



***Society of Cable
Telecommunications
Engineers***

**ENGINEERING COMMITTEE
Data Standards Subcommittee**

AMERICAN NATIONAL STANDARD

ANSI/SCTE 22-2 2012

**Data-Over-Cable Service Interface Specification
DOCSIS 1.0 Baseline Privacy Interface (BPI)**

NOTICE

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

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

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

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

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2012
140 Philips Road
Exton, PA 19341

Table of Contents

1	SCOPE AND PURPOSE.....	1
1.1	SCOPE	1
1.2	REQUIREMENTS	1
1.3	BACKGROUND	1
1.3.1	<i>Service Goals</i>	<i>1</i>
1.3.2	<i>Reference Architecture</i>	<i>2</i>
2	BASELINE PRIVACY OVERVIEW	5
2.1	OPERATIONAL OVERVIEW.....	6
2.1.1	<i>Cable Modem Initialization</i>	<i>6</i>
2.1.2	<i>Cable Modem Key Update Mechanism</i>	<i>7</i>
3	VARIABLE-LENGTH PACKET PDU FORMAT	9
4	BASELINE PRIVACY KEY MANAGEMENT (BPKM) PROTOCOL	13
4.1	STATE MODELS	13
4.1.1	<i>Introduction</i>	<i>13</i>
4.1.2	<i>Authorization State Machine</i>	<i>15</i>
4.1.3	<i>TEK State Machine.....</i>	<i>24</i>
4.2.1	<i>Packet Formats.....</i>	<i>32</i>
4.2.2	<i>BPKM Attributes.....</i>	<i>39</i>
5	KEY USAGE.....	53
5.1	CABLE MODEM	53
5.2	CMTS.....	53
5.3	MULTICAST KEY HANDLING.....	55
6	CRYPTOGRAPHIC METHODS	57
APPENDIX A.	TFTP CONFIGURATION FILE EXTENSIONS (NORMATIVE).....	59
APPENDIX B.	EXAMPLE MESSAGES AND PDUS (INFORMATIVE)	65
APPENDIX C.	REFERENCES	83

This page intentionally left blank.

Figures

FIGURE 1-1.	TRANSPARENT IP TRAFFIC THROUGH THE DATA-OVER-CABLE SYSTEM	2
FIGURE 1-2.	DATA-OVER-CABLE REFERENCE ARCHITECTURE	3
FIGURE 3-1.	FORMAT OF ETHERNET/802.3 PACKET PDU WITH PRIVACY EH ELEMENT	9
FIGURE 4-1.	AUTHORIZATION STATE MACHINE FLOW DIAGRAM	17
FIGURE 4-2.	TEK STATE MACHINE FLOW DIAGRAM	25

Tables

TABLE 3-1.	BASELINE PRIVACY EH ELEMENT FORMATS	11
TABLE 4-1.	AUTHORIZATION FSM STATE TRANSITION MATRIX	18
TABLE 4-2.	TEK FSM STATE TRANSITION MATRIX	26
TABLE 4-3.	BASELINE PRIVACY KEY MANAGEMENT MAC MESSAGES	32
TABLE 4-4.	BASELINE PRIVACY KEY MANAGEMENT MESSAGE CODES	33
TABLE 4-5.	AUTHORIZATION REQUEST ATTRIBUTES	35
TABLE 4-6.	AUTHORIZATION REPLY ATTRIBUTES	35
TABLE 4-7.	AUTH REJECT ATTRIBUTES	36
TABLE 4-8.	KEY REQUEST ATTRIBUTES	36
TABLE 4-9.	KEY REPLY ATTRIBUTES	37
TABLE 4-10.	KEY REJECT ATTRIBUTES	38
TABLE 4-11.	AUTHORIZATION INVALID ATTRIBUTES	39
TABLE 4-12.	TEK INVALID ATTRIBUTES	39
TABLE 4-13.	BPKM ATTRIBUTE TYPES	40
TABLE 4-14.	ATTRIBUTE VALUE DATA TYPES	41
TABLE 4-15.	TEK-PARAMETERS SUB-ATTRIBUTES	49
TABLE 4-16.	ERROR-CODE ATTRIBUTE CODE VALUES	52
TABLE A-1.	RECOMMENDED OPERATIONAL RANGES FOR BPI CONFIGURATION PARAMETERS	62
TABLE A-2.	SHORTENED BPI PARAMETER VALUES FOR PROTOCOL TESTING	63

This page intentionally left blank.

1 Scope and Purpose

1.1 Scope

The intent of this specification is to describe a simple Data Privacy function for CMTS-CM communications in the Data-Over-Cable system. While there exists a requirement for secure communications over the cable network in order to protect broadcast content and other high value data transactions, this specification is intended to provide a minimum level of Data Privacy and protection from theft of service for Internet access-like services.

1.2 Requirements

Throughout this document, 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 this specification. |
| “MUST NOT” | This phrase means that the item is an absolute prohibition of this 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. |

Other text is descriptive or explanatory.

1.3 Background

1.3.1 Service Goals

Cable operators are interested in deploying high-speed data communications systems on cable television systems that are capable of supporting a wide variety of services. Services under

consideration by cable operators include packet telephony service, video conferencing service, T1/frame relay equivalent service, and many others. To this end, CableLabs' member companies have prepared a series of interface specifications that permit the definition, design, development, and deployment of data-over-cable systems on a uniform, consistent, open, non-proprietary, multi-vendor interoperable basis.

The service allows transparent bi-directional transfer of Internet Protocol (IP) traffic, between the cable system headend and customer locations, over an all-coaxial or hybrid fiber/coax (HFC) cable television network. This is shown in simplified form in Figure 1-1.

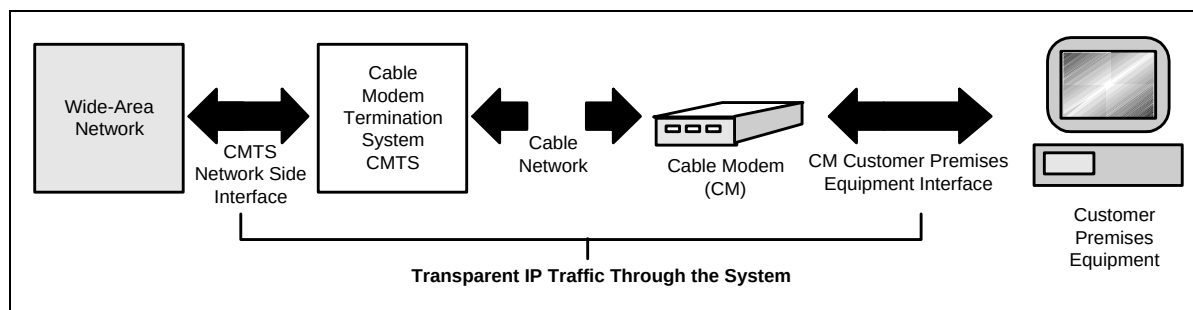


Figure 1-1. Transparent IP Traffic Through the Data-Over-Cable System

The transmission path over the cable system is realized at the headend by a CMTS, and at each customer location by a CM. At the headend (or hub), the interface to the data-over-cable system is called the Cable Modem Termination System - Network-Side Interface (CMTS-NSI) and is specified in [DOCSIS3]. At the customer locations, the interface is called the cable-modem-to-customer-premise-equipment interface (CMCI) and is specified in [DOCSIS4]. The intent is for the DOCSIS operators to transparently transfer IP traffic between these interfaces, including but not limited to datagrams, DHCP, ICMP, and IP Group addressing (broadcast and multicast).

1.3.2 Reference Architecture

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

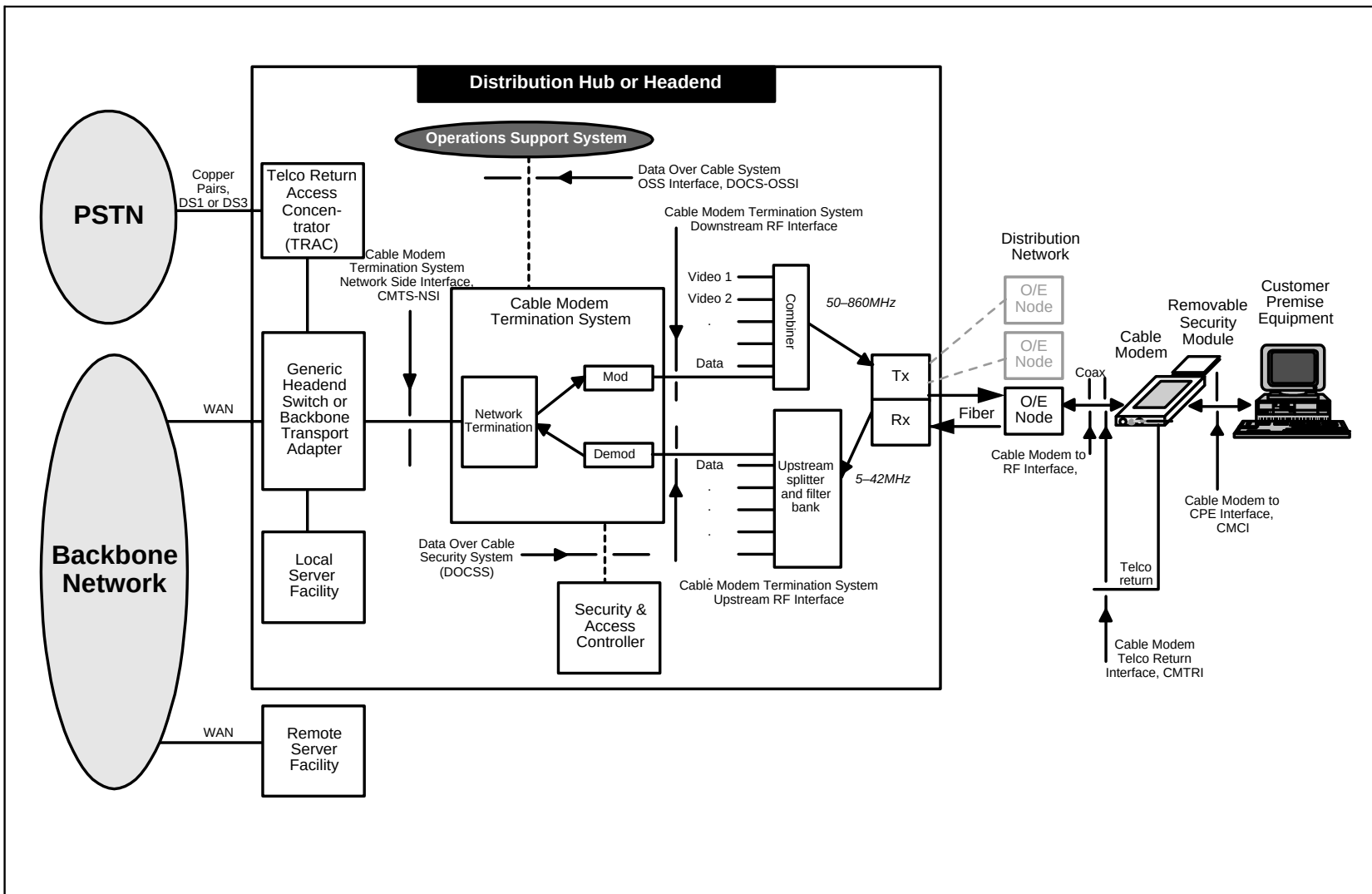


Figure 1-2. Data-over-Cable Reference Architecture

1.3.2.1 Categories of Interface Specification

The basic reference architecture of Figure 1-2 involves three categories of interfaces.

a) Category 1

Data Interfaces - These are the CMCI [DOCSIS4] and CMTS-NSI [DOCSIS3], 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) Category 2

Operations Support System Interfaces - OSSI is the element management layer interface between the network elements and higher level OSSes which support the basic business processes and are documented in [DOCSIS5].

c) Category 3

RF Interfaces -

- Between the cable modem and the HFC network [DOCSIS1]
- Between the CMTS and the HFC network, in the downstream direction (traffic toward the customer) [DOCSIS1]
- Between the CMTS and the HFC network, in the upstream direction (traffic from the customer) [DOCSIS1]

Security requirements -

- The Data-Over-Cable Baseline Privacy interface specification is this document.

1.3.2.2 Data-Over-Cable Interface Documents

A list of the documents in the Data-Over-Cable Interface Specifications family is provided below. For updates, please refer to <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-BPI	Operations Support System Interface Baseline Privacy Interface
SP-OSSI-RFI	Operations Support System Interface Radio Frequency MIB
SP-RFI	Radio Frequency Interface Specification

Key to Designation:

SP Specification

2 Baseline Privacy Overview

Baseline Privacy provides cable modem users with data privacy across the RF network. It provides user data privacy by encrypting traffic flows between CM and CMTS.

A secondary goal of Baseline Privacy is to provide cable operators with basic protection from theft of service. To provide *strong* protection against theft of service, the CMTS would need to authenticate client CMs: the CMTS would need to establish a unique, verifiable identity for a cable modem and authenticate key requests claiming to be from that cable modem. In addition, the CMTS would need to link the cable modem identity to a paying subscriber, and to the data services that subscriber is authorized to access.

Since data privacy is Baseline Privacy's principal service goal, and given neither CM nor CMTS authentication are prerequisite for providing user data privacy, Baseline Privacy's key distribution protocol does not authenticate CM and CMTS (i.e., it does not employ authentication mechanisms such as passwords or digital signatures). In the absence of authentication, Baseline Privacy provides basic protection of service by insuring that a modem, uniquely identified by its 48-bit IEEE MAC address, can only obtain keying material for services it is authorized to access. Since it does not authenticate CMs, it cannot protect against an attacker employing a *cloned* modem, masquerading as an authorized modem.

Baseline Privacy security services are defined as a set of extended services within the Media Access Control (MAC) sublayer. Packet header information specific to Baseline Privacy is located in a Privacy Extended Header (EH) element in the MAC Extended Header, as defined in. Figure 3-1 depicts an MAC Packet Data PDU containing the Privacy EH element. Two new MAC management message types, BPKM-REQ and BPKM-RSP, have been defined to support the Baseline Privacy Key Management (BPKM) protocol.

Baseline Privacy uses the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm [FIPS-46, FIPS-46-1, FIPS-74, FIPS-81] to encrypt the Packet PDU field in both upstream and downstream RF MAC Packet Data PDUs. The MAC headers of these Packet Data PDUs MUST NOT be encrypted. The payloads, as well as headers, of MAC management messages MUST be sent in the clear to facilitate registration, ranging, and normal operation of the MAC sublayer.

Baseline Privacy extends the definition of the MAC sublayer's Service ID (SID). The Radio Frequency Interface Specification defines a SID as a mapping between CM and CMTS for the purposes of upstream bandwidth allocation and class-of-service management. In this context, the SID only has upstream significance. When Baseline Privacy is in operation, the SID also identifies a particular security association and, thus, has both upstream and downstream significance. A downstream multicast traffic flow, then, which normally would have no SID associated with it, will have an associated SID when Baseline Privacy is operational. The Privacy Extended Header Element includes the SID associated with the MAC Packet Data PDU; the SID, in combination with other components of the extended header element, identifies to a modem the keying material required to decrypt the MAC PDU's Packet Data field.

Baseline Privacy's key management protocol runs between CM and CMTS; CMs use the protocol to obtain authorization and traffic keying material (pertaining to a particular SID) from the CMTS, and to support periodic reauthorization and key refresh. The key management protocol uses RSA [RSA, RSA1], a public-key encryption algorithm, and the Electronic Codebook (ECB) mode of DES [FIPS-81] to secure key exchanges between CM and CMTS. CMs **MUST** have factory-installed RSA private/public key pairs, or provide an internal algorithm to generate such key pairs dynamically. If a CM relies on an internal algorithm to generate its private/public key pair, the CM **MUST** generate the key pair prior to its first Baseline Privacy establishment, defined in Section 2.1.1. Internal key pair generation **MUST** be a one-time-only operation: once a key pair is generated, it **MUST** be retained for the operational life of the CM.

A SID's keying material (DES key and CBC Initialization Vector) has a limited lifetime. When the CMTS delivers SID keying material to a CM, it also provides the CM with that material's remaining lifetime. It is the responsibility of the CM to request new keying material from the CMTS before the current set of keying material expires at the CMTS.

2.1 Operational Overview

2.1.1 Cable Modem Initialization

[DOCSIS1] divides cable modem initialization into the following sequence of tasks:

- scan for downstream channel and establish synchronization with the CMTS
- obtain transmit parameters
- perform ranging
- establish IP connectivity (DHCP)
- establish time of day
- transfer operational parameters (download parameter file via TFTP)
- perform CMTS registration

Baseline Privacy establishment follows CMTS registration.

If a CM is to run Baseline Privacy, its parameter file, downloaded during the transfer of operational parameters, **MUST** include Baseline Privacy Configuration Settings. These additional configuration settings are defined in Appendix A.

Upon completing CMTS registration, the CMTS will have assigned Service IDs (SIDs) to the registering CM that match the CM's class-of-service provisioning. If a CM is configured to run Baseline Privacy, CMTS registration is immediately followed by initialization of the CM's Baseline Privacy security functions.

Baseline Privacy initialization begins with the CM sending the CMTS an authorization request, containing data identifying the CM (e.g., MAC address), the CM's RSA public key,

and a list of zero or more assigned unicast SIDs that have been configured to run Baseline Privacy. (The list is empty if a cable modem is configured to run Baseline Privacy only on multicast SIDs.)

If the CMTS determines the requesting CM is authorized for these services, the CMTS responds with an authorization reply containing a list of SIDs (both unicast and multicast) on which the CM is permitted to run Baseline Privacy. The reply also includes an authorization key from which the CM and CMTS derive the keys needed to secure a CM's subsequent requests for per-SID traffic encryption keys, and the CMTS's responses to these requests. The authorization key is encrypted with the receiving cable modem's public key.

After successfully completing authorization with the CMTS, the cable modem sends key requests to the CMTS, requesting traffic encryption keys to use with each of its Baseline Privacy SIDs. A CM's traffic key requests are authenticated using a keyed hash (the HMAC algorithm [RFC2104]); the message authentication key is derived from the authorization key obtained during the earlier authorization exchange. The CMTS responds with key replies containing the traffic encryption keys; the keys are DES-encrypted with a key encryption key derived from the authorization key. Like the Key Requests, Key Replies are authenticated with a keyed hash, where the message authentication key is derived from the authorization key.

2.1.2 Cable Modem Key Update Mechanism

The traffic encryption keys which the CMTS provides to client CMs have a limited lifetime. The CMTS delivers a key's remaining lifetime, along with the key value, in the key replies it sends to its client CMs. The CMTS controls which keys are current by flushing expired keys and generating new keys. It is the responsibility of individual cable modems to ensure the keys they are using match those the CMTS is using. Cable modems do this by tracking when a particular SID's key is scheduled to expire and issuing a new key request for the latest key prior to that expiration time.

In addition, cable modems are required to periodically reauthorize with the CMTS; as with traffic encryption keys, an authorization key has a finite lifetime which the CMTS provides the CM along with the key value. It is the responsibility of the cable modem to reauthorize and obtain a new authorization key and a current list of supported SIDs before the CMTS expires the current authorization key.

Baseline Privacy initialization and key update is implemented within the Baseline Privacy Key Management protocol, defined in detail in Section 4.

This page intentionally left blank.

3 Variable-Length Packet PDU Format

Figure 3-1 depicts the format of a variable-length Packet Data PDU with a Privacy Extended Header (EH) element and encrypted Packet PDU payload. The first 12 octets of the Packet PDU, containing the Ethernet/802.3 destination and source addresses (DA/SA), **MUST NOT** be encrypted. Transmitting a frame's destination and source addressing in the clear provides vendors with greater flexibility in how they integrate encryption/decryption with MAC functionality; e.g., vendors have freedom to choose between filtering on DA/SA or SID first. On a SID for which BPI has been activated, the entire Packet PDU, apart from the first 12 octets, **MUST** be encrypted. The Ethernet/802.3 CRC is included in the encrypted section of the Packet PDU.

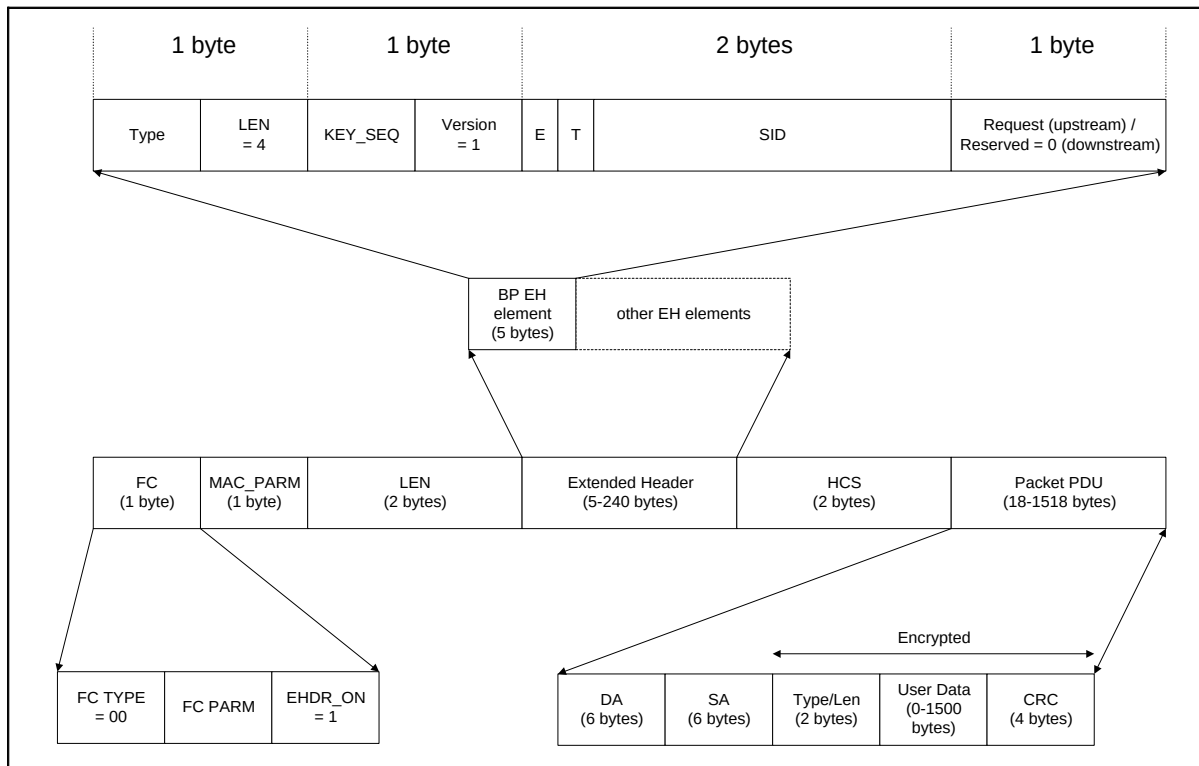


Figure 3-1. Format of Ethernet/802.3 Packet PDU with Privacy EH Element

The CMTS includes the Privacy EH element in all downstream Packet Data PDUs it encrypts under Baseline Privacy. Similarly, a CM includes the Privacy EH element in all upstream Packet Data PDUs it encrypts under Baseline Privacy.

The Privacy Extended Header element employs two EH element type values, BPI_UP and BPI_DOWN, for use with upstream and downstream Packet Data PDUs, respectively. This defines the specific EH element type values assigned to BPI_UP and BPI_DOWN.

The Privacy EH element's value field is 4 bytes long. The high-order 4 bits of the value field's first byte contain a key sequence number, KEY_SEQ. Recall that the keying material associated with a Privacy-enabled SID has a limited lifetime, and that it is the cable modem's

responsibility to request and obtain updated keying material from the CMTS before the current material expires. The CMTS distributes its latest keying material in response to a client CM's traffic key requests. The CMTS manages a 4-bit key sequence number independently for each SID and distributes this key sequence number along with the SID's keying material. The CMTS **MUST** increment the key sequence number with each new generation of keying material. The Privacy EH element includes this sequence number, along with the SID, to identify the specific generation of that SID's keying material being used to encrypt the attached Packet PDU. Being a 4-bit quantity, the sequence number wraps around to 0 when it reaches 15.

Comparing a received frame's key sequence number with the "current" key sequence number, a CM or CMTS can easily recognize a loss of key synchronization with its peer. A CM **MUST** maintain a minimum of two keys (and their respective CBC Initialization Vectors) for each Privacy-enabled SID. Keeping on-hand at least the two most recent key generations is necessary to maintain uninterrupted multicast service during a multicast SID's key transition.

The 4 bits following KEY_SEQ contain a protocol version number, which for this initial release will be set to 1.

The next two bytes contain the 2 bits of encryption status and the 14-bit SID. The ENABLE encryption status bit indicates whether encryption is enabled or disabled for that PDU. If the ENABLE bit is 0, the Packet PDU is not encrypted and the Privacy EH element **MUST** be ignored (with the exception of the optional piggybacked bandwidth request—see below). The TOGGLE bit **MUST** match the state of the Least-Significant Bit (LSB) of KEY_SEQ, the Key Sequence Number.

The RF MAC protocol defines a Request EH element for piggybacking a bandwidth request on a data transmission. Baseline Privacy defines an additional mechanism for piggybacking bandwidth requests: the final byte of Baseline Privacy's upstream EH element (EH element type = BPI_UP) is used to carry an optional piggybacked bandwidth allocation request. If there is a piggybacked request, the byte represents the number of requested mini-slots or ATM cells. The 14-bit SID within the Privacy EH element **MUST** identify the Service ID making the request. If there is no piggybacked request within the Privacy EH element, the request byte is set to zero. A piggybacked request within the Privacy EH element **MUST** be processed regardless of the status of the ENABLE bit.

In downstream packets (extended header element type = BPI_DOWN) the final byte is reserved and set to zero.

When operating Baseline Privacy, the two EH Element types, one for upstream, one for downstream, **MUST** be used on encrypted Packet Data PDUs. The BPI Extended Header elements **MUST** be formatted as shown in Table 3-1.

Table 3-1. Baseline Privacy EH Element Formats

EH_TYPE	EH_LEN	EH_VALUE
BPI__UP See [DOCSIS1]	4	KEY_SEQ (4 bits), Version (4 bits), SID (2 bytes), Request [piggyback] (1 byte) [CM --> CMTS] KEY_SEQ field (4 bits): Key sequence number Version field (4 bits) is defined as: 0x1 SID field is defined as: Bit[15]: ENABLE: 1..Encryption enabled; 0..Encryption Disabled Bit[14]: TOGGLE: 1..Odd Key; 0..Even Key Bit[13:0]: Service ID Request field contains the number of mini-slots requested for upstream bandwidth.
BPI__DOWN See [DOCSIS1]	4	KEY_SEQ (4 bits), Version (4 bits), SID (2 bytes), Reserved (1 byte) [CMTS --> CM] KEY_SEQ field (4 bits): Key sequence number Version field (4 bits) is defined as: 0x1 SID field is defined as: Bit[15]: ENABLE: 1..Encryption enabled; 0..Encryption Disabled Bit[14]: TOGGLE: 1..Odd Key; 0..Even Key Bit[13:0]: Service ID Reserved field is set to 0.

The format of the extended header element remains the same whether or not encryption is used for that particular frame and whether or not there is a piggybacked request. In the case that encryption is not used for that PDU, ENABLE, Bit[15] of the SID field, MUST be set to zero. If there is a piggybacked request, the request byte represents the number of mini-slots or ATM cells required.

If Baseline Privacy Encryption is being applied to a particular traffic session (either a unicast bidirectional flow or a multicast downstream flow), then all Packet Data PDUs associated with that flow, including any upstream Packet Data PDUs transmitted in contention intervals, MUST include a Privacy Extended Header element. If there are multiple Extended Header elements present, the Data Privacy Header element MUST be first.

In the case of encrypted transmissions in an upstream contention interval, the SID in the Data Privacy Header MUST identify the security association; it MUST NOT be set to the Request/Data contention interval's well-known Multicast Service ID.

If Privacy is not enabled on a particular traffic flow (e.g., a downstream multicast service), the Privacy Extended Header element SHOULD NOT be used.

This page intentionally left blank.

4 Baseline Privacy Key Management (BPKM) Protocol

4.1 State Models

4.1.1 Introduction

The BPKM protocol is specified by two separate, but interdependent, state models: an authorization state model (the Authorization state machine) and an operational service key state model (the Traffic Encryption Key, or *TEK* state machine). These state models are for explanatory purposes only, and should not be construed as constraining an actual implementation.

Cable modem authorization, controlled by the Authorization state machine, is the process of obtaining:

- the list of SIDs identifying the particular encrypted traffic services a cable modem is authorized to access
- an authorization key, from which a key encryption key (KEK) and message authentication keys are derived

The KEK is a DES encryption key that the CMTS uses to encrypt the traffic encryption keys (TEKs) it sends to the modem. Traffic encryption keys are used for encrypting user data traffic. CM and CMTS use message authentication keys to authenticate, via a keyed message digest, the key requests and responses they exchange.

After achieving authorization, a cable modem periodically seeks reauthorization with the CMTS; reauthorization is managed by the CM's Authorization state machine. A CM must maintain its authorization status with the CMTS in order to be able to refresh aging traffic encryption keys. TEK state machines manage the refreshing of traffic encryption keys.

A cable modem begins authorization by sending an Authorization Request message to its CMTS. This is a request for an authorization key, and for the identities of the security associations (i.e., the SIDs) the CM is authorized to participate in. The Authorization Request includes:

- a convenient cable modem identifier unique to that cable modem (e.g., a cable modem MAC)
- the cable modem's public key
- a list of zero or more unicast SIDs corresponding to provisioned class-of-service settings configured for Baseline Privacy. The CMTS will have assigned these SIDs to the CM during RF MAC registration.

Note that it is not practical to use a cable modem's public key as a cable modem identifier. While the public key is unique to the cable modem, it is long, i.e., the modulus is 768 or 1024 bits, and cannot conveniently be used by the CMTS software as a table index or CM "handle".

In response to an Authorization Request message, a CMTS generates a new authorization key, encrypts it with the cable modem's public key, and sends it back to the CM in an Authorization Reply message. The authorization reply includes:

- the new authorization key encrypted with the CM's public key
- a 4-bit key sequence number, used to distinguish between successive generations of authorization keys (with each reauthorization, a new authorization key is generated)
- a list of SIDs for which the CM is authorized to maintain keying information (including the unicast SID(s) presented in the authorization request)

The CMTS, in responding to a CM's Authorization Request, will determine whether the requesting cable modem, identified by the cable modem ID (e.g., MAC address), is authorized for basic unicast services, and which additional multicast services the cable modem's user has subscribed for.

Upon achieving authorization, a CM starts a separate TEK state machine for each of its authorized SIDs. Each TEK state machine operating within the CM is responsible for managing the keying material associated with its respective SID. TEK state machines periodically send Key Request messages to the CMTS, requesting a refresh of keying material for their respective SIDs. A Key Request includes:

- a cable modem identifier unique to that cable modem
- the SID whose keying material is being requested
- an HMAC keyed message digest, authenticating the Key Request

The CMTS responds to a Key Request with a Key Reply message, containing current keying material for a specific SID. This keying material includes:

- the DES-encrypted traffic encryption key
- a CBC initialization vector
- a key sequence number
- a key lifetime
- an HMAC keyed message, authenticating the Key Reply

The traffic encryption key (TEK), in the Key Reply, is DES (ECB mode) encrypted with a key encryption key (KEK), derived from the authorization key.

A TEK state machine remains active as long as:

- the CM is authorized to operate in the CMTS's security domain; i.e., it has a valid authorization key, and
- the CM is authorized to participate in that particular Security Association; i.e., the CMTS continues to provide fresh keying material during re-key cycles.

The parent Authorization state machine stops *all* of its child TEK state machines when the CM receives an Authorization Reject from the CMTS during a reauthorization cycle. Individual TEK state machines can be started or stopped during a reauthorization cycle if a CM's SID authorizations change between successive re-authorizations.

Communication between Authorization and TEK state machines occurs through the passing of events and protocol messaging. The Authorization state machine generates events (i.e., Stop, Authorized, Authorization Pending, and Authorization Complete events) that are targeted at its child TEK state machines. TEK state machines do not target events at their parent Authorization state machine. The TEK state machine affects the Authorization state machine indirectly through the messaging a CMTS sends in response to a modem's requests: a CMTS MAY respond to a TEK machine's Key Requests with a failure response (i.e., Authorization Invalid message) that will be handled by the Authorization state machine.

4.1.2 Authorization State Machine

The Authorization state machine consists of five states and seven distinct events (including receipt of messages) that can trigger state transitions. The Authorization finite-state machine (FSM) is presented below in a graphical format, as a state flow model (Figure 4-1), and in a tabular format, as a state transition matrix (Table 4-1).

The state flow diagram depicts the protocol messages transmitted and internal events generated for each of the model's state transitions; however, the diagram does not indicate triggering conditions or additional internal actions, such as the clearing or starting of timers, that accompany the specific state transitions. Accompanying the state transition matrix (including the detail of states, messages, events, parameters, and actions) is a detailed description of the triggering conditions and the specific actions accompanying each state transition. The state transition matrix **MUST** be used as the definitive specification of triggering conditions and protocol actions associated with each state transition. That is, unless explicitly required, the CMTS and the CM are only allowed to take actions specified in this section.

The following legend applies to the KEK state flow diagram in Figure 4-1.

- Ovals are states
- Events are in *italics*
- Messages are in normal font
- State transitions (i.e., the lines between states) are labeled with <what causes the transition>/<messages and events triggered by the transition>. Thus, "*timeout*/Auth Request" means that the state has received a "timeout" event and sends an Authorization Request ("Auth Request") message. If there are multiple events or messages before the slash "/" separated by a comma, *any* of them can cause a transition. If there are multiple events or messages listed after the slash, *all* of the specified actions must accompany the transition.

The Authorization state transition matrix presented in Table 4-1 lists the five Authorization machine states in the top row and the seven Authorization machine events (including message receipts) in the left-hand column. Any cell within the matrix represents a specific combination of state and event, with the next state (the resulting state) displayed within the cell. For example, cell 3-B represents the receipt of an Authorization Reply (Auth Reply) message when in the Authorize Wait (Auth Wait) state. Within cell 3-B is the name of the next state, “Authorized.” Thus, when a CM’s Authorization state machine is in the Authorize Wait state and an Authorization Reply message is received, the Authorization state machine will transition to the Authorized state. In conjunction with this state transition, several protocol actions must be taken; these are described in the listing of protocol actions, under the heading 3-B, in Section 4.1.2.5.

A shaded cell within the state transition matrix implies that either the specific event cannot or should not occur within that state, and if the event does occur, the state machine **MUST** ignore it. For example, if an Authorization Reply message arrives when in the Authorized state, that message should be ignored (cell 3-C). The CM **MAY**, however, in response to an improper event, log its occurrence, generate an SNMP event, or take some other vendor-defined action. These actions, however, are not specified within the context of the Authorization state machine, which simply ignores improper events.

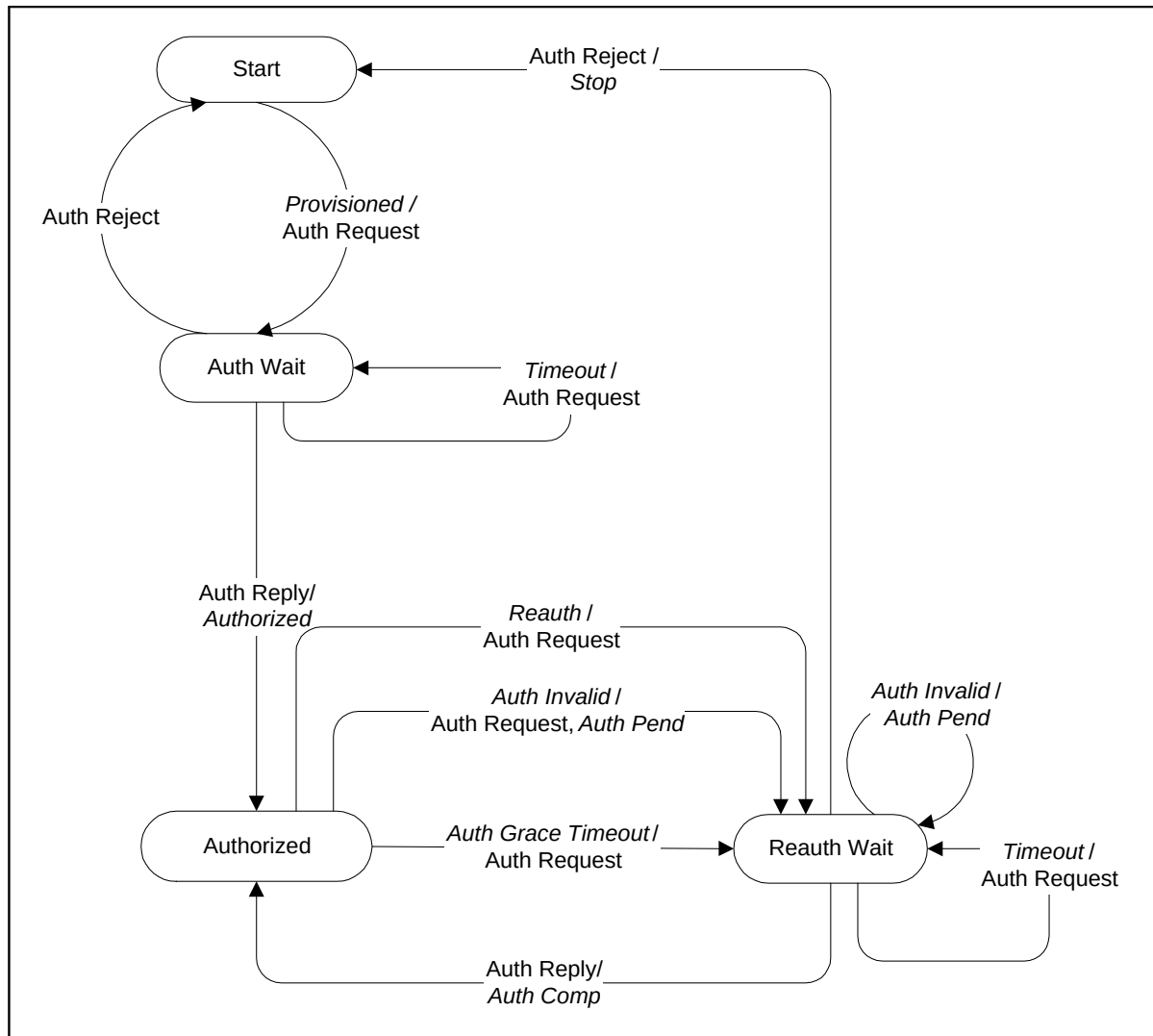


Figure 4-1. Authorization State Machine Flow Diagram

Table 4-1. Authorization FSM State Transition Matrix

<i>State Event or Rcvd Message</i>	(A) Start	(B) Auth Wait	(C) Authorized	(D) Reauth Wait	(E) Auth Reject Wait
(1) <i>Provisioned</i>	Auth Wait				
(2) <i>Auth Reject</i>		Auth Reject Wait		Auth Reject Wait	
(3) <i>Auth Reply</i>		Authorized		Authorized	
(4) <i>Timeout</i>		Auth Wait		Reauth Wait	Start
(5) <i>Auth Grace Timeout</i>			Reauth Wait		
(6) <i>Auth Invalid</i>			Reauth Wait	Reauth Wait	
(7) <i>Reauth</i>			Reauth Wait		

4.1.2.1 States

4.1.2.1.1 Start

This is the initial state of the FSM. No resources are assigned to or used by the FSM in this state—e.g., all timers are off, and no processing is scheduled.

4.1.2.1.2 Authorize Wait (Auth Wait)

The CM has received the “Provisioned” event indicating that it has completed RF MAC registration with the CMTS. In response to receiving the event, the CM has sent the Authorize Request message to the CMTS and is waiting for the reply.

4.1.2.1.3 Authorized

The CM has received a Authorization Reply message which contains a list of valid SIDs for this CM. At this point, the modem has a valid authorization key and SID list. Transition into this state triggers the creation of one TEK FSM for each of the CM’s privacy-enabled SIDs.

4.1.2.1.4 Reauthorize Wait (Reauth Wait)

The CM has an outstanding re-authorization request. The CM was either about to time out its current authorization or received an indication (an Authorization Invalid message from the CMTS) that its authorization was no longer valid. The CM has sent an Authorization Request message to the CMTS and is waiting for a response.

4.1.2.1.5 Authorize Reject Wait (Auth Reject Wait)

The CM received an Authorization Reject message in response to its last Authorization Request. In response to receiving this reject message, the CM sets a timer and transitions to the Authorize Reject Wait state. The CM remains in this state until the timer expires.

4.1.2.2 Messages

The message formats are defined in detail in Section 4.2.

4.1.2.2.1 Authorization Request (Auth Request)

Request an authorization key and list of authorized SIDs. Sent from CM to CMTS.

4.1.2.2.2 Authorization Reply (Auth Reply)

Receive an authorization key and list of authorized SIDs. Sent from CMTS to CM. The authorization key is encrypted with the CM's public key.

4.1.2.2.3 Authorization Reject (Auth Reject)

Attempt to authorize was rejected. Sent from the CMTS to the CM.

4.1.2.2.4 Authorization Invalid (Auth Invalid)

The CMTS can send an Authorization Invalid message to a client CM as:

- an unsolicited indication, or
- a response to a message received from that CM

In either case, the Authorization Invalid message instructs the receiving CM to re-authorize with its CMTS.

The CMTS responds to a Key Request with an Authorization Invalid message if (1) the CMTS does not recognize the CM as being authorized (i.e., no valid authorization key associated with cable modem) or (2) verification of the Key Request's keyed message digest (in HMAC-Digest Attribute) failed. Note that the Authorization Invalid *event*, referenced in

both the state flow diagram and the state transition matrix, signifies either the receipt of an Authorization Invalid message or an internally generated event.

4.1.2.3 Events

4.1.2.3.1 Provisioned

The Authorization state machine generates this event upon entering the Start state if the RF MAC has completed initialization, i.e., CMTS registration. If the RF MAC initialization is not complete, the CM sends a Provisioned event to the Authorization FSM upon completing CMTS registration. The Provisioned event triggers the CM to begin the process of getting its authorization key and TEKs.

4.1.2.3.2 Timeout

A retransmission or wait timer timed out. Generally a request is resent.

4.1.2.3.3 Authorization Grace Timeout

The Authorization grace timer timed out. This timer fires a configurable amount of time (the Authorization “Grace” Time) before the current authorization is supposed to expire, signalling the CM to re-authorize before its authorization expires. The Authorization Grace Time is specified in a configuration setting within the TFTP-downloaded parameter file.

4.1.2.3.4 Reauthorize (Reauth)

The CM’s set of authorized SIDs may have changed. This event is generated in response to an SNMP set [DOCSIS5], and is meant to trigger a reauthorization cycle.

4.1.2.3.5 Authorization Invalid (Auth Invalid)

This event MUST be generated by the CM when there is a failure authenticating a Key Reply, Key Reject, or TEK Invalid message, or after receiving an Authorization Invalid message from the CMTS. A CMTS responds to a Key Request with an Authorization Invalid if verification of the request’s message authentication code fails. Authentication failures in either the CMTS or CM indicate that the CMTS and CM have lost KEK synchronization.

A CMTS may also send a CM an unsolicited Authorization Invalid message to a CM, forcing an Authorization Invalid event.

[Note: the following events are sent by a parent Authorization state machine to its child TEK state machines.]

4.1.2.3.6 Stop

Sent by the Authorization FSM to an active (non-START state) TEK FSM to terminate their traffic keys.

4.1.2.3.7 Authorized

Sent by the Authorization FSM to a non-active (START state) but valid TEK FSM.

4.1.2.3.8 Authorization Pending (Auth Pend)

Sent by the Authorization FSM to a specific TEK FSM to place that TEK FSM in a wait state until the Authorization FSM can complete its re-authorization operation.

4.1.2.3.9 Authorization Complete (Auth Comp)

Sent by the Authorization FSM to a TEK FSM in the Operational Reauthorize Wait (Op Reauth Wait) or Rekey Reauthorize Wait (Rekey Reauth Wait) states to clear the wait state initiated by an Authorization Pending event.

4.1.2.4 Parameters

All configuration parameter values are specified in the TFTP-downloaded parameter file (see Appendix A: TFTP Configuration File Extensions).

4.1.2.4.1 Authorize Wait Timeout

Timeout period between sending Authorization Request messages from Authorize Wait state.

4.1.2.4.2 Reauthorize Wait Timeout (Reauth Wait Timeout)

Timeout period between sending Authorization Request messages from Reauthorize Wait state.

4.1.2.4.3 Authorization Grace Time

Amount of time before authorization is scheduled to expire that the CM starts re-authorization.

4.1.2.4.4 Authorize Reject Wait Timeout

Length of time to remain in the Authorize Reject Wait state.