Superseded

PacketCable™ Event Messages Specification

PKT-SP-EM-I01-991201

Interim

Notice

This PacketCable specification is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Abstract

This specification describes the concept of Event Messages used to collect usage for the purposes of billing within the PacketCable™ architecture. It details the RADIUS protocol used to carry these messages, defines the various Event Messages, lists the attributes each Event Message contains, and lists the required and optional Event Messages associated with each type of end-user service supported. This specification describes the Event Messages for the PacketCable project, selected under the direction of the CableLabs® Executive Committee. It is being issued to facilitate design and field-testing leading to the early manufacturability and interoperability of conforming hardware and software by multiple vendors.

Document Status Sheet

Document Control Number:	PKT-SP-EM-I01-991201			
Document Title:	PacketCable™ Event Messages Specification			
Revision History:	I01-991201: release			
Date:	December 1, 1999			
Status:	~~Work in Progress~~	~~Draft~~	Interim	~~Released~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	Public

Key to Document Status Codes:

Work in Progress	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 reviews by Members and vendors. Drafts are susceptible to substantial change during the review process.
Interim	A document, which has undergone rigorous Member and vendor review, suitable for use by vendors to design in conformance to and for field testing. For purposes of the “Contribution and License Agreement for Intellectual Property" which grants licenses to the intellectual property contained in the PacketCable Specification, an "Interim Specification" is a "Published” Specification.
Released	A stable document, reviewed, tested and validated, suitable to enable cross-vendor interoperability.

Contents

Figures

Tables

1 INTRODUCTION

1.1 PacketCable Overview

PacketCable™, a project conducted by Cable Television Laboratories, Inc. (CableLabs®) and its member companies, is identifying and defining specifications for delivery of enhanced communications services using packetized data transmission technology over two-way cable television (hybrid fiber coax (HFC) data-over-cable) networks using the DOCSIS protocol. PacketCable specifies network structure that overlays the two-way data-ready broadband cable access network.

Superseded

While PacketCable 1.0 is initially focused on packet voice over cable, PacketCable will ultimately encompass additional voice services as well as other services such as data, video, and other real-time multimedia.

1.2 PacketCable Event Messages

An Event Message is a data record containing information about network usage and activities. A single Event Message may contain a complete set of data regarding usage or it may only contain part of the total usage information. When correlated by the Record Keeping System (RKS), information contained in multiple Event Messages provides a complete record of the service. This complete record of the service is often referred to as a Call Detail Record (CDR). Event Messages or CDRs may be sent to one or more back office applications such as a billing system, fraud detection system, or pre-paid services processor.

The structure of the Event Message data record is designed to be flexible and extensible in order to carry information about network usage for a wide variety of services. Examples of these services include PacketCable voice, video and other multimedia services, OpenCable services such as Video-On-Demand, Pay-Per-View and DOCSIS high-speed data services.

This PacketCable Event Messages specification defines the structure of the Event Message data record and defines RADIUS as the transport protocol. Additional transport protocols may be recommended in future releases of this specification. Although the scope of this Event Message specification is limited to defining Event Messages for simple voice communications activities, it is expected that this specification will be expanded to support additional PacketCable services as well as OpenCable and high-speed data services.

1.3 PacketCable Reference Architecture

Figure 1 shows the reference architecture for the PacketCable Network. Refer to the PacketCable Architecture Document [6] for more detailed information on this reference architecture.

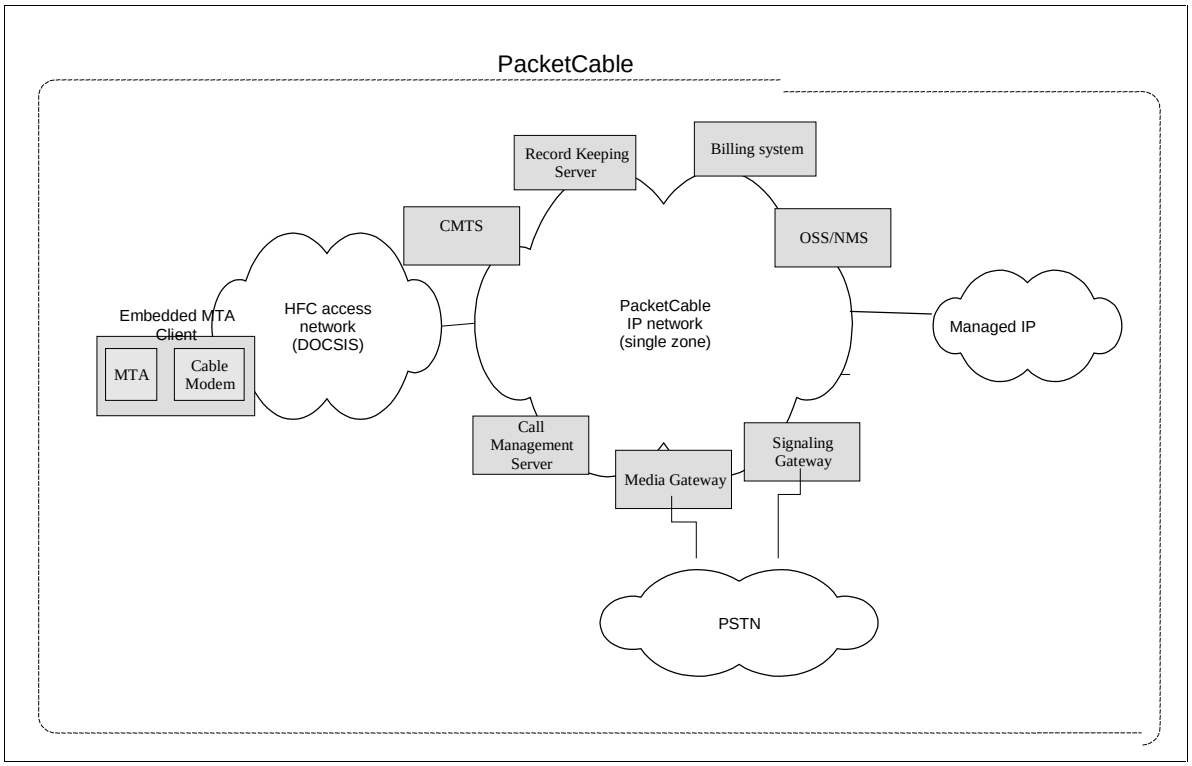

Figure 1: PacketCable Network Component Reference Model (partial)

1.4 PacketCable, Voice over IP over Cable

Cable operators are deploying high-speed data communications systems and offering voice, video, and data services based on bi-directional transfer of Internet protocol (IP) traffic. The transfer takes place between the cable system headend and customer locations, over an all-coaxial or hybrid-fiber/coax (HFC) cable network, defined by the data over cable service interface specification (DOCSIS). This is shown in simplified form in the following diagram.

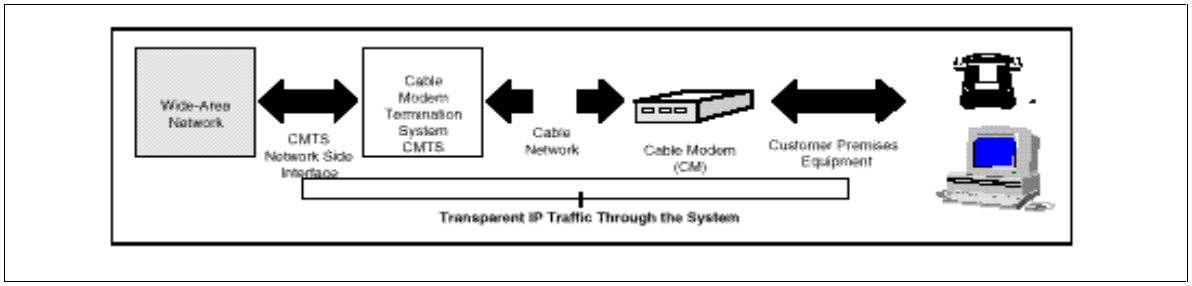

Figure 2: Transparent IP Traffic through the Data-Over-Cable System

The transmission path over the cable system is realized at the headend by a cable modem termination system (CMTS) and at each customer location by a cable modem (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 [2]. At customer locations, the interface is called the cable-modem-to-

customer-premises-equipment interface (CMCI) and is specified in [1]. The intent is for operators to transfer IP traffic transparently between these interfaces.

One critical Operations Support System (OSS) function required to operate such a system is the capturing of usage on a call-by-call basis for each subscriber. Such functionality is critical in allowing MSO's to bill for services provided on a usage-sensitive basis, but also plays an important role in areas such as network usage monitoring and fraud management. The usage collection concept lies in requiring network elements involved in key portions of each call to notify a centralized Record Keeping Server (RKS) with what are termed Event Messages detailing the relevant data pertaining to the portion of the call handled by that given network element. This Event Message concept, and the architecture, which underlies it are described in greater detail in this document.

1.5 Document Scope

The scope of this document encompasses the definition of the Event Message architecture; the services for which Event Messages are defined; the set of Event Messages defined for each supported service; the format and coding of the Event Messages; and finally the transport protocol used to pass Event Messages between PacketCable network elements.

The Event Messages are designed to be flexible and extensible in order to support new and innovative PacketCable and value-added services. In an effort to describe some of these features and possible uses of these Event Messages, this document may describe interfaces and signaling protocols that are outside the scope of PacketCable 1.0. It should be understood that the primary purpose of this document is to support the PacketCable 1.0 architecture and the PacketCable 1.0 services as defined in this document.

In order to support early deployment of PacketCable networks, the PacketCable project is developing specifications in a phased approach. In an effort to keep pace with the larger PacketCable project and interface specification development effort, the Event Messages are also addressed in a phased approach. Possible future extensions to this document may include topics such as settlements, domain-domain signaling and other issues, expanded support for fraud detection and other back office applications.

From time to time this document refers to the voice communications capabilities of a PacketCable network in terms of "IP Telephony." The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined by appropriate legal and regulatory authorities. Nothing in this document is addressed to, or intended to affect, those issues. In particular, while this document uses standard terms such as "call," "call signaling," "telephony," etc., it should be recalled that while a PacketCable network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers, and that these differences may be significant for

legal/regulatory purposes. Moreover, while reference is made here to "IP Telephony," it should be recognized that this term embraces a number of different technologies and network architecture, each with different potential associated legal/regulatory obligations. No particular legal/regulatory consequences are assumed or implied by the use of this term.

1.6 Document Overview

The document contains the following sections. Section 2 motivates the need for Event Messages. Section 3 describes objectives of the Event Message architecture followed by section 4 describing the Event Message architecture itself. Section 5 describes the services PacketCable 1.0 will support for which Event Messages need to be generated. Section 6 defines the Event Messages needed in order to bill these supported services. Section 7 defines the PacketCable Event Message attributes. Finally, section 8 describes the protocol used for transport of Event Messages between PacketCable network elements.

1.7 Requirements Syntax

Throughout this document, 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 is explanatory.

2 BACKGROUND

2.1 Traditional Telephony Billing Formats

The telephony industry has traditionally recorded call detail transactions on telephone switches utilizing various standard and proprietary billing formats such as Automated Message Accounting (AMA), sometimes referred to as Bellcore AMA Format (BAF). The switches generate multiple transactions based upon the type of call the customer placed. These transactions are correlated and packaged into a single Call Detail Record (CDR) at the end of the service instance for billing purposes. In this traditional telephony model, services and awareness of "call state" is usually maintained in one or at most two nodes of the network, which makes such correlation relatively straightforward. The CDR is then delivered to the billing system for the purpose of placing a charge on the customer's account.

2.2 Motivation for Event Based Billing

The event-based approach to capturing information to be used for billing is necessary to accommodate the distributed architecture of PacketCable. "Call state awareness" no longer resides in one or two network elements, but is instead spread out among many. Each network element MUST be responsible for generating Event Messages for the portion of the communication pertaining to them.

The primary motivating factor behind articulating the structure and details of these various Event Messages is to support multi-vendor interoperability between network elements and record keeping servers. This specification defines the Event Message syntax and in addition it describes a recommended transport protocol.

Event based billing has the added advantage that it enables PacketCable services to be billed in real-time, making the information about billable communications available as the network equipment processes them. This allows the system as a whole to be more responsive, allowing, for example, fraudulent behavior to be detected sooner, saving revenue for the provider. It also allows a more fully integrated solution, as it becomes possible for the billing system and the network equipment to exchange information about the availability of a service as the customer is requesting that service.

With respect to the Event Message format, there are a large number of formats in use today. The most widely used formats carry the legacy of the traditional CDR, which is generated at the end of the call. While these formats capture much of the information content needed to bill for PacketCable services, bringing along their full structure would make it difficult to support the real-time nature of certain enhanced PacketCable services. This specification leverages the value of the information content from the existing billing formats, augmenting that with the distributed nature of the PacketCable architecture.

2.3 Real-Time Billing

The billing system can be regarded as a functional block of the back office Operations Support System (OSS). The inputs to the billing system are the billing events and the outputs are the account balance and invoice. The billing system relates the billing events to the account balance by rating the events according to the pricing structure and other business logic.

Real-time Billing Systems relate the billing events to the account balance as events occur. As the billing system receives these real-time billing events, its rating engine rates the events and immediately posts balances. Real-time Billing Systems may be required to support advanced PacketCable features such as pre-paid calling card, real-time fraud prevention, and real-time credit enforcement.

The PacketCable Event Message architecture can be used to support both real-time and batch billing systems.

2.4 Real-Time and Batch Event Message Delivery

Event Messages may be delivered to the RKS in real time as they are created. This enables support for a growing number of services that require purchase limits such as prepaid calling cards.

As an alternative, Event Messages may be stored for some period of time and batched together before being sent to the RKS. This approach provides a more efficient use of network resources.

2.5 Terminology and Concepts

This section defines terminology associated with usage data as it relates to PacketCable Services. The concept of a "call" is well understood and used within the telecommunications marketplace today. A traditional telephony "call" involves establishing a dedicated, circuit-switched path between the calling and called parties. Packet-switched architectures, including PacketCable, do not establish any such dedicated paths. To the contrary, the PacketCable architecture assumes a shared medium between the head-end and the customer, as compared to the dedicated loop plant in traditional telephony; and during a traditional telephone call, as noted above, a circuit-switched "connection" is established between the parties, whereas packet switching is inherently "connectionless." All that said, the term "call" is sufficiently well entrenched that it will be used in this document to refer to packet-mode voice communications between two parties over a PacketCable network, even though in technical terms (as will be seen) there is little resemblance to a traditional telephone "call." It is envisioned that many new voice, video, data and other multimedia services will be developed to take advantage of the inherent extensibility of the PacketCable architecture. These new services, which likely will not be derived from traditional telephony principals, will be based on the term transaction, which is more indicative of the data flows across the PacketCable network. The Event Message structure is designed to be flexible and enable the addition of new PacketCable services and features while maintaining backward compatibility with existing

applications. Event Messages MAY support information required for billing of DOCSIS data services, OpenCable video services, and the encapsulation of vendor specific proprietary data

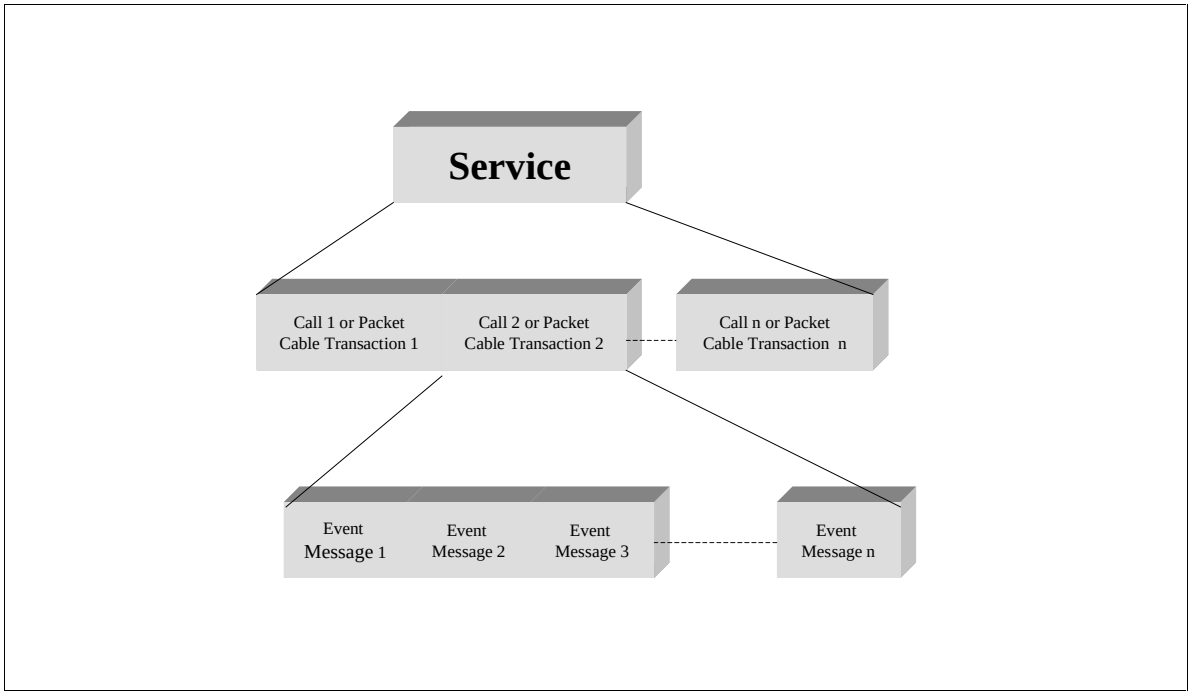

Figure 3. PacketCable Terminology

2.5.1 Service

A ***service*** is an individual or package of communications features a subscriber may select. A service is identified by a set of one or more "calls" or transactions that deliver the desired functionality to the subscriber. Examples of a service include: a voice communication between two local PacketCable subscribers, a 3-way call, pay-per-view movie, and a web surfing session. A service may be instantaneous or persist over time. Service in the context of PacketCable 1.0 implies voice communications only and may not necessarily apply to the variety of other services such as Data, traditional IP, E-Commerce, etc.

2.5.2 PacketCable Transaction

A ***PacketCable transaction*** is a collection of events on the PacketCable network when delivering a service to a subscriber. Event Messages for the same transaction are identified by one unique Billing Correlation ID (as described in Table 33). For some services, multiple transactions may be required to provide information that is necessary to collect the total usage for the service. Multiple Event Messages may be required to track resources for each individual service used. A Transaction may persist over time.

2.5.3 Call

A ***call*** is an instance of user-initiated voice communication capabilities. In traditional telephony, a call is generally considered as the establishment of connectivity directly between two points: originating party and terminating party. In the PacketCable context, as noted above, the communication between the parties is "connectionless" in the traditional sense.

2.5.4 Event Message

An ***Event Message*** is a set of data, representative of an event in the PacketCable architecture that could be indicative of usage of one or more billable PacketCable capabilities. An Event Message by itself may not be fully indicative of a customer's billable activities, but an Event Message correlated with other Event Messages builds the basis of a billable Usage Detail Record

2.5.5 Attribute

An ***Event Message Attribute*** is a predefined data element described by an attribute definition and attribute type.

2.6 Supporting Documentation

A number of documents and specifications describe the PacketCable project. The PacketCable Architecture Framework [6] is the starting point for understanding the PacketCable project and the various PacketCable Interface Specifications, technical reports and other PacketCable documents. Please refer to URL www.packetcable.com.

3 PACKETCABLE OBJECTIVES

3.1 PacketCable 1.0 Required Services and Capabilities

PacketCable 1.0 provides basic voice capabilities and therefore MUST support Event Messages for the following services. These services are described in more detail in section 5 of this document.

- Interconnection with circuit-switched PSTN
- Support for 911 Emergency Services
- n11 (411, 611, etc.) assume outside directory service
- Toll-Free Services (800, 888, 877…)
- Operator Services
- Call Block Service
- Call Waiting Service
- Call Forwarding/Call Redirection Services
- Return Call Service
- Repeat Call Service
- Voice Mail Service
- Message Waiting Indicator Service (Email/Voice Mail notification)

3.2 PacketCable 1.0+ Supported Services and Capabilities

The following represents a list of possible additional PacketCable 1.0 services that MAY be supported. The list, though meant as a rough guideline, is by no means comprehensive, and it is expected that as the scope of services grows, so too will this list. A detailed definition of these services is not defined in this document.

- 3-way Communication
- Call Transfer
- Speed Dialing
- Caller Name and Number
- Caller Name and Number Privacy
- Selective Screening Services
- Pay-Per-Communication Services (900, etc.)
- Distinctive Notification(to identify callee in a multiple-party household)
- Priority Notification (to prioritize incoming communications)
- Customer Originated Trace

- Selective Forwarding
- Rejection(activate and deactivate)
- Teletype Translation Services
- Multi-line Hunt Group Services
- Virtual second line (Multiple lines)
- Alternate billing methods (collect, third number billed, credit card, pre-paid services, etc.)

3.3 Assumptions

The following assumptions have been made which apply to the entire document:

- PacketCable 1.0 does NOT support distributed call signaling (DCS), slated for later PacketCable releases.
- PacketCable 1.0 assumes proprietary signaling for CMS-CMS or CMS-MGC signaling. These interfaces will be defined in future PacketCable releases.
- PacketCable 1.0 does not specify the interface between an RKS and a billing system.
- All IP based Intelligent Peripherals (these include Announcement Servers, for example) will be connected to the originating CMS or MGC.
- PacketCable 1.0 does NOT support Line Information Database (LIDB) queries. Calls requiring LIDB determination, such as calling card personal identification number validation, are sent directly to the PSTN.
- PacketCable 1.0 supports local number portability (LNP).
- Non-PacketCable network elements, such as those residing in the public switched telephone network (PSTN) to which a PacketCable system may interconnect with, will NOT generate and send Event Messages to the RKS.
- PSTN Intelligent Peripheral Event Messages are generated by the originating CMS.
- PacketCable 1.0 Event Messages currently only support messages for actual billable events. This document does not specify messages related to provisioning of services by the operator of a PacketCable network. This document does support Event Messages for Subscriber service activation. This document does not specify messages related to selection of an entity other than the PacketCable network operator to handle off-network activities (e.g., inter-exchange communications).
- The initiating party number and the terminating party number are the only two attributes defined in PacketCable 1.0 that can be used to associate a subscriber with usage of network resources.
- PacketCable 1.0 supports interconnection to both Class 4 and Class 5 Switches.

- PacketCable supports a 911 Trunk Group.
- PacketCable 1.0 trusted network elements are expected to be pre-provisioned with a minimum set of data using a vendor-proprietary mechanism. Examples of this data may include:
  - Element Type, identifying the element as a CMTS, CMS, or MGC.
  - Element ID. It is assumed the Element ID will be a MAC address for PacketCable 1.0, but in future PacketCable releases may be changed to a more globally unique value, similar to the CLLI code in the PSTN.
  - Frequency (in minutes) of long-duration-call message generation (0 = never, 60 = hourly).
  - A list of which Event Messages are required and which Event Messages are optional as defined by the MSO. For each of these Event Messages, identify if the Event Messages are to be 1) transported to the RKS as a single Event Message in real-time or 2) batched and transported to the RKS as multiple Event Messages at a later time. 3) provide capability to configure both how many Event Messages are batched before being sent to the RKS.
  - number of days to keep Event Messages for short-term storage.
  - RADIUS protocol parameters:
    - Retry interval and Retry count.
    - For each RKS that may receive Event Messages, its IP address and UDP port.
    - The IP address of each RADIUS server that it may communicate with.

4 EVENT MESSAGES ARCHITECTURE

Figure 4 shows a representative PacketCable Event Messages Architecture. By standardizing the transport, syntax and collection of appropriate Event Message attributes from a distributed set of network elements, the PacketCable architecture provides a single reference point to interface to existing billing, settlement, reconciliation, and other systems**.** Note that only the shaded components are included within the scope of the PacketCable 1.0 architecture. Interfaces between the RKS and the shaded PacketCable network elements are within scope of PacketCable 1.0. Interfaces between the RKS and back office servers or applications are NOT within the scope of PacketCable 1.0. It should be understood that the back office servers and applications shown Figure 4 are representative, and are not mandated by the PacketCable 1.0 architecture.

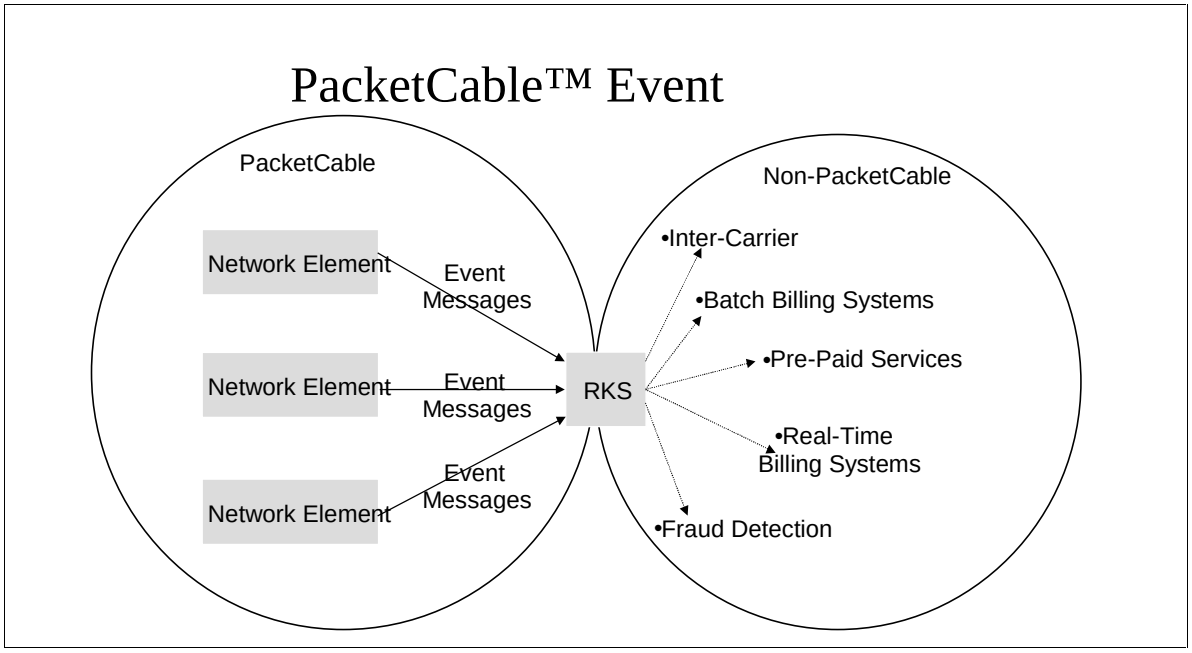

Figure 4: Representative PacketCable Event Messages Architecture

4.1 PacketCable Event Message Collection

Event Message collection occurs as follows: when trigger events occur [such as call signaling starts, activation of QoS service resources, call signaling stops, etc.], the relevant PacketCable network element generates an Event Message. These messages may be sent immediately to the RKS, or a group of messages may be collected and sent at a later time. In either case, the actual time of the trigger event is reported allowing the back office applications to accurately calculate time-based resource usage. As these Event Messages are accumulated within the RKS, the network operator can then export them into their billing systems based on their business requirements. The data from multiple network elements are linked to a transaction [e.g. call] via a unique Billing Correlation identifier, which can be leveraged for reconciliation and non-repudiation purposes.

4.2 PacketCable Network Elements

The PacketCable architecture supports a system capable of creating, collecting, and delivering usage data from a subset of PacketCable network elements to a cable operator's back office applications. Trusted PacketCable 1.0 network elements that create Event Messages include the Call Management Server (CMS) and Cable Modem Termination System (CMTS), Media Gateway Controller (MGC).

The PacketCable architecture contains trusted and untrusted network elements. Trusted network elements are typically located within a MSO's facility and are controlled by the MSO. Untrusted network elements are typically located within the consumer's home or outside of the MSO's facility or exclusive control. In the PacketCable 1.0 architecture, Event messages are only accepted from trusted PacketCable network elements.

The PacketCable Architecture Document [7] contains a detailed description of the PacketCable network elements. A brief explanation of the PacketCable network elements that will most likely generate PacketCable Event Messages is listed in this section for completeness.

4.2.1 Call Management Server (CMS)

The Call Management Server (CMS) provides signaling services necessary for voice communications. The primary purpose of the CMS is to establish standard "calls," as that term is used in the PacketCable context. The media servers also provide support services for the media streams such as conference mixing bridges and announcement servers.

The CMS MUST create a Billing Correlation ID on receipt of an NCS-signaling NTFY message from an MTA.

The CMS MUST send the Billing Correlation ID and other data as defined in Table 1 to the CMTS via the DQoS GateSet message as specified in the DQoS specification [8].

Table 1: PacketCable Event Reporting Common Elements

1. Billing_Correlation_ID (see Table 33)
2. IP address and port number of the primary RKS
3. IP address and port number of the secondary and other RKSs (optional)
4. Flag indicating if CMTS should send Event Messages to the RKS in real-time

The CMS MUST generate the appropriate Event Messages as defined in this specification.

4.2.2 Media Gateway Controller (MGC)

The Media Gateway Controller (MGC) is the overall controller function of the PSTN gateway. It receives, mediates, and routes call signaling information between the PacketCable and PSTN domains and it maintains and controls the overall call state

for all calls connecting to and from the PSTN. It controls the Media Gateway function and communicates with the Signaling Gateway function via the MGC-SG protocol defined for the major protocol family in question, i.e., ISUP, In-band or TCAP.

The MGC MUST create a Billing Correlation ID on receipt of:

- an SS7 IAM message, or
- a TCGP NTFY with digits (operator services)

The MGC MUST generate the appropriate Event Messages as defined in this specification.

4.2.3 Cable Modem Termination System (CMTS)

The Cable Modem Termination System terminates the connection from the cable modem on the customer premises into the PacketCable network. The CMTS generates QoS Event Messages.

The CMTS MUST generate the appropriate Event Messages as defined in this specification.

4.2.4 Record Keeping Server (RKS)

The Record Keeping Server (RKS) is a trusted network element function. In many cases, for simplicity reasons, the RKS is depicted in this document as a separate standalone element, but this specification does not preclude a CMS, Billing System, or other application from performing the RKS functionality. The RKS is the mediation layer between the call signaling and transport layer and the back-office applications. The RKS is expected to pre-process the data from the Call Signaling and Transport layer and present it to the back-office applications in the format and within the time constraints deemed necessary by the MSO.

The RKS also, at a minimum, is a short-term repository for PacketCable Event Messages. It receives Event Messages from various trusted PacketCable network elements. The RKS assembles the Event Messages into coherent sets, which are then made available to a usage-processing platform and potentially to several other back office systems. It acts as the demarcation point between the PacketCable network and the back office applications.

Figure 4 gives a representative RKS deployment for information only and does not imply an implementation requirement.

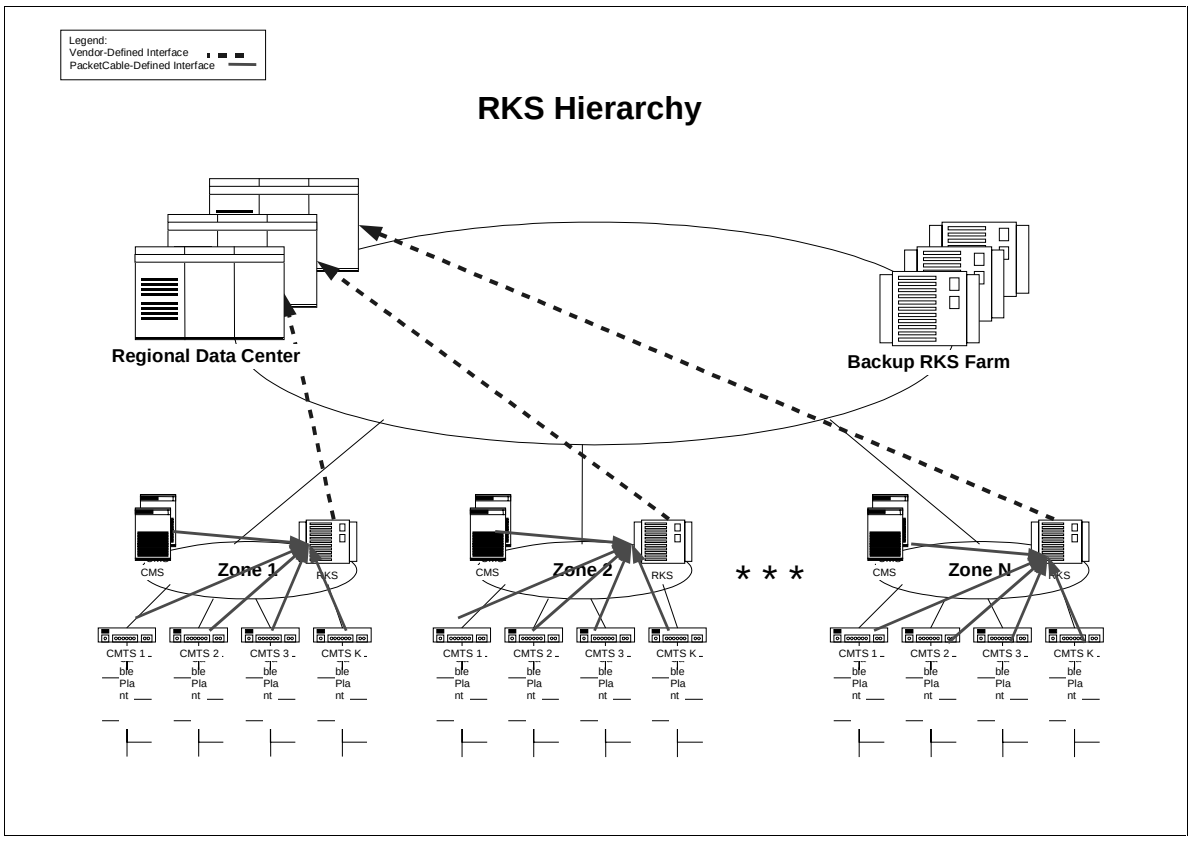

Figure 5: Example RKS Architecture

The RKS is expected to perform the following functions:

- The RKS MUST receive Event Messages.
- The RKS MUST be capable of correlating all Event Messages related to an individual call and have an extensible output to meet the needs of the downstream applications.
- The RKS MUST assemble Events and Determine Completeness—This MUST include the capability to distinguish Event Messages, and recognize when a complete set, representing a coherent set of billing data is available for transport to the back office system.
- The RKS MUST provide interface network functions that require real time or near real time based on priority and where messages are being sent, as defined in Section 6. For example, a call may be sent real-time and a report may be sent at night. The correlation process MUST be user definable to support the various call events defined herein and defined in the future.
- The RKS MUST have the ability to store the Event Messages for at least one week or until sent to the other back office systems and successful receipt is acknowledged from those systems.

- The RKS MUST have the ability to dump the Event Messages to some other type of offline storage device on a regular basis (CD, TAPE, or other media) for retrieval and regulatory purposes.

The following list deals with other possible capabilities of an RKS. They are therefore beyond the scope of the requirements of this current document, and are included here for informational use only. Decisions on these optional requirements will be based upon the MSO response to many regulatory and business variables.

- An RKS-RKS security interface MAY be required. PacketCable 1.0 does not define this interface. The security interface between the RKS and other PacketCable trusted network elements is defined in [5].
- The RKS MAY support Backup and Recovery —This includes a nominal ability to restore the state and contents of billing data in the event of application or platform failures.
- The RKS MAY support distribution of billing data to all appropriate systems– This includes the implementation of a protocol that ensures data integrity and reliability on the usage collator interface.
- The RKS MAY support monitoring and reporting – This includes the ability to produce and send alarms to a network management system, and create various audit and measurement reports.
- The RKS MAY allow remote testing and maintenance capability.
- The RKS MAY support a Service Creation Environment.
- The RKS MAY support user defined fault handling in the case of incomplete Event Messages or other such anomalies.
- The RKS MAY support multiple downstream applications, and various transport methodologies.
- The RKS MAY support full auditability of data and processes.
- The RKS MAY support a user definable long-term storage mechanism.
- The RKS MAY support disaster planning and recovery processing.

4.3 General PacketCable Network Element Requirements

This section lists requirements placed on the PacketCable network elements:

The CMS and CMTS MUST create a security relationship with each RKS that these network elements will send Event Messages as defined in the PacketCable Security Specification [5]. The MGC MUST create a security relationship with each RKS that the MGC will send Event Messages.

The CMS MUST support multiple primary RKS's, which might be required in cases in which total Event Message traffic exceeds the throughput capability of a single RKS.

For each call, the CMS or the MGC MUST create a unique Billing_Correlation_ID, identify the primary and all other RKS's and determine if the Event Messages are to be delivered in real time or they may be batched and sent at a later time.

- The trusted PacketCable network elements that generate Event Messages MUST timestamp Event Messages in 1 millisecond granularity +/- 100 milliseconds based on information reported by network time sources such as edge devices (Clients and Gateways).
- All PacketCable network elements that generate Event Messages MUST synchronize their clocks at least once per hour to a network clock source. This synchronization MUST assure the reporting device's own clock remains within ±100 milliseconds real time of the last synchronization value.
- PacketCable network elements that generate Event Messages MUST support system wide Network Time Protocol (NTP) time synchronization.
- The PacketCable network elements MUST support transport to multiple RKS's for processing system segmentation, downstream overload conditions, and disaster recovery.
- PacketCable network elements MUST support the transport of a single Event Message as well as a batch of Event Messages.
- All PacketCable Event Messages are transported to the RKS via the RADIUS protocol with a predefined message header.
- PacketCable elements that generate Event Messages MUST be capable of re-transmitting any Event Messages in storage, upon request.
- Each trusted PacketCable network element that generates an Event Message MUST identify itself with a static, unique element ID.
- The same PacketCable network element MUST generate a matched pair of event start/stop messages. Note that this may be problematic in later releases in the DCS call-signaling model where, for example the DCS-proxy generates the Signaling_Start, the CMTS generates the QoS start/stop, and no element generates the Signaling_Stop.

4.4 Event Message Interfaces

This section describes the interfaces between the PacketCable network elements that are involved in the Event Messages process. It should be noted that additional requirements are imposed on these by other PacketCable specifications and that the requirements listed in this document are specific to Event Messages. It should also be noted that additional requirements are specified for these interfaces and these PacketCable network elements in other sections of this document.

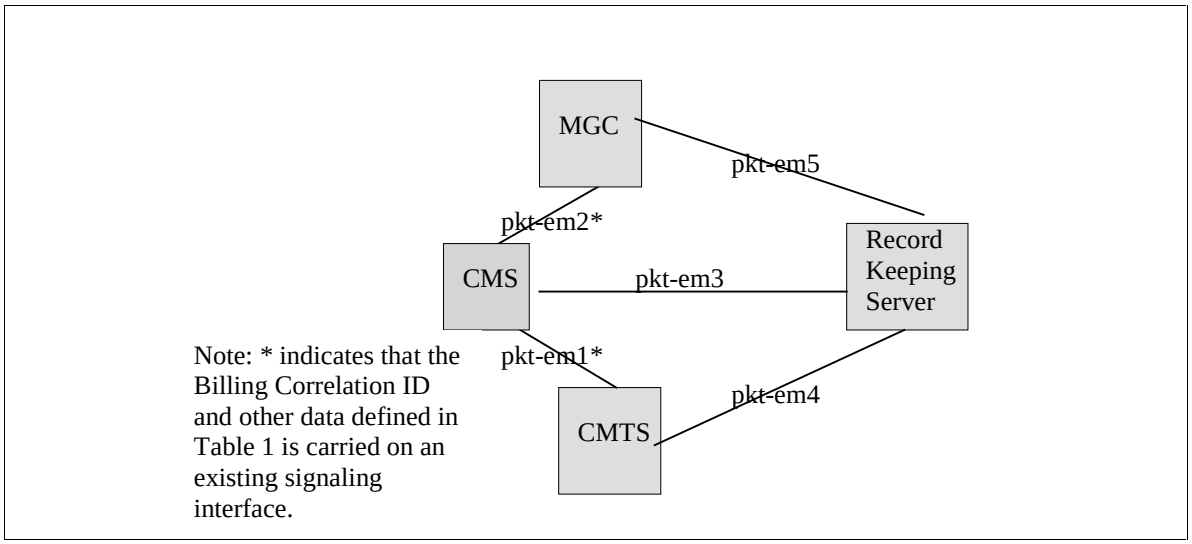

Figure 6: Event Message Billing Interfaces

4.4.1 CMS to CMTS (pkt-em1*)

The CMS to CMTS interface is defined by the PacketCable DQoS protocol [8].

The CMS sends the Billing Correlation ID and other data as defined in Table 1 to the CMTS via the DQoS GateSet message as specified in the DQoS specification [8].

4.4.2 CMS to MGC (pkt-em2*)

The CMS to MGC interface is vendor proprietary in PacketCable 1.0. This interface will be defined in a future PacketCable Specification.

If the CMS routes a call to the MGC, then the CMS MUST send the Billing Correlation ID and other data as defined in Table 1 to the MGC via a vendor-proprietary interface.

If the MGC routes a call to the CMS, then the MGC MUST send the Billing Correlation ID and other data as defined in Table 1 to the CMS via a vendor-proprietary interface.

4.4.3 CMS to RKS (pkt-em3)

The CMS to RKS interface is defined by the PacketCable security specification [5] and also by the Event Message transport and syntax rules defined in this document.

4.4.4 CMTS to RKS (pkt-em4)

The CMTS to RKS interface is defined by the PacketCable security specification [5] and by the Event Message transport and syntax rules defined in this document.

4.4.5 MGC to RKS (pkt-em5)

The MGC to RKS interface is defined by the PacketCable security specification [5] and by the Event Message transport and syntax rules defined in this document.

4.4.6 Security Requirements

When the network IPSec Security Associations are established, security keys MUST be created and exchanged between each RKS (primary, secondary, etc) and every CMS, and CMTS that will send Event Messages to any of those RKS's. A security association MUST exist between the MGC and RKS and is left to vendor implementation in PacketCable 1.0. The Event Messages are sent from the CMS and CMTS to the RKS using the RADIUS transport protocol, which is in turn secured by IPSec. Refer to the PacketCable Security Specification [5] for a detailed description of the security requirements for the PacketCable Event Message interfaces.

4.4.7 Storage Requirements

PacketCable network elements that generate Event Messages MUST support storage of Event Messages in a secure manner, until an acknowledgment from an RKS for those Event Messages is received. A user-configurable retention time for storage of these Event Messages, beyond the above requirement is recommended. It is recommended that PacketCable network elements support a minimum of 24 hours of Event Message storage.

The RKS MUST have the ability to store the Event Messages for at least one week or until sent to the other operating systems and successful receipt is acknowledged from those systems. The RKS must also have the ability to dump the Event Messages to some type of off-line storage device on a regular basis (CD, TAPE, or other media) for retrieval and regulatory purposes.

5 PACKETCABLE SERVICES AND THEIR ASSOCIATED EVENT MESSAGES

This section defines the supported PacketCable 1.0 Services and their associated Event Messages. Although many of the PacketCable 1.0+ services can be billed using the Event Messages and attributes defined in this document, the services described in this section are currently limited to PacketCable 1.0 services.

In order to identify appropriate Event Messages required for each service, representative call flows were developed for PacketCable 1.0 basic call configurations. The PacketCable Call Flow documents [12], [13], [14] provide a description of the call configuration along with any assumptions made about a specific service and an example call flow. It is not the intention of these call flow documents to limit the realization of any of these services to any specific implementation.

5.1 PacketCable Call Configurations

This section describes the three basic PacketCable 1.0 call configurations: On-Net to On-Net, On-Net to Off-Net, and Off-Net to On-Net. A required minimum set of Event Messages MUST be generated for each of these three basic call configurations. If specific services are initiated in along with the basic call, then refer to section 5.2 for a list of additional Event Messages for these specific services.

5.1.1 On-Net to On-Net Call Configuration

The most basic PacketCable call configuration is an On-Net to On-Net call within a single MSO's network, using 2 different MTAs that are both connected to the same CMS. For PacketCable 1.0, it is assumed that both the originating and terminating MTAs are using the same CMS and possibly 2 different CMTSs.

Refer to the PacketCable Call Flow document [12] for a complete description of this call configuration including an example call flow showing the triggers for these Event Messages.

Table 2: On-Net to On-Net Call Configuration

Event Message	Required or Optional	Comments
Signaling_Start	R	CMS is starting signaling to support a call start
QoS_Start	R	For Calling Party
QoS_Start	R	For Called Party
Database_Query	O	If LNP is required
Intelligent_Peripheral_Usage_Start	O	e.g. if an announcement is needed *NOTE: This Event Message will be defined in a future release of this PacketCable*

Event Message	Required or Optional	Comments
		specification.
Intelligent_Peripheral_Usage_Stop	O	e.g. if an announcement is needed *NOTE: This Event Message will be defined in a future release of this PacketCable specification.*
Call_Answer	R	Indicates start of media stream
Signaling_Stop	R	Generated for whichever party hangs up first
Call_Disconnect	R	Indicates termination of media steam
QoS_Stop	R	For Calling Party
QoS_Stop	R	For Called Party

5.1.2 On-Net to Off-Net Call Configuration (Outgoing PSTN Interconnect)

The only Off_Net interconnection supported by PacketCable 1.0 is to the PSTN. Therefore the CMS sends all Off_Net calls to the PSTN. The Interconnect_Start Event Message identifies the type of Off_Net trunk, for example SS7/FG-D trunks, Type 1/DTMF trunks or some other type of trunks as required. The Off_Net call (i.e. non-special access codes calls e.g. 800, 900, N11 etc.) may require an LNP query. The CMS MUST generate a database query Event Message each time a LNP database is accessed (regardless of whether this query is requested from a PSTN database or IP database).

Refer to the PacketCable Call Flow document [13] for a complete description of this call configuration including an example call flow showing the triggers for these Event Messages.

Table 3: On-Net to Off-Net Call Configuration

Event Message	Required or Optional	Comments
Signaling_Start	R	CMS is starting signaling to support a call start
QoS_Start	R	For Calling Party
Database_Query	O	If LNP is Required
Intelligent_Peripheral_Usage_Start	O	e.g. if an announcement is needed *NOTE: This Event Message will be defined in a future release of this PacketCable specification.*
Intelligent_Peripheral_Usage_Stop	O	e.g. if an announcement is needed *NOTE: This Event Message will be defined in a future release of this PacketCable specification.*
Interconnect_Start	R	For call setup

Event Message	Required or Optional	Comments
Call_Answer	R	Indicates start of media stream
Signaling_Stop	R	Generated for whichever party hangs up first
Interconnect_Stop	R	For call tear-down
Call_Disconnect	R	Indicates termination of media steam
QoS_Stop	R	For Calling Party

5.1.3 Off-Net to On-Net Service (Incoming PSTN Interconnection)

The CMS receives calls that are incoming from other entities and establishes communications with the MTA on the MSO's network. For PacketCable Release 1.0, it is assumed that all incoming calls are from the PSTN.

Refer to the PacketCable Call Flow document [14] for a complete description of this call configuration including an example call flow showing the triggers for these Event Messages.

Table 4: Off-Net to On-Net Call Configuration

Event Message	Required or Optional	Comments
Interconnect_Start	R	For call setup
QoS_Start	R	For Called Party
Intelligent_Peripheral_Usage_Start	O	e.g. if an announcement is needed *NOTE: This Event Message will be defined in a future release of this PacketCable specification.*
Intelligent_Peripheral_Usage_Stop	O	e.g. if an announcement is needed *NOTE: This Event Message will be defined in a future release of this PacketCable specification.*
Signaling_Start	R	CMS is starting signaling to service a request to start a call
Call_Answer	R	Indicates start of media stream
Signaling_Stop	R	Generated for whichever party hangs up first
Interconnect_Stop	R	For call tear-down
Call_Disconnect	R	Indicates termination of media steam
QoS_Stop	R	For Called Party

5.2 Specific Services

A basic set of Event Messages MUST be generated based on the type of call configuration: On_Net to On_Net, On_Net to Off_Net, Off_Net to On_Net. The basic set of Event Messages is described in section 5.1.

This section describes additional Event Messages that MUST be generated along with the basic set in order to describe specific PacketCable 1.0 services. This section also

describes optional Event Messages that MAY be generated along with the basic set and any additional required Event Messages. These additional required and optional Event Messages are identified in the tables in this section. It is expected that these additional Event Messages will be able to be generated regardless of the particular implementation of the service.

5.2.1 911 Service

A 911 call follows the standard On-Net to Off-Net Event Message flow described above in Section 5.1.2. 911 calls require special treatment. In PacketCable Release 1.0, it is assumed that the MSO sends 911 calls to the PSTN on a special trunk. The Trunk Group ID is captured in the Interconnect_Start and Interconnect_Stop Event Messages, and it is assumed that the RKS or some element downstream of the RKS has the capability of inferring this trunk group type from that unique Trunk Group ID.

No additional Event Messages are required beyond the basic ones listed for an On_Net to Off_Net call in Section 5.1.2

5.2.2 Other N11 Services (311, 411, 611)

These calls are identical to the 911 call both from a call flow and Event Message perspective. The determination of whether to bill or not can be performed at the Billing System based on the “Called Party Number” attribute. For example, charges for calls to 411 for directory assistance may be different than charges for 911 emergency calls, which are free, but the Event Messages, which capture the usage for both types of services, are the same. They would differ only in the content of specific attribute values such as the Called_Party_Number (411 vs. 911) within the Call_Answer Event Message. The billing system is expected to make a determination as to how much to bill the customer based on these attributes together with other factors such as whether the call is completed or not.

5.2.3 Toll-Free Services

Toll-Free Services follow the standard On-Net to Off-Net Event Message flow described above in Section 5.1.2. In PacketCable 1.0, toll-free calls can be handled two ways:

- Send all Toll-free calls to the PSTN on a special trunk. The call is treated exactly like the 911 case discussed above in Section 5.2.1 in terms of Event Messages, meaning that no additional Event Messages are required.
- Initiate a query to the toll-free SCP (in IP or PSTN) and, depending on the specified Carrier Identification Code, route the call to the appropriate network. A Database_Query Event Message MUST be generated to record the query to the toll-free database.

Table 5: Toll-Free Services

Additional Event Messages	Required or Optional	Comments
Database_Query	R	Not used for Scenario 1 but required for scenario 2

5.2.4 Operator Services

Operator Services follow the standard On-Net to Off-Net Event Message configuration described above in Section 5.1.2. There will be no new additional Event Messages beyond those already described for the On-Net to Off-Net calls in that section. The CMS will send that call to the designated Operator Service Provider using the PSTN. There may be multiple Operator Service Providers with which the MSO has contracts. The caller will just dial 0.

The CMS will generate an event identifying that call as 0- (denoting the single digit "0" dialed without any subsequent digits) with "0" in the Called number field. The CMS will replace the "0" in the Called Number field with the number of the Operator Service Provider (OSP). These parameters will be sent to PSTN so that call can be sent via PSTN to the OSP. It is assumed dedicated private lines to the OSP from each IP-switch are impractical and expensive for MSO and not considered as an option.

For the purposes of PacketCable 1.0, it is assumed that operator services only encompasses 0- services. 0+ service, in which the customer keys the dialed number in together with the initial "0", is not supported in PacketCable 1.0.

5.2.5 Call Block Service

Event Messages are generated for Call Block Service only if the CMS blocks a call. Call Blocking is supported by all of the three basic call configurations: On_Net to On_Net, On_Net to Off_Net, and Off_Net to On_Net.

The CMS can block calls depending on the policies laid out by the MSO. For example, the MSO may allow the end-user to block all 900 calls at the user's request. As another example, the MSO may recognize some calls as fraudulent and block those fraudulent calls. In this case an Event Message needs to be generated with some reason attributes as to why the call was blocked. In addition, depending on the type of blockage, the MSO may desire to play an appropriate announcement (e.g. "Sorry your time is up …."). The CMS may initiate another call to the Announcement Server via the PSTN and play it to the caller. A series of Event Messages will be generated for this call, using the same Billing_Correlation_ID as the standard Event Messages associated with the off-hook, dialing, etc., which is not expected to be used for billing this call to the end-user.

Table 6: Call Block Service

Additional Event Messages	Required or Optional	Comments
Service_Instance	R	none.
Intelligent_Peripheral_Usage_Start	O	*NOTE: This Event Message will be defined in a future release of this PacketCable specification.*
Intelligent_Peripheral_Usage_Stop	O	*NOTE: This Event Message will be defined in a future release of this PacketCable specification.*

5.2.6 Call Waiting Service

At any given time the caller may be talking and will hear the call waiting tone when another call is incoming. It is understood that at some point prior to this call, the called party subscribed to call waiting service. The called party can switch back and forth between the two calls by using the flash hook. Call Waiting can be supported by any of the three basic call configurations: On_Net to On_Net, On_Net to Off_Net, and Off_Net to On_Net.

The call flow is as follows:

There is an existing call to a number connected via the MTA/CMTS/CMS. Another call attempt is made to that number, the CMS:

Verifies that an existing call is already in progress,

Checks its internal database to verify whether the called party has subscribed to Call Waiting, if yes:

Establishes a voice connection to the Announcement Server (which will play the call waiting tone),

Creates a Event Message indicating that Call Waiting is being initiated

Mixes the two voice calls (the currently established voice call and the Call Waiting tone voice call) so that the called party can hear the call waiting tone.

It is assumed that Call Waiting only supports 2 calls (one active and the other on hold) in PacketCable 1.0. The call on hold will not be connected to any announcement server.

Both of the calls between which the subscriber is switching will generate a complete set of Event Messages on their own as detailed in Sections 5.1.2 and 5.1.3, but there may also be three additional Event Messages associated with this instance of Call Waiting, as detailed below. If the Announcement Server is located on the PSTN, then the previously discussed Call_Answer and Call_Disconnect Event Messages will be generated for this call.

Table 7: Call Waiting Service

Event Message	Required or Optional	Comments
Interconnect_Start	O	Required only if Announcement Server for Call Waiting tone is Off_Net on PSTN
Interconnect_Stop	O	Required only if Announcement Server for Call Waiting tone is Off_Net
Intelligent_Peripheral_Usage_Start	O	Required only if Announcement Server On_Net. *NOTE: This Event Message will be defined in a future release of this PacketCable specification*
Intelligent_Peripheral_Usage_Stop	O	Required only if Announcement Server On_Net. *NOTE: This Event Message will be defined in a future release of this PacketCable specification*
Service_Instance	R	none.

5.2.7 Call Forwarding Service

Call Forwarding Service applies only to calls terminating On_Net as described in sections 5.1.1 and 5.1.3.

The CMS gets notification that a call needs to be completed to a specific dialed number/end device. The CMS checks its internal database and determines that the called number has subscribed to Call Forwarding, Call Forwarding is currently active, and the forwarding number is XYZ. The CMS will initiate ANOTHER call with the new Calling Party Number as the old Dialed number and the Forwarded Number (XYZ) as the new Dialed Number. Event Messages will be generated for the fact that a Call Forwarding instance was initiated. The Billing_Correlation_ID for this leg will be different than the first call. The rationale for using the Related Billing Correlation ID as the common identifier for call forwarding is that it may be desirable to flag calls made automatically by invocation of call forwarding on the subscribers monthly statement in order to make it clear the reason those calls were placed. For all purposes the original call and the forwarded call will be two different billable calls.

Table 8: Call Forwarding Service

Event Message	Required or Optional	Comments
Service_Instance	R	none

5.2.8 Return Call Service

This service applies only to calls originating On_Net, described in sections 5.1.1 and 5.1.2. The CMS MUST keep a register with the Calling Party Number of the last call.

Return Call Service will return the last call that was made to an MTA. Upon instantiation of Return Call feature, the CMS will initiate another call with the Calling Party Number of the last call, retrieved from the register just described, as the Dialed number. Event Messages will be generated for the fact that the Return Call feature was initiated, using the Billing_Correlation_ID of this call. If the Calling Party Number of the last call had Caller ID privacy restrictions, then CMS may conference in a recording from an announcement server saying that this call can not be completed.

Table 9: Return Call Service

Event Message	Required or Optional	Comments
Service_Instance	R	none.
Interconnect_Start	O	Required only if Announcement Server for delivering the Message indicating reason Return Call cannot be activated is Off_Net on PSTN
Interconnect_Stop	O	Required only if Announcement Server for delivering the Message indicating reason Return Call cannot be activated is Off_Net on PSTN
Intelligent_Peripheral_Usage_Start	O	Required only if Announcement Server for delivering the Message indicating reason Return Call cannot be activated is On_Net. *NOTE: This Event Message will be defined in a future release of this PacketCable specification*
Intelligent_Peripheral_Usage_Stop	O	Required only if Announcement Server for delivering the Message indicating reason Return Call

Event Message	Required or Optional	Comments
		cannot be activated is On_Net. *NOTE: This Event Message will be defined in a future release of this PacketCable specification*

5.2.9 Repeat Call Service

Repeat Call Service applies only to calls terminating On_Net as described in sections 5.1.1 and 5.1.3.

Repeat Call can be initiated when the caller dials a number and gets a busy signal. With this feature the caller dials a special pre-determined string of digits (*66 in USA) which then instructs the network to keep polling the called and calling party and when both free, establish the communication. In PacketCable 1.0, the originating CMS will keep trying to establish communications to the called number for a pre-determined amount of time.

Table 10: Repeat Call Service

Event Message	Required or Optional	Comments
Service_Instance	R	none.
Interconnect_Start	O	Required if Announcement Server for delivering the Message indicating reason Repeat Call cannot be activated is Off_Net on PSTN
Interconnect_Stop	O	Required only if the appropriate Interconnect_Start was activated
Intelligent_Peripheral_Usage_Start	O	Required only if Announcement Server for delivering the Message indicating reason Repeat Call cannot be activated is On_Net. *NOTE: This Event Message will be defined in a future release of this PacketCable specification*
Intelligent_Peripheral_Usage_Stop	O	Required only if Announcement Server for delivering the Message indicating reason Repeat Call cannot be activated is

Event Message	Required or Optional	Comments
		On_Net, *NOTE: This Event Message will be defined in a future release of this PacketCable specification*

Note: There may be multiple Interconnect_Start and Stops capturing the multiple different times the originating CMS tries to make an Off-Net call to try to complete a Repeat Call request.

5.2.10 Voice Mail Service

Voice Mail Service only applies to calls terminating On_Net, described in sections 5.1.1 and 5.1.3.

It is assumed that the voice mail server will be located Off_Net for PacketCable 1.0. It is therefore assumed if voicemail billing is usage sensitive, that connections to the Off_Net voicemail system will be counted in the same way whether they are voicemail messages being left for the subscriber (deposit) or calls to retrieve the messages on the voicemail server.

Voice mail deposit and retrieval scenarios will be treated as separate transactions that have associated Event Messages. Event Messages for voice mail deposit will look like a standard On_Net to Off_Net call. When the call is transferred to the Voice Mail Server, the Routing Number MUST be captured and populated with the Voice Mail Server Address.

The connection time to the Voice Mail Server MAY also be derived through the standard On_Net to Off_Net Event Messages. Since the Voice Mail Server is located Off_Net, Event Messages for voice mail retrieval MAY only be generated if the retrieval is initiated from a device within the MSO's network (e.g. On_Net to Off_Net call).

5.2.11 Message Waiting Indicator Service

It is assumed that an Off_Net voicemail system is used as described in Section 5.2.10. Because it seems unreasonable for the CMS to have to place a separate call to the Off_Net system each time a voicemail subscriber goes off-hook, it is assumed that a mechanism exists which allows the Off_Net voicemail system pass the information to the CMS indicating which subscribers have voicemail waiting. A further assumption is that the MTA is capable of delivering the audible stutter-tone message-waiting indicator to the subscriber's MTA port going off-hook, on the command of the CMS.

Under the scenario described in the assumptions section, and given the fact that billing will not be based on any per use delivery of the stutter tone, there will be no Event Messages required for this service. Billing will be based on a combination of information obtained from the Voicemail send/retrieve Event Messages discussed in Section 5.2.10 and provisioning information indicating when a subscriber has signed up for voicemail services.

6 PACKETCABLE EVENT MESSAGE STRUCTURE

This section describes the various Event Messages, together with their associated list of attributes. Refer to Section 7 for a detailed description of the attributes described in this section. Refer to Section 5 a detailed description of the services and their associated Event Messages.

The following tables show association between PacketCable 1.0 services, supported by the aforementioned call configurations, and proposed Event Messages that may be generated for each service. Voice communications services that PacketCable 1.0 will provide are based on three main call configurations:

- On-Net to On-Net;
- On-Net to Off-Net;
- Off-Net to On-Net.

Table 11 provides a list of PacketCable Event Messages defined in this document. More than one set of Event Messages MAY be generated during a particular service instance.

Table 11. PacketCable Event Message Summary

Event Message ID	PacketCable Event Message	Description
0	Reserved	
1	Signaling_Start	Start of signaling for originating or terminating part of the call.
2	Signaling_Stop	Stop of signaling for originating or terminating part of the call.
3	Database_Query	An inquiry into an external database; for example a toll-free number database.
4	Intelligent_Peripheral_Usage_Start	Deferred.
5	Intelligent_Peripheral_Usage_Stop	Deferred.
6	Service_Instance	Indicates an occurrence of a service
7	QoS_Start	Start of QoS for originating or terminating part of the call.
8	QoS_Stop	Stop of QoS for originating or terminating part of the call.
9	Service_Activation	Indicates a subscriber has activated a service.
10	Service_Deactivation	Indicates a subscriber has deactivated a service
11	Undefined	
12	Undefined	
13	Interconnect_(Signaling)_Start	Start of network interconnect signaling (between PacketCable and PSTN) for originating or terminating part of the call.
14	Interconnect_(Signaling)_Stop	Stop of network interconnect signaling (between PacketCable and PSTN) for originating or terminating part of the call.
15	Call_Answer	Indicates that all network resources for have been allocated for originating or terminating part of the call.
16	Call_Disconnect	Indicates that all network resources for have

Event Message ID	PacketCable Event Message	Description
		been released for originating or terminating part of the call.
17	Time_Change	Indicates time change on a network element.
19	QoS_Change	Indicates a Change in QoS.

Table 12. Services supported by On-Net to On-Net call configuration

Service	Event Message ID																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	19
Basic	X	X	X	X	X		X	X			UNDEFINED	UNDEFINED			X	X		
Call Block	X	X		X	X	X	X	X	X	X					X	X		
Call Waiting	X	X		X	X	X	X	X	X	X					X	X		
Call Forwarding	X	X		X	X	X	X	X	X	X					X	X		
Return Call	X	X		X	X	X	X	X							X	X		
Repeat Call	X	X		X	X	X	X	X							X	X		
Voice Mail	X	X		X	X		X	X							X	X		

Table 13: Services supported by On-Net to Off-Net call configuration.

Service	Event Message ID																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	19
Basic	X	X	X	X	X		X	X			UNDEFINED	UNDEFINED	X	X	X	X		
Call Block	X	X		X	X	X	X	X	X	X			X	X	X	X		
Call Waiting	X	X		X	X	X	X	X	X	X			X	X	X	X		
Return Call	X	X		X	X	X	X	X					X	X	X	X		
Repeat Call	X	X		X	X	X	X	X					X	X	X	X		
911	X	X	X	X	X		X	X					X	X	X	X		
N11	X	X	X	X	X		X	X					X	X	X	X		
Toll-Free	X	X	X	X	X		X	X					X	X	X	X		
Operator	X	X		X	X		X	X					X	X	X	X		

Table 14. Services supported by Off-Net to On-Net call configuration

Service	Event Message ID																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	19
Basic	X	X	X	X	X		X	X			UNDEFINED	UNDEFINED	X	X	X	X		
Call Block	X	X		X	X	X	X	X	X	X			X	X	X	X		
Call Waiting	X	X		X	X	X	X	X	X	X			X	X	X	X		
Repeat Call	X	X		X	X	X	X	X					X	X	X	X		
Call Forwarding	X	X		X	X	X	X	X	X	X					X	X		
Voice Mail	X	X		X	X		X	X					X	X	X	X		

6.1 Event Message Structure

An Event Message contains a header followed by attributes. The header is required on every Event Message. The attributes will vary based on the type of service the Event Message is describing. Refer to Table 32 for a description of the Event Message Header. Example information contained in the header includes: version of Event Message structure, timestamp indicating when the trigger event occurred, Billing

Correlation ID used to associate multiple Event Messages with a single service. Example information contained in attributes includes: Called Party Number, Calling Party Number, Trunk Group ID.

Header
Attribute #1
Attribute #2
Attribute #3
⋮
Attribute #n

6.2 Service_Instance

This event captures the fact that a service event has happened. The Event_Time attribute in the Event Message Header (see Table 32) MUST contain the time at which the service occurred.

This Event Message indicates the time at which the CMS provides an instance of a call control/feature service. For example, the time at which a call is put on hold, the time at which a call is forwarded, the time at which a last call return service is provided, the time at which a call-waiting service is provided, etc.

The CMS MUST timestamp these messages immediately upon operation of the service instance being reported.

Table 15. Service_Instance Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Service_Name	R	Class Service name 1. Call_Block 2. Call_Forward 3. Call_Waiting 4. Repeat_Call 5. Return_Call
Call_Termination_Cause	O	1 = Required
Related_Call_Billing_Correlation_ID	O	2,3 = Required
Charge_Number	O	2,3,4,5 = Required
First_Call_Calling_Party_Number	O	3 = Required
Second_Call_Calling_Party_Number	O	3 = Required
Called_Party_Number	O	3 = Required
Routing_Number	O	4,5 = Required
Calling_Party_Number	O	4,5 = Required

6.3 Service_Activation

This event captures a subscriber activating a service. The Event_Time attribute in the Event Message Header (see Table 32) MUST contain the time when the service was activated.

This Event Message indicates the time at which the CMS records an attempt to activate a service. For example, the time at which call-forwarding is activated by the MTA user, the time at which the call-waiting service is activated by the MTA user, etc. These service activations are typically requested via a ∗XX dial-string.

The CMS MUST timestamp this message immediately upon successful activation of the requested service.[1] .

The CMS MUST create a new Billing Correlation ID for this Event Message even if a service is activated during an existing call.

Table 16. Service_Activation Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Service_Name	R	Class Service name 1. Call_Block 2. Call_Forward 3. Call_Waiting
Forwarded_Number	O	2 = Required

6.4 Signaling_Start

This Event Message indicates the time at which signaling starts. The originating CMS or MGC MUST issue this Event Message for any given call. The originating CMS or MGC that issues this Event Message MUST issue the corresponding Signaling_Stop Event Message.

The terminating CMS or MGC MAY issue this Event Message. If the terminating CMS or MGC issues this Event Message, then that terminating CMS or MGC MUST also issue the corresponding Signaling_Stop Event Message.

The CMS or MGC MUST timestamp this message prior to digit translation. Note that the attributes contained in this Event Message contain information that is obtained after digit translation.

The CMS MUST timestamp this message immediately upon receipt of:

- an NCS-signaling NTFY message with a routable set of digits that indicate a call attempt

The MGC MUST timestamp this message immediately upon receipt of:

[1] Failed activation attempts are not reported at this time.

- an SS7 IAM message, or
- a TCGP NTFY with digits (operator services)

Table 17. Signaling_Start Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Direction_indicator	R	none.
MTA_Endpoint_Name	R	This attribute if required when the CMS generates this message. This attribute is NOT required when the MGC generates this message.
Calling_Party_Number	R	none.
Called_Party_Number	R	none.
Carrier_Identification_Code	O	This attribute MUST be included when the MGC generates this message.
Trunk_Group_ID	O	This attribute MUST be included when the MGC generates this message.

6.5 Signaling_Stop

This Event Message indicates the time at which signaling terminates. The originating CMS or MGC that issues the corresponding Signaling_Start Event Message MUST issue this Signaling_Stop Event Message.

If the terminating CMS or MGC issues a corresponding Signaling_Start Event Message, then that terminating CMS or MGC MUST also issue this corresponding Signaling_Stop Event Message.

The CMS MUST timestamp this message immediately upon receipt of the last signaling event in the following list:

- acknowledgement of the CMS-issued NCS-signaling DLCX message,
- transmission of the acknowledgement of an MTA-issued NCS-signaling DLCX message, or
- the last signaling message to/from a peer CMS or MGC associated with this call.

The MGC MUST timestamp this message immediately upon receipt of the last signaling event in the following list:

- transmission/receipt of an RLC to/from the Signaling Gateway that communicates with the SS7 network
- receipt of the acknowledgement of the MGC-issued TGCP DLCX,
- transmission of the acknowledgement of an MG-issued TGCP DLCX, or
- transmission/receipt of the last signaling message to/from a CMS associated with this call.

Table 18. Signaling_Stop Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Direction_indicator	R	none.
MTA_Endpoint_Name	R	This attribute MUST be included if the CMS generates this message. This attribute is NOT required if the MGC generates this message.

6.6 Service_Deactivation

This Event Message indicates the time at which the CMS records an attempt to deactivate a service. For example, the time at which call-forwarding is deactivated by the MTA user, the time at which the call-waiting service is deactivated by the MTA user, etc. These service deactivations are typically requested via a *XX dial-string.

The CMS MUST timestamp this message immediately upon successful deactivation of the requested service. Failed Deactivation attempts are not reported at this time

The CMS MUST create a new Billing Correlation ID for this Event Message even if a service is deactivated during an existing call.

Table 19. Service_Deactivation Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Service_Name	R	none.

6.7 Database_Query

This Event Message indicates the time at which a one-time request/response transaction or database dip is completed by an intelligent peripheral (800 number database, LNP database, etc.).

- The CMS originating the call MUST timestamp this message immediately upon a receipt of the response from the Intelligent Peripheral.

Table 20. Database_Query Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (Table 32)	R	none.
Database_ID	R	none.
Query_Type	R	Toll Free Number Lookup, LNP lookup, etc.
Called_Party_Number	R	none.

Attribute Name	Required or Optional	Comment
Returned_Number	R	Note: There may be multiple numbers returned. If multiple numbers are returned this Attribute MUST be included for each number returned.

6.8 Intelligent_Peripheral_Usage_Start

Deferred.

6.9 Intelligent_Peripheral_Usage_Stop

Deferred.

6.10 Interconnect_Start

This Event Message indicates the time at which the start of network interconnect occurrs. Only the MGC is permitted to issue this Event Message.

- The MGC MUST timestamp this message immediately upon commitment of bandwidth between the PacketCable network and the PSTN.

Table 21. Interconnect_Start Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32))	R	none.
Carrier_Identification_Code	R	CIC Code of connecting operator.
Trunk_Group_ID	R	TGID of the trunk over which the interconnection is occurring
Routing_Number	R	none.

6.11 Interconnect_Stop

This Event Message indicates the termination of bandwidth between the PacketCable network and the PSTN. Only the MGC is permitted to issue this Event Message.

- The MGC MUST timestamp this message immediately upon release of bandwidth between the PacketCable network and the PSTN

Table 22. Interconnect_Stop Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Carrier_Identification_Code	R	CIC Code of connecting operator.
Trunk_Group_ID	R	TGID of the trunk over which the

Attribute Name	Required or Optional	Comment
		interconnection is occurring.

6.12 Call_Answer

This Event Message indicates that the media connection is open because answer has occurred. The terminating CMS or MGC MUST generate this Event Message. The originating CMS or MGC MAY generate this Event Message.

The CMS MUST timestamp this message immediately upon receipt of:

- an NCS-signaling NTFY message indicating off-hook at the destination MTA.

The MGC MUST timestamp this message immediately upon receipt of:

- an SS7 ANS message from the PSTN, or
- an answer indication from the MG indicating answer has occurred on an operator services trunk.

Table 23. Call_Answer Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Called_Party_Number	R	none.
Routing_Number	R	none.
Charge_Number	R	none.
Location_Routing_Number	R	For local number portability use.

6.13 Call_Disconnect

T This Event Message indicates the time at which the media connection is closed because the calling party has terminated the call by going on-hook, or that the destination party has gone on-hook and the called-party's call-continuation timer[2] has expired. This message MUST be issued by the first party, either terminating or originating, to detect call termination as indicated below:

The CMS MUST timestamp this message immediately upon receipt of:

- an NCS-signaling NTFY message indicating on-hook at the calling party MTA[3], or
- on expiration of the destination MTA's call-continuation timer

The MGC MUST timestamp this message immediately upon receipt of:

[2] In the current telephony network, when the called party goes on-hook, a 10-11 second timer is started. If the calling party remains off-hook, and the called party goes off-hook again within that time period, the call continues.

[3] For emergency services calls, the CMS will normally NOT issue this Event Message as the call duration is controlled by the emergency services operator.

- an SS7 REL message from the PSTN via the SG, or
- an indication from the MG that an operator services trunk has disconnected.

Table 24. Call_Disconnect Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Direction_indicator	O	none.
Call_Termination_Cause	R	Normal Termination

6.14 QoS_Start

This Event Message indicates the time at which the CMTS committed bandwidth on the PacketCable access network. The commitment MAY have been done either through a DOCSIS message or a RSVP message.

The CMTS MUST timestamp this message immediately upon receipt of:

- the first request for bandwidth commitment by the MTA as indicated in a DOCSIS or RSVP message.

Table 25. QoS_Start Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Direction_indicator	O	none.
QoS_Descriptor	O	none.
MTA_UDP_Portnum	R	none.

6.15 QoS_Stop

This Event Message indicates the time at which the MTA released its bandwidth commitment on the PacketCable access network. The release MAY be done either through a DOCSIS message or an RSVP message.

The CMTS MUST timestamp this message immediately upon receipt of:

- a release of bandwidth reservation by the MTA as indicated in a DOCSIS or RSVP message.

Table 26. QoS_Stop Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.

Attribute Name	Required or Optional	Comment
Direction_indicator	O	none.
QoS_Descriptor	O	none.
SF_ID	R	none.

6.16 Time_Change

This event captures an instance of a time change. The Event_Time attribute in the Event Message Header (Table 32) MUST contain the time at which the clock on the trusted network element was adjusted.

Table 27. Time_Change Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Time_Adjustment	R	none.

6.17 QoS_Change

This Event Message indicates the time at which the MTA modified its bandwidth commitment on the PacketCable access network. The change MAY be done either through a DOCSIS message or an RSVP message.

The CMTS MUST timestamp this message immediately upon receipt of:

- A change in bandwidth reservation by the MTA as indicated in a DOCSIS or RSVP message.

Table 28. QoS Change Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	none.
Direction_indicator	O	none.
QoS_Descriptor	O	none.
MTA_UDP_Portnum	R	none.

6.18 RTP_Connection_Parameters Event Message

Deferred.

7 PACKETCABLE EVENT MESSAGE ATTRIBUTES

This section describes the PacketCable attributes that are included in the PacketCable Event Messages.

Table 29 shows a mapping of the PacketCable Event Messages and their associated PacketCable attributes. Table 30 contains a detailed description of the PacketCable attributes. Table 31 contains special PacketCable attributes that MAY be added to the RADIUS accounting-response messages to support a request for retransmission of Event Messages.

Table 29. PacketCable Attributes Mapped to PacketCable Event Messages

EM Attribute ID	EM Attribute Name	Event Message ID																
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**19**
0	Reserved																		
1	EM_Header	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
2	Undefined																		
3	MTA_Endpoint_Name	X	X																
4	Calling_Party_Number	X					X												
5	Called_Party_Number	X		X			X			X						X			
6	Database_ID			X															
7	Query_Type			X															
8	Undefined																		
9	Returned_Number			X															
10	Undefined																		
11	Call_Termination_Cause						X										X		
12	Undefined																		
13	Related_Call_Billing_Correlation_ID						X												
14	First_Call_Calling_Party_Number						X												
15	Second_Call_Calling_Party_Number						X												
16	Charge_Number						X									X			
17	Forwarded_Number									X									
18	Service_Name						X			X	X								
19	Undefined																		
20	Undefined																		
21	Undefined																		
22	Location_Routing_Number															X			
23	Carrier_Identification_Code	X												X	X				
24	Trunk_Group_ID	X												X	X				
25	Routing_Number						X							X		X			
26	MTA_UDP_Portnum							X											X
27	Undefined																		
28	Undefined																		
29	Undefined																		

EM Attribute ID	EM Attribute Name	Event Message ID																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	19
30	SF_ID								X										
31	Error_Description																		
32	QoS_Descriptor							X	X										X
33	Undefined																		
34	Undefined																		
35	Undefined																		
36	Undefined																		
37	Direction_indicator	X	X					X									X		X
38	Time_Adjustment																	X	

Table 30 provides a detailed list of the PacketCable Event Message attributes. A data value of an attribute may be represented by a simple data format (one data field) or by a more complex data format (Data Structure). Data Structure formats of the appropriate attributes are detailed in Table 32 through Table 38. It should be noted that Event Message 17 it not service dependant.

Table 30. PacketCable Event Message attributes

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
0	Reserved			
1	59 bytes	EM_Header	Data structure See Table 32.	Common data required on every PacketCable Event Message
2	Undefined			
3	variable length, maximum of 255 bytes	MTA_Endpoint_ Name	ASCII character string.	Physical Port name (aaln/#) as defined in the PacketCable NCS Spec [4]
4	20 bytes	Calling_Party_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number of the Originating party. In the future other numbering plans will be addressed.
5	20 bytes	Called_Party_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number of the terminating party. In the future other numbering plans will be addressed.
6	Variable length, maximum of 255 bytes	Database_ID	Right justified, space padded ASCII character string.	A unique identifier of the referenced database.
7	2 bytes	Query_Type	Unsigned integer	Query type: 0=Reserved 1=Toll Free Number Lookup

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
				2=LNPNumberLookup
8	Undefined			
9	20 bytes	Returned_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number resulting from a database query. In the future other numbering plans will be addressed.
10	Undefined			
11	6 bytes	Call_Termination_Cause	Data structure See Table 35.	Termination code identifier.
12	Undefined			
13	16 bytes	Related_Call_Billing_Correlation_ID	Data structure. See Table 33	Billing Correlation ID for possible use in value added services.
14	20 bytes	First_Call_Calling_Party_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number of the calling party. In the future other numbering plans will be addressed.
15	20 bytes	Second_Call_Calling_Party_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number of the calling party. In the future other numbering plans will be addressed.
16	20 bytes	Charge_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number of billable party. In the future other numbering plans will be addressed.
17	20 Bytes	Forwarded_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number of the Forwarded Number. In the future other numbering plans will be addressed.
18	32 Bytes	Service_Name	Right justified, space padded ASCII character string.	Class Service Name. Allowed names are: “Call_Block”. “Call_Forward” “Call_Waiting”, “Repeat_Call”, “Return_Call”,
19	Undefined			
20	Undefined			
21	Undefined			
22	20 bytes	Location_Routing_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number of the terminating party. In the future other numbering plans will be

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
				addressed. For LNP uses.
23	8 bytes	Carrier_Identification_Code	Right justified, space padded ASCII character string.	If the MSO provides a service for a telecommunications operator, the Carrier Identification Code (CIC) or other identification is recorded in this field.
24	6 bytes	Trunk_Group_ID	Data structure See Table 36.	Trunk group identification.
25	20 bytes	Routing_Number	Right justified, space padded ASCII character string.	PacketCable 1.0 will use E.164 formatted address specifying the number of the terminating party. In the future other numbering plans will be addressed.
26	4 bytes	MTA_UDP_Portnum	Unsigned Integer	MTA Endpoint UDP Port Number.
27	Undefined			
28	Undefined			
29	Undefined			
30	4 bytes	SF_ID	Unsigned integer	Service Flow ID, a 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSISRF MAC domain. Any 32-bit SFID MUST not conflict with a zero-extended 14-bit SID. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). USFIDs and DSFIDs are allocated from the same SFID number space.
31	32 bytes	Error_Description	Right justified, space padded ASCII character string.	A user-defined description of the error conditions. Refer to Table 34
32	Variable; Min 8 bytes	QoS_Descriptor	Data structure See Table 37.	QoS parameters data See Appendix C of DOCSIS1.1 refer to . [7].
37	2 bytes	Direction_indicator	Unsigned integer	Specifies if a device acts on behalf of an originating or terminating part of the call at the time an Event Message is being generated. 0=undefined 1 =Originating 2=Terminating
38	8 bytes	Time_Adjustment	signed integer	Time adjustment of an element's (CMS, CMTS, MGC's) clock. This time is in millisecond, detailing the amount of the time change.

7.1 RADIUS Accounting-Response Retransmit Request Attributes

Due to the presence of the sequence number in the Event Message Header, it is possible for the RKS to detect missing Event Messages. The RKS MAY request retransmission of these Event Messages by including additional attributes in an Accounting-Response sent from the RKS to a PacketCable network element. Refer to Table 31 for a detailed description of the PacketCable retransmit attributes.

Table 31. RADIUS Accounting-Response Retransmit Request Attributes

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
240	18 Bytes	Missing_Events_Start_Time	Right justified, space padded ASCII Character String	The time at which the RKS stopped receiving Event Messages from this client. YYYYMMDDHHMMSS.MMM ASCII formatted date and time from NTP time reference. Millisecond granularity.
241	18 Bytes	Missing_Events_End_Time	Right justified, space padded ASCII Character String	The time at which the RKS recommenced receiving Event Messages from this client. YYYYMMDDHHMMSS.MMM ASCII formatted date and time from NTP time reference. Millisecond granularity.
242	4 Bytes	Missing_Events_Start_Sequence	Unsigned integer	The sequence number of the first Event Message that the RKS is missing from this client.
243	4 Bytes	Missing_Events_Stop_Sequence	Unsigned integer	The sequence number of the last Event Message that the RKS is missing from this client.

7.2 EM_Header Attribute Structure

Table 32 contains a detailed description of the fields in the EM_Header attribute structure. This Event Message Header attribute MUST be the first attribute in every PacketCable Event Message.

Table 32. EM_Header Attribute Structure

Field Name	Semantics	Value Type	Length
Version ID	Identifies version of this structure. 1 = PacketCable 1.0	Unsigned integer	2 bytes
Billing Correlation ID	Unique identifier for a transaction within a network. See following section.	Data Structure Table 33	16 bytes
Event	Identifies the type of Event Message.	Unsigned integer	2 bytes

Field Name	Semantics	Value Type	Length
Message Type	refer to Table 11 for a listing of Event message types.		
Element Type	Identifies Type of Originating Element: 0 = Reserved 1 = CMS 2 = CMTS 3 = Media Gateway Controller	Unsigned integer	2 bytes
Element ID	Unique code indicating the originating PacketCable network element For PC 1.0 this is the MAC for PC 1.0+ this is the CLLI	Right justified, space padded ASCII Character String	8 bytes
Sequence Number	Each network element MUST assign a unique and monotonically increasing unsigned integer for each Event Message sent to a given RKS. This is used by the RKS to determine if Event Message are missing from a given network element.	Unsigned integer	4 bytes
Event_time	Event generation time and date. Millisecond granularity. Format: yyyymmddhhmmss.mmm	ASCII character string	18 bytes
Status	Status indicators.	See Table 34	4 bytes
Priority	Indicates the importance to assign relative to other network traffic. For PacketCable Release 1.0, values for this field will be user defined	Unsigned integer	1 byte
Attribute Count	Indicates the number of attributes that follow (or are appended to) this header in the current Event Message	Unsigned integer	2 bytes
Event Object	This is a “place holder” for future PacketCable releases to allow for a grouping of services. It may be PacketCable Voice, PacketCable Video, etc. or it could be PacketCable, DOCSIS, etc. It MUST have a value of zero for PacketCable Release 1.0	Unsigned integer	1 byte

7.2.1 Billing Correlation ID Attribute Structure

Table 33 describes the Billing Correlation ID. The RKS, or some other back office application, uses the Billing Correlation ID to correlate Event Messages that are generated for a single transaction. It is one of the fields in the Event Message Header. The Billing Correlation ID is unique for each Transaction in the network. All Event Messages with the same Billing Correlation ID SHOULD be sent to the same primary RKS except in failover circumstances in which case the Event Messages MUST be sent to the next RKS on the failover RKS list.

Table 33. Billing_Correlation_ID Description

Field Name	Semantics	Value Type	Length
Timestamp	High-order 32 bits of NTP time reference	Unsigned integer	4 bytes
Element_ID	Network wide unique identifier for the originating CMS	Right justified, space padded ASCII Character String	8 bytes
Event Counter	Monotonically increasing for each Transaction	Unsigned integer	4 bytes

7.2.2 Status Field Attribute Structure

The Status field of the Event Message Header is a 32-bit mask. Bit 0 is the low-order bit; the field is treated as a 4 byte unsigned integer. Table 34 presents Status Field description.

Table 34.Status Field Description

Start Bit	Semantics	Bit Count
0	Error Indicator: 0 = No Error 1 = Possible Error 2 = Known Error 3 = Reserved Note: if Known error, then attribute 31 MUST be included in the Event Message corresponding to this header. If Possible error, then attribute 31 MAY be included in the Event Message corresponding to this header	2
2	Event Origin: 0 = Trusted Element 1 = Untrusted Element	1
3	Event Message Proxied: 0 = Not proxied, all data known by sending element 1 = proxied, data sent by a trusted element on behalf of an untrusted element	1
4	Reserved. PacketCable 1.0 value MUST be 0	28

7.3 Call Termination Cause Attribute Structure

Table 35 describes data structure of the Call_Termination_Cause attribute.

Table 35. Call Termination Cause Data Structure

Field Name	Semantics	Value Type	Length
Source_Document	Identifies the source Document of the Cause Codes: 0 = Reserved 1 = BAF (Bellcore Generic Requirements 1100 CORE). [15] 2 = Future	Unsigned integer	2 bytes
Cause_Code	Cause Code Identifier. Meaning determined by Source_Document defined in previous field.	Unsigned integer	4 bytes

7.4 Trunk Group ID Attribute Structure

Table 36 describes Trunk Group ID Data Structure.

Table 36. Trunk Group ID Data Structure

Field Name	Semantics	Value Type	Length
Trunk_Type	1 = Not Used 2 = Not Used 3 = SS7 direct trunk group number 4 = SS7 from IC to AT and SS7 from AT to EO 5 = Not Used 6 = SS7 from IC to AT and non-SS7 from AT to EO (terminating only) 9 = Signaling type not specified	Unsigned integer	2 bytes
Trunk_Number	ASCII Identifier. Values in the range 0000-9999.	Right justified, space padded ASCII character string.	4 bytes

7.5 QoS Descriptor Attribute Structure

Table 37 describes QoS Descriptor Data Structure.

Table 37. QoS Descriptor Data Structure

Field Name	Semantics	Value Type	Length
Status_Bitmask	Bitmask describing structure contents. See Table 32)	Bit map	4 bytes
Service_Class_Name	Service profile name	Right justified, space padded ASCII character string.	4 bytes

Field Name	Semantics	Value Type	Length
QoS_Parameter_Array	QoS Parameters. Contents determined by Status Bitmask.	Unsigned integer array	Variable length array of 32-bit unsigned integers

Table 38 describes the QoS Status Bitmask field of the QoS Descriptor attribute. Bits 2-17 describe the contents of the QoS_Parameter_Array. Each of these bits indicates the presence (bit=1) or absence (bit=0) of the named QoS parameter in the array. The location of a particular QoS parameter in the array matches the order in which that parameter's bit is encountered in the bitmask, starting from the low order bit.

Each QoS parameter present in the QoS_Parameter_Array must occupy four bytes. The definition and encoding of the QoS parameters can be found in Appendix C of the DOCSIS 1.1 specification [7]. QoS parameters whose definition specifies less than four bytes must be right justified (were the 4 bytes to be treated as an unsigned integer) in the four bytes allocated for the array element.

Table 38. QoS Bit Mask

Start Bit	Semantics	Bit Count
0	State Indication: 0 = Illegal Value 1 = Resource Reserved but not Activated 2 = Resource Activated 3 = Resource Reserved & Activated	2
2	Service Flow Scheduling Type	1
3	Nominal Grant Interval	1
4	Tolerated Grant Jitter	1
5	Grants Per Interval	1
6	Unsolicited Grant Size	1
7	Traffic Priority	1
8	Maximum Sustained Rate	1
9	Sustained Traffic Rate	1
10	Maximum Traffic Burst	1
11	Minimum Reserved Traffic Rate	1
12	Maximum Concatenated Burst	1
13	Request/Transmission Policy	1
14	Nominal Polling Interval	1
15	Tolerated Poll Jitter	1
16	IP Type of Service Override	1
17	Maximum Downstream Latency	1

8 TRANSPORT PROTOCOL

This section provides an overview of the transport protocol between the PacketCable network elements that generate Event Messages (CMS, CMTS, MGC) and the Record Keeping Server (RKS). The transport protocol for PacketCable 1.0 is RADIUS Accounting (RFC2139) with PacketCable extensions.

8.1 PacketCable 1.0 Transport Requirements

- The Event Message transactions MUST be authenticated.
- The transport protocol MAY support confidentiality of Event Messages.
- End-to-end security across multiple administrative domains is not required.

8.2 RADIUS Accounting Protocol

The RADIUS Accounting protocol is a client/server protocol that consists of two message types: Accounting–Request and Accounting-Response. PacketCable network elements that generate Event Messages are RADIUS clients that send Accounting-Request messages to the RKS. The RKS is a RADIUS server that sends Accounting-Response messages back to the PacketCable network elements indicating that it has successfully received and stored the Event Message.

The Event Messages are formatted as RADIUS Accounting-Request and Accounting-Response packets as specified in RFC2139. Although PacketCable 1.0 specifies RADIUS as the transport protocol, alternate transport protocols MAY be supported in future PacketCable releases.

8.2.1 Reliability

The RADIUS messages are transported over UDP, which does not guarantee reliable delivery of messages, hence the request/response nature of the protocol (see RFC2138 for the technical justification of choosing UDP over TCP for the transport of Authentication, Authorization and Accounting messages).

When an RKS receives and successfully records all PacketCable Event Messages in a RADIUS Accounting-Request message, it MUST send an Accounting-Response message to the client. If the PacketCable network element does not receive an Accounting-Response within the configured retry interval, it MUST resend the same Accounting-Request either to the same RKS or the next RKS on its failover list. The PacketCable network element SHOULD continue resending the Accounting-Request until it receives an acknowledgement from an RKS or the message expires from its cache. The RADIUS server MUST NOT transmit any Accounting-Response reply if it fails to successfully record the Event Message.

8.2.2 Authentication and Confidentiality

Refer to the PacketCable security specification [5] for details concerning the use of IPSec to provide both authentication and confidentiality of the RADIUS messages.

Each PacketCable network element generating Event Messages MUST use a shared secret consisting of a 16-byte, all zero value to calculate the Authenticator field in the RADIUS message header. In order to improve interoperability with existing RADIUS server implementations, the RADIUS clients and servers MUST still calculate and populate the Authenticator field as described in RFC2139.

8.2.3 Standard RADIUS Attributes

Each RADIUS message starts with the standard RADIUS header shown in Table 39.

Table 39. RADIUS Message Header

Field Name	Semantics	Field Length
Code	Accounting-Request = 4 Accounting-Response = 5	1 byte
Identifier	Used to match accounting-request and accounting-response messages.	1 byte
Length	Total length of RADIUS message. min value = 20, max value = 4096	2 bytes
Authenticator	value = 0 as per PacketCable Security Specification [5].	16 bytes

The standard RADIUS Acct_Status_Type attribute MUST follow the RADIUS Message Header in every Accounting-Request message. This attribute indicates the type of this RADIUS Accounting-Request and is specific to the use of RADIUS as the transport protocol. An Acct-Status-Type value of Interim-Update is used to represent PacketCable Event Messages. This improves interoperability with existing RADIUS server implementation.

Table 40. RADIUS Acct_Status_Type

Type	Length	Value
40	6 bytes	Interim-Update = 3

The Acct_Status_Type attribute is the only standard RADIUS attribute used by PacketCable. PacketCable attributes are defined in Section 7 of this document. PacketCable attributes are encoded in the RADIUS Vendor Specific Attributes (VSA) structure as described in Table 41. Additional PacketCable or vendor-specific attributes can be added to existing Event Messages by adding additional RADIUS VSA's to the message.

The Vendor-Specific attribute includes a field to identify the vendor and the Internet Assigned Number Authority (IANA) has assigned PacketCable an SMI Network Management Private Enterprise Number of 4491 for the encoding of these attributes. The RKS server SHOULD ignore Event Messages where the PacketCable "Event

Message type" is unidentified. The RKS server SHOULD also ignore PacketCable event attributes where the event attribute type is unidentified

Table 41. Radius VSA Structure for PacketCable Attributes

Field Name	Semantics	Field Length
Type	Vendor Specific = 26	1 byte
Length	Total Attribute Length note: value is Vendor Length + 8	1 byte
Vendor ID	CableLabs = 4491	4 bytes
Vendor Attribute Type	PacketCable Attribute Type (refer to table 34)	1 byte
Vendor Attribute Length	PacketCable Attribute Length (refer to table 34)	1 byte
Vendor Attribute Value	PacketCable Attribute Value	Vendor Length bytes

8.3 PacketCable Extensions

8.3.1 PacketCable RADIUS Accounting-Request Packet Syntax

```
<RADIUS Accounting-Request> :==
<RADIUS message Header>
<RADIUS Acct_Status_Type>
<RADIUS VSA for PacketCable Event Message Header attribute>
<RADIUS VSA for PacketCable Event Message Attributes>
```

8.3.2 Retransmission Using RADIUS Accounting-Response Packet Syntax

Due to the presence of the sequence number in the Event Message Header, it is possible for the RKS to detect missing Event Messages. The RKS MAY request retransmission of these Event Messages by including additional PacketCable Event Message attributes in an Accounting-Response. Refer to table 33 for a description of these attributes.

```
<RADIUS Accounting-Response> :==
<RADIUS message Header>
<RADIUS VSA for PacketCable Missing_Event_Time_Start attribute>
<RADIUS VSA for PacketCable Missing_Event_Time_Stop attribute>

<RADIUS Accounting-Response> :==
<RADIUS message Header>
<RADIUS VSA for PacketCable Missing_Event_Sequence_Start attribute>
<RADIUS VSA for PacketCable Missing_Event_Sequence_Stop attribute>
```

Two mechanisms for retransmission request SHOULD be supported by the PacketCable network elements and the RKS:

- Time based: Refer to table 33 for a detailed description of the PacketCable Event Message time-based retransmission attributes: Missing_Event_Start_Time and Missing_Event_Stop_Time.

- Sequence number based: Refer to table 33 for a detailed description of the PacketCable Event Message sequence-based retransmission attributes: Missing_Event_Start_Sequence and Missing_Event_Stop_Sequence.

The PacketCable network element behavior on receipt of a retransmission request for Event Messages, which are still in its cache depends on whether the requested Event Messages have already been acknowledged by an RKS and if so, the RKS that acknowledged them.

- If the PacketCable network element still has the requested events in its event cache and has not received confirmation from any RKS that the events have been successfully recorded, it MUST send the Event Messages to the requesting RKS.
- If the PacketCable network element still has the requested events in its event cache but has already received confirmation that the events have been successfully recorded from the RKS requesting the retransmission, it SHOULD send the Event Messages to the requesting RKS.
- If the PacketCable network element still has the requested events in its event cache but has already received confirmation from an RKS other than the one requesting the retransmission that the events have been successfully recorded, it SHOULD send the Event Messages to the requesting RKS.

8.3.3 Batching of Multiple Event Messages in a Single RADIUS Accounting-Request

Multiple PacketCable Event Messages MAY be sent in a single RADIUS message simply by adding the Event Message to the Previous Event Message.

```
<RADIUS Accounting-Request> :==
<RADIUS message Header>
<RADIUS Acct_Status_Type>
<Message #1 RADIUS VSA for PacketCable Event Message Header
attribute>
<Message #1 RADIUS VSA for PacketCable Event Message Attributes>
<Message #1 RADIUS VSA for PacketCable Event Message Attributes>
<Message #2 RADIUS VSA for PacketCable Event Message Header
attribute>
<Message #2 RADIUS VSA for PacketCable Event Message Attributes>
```

The potential of a high Event Message volume raised the concern that the RADIUS mechanism for ensuring reliability via request/response may consume too much bandwidth or be too computationally intensive. This led to the requirement that it be possible to transit multiple PacketCable Event Messages in a single RADIUS message. The use of this 'batch mode' is left to the discretion of the PacketCable network element and will likely depend on the latency requirements of the particular event type. The number of Event Messages encapsulated in a single RADIUS message is still subject to the maximum RADIUS message length restriction of 4096 bytes.

PacketCable extends RADIUS Accounting, by introducing new attributes and new values for existing attributes. Since the RADIUS protocol is extendable in this

manner, it is expected that existing RADIUS server implementations will require minimal modifications to support the batch collection of PacketCable Event Messages.

The only mandatory attribute in a RADIUS Accounting-Request message is the Acct-Status-Type, which typically indicates whether the Accounting-Request marks the beginning of the user service (Start) or the end (Stop). Since a PacketCable Accounting-Request message may contain multiple Event Message Packets, a single message may contain Event Messages, which mark both the beginning and end of the user service. For this reason, an Acct-Status-Type value of Interim-Update is used to represent PacketCable Event Messages. This improves interoperability with existing RADIUS server implementation.

Appendix A. Glossary

AAA	Authentication, Authorization and Accounting
Access Control	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes or other system resources on a network.
Active	A service flow is said to be "active" when it is permitted to forward data packets. A service flow must first be admitted before it is active.
Admitted	A service flow is said to be "admitted" when the CMTS has reserved resources (e.g. bandwidth) for it on the DOCSIS network.
AF	Assured Forwarding. A Diffserv Per Hop Behavior.
AH	Authentication header is an IPSec security protocol that provides message integrity for complete IP packets, including the IP header.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access".
Announcement Server	An announcement server plays informational announcements in PacketCable network. Announcements are needed for communications that do not complete and to provide enhanced information services to the user.
AMA	Automated Message Accounting., a standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies)
Asymmetric Key	An encryption key or a decryption key used in a public key cryptography, where encryption and decryption keys are always distinct.
AT	Access Tandem
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information.
Authorization	The act of giving access to a service or device if one has the permission to have the access.
BAF	Bellcore AMA Format, another way of saying AMA
BPI+	Baseline Privacy Interface Plus is the security portion of the DOCSIS 1.1 standard which runs on the MAC layer.
CBC	Cipher block chaining mode is an option in block ciphers that combine (XOR) the previous block of ciphertext with the current block of plaintext before encrypting that block of the message.
CBR	Constant Bit Rate.
CA	Certification Authority - a trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CA	Call Agent. In this specification "Call Agent" is part of the CMS that maintains the communication state, and controls the line side of the communication.
CDR	Call Detail Record. A single CDR is generated at the end of each billable activity. A single billable activity may also generate multiple CDRs

CIC	Circuit Identification Code. In ANSI SS7, a two octet number that uniquely identifies a DSO circuit within the scope of a single SS7 Point Code.
CID	Circuit ID (Pronounced "Kid"). This uniquely identifies an ISUP DS0 circuit on a Media Gateway. It is a combination of the circuit's SS7 gateway point code and Circuit Identification Code (CIC). The SS7 DPC is associated with the Signaling Gateway that has domain over the circuit in question.
CIF	Common Intermediate Format
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set which must contain both an encryption algorithm and a message authentication algorithm (e.g. a MAC or an HMAC). In general, it may also contain a key management algorithm, which does not apply in the context of PacketCable.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
CIR	Committed Information Rate.
Cleartext	The original (unencrypted) state of a message or data.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax
CMS	Call Management Server. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology.
CMTS	Cable Modem Termination System, the device at a cable head-end which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
Codec	COder-DECoder
Confidentiality	A way to ensure that information is not disclosed to any one other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
COPS	Common Open Policy Service Protocol is currently an internet draft which describes a client/server model for supporting policy control over QoS Signaling Protocols and provisioned QoS resource management.
CoS	Class of Service. The type 4 tuple of a DOCSIS 1.0 configuration file.
CSR	Customer Service Representative
Cryptoanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
DA	Directory Assistance
DE	Default. A Diffserv Per Hop Behavior.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default - Network Provider DHCP Server
Digital certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate

Digital signature	A data value generated by a public key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum
DNS	Domain Name Server
Downstream	The direction from the head-end toward the subscriber location.
DSCP	Diffserv Code Point. A field in every IP packet which identifies the Diffserv Per Hop Behavior. In IP version 4, the TOS byte is redefined to be the DSCP. In IP version 6, the Traffic Class octet is used as the DSCP. See Appendix A.
DOCSIS	Data Over Cable System Interface Specification.
DPC	Destination Point Code. In ANSI SS7, a 3 octet number which uniquely identifies an SS7 Signaling Point, either an SSP, STP, or SCP.
DQoS	Dynamic Quality of Service, i.e. assigned on the fly for each communication depending on the QoS requested
DTMF	Dual-tone Multi Frequency (tones)
EF	Expedited Forwarding. A Diffserv Per Hop Behavior.
E-MTA	Embedded MTA – a single node which contains both an MTA and a cable modem.
Encipherment	A method used to translate information in plaintext into ciphertext.
Encryption	A method used to translate information in plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or MCU
EO	End Office
Errored Second	Any 1-sec interval containing at least one bit error.
ESP	IPSec Encapsulation Security Payload protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute
Event Message	Message capturing a single portion of a connection
FGD	Feature Group D signaling
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated"
Flow [IP Flow]	A unidirectional sequence of packets identified by ISO Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow"). A unidirectional sequence of packets associated with a SID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 821 for details.
Gateway	Devices bridging between the PacketCable IP Voice Communication world and the PSTN. Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signaling Gateway which sends and receives circuit switched network signaling tot he edge of the PacketCable network.
H.323	An ISO standard for transmitting and controlling audio and video information. The H.323 standard requires the use of the H.225/H.245 protocol for

	communication control between a "gateway" audio/video endpoint and a "gatekeeper" function.
Header	Protocol control information located at the beginning of a protocol data unit.
HFC	Hybrid Fiber/Coax(ial [cable]), HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the head-end and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.
H.GCP	A protocol for media gateway control being developed by ITU.
HMAC	Hashed Message Authentication Code – a message authentication algorithm, based on either SHA-1 or MD5 hash and defined in RFC 2104.
HTTP	Hyper Text Transfer Protocol. Refer to IETF RFC 1945 and RFC 2068.
IANA	Internet Assigned Numbered Authority. See www.ietf.org for details.
IC	Inter-exchange Carrier
IETF	Internet Engineering Task Force. A body responsible, among other things, for developing standards used in the Internet.
IKE	Internet Key Exchange is a key management mechanism used to negotiate and derive keys for SAs in IPSec.
IKE–	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
IKE+	A notation defined to refer to the use of IKE, which requires digital certificates for authentication.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access Transport Area
IP	Internet Protocol. An Internet network-layer protocol.
IPSec	Internet Protocol Security, a collection of Internet standards for protecting IP packets with encryption and authentication.
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part is a protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ISTP	Internet Signaling Transport Protocol
ISTP – User	Any element, node, or software process that uses the ISTP stack for signaling communications.
ITU	International Telecommunication Union
IVR	Interactive Voice Response System
Jitter	Variability in the delay of a stream of incoming packets making up a flow such as a voice communication.
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.
Key Management	The process of distributing shared symmetric keys needed to run a security protocol.

Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Key Pair	An associated public and private key where the correspondence between the two are mathematically related, but it is computationally infeasible to derive the private key from the public key.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
LATA	Local Access and Transport Area
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
LD	Long Distance
LIDB	Line Information Data Base, containing information on customers required for real-time access such as calling card personal identification numbers (PINs) for real-time validation
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
LLC	Logical Link Control, used here to mean the Ethernet Packet header and optional 802.1P tag which may encapsulate an IP packet. A sublayer of the Data Link Layer.
LNP	Local Number Portability. Allows a customer to retain the same number when switching from one local service provider to another.
LSSGR	LATA Switching Systems Generic Requirements
MAC	Message Authentication Code - a fixed length data item that is sent together with a message to ensure integrity, also known as a MIC.
MAC	Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
MC	Multipoint Controller
MD5	Message Digest 5 - a one-way hash algorithm which maps variable length plaintext into fixed length (16 byte) ciphertext.
MDCP	A media gateway control specification submitted to IETF by Lucent. Now called SCTP.
MDU	Multi-Dwelling Unit. Multiple units within the same physical building. The term is usually associated with high rise buildings
MEGACO	Media Gateway Control IETF working group. See www.ietf.org for details.
MG	The media gateway provides the bearer circuit interfaces to the PSTN and transcodes the media stream.
MGC	An Media Gateway Controller is the overall controller function of the PSTN gateway. It receives, controls and mediates call signaling information between the PacketCable and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow on to SGCP.
MIB	Management Information Base
MIC	Message integrity code, a fixed length data item that is sent together with a message to ensure integrity, also known as a MAC.
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSO	Multi-System Operator, a cable company that operates many head-end

	locations in several cities.
MSU	Message Signal Unit
MTA	Media Terminal Adapter – contains the interface to a physical voice device, a network interface, CODECs, and all signaling and encapsulation functions required for VoIP transport, class features signaling, and QoS signaling.
MTP	The Message Transfer Part is a set of two protocols (MTP 2, 3) within the SS7 suite of protocols that are used to implement physical, data link and network level transport facilities within an SS7 network.
MWD	Maximum Waiting Delay
NANP	North American Numbering Plan
NANPNAT	North American Numbering Plan Network Address Translation
NAT Network Layer	Network Address Translation Layer 3 in the Open System Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.
Network Layer	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
Network Management	The functions related to the management of data across the network.
Network Management OSS	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.
NCS	Network Call Signaling
Nonce	A random value used only once which is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP)
NTP	Network Time Protocol, an internet standard used for synchronizing clocks of elements distributed on an IP network
NTSC	National Television Standards Committee which defines the analog color television, broadcast standard used today in North America.
Off-Net Call	A communication connecting a PacketCable subscriber out to a user on the PSTN
On-Net Call	A communication placed by one customer to another customer entirely on the PacketCable Network
One-way Hash	A hash function that has an insignificant number of collisions upon output.
OSP	Operator Service Provider
OSS-D	OSS Default – Network Provider Provisioning Server
OSS	Operations Systems Support. The back office software used for configuration, performance, fault, accounting and security management.
PAL	Phase Alternate Line – the European color television format which evolved from the American NTSC standard.

PDU	Protocol Data Unit
PKCS	Public Key Cryptography Standards, published by RSA Data Security Inc. Describes how to use public key cryptography in a reliable, secure and interoperable way.
PKI	Public Key Infrastructure - a process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
PKINIT	The extension to the Kerberos protocol that provides a method for using public key cryptography during initial authentication.
PHS	Payload Header Suppression, a DOCSIS technique for compressing the Ethernet, IP and UDP headers of RTP packets.
Plaintext	The original (unencrypted) state of a message or data.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to any one other then the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves.
PSC	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
PSFR	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
PSTN	Public Switched Telephone Network.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A users private key is kept secret and is the only key which can decrypt messages sent encrypted by the users public key.
PCM	Pulse Code Modulation – A commonly employed algorithm to digitize an analog signal (such as a human voice) into a digital bit stream using simple analog to digital conversion techniques.
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service, guarantees network bandwidth and availability for applications.
RADIUS	Remote Access Dial-In User Service, an internet protocol (RFC 2138 and RFC 2139) originally designed for allowing users dial-in access to the internet through remote servers. Its flexible design has allowed it to be extended well beyond its original intended use
RAS	Registration, Admissions and Status. RAS Channel is an unreliable channel

	used to convey the RAS messages and bandwidth changes between two H.323 entities.
RC4	A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in PacketCable.
RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
RKS	Record Keeping Server, the device which collects and correlates the various Event Messages
Root Private Key	The private signing key of the highest level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures that it generated with the corresponding root private key.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
RSVP	Resource reSerVation Protocol
RTCP	Real Time Control Protocol
RTO	Retransmission Timeout
RTP	Real Time Protocol, a protocol defined in RFC 1889 for encapsulating encoded voice and video streams.
S-MTA	Standalone MTA – a single node which contains an MTA and a non DOCSIS MAC (e.g. ethernet).
SA	Security Association - a one-way relationship between sender and receiver offering security services on the communication flow .
SAID	Security Association Identifier - uniquely identifies SAs in the BPI+ security protocol, part of the DOCSIS 1.1 specification.
SCCP	The Signaling Connection Control Part is a protocol within the SS7 suite of protocols that provides two functions in addition to those that are provided within MTP. The first is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	A Service Control Point is a Signaling Point within the SS7 network, identifiable by a Destination Point Code, that provides database services to the network.
SCTP	Simple Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information that is delivered as a unit between peer service access points.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.
Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.

SF	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
SFID	Service Flow ID, a 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. Any 32-bit SFID must not conflict with a zero-extended 14-bit SID. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). USFIDs and DSFIDs are allocated from the same SFID number space.
SFR	Service Flow Reference, a 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
SG	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1 - a one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed by using encryption.
SIP	Session Initiation Protocol is an application layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants.
SIP+	Session Initiation Protocol Plus is an extension to SIP.
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SPI	Security Parameters Index - a field in the IPSEC header that along with the destination IP address provides a unique number for each SA.
SS7	Signaling System Number 7. SS7 is an architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Signal Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
STP	Signal Transfer Point. An STP is a node within an SS7 network that routes signaling messages based on their destination address. It is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and source and destination UDP/TCP port.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.
Systems Management	Functions in the application layer related to the management of various open systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.
TCAP	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling

	Control Point.
TCP	Transmission Control Protocol
TD	Timeout for Disconnect
TFTP	Trivial File Transfer Protocol
TFTP-D	Default – Trivial File Transfer Protocol
TGS	Ticket Granting Server used to grant Kerberos tickets.
TGW	Telephony Gateway
TIPHON	Telecommunications & Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value tuple within a DOCSIS configuration file.
TN	Telephone Number
ToD	Time of Day Server
TOS	Type of Service. An 8-bit field of every IP version 4 packet. In a Diffserv domain, the TOS byte is treated as the Diffserv Code Point, or DSCP.
Transit Delays	The time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.
Trunk	An analog or digital connection from a circuit switch which carries user media content and may carry voice signaling (MF, R2, etc.).
TSG	Trunk Subgroup
Tunnel Mode	An IPSEC (ESP or AH) mode that is applied to an IP tunnel, where an outer IP packet header (of an intermediate destination) is added on top of the original, inner IP header. In this case, the ESP or AH transform treats the inner IP header as if it were part of the packet payload. When the packet reaches the intermediate destination, the tunnel terminates and both the outer IP packet header and the IPSEC ESP or AH transform are taken out.
UDP	User Datagram Protocol, a connectionless protocol built upon Internet Protocol (IP).
Upstream	The direction from the subscriber location toward the head-end.
VAD	Voice Activity Detection
VBR	Variable bit-rate
VoIP	Voice over IP
WBEM	Web-Based Enterprise Management (WBEM) is the umbrella under which the DMTF (Desktop Management Task Force) will fit its current and future specifications. The goal of the WBEM initiative is to further management standards using Internet technology in a manner that provides for interoperable management of the Enterprise. There is one DMTF standard today within WBEM and that is CIM (Common Information Model). WBEM compliance means adhering to the CIM. See www.dmtf.org
X.509 certificate	a public key certificate specification developed as part of the ITU-T X.500 standards directory

Appendix B. Revisions

Engineering Change Numbers

ECN	Date Ratified	Summary

Appendix C. References and Bibliography

[1]. *Cable Modem to Customer Premises Equipment Interface (CMCI) Specification*, P-CMCI-I03-991115, Cable Television Laboratories, Inc., November 15, 1999, http://www.CableLabs.com/

[2]. *Cable Modem Termination System - Network Side Interface Specification*, Cable Television Laboratories, Inc., July 22, 1996, http://www.CableLabs.com/.

[3]. *PacketCable Product Specification*, Cable Television Laboratories Inc., November 25, 1998.

[4]. *PacketCable Network-Based Call Signaling Protocol Specification*, PKT-SP-EC-MGCP-I02-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[5]. *PacketCable Security Specification*, PKT-SP-SEC-I01-991201, Cable Television Laboratories, Inc., December 1, 1999, http://www.PacketCable.com./

[6]. *PacketCable 1.0 Architecture Framework Technical Report*, PKT-TR-ARCH-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./.

[7]. *Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification*, SP-RFIv1.1-I03-991105, Cable Television Laboratories, Inc., November 05, 1999. http://www.CableLabs.com/

[8]. *PacketCable Dynamic Quality of Service Specification*, PKT-SP-DQOS-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[9]. PacketCable Event Messages White Paper, PKT-OSS-TD01-990329.

[10]. C. Rigney, A. Rubens, W. Simpson, S. Willens, “Remote Authentication Dial In User Service (RADIUS)”, IETF RFC-2138, April 1997

[11]. C. Rigney, “RADIUS Accounting”, IETF RFC-2139, April 1997

[12]. PacketCable Architecture Call Flow Technical Report, On-Net MTA to On-Net MTA, PKT-TR-CF-ON-ON-D01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[13]. PacketCable Architecture Call Flow Technical Report, On-Net MTA to PSTN, PKT-TR-CF-ON-PSTN-D01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com/

[14]. PacketCable Architecture Call Flow Technical Report, PSTN to On-Net MTA, PKT-TR-CF-PSTN-ON-D01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com/

[15]. Telcordia GR-1100-CORE Bellcore Automatic Message Accounting Format (BAF)Requirements

Appendix D. Acknowledgements

The PacketCable project would like to thank and formally acknowledge the significant contributions of the OSS Billing Team group who helped formulate the initial draft of this document. Those contributors include the following individuals and companies:

Donna Fryer, Anurag Goel, Jim Harbison, Mike Heffner, Mark Jones, Keith Kelly, Wes Porter, Robert Sayko, Esfira Slutsman, Bill Willcox, Jim Wilburn, Jian Zhang.

AP Engines, AT&T, Bridgewater, CSG, DSTI (formerly CableData), ipVerse, NetSpeak, Portal, Telcordia Technologies, Telesciences, and Telogy/Xybridges.

Without their tireless efforts to bring the basic idea of an event-based usage collection scheme from concept to fruition, this document detailing the results of their effort would have never been possible.

Maria Stachelek, CableLabs