Data-Over-Cable Service Interface Specification

Cable Modem Telephony Return Interface Specification

SP-CMTRI-I01-970804

INTERIM

Notice

Document Status Sheet

Document Control Number:	SP-CMTRI-I01-970804			
Reference:	Cable Modem Telephony Return Interface Specification			
Revision History:	I01 970804 Released for publication			
Date Posted:	August 4, 1997			
Status Code:	~~Work in Process~~	~~Draft~~	**Interim**	~~Released~~
Distribution Restrictions:	~~Arthur D. Little only~~	~~ADL/MCNS~~	**MCNS/Vendor**	~~Public~~

Key to Document Status Codes

Work in Process An incomplete document, designed to guide discussion and generate feedback, that may include several alternative requirements for consideration.

Draft A document in specification format considered largely complete, but lacking review by DOCSIS and vendors. Drafts are susceptible to substantial change during the review process.

Interim A document which has undergone rigorous DOCSIS and vendor review, suitable for use by vendors to design in conformance with, and suitable for field testing.

Released A stable document, reviewed, tested and validated, suitable to enable cross-vendor interoperability.

Contents

Figures

Tables

1 Specification Overview

1.1 Terminology

In this specification, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word or the adjective "REQUIRED" means that the item is an absolute requirement of the specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of the specification.
"SHOULD"	This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

1.2 System Overview

1.2.1 System Components

Figure 1-1 depicts a high-level block diagram of the Data-Over-Cable system using a return path via the public switched telephone network (PSTN). The system consists of the Cable Modem Termination System (CMTS), the cable network, the Cable Modem (CM), the PSTN, and the Telephone Remote Access Concentrator (TRAC). While Figure 1-1 shows the telephone modem integral to the CM, this specification allows the telephone modem to be a unit external to the CM.

The CMTS and the TRAC may be collocated at the cable headend, or the TRAC may be located elsewhere and have routing associations to the CMTS. The CMTS and TRAC together are called the Telephone Return Termination System (TRTS), whether they are collocated or not. TRACs may be in different geographic locations. Content, operations, administrative and maintenance servers may also be in different locations. These access points are

internetworked to one or more CMTSs and cable headend access points. Such configurations may be “one to one”, “one to many,” or “many to many.” They may be interconnected by various LAN and WAN media.

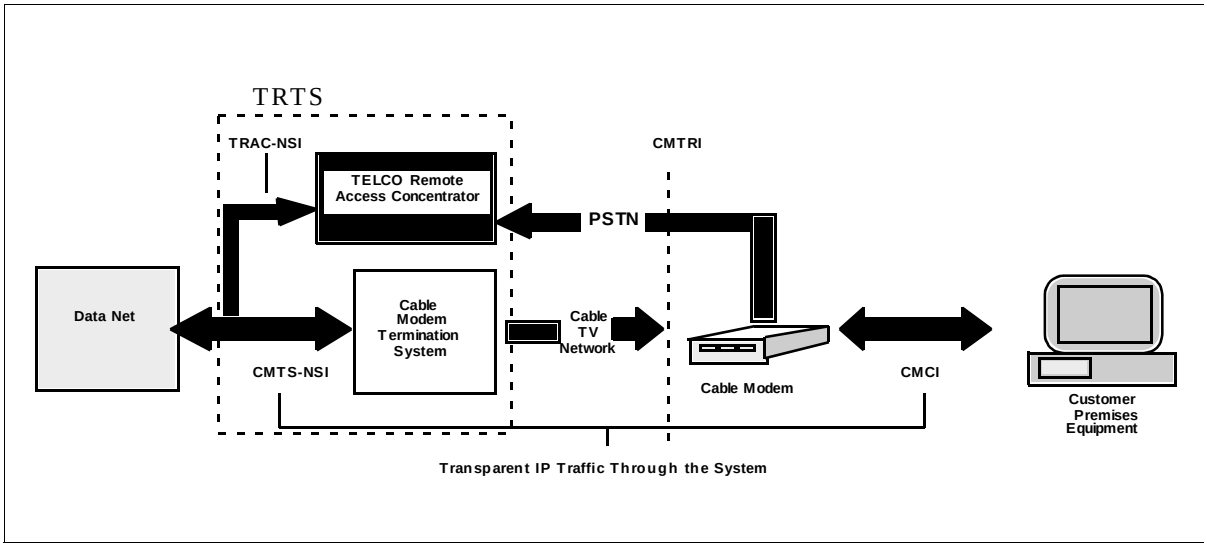

Figure 1-1. Telephone Return Delivery System Block Diagram

The data path through the system is illustrated below:

- An IP datagram from the Internet, destined for the CPE, enters the CMTS via the CMTS-NSI.
- The CMTS encodes the IP datagram per the MCNS RF Interface Specification [MCNS2], and transmits it down the cable plant.
- The CM recognizes the frame as destined for an attached CPE address. The CM decodes the frame, and passes it to the CPE via the CMCI.
- The CPE responds to the frame. The response enters the CM via the CMCI.
- The CM encapsulates the response IP datagram in a Point-to-Point Protocol (PPP) [RFC-1661,1662,1663] frame, and transmits it to the TRAC across the PSTN.
- The TRAC decodes the IP datagram and forwards it to its destination via the TRAC-NSI. The interface at the TRAC-NSI is implementation-dependent and not covered by this specification.

In addition to the data path in the above example, there are several management paths in the telephone return system. These include the PPP negotiations between the CM and the TRAC, as well as SNMP management paths from a network management console to the CMTS, the TRAC, and the CM.

Figure 1-2 is a more detailed diagram which illustrates how this architecture looks in the case where the TRAC and the CMTS are physically collocated. Note that although the figure

shows both telephone and RF return paths, a CMTS MAY support only a downstream RF path.

This specification supports coexistence of cable return and telephone return CMs, using the same downstream RF channel. In order for a CMTS to support both telephone return and two-way CMs it MUST do IP forwarding. Similarly, a CM MAY provide support for both upstream data paths. Such three-way CMs MAY do IP forwarding or transparent bridging per [MCNS2].

1.2.2 Reference Architecture

The reference architecture for the data-over-cable services and interfaces is shown in Figure 1-2.

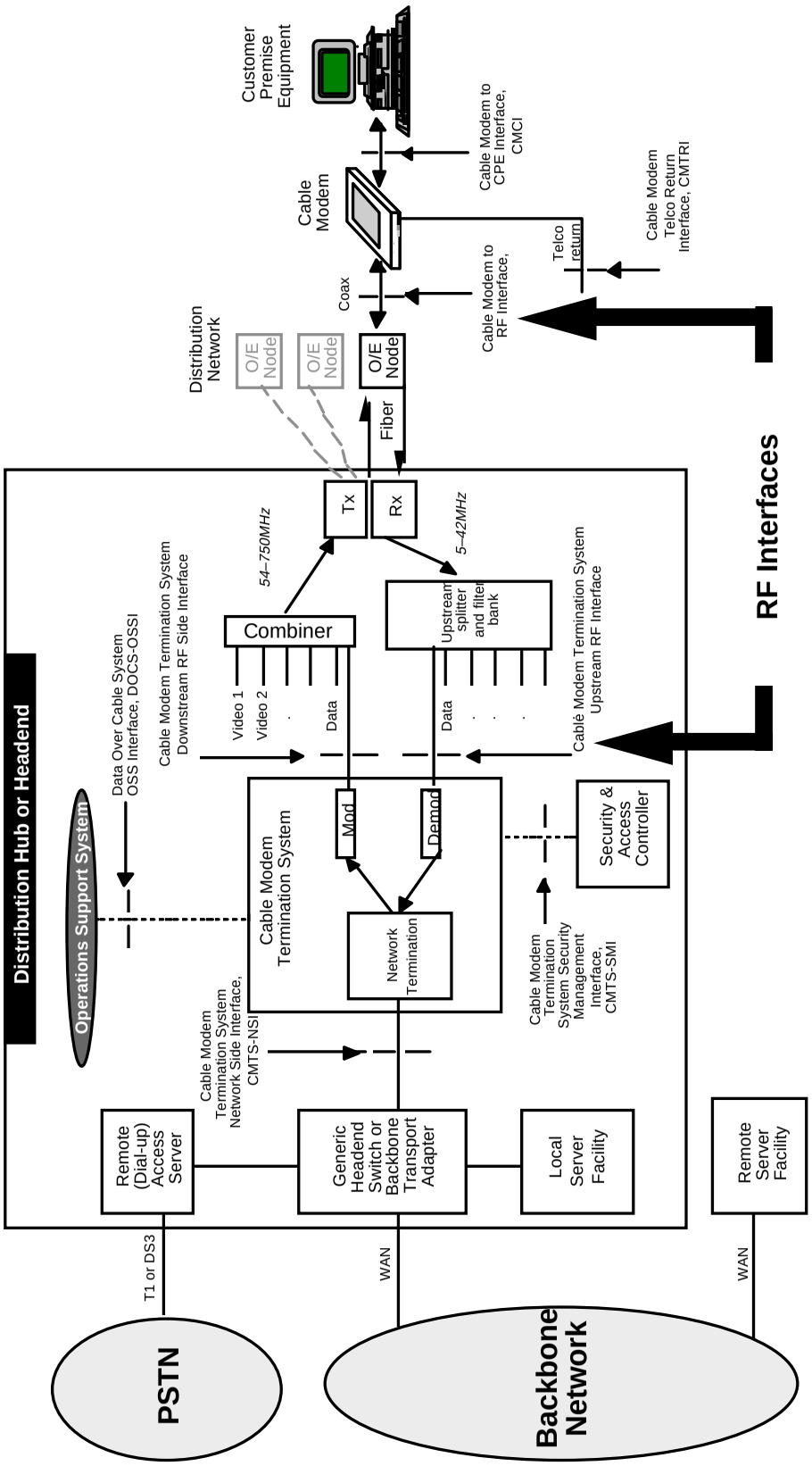

Figure 1-2. Data-Over-Cable Reference Architecture

1.2.2.1 Categories of Interface Specification

The basic reference architecture of Data-Over-Cable involves three categories of interface. These are being developed in phases.

a. Phase 1

Data Interfaces - These are the CMCI [MCNS4] and CMTS-NSI [MCNS3], corresponding respectively to the cable modem to customer-premises-equipment (CPE) interface (for example between the customer's computer and the cable modem), and the cable modem termination system network-side interface between the cable modem termination system and the data network.

b. Phase 2

Operations Support Systems Interfaces - These are network element management layer interfaces between the network elements and the high level OSSs (operations support systems) which support the basic business processes, and are documented in [MCNS5].

Telephone Return Interface - CMTRI - This is the interface between the cable modem and a telephone return path, for use in cases where the return path is not provided or not available via the cable network, and is covered by this document.

c. Phase 3

RF Interfaces - The RF interfaces, which are defined in [MCNS2], are the following:

- Between the cable modem and the cable network.
- Between the CMTS and the cable network, in the downstream direction (traffic toward the customer)
- Between the CMTS and the cable network, in the upstream direction (traffic from the customer)

Security requirements -

- The Data Over Cable Security System (DOCSS) is defined in [MCNS6].
- The CM Removable Security Module (RSM) is defined in [MCNS7].
- Baseline data-over-cable security is defined in [MCNS8].

1.2.2.2 Data-Over-Cable Interface Documents

A list of the documents in the Data-Over-Cable Interface Specifications family is provided below. For update, please refer to URL http://www.cablemodem.com.

Designation	Title
SP-BPI	Baseline Privacy Interface Specification
SP-CMCI	Cable Modem-to-Customer Premises Equipment Interface Specification
SP-CMTRI	Cable Modem Telephony Return Interface Specification
SP-CMTS-NSI	Cable Modem Termination System Network Side Interface Specification
SP-OSSI	Operations Support System Interface Specification
SP-OSSI-RF	Operations Support System Interface Radio Frequency MIB
SP-OSSI-SS	Operations Support System Interface Specification Security System MIB
SP-OSSI-TR	Operations Support Systems Interface Telephony Return MIB
SP-RFI	Radio Frequency Interface Specification
SP-RSM	Removable Security Module Interface Specification
SP-SS	Security System Specification

Key to Designation:

SP Specification

2 Protocols

Internet Protocol (IP) version 4 datagrams [RFC-791] are transparently passed from the CMTS-NSI, through the CMTS, the cable plant, and the CM to the CPE at the CMCI. Upstream datagrams are transparently passed from the CMCI, through the CM, across the PSTN to the TRAC, and delivered to the network at the TRAC-NSI.

2.1 Telephone Return CM Protocol Stack

The protocol stack on the cable and telephone interfaces of the telephone return CM MUST be as shown in Figure 2-1.

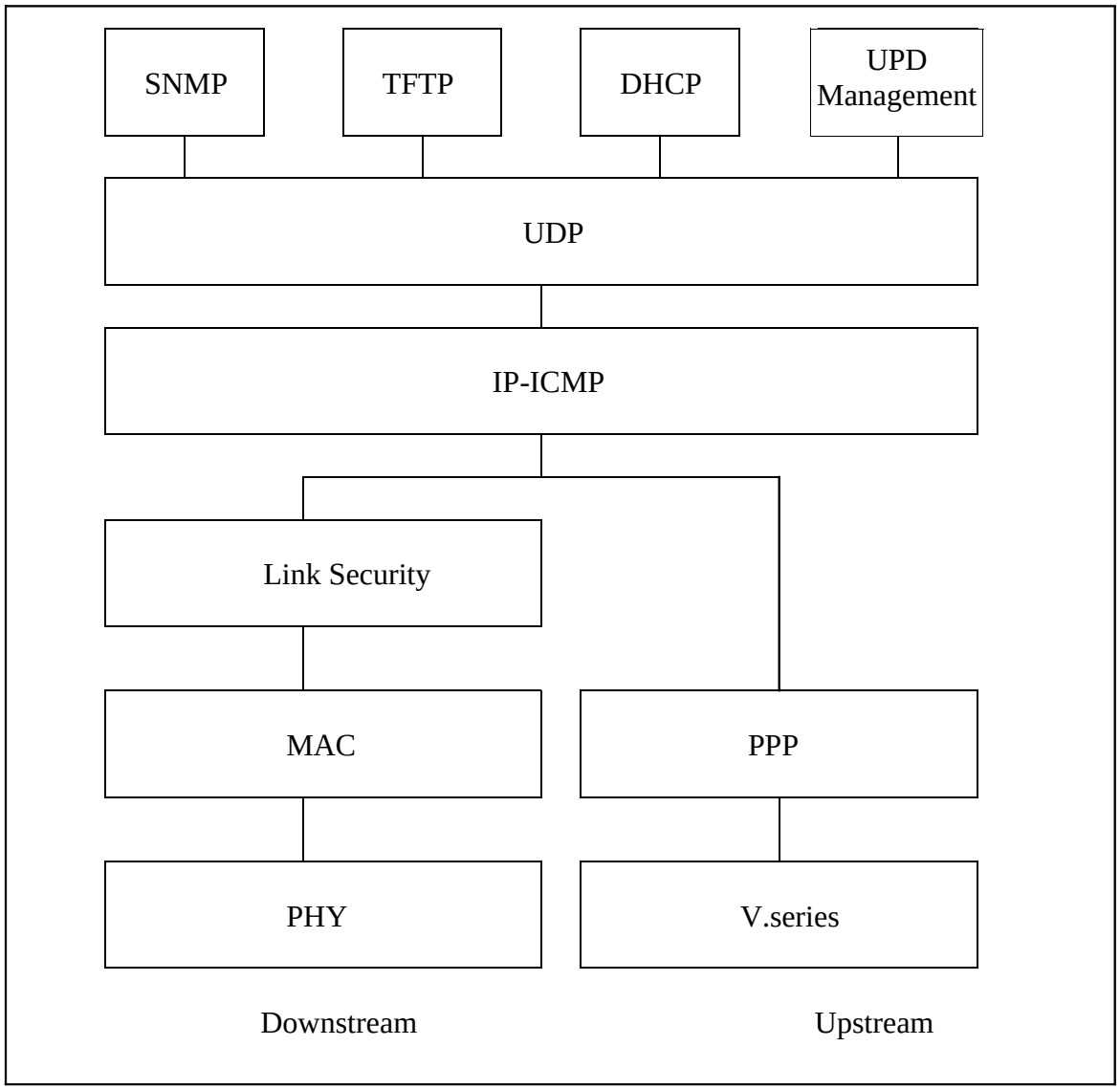

Figure 2-1. Protocol Stack for a Telephone Return Cable Modem

2.2 Physical Layer - Telephone Return

2.2.1 Telephony Interface

The CM and TRAC MAY provide a direct telephony interface (i.e., the CM and TRAC MAY incorporate internal telephone modems). If the CM or TRAC incorporates an internal telephone modem, the CM and TRAC MUST adhere to the following:

- The CM physical layer interface MUST be in accordance with one or more of the ISO/ITU-T V.series recommendations (see Appendix A). An RJ-11 jack MUST be provided in accordance with FCC 47CFR68.500(b)(2)(l).
- CMs and TRACs MAY support data rates faster than those specified in Appendix A, but MUST be capable of automatically falling back to one of the listed data rates if the higher data rates are not supported by the CM, the TRAC, or the signal quality of the given call.

2.2.2 Asynchronous Interface

The CM MAY provide an asynchronous data port to allow interconnection to an external telephony modem. If the CM incorporates an asynchronous data interface, that interface must comply with the following:

- The physical interface MUST be a shielded male 9-pin D subminiature connector which conforms to the electrical and mechanical requirements specified in [EIA RS-232E].
- Asynchronous data rates from 9,600 b/s to 115,200 b/s MUST be supported. Faster data rates MAY be supported.
- The interface MUST use 8 data bits, one start bit, one stop bit, and no parity bits.
- The asynchronous interface on the CM MUST support hardware flow control, using RTS/CTS [EIA RS-232E].

The signals on the interface MUST conform to [EIA RS-232E] voltage levels. Signal transition times MAY be faster than those specified by [EIA RS-232E].

2.3 Physical Layer - Downstream RF Interface

The physical layer in the downstream direction MUST comply to that specified by [MCNS2].

2.4 MAC Protocol

A telephone return CM MUST be compliant with the protocols outlined in [MCNS2], with the following exceptions:

- Upstream communication via the RF interface is not required.
- The RF upstream parameter acquisition and ranging processes are not required.
- The telephone return CM MUST NOT transmit MCNS MAC management messages across the telephone link. (Note: The CM registration with the CMTS is defined as a MAC management message in [MCNS2] but formatted and transmitted as a UDP packet [RFC-768] for telephony return as described in Section 3.4.6.1).

Specifically, a CM operating in telephone return mode MUST:

- Support the reception of all MAC frames specified in the MCNS RFI Specification [MCNS2].
- Silently discard any MAC management messages which relate to upstream channel acquisition or upstream data traffic over the RF channel.
- Perform downstream channel acquisition without the use of SYNC messages.

A modem with an optional upstream cable path enabled MUST function in a mode which is compliant with 2-way CMs [MCNS2] with the following exception:

- Data forwarding through the CM MAY be IP forwarding as shown in Figure 2-5 of this document.

2.4.1 Telephony Channel Descriptor

The Telephony Channel Descriptor (TCD) is used to provide dialing and access instructions via the downstream RF channel to unconfigured (in their factory default or reset state) telephone return cable modems. Information in the TCD is used by these CMs to connect to a primary access and activation TRAC. The TCD MUST be transmitted by the CMTS at a periodic interval. The TCD is transmitted as a MAC management message with TCD management type value of TRI_TCD as defined in [MCNS2] .

To provide for flexibility, the message parameters are encoded in a type/length/value (TLV) form in which the type and length fields are each 1 octet long. Using this approach, new parameters may be added which not all CMs can interpret. A CM which does not recognize a parameter type MUST skip over this parameter and MUST NOT treat the event as an error condition.

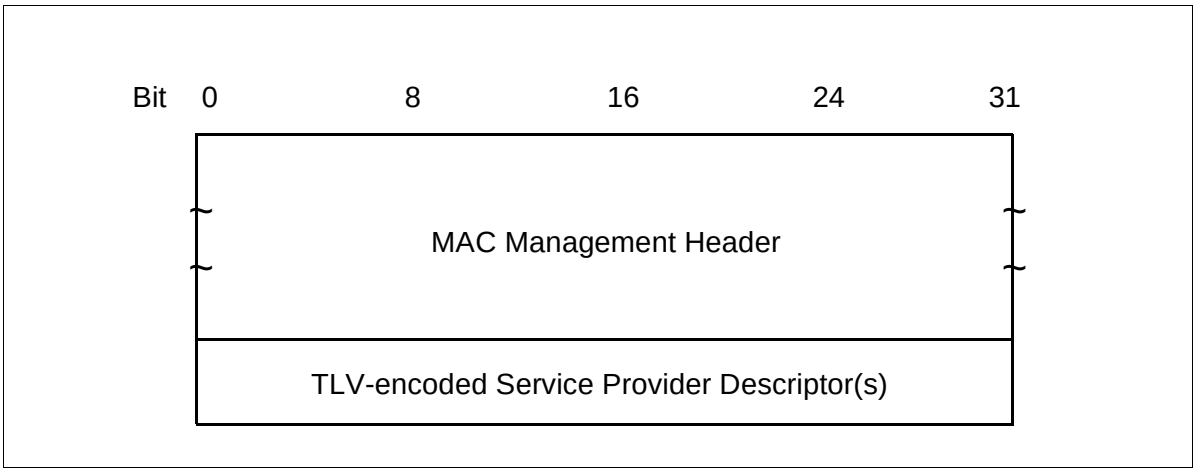

Figure 2-2. Telephony Channel Descriptor (TCD) Message Format

A CMTS MUST generate TCDs in the format shown in Figure 2-2 including the following parameter:

2.4.2 Service Provider Descriptor

Service Provider Descriptors (SPD) are compound TLV encodings that define the telephony physical-layer characteristics that are to be used by the CM to initiate a factory default telephone call.

The TCD message will contain the parameter shown in Table 2-1.

Table 2-1. TCD TLV Messages

Name	Type (1 byte)	Length (1 byte)	Value ('Length' bytes)
Service Provider Descriptor	1	1-255	Service Provider Descriptor, There may be multiple instances of these in the TCD.

2.4.2.1 Service Provider Descriptors

The Service Provider Descriptor (SPD) is a TLV-encoded data structure that contains sets of dialing and access parameters for the telephone return CMs. The SPD is contained within the TCD message. There may be multiple SPD messages within a single TCD. There MUST be at least one SPD in the message. All parameters are coded as service provider descriptor TLV tuples (See "- General TLV Encoding and Cable Modem Configuration File Additions For Telephone Return" on page 55.) The CMTS MUST generate SPDs in the format shown in Figure 2-3.

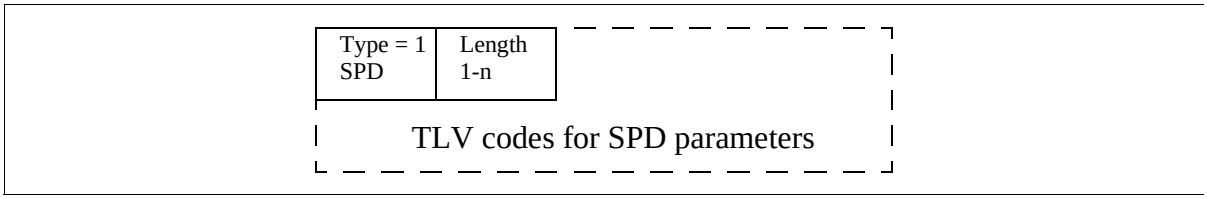

Figure 2-3. Top-Level Encoding for a Service Provider Descriptor

Within each SPD, is an unordered list of telephony related attributes, encoded as TLV values. These attributes are shown in Table 2-2.

Table 2-2. SPD TLV Parameters

Name	Type (1 byte)	Length (1 byte)	Value ('Length' bytes)
Factory Default Flag	1	1	Boolean - mandatory
Service Provider Name	2	variable	Service Provider String - optional
Phone Number1	3	variable	Phone Number String 1 - mandatory
Phone Number2	4	variable	Phone Number String 2 - optional
Phone Number3	5	variable	Phone Number String 3 - optional
Connection Threshold	6	1	Connection Attempt Threshold - optional
Username	7	variable	Username String - optional
Password	8	variable	Password String - optional
DHCP Authenticate	9	1	DHCP authenticate Boolean - optional
DHCP Server	10	4	IP address of DHCP server - optional
RADIUS Realm	11	variable	Realm String - optional
PPP Authentication	12	1	PPP authentication: (0) Negotiate PAP/ CHAP, Use only PAP (1), Use only CHAP(2). - optional
Demand Dial Timer	13	4	Inactivity timer - optional

The SPD message MUST contain the mandatory parameters shown in Table 2-2 and MAY contain optional parameters described below and optional vendor-specific data as defined in [MCNS2]. The default values shown for all optional SPD parameters indicate values that MUST be used by the CM initialization procedures (see Section 3.3) if an optional parameter is not otherwise present in an SPD.

Factory Default Flag Boolean value, if TRUE(1), indicates the SPD which SHOULD be used by the CM during factory default procedure (see Section 3.3).

Service Provider Name This parameter includes the name of the service provider. Format is standard NVT ASCII string composed of:

- numbers [ASCII (decimal) codes 048-057],
- letters [ASCII (decimal) codes 065-090 and 097-122]

Telephone Numbers These parameters contain telephone numbers that the CM will use to initiate the telephone modem link during the login process. Connections MUST be attempted in ascending numeric order (i.e., Phone Number1, Phone Number2…). The SPD MUST contain a valid telephony dial string as the primary dial string (Phone Number1), secondary dial-strings are optional. Format is NVT-ASCII string(s) composed of:

- any sequence of numbers [ASCII (decimal) codes 048-057],

- pound and star keys [ASCII (decimal) codes 035 and 042 respectively] and
- comma character [ASCII (decimal) 042]. (The 'comma' character is used to indicate a two second pause in dialing.[1])

Connection Threshold

The number of sequential connection try failures before indicating connection failure. A dial attempt that does not result in an answer and connection after no more than ten rings is a connection failure. The default value is one.

Login Username

This contains the username the CM will use during Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) authentication over the telephone link during the initialization procedure. Format is a monolithic sequence of alphanumeric characters in an NVT-ASCII string composed of:

- numbers [ASCII (decimal) codes 048-057],
- letters [ASCII (decimal) codes 065-090 and 097-122)

If this option is not present, the default value is "guest."

Login Password

This contains the password that the CM will use during the PAP or CHAP authentication over the telephone link during the initialization procedure. Format is a monolithic sequence of alphanumeric characters in an NVT-ASCII string composed of:

- numbers [ASCII (decimal) codes 048-057],
- letters [ASCII (decimal) codes 065-090 and 097-122]

If this option is not present, the default is no password.

DHCP Authenticate

Boolean value, reserved to indicate that a CM MUST use an indicated DHCP Server (see next parameter) for DHCP Client (see Section 3.4.4.1) and BOOTP Relay Process when TRUE (one). The default is FALSE (zero) which allows any DHCP Server.

DHCP Server

IP address value of the DHCP server the CM MUST use for DHCP Client and BOOTP Relay Process (Section 3) if this attribute is present and DHCP Authenticate attribute is TRUE(1). The default value is integer zero.

1. Other dial modem specific instruction, like command and escape sequences, may differ between modem manufacturers and are not specified as part of a telephone number.

RADIUS Realm

The realm name is a string which defines a RADIUS server domain. Format is a monolithic sequence of alphanumeric characters in an NVT-ASCII string composed of:

- numbers [ASCII (decimal) codes 048-057],
- letters [ASCII (decimal) codes 065-090 and 097- 122]

TRAC RADIUS MUST proxy requests to a server realm if this option is present. RADIUS syntax is to address a login name as a fully qualified domain name: Username-String@Realm-String – The domain MUST be correlated at the TRAC RADIUS to point to the IP address of a proxy RADIUS server which contains the designated user profile. If the TRAC RADIUS is the server for the designated user profile, this option would not be used, the default value is the null string.

If the Realm-String is not a null string, CMs MUST be able to construct a fully qualified domain name for a login response string and MUST respond to a PPP login query with the constructed login response string.

PPP Authentication

This parameter instructs the telephone modem which authentication procedure to perform over the telephone link. Allowed values are: (zero) Negotiate PAP or CHAP, (one) Use PAP only, (two) Use CHAP only. The default value is zero.

Demand Dial Timer

This parameter indicates time (in seconds) of inactive networking time that will be allowed to elapse before hanging up a telephone connection at the CM. If this optional parameter is not present, or set to zero, then the demand dial feature is not activated. The default value is zero.

Vendor specific extensions

Optional vendor extensions MAY be added as TLV encoded data [RFC-2131][RFC-2132][MCNS2].

2.4.3 Termination System Information

A Termination System Information (TSI) message MUST be transmitted by the CMTS at a periodic interval to report the CMTS Information to the CM. The TSI is transmitted as a MAC management message as defined in [MCNS2]. The TSI provides a CMTS boot record in a downstream RF channel to telephone return cable modems. Information in the TSI is used by attached CMs to obtain information about the CMTS status (see Section 3.2.2). The TSI message has a MAC management type value of TRI_TSI[MCNS2].

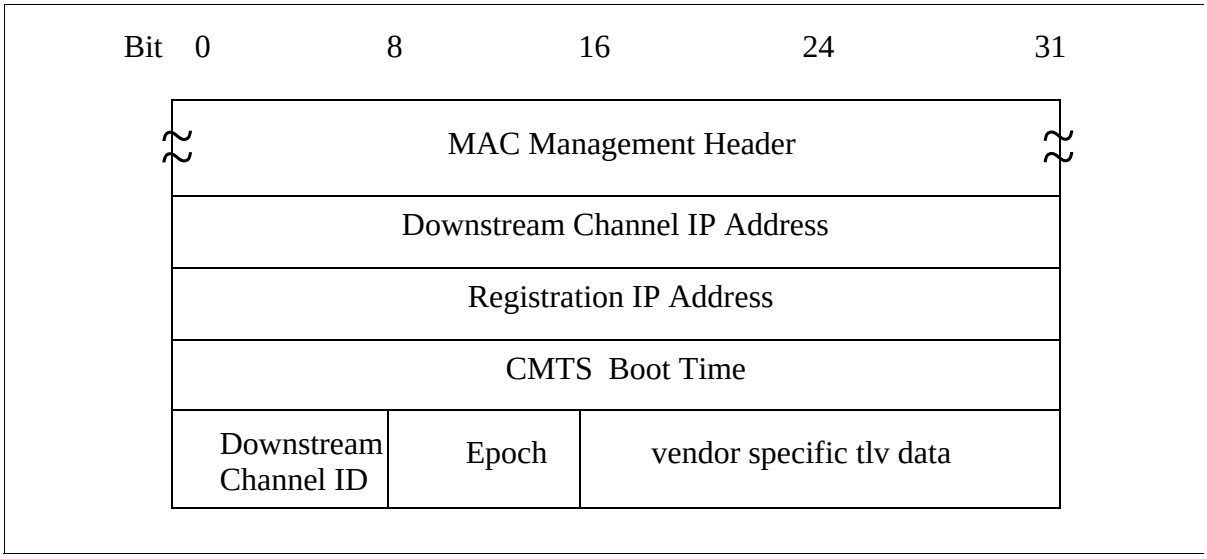

Figure 2-4. Termination System Information (TSI) Message Format

A CMTS MUST generate TSIs in the format shown in Figure 2-4 including all of the following parameters:

Downstream Channel IP Address This field contains the IP address of the CMTS associated with this downstream channel.

Registration IP Address This field contains the IP address the CM should send its registration request messages to. This address MAY be the same as the Downstream Channel IP Address.

CMTS Boot Time Specifies absolute-time of recorded epoch. The clock setting for this epoch uses the current clock time with an unspecified accuracy. Time MUST be represented as a 32 bit binary number as specified in [RFC868].

Downstream Channel ID An identifier of the downstream channel on which this message has been transmitted. This identifier is arbitrarily chosen by the CMTS and is unique within the MAC-Sublayer domain.

Epoch The Epoch field is an integer value that is incremented each time the CMTS is either re-initialized or performs an Address Resolution Protocol (ARP) cache flush. If there is no previous epoch value in non-volatile storage, the CMTS should use a default value of one.

Vendor specific extensions Optional vendor extensions MAY be added as TLV encoded data [RFC-2131][RFC-2132][MCNS2].

2.5 PPP Data Link Layer

Telephone Return CMs MUST access the network (and resources on the network) by dialing into the TRAC. The CM MUST support the Point-to-Point Protocol (PPP) [RFC 1661,1662,1663] datalink protocol on the dial-up connections. PPP Link Control Protocol (LCP) and Network Control Protocol (NCP) options and extensions MAY be configurable. The default initial PPP session MUST request Internet Protocol Control Protocol (IPCP) [RFC-1332] address negotiation.

2.6 IP Protocol

The CM, CMTS, and TRAC MUST support transmission and reception of IP version 4 datagrams as specified by [RFC-791]. The CMTS and TRAC MAY perform filtering of IP datagrams.

The CM MUST be configurable for IP datagram filtering to restrict the CM and CPE to the use of only their assigned IP addresses. The CM MAY be configurable for IP datagram TCP/ UDP port filtering (deep filtering).The following sections indicate which portions of IP support are required at the different system components.

2.6.1 Unicast Support

The CMTS, CM, and TRAC MUST be capable of forwarding IP datagrams destined to an IP unicast address which is across the cable network or telephone link. Some routers have security features intended to filter out invalid users who alter or *masquerade* packets as if sourced from a valid user. Since routing policy is under the control of the operators, such filtering is a vendor specific implementation. For example, dedicated interfaces (i.e., Frame Relay) may exist between the TRAC and CMTS which preclude filtering, or various forms of tunneling and reverse tunneling could be used to virtually source upstream packets from the CM.

2.6.2 Multicast Support

The CMTS and CM MUST be configurable for IP multicast datagram filtering. The CMTS, and CM, MUST be capable of forwarding IP datagrams destined to an IP multicast address which is across the cable network or telephone link [RFC-1112].

The CMTS and CM SHOULD be configurable to keep IP multicast forwarding tables and to use group membership protocols [DVMRP1]. The CM and CMTS MUST be capable of IP tunneling upstream through the telephony path [RFC-2003]. A CM that wants to send a

multicast packet across a tunnel will prepend another IP header, set the destination address in the new header to be the unicast address of the CMTS at the other end of the tunnel, and set the IP protocol field in the new header to be 4 (which means the next protocol is IP). The CMTS at the other end of the tunnel receives the packet, strips off the encapsulating IP header, and forwards the packet as appropriate.

The CMTS MUST decapsulate IP multicast control and data datagrams and make forwarding decisions based on Time To Live (TTL) and group membership. The CMTS MUST treat the "upstream" multicast tunnel as a unidirectional link. Downstream multicast traffic MUST NOT be tunneled.

2.6.3 Broadcast Support

A broadcast IP capability is dependant upon the configuration of the direct linkage, if any, between a TRAC and CMTS. The CMTS, CM, and TRAC MUST be capable of forwarding IP datagrams destined to an IP broadcast address which is across the cable network or telephone link if so configured. The CM MUST be configurable for IP broadcast datagram filtering.

2.6.4 Internet Control Message Protocol (ICMP) Support

The CM, CMTS and TRAC MUST be capable of transmitting, receiving, and responding to ICMP [RFC-792] messages. Specifically:

- The CM, the CMTS, and the TRAC MUST respond to ICMP echo request messages. That is, they must be capable of being "pinged."
- The CM MUST allow attached CPE[2] to respond to ICMP echo request messages.
- The CM SHOULD be configurable via SNMP to allow or restrict ICMP echo request messages generated by attached CPE.
- The TRAC, CMTS and CM SHOULD support ICMP router discovery messages per [RFC-1256].
- When supporting IP in IP tunneling for IP multicast (Section 2.6.2), the CM MUST follow ICMP rules set forth in [RFC-2003].

2.6.5 Address Resolution Protocol (ARP) Support

The CM and CMTS MUST be capable of filtering ARP packets per [RFC-826]. The TRAC, CMTS and CM MAY generate ARP packets on the TRAC-NSI, CMTS-NSI and CMCI respectively.

2. CPE in this section refers only to thoses devices which obtained their IP addresses through the processes described in Section 2.6.6

2.6.5.1 CMTS to CM ARP Support

For CMTS to CM ARP support, the CMTS SHOULD NOT generate ARP messages over the downstream RF plant for the IP addresses assigned to telephone return CMs. Telephone return CMs MUST ignore any ARP Request messages that they receive on the downstream RF link.

For telephone return CMs and their hosts, their associated CMTS ARP table entries MUST be initialized by gleaning from DHCP messages (see Section 3.4.4.1). The CM and CMTS MUST function as BOOTP relay agents [RFC-1542]. The CMTS MUST be configurable to control aging of its ARP table.

2.6.5.2 CM to CMTS ARP Support

For CM to CMTS ARP support, the CM MUST NOT generate ARP messages on the upstream telephony link.

2.6.5.3 CM to CM ARP Support

For CM to CM ARP support, the CMTS MUST proxy ARP [RFC-1027] for all registered CMs in its MAC-sublayer domain.

2.6.5.4 CPE ARP Support

For CPE ARP support, the CM MUST keep an ARP table which includes all DHCP administered IP addresses of attached CPE (Section 3.4.8). An entry in this table validates the CPE received its IP address through processes described in Section 2.6.6. The CM MUST respond in the normal manner (as a default gateway) to ARP requests from attached CPE on its CMCI. If those requests originate from CPE that have entries in this table, the CM will forward subsequent data from those respective sources. Data from CPE without entries in the ARP table MUST NOT be forwarded by the CM.

In cases where the CM is not a default gateway (CPE is performing ARP for an address on its same IP subnet), the CM MUST proxy ARP for attached CPE if the ARP originator has a valid entry in the CM ARP table. The CM MUST NOT respond with a proxy ARP if the ARP originator does not have a valid entry in the CM ARP table, or, if the ARP request is for the hardware address of another valid IP address entry within the CM ARP table. (see also service recovery exceptions - Section 4.3.2.)

ARP requests from attached CPE MUST NOT be forwarded on the upstream telephony link.

The CMTS MUST also keep an ARP table built and validated by DHCP requests (The CMTS learns these validated ARP table entries using processes defined in Section 3.4.4.1 and Section 3.4.8). The CMTS MUST proxy ARP for CM attached CPE with valid entries in its

ARP table. If the CMTS supports CMs which are not telephone return CMs, it MUST forward ARP requests for addresses not found in the ARP table.

2.6.6 IP Address Assignment

The IP address management policies in the TRTS MUST encompass the DHCP server. Specific provisioning policies for IP addresses are beyond the scope of this document and need to be flexible in order to support a variety of configurations. The general policy of host IP address assignment to the CM is as follows:

- The CM SHOULD be assigned no more than one globally-unique IP address.
- The CM MAY be assigned private enterprise IP addresses as described in [RFC-1918].
- During PPP IPCP negotiation, the CM MAY request a specific host IP address (static IP address). If the TRAC is configured to override any CM-requested address, the CM MUST permit the TRAC to reject the request, and MUST accept the address offered by the TRAC.
- If an IP address is delivered to the CM during the PPP IPCP negotiation, the CM MUST still use the DHCP mechanisms for obtaining configuration information and assign the IP address negotiated from DHCP to the CM host. Refer to Section 3.4.4.1.

2.7 The IP Forwarder

Data forwarding through the CM, the CMTS, and the TRAC is via network layer routing per RFC-791, as shown in Figure 2-5.

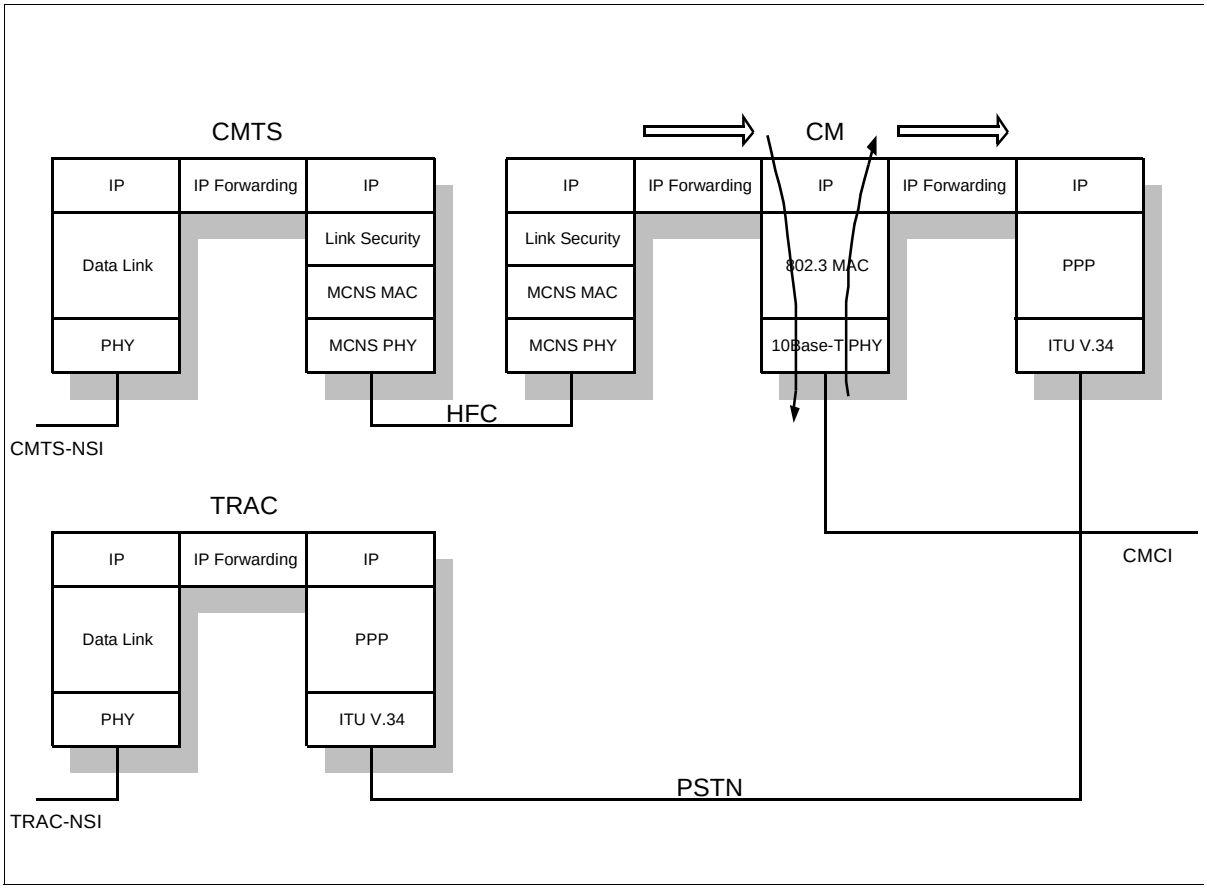

Figure 2-5. User Data Forwarding Protocol Stacks

The CMTS, CM, and TRAC MUST forward IP traffic based on the IP destination address per RFC-791.

The TRTS MUST be capable of configuring route information which forces a packet addressed to a CM or CPE to take the cable downstream path (via the CMTS-NSI) instead of the telephone downstream path (via the TRAC-NSI).

2.8 Above the Network Layer

The CM MUST support use of the transparent IP capability as a bearer for higher-layer services. Use of these services MUST be transparent to the CM. The CM-to-subscriber interface is beyond the scope of this specification.

In addition to the transport of user data, there are several network management and operation capabilities which depend upon the Network Layer that the CM itself MUST support from the network's perspective. These are shown in the protocol stack of Figure 2-1, and include:

- Simple Network Management Protocol (SNMP): To support network management functions. [RFC-1157]
- Trivial File Transfer Protocol (TFTP): A file transfer protocol used to download configuration information. [RFC-1350]
- Dynamic Host Configuration Protocol (DHCP): A framework for passing configuration information to hosts on a TCP/IP network. [RFC-2131][RFC-2132]
- The MCNS baseline privacy and security management protocols as defined in [MCNS6],[MCNS8] and Section 6 of this specification.
- UDP Management Messages to exchange general system management messages defined in this specification.

2.8.1 UDP Management Messages

In RF-return CMs [MCNS2] layer 2 (MAC layer) transport is utilized for MAC management and baseline privacy key management messaging. For telephone return CMs, using UDP IP packets is a straightforward way of handling these messages at a higher layer, see Figure 2-6. The UDP management messages (defined in Section 3.4.6 and Section 4.1.1) and the UDP baseline privacy messages (defined in Section 6.2) share the well-known MCNS Service UDP port 3311. The UDP message type parameter defined within these messages is used to distinguish and route packets to the appropriate service.

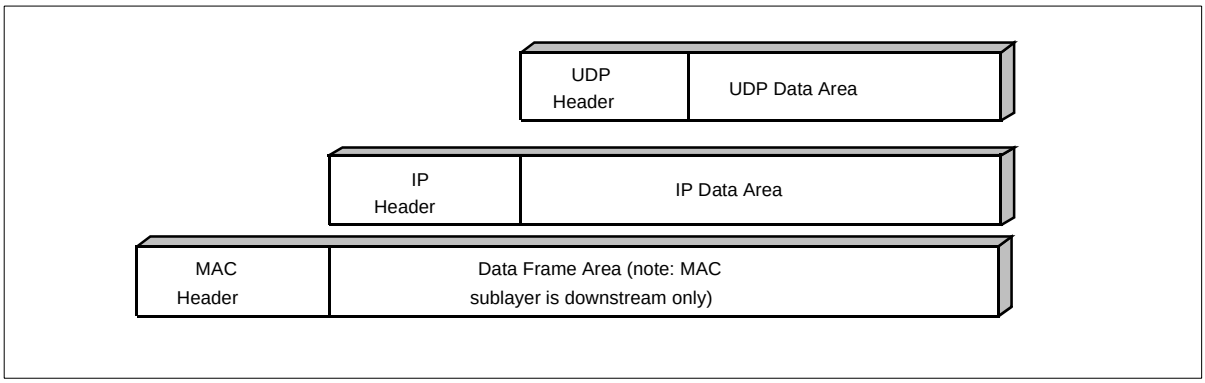

Figure 2-6. UDP Protocol

The order of transmission of the header and data for UDP packets described in this document is resolved to the octet level. Whenever a diagram shows a group of octets, the order of transmission of those octets is the normal order in which they are read in English. For example, in the following diagram, the octets are transmitted in the order they are numbered.

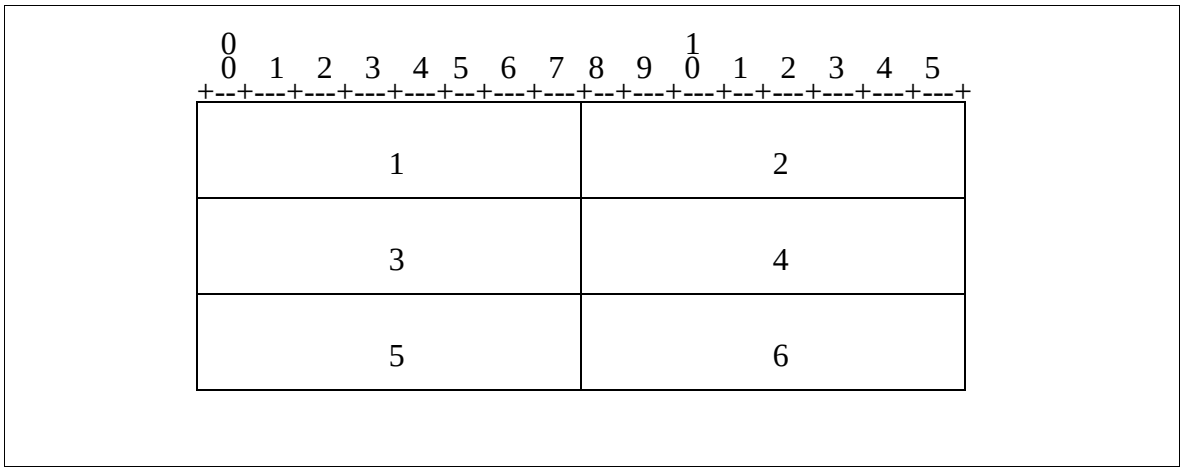

Figure 2-7. Order Of Octets

Whenever an octet represents a numeric quantity, the leftmost bit in the diagram is the high order or most significant bit. That is, the bit labeled 0 is the most significant bit. For example, the following diagram represents the value 170 (decimal).

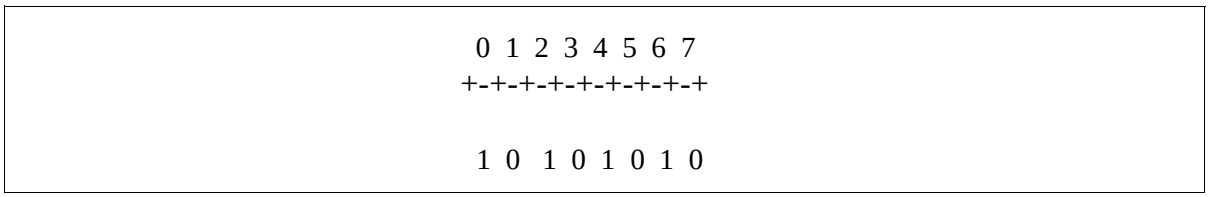

Figure 2-8. Octet Representation

Similarly, whenever a multi-octet field represents a numeric quantity the leftmost bit of the whole field is the most significant bit. When a multi-octet quantity is transmitted the most significant octet is transmitted first.

This page intentionally left blank.

3 Initialization and Administration

This section specifies procedures for the initialization and administration of the CM, CMTS, and TRAC in a telephone return system.

3.1 CMTS Initialization

The mechanism utilized for CMTS initialization (local terminal, file download, SNMP, etc.) is described in [MCNS5]. The criteria for system interoperability is described in [MCNS2].

3.2 CMTS Operation

Once the CMTS is operational, it MUST perform the following functions which are specific to telephone return systems.

3.2.1 TCD Enrollment Message

The CMTS MUST send TCD enrollment messages (see Section 2.4.1) using MAC layer messaging as specified in [MCNS2]. The CMTS MUST send enrollment messages at least every two seconds. The enrollment message broadcast interval SHOULD be configurable.

The CMTS MUST send TCD enrollment messages to the MCNS multicast CM management address group. The values in the message are assumed to be valid for all telephone return CMs on a CMTS downstream channel.

3.2.2 TSI Message

The CMTS MUST send TSI messages (see Section 2.4.3), using MAC layer messaging as specified in [MCNS2]. The TSI message broadcast interval SHOULD be configurable. The broadcast interval for the TSI is at least every 2 seconds.

The CMTS MUST send TSI messages to the MCNS multicast CM management address group. The values in the message are assumed to be valid for all telephone return CMs on a CMTS downstream channel.

3.3 Cable Modem Initialization - Factory Default

When a telephone return CM is initially powered on, or after it is reset to factory defaults by the user or administrator, the following procedure MUST be followed (Figure 3-1).

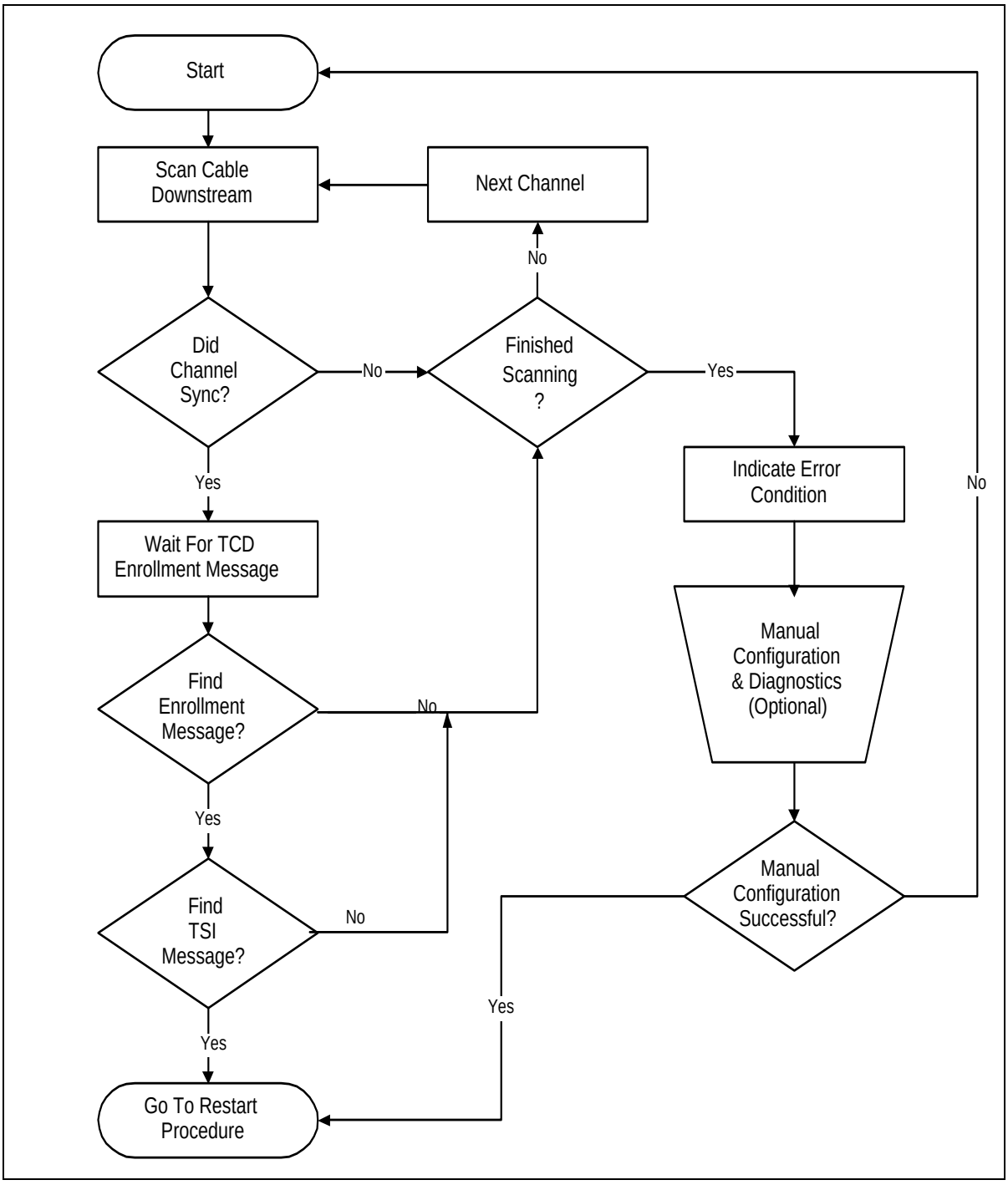

Figure 3-1. CM Factory Default Procedure

The factory default procedure for the cable modem that incorporates a telephone return channel is different from the enrollment procedure for a modem with only cable return capability.

The steps are:

1. Scan for downstream channel.
2. For modems equipped with both cable and telephone return, for each valid downstream channel, wait for upstream channel descriptor (UCD); if none found, wait for TCD enrollment message.
3. For modems equipped with only telephone return, for each valid downstream channel, wait for TCD enrollment message.
4. If no functional enrollment message can be found on any downstream channel, the CM MUST enter a manual configuration state.
5. When valid parameters have been obtained, go to restart procedure.

Each of these steps is detailed in the following sections. Modems operating in cable return mode will follow the procedures in [MCNS2].

3.3.1 Scan for Downstream Channel

The telephone return cable modem is considered locked to the downstream channel, when it has acquired:

- Synchronization of the QAM symbol timing,
- Synchronization of the FEC framing
- Synchronization of the MPEG framing

Note that reception of downstream SYNC messages is NOT required for telephone return operation.

3.3.2 Wait For TCD Enrollment Message

After a downstream channel has been acquired, the CM MUST wait for a minimum period T_w for reception of a TCD MAC management message (see Section 2.4.1). A TSI MAC management message MUST also be acquired

The default value for T_w is 2 seconds. T_w MAY be longer, but MUST NOT be shorter.

If, at the end of the time-out period T_w no enrollment message has been received, the CM MUST continue scanning for another candidate downstream channel.

If a TCD is acquired, the CM MUST find a TSI message on the selected downstream channel. If a period of 4 seconds elapses without reception of a TSI message, the CM MUST continue scanning for another candidate downstream channel[3].

When all downstream channels have been scanned, if a valid TCD enrollment message has not been received, the CM equipped with a telephone return capability MUST enter a manual enrollment mode. A CM user interface or other mechanism for performing this mode is a vendor-specific implementation.

3.3.3 Manual Configuration Mode

If the CM cannot find a valid downstream channel, or does not receive a valid enrollment message on any valid downstream channel, the CM MUST enter a manual configuration mode.

The manual configuration mode MUST provide all information necessary to complete a normal restart

3.3.4 Go To Restart Procedure

Upon reception of TCD and TSI messages, the CM MUST perform the Restart Procedure, outlined below. The CM MUST use the parameters obtained in section above.

3.4 Cable Modem Initialization - Restart

When a CM is restarted or powered on after having successfully completed the procedure outlined above, the procedure outlined in this section MUST be followed in order to establish a data over cable session with telephone return. The process is outlined in Figure 3-2.

3. A CMTS downstream channel MUST have both TCD and TSI messages or neither.

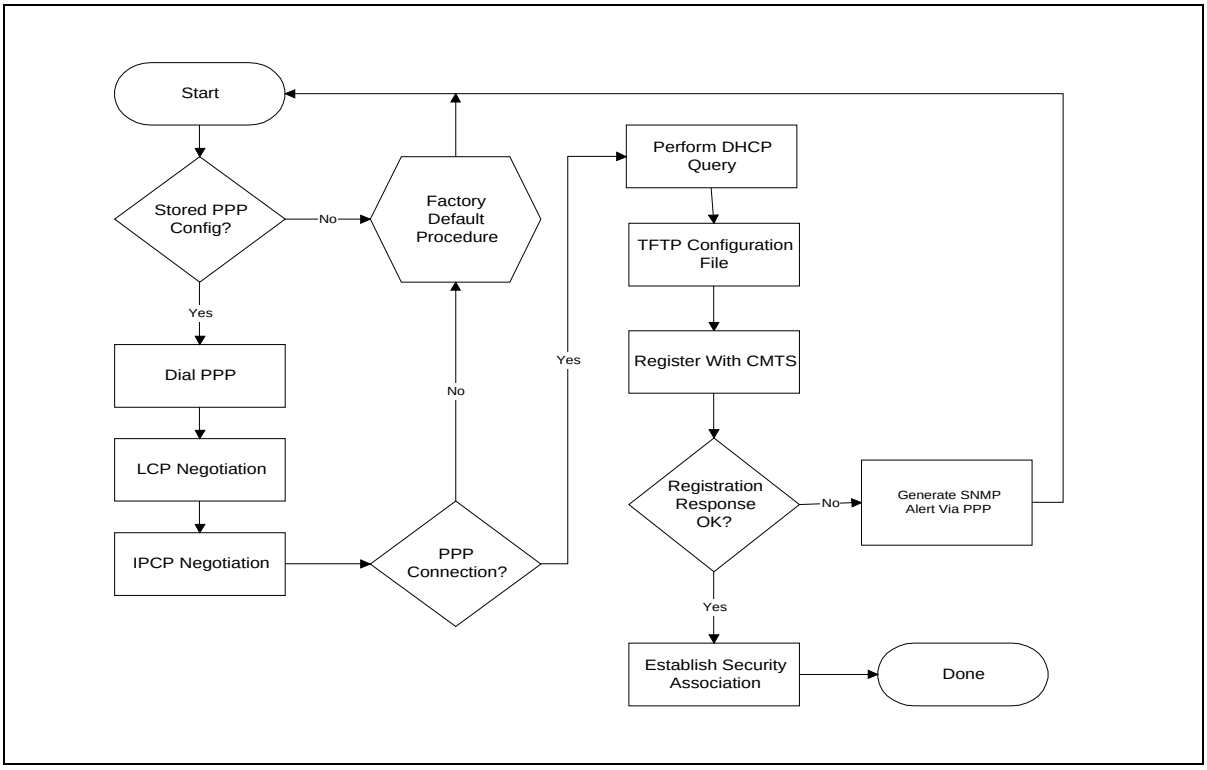

Figure 3-2. CM Restart Overview

The procedure can be divided into the following phases:

- Acquire telephone parameters
- Establish telephone PPP session
- Establish telephone IP connectivity
- Perform DHCP query for address and TFTP information
- Transfer operational parameters
- Register CM with CMTS
- Establish Security Association

Each of the processes listed above is described in detail in the following sections.

Each CM contains the following information when shipped from the manufacturer:

- A unique IEEE 802 [IEEE802] 48-bit MAC address which is assigned during the manufacturing process. This is used to identify the modem to the various provisioning servers during initialization.
- Security information as defined in [MCNS6][MCNS7][MCNS8].

3.4.1 Acquire Telephone Parameters

The CM MUST maintain a copy of the upstream parameters used during the last session, or obtained during the factory default procedure specified in Section 3.3. This list MUST include:

- The dial-up telephone number(s), which MAY include dial string prefix information
- The PPP username assigned.
- The PPP password assigned.

3.4.2 Establish Telephone PPP Session

The CM MUST dial the configured access number. If a modem answer connection is not made on the first dial-up attempt[4], the CM MUST compare its count of failed connections in this dial-up session with the Connection Threshold parameter[5]. If the Connection Threshold is not exceeded, the CM MUST continue to retry dialing. If multiple phone numbers exist, the CM MUST use each of them in a round-robin manner until threshold is exceeded, or, a connection is made.

Upon the completion of a successful connection, the CM MUST perform PPP Link Control Protocol (LCP) negotiation, as specified by [RFC-1661,1662,1663]. The TRAC MUST begin LCP negotiation immediately upon carrier detection. The TRAC MUST support PAP authentication. The CM MUST support both CHAP and PAP authentication. If CHAP authentication is supported by a TRAC, CHAP authentication MUST be used and indicated in the TCD message. The CM MUST negotiate and use PAP authentication only if CHAP is not supported by the TRAC.

3.4.2.1 CM Telephone Dial-Up Networking Script

The CM MUST provide scripts to automate the process of establishing a session with a remote host. This session MUST support a dial-up PPP connection. The CM script(s) MUST handle initializing the modem, dialing, waiting for a connection, and logging in to the remote host.

3.4.3 Establish Telephone IP

Once LCP negotiation is completed, the CM MUST enter into an IPCP negotiation phase. During this phase, the CM MUST negotiate an IP address with the TRAC (see Section 2.6.6).

4. A CM SHOULD set a maximum RING NO ANSWER threshold. This threshold MAY be vendor specific but SHOULD be no more than ten rings.
5. This parameter may be configured by the TCD message, configuration file, SNMP or defaulted to a value of one.

3.4.4 Perform DHCP Query

When the CM has established an IP link to the TRAC via the PPP session, it MUST transmit a DHCP Discover message to the TRAC as described in the following sections.

3.4.4.1 DHCP Process

The DHCP process is outlined in Figure 3-3. This figure assumes a DHCP proxy between the TRAC and the DHCP server, although this proxy is not required. Note: The CM MUST use information from the TSI message in the DHCP process. This message comes at a periodic rate at the control of the CMTS.

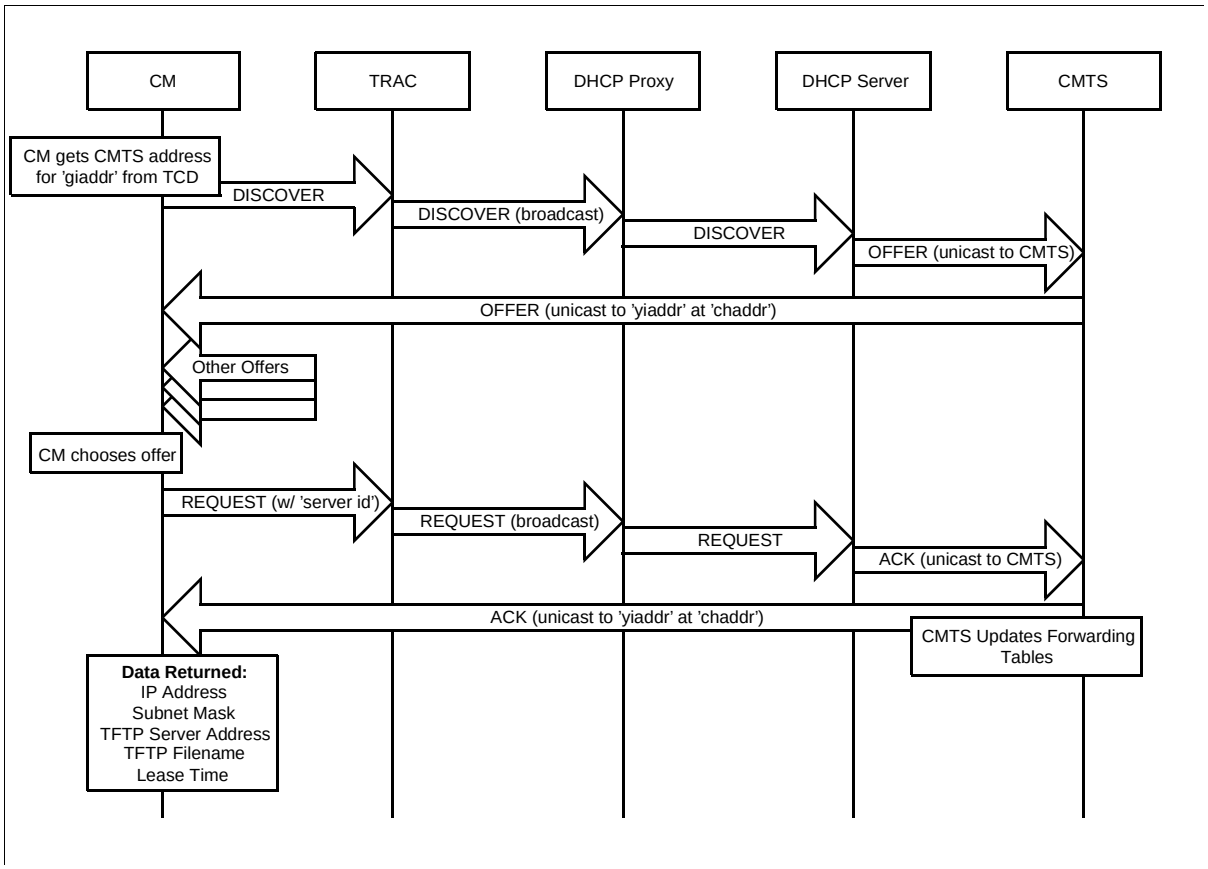

Figure 3-3. DHCP Process

Table 3-1. Key - Figure 3-3

KEY	Octets	Description
giaddr	4	Relay agent IP address
yiaddr	4	'your' (client) IP address.
chaddr	16	Client hardware address.

The steps in the process are:

1. The CM generates a DHCPDISCOVER message with fields set as specified in Section 3.4.4.2, and sends the message up the PPP link to the TRAC.
2. The TRAC broadcasts the DHCPDISCOVER message on its local network.
3. The DHCP proxy recognizes the discovery message, and forwards it to a configured interface. Since the 'giaddr' field is already non-zero, the proxy leaves the field intact.
4. The DHCP server receives the discovery message, and generates a DHCPOFFER message. It sends the offer to the address specified in the 'giaddr' field, which is the downstream channel IP address.
5. The CMTS receives the DHCPOFFER message. It examines the 'yiaddr' and 'chaddr' fields, and sends the offer message down the cable plant to these IP and MAC addresses, respectively. If the BROADCAST bit in the 'flags' field is set to one, the CMTS MUST send the downstream packet to the broadcast IP address (255.255.255.255), instead of the address specified in 'yiaddr'. The CM MUST use the MAC address specified in 'chaddr' even if the BROADCAST bit is set. The CMTS MUST NOT update its ARP or routing tables based upon this 'yiaddr' 'chaddr' pair.
6. The CM receives one or more offer messages. It chooses an offer, and generates a DHCPREQUEST message. The request message MUST have all fields set as specified in Section 3.4.4.2 for the discovery message, except that it MUST also set the 'server identifier' option to the value returned in the accepted offer message. The 'secs' field MUST be set to the same value as in the original discovery message. The request message MUST be sent up the PPP link, destined to the broadcast IP address (255.255.255.255).
7. The TRAC broadcasts the request message on its local network.
8. The DHCP proxy recognizes the DHCPREQUEST message, and forwards it to a configured interface. Since the 'giaddr' field is already non-zero, the proxy leaves the field intact.
9. The DHCP server receives the request message, and generates a DHCPACK message. It sends the offer to the address specified in the 'giaddr' field, which is the downstream channel IP address.
10. The CMTS receives the DHCPACK message. It examines the 'yiaddr' and 'chaddr' fields, and updates its routing and ARP tables to reflect the address pairing. It then sends the offer message down the cable plant to these IP and MAC addresses, respectively. If the BROADCAST bit in the 'flags' field is set to one, the CMTS MUST send the downstream packet to the broadcast IP address (255.255.255.255), instead of the address specified in 'yiaddr'. The CM MUST use the MAC address specified in 'chaddr' even if the BROADCAST bit is set.
11. The CM receives the DHCPACK message. The CM MUST use the fields specified in Section 3.4.4.3 from this message.

12. In the event that the CM is not compatible with the configuration received in the DHCPACK message, the CM MAY generate a DHCPDECLINE message, per [RFC-2131][RFC-2132], and transmit it up the PPP link.
13. The CM MUST also send a copy of the DHCPDECLINE message directly to the CMTS. On seeing a DHCPDECLINE message, the CMTS MUST examine the 'yiaddr' and 'chaddr' fields, and update its routing and ARP tables to flush any invalidated pairing.
14. The CM MUST also send a copy of any DHCPRELEASE messages directly to the CMTS. On seeing a DHCPRELEASE message, the CMTS MUST examine the 'yiaddr' and 'chaddr' fields, and update its routing and ARP tables to flush any invalidated pairing.

Upon completion of these steps, the CMTS has a valid IP/MAC address pair in its forwarding tables, and the CM has all parameters necessary to proceed to the next phase of initialization, the TFTP of the configuration file.

If an IP address is returned that is different from the IP address requested by the CM in the DHCP OFFER, the CM MUST accept the DHCP returned address as the CM host IP address. The CM MUST continue to use the address negotiated by IPCP for any packets which should use the PPP link for a return path. The CM MUST use its DHCP returned address for all communication on the broadband media.

3.4.4.2 DHCP Discovery and Request Message

The DHCP Discover and Request IP packets:

- MUST be IP UDP packets.
- MUST default to being addressed to the IP broadcast address (255.255.255.255)[6].
- MUST be formatted per Figure 1 in [RFC-2131][RFC-2132]

The CM MUST construct the DHCP message as follows:

- The 'op' field MUST be set to BOOTREQUEST.
- The 'htype' field MUST be set to 1 (10Mb/s Ethernet)
- The 'hlen' field MUST be set to 6.
- The 'hops' field MUST be set to zero.
- The BROADCAST bit in the 'flags' field SHOULD be set to 0.
- If the CM has previously been assigned an IP address, it SHOULD put this address in the 'ciaddr' field. If the CM has previously assigned an IP address by DHCP, and also has been assigned an IP address via IPCP, the CM SHOULD place the previous DHCP assigned address in the 'ciaddr' field.

6. The DCHP DISCOVER MAY be unicast or multicast to specific DHCP authenticated server(s) if the implied parameters, DHCP Authenticate and DHCP Server, are configured.

- The CM MUST place the Downstream Channel IP address, obtained from the TSI message on the cable downstream, in the ‘giaddr’ field.
- The ‘chaddr’ field MUST contain the 48-bit CM LAN MAC address.

3.4.4.3 DHCP Offer and Acknowledge Message

The following information is returned in the DHCP offer, and MUST be used by the CM:

- The TFTP server address is returned in the 'siaddr' field.
- The configuration filename is returned in the 'file' field.
- The CM IP address is returned in the ‘yiaddr’.
- The DHCP server identifier is returned in the ‘server identifier’ option of the DHCPOFFER message. The server identifier may not be present in the DHCPACK message.

The DCHP OFFER MAY be authenticated to a specific DHCP server if the DHCP authenticate parameter in the TCD message is set to TRUE(1).

3.4.5 Transfer Operational Parameters

The CM MUST transfer operation parameters at the beginning of every session. The CM MUST use the IP address and configuration filename passed by the DHCP response above, and must initiate a TFTP exchange to receive the configuration file.

The parameters downloaded include all required parameters specified in [MCNS2], as well as the additional parameters specified in “- General TLV Encoding and Cable Modem Configuration File Additions For Telephone Return” on page 55 of this document.

3.4.5.1 MIC and Termination Mode Verification

The CM and CMTS Message Integrity Check (MIC) configuration setting MUST be calculated by performing an MD5 digest over the configuration setting fields described in [MCNS2] and in the order shown in [MCNS2], treated as if they were contiguous data.

As in [MCNS2], the CMTS MIC MUST contain an authentication string shared secret between the provisioning server and the CMTS to allow the CMTS to authenticate the CM provisioning.

Differences to the MIC descriptions in [MCNS2] for a telephone return service are:

- Only the Class ID and Maximum Downstream Rate Configuration Setting quality of service settings contain content which is valid for a telephone return service. However, all quality of service settings MUST be present in the MIC message digest. Inapplicable upstream related settings MUST be ignored for telephone return service.

The digest MUST be added to the configuration file as its own configuration setting field using the CM MIC Configuration Setting encoding. On receipt of a configuration file, the CM MUST recompute the digest and compare it to the CM MIC configuration setting in the file. If the digests do not match then the configuration file MUST be discarded.

If the digests match, the CM MUST verify its upstream service matches the type of termination mode indicated by the Upstream Channel ID:

The Upstream Channel ID Configuration Setting for telephone return CM termination mode MUST be zero, any other value indicates that the CM MUST be configured for a 2-way upstream cable termination mode. If the setting is non-zero, and the upstream path was established via PPP, the CM:

- MUST discard the configuration file.
- SHOULD go into a manual configuration mode.

The Upstream Channel ID Configuration Setting for an upstream cable CM termination mode MUST be non-zero, a value of zero indicates that the CM MUST be configured for a telephone return cable termination mode. If the setting is zero, and the upstream path was established on an RFI cable channel, the CM MUST respond as follows:

If the CM telephone connection is not idle or it cannot establish dial tone, then the CM:

- MUST discard the configuration file.
- SHOULD go into manual configuration mode.

If the CM telephone connection is idle and dial tone is available, the CM:

- MAY store the PPP configuration from the configuration file.
- MAY execute the restart procedures in Section 3.4.

3.4.6 Register CM with CMTS

Once a CM has been initialized, it MUST register with the CMTS.

The configuration parameters downloaded to the CM MUST include a network access control object. If this object is set to “no forwarding,” the CM MUST NOT forward data to the network. The CM MUST respond to network management requests. This allows the CM to be configured in a mode in which it is manageable but will not forward data.

The CM MUST forward its operational parameters to the CMTS as part of a Registration Request. The CMTS MUST perform the following operations to confirm the CM authorization:

- check the MAC and the authentication signature on the parameter list
- build a profile for the modem based on the standard options (see Appendix B and [MCNS2] Appendix C)
- reply to the modem registration request.

The IP destination address for UDP IP packets is received in the Registration IP address parameter of the TSI message. Exactly one registration packet is encapsulated in the UDP Data field where the UDP Destination Port field indicates well-known port number 3311.

The CM MUST pass information to the registration IP address in UDP IP datagrams to a well known MCNS UDP destination port. If a CM fails to receive a valid registration response within a defined timeout period after transmitting a request, the request will be retried a number of times (as defined in Appendix B). Failure to receive a valid registration response after the requisite number of attempts will cause the modem to reset and reinitialize its MAC connection.

3.4.6.1 Registration Request

A Registration Request, in the format shown in Figure 3-4, MUST be transmitted by a CM at initialization after receipt of a CM parameter file.

To provide for flexibility, the message parameters following the CM MAC address field MUST be encoded in a type/length/value form. Using this encoding, new parameters may be added which not all CMTSs can interpret. A CMTS which does not recognize a parameter type MUST skip over this parameter and MUST NOT treat the event as an error condition. A Message Integrity Check (MIC) must be computed and added to the TLV data (see Section 3.4.5.1).

The TLV data and order of that data MUST be as described in [MCNS2] for registration requests.

The following additional data item MUST also be encapsulated in the telephone return interface UDP packet TLV data:

CPE IP addresses List of CPE IP addresses associated with this CM through DHCP gleaning process at CM (see Section 3.4.8). *This TLV data type is listed first in TLV data and not computed in MIC.*

TLV for List of CPE IP addresses at CM

Type (1 byte)	Length(1 byte)	Value('Length' bytes)
TR_HOSTS[7]	n * 4	CPE IP addr, CPE IP addr,...

A summary of the REG-REQ data format is shown below. The fields are transmitted from left to right.

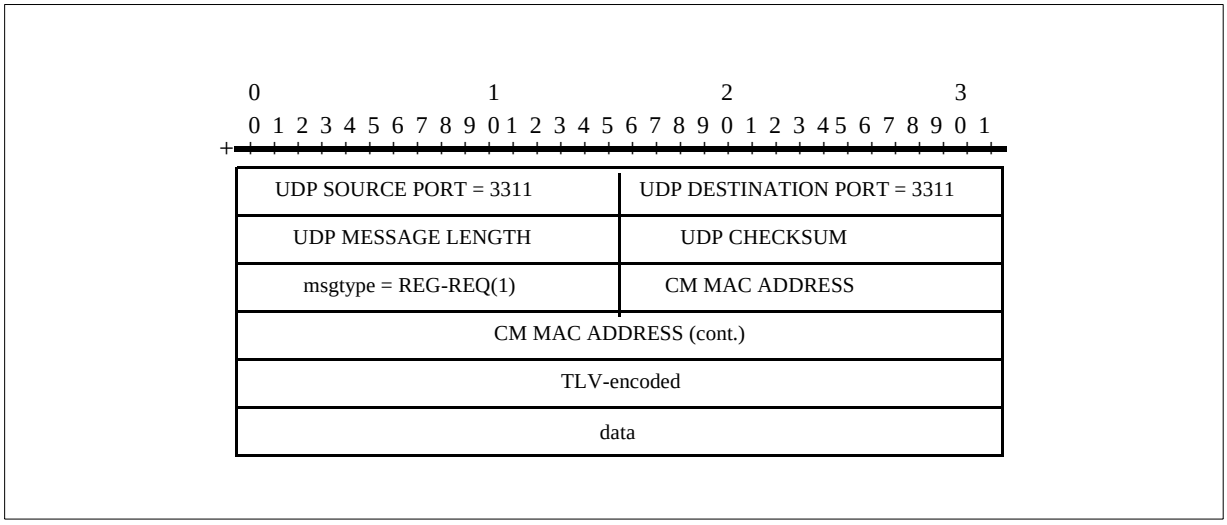

Figure 3-4. Registration Request Packet

This message contains the following:

Message type Distinguishes between registration services (message types = 1 - 2) and other services.

CM MAC Address CM MAC hardware address in network byte order, used to identify this request.

TLV data The configuration settings, vendor specific data and MICs as defined in [MCNS2].

3.4.6.2 Registration Response (REG-RSP)

A Registration Response, in the format shown in Figure 3-5, MUST be transmitted by CMTS in response to received REG-REQ.

7. [MCNS2] defines specific values for TR_HOSTS

To provide for flexibility, the message parameters following the CM MAC Address MUST be encoded in a type/length/value form. Using this encoding, new parameters MAY be added which not all CMs can interpret. A CM which does not recognize a parameter type MUST skip over this parameter and MUST NOT treat the event as an error condition. A MIC must be computed and added to the TLV data (see MCNS2).

The TLV data and order of that data MUST be as described in [MCNS2] for registration response. The following additional data item MUST also be encapsulated in the telephone return interface UDP packet TLV data:

CPE IP addresses List of CPE IP addresses associated with this CM MAC address through the DHCP gleaning process at CMTS (see Section 3.4.8). *Listed first in TLV data and not computed in MIC*

TLV for List of CPE IP addresses at CMTS

Type (1 byte)	**Length(1 byte)**	**Value('Length' bytes)**
TR_HOSTS[8]	n * 4	CPE IP addr, CPE IP addr,...

A summary of the REG-RSP data format is shown below. The fields are transmitted from left to right.

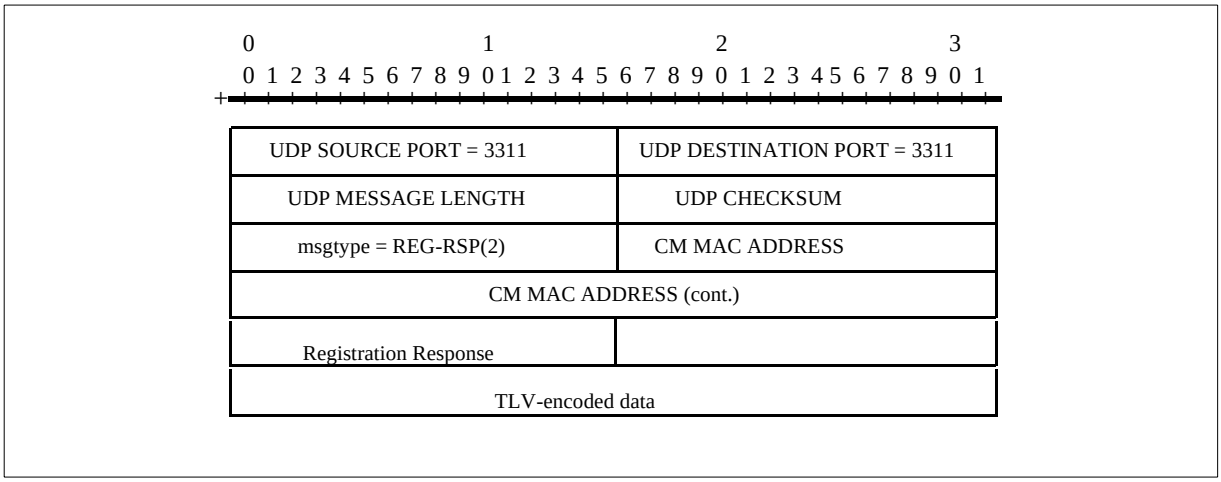

Figure 3-5. Registration Response Packet

This message contains the following:

Message type Distinguishes between registration services (message types = 1 - 2) and other services.

8. [MCNS2] defines specific values for TR_HOSTS

CM MAC Address	CM MAC hardware address in network byte order, used to identify this request.
Response	Response to this request 0 = ok 1 = authentication failure 2 = class of service failure
TLV encoded data	The Modem Capabilities, Service Class Data (Returned when response = ok), Service not available (Returned when response = class of service failure) and Vendor-Specific Data as defined in [MCNS2].

Note: SID associations returned in the Class of Service are required for telephone return CMs to establish a security association for (downstream only) baseline privacy (see Section 6).

3.4.7 Establish Security Association

If security is required on the network and no security association has been established, then the CM MUST establish a security association at this point. The IP address of the security server (or servers) MUST be provided as part of the DHCP response. The procedures required are fully defined in [MCNS6] and [MCNS8].

3.4.8 CM and CMTS Interaction With CPE Initialization

Customer Premises Equipment (CPE) attached as hosts to the CMCI MUST use standard DHCP client procedures [RFC-2131][RFC-2132] to generate requests to obtain IP addresses. The CM MUST function as a standard BOOTP relay agent/DHCP Proxy [RFC-1542] to facilitate CPE access to the DHCP Server. The DHCP gleaning process which MUST be used by the CMTS and CM is shown in Figure 3-6. This figure shows an (optional) DHCP proxy, which could be at the TRAC location, and the DHCP server. Note: The CM and CMTS MUST use information from the DHCP process to construct IP forwarding and ARP table entries for hosts attached to the CMCI.

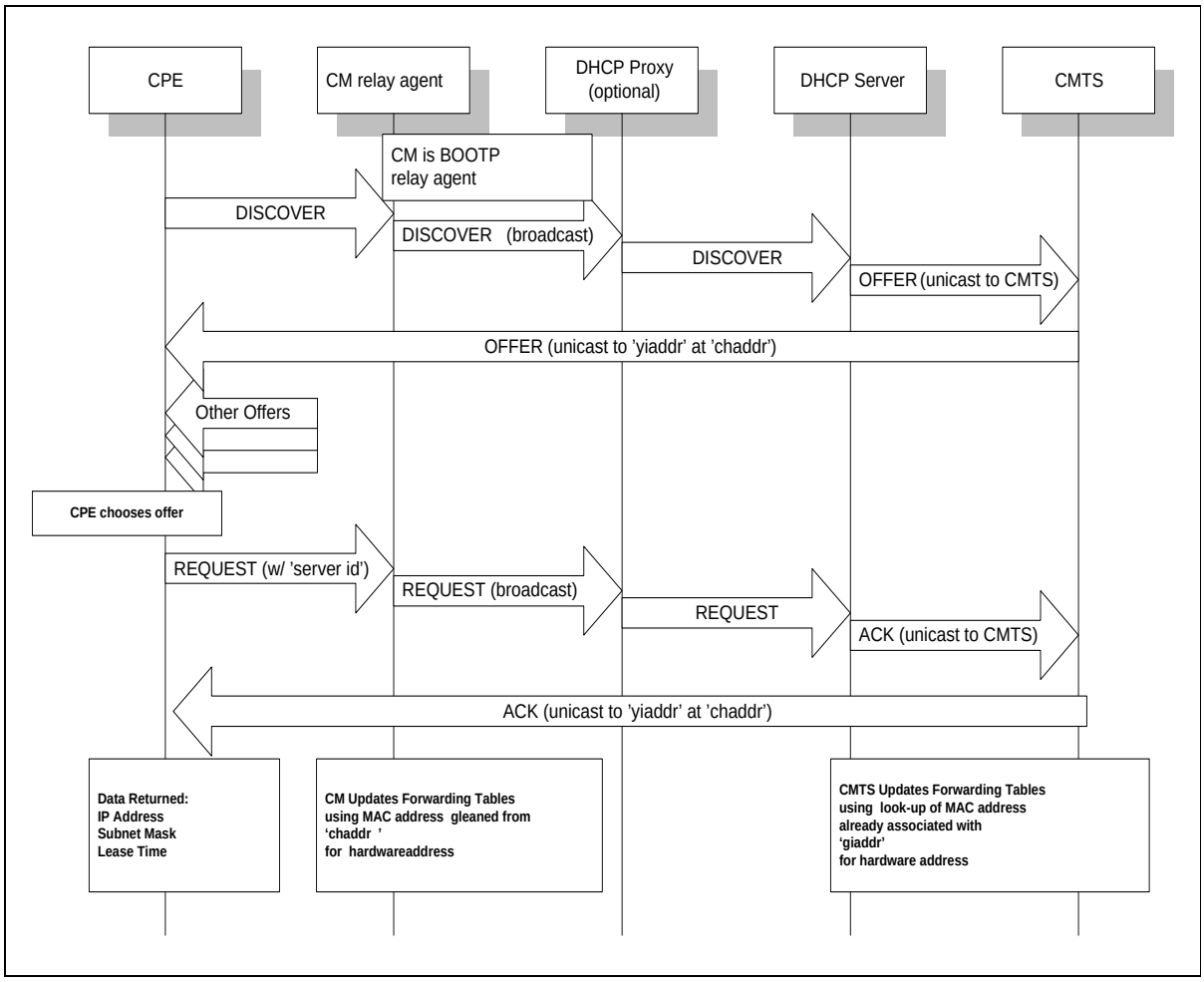

Figure 3-6. DHCP Process (CPE)

The steps in the process are:

1. The CPE DHCP client generates a DHCPDISCOVER message with fields set as specified in [RFC-2131][RFC-2132].
2. The CPE broadcasts the DHCPDISCOVER message on its local network. The CM will receive this message as a standard BOOTP relay agent [RFC-1542]. As a BOOTP relay agent, the CM MUST check the 'giaddr' field. If the field is set to '0' (zero), the CM MUST put it's IP address into the 'giaddr' field. If the 'giaddr' field is non-zero, the CM MUST NOT alter the 'giaddr'. Note: There could be a BOOTP relay agent on the client network side which MAY set the 'giaddr' field. Any client-side BOOTP relay agent that complies with MCNS MUST also have acquired it's IP address from this DHCP process.
3. The default destination address for the CM BOOTP relay agent to send the discover packet is the broadcast IP address (255.255.255.255).

4. An additional DHCP proxy(s), if present, recognizes the discovery message, and forwards it to a configured interface. Since the 'giaddr' field is already non-zero, the proxy leaves the field intact.

5. The DHCP server receives the discovery message, and generates a DHCPOFFER message. It sends the offer to the address specified in the 'giaddr' field, which is an IP address already associated with a CMTS ARP cache.

6. The CMTS receives the DHCPOFFER message. It examines the 'yiaddr' and 'giaddr' fields, and sends the offer message down the cable plant to this IP address. The MAC address is learned through a look-up of the hardware address associated with the 'giaddr'. If the BROADCAST bit in the 'flags' field is set to one, the CMTS MUST send the downstream packet to the broadcast IP address (255.255.255.255), instead of the address specified in 'yiaddr'. The CM MUST use the MAC address specified determined by the 'giaddr' look-up even if the BROADCAST bit is set. The CMTS MUST NOT update its ARP or routing tables based upon this 'yiaddr' 'chaddr' pair.

7. The CPE receives one or more offer messages. It chooses an offer, and generates a DHCPREQUEST message.

8. The TRAC broadcasts the request message on its local network.

9. The DHCP proxy recognizes the DHCPREQUEST message, and forwards it to a configured interface. Since the 'giaddr' field is already non-zero, the proxy leaves the field intact.

10. The DHCP server receives the request message, and generates a DHCPACK message. It sends the offer to the address specified in the 'giaddr' field, which is the downstream channel IP address.

11. The CMTS receives the DHCPACK message. It examines the 'giaddr' field and looks up that IP address in the ARP table for the associated MAC address. This is always going to be the originating CM MAC address. The CMTS uses the MAC address associated with the `giaddr' and the 'yiaddr' to update its routing and ARP tables reflecting this address pairing. It then sends the offer message down the cable plant to these IP and MAC addresses, respectively. If the BROADCAST bit in the 'flags' field is set to one, the CMTS MUST send the downstream packet to the broadcast IP address (255.255.255.255), instead of the address specified in 'yiaddr'. The CM MUST use the MAC address associated with the 'giaddr' even if the BROADCAST bit is set.

12. The CM receives the DHCPACK message. It examines the 'yiaddr' and 'chaddr' fields, and updates its routing and ARP tables to reflect the address pairing. It then sends the offer message down the CMCI to these IP and MAC addresses, respectively. If the BROADCAST bit in the 'flags' field is set to one, the CM MUST send the downstream packet to the broadcast IP address (255.255.255.255), instead of the address specified in 'yiaddr'. The CM MUST use the MAC address specified in 'chaddr' even if the BROADCAST bit is set.

13. The CPE receives the DHCPACK message.

14. In the event that the CPE is not compatible with the configuration received in the DHCPACK message, the CPE MAY generate a DHCPDECLINE message, per [RFC-2131][RFC-2132], and transmit it up the PPP link.
15. On seeing a DHCPDECLINE (or DHCPRELEASE) message the CM MUST send a unicast copy of this message to the CMTS. The CMTS MUST examine the 'yiaddr' and 'giaddr'(associated) fields, and update its routing and ARP tables to flush any invalid pairing.

Upon completion of these steps, the CM and CMTS have valid IP/MAC address pairings in their forwarding tables. These tables store the same set of IP addresses, but do not associate them with the same MAC addresses. This is because the CMTS MUST resolve all CPE IP addresses to the MAC address of their CM. The CMs, on the other hand, MUST be able to address the respective MAC addresses of its CPE hosts. This gleaning process MUST allow CPE DHCP clients to function normally. That is, the DHCP gleaning processes in the CM and CMTS MUST be transparent to CPE hosts.

4 Service Recovery

This section addresses CM and CMTS service-recovery requirements for effective fault tolerance. This section explains mechanisms available to the CM, CMTS and TRAC for such recovery. This fault-handling method consists of several stages: boot-state detection, required response for each network location, and recovery. This section does not preclude the addition of hardware and/or software to further facilitate robust service. The required responses SHOULD be configurable to allow them to be dependent upon additional underlying fault-handling mechanisms. Additional mechanisms for fault recovery are vendor-specific implementations and are beyond the scope of this specification.

While the method described in this section can mask the effects of a single faulty module, they cannot tolerate coincident faults in multiple modules possibly caused by a common source, such as an environmental disruption, malfunction of a shared component, or misguided user intervention.

4.1 Recovery Messages

4.1.1 User Station Restart Request (USR-REQ) and Response (USR-RSP)

The CMTS MAY request that the CM perform a Restart procedure. This is done by the CMTS sending a User Station Restart Request (USR-REQ) message. When the CM receives this message, it will respond to the request with a User Station Restart Response (USR-RSP) message. These messages are carried as UDP/IP datagrams, and are sent between the MCNS Service UDP ports (port 3311) in the CM and CMTS.

The format of the USR-REQ message is shown in Figure 4-1.

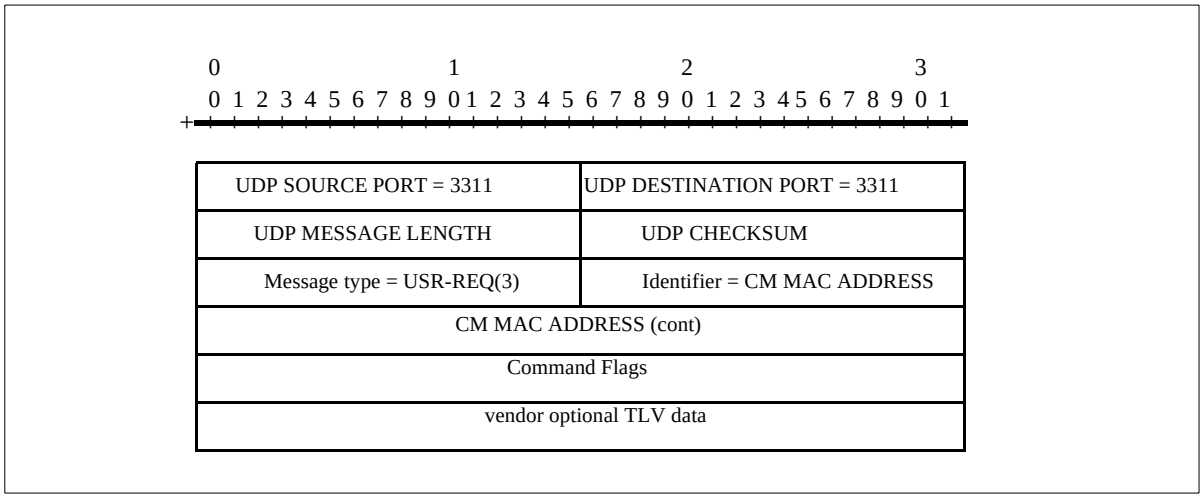

Figure 4-1. Format of the USR-REQ message

This message contains the following:

Message type Distinguishes between recovery services (message types = 3 - 4) and other services.

Identifier The CMTS uses the identifier field (CM MAC address) to match responses to requests.

Command Flags Flags to indicate which portions of the CM initialization procedure the CM should perform. The Command Flags have the following meaning:

0x0001 Restart PPP Link
0x0002 Restart DHCP process
0x0004 Re-perform transfer of operational parameters
0x0008 Re-register with the CMTS

TLV-encoded data Optional TLV-encoded information.

The format of the USR-RSP message is shown in Figure 4-2. When the CM receives a USR-REQ message, it will copy the Identifier field from the request message into the response message. The response message is sent to the CMTS Registration IP address.

After sending the USR-RSP message to the CMTS, the CM performs the restart procedure(s) as requested by each bit in the Command Flags field.

The CMTS SHOULD perform a configurable backoff and resend procedure for a USR-REQ which has not been acknowledged by a corresponding USR-RSP. The handling of this procedure and any subsequent fault handling is a vendor specific implementation.

The USR-REQ provides a mechanism that the CMTS may use to force the CMs to restart themselves, and may be used to force the CMs to re-register with the CMTS, or to change the downstream channel by supplying a different configuration file.

A summary of the USR-RSP data format is shown below. The fields are transmitted from left to right.

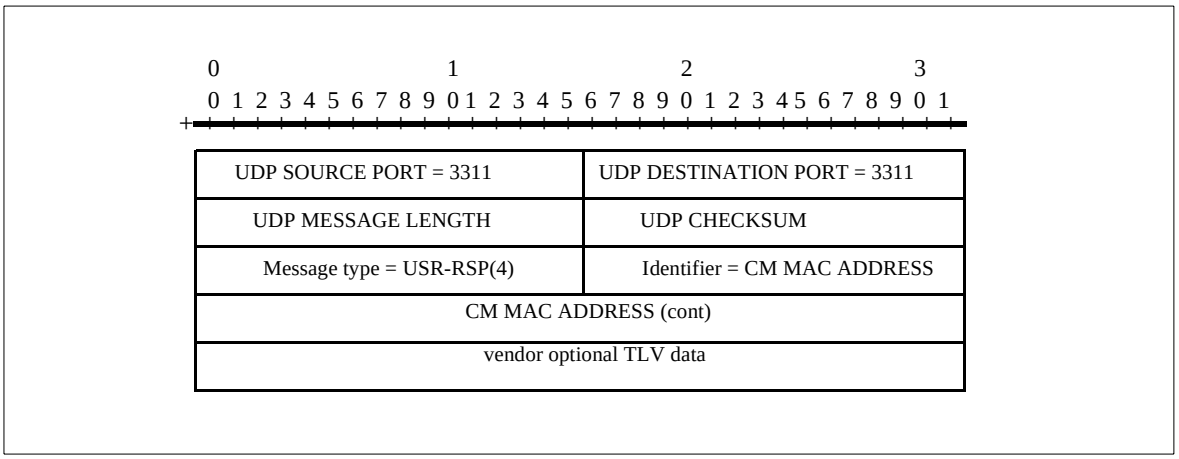

Figure 4-2. Format of the USR-RSP message

4.2 CMTS Service Recovery

4.2.1 Boot-State Detection

The CMTS MUST send periodic checkpoint status to the CMs in the TSI management message. This message consists of an epoch integer (specifies the epoch number) and the CMTS boot time (specifies the clock setting for this epoch, which uses the current clock time at boot with an unspecified accuracy). The CMTS must save these values in non-volatile RAM.

After a full CMTS initialization, on initial CMTS boot and any reboot from unplanned outages, the CMTS MUST reset the epoch integer to the default value of one, and record the current time in the CMTS boot time parameter.

If the CMTS epoch integer survives a boot/reboot, the epoch integer MUST be incremented. If there is no stored epoch value, the TSI epoch integer MUST be initialized to its default value, one.

The CMTS MUST also increment the epoch integer and add current clock time to CMTS boot time parameter whenever it flushes the forwarding and ARP tables but has not undergone full reinitialization.

4.2.2 Required Responses for Recoverable Data

The CMTS learns the CMs and CPE on the cable network through DHCP gleaning (Section 3.4.4.1 and Section 3.4.8). If a CMTS is reinitialized for recovery or maintenance, it may lose that information. In order to rebuild the CMTS forwarding and ARP tables, the CMTS MUST

rebuild CM IP address and CM MAC address information from CM registration requests. On reception of a registration request message, the CMTS MUST:

- Confirm the CM authorization (see Section 3.4.5.1).
- Update its routing and ARP tables to reflect the CM address pairing in the request. The CMTS MUST generate an SNMP trap if the IP address in the registration message is paired with a different MAC address in its tables.
- Update its routing and ARP tables to reflect the CPE IP addresses, CM MAC address pairing in the request. CPE IP addresses MUST be paired with the CM MAC address. The CMTS MUST generate an SNMP trap if the IP address in the registration is paired with a different MAC address in its tables.
- Send a modem registration response which includes all CPE IP addresses in the CMTS routing and ARP tables which are associated with the CM MAC address.

4.3 CM Service Recovery

The following sections describe service recovery for a CM that is configured in a telephone return termination mode.

4.3.1 Boot-State Detection

The CM MUST be able to determine the CMTS status. The CM MUST save the last values of the epoch integer and its associated time each time it registers. A power-cycled or reset CM MUST initialize saved epoch integer to zero. CMs MUST periodically check the state of the CMTS by comparing the epoch integer and time parameters in periodic TSI management messages with its saved values.

4.3.2 Required Responses for Recoverable Data

The CM MUST take appropriate actions based on the epoch and time parameters in the TSI message.

- If the TSI epoch integer and time do not match the epoch and time pair saved in the CM, and the CM saved epoch integer is non-zero,
    - The CM MUST go through a complete restart initialization (see Section 3.4).
    - The CM MUST include in the registration request the IP address for each valid CPE[9] on its CMCI.
    - The CM MAY proxy ARP for any CPE IP addresses in the registration response message. The CM MUST ARP on the CMCI for the hardware addresses of the CPE IP addresses and update its routing and ARP tables.

9. IP address is gleaned in CM from CMCI host DHCP requests

- The CM has just powered up (saved CM epoch integer is zero),
    - The CM MUST go through a complete reset initialization (see Section 3.4).
    - The CM MUST send a registration request and will have no CPE IP address information available to add to the request.
    - The CM MAY proxy ARP for any CPE IP addresses in the registration response message. The CM MUST ARP on the CMCI for the hardware addresses of the CPE IP addresses and update its routing and ARP tables.
    - If the TSI epoch integer is one, the CMTS has reinitialized, and would have no knowledge of prior CM CPE IP addresses. If the registration response does not have CPE IP address information for the CM, the CM MUST NOT proxy ARP for any CPE traffic on the CMCI except DHCP requests.

This page intentionally left blank.

5 Telephone Return CM Termination Mode Capabilities

Following is a non-exclusive set of capabilities addressing CM telephone connections.

5.1 Factory Default

The CM and TRAC MUST support establishment of a reliable duplex telephony[10] authenticated timed connection. The CM MUST provide a means to manually interrupt (hang up) the telephone link. The CM MAY be configured for hang-up on voice or off-hook detect. The CM MUST provide telephone-line activity monitoring.

5.2 CM Demand Dial

This is an operational model which emulates a 24-hour connected session without requiring a continuous telephony upstream connection. The CM MUST implement demand dial. Demand dial is a feature where that drops the upstream telephony path connection when a configured timer[11] determines there is no upstream activity. Whenever upstream activity is sensed, a new telephony connection is made. Demand dial is activated by a non-zero value in the Demand Dial Timer configuration setting.

10. 2-way twisted pair through PSTN
11. This timer MAY be configured by TCD message, configuration file or SNMP.

This page intentionally left blank.

6 Security

6.1 Dial-Up Authentication, Authorization and Accounting Interfaces

Remote Authentication Dial In User Service (RADIUS) authentication and accounting MUST be supported on the CM upstream telephone link [RFC-2139, RFC-2140]. RADIUS security mechanisms SHOULD be utilized with RADIUS messages.

6.2 Baseline Privacy

Telephone return CMs MUST support Baseline Privacy (BP) as is defined in [MCNS8]with the following exceptions:

- There MUST be no BP encryption over the upstream telco path.
- Key management protocol MUST use UDP/IP transport as described in this specification.
- Key management MUST NOT use the optional implicit ACK described in [MCNS8].

In [MCNS8], encryption is used on both the upstream and downstream cable paths to effectively emulate the privacy of a point-to-point connection over shared media. In telephony return, the upstream path is point-to-point, and, by definition, private. Thus, for telephony return, baseline privacy, MUST be supported unidirectionally on the downstream path only. An upstream telco link MAY use IPSEC encryption [RFC-1825][RFC-1826][RFC-1827] independent of [MCNS8].

The downstream encryption link requires key management defined in [MCNS8]. Message formats for the BPKM protocol are modeled after those of the RADIUS protocol. In RF-return CMs, BPKM transport protocol is through MAC management messages. For telephone return CMs, BPKM messages, like RADIUS messages, will run over UDP/IP. BPKM requests are addressed to well known UDP Destination Port, MCNS_SEC (to be defined). Exactly one BPKM packet is encapsulated in the UDP data field. When the server (either CMTS or a separate server) generates a response, source and destination ports are reversed . The UDP message format is shown as follows:

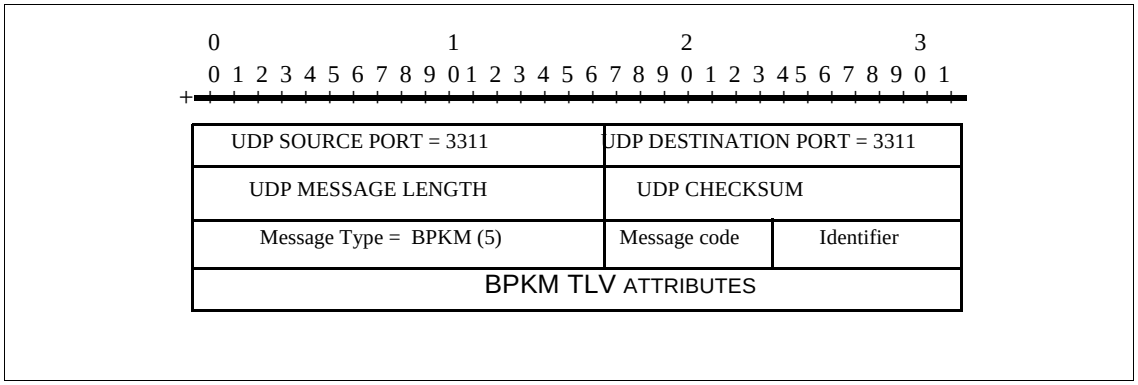

Figure 6-1. Privacy Key Management Packet

These messages contain the following:

Message type Distinguishes between BPKM services (message type = 5) and other services.

Message Code Distinguishes between BPKM requests (CM to CMTS) and responses (CMTS to CM) as well as the type of BPKM packet. This page intentionally left blank.

Identifier Aids to matching requests to responses.

TLV-encoded data Attributes are the TLV encoded key management data associated with each message.

More detailed information about message codes and their contents are defined in [MCNS8].

6.3 Full Security

Telephone return CMs MAY support security interfaces as defined in [MCNS6] [MCNS7] with the following exceptions/restrictions:

- There MUST be no Security encryption over the upstream telco path.
- Transmit control message through IP/UDP facilities as defined in [MCNS6].

In [MCNS6] encryption is used on both the upstream and downstream cable paths. In telephone return, the upstream path MUST NOT implement Security[MCNS6] encryption but MAY use IPSEC encryption [RFC-1825][RFC-1826][RFC-1827] independent of [MCNS6].

Appendix A - ITU Recommended Modulation Specifications

Modem modulations represent the physical layer used to establish connections. Issues such as connection establishment rules, transmission methods, echo cancellation, speed shifting, and retrains are defined by each modulation standard. The following ITU-T standards that the CM and TRAC SHOULD support are listed in the table below.

Modulation	Connection Rate (bps)
V.34+	2400,4800,7200,9600,12000,14400,16800,19200,21600,24000,26400,28800,31200,33600
V.34	2400,4800,7200,9600,12000,14400,16800,19200,21600,24000,26400,28800
V.FC	14400,16800,19200,21600,24000,26400,28800
V.32ter	4800,7200,9600,12000,14400,19200
V.32bis	4800,7200,9600,12000,14400
V.32	4800,9600
V.29	7200,9600 (FAX)
V.27ter	1200,4800 (FAX)
V.22bis	2400
V.22	1200
V.17	12000,14400 (FAX)

This page intentionally left blank.

Appendix B - General TLV Encoding and Cable Modem Configuration File Additions For Telephone Return

B.1 Introduction

The following table shows general TLV encoding rules for TLV attributes.

Type	The Type field is one octet. Up-to-date values of the MCNS (configuration file TLV) Typefield are specified in the most recent [MCNS2]. TLV type fields defined for Telephone Return messages are defined in this specification.
Length	The Length field is one octet, and indicates the length of the Value field. The length value excludes the length of the Type and Length fields.
Value	The Value field is zero or more octets and contains information specific to the Attribute. The format and length of the Value field is determined by the Type and Length fields. A String type is one or more octets, and its contents are implementation dependent. It is intended to be human readable but MUST NOT be null terminated, length is determined by the TLV Length parameter. The encoding format for character strings is standard NVT-ASCII [RFC-856]. A Boolean type is a 8 bit value of 0 or 1. An Integer type is a 32 bit value, most significant octet first. A Time type is a 32 bit value, most significant octet first -- seconds since 00:00:00 GMT, January 1, 1970. An undistinguished octet is an unsigned 8-bit value to be interpreted within the context of the Type field.

For the CM configuration file, the telephone return CM MUST use the configuration settings specified in [MCNS2]. A configuration file for a telephone return CM MUST have an Upstream Channel ID Configuration Setting value of zero. This setting identifies the upstream channel as a link outside of the cable plant. Additional configuration settings specific to the telephone upstream path MAY be included in a telephone return CM configuration file. This appendix lists the additional required parameters.

B.2 Telephone Return Configuration Settings

The following parameters MAY be provided in the telephone return CM configuration file. These parameters are in the same TLV format described in [MCNS2].

B.2.1 Telephone Settings Option

This configuration setting describes parameters which are specific to telephone return systems. It is composed from a number of encapsulated type/length/value fields. The encapsulated fields define the specific parameters for the modem in use. Note that these type fields are only valid within the encapsulated capabilities option string.

- **Telephony Return Interface SPD Settings** - sub-types containing per-modem telephone return SPD configuration settings.

Type	Len	Value
TRI_CFG01	n = length of all following sub-types	sub-types

- **Service Provider Name** - This service provider name supersedes and replaces any stored number from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	2	n	NVT-ASCII string representing service provider.

- **Telephone Number** - This number supersedes and replaces any stored number from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	3	n	NVT-ASCII string representing phone number (1).

- **Telephone Number** - This number supersedes and replaces any stored number from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	4	n	NVT-ASCII string representing phone number (2)

- **Telephone Number** - This number supersedes and replaces any stored number from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	5	n	NVT-ASCII string representing phone number (3).

- **Connection Threshold** - This value supersedes and replaces any stored connection threshold from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	6	1	This is the retry count threshold for registration attempts.

- **Login Username** -
  This name supersedes and replaces any stored username from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	7	n	NVT-ASCII string representing login username to be used for PPP authentication.

- **Login Password** - This name supersedes and replaces any stored name from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	8	n	NVT-ASCII string representing password name to be used for PPP authentication.

- **DHCP Authenticate** - This value supersedes and replaces any stored value from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	9	1	Boolean value representing true/ false DHCP Server authentication.

- **DHCP Server** - This value supersedes and replaces any stored address for DHCP server from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	10	4	Integer IPaddress

- **RADIUS realm** - This realm name supersedes and replaces any stored realm name from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	11	n	NVT-ASCII string representing a RADIUS realm name to be used for PPP authentication.

- **PPP Authenticate** - Type/sub-typeLenValue(sub-type) TRI_CFG01/121 This value supersedes and replaces any stored value from the TCD management message.

Type	sub-type	Len	Value
TRI_CFG01	12	1	Undistinguished octet value representing PPP authentication method.

- **Demand Dial Inactivity Timer Threshold**- Demand dial inactivity timer monitors network inactivity at the CM. The purpose of demand dial is to limit the CM (upstream) network connectivity to periods of time when connectivity is required. The amount of time (in seconds) of this parameter is the measure of inactive networking time allowed to elapse before hanging up a telephone connection at the

CM. If this optional parameter is not present, or set to 0, then the demand dial feature is not used.

Type	sub-type	Len	Value
TRI_CFG01	13	4	Integer

- **SNMP IP Address** - This is the IP address of the SNMP Manager. The CM uses this address to report a problem with the cable network.

Type	sub-type	Len	Value
TRI_CFG02	none	4	Integer IPaddress

[MCNS2] defines specific values for TRI_CFG01 and TRI_CFG02.

This page intentionally left blank.

Appendix C - Sample Dial-Up Networking Script

Following is a generic dial-up networking script:

```
proc main
 ; Initialize modem and send dial string
 ; Wait for "connect" and immediately enter PPP negotiation with TRAC
 transmit AT command sequence for initialization (Vendor Specific)
 transmit AT command sequence for dial sequence (Vendor Specific)
 waitfor "Connect"
 ; Wait a couple of seconds and then prod the terminal server
 delay 2
 transmit "^M"

 ; TRAC MAY prompt to enter username and password from TCD.
 ; Send the user name and password.
 ; Note that "^M"  <ENTER> key character MAY be necessary

 waitfor "Username:"
 transmit $USERID
 transmit "^M”

 waitfor "Password:"
 transmit $PASSWORD
 transmit "^M"
```

```
delay 5

endproc
```

Appendix D - References

[DVMRP1] "Distance Vector Multicast Routing Protocol," T. Pusateri, Juniper Networks, February 1997. IETF Draft: draft-ietf-idmr-dvmrp-v3-04.txt.

[EIA RS-232E] "Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange," Electronic Industries Association, July, 1991.

[IEEE802] IEEE Std 802-1990, Local and Metropolitan Area Networks: Overview and Architecture.

[MCNS1] MCNS Data Over Cable Service Interface Specification Request for Proposals, December 11, 1995 (can be downloaded on the World Wide Web from http://www.cablemodem.com/).

[MCNS2] MCNS Cable Modem Termination System - Radio Frequency Interface Specification SP-RFII01-970321, March 21, 1997.

[MCNS3] MCNS Cable Modem Termination System - Network-Side Interface Specification SP-CMTS-NSID04-960409 (CMTS-NSI), April 9, 1996.

[MCNS4] MCNS Cable Modem to Customer Premises Equipment Interface Specification SP-CMCID04-960409 (CMCI), April 9, 1996.

[MCNS5] MCNS Data Over Cable System Operations Support System Interfaces, SP-OSSI01-970403, April 4,1997.

[MCNS6] MCNS Data Over Cable System Services Security Specification, SP-DOCSS, SP-SSI01970422, April 22, 1997.

[MCNS7] MCNS Cable Modem Removable Security Module SP-RSM (in preparation).

[MCNS8] MCNS Baseline Privacy Interface Specification SP-BPI (in preparation).

[RFC-768] J. Postel, "User Datagram Protocol", 08/28/1980.

[RFC-791] J. Postel, "Internet Protocol", 09/01/1981.

[RFC-792] J. Postel, "Internet Control Message Protocol", 09/01/1981.

[RFC-793] J. Postel, "Transmission Control Protocol", 09/01/1981.

[RFC-826] D. Plummer, “Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware”, 11/01/1982.

[RFC-856] J. Postel, J. Reynolds, “TELNET Binary Transmission”, May 1983.

[RFC-1027] Smoot Carl-Mitchell, John S. Quarterman, “Using ARP to Implement Transparent Subnet Gateways”, October 1987.

[RFC-1058] C. Hedrick, “Routing Information Protocol”, 06/01/1988.

[RFC-1112] S. Deering, “Host extensions for IP multicasting”, 08/01/1989.

[RFC-1157] M. Schoffstall, M. Fedor, J. Davin, J. Case, “A Simple Network Management Protocol (SNMP)”, 05/10/1990.

[RFC-1256] S. Deering, “ICMP Router Discovery Messages”, 09/05/1991.

[RFC-1332] G. McGregor, “The PPP Internet Protocol Control Protocol (IPCP)”, 05/26/1992.

[RFC-1350] K. Sollins, "THE TFTP PROTOCOL (REVISION 2)", 07/10/1992.

[RFC-1542] W. Wimer, “Clarifications and Extensions for the Bootstrap Protocol”, 10/08/1993.

[RFC-1583] J. Moy, “OSPF Version 2", 03/23/1994.

[RFC-1661] W. Simpson, “The Point-to-Point Protocol (PPP)”, 07/21/1994.

[RFC-1662] W. Simpson, “PPP in HDLC-like Framing”, 07/21/1994.

[RFC-1663] D. Rand, “PPP Reliable Transmission”, 07/21/1994.

[RFC-1723] G. Malkin, “RIP Version 2 Carrying Additional Information”, 11/15/ 1994.

[RFC-1825] R. Atkinson, “Security Architecture for the Internet Protocol”, 08/09/ 1995.

[RFC-1826] R. Atkinson, “IP Authentication Header”, 08/09/1995.

[RFC-1827] R. Atkinson, “IP Encapsulating Security Payload (ESP)”, 08/09/1995.

[RFC-1918] Y. Rekhter, R. Moskowitz, D. Karrenberg, G. de Groot, E. Lear, “Address Allocation for Private Internets”, 02/29/1996.

[RFC-2003] C. Perkins, "IP Encapsulation within IP", 10/22/1996

[RFC-2131] R. Droms, "Dynamic Host Configuration Protocol", 04/07/1997.

[RFC-2132] S. Alexander, R. Droms, "DHCP Options and BOOTP Vendor Extensions", 04/07/1997.

[RFC-2139] C. Rigney, "RADIUS Accounting", 4/18/1997

[RFC-2140] C. Rigney, A. Rubens, W. Simpson, S. Willens,"Remote Authentication Dial-In User Service (RADIUS)", RFC-2140, 4/18/ 1997

[SMS] The Spectrum Management Application (SMA) and the Common Spectrum Management Interface (csmi). Time Warner Cable, December 24, 1995.

This page intentionally left blank.

Appendix E - Glossary

Address Resolution Protocol (ARP)
A protocol of the IETF for converting network addresses to 48-bit Ethernet addresses.

American Standard Code for Information Interchange (ASCII)
The ASCII character set is as defined in the ARPA-Internet

Asynchronous Transfer Mode (ATM)
A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.

Broadcast Addresses
A predefined destination address that denotes the set of all data network service access points

Cable Modem (CM)
A modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system.

Cable Modem Termination System (CMTS)
Cable modem termination system, located at the cable television system headend or distribution hub, which provides complementary functionality to the cable modems to enable data connectivity to a wide-area network.

Cable Modem Telephone Return Interface (CMTRI)
The interface between a CM and the public switched telephone network, for CMs that use the telephone network for the return or upstream path.

Cable Modem Termination System - Network Side Interface (CMTS-NSI)
The interface, defined in [MCNS3], between a CMTS and the equipment on its network side.

Cable Modem to CPE Interface (CMCI)
The interface, defined in [MCNS4], between a CM and CPE.

Customer Premises Equipment (CPE)
Equipment at the end user's premises; MAY be provided by the end user or the service provider.

Data Link Layer
Layer 2 in the Open System Interconnection (OSI) architecture; the layer that provides services to transfer data over the transmission link between open systems.

Downstream
In cable television, the direction of transmission from the headend to the subscriber.

Dynamic Host Configuration Protocol (DHCP)
An Internet protocol used for assigning network-layer (IP) addresses.

End User
A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network.

Forward Channel
The direction of RF signal flow away from the headend toward the end user; equivalent to Downstream.

Headend
The central location on the HFC network that is responsible for injecting broadcast video and other signals in the downstream direction. See also Master Headend, Distribution Hub.

Hybrid Fiber/Coax (HFC) System
A broadband bidirectional shared-media transmission system using fiber trunks between the headend and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.

Internet Control Message Protocol (ICMP)
An Internet network-layer protocol.

Institute of Electrical and Electronic Engineers (IEEE)
A voluntary organization which, among other things, sponsors standards committees and is accredited by the American National Standards Institute.

Internet Engineering Task Force (IETF)
A body responsible, among other things, for developing standards used in the Internet.

Internet Protocol (IP)
An Internet network-layer protocol.

International Organization for Standardization (ISO)
An international standards body, commonly known as the International Standards Organization.

Local Area Network (LAN)
A non-public data network in which serial transmission is used for direct data communication among data stations located on the user's premises.

Logical Link Control (LLC) Procedure
In a local area network (LAN) or a Metropolitan Area Network (MAN), that part of the protocol that governs the assembling of data link layer frames and their exchange between data stations, independent of how the transmission medium is shared.

MAC Service Access Point
See [MCNS2].

Media Access Control (MAC) Address
The "built-in" hardware address of a device connected to a shared medium.

Media Access Control (MAC) Procedure
In a subnetwork, that part of the protocol that governs access to the transmission medium independent of the physical characteristics of the medium, but taking into account the topological aspects of the subnetworks, in order to enable the exchange of data between nodes. MAC procedures include framing, error protection, and acquiring the right to use the underlying transmission medium.

Media Access Control (MAC) Sublayer
The part of the data link layer that supports topology-dependent functions and uses the services of the Physical Layer to provide services to the logical link control (LLC) sublayer.

Multimedia Cable Network System (MCNS) Partners
A consortium of Comcast Cable Communications, Inc., Cox Communications, Tele-Communications, Inc., and Time Warner Cable, interested in deploying high-speed data communications systems on cable television systems.

National Cable Television Association (NCTA)
A voluntary association of cable television operators which, among other things, provides guidance on measurements and objectives for cable television systems in the USA

National Television Systems Committee (NTSC)
Committee which defined the analog color television broadcast standard used today in North America.

Network Layer
Layer 3 in the Open System Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.

Network Management
The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.

Network Virtual Terminal (NVT)
The Network Virtual Terminal is defined in the Telnet Protocol [RFC-856] with respect to enhanced ASCII standards.

Open Systems Interconnection (OSI)
A framework of ISO standards for communication between different systems made by different vendors, in which the communications process is organized into seven different

categories that are placed in a layered sequence based on their relationship to the user. Each layer uses the layer immediately below it and provides a service 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.

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 Std 802 for use in Local and Metropolitan Area Network applications.

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.

Protocol
A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions.

Quadrature Amplitude Modulation (QAM)
A method of modulating digital signals onto a radio-frequency carrier signal involving both amplitude and phase coding.

Quartenary Phase-Shift Keying (QPSK)
A method of modulating digital signals onto a radio-frequency carrier signal using four phase states to code two digital bits.

Radio Frequency (RF)
In cable television systems, this refers to electromagnetic signals in the range 5 to 1000 MHz.

Reverse Channel
The direction of signal flow towards the headend, away from the subscriber; equivalent to Upstream.

Request For Comments (RFC)
A technical policy document of the IETF; these documents can be accessed on the World Wide Web at http://ds.internic.net/ds/rfcindex.html.

Service Access Point (SAP)
The point at which services are provided by one layer, or sublayer to the layer immediately above it.

Service Data Unit (SDU)
Information that is delivered as a unit between peer service access points

Service Identifier (SID)
See[MCNS2].

Simple Network Management Protocol (SNMP)
A network management protocol of the IETF.

Spectrum Management System (SMS)
A system, defined in [SMS], for managing the RF cable spectrum.

Sublayer
A subdivision of a layer in the Open System Interconnection (OSI) reference model.

Subnetwork
Subnetworks are physically formed by connecting adjacent nodes with transmission links.

Subnetwork Access Protocol (SNAP)
An extension of the LLC header to accommodate the use of 802-type networks as IP networks.

Telephone Return Termination System (TRTS)
The equipment which connects both the upstream and downstream paths from the Cable Modem to the LAN or Internet. The TRTS consists of the CMTS and the TRAC, which are not necessarily located at the same site.

Telephone Return Access Concentrator (TRAC)
The equipment which terminates dial-up PPP sessions from the CMs. Also called “Remote Access Servers.”

Telephone Return Access Concentrator - Network Side Interface (TRAC-NSI)
The interface between a TRAC and the equipment on its network side.

Transmission Control Protocol (TCP)
A transport-layer Internet protocol which ensures successful end-to-end delivery of data packets without error.

Trivial File-Transfer Protocol (TFTP)
An Internet protocol for transferring files without the requirement for user names and passwords that is typically used for automatic downloads of data and software.

Type/Length/Value (TLV)
An encoding of three fields, in which the first field indicates the type of element, the second the length of the element, and the third field the value.

Upstream
The direction from the subscriber location toward the headend.

This page intentionally left blank.

Acknowledgement

Jack Fijolek, David Willming and Levent Gun of US Robotics, Inc. wrote most of this document.

We are grateful to these individuals and their organization for their contribution.

This page intentionally left blank.