored in non-volatile memory for proper initialization of the NE after a power failure. Note that this list is not exhaustive; it simply gives the minimal parameters required for operation after a reset.

Table 28 – Non-volatile parameters

Parameter
Forward channel frequency
Return channel frequency
Return channel power
MAC address
IP address
k parameter (to calculate backoff period before attempting a new transmission in contention mode, see 6.8.5)

The IP address is inserted into the SNMP trap message in the appropriate field.

6.2 Duplex capabilities

All NEs shall support half-duplex operation. There is no requirement for full-duplex operation.

6.3 Packet priorities

The MAC layer shall treat all packets with equal priority regardless of protocol. Both the HE and the NEs shall transmit packets on a first-in, first-out (FIFO) basis.

6.4 Packet reception

The receiving device (NE or HE) looks for a proper synch byte followed by a non-synch byte combination to indicate the start of a packet. Data is discarded until a proper packet start is found. Once a proper packet start is identified, packet length is determined using the length field, reception is completed and the FCS is calculated on the incoming data. The calculated

FCS is compared to the transmitted FCS. If they match, the packet is declared valid and passed on to the appropriate higher layer protocol. If the calculated FCS does not match the transmitted FCS, the packet is discarded. If the FCS is valid, but subsequent decoding of the message shows invalid contents, the packet is discarded. Synch bytes added for data transparency are *not* counted toward the length of the packet, and are *not* included in the FCS calculation for a packet by either the sender or the receiver.

6.5 NE responses

6.5.1 NE processing times – broadcast and multicast messages

The NE shall *never* respond to any message containing a MAC address with the I/G address bit set to 1. This indicates either a multicast address or the broadcast address. However, if the contention state for the NE is turned ON as a result of such a message, the NE is permitted to send TALKRQST messages until the contention state is reset.

Processing times for messages received at the NE must conform to the following rules:

a) an NE must be able to process a packet 250 ms after reception of a MAC packet with the I/G address bit set to 1. See 5.3.3 for details about address.

b) an NE must be able to process a packet 5 s after reception of a SNMP packet with the I/G address bit set to 1.

6.5.2 NE response times – Unicast messages

When an NE receives a MAC PDU management message (protocol identifier 0000) addressed to its unicast address and that requires a response, the NE shall begin to respond within 15 ms, i.e. transmit the first byte of its response. This interval begins following the receipt of a valid forward channel packet and ends when transmission of the response begins on the return channel.

The target response time was chosen to allow a write to non-volatile memory to complete; many of these memory devices require 10 ms to complete.

If an NE does not respond to a MAC management message within 15 ms, i.e. it times out, the HE can assume that the NE will not respond to this particular message. The HE may then initiate an error handling procedure which may attempt to contact the NE again or other NEs around it in the network, or it may invoke other such actions that the HE vendor deems appropriate.

Any time the NE receives a non-MAC PDU management message, i.e. a message with protocol identifier other than 0000, addressed to its MAC unicast address and that requires a response, the NE shall begin to respond within 5 s, i.e. the timeout period shall be 5 s.

6.6 Message sequence numbers and transaction synchronization

The HMS MAC protocol is transaction-based, i.e. every originating message from a “requestor” has a corresponding response from the “responder” regardless of which device originated the message. The sequence field in all HMS MAC packet headers consists of a single byte and defines a message sequence number to ensure message exchanges are synchronized. In order to handle possible loss of messages in either the forward or the return channel, and to avoid duplication of messages at the application layer, all messages have a sequence number. The sequence field in all HMS MAC packet headers and the rules governing its use are described in detail in 5.3.4.

In addition, this HMS MAC specification also defines a one-byte ACKSEQ data field associated with the MAC TALK PDU (see 5.5.6). The ACKSEQ field in the TALK PDU identifies the sequence number of a previous message that *this* packet is acknowledging. The HE uses the TALK PDU to give the addressed NE access to the return channel to transmit a single message while also acknowledging reception of the previous message the NE transmitted.

Table 29 illustrates an example of the usage of the sequence field in the HMS MAC packet headers and the ACKSEQ data field associated with the MAC TALK PDU. The event column is for reference only. The value in parenthesis for the TALK PDU is the value of the ACKSEQ field.

Table 29 – MAC sequence field example (non-contention mode)

Event	HE	Message sequence number		NE	Message sequence number
1	STATRQST	x40	->		
2			<-	STATRESP CHNLRQST = 1	x40
3	TALK (0xFF) [4]	x41	->		
4			<-	SNMP trap 1	x41
5	TALK (0x41) [1]	x42	->		
6			<-	SNMP trap 2 [1]	x42
7	TALK (0x42) [2]	x43	->	*Forward path message lost*	
8	*Timeout* [2]				
9	TALK (0x42) [2]	x43	->		
10			<-	SNMP trap 3	x43
11	TALK (0x43)	x44	->		
12	*Return path message lost* [3]		<-	SNMP trap 4	x44
13	*Timeout* [3]				
14	TALK (0x43) [3]	x44	->		
15			<-	SNMP trap 4	x44
16	TALK (0x44)	x45	->		
17			<-	NAK	x45

[1] Normal case: The sequence number is different from the last one seen, so the NE will increment its internal pointer to the next message to be transmitted.

[2] The NE did not see this message at all, so the transaction does not complete. The HE must retransmit its message using the same sequence number.

[3] The trap was lost in the return path. The HE times out, but does not know which message (forward path or the return path) was lost. Retry of the TALK is required. The NE will see that the sequence number is the same as the last one, so it will simply resend its last message.

[4] The HE has no previous message to acknowledge, so the value of the ACKSEQ field is 0xFF

6.7 Solicited messages

Solicited messages are packets that are sent in response to a HE query. The HE does not transmit an ACK PDU in response to these packets.

6.8 Autonomous (unsolicited) messages

Autonomous, or unsolicited messages are packets that are generated automatically by the NE, for example the result of an unexpected alarm condition occurring at the NE. An NE must signal the HE with the TALKRQST PDU when the NE contention state is ON (C_C = 1). Only the TALKRQST PDU is permitted when the NE contention state is ON and no alarm information is transmitted since delivery to the HE is not guaranteed (collisions may occur). The HE must send an ACK message back to the NE when it receives a TALKRQST PDU. Only a single packet requiring an ACK response may be outstanding at the NE at any time. Retry packets are retransmissions of previously sent autonomous messages for which an ACK PDU was not received. Subclauses 7.8.1 through 7.8.7 describe how autonomous messages and collisions are handled in this MAC.

6.8.1 NE contention state

Each NE has a contention state (C_C). The contention state indicates the following:

a) contention state is ON: the NE is permitted to transmit unsolicited messages on the return channel;

b) contention state is OFF: the NE may transmit only solicited messages. It cannot transmit unsolicited messages;

c) at NE boot, the NE contention state is initialized to OFF.

The contention state for an NE is determined by

a) the address used to access this NE (unicast, multicast, or broadcast); and

b) the value of the MODE field in the CONTMODE PDU that addressed this NE. Refer to 5.5.7.

The contention state setting is persistent across forward path transmissions. See Table 30.

Table 30 – Contention state settings versus forward channel packets

Forward path message	Address	CONTMODE MODE value	NE contention state C_C		
			NE X	NE Y	NE Z
1	Broadcast	0 (off)	OFF	OFF	OFF
2	Unicast X	0 (off)	OFF	OFF	OFF
3	Unicast X	1 (on)	ON	OFF	OFF
4	Unicast Y	0 (off)	ON	OFF	OFF
5	Unicast Y	1 (on)	ON	ON	OFF
5	Multicast (X,Y)	0 (off)	OFF	OFF	OFF
6	Multicast (Y,Z)	1 (on)	OFF	ON	ON
7	Broadcast	2 (inh)	OFF	OFF	OFF
8	Broadcast	3 (res)	OFF	ON	ON
9	Multicast (X,Y)	1 (on)	ON	ON	ON
10	Multicast (Y,Z)	0 (off)	ON	OFF	OFF
11	Broadcast	1 (on)	ON	ON	ON
12	Broadcast	0 (off)	OFF	OFF	OFF
ON – the NE is permitted to send any unsolicited messages it has for any protocol. OFF – the NE is NOT permitted to send any unsolicited messages.					

6.8.2 Collisions

A collision is defined as multiple unsolicited messages from different NEs arriving at the HE receiver simultaneously so that none of the messages is received properly. True collisions should occur only during a period when multiple NEs on the same return path have the contention state ON. It is also possible that improper reception of an unsolicited message from the NE is a result of message corruption during transmission due to noisy conditions in the return channel such as ingress or impulse noise. Although message corruption in the latter case is not a direct result of a collision, both conditions will force re-transmission of the corrupted message.

6.8.3 HE collision detection

The HE may declare a collision. How this is done is at the vendor's discretion. This standard does not describe what an HE should do in the event of a collision. However, the following collision detection techniques are possible:

a) Received Signal Strength Indication (RSSI) higher than “normal". Since the arriving return channel packets have a variable size and arrival time, the HE may utilize a power detector on a receiver to roughly detect the beginning and the end of the received packet on the return channel;

b) bytes not received in time (inter-byte gaps), or entire packet not received in time;

c) framing errors;

d) improper protocol; and

e) invalid FCS.

6.8.4 NE collision indication

The HE must respond with an ACK message to all return channel packets that require it within a predetermined timeout period. Currently, only the TALKRQST PDU requires an ACK. Collisions on the return channel are indicated to the originating NEs by the *lack* of the required ACK message from the HE because no specific indication of a collision is provided at the MAC layer.

The non-receipt of the HE ACK message within the timeout period indicates to the NE that something, for example a collision, excessive ingress noise, or other unknown condition, has prevented the proper reception of the return channel packet at the HE, and the NE must retransmit the message (see 6.8.5). This collision detection mechanism is part of the general technique known as ALOHA to support multiple user access to a common transmission channel.

6.8.5 Backoff algorithm

The “Backoff” state is defined as the contention state when C_C = 1 and the NE is waiting for a random delay period *Y* to elapse, after which it will attempt to send a message again. The backoff or random delay *Y* is calculated using the following formula:

Y = random[1, 2^k] * BackoffPeriod,

where

Y	=	Period of time to wait in milliseconds (backoff)
k	=	0 to 15 (default value of 6, default maximum is 15, absolute maximum is 15)
random[ ]	=	Random number in range of 1 to 2^k
BackoffPeriod	=	Variable in milliseconds for *incremental* backoff time to wait. Default value is 6 ms, for a maximum backoff *Y* of approximately 197 s.

6.8.6 Backoff state machine description

When the NE has a packet to be transmitted *for the first time* when C_C = 1, the NE must first enter the “backoff” state. For this first backoff, the initial value of *k* currently set is used (default value is 6). When the calculated backoff period *Y* has elapsed, the NE may then send the packet

After the NE sends a packet requiring an ACK, the NE waits for the ACK PDU from the HE to determine if the transmission was successful. If the NE receives the ACK PDU within the predetermined timeout period following the transmission of the reverse channel packet, it declares a successful transmission and discards the successful packet.

Note that if the packet was successfully transmitted without a collision, then the HE received the packet *while* it was being transmitted. Therefore, the time required to receive the required ACK packet is equal to [processing time of the HE] + [time required to transmit ACK packet] + [propagation delay].

If the transmission was not successful, as indicated by non-receipt of the ACK packet within the timeout period, the NE will delay for a new backoff period *Y*. In this case, the NE increments *k* by 1 (increasing the random number range by a factor of 2) to a maximum of 15 (or the value currently set in SCTE HMS COMMON MIB, *HMS Common Management Information Base*), calculates a new backoff period *Y*, enters the "Backoff" state again until period *Y* expires, then retransmits the packet. It then waits again to see if the retransmitted packet reaches the HE successfully (confirmed by reception of the ACK PDU within the timeout period). This process continues until any of the following conditions occur:

a) an ACK PDU is received for this packet (indicating the packet was received successfully); or

b) the maximum allowed number of MAC layer transmission retries is exceeded; or

c) CC is set to 0.

After the maximum allowed number of MAC layer transmission retries has been exceeded, the NE gives up this attempt and no further transmissions are permitted until a backoff reset occurs (see 6.8.7). When the backoff state machine is reset, the NE may attempt to send this packet again.

If the correct ACK PDU is received late during the "backoff" state the ACK is accepted and it is assumed that the original packet was received successfully.

If C_C is explicitly set to 0 by a new CONTMODE message or after expiration of the duration timer (see 5.5.7), then retries are cancelled. This also resets the backoff state machine to its initial starting point.

IMPORTANT NOTE

Although the term "random" has been used in this subclause, it is recognized that it is extremely difficult to implement a true random number generator. Because of this difficulty, it is incumbent upon the vendors of OSP monitoring equipment to implement the best possible pseudo-random number generator available. This standard cannot and does not dictate how this pseudo-random number generator works.

6.8.7 Backoff reset

The backoff state machine is reset in the NE upon any of the following conditions:

a) when the NE has a new/different packet to be transmitted for the first time when C_C = 1; or

b) upon expiration of the duration timer (see 5.5.7); or

c) upon receipt of any CONTMODE PDU; or

d) when the NE responds with a NAK PDU in response to a TALK PDU.

The resetting of the backoff state machine includes the timers and other logic in use for the transmission of unsolicited messages and implementation of the backoff algorithm. The resetting of the state machine permits the NE to attempt to resend a message that had previously failed due to exceeding the allowed MAC layer transmission retry limit.

6.8.8 Parameters

The parameters controlling autonomous message transmission for the HMS MAC layer are defined explicitly in Table 31. See also the latest revision of document *Common Management Information Base*.

Table 31 – Backoff state machine parameters

Parameter name	Description	Value
AckTimeout	Time that the NE waits for a HE ACK message after completing a return channel packet transmission	15 ms (HE processing time) +3 ms (time to transmit ACK message) +1 ms (propagation delay) Default: 19 ms

BackoffPeriod	Basic unit of time that the NE waits after *not* receiving an HE ACK message prior to message re-transmission	6 ms (see 6.8.5)
k	Controls the size of the random number window	Default value: 6 Absolute maximum value: 15 Default maximum value: 15
MaxMACLayerRetries	Number of times the NE will attempt to transmit its autonomous message	This parameter must default to a value of 16
Y	Backoff time resulting from backoff algorithm calculation	Calculated

6.9 Return channel transmissions

There are two times when an NE is permitted to transmit:

a) contention state in the NE is OFF

the NE may transmit a single return channel packet any time following the reception of a valid forward channel packet requiring NE response until NE access is turned OFF by a subsequent packet that disables its access. For example, a forward channel packet addressing a different NE. See Figure 8.

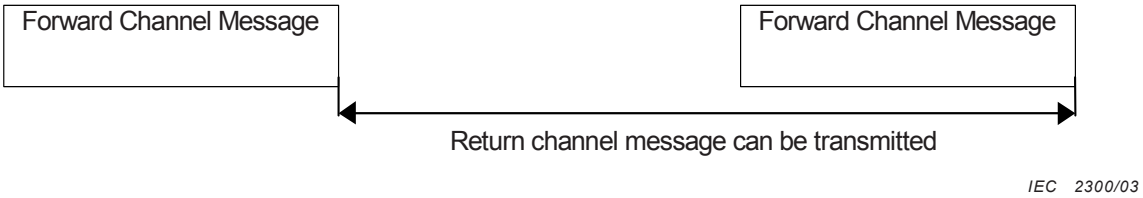


Figure 8 – Return channel transmission permitted

b) contention state in the NE is ON

the NE may transmit a return channel packet any time following the reception of a valid CONTMODE PDU that turns the contention state ON in the NE until its access is turned OFF by either a subsequent CONTMODE PDU that disables its access, or expiration of the duration timer for C_C = 1 (as set by the CONTMODE PDU). Note that return channel packet transmission in this case must follow the rules of contention and backoff.

6.10 MAC state machines

The NE shall implement the state diagrams included in this clause.

6.10.1 Contention state machine

Figure 9 illustrates the state diagram for the contention state machine.

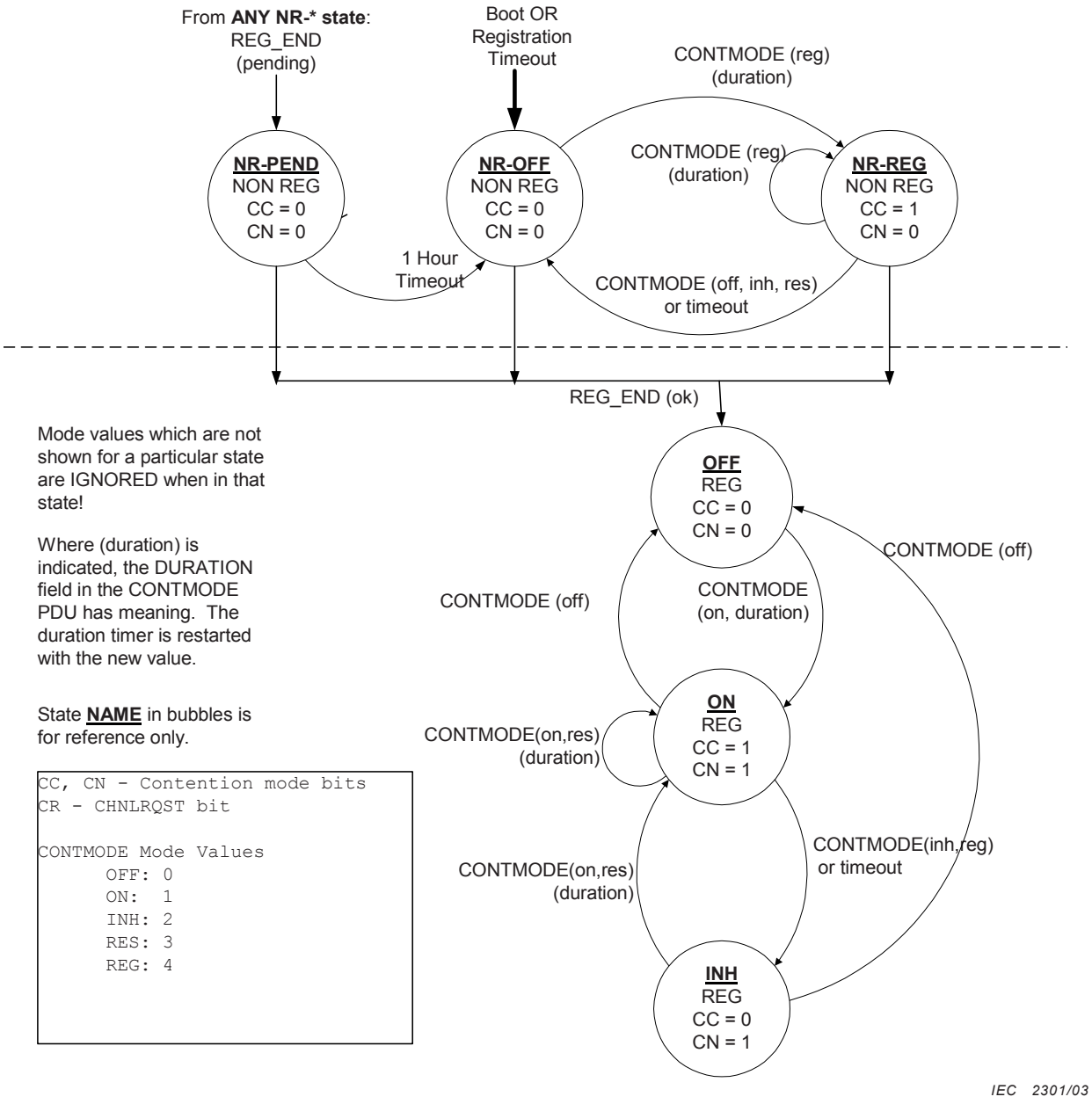


Figure 9 – Contention state diagram

6.10.2 Backoff state machine

Figure 10 illustrates the state diagram for the backoff state machine.

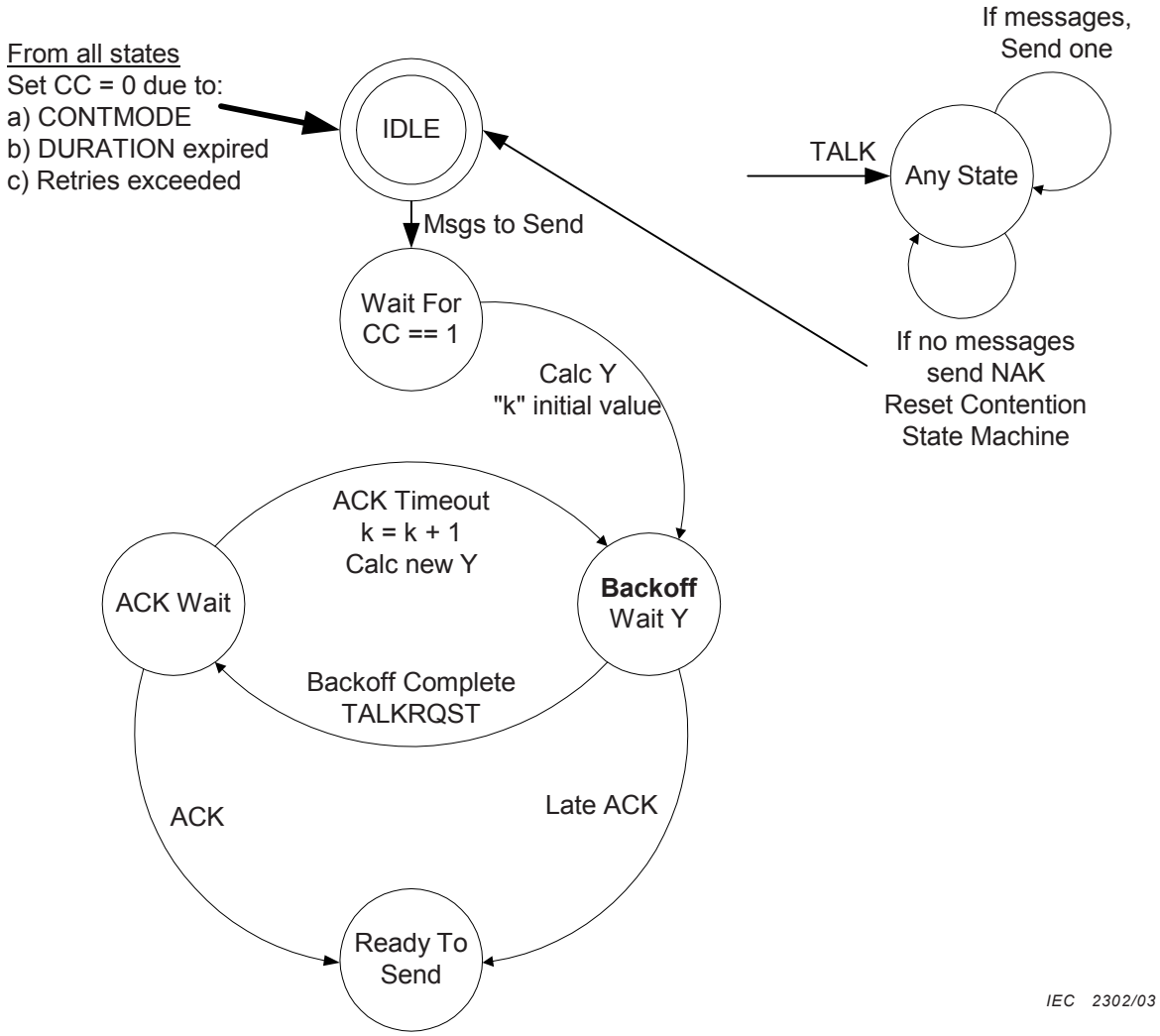


Figure 10 – Backoff state diagram

Annex A
(informative)

Operational details

A.1 Introduction

This annex addresses various operational aspects concerning implementation of the MAC protocol. Neither the main section of these specifications nor RFC 1157, *A Simple Network Management Protocol (SNMP),* specifically addresses these issues.

A.2 Time of day

The NE is required to maintain a time of day clock so that alarms may be time-stamped. However, the NE is not required to have a real-time hardware clock. After NE power-up, the clock should begin at 0 (midnight January 1, 1970) and will maintain time from there until the time is synchronized by the management system. Vendors should specify the accuracy for their clock. A resolution of 1 s is required. The drift of the clock (unsynchronized) should be no more than 30 s over a period of 24 h.

A.2.1 Integer representation

Any MIB variable specifying time in an Integer format will use the POSIX standard format of the number of seconds since January 1, 1970 and requires a 32-bit integer at a minimum. See also document COMMON MIB, *Common Management Information Base.*

A.3 Firmware downloads

Remote NE firmware downloads, i.e. downloads performed over the RF serial link, should be accomplished via SNMP. The exact mechanism is detailed in document DOWNLOAD MIB, *Transponder Firmware Download Management Information Base.*

A.4 NE addressing

Each NE is assigned a unique IEEE MAC address as specified in 5.3.3 of this standard. However, for addressing the NE in a system, two approaches are possible. Neither has any effect on the NE since the NE responds only to MAC addresses.

A.4.1 Direct addressing using individual IP address

Element Management Systems (EMSs) that support assignment of individual IP addresses to each NE within a MAC layer domain may find this a suitable approach. A unique IP address is assigned to each NE through the registration mechanism. The NE may then be addressed directly by IP address with the HE acting as a router or bridge.

SNMP trap messages with NE alarms will have the IP address of the NE in the trap. The NE is not required to have a full IP protocol stack, however this standard does provide for a mechanism to support such implementations (see 5.3.2).

A.4.2 Proxy addressing using common IP address

EMSs that assign common IP addresses to support communications to all NEs within a MAC layer domain may find this a suitable approach. A common IP address is used to channel all communications between an HE and multiple NEs. Assignment and management of individual IP addresses for each NE is not required.

The HE serves as an SNMP proxy agent for the NEs. All SNMP messages sent to the HE contain the MAC address of the NE in the community string of the SNMP PDU. The format of this string does not matter as long as it uniquely identifies the NE to the HE. A recommended format for identifying an NE with MAC address 12-34-56-78-9A-BC is “123456789ABC”. The HE then performs a lookup function in an internal database using this community string to find the NE MAC address and sends the new SNMP PDU to the NE that was identified.

The community string has a maximum size of 64 bytes. See also document COMMON MIB, *Common Management Information Base.* An NE should ignore the community string in SNMP packets it receives. The NE should set the SNMP packet community string for the GetResponse PDU to the same value it received for the originating PDU, i.e. a GetRequest PDU.

A.5 Alarm processing HMS MAC protocol

A.5.1 Managed parameter properties

Document SCTE HMS PROPERTY MIB, *HMS Alarm Property Management Information Base* defines the properties that may be associated with each managed NE parameter. The properties defined in the SCTE HMS PROPERTY MIB can be applied to *any* parameter because the index to the MIB is the object identifier of the parameter. See Figure A.1. In this example, the property analogAlarmLO is associated with managed NE parameter psOutputVoltage.

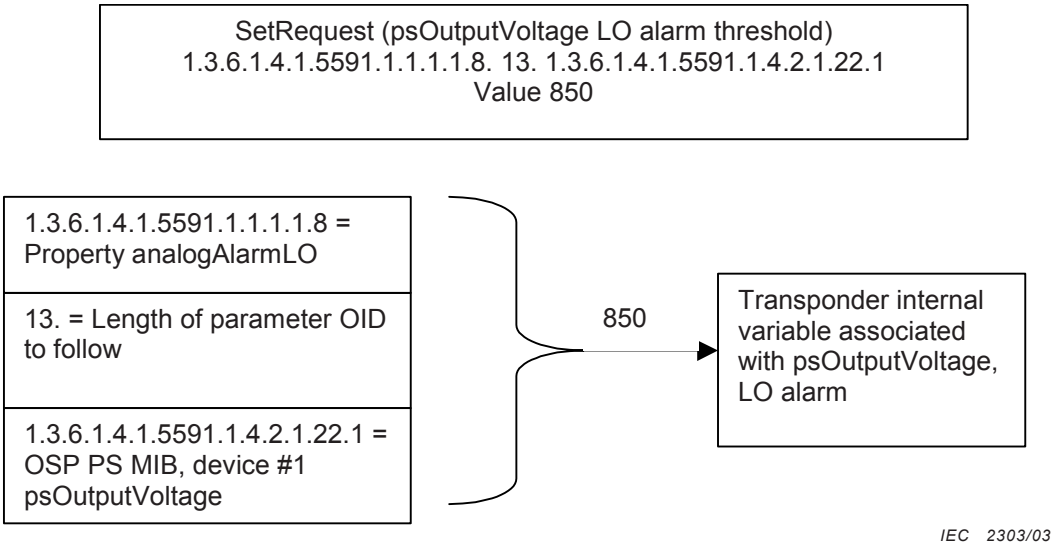


Figure A.1 – Property MIB usage

It is up to the vendor to indicate which properties apply to any given parameter. See Table A.1 for a list of properties that can be applied. For example, analogue properties need not apply to a digital parameter (e.g. tamper switch).

NOTE NE vendors may, at their discretion, support *additional* properties for parameters through a vendor-specific property MIB. This standard *recommends* that the same mechanism described here be used to associate the additional properties with each managed NE parameter.

Table A.1 – Properties

Property name	Description
LOLO	Alarm threshold for the extreme low condition
LO	Alarm threshold for the low condition
HI	Alarm threshold for the high condition
HIHI	Alarm threshold for the extreme high condition
Deadband	Deadband that applies to all alarm thresholds. After an alarm occurs, the parameter value must pass back over the alarm threshold by this amount for the alarm to be cleared.
Alarm enable	Permits enabling and disabling of specific alarms: Bit 0: LOLO alarm Bit 1: LO alarm Bit 2: HI alarm Bit 3: HIHI alarm Bit 4: Reserved Bit 5: Reserved Bit 6: Reserved Bit 7: Reserved

NOTE Nothing in this standard implies the severity of any particular alarm. See document SCTE HMS PROPERTY MIB, HMS Alarm Property Management Information Base for complete details about each field.

The thresholds and the dead band for any parameter must be of the same precision as the parameter. For example, if battery voltage value V_{DC} is presented with two decimals, then the thresholds and dead band must also be presented with two decimals.

A.5.2 Alarm thresholds and operation

In the event that an alarm condition is detected, the alarm thresholds function as follows:

a) LOLO: when a parameter value crosses this threshold (value < threshold), the alarm will be indicated. The parameter returns from alarm when (value > threshold + dead band);

b) LO: when a parameter value crosses this threshold (value < threshold), the alarm will be indicated. The parameter returns from alarm when (value > threshold + dead band);

NOTE If a parameter value crosses directly to the LOLO alarm state, a LO alarm should not be triggered. For example, consider a parameter having LOLO and LO thresholds of 5 and 10 respectively and a deadband of 1. The parameter value is quiescent at a value of 15. Suddenly, the value drops to 2 with no intermediate values sensed. In this case, *only* the LOLO alarm should be triggered. If the value subsequently rises to a value of 7, the LO alarm should then be triggered. Conversely, if a LO alarm occurs first and the value progresses over the LOLO alarm threshold, that alarm should then be triggered.

c) HI: when a parameter value crosses this threshold (value > threshold), the alarm will be indicated. The parameter returns from alarm+ when (value < threshold – deadband);

d) HIHI: when a parameter value crosses this threshold (value > threshold), the alarm will be indicated. The parameter returns from alarm when (value < threshold – deadband). Just as in the case of LO and LOLO, an excursion past the HI threshold directly to the HIHI alarm level will cause only a HIHI alarm.

Only one alarm state should be active at any time. In the note above for the LO alarm, only the LO *or* the LOLO alarm is active and not both at the same time. In all cases, disabling the alarm *while* the alarm is active should generate the following actions:

a) the alarm is reset to the nominal state and a trap is issued;

b) the alarm is deleted from the current alarm table; and

c) the alarm remains in the alarm log table (this is a history table).

A.5.3 Alarms MIB information

Document SCTE HMS ALARMS MIB, *HMS Alarms Management Information Based,* is simple and provides for organized and effective alarm retrieval. The contents of the NE alarm list are defined and transferred as an octet string containing all of the recorded information for a particular alarm. This permits the efficient retrieval of *all* the information for a given alarm. The alarm list acts as a simple circular first in first out (FIFO), wrapping around and overwriting alarms in the list. Alarms are not removed from the list.

A.5.4 NE alarm processing

The NE must not send any SNMP traps or perform alarm processing (detection, etc.) until a REG_END PDU is received with STATUS of 0 (SUCCESS). At that time, alarm processing is governed by the commonAlarmDetectionControl variable as defined in document COMMON MIB, *HMS Common Management Information Base* as well as all other applicable MIB variables. Upon detecting an event, the NE stores it in an internal list for transmission later. Alarm notification and retrieval mechanisms and relevant examples are described in A.5.5.

A.5.5 Alarm notification and retrieval

The MAC layer provides a “notify and gather” mechanism where the HE is notified that an NE wants to transmit unsolicited messages. The HE can retrieve these messages by permitting the NE to send the messages reliably in a non-contention environment. The HE may then forward these messages via SNMP trap mechanism to a higher layer EMS or cache them. Note that there is no requirement to perform message retrieval in a contention-free environment; however, that method is recommended.

There are two methods for determining that an NE has alarms to be transferred. These are described in A.5.5.1 and A.5.5.2.

A.5.5.1 Notification – Polled mode

The STATRESP PDU serves as the message *notification* mechanism via the CHNLRQST bit (see 5.5.4). In a strictly poll-based implementation of the HMS MAC protocol, the STATRQST/STATRESP transaction supports background polling and alarm notification. When the HE receives a STATRESP PDU message from an NE with the CHNLRQST bit in the STATUS field set to 1, it should add this NE to a list of NEs requesting permission to transmit unsolicited messages and process this list at its convenience. If the list is empty, the NE can be processed immediately, i.e. it can be granted immediate access to the return channel to transmit a single message.

A.5.5.2 Notification – Contention mode

The TALKRQST PDU originated from an NE serves as the message notification mechanism when contention mode is in the ON state (see 5.5.5). When the HE receives a TALKRQST PDU message, it must respond with the ACK PDU to signal the NE that the message has been received and that no additional TALKRQST PDU is necessary. Only the TALKRQST PDU is permitted when the NE contention state is ON (see 6.8) and no alarm information is transmitted until after the HE explicitly grants the NE access to the return channel.

A.5.5.3 Retrieval

To retrieve unsolicited messages from an NE, the HE can at its discretion first ensure that return channel contention is turned OFF for all NEs within the particular MAC layer domain through generation of the CONTMODE PDU with MODE value of OFF or INH (see 5.5.7). Following this, the HE must:

a) transmit a TALK PDU to the NE to grant it immediate access to the return channel for transmission of a single message (packet);

b) process the received packet from the NE. Typically, this packet will be of protocol type SNMP trap over serial; and

c) repeat sequences 1 and 2 at its discretion until the NE has no more messages to send. At this point, the NE response to the HE TALK PDU is a NAK PDU. Note that steps 1 and 2 constitute a single HMS MAC protocol transaction.

This standard does not state in what order the NE alarms should be sent. However, for consistency, it is *highly* recommended that the alarms be transmitted in the order in which they occurred. See A.5.3 for additional detail on alarm retrieval during alarm overflow situations.

A.5.5.4 Alarm and message flows

Table A.2 illustrates the expected message flow between HE and NE in a poll-based implementation of the HMS MAC protocol. In this instance, HE reception of a STATRESP PDU message with the CHNLRQST bit in the STATUS field set to 1 signals the HE that the NE has one or more messages to transmit. The HE immediately grants the NE access to the return channel via the TALK PDU to transmit a single message at a time until the NE generates a NAK PDU in response to the HE TALK PDU to signal it no longer has any outstanding messages to transmit. The value in parentheses for the TALK PDU is the value of the ACKSEQ field.

Table A.3 illustrates the potential message flow between HE and NE in a contention-based implementation of the HMS MAC protocol. This example assumes contention has been enabled on the return channel and one or multiple NEs signals the HE via the TALKRQST PDU that it has one or more messages to transmit. The HE acknowledges each TALKRQST PDU via an ACK PDU back to each of the NEs.

Note that in Table A.3 that for NEs B and C, even though initial transmissions over the return channel result in a collision, the TALKRQST PDUs are successfully transmitted after invoking the HMS MAC backoff and retransmission algorithm (see 6.8). Following transmission of ACK PDUs, the HE in this example turns return channel contention OFF via the CONTMODE PDU first. It then grants each NE access to the return channel via the TALK PDU to transmit a single message at a time until the NE generates a NAK PDU in response to the HE TALK PDU to signal it no longer has any outstanding messages to transmit. The process continues until all outstanding NE transmissions have been completed.

Table A.2 – Alarm notification and retrieval – Polled mode

HE	Message sequence number		To/from	NE	Message sequence number	CHNLR QST bit	Contention
STATRQST	41	->	A			0	0
		<-	A	STATRESP	41	0	0
				Alarm detected		1	0
STATRQST	42	->	A			1	0
		<-	A	STATRESP CHNLRQST = 1[1]	42	1	0
TALK (0xFF)	43	->	A			1	0
		<-	A	SNMP Trap[2]	43	1	0
TALK (0x43)	44	->	A			1	0
		<-	A	SNMP Trap[2]	44	1	0
TALK (0x44)	45	->	A			0	0
		<-	A	NAK[3]	45	0	0

[1] Notification

[2] The HE is simply giving permission for the NE to transmit uninterrupted. The actual message could be any protocol.

[3] This is used to indicate that the NE has no more messages to be transmitted.

Table A.3 – Alarm notification and retrieval – Contention mode

HE	Message sequence number		To/from	NE	Message sequence number	CHNLRQST bit	Contention
CONTMODE ON	0	->	*			0	1
		<-	A	TALKRQST[1]	15	A=1	1
ACK	15	->	A			A=1	1
		<-	B	TALKRQST[1]	25	A,B,C=1	1
		<-	C	TALKRQST[1]	35	A,B,C=1	1
B and C collide, backoff						A,B,C=1	1
Time passes						A,B,C=1	1
		<-	B	TALKRQST[1]	25	A,B,C=1	1
ACK	25	->	B			A,B,C=1	1
		<-	C	TALKRQST[1]	35	A,B,C=1	1
ACK	35	->	C			A,B,C=1	1
CONTMODE OFF	0	->	*	Disables contention for this return path		A,B,C=1	0
TALK(0xFF)	43	->	A			A,B,C=1	0
		<-	A	SNMP trap[2]	43	A,B,C=1	0
TALK(0x43)	44	->	A			A,B,C=1	0
(message garbled)		<-	A	SNMP trap[2]	44	A,B,C=1	0
Timeout occurs						A,B,C=1	0
TALK (0x43)	44	->	A	Retry		A,B,C=1	0
		<-	A	SNMP trap[2]	44	A,B,C=1	0
TALK (0x44)	45	->	A			A,B,C=1	0
		<-	A	SNMP trap[2]	45	A,B,C=1	0
TALK (0x45)	46	->	A	A has no more alarms to send		A=0 B,C=1	0
		<-	A	NAK[3]	46	B,C=1	0
Repeat sequence			B			B,C=1	0

[1] Notification

[2] The HE is simply giving permission for the NE to transmit uninterrupted. The actual message could be any protocol.

[3] This is used to indicate that the NE has no more messages to be transmitted.

A.6 Automatic channel discovery

This version of the MAC protocol defines a CHNLDESC PDU (see 5.5.11) that the HE originates to communicate forward and return channel frequencies in use to the NE. This can support optional implementation of an automatic channel discovery feature in the NE. At the vendor's discretion, the NE may be configured to automatically search for the forward and return channel frequencies currently in use. Since the HE is required to periodically transmit the CHNLDESC PDU, the following mechanism is suggested:

a) the NE starts by choosing a forward path channel and monitors it for valid forward path messages over a pre-determined time interval. This standard does *not* specify how a forward channel may be chosen or how long an NE should stay tuned to a particular forward channel;

b) once the NE has found a forward path channel with valid MAC messages, it listens for the CHNLDESC PDU for up to 35 s. If no PDU is heard, the NE may move onto a different forward path channel at its discretion. This standard does not specify how another forward channel may be chosen;

c) after hearing a CHNLDESC PDU with valid forward and return channel frequencies, the NE should tune its return path transmitter to the frequency specified and attempt the auto-registration procedure described in A.7;

d) if the auto-registration procedure fails, the NE may attempt to try another valid forward path channel at its discretion. This standard does not specify what the NE should do.

A.7 Auto-registration

This version (1.0) of the HMS MAC protocol requires that NEs register with the HE and provides the procedure and mechanisms to perform this function. Following NE reboot either by power-up, watchdog reset, commanded reset, manual reset, or other method, it should perform any required internal initialization. After internal initialization is complete, the NE *may* use an automatic channel discovery mechanism similar to the one described in A.6 to search for the forward and return channel frequencies currently in use. Alternatively, the NE may use frequencies already provisioned.

Once the NE has found a valid set of frequencies, it requests registration. The following sequence and the example in Table A.4 illustrate a *potential* implementation of the auto-registration process:

a) the HE periodically transmits a CONTMODE PDU with MODE value of 4 (REG). Only those NEs that are *not* yet registered may respond;

b) the NE indicates it has messages to transmit by transmitting a TALKRQST PDU;

c) the HE transmits an ACK PDU to indicate to the NE that its TALKRQST PDU was received;

d) the HE eventually transmits a CONTMODE PDU with MODE value of INH to turn off registration requests;

e) the HE eventually transmits a TALK PDU to the NE;

f) the NE transmits a REG_REQ message with the IP address of the NE as it is currently configured. Refer to 5.5.8 of this standard;

g) the HE transmits a TALK PDU to the NE with the sequence number of the transaction in steps e) and f). The NE responds with a NAK indicating no more messages;

h) the HE determines the correct IP address for the NE. How the correct IP address is determined is beyond the scope of this standard;

i) optionally, the HE transmits a SET_ADDR PDU to the NE with the correct IP address. The NE transmits an ACK PDU back to the HE upon successful processing of the SET_ADDR PDU. Refer to 5.5.9 of this standard. Note that this transaction is not required if the HE determines that the NE is already configured;

j) the HE transmits a REG_END PDU with the appropriate status value (SUCCESS, DENIED, FAILED, or PENDING). The NE responds with an ACK PDU. Refer to 5.5.10 of this standard;

k) if the NE registration request was denied, the NE may opt to use the CHNLDESC PDU mechanism to search for another channel, or it may request registration on the current return channel again. If the registration request failed, the NE must wait until the next registration opportunity. If the registration request is pending, the NE must not send any further registration requests. *The NE must not send any SNMP traps or perform alarm*

processing (detection, etc.) until a REG_END PDU is received with STATUS of 0 (SUCCESS);

l) the HE restores the contention mode of the system using the CONTMODE PDU with MODE value of RES;

m) if the HE wants the contention mode of the NE turned ON, the HE transmits the CONTMODE PDU with MODE value of ON to the NE. This should be done using the unicast address of the NE. The NE must respond with an ACK PDU;

n) when ready, the NE must generate a SNMP trap. The mechanisms described in A.5.5 must be implemented for alarm notification and retrieval. *No SNMP traps are permitted until the REG_END transaction is completed*;

o) the HE performs any other configuration required by the NE.

Table A.4 – Auto-registration implementation example

HE	Message sequence number		To/from	NE	Message sequence number	CHNLRQST bit	Contention
CONTMODE REG	00	->	*			0	1
		<-	A	TALKRQST[1]	1	1	1
ACK	1	->	A			1	1
CONTMODE INH1		->	*			1	0
TALK (0xFF)	42	->	A			1	0
		<-	A	REG_REQ	42	0	0
TALK (0x42)	43	->	A			0	0
		<-	A	NAK	43	0	0
SET_ADDR	44	->	A			0	0
		<-	A	ACK	44	0	0
REG_END (0)	45	->	A			0	0
		<-	A	ACK	45	0	0
CONTMODE RES	00	->	*				
CONTMODE ON[2]	46	->	A				
		<-	A	ACK	46		

[1] This is required to turn OFF the registration contention mode.

[2] This transaction is optional and it depends on whether the HE wants the NE in contention mode or not.

A.8 Configuration changes and SNMP trap generation

The NE must be capable of recognizing configuration changes and notifying the upstream EMS of this event. To accomplish this, the NE must maintain a check code value of 32 bit in size. See also SNMP commonCheckCode variable definition in document SCTE HMS COMMON MIB, *HMS Common Management Information Base.* The algorithm and data used to calculate this check code is vendor-specific. One suggested approach is CCITT CRC-16 as implemented for HMS MAC layer packets (see 5.3.7). The check code is calculated under any of the following conditions:

a) upon NE reset (power-up or other reset);

b) an SNMP request for the check code; or

c) at the vendor’s discretion.

The NE must keep track of the last check code it calculated. It must generate appropriate hmsColdStart and hmsWarmStart SNMP traps as defined in document SCTE HMS COMMON MIB, *HMS Common Management Information Base.*

The NE must generate the hmsColdStart SNMP trap under any of the following conditions:

a) the NE has been reset and the calculated check code differs from the last saved check code; or

b) the check code was calculated at the vendor's discretion and it differs from the last saved check code.

The NE must generate the hmsWarmStart SNMP trap under the following conditions:

a) the NE has been reset and the calculated check code is the same as the last saved check code.

The hmsColdStart and hmsWarmStart traps will *not* be generated by a simple SNMP Get of the check code. Once the appropriate SNMP trap has been generated, the newly calculated check code should be stored in non-volatile memory.

———————

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL