PacketCable™ Event Messages Specification

PKT-SP-EM-I05-021127

ISSUED

Notice

Document Status Sheet

Document Control Number:	PKT-SP-EM-I05-021127			
Document Title:	PacketCable™ Event Messages Specification			
Revision History:	I01 – First issued release 12/01/99 I02 – Second issued release 11/28/00 I03 – Third issued release 12/21/01 I04 – Fourth issued release 10/18/02 I05 – Fifth issued release 11/27/02			
Date:	November 27, 2002			
Status:	~~Work in Progress~~	~~Draft~~	Issued	~~Closed~~
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.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Contents

List of Figures

List of Tables

This page left blank intentionally.

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 advanced communications services using packetized data transmission technology over the cable television hybrid fiber coax (HFC) infrastructure running the Data Over Cable Service Interface Specifications (DOCSIS) protocol. PacketCable specifies a network infrastructure that overlays the existing two-way cable television broadband cable access network.

While PacketCable is initially focused on packet voice over cable, it 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

This specification describes the concept of Event Messages used to collect usage for the purposes of billing within the PacketCable™ architecture. It details a transport protocol independent Event Message attribute TLV format, an Event Message file format, mandatory and optional transport protocols, 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. In order to support vendor interoperability, implementations must minimally support RADIUS as a transport protocol. It is issued to facilitate design and field-testing leading to manufacturability and interoperability of conforming hardware and software by multiple vendors.

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 Server (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.

The PacketCable Event Message specification defines a transport protocol independent Event Message attribute Type-Length-Value (TLV) format, an Event Message file format, as well as the mandatory RADIUS protocol and the optional FTP transport protocol.

1.3 PacketCable Reference Architecture

Figure 1 shows the reference architecture for the PacketCable Network. Refer to the PacketCable Architecture Document [12] for more detailed information on this reference architecture.

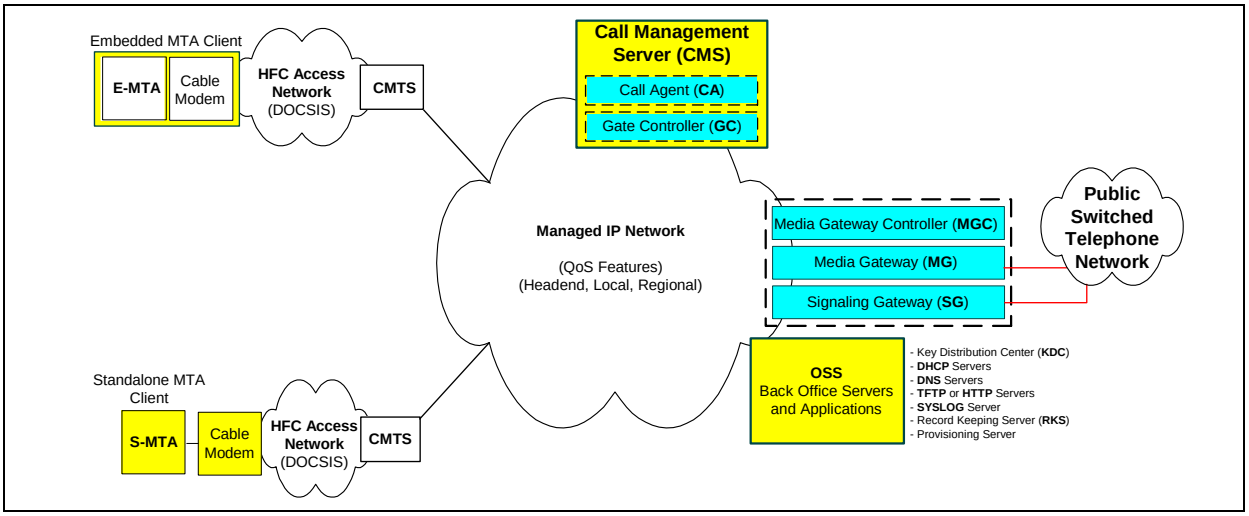

Figure 1. PacketCable Network Component Reference Mode

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.

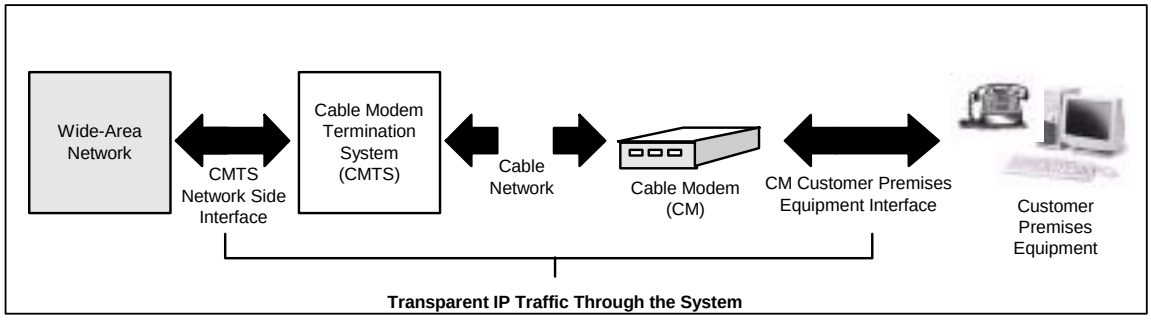

Figure 2. Transparent IP Traffic through the Data-Over-Cable System

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 [11]. At customer locations, the interface is called the cable-modem-to-customer-premises-equipment interface (CMCI) and is specified in [10]. 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 MSOs 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.x 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 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 5 motivates the need for Event Messages. Section 6 describes objectives of the Event Message architecture followed by Section 7 describing the Event Message architecture itself. Section 8 describes the services PacketCable 1.0 will support for which Event Messages need to be generated. Section 9 defines the Event Messages needed in order to bill these supported services. Section 10 defines the PacketCable Event Message attributes. Section 11 describes the transport independent Event Message attribute TLV format. Section 12 describes the Event Message file format. Finally, Section 13 describes the mandatory and optional transport protocols.

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 explanatory.

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 specification 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 will be evident from this document that while a Packet-Cable 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. These differences may be significant for legal/regulatory purposes.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

[1] PacketCable Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I06-021127, November 27, 2002, Cable Television Laboratories, Inc., http://www.PacketCable.com

[2] PacketCable Security Specification, PKT-SP-SEC-I07-021127, November27, 2002, Cable Television Laboratories, Inc., http://www.PacketCable.com

[3] PacketCable Dynamic Quality of Service Specification, PKT-SP-DQOS-I05-021127, November 27, 2002, Cable Television Laboratories, Inc., http://www.PacketCable.com

[4] IETF RFC-2865, June 2000, C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)"

[5] IETF RFC-2866, June 2000, C. Rigney, "RADIUS Accounting"

[6] Telcordia GR-1100-CORE Bellcore Automatic Message Accounting Format (BAF) Requirements Terms and Definitions

[7] PacketCable CMS to CMS Signaling Specification, PKT-SP-CMSS-I01-001128, November 28, 2000, Cable Television Laboratories, Inc., http://www.PacketCable.com

[8] PacketCable Electronic Surveillance Specification, PKT-SP-ESP-I01-991230, December 30, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com

[9] International Telecommunication Union (ITU), The International Public Telecommunication Numbering Plan, E.164 ITU-T, May 1997

2.2 Informative References

[10] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premises Equipment Interface (CMCI) Specification, SP-CMCI-I08-0-20830, August 29, 2001, Cable Television Laboratories, Inc., http://www.cablemodem.com

[11] Data-Over-Cable Service Interface Specifications, Cable Modem Termination System - Network Side Interface Specification, SP-CMTS-NSI-I01-960702, July 2, 1996, Cable Television Laboratories, Inc., http://www.CableLabs.com

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

[13] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFIv1.1-I09-020830, August 30, 2002, Cable Television Laboratories, Inc., http://www.CableLabs.com

[14] PacketCable Architecture Call Flow Technical Report, On-Net MTA to On-Net MTA, PKT-TR-CF-ON-ON-V01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com

[15] PacketCable Architecture Call Flow Technical Report, On-Net MTA to PSTN, PKT-TR-CF-ON-PSTN-V01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com

[16] PacketCable Architecture Call Flow Technical Report, PSTN to On-Net MTA, PKT-TR-CF-PSTN-ON-V01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com

[17] PacketCable Line Control Signaling System Architecture Technical Report, PKT-TR-ARCH-LCS-V01-010730, July 30, 2001, Cable Television Laboratories, Inc., http://www.packetcable.com

[18] GR-1298-CORE, AINGR: Switching Systems (GR-1298)

[19] GR-1299-CORE, AINGR: Switch - Service Control Point (SCP)/Adjunct Interface (GR-1299)

[20] GR-533-CORE, LSSGR: Database Services Service Switching Points - Toll-Free Service (FSD 31-01-0000), A Module of LSSGR, FR-64 (GR-533), Telcordia

[21] GR-2892-CORE, Switching and Signaling Generic Requirements for Toll-Free Service Using AIN (GR-2892), Telcordia

[22] TRQ No. 2, Technical Requirements Number 2, Number Portability Switching Systems (ANSI T1S1.6 Working Group)

3 TERMS AND DEFINITIONS

PacketCable specifications use the following terms:

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.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access."
Asymmetric Key	An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct.
Audio Server	An Audio Server plays informational announcements in PacketCable network. Media announcements are needed for communications that do not complete and to provide enhanced information services to the user. The component parts of Audio Server services are Media Players and Media Player Controllers.
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 that claims to have given the information.
Authorization	The act of giving access to a service or device if one has permission to have the access.
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.
Cleartext	The original (unencrypted) state of a message or data. Also called plaintext.
Confidentiality	A way to ensure that information is not disclosed to anyone other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
Cryptanalysis	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.
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.
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.
Downstream	The direction from the head-end toward the subscriber location.
Encipherment	A method used to translate plaintext into ciphertext.
Encryption	A method used to translate plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or Multipoint Conference Unit.
Errored Second	Any 1-second interval containing at least one bit error.
Event Message	A message capturing a single portion of a connection.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
Flow [DOCSIS Flow]	A unidirectional sequence of packets associated with a Service ID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow. Also known as a DOCSIS-QoS "service flow"
Flow [IP Flow]	A unidirectional sequence of packets identified by OSI 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.
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 to the edge of the PacketCable network.
H.323	An ITU-T recommendation for transmitting and controlling audio and video information. The H.323 recommendation requires the use of the ITU-T H.225 and ITU-T 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.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access and Transport Area.
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.
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.

Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
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.
Nonce	A random value used only once that 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.
Off-Net Call	A communication connecting a PacketCable subscriber to a user on the PSTN.
One-way Hash	A hash function that has an insignificant number of collisions upon output.
On-Net Call	A communication placed by one customer to another customer entirely on the PacketCable Network.
Plaintext	The original (unencrypted) state of a message or data. Also called cleartext.
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, thereby eliminating the need for a host to support the service.
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 an 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 user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.

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 generated with the corresponding root private key.
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.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed using encryption.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and single 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.
Transit Delays	The time difference between the instant at which the first bit of a Protocol Data Unit (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 that carries user media content and may carry voice signaling (M_F, R_2, etc.).
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.
Upstream	The direction from the subscriber location toward the headend.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.

4 ABBREVIATIONS

PacketCable specifications use the following abbreviations.

AAA	Authentication, Authorization and Accounting.
AES	Advanced Encryption Standard. A block cipher, used to encrypt the media traffic in PacketCable.
AF	Assured Forwarding. This is a DiffServ Per Hop Behavior.
AH	Authentication header. An IPSec security protocol that provides message integrity for complete IP packets, including the IP header.
AMA	Automated Message Accounting. A standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies).
ASD	Application-Specific Data. A field in some Kerberos key management messages that carries information specific to the security protocol for which the keys are being negotiated.
AT	Access Tandem.
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
BAF	Bellcore AMA Format, also known as AMA.
BCID	Billing Correlation ID.
BPI+	Baseline Privacy Plus Interface Specification. The security portion of the DOCSIS 1.1 standard that runs on the MAC layer.
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. The part of the CMS that maintains the communication state, and controls the line side of the communication.
CBC	Cipher Block Chaining Bode. 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.
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.
CIR	Committed Information Rate.
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. This is one example of an Application Server.

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.
CMSS	CMS-to-CMS Signaling.
Codec	COder-DECoder.
COPS	Common Open Policy Service protocol. 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 configuration file.
CSR	Customer Service Representative.
DA	Directory Assistance.
DE	Default. This is a DiffServ Per Hop Behavior.
DES	Data Encryption Standard.
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default. Network Provider DHCP Server.
DNS	Domain Name Service.
DOCSIS™	Data-Over-Cable Service Interface Specifications.
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. Assigned on the fly for each communication depending on the QoS requested.
DSCP	DiffServ Code Point. A field in every IP packet that 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.
DSFID	Downstream Service Flow ID. See SFID.
DTMF	Dual-tone Multi Frequency (tones).
EF	Expedited Forwarding. A DiffServ Per Hop Behavior.
E-MTA	Embedded MTA. A single node that contains both an MTA and a cable modem.
EO	End Office.
ESP	IPSec Encapsulating Security Payload. Protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute.
FEID	Financial Entity ID.
FGD	Feature Group D signaling.
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 821 for details.
GC	Gate Controller.
GTT	Global Title Translation.
HFC	Hybrid Fiber/Coax coaxial cable. An 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.
HMAC	Hashed Message Authentication Code. A message authentication algorithm based on either SHA-1 or MD5 hash and defined in IETF RFC 2104.
HTTP	Hypertext 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 on the Internet. See www.ietf.org for details.
IKE	Internet Key Exchange. 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 with X.509 certificates for authentication.
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.
ISTP	Internet Signaling Transport Protocol.
ISUP	ISDN User Part. A protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ITU	International Telecommunications Union.
ITU-T	International Telecommunications Union–Telecommunications Standardization Sector
IVR	Interactive Voice Response system.
KDC	Key Distribution Center.
LATA	Local Access and Transport Area.
LD	Long Distance.
LIDB	Line Information Database. Contains customer information required for real-time access such as calling card personal identification numbers (PINs) for real-time validation.
LLC	Logical Link Control. 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.
lsb	Least significant bi.t
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.
MCU	Multipoint Conferencing Unit.
MD5	Message Digest 5. A one-way hash algorithm that maps variable length plaintext into fixed-length (16 byte) ciphertext.
MDCP	Media Device Control Protocol. 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	Media Gateway. Provides the bearer circuit interfaces to the PSTN and transcodes the media stream.

MGC	Media Gateway Controller. The overall controller function of the PSTN gateway. Receives, controls and mediates call-signaling information between the PacketCable and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF 2705.
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 Message Authentication Code (MAC).
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSB	Most Significant Bit
MSO	Multi-System Operator. A cable company that operates many head-end locations in several cities.
MSU	Message Signal Uni.
MTA	Multimedia 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. A set of two protocols (MTP 2 and 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. This layer provides services to establish a path between open systems.
NCS	Network Call Signaling.
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 numbers (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. Defines the analog color television broadcast standard used today in North America.
OID	Object Identifier.
OSP	Operator Service Provider.
OSS	Operations Systems Support. The back-office software used for configuration, performance, fault, accounting, and security management.
OSS-D	OSS Default. Network Provider Provisioning Server.
PAL	Phase Alternate Line. The European color television format that evolved from the American NTSC standard.
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.

PDU	Protocol Data Unit.
PHB	Per-Hop Behavior.
PHS	Payload Header Suppression. A DOCSIS technique for compressing the Ethernet, IP, and UDP headers of RTP packets.
PKCROSS	Public-Key Cryptography for Cross-Realm Authentication. Utilizes PKINIT for establishing the inter-realm keys and associated inter-realm policies to be applied in issuing cross-realm service tickets between realms and domains in support of Intradomain and Interdomain CMS-to-CMS signaling (CMSS).
PKCS	Public-Key Cryptography Standards. Published by RSA Data Security Inc. These Standards describe 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	Public-Key Cryptography for Initial Authentication. The extension to the Kerberos protocol that provides a method for using public-key cryptography during initial authentication.
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.
QCIF	Quarter Common Intermediate Format.
QoS	Quality of Service. Guarantees network bandwidth and availability for applications.
RADIUS	Remote Authentication Dial-In User Service. An internet protocol (IETF 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	Rivest Cipher 4. A variable length stream cipher. Optionally 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	Registered Jack-11. A standard 4-pin modular connector commonly used in the United States for connecting a phone unit into a wall jack.
RKS	Record Keeping Server. The device, which collects and correlates the various Event Messages.
RSA	A public-key, or asymmetric, cryptographic algorithm used to provide authentication and encryption services. RSA stands for the three inventors of the algorithm; Rivest, Shamir, Adleman.
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 Transport Protocol. A protocol for encapsulating encoded voice and video streams. Refer to IETF RFC 1889.
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 DOCSIS Baseline Privacy Plus Interface (BPI+) security protocol.
SCCP	Signaling Connection Control Part. A protocol within the SS7 suite of protocols that provides two functions in addition to those provided within MTP. The first function is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	Service Control Point. A Signaling Point within the SS7 network, identifiable by a Destination Point Code that provides database services to the network.
SCTP	Stream Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information delivered as a unit between peer service access points.
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 variant 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.
SIP	Session Initiation Protocol. An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
SIP+	Session Initiation Protocol Plus. An extension to SIP.
S-MTA	Standalone MTA. A single node that contains an MTA and a non-DOCSIS MAC (e.g., ethernet).
SNMP	Simple Network Management Protocol.
SOHO	Small Office/Home Office.
SS7	Signaling System number 7. An architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Service 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. A node within an SS7 network that routes signaling messages based on their destination address. This is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.

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. A sub-system of the KDC used to grant Kerberos tickets.
TGW	Telephony Gateway.
TIPHON	Telecommunications and Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value. A 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.
TSG	Trunk Subgroup.
USFID	Upstream Service Flow ID. See SFID.
UDP	User Datagram Protocol. A connectionless protocol built upon Internet Protocol (IP).
VAD	Voice Activity Detection.
VBR	Variable Bit Rate.
VoIP	Voice-over-IP.

5 BACKGROUND

5.1 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.

5.2 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 the transport protocols.

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.

5.3 Originating/Terminating Call Model to Support Customer Billing and Settlements

The PacketCable Event Messages contain sufficient per-call information to support customer billing for service as well as settlement between PacketCable network providers for access. The information contained in the Event Messages supports a wide variety of billing and settlement models. PacketCable does not mandate the use of specific billing or settlement models as these models are defined by and based on the specific business requirements of the individual MSOs. PacketCable neither mandates nor precludes the use of a clearinghouse for settlements.

The PacketCable Event Messages are based on a model where a call or service is divided into an originating half and a terminating half. The originating CMS or MGC must generate a unique Billing Correlation ID (BCID) to identify all Event Messages associated with the originating half of the call. The terminating CMS or MGC must generate a unique BCID to identify all Event messages associated with the terminating half of the call. For each half of the call or service, the set of PacketCable network elements that generate Event Messages (CMS, MGC, CMTS) must provide all necessary information required for billing and/or settlements as appropriate based on the service. The information generated by the originating half must be sent to the RKS supporting the originating half. The information generated by the terminating half must be sent to the RKS supporting the terminating half.

The PacketCable Event Messages support billing and settlement for single-zone, intra-domain and inter-domain architectures. In most cases, the basic set of Event Messages, their associated attributes, and the triggers for the Event Message are identical for these three architectures. In the case of intra-domain and inter-domain architectures, additional triggers exist for a subset of the Event Messages. The PacketCable Event Message specification details these requirements.

For the purposes of settlements, each PacketCable zone is divided into one or more logical Financial Entities. Settlements occur between Financial Entities. Each Financial Entity is identified by a Financial Entity ID (FEID). FEIDs are pre-assigned to every CMS and MGC in the PacketCable network. A single CMS may be assigned at most one FEID. One or more CMSes may be assigned the same FEID.

In the Intra-domain and Inter-domain cases, the originating and terminating CMSes exchange BCIDs and FEIDs. The originating CMS sends its BCID and FEID in the INVITE message. The terminating CMS sends its BCID and FEID in the first response to the INVITE message which is typically the 183 SDP.

5.4 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.

5.5 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.

5.6 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 .

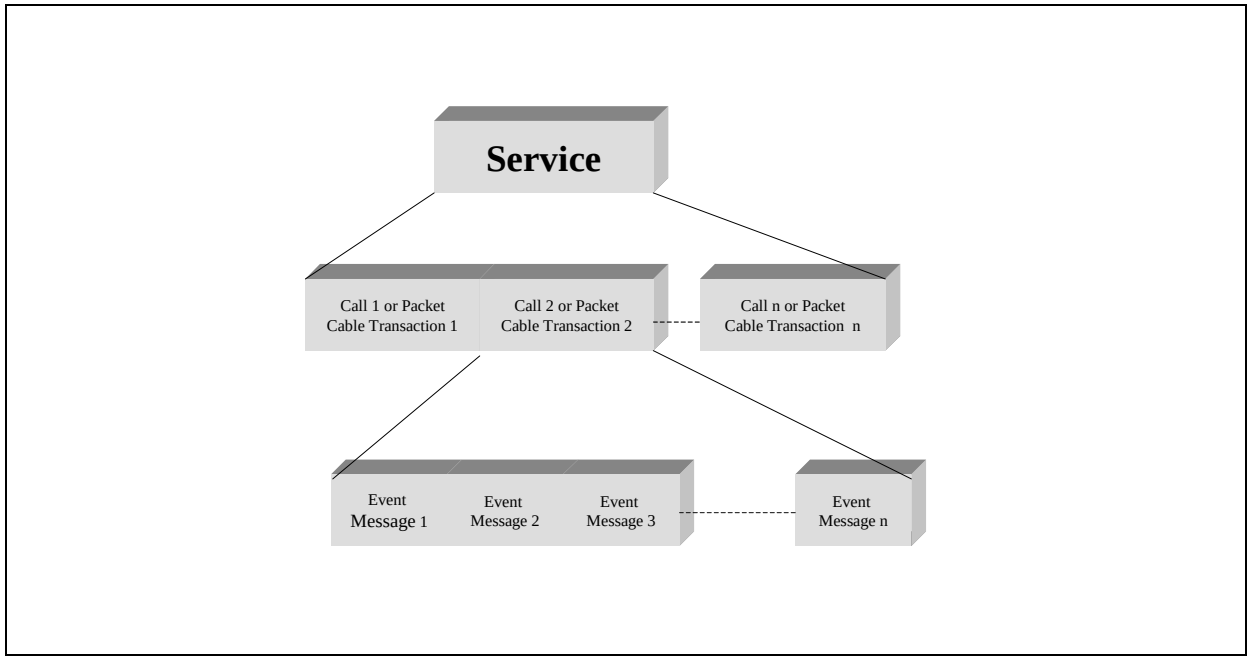

Figure 3. PacketCable Terminology

5.6.1 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.

5.6.2 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 BCID (as described in Table 35). 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.

5.6.3 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.

5.6.4 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.

5.6.5 Attribute

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

5.7 Supporting Documentation

A number of documents and specifications describe the PacketCable project. The PacketCable Architecture Framework [12] 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 http://www.packetcable.com.

6 PACKETCABLE OBJECTIVES

6.1 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 8 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)

6.2 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. These services are not defined in more detail 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.)

6.3 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 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:

  a) Element Type, identifying the element as a CMTS, CMS, or MGC

  b) Element ID

  c) 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:

     1) be 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.

  d) Number of days to keep Event Messages for short-term storage

  e) Others

- Enable or disable Media_Alive Event Message, configure the frequency of Media_Alive message (suggested 0 to 1440 minutes, with 0 being no Media_Alive Events).
- PacketCable Event Messages generation is not required to support subscriber billing for services provided by the PacketCable Line Control Signaling (LCS) System. In the LCS system, the Local Digital Switch (LDS) is responsible for subscriber billing. PacketCable Event Message generation by the LCS system to support uses other than subscriber billing is out of scope at this time. For a description of call control in the LCS sub-system, please refer to the PacketCable Line Control Signaling System Architecture Technical Report [17].

7 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.

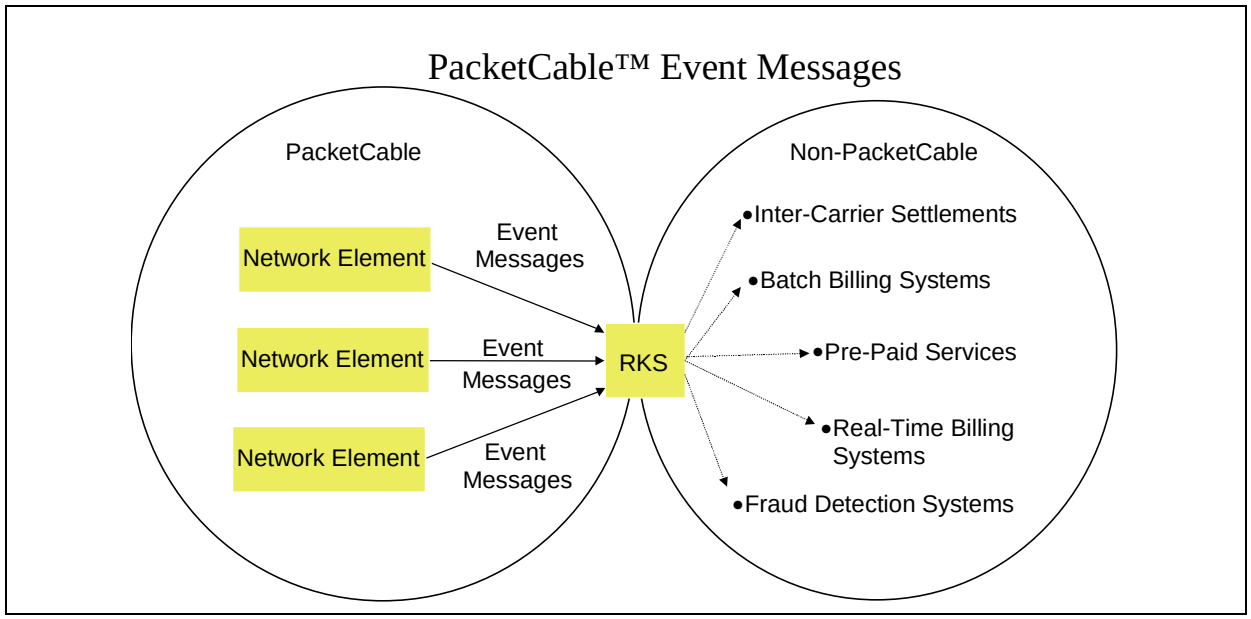

Figure 4. Representative PacketCable Event Messages Architecture

7.1 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 BCID, which can be leveraged for reconciliation and non-repudiation purposes.

7.2 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 [12] 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.

7.2.1 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 BCID on receipt of an NCS-signaling NTFY message from an MTA.

The CMS MUST send the BCID and other data as defined in Table 1 to the CMTS via the DQoS GateSet message as specified in the DQoS specification [3].

Table 1. PacketCable Event Reporting Common Elements

BCID (see Table 33)
IP address and port number of the primary RKS
IP address and port number of the secondary RKS
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.

7.2.2 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 BCID 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.

7.2.3 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. QoS event messages are generated individually for both upstream and downstream bandwidth.

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

7.2.4 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 5 gives a representative RKS deployment for information only and does not imply an implementation requirement.

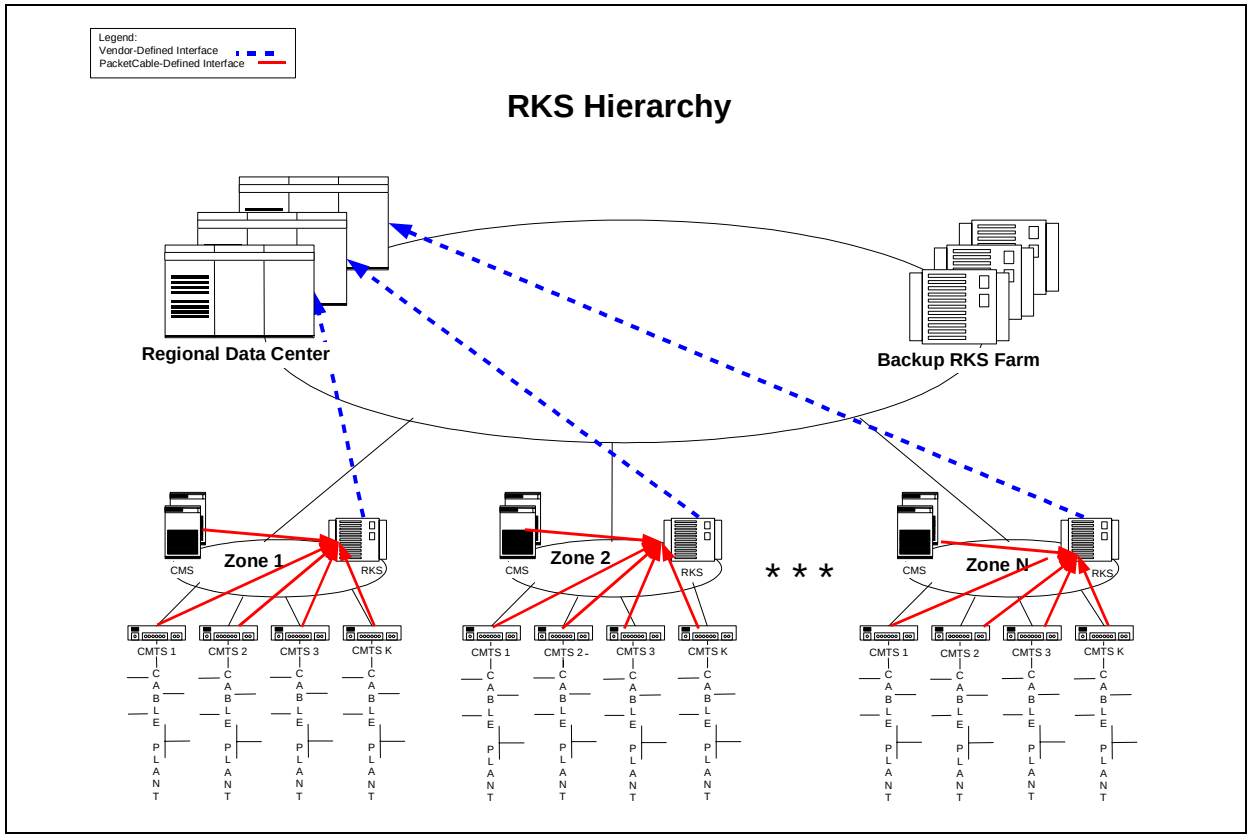

Figure 5. Example RKS Architecture

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 9. 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 [2].
- 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.

7.3 General PacketCable Network Element Requirements

This section lists requirements placed on the PacketCable network elements:

The CMS, CMTS, and MGC MUST create a security relationship with each RKS that these network elements will send Event Messages as defined in the PacketCable Security Specification [2].

The CMS MUST support multiple sets of primary and secondary RKSes, 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 BCID, identify the primary and secondary RKS and determine whether the Event Messages are to be delivered in real time or 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 Network Time Protocol (NTP) time synchronization.
- The PacketCable network elements MUST support transport to a primary RKS and failover to a secondary RKS when communication with the primary RKS fails for any reason (including situations where the primary RKS becomes inoperable).
- PacketCable network elements MUST support the transport of a single Event Message as well as a batch of Event Messages (batch mode = multiple Event Message per single Radium message).
- Each trusted PacketCable network element that generates an Event Message MUST identify itself with a static, unique element ID.

7.4 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.

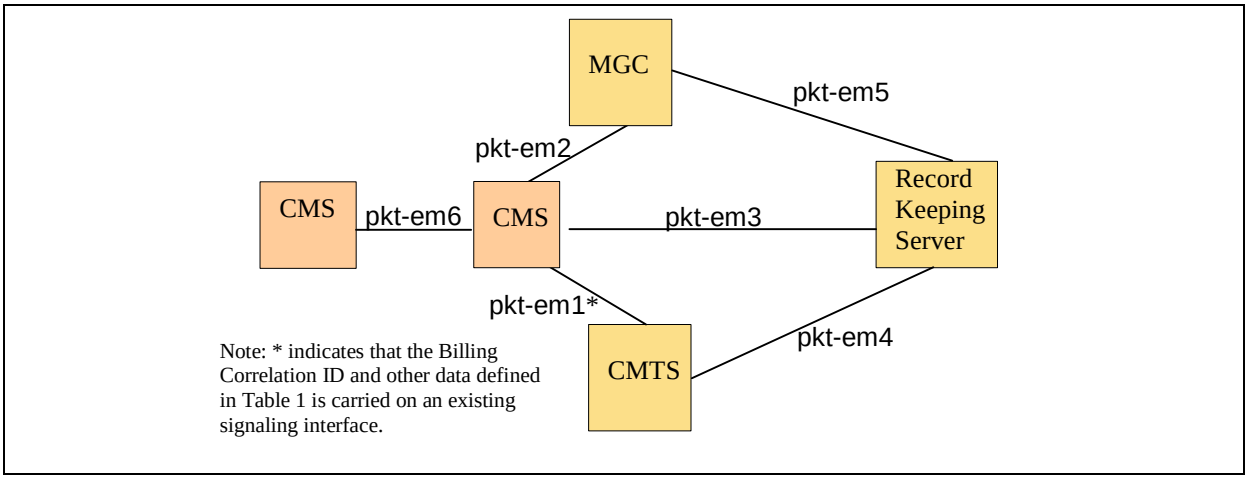

Figure 6. Event Message Billing Interfaces

7.4.1 CMS to CMTS (pkt-em1*)

The CMS to CMTS interface is defined by the PacketCable DQoS protocol [3].

The CMS sends the BCID and other data as defined in Table 1 to the CMTS via the DQoS GateSet message as specified in the DQoS specification [3].

7.4.2 CMS to MGC (pkt-em2)

The CMS to MGC interface is defined by the PacketCable CMSS specification [7]. The CMS and MGC exchange originating/terminating information such as BCID, FEID, etc. across this interface as defined in [7].

7.4.3 CMS to RKS (pkt-em3)

The CMS to RKS interface is defined by the PacketCable security specification [2] and also by the Event Message transport and syntax rules defined in this document.

7.4.4 CMTS to RKS (pkt-em4)

The CMTS to RKS interface is defined by the PacketCable security specification [2] and by the Event Message transport and syntax rules defined in this document.

7.4.5 MGC to RKS (pkt-em5)

The MGC to RKS interface is defined by the PacketCable security specification [2] and by the Event Message transport and syntax rules defined in this document.

7.4.6 CMS to CMS (pkt-em6)

The CMS to CMS interface is defined by the PacketCable CMSS specification [7]. The originating CMS and terminating CMS exchange originating/terminating information such as BCID, FEID, etc., across this interface as defined in [7].

7.4.7 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, CMTS, and MGC that will send Event Messages to any of those RKSes. The Event Messages are sent from the CMS, CMTS, and MGC to the RKS using one of the supported transport mechanisms, each of which it must be possible to secure with IPSec. Refer to the PacketCable Security Specification [2] for a detailed description of the security requirements for the PacketCable Event Message interfaces.

8 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 [14], [15], [16], 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.

8.1 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 along with the basic call, then refer to Section 8.2 for a list of additional Event Messages for these specific services.

8.1.1 On-Net to On-Net Call Configuration

A single-zone On-Net to On-Net call is within a single MSO's network, using two 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 two different CMTSes.

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

Both intra-domain and inter-domain On-Net to On-Net call configurations use two different MTAs that are both connected to two different CMSes.

For any On-Net to On-Net call configuration, the originating half and the terminating half of the call MUST each generate a complete set of Event Messages.

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

Event Message	Required or Optional	Comments
Database_Query	O	If LNP is required
Signaling_Start	R	CMS is starting signaling to support a call start
QoS_Reserve	R	CMTS is reserving QoS
QoS_Commit	R	CMTS is committing QoS
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.*
Call_Answer	R	Indicates start of media stream
Call_Disconnect	R	Indicates termination of media steam
QoS_Release	R	CMTS is releasing QoS
Signaling_Stop	R	Signaling for the service is complete

8.1.2 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 [15] for a complete description of this call configuration including an example call flow showing the triggers for these Event Messages.

For any On-Net to Off-Net call configuration, the originating half and the terminating half of the call MUST each generate a complete set of Event Messages.

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

Event Message	Required or Optional	Comments
Database_Query	O	If LNP is Required
Signaling_Start	R	Starting signaling to support a call start
QoS_Reserve	R	CMTS reserves QoS
QoS_Commit	R	CMTS commits QoS
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
Call_Answer	R	Indicates start of media stream
Call_Disconnect	R	Indicates termination of media steam
Interconnect_Stop	R	For call tear-down
QoS_Release	R	CMTS releases bandwidth
Signaling_Stop	R	Indicates end of signaling

8.1.3 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 [16] for a complete description of this call configuration including an example call flow showing the triggers for these Event Messages.

For any Off-Net to On-Net call configuration, the originating half and the terminating half of the call MUST each generate a complete set of Event Messages.

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

Event Message	Required or Optional	Comments
Signaling_Start	R	Starting signaling to service a request to start a call
Interconnect_Start	R	For call setup
QoS_Reserve	R	CMTS reserves bandwidth
QoS_Commit	R	CMTS commits bandwidth
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.*
Call_Answer	R	Indicates start of media stream
Call_Disconnect	R	Indicates termination of media steam
Interconnect_Stop	R	For call tear-down
QoS_Release	R	CMTS releases bandwidth.
Signaling_Stop	R	Indicates end of signaling

8.2 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 8.1.

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.

8.2.1 911 Service

A 911 call follows the standard On-Net to Off-Net Event Message flow described above in Section 8.1.2.
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 8.1.2.

8.2.2 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.

8.2.3 Toll-Free Services

Toll-Free Services follow the standard On-Net to Off-Net Event Message flow described above in Section 8.1.2. 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 in Section 8.2.1 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

8.2.4 Operator Services

Operator Services follow the standard On-Net to Off-Net Event Message configuration described above in Section 8.1.2. There are no new additional Event Messages beyond those already described for the On-Net to Off-Net calls in that section. The CMS sends 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 just dials "0."

The CMS generates 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 replaces the "0" in the Called Number field with the number of the Operator Service Provider (OSP). These parameters are 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 encompasses only 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.

8.2.5 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 BCID 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.*

8.2.6 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 two 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 generate a complete set of Event Messages on their own as detailed in Sections 8.1.2 and 8.1.3, 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 are 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

8.2.7 Call Forwarding Service

Call Forwarding Service applies only to calls terminating On-Net as described in Sections 8.1.1 and 8.1.3.

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 initiates 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 are generated for the fact that a Call Forwarding instance was initiated. The BCID for this leg is different than the first call. The rationale for using the Related BCID 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 subscriber's monthly statement in order to make it clear the reason those calls were placed. For all purposes the original call and the forwarded call are two different billable calls.

Table 8. Call Forwarding Service

Event Message	Required or Optional	Comments
Service_Instance	R	None

8.2.8 Return Call Service

This service applies only to calls originating On-Net, described in Sections 8.1.1 and 8.1.2. The CMS MUST keep a register with the Calling Party Number of the last call.

Return Call Service returns the last call that was made to an MTA. Upon instantiation of Return Call feature, the CMS initiates another call with the Calling Party Number of the last call, retrieved from the register just described, as the Dialed number. Event Messages are generated for the fact that the Return Call feature was initiated, using the BCID 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 cannot 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 cannot be activated is On-Net. *NOTE: This Event Message will be defined in a future release of this PacketCable specification*

8.2.9 Repeat Call Service

Repeat Call Service applies only to calls terminating On-Net as described in Sections 8.1.1 and 8.1.3.

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 the United States of America) 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 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.

8.2.10 Voice Mail Service

Voice Mail Service only applies to calls terminating On-Net, described in Sections 8.1.1 and 8.1.3.

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 are treated as separate transactions that have associated Event Messages. Event Messages for voice mail deposit 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).

8.2.11 Message Waiting Indicator Service

It is assumed that an Off-Net voicemail system is used as described in Section 8.2.10. 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 is not based on any per use delivery of the stutter tone, there are no Event Messages required for this service. Billing is based on a combination of information obtained from the Voicemail send/retrieve Event Messages discussed in Section 8.2.10 and provisioning information indicating when a subscriber has signed up for voicemail services.

9 PACKETCABLE EVENT MESSAGE STRUCTURE

This section describes the various Event Messages, together with their associated list of attributes. Refer to Section 10 for a detailed description of the attributes described in this section. Refer to Section 8 for a detailed description of the services and their associated Event Messages.

The following tables show the 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 provides 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_Reserve	Reservation of QoS for originating or terminating part of the call
8	QoS_Release	Release 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

Event Message ID	PacketCable Event Message	Description
		been allocated for originating or terminating part of the call
16	Call_Disconnect	Indicates that all network resources for have been released for originating or terminating part of the call
17	Time_Change	Indicates time change on a network element
19	QoS_Commit	Commitment of QoS for originating or terminating part of the call
20	Media_Alive	Indicates if the call is still active

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**	**20**
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	
Call Waiting	X	X		X	X	X	X	X	X	X					X	X		X	
Call Forwarding	X	X		X	X	X	X	X	X	X					X	X		X	
Return Call	X	X		X	X	X	X	X							X	X		X	
Repeat Call	X	X		X	X	X	X	X							X	X		X	
Voice Mail	X	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**	**20**
Basic	X	X	X	X	X		X	X			UNDEFINED	UNDEFINED	X	X	X	X		X	X
Call Block	X	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		X	
Return Call	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		X	
911	X	X	X	X	X		X	X					X	X	X	X		X	
N11	X	X	X	X	X		X	X					X	X	X	X		X	
Toll-Free	X	X	X	X	X		X	X					X	X	X	X		X	
Operator	X	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	20
Basic	X	X	X	X	X		X	X			UNDEFINED	UNDEFINED	X	X	X	X		X	X
Call Block	X	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		X	
Repeat Call	X	X		X	X	X	X	X					X	X	X	X		X	
Call Forwarding	X	X		X	X	X	X	X	X	X					X	X		X	
Voice Mail	X	X		X	X		X	X					X	X	X	X		X	

9.1 Event Message Structure

An Event Message contains a header followed by attributes. The header is required on every Event Message. The attributes vary based on the type of service the Event Message is describing. Refer to Table 32 for a description of the Event Message Header.

9.2 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

9.3 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 BCID 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
Calling_Party_Number	R	
Charge_Number	R	
Forwarded_Number	O	2 = Required

9.4 Signaling_Start

This Event Message indicates the time at which signaling starts.

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. In the event that a database dip is required, then the Signaling_Start message MUST be generated after the response from the database dip.

Originating CMS

In all scenarios, the originating 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.

Terminating CMS

In the single-zone scenario, the terminating CMS MUST timestamp this Event Message based on a vendor-proprietary trigger.

In the intra-domain and inter-domain scenarios, the terminating CMS MUST timestamp this Event Message immediately upon receipt of an INVITE message with a routable set of dialed digits.

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

Originating MGC (off-on)

The originating MGC MUST timestamp this message immediately upon receipt of an SS7 IAM message or a TGCP NTFY with digits (operator services).

Terminating MGC (on-off)

The terminating MGC MUST timestamp this message immediately upon receipt of an INVITE message with a routable set of dialed digits. If the MGC is integrated with the CMS, the terminating MGC MUST timestamp this message based on vendor proprietary trigger. The proprietary trigger MAY be based on when the IAM is transmitted. The Trunk_Number in the Trunk_Group_ID attribute in this message is the trunk group number used to formulate the first IAM transmitted to the Signaling Gateway that communicates with PSTN SS7 network for this call. It is referenced to the first IAM because potentially due to reattempt handling another IAM may be attempted to complete the same call.

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	If the originating CMS generates this message, this attribute MUST contain the endpoint name of the originating MTA. If the terminating CMS generates this message, this attribute MUST contain the endpoint name of the terminating MTA. If the originating MGC generates this message, this attribute MAY contain the endpoint ID of the originating MG. If the terminating MGC generates this message, this attribute MAY contain the endpoint ID of the terminating MG.
Calling_Party_Number	R	none
Called_Party_Number	R	terminating address (E.164 [9] format)
Routing_Number	R	routable number
Location_Routing_Number	O	This attribute MUST be included for local number portability use.
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.
Intl_Code	O	This attribute MUST be included for call origination of an internationally routed call.
Dial_Around_Code	O	This attribute MUST be included for call origination where the inter-exchange carrier was specified by keying in a dial-around code (e.g., 1010288).

9.5 Signaling_Stop

This Event Message indicates the time at which signaling terminates.

Originating CMS

In the single-zone scenario, the originating CMS MUST timestamp this message immediately upon receipt of the 250 RSP to the NCS-signaling DLCX message.

In the intra-domain or inter-domain scenarios, the originating CMS MUST timestamp this message upon receipt of the last signaling event in the following list:

- receipt of the 250 RSP to the NCS-signaling DLCX message, or
- receipt of the 200 RSP to the BYE.

Terminating CMS

In the single-zone scenario, the terminating CMS MUST timestamp this message immediately upon receipt of the 250 RSP to the NCS-signaling DLCX message.

In the intra-domain or inter-domain scenarios, the terminating CMS MUST timestamp this message upon receipt of the last signaling event in the following list:

- receipt of the 250 RSP to the NCS-signaling DLCX message, or
- receipt of the 200 RSP to the BYE.

Originating MGC (off-on)

The originating 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.

Terminating MGC (on-off)

The terminating MGC MUST timestamp this message immediately upon receipt of: the 250 OK that is sent in response to the TGCP DLCX message.

Table 18. Signaling_Stop Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	None
BCID	R	If the originating CMS or MGC generates this message, this attribute MUST contain the BCID of the terminating CMS or MGC. If the terminating CMS or MGC generates this message, this attribute MUST contain the BCID of the originating CMS or MGC.
FEID	R	If the originating CMS or MGC generates this message, this attribute MUST contain the FEID of the terminating CMS or MGC. If the terminating CMS or MGC generates this message, this attribute MUST contain the FEID of the originating CMS or MGC.

9.6 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 BCID 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	Class Service Name 4 Call_Block 5 Call_Forward 6 Call_Waiting
Calling_Party_Number	R	
Charge_Number	R	

9.7 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
Returned_Number	R	Note: In the PSTN, only a single number is returned per a query for Toll-free/LNP/Calling Name service ([20],[21],[22]). There may be multiple numbers returned such as the 800 translation results in a ported number in an optimized response available in AIN 0.2 ([18], [19]). This is optional for use in TCAP query of these services. If multiple numbers are returned, this attribute SHOULD reflect the result associated with the original query as indicated in the attribute Query_Type in this message. Any additional database dip result SHOULD be included in the corresponding specific attribute. In the case of LNP

Attribute Name	Required or Optional	Comment
		as a bundled response to the toll free query, the Location_Routing_Number SHOULD be included to convey the additional returned number result from a single database query to the SCP. As an alternative, the Returned_Number MAY be included for each number returned , but SHOULD be included as a pair with Query_Type in an ordered sequence. The first pair denotes the returned number associated with the original query type. The next pair denotes the next returned number of the next bundled database dip of the same original query. This repeats until the last returned number is conveyed.
Location_Routing_Number	O	See note above.
Query_Type	O	As a pair with Returned_Number for each of the subsequent database dip result within a single original database query. See note in the Returned_Number comment column above.
Returned_Number	O	As a pair with Query_Type for each of the subsequent database dip result within a single original database query. See note above.

9.8 Intelligent_Peripheral_Usage_Start

Deferred.

9.9 Intelligent_Peripheral_Usage_Stop

Deferred.

9.10 Interconnect_Start

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

The MGC MUST timestamp this message immediately upon transmission/receipt of an IAM to/from the Signaling Gateway that communicates with the SS7 network.

The terminating MGC MUST generate this message only after the ACM/ANM is received. This is so that if another IAM is attempted due to reattempt handling with a different trunk group number before the ACM/ANM is received, the Interconnection_Start reports the latest trunk group number along with the latest timestamp of the final IAM used to complete the call. (The Signaling_Start reports the first IAM attempted trunk group number of the same call.)

The originating MGC MAY generate this message when the ACM is transmitted although it is timestamp upon receipt of an IAM.

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

9.11 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 transmission/receipt of an RLC to/from the Signaling Gateway that communicates with the SS7 network.

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 interconnection is occurring

9.12 Call_Answer

This Event Message indicates that the media connection is open because answer has occurred.

Originating CMS

The originating CMS MUST timestamp this message immediately upon receipt of the 200 OK sent in response to the original INVITE message indicating call answer.

Terminating CMS

The terminating CMS MUST timestamp this message immediately upon receipt of the NCS-signaling NTFY message indicating off-hook at the terminating MTA.

Originating MGC (off-on)

The originating MGC MUST timestamp this message immediately upon

- transmission of an SS7 ANM message to the PSTN via the SG, or
- commanding the MG to generate answer indication on the operator services trunk.

Terminating MGC (on-off)

The terminating MGC MUST timestamp this message immediately upon

- receipt of an SS7 ANM message from the PSTN via the SG, 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
Charge Number	R	This attribute MUST contain the charge number in the appropriate cases such as collect call, calling-card call, call billed to a 3rd party, or others.
BCID	R	If the originating CMS or MGC generates this message, this attribute MUST contain the BCID of the terminating CMS or MGC. If the terminating CMS or MGC generates this message, this attribute MUST contain the BCID of the originating CMS or MGC.
FEID	R	If the originating CMS or MGC generates this message, this attribute MUST contain the FEID of the terminating CMS or MGC. If the terminating CMS or MGC generates this message, this attribute MUST contain the FEID of the originating CMS or MGC.

9.13 Call_Disconnect

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.

Originating CMS

The originating CMS MUST timestamp this message immediately upon transmission of the DLCX.

[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.

Terminating CMS

The terminating CMS MUST timestamp this message immediately upon transmission of the DLCX or upon expiration of the terminating MTA's call-continuation timer.

Originating MGC (off-on)

The originating MGC MUST timestamp this message upon receipt of an SS7 REL message, or upon sending a BYE message in response to an SS7 REL message from the terminating CMS.

Terminating MGC (on-off)

The terminating MGC MUST timestamp this message upon receipt of an SS7 RLC message, 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
Call_Termination_Cause	R	Normal Termination

9.14 QoS_Reserve

This Event Message indicates the time at which the CMTS reserves bandwidth on the PacketCable access network. The CMTS MUST also generate this event if the Reserved bandwidth changes.

The originating and terminating CMTS MUST timestamp this message immediately upon:

Table 25. QoS Reserve Timestamp Generation

Client initiated	CMTS initiated
Client initiated DSA-REQ	CMTS initiated DSA-REQ
reception of a DSA-ACK acknowledging a successful DSA-RSP (confirmation code == success).	transmission of a DSA-ACK acknowledging a successful DSA-RSP (confirmation code == success)
If a DSA-ACK is not received, the CMTS MUST NOT generate this message.	If a DSA-ACK is not transmitted, the CMTS MUST NOT generate this message .

If the DSA-RSP confirmation code is not successful, the CMTS MUST NOT generate this message.

Table 26. QoS_Reserve Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	None
QoS_Descriptor	O	None
MTA_UDP_Portnum	R	None
SF ID	R	None
Flow_Direction	R	None

9.15 QoS_Release

This Event Message indicates the time at which the CMTS released its bandwidth commitment on the PacketCable access network.

The originating and terminating CMTS MUST timestamp this message immediately upon:

- transmission of a DSD-RSP that indicates the request to delete bandwidth contained in the DSD-REQ from the MTA was successful, or
- transmission of a DSD-REQ that indicates the request to delete bandwidth.

Table 27. QoS_Release Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	None
SF_ID	R	None
Flow Direction	R	None

9.16 Time_Change

This event captures an instance of a time change. .Whenever the (PacketCable) clock on the network element (CMS,MGC or CMTS) is changed by more than 200 milliseconds, the network element MUST generate a Time Change message. This includes time shift events (Daylight savings time), step adjustments to synchronize with the NTP reference clock and manual time setting changes. The Event_Time attribute in the Event Message header (Table 32) MUST reflect the new (adjusted) notion of time. Note that Time_Change message is not required for slew adjustments performed by NTP.

The network element (CMS, MGC and CMTS) MUST send the Time Change event message to the active (current primary) RKS. The Time Change event message MUST be generated when one or more calls are active or in the process of being set up . For the CMS and MGC active or in process is after a Signaling Start event has been generated. For the CMTS active or in process is indicated by the presence of a DQoS gate. The Time Change event message need not be generated when calls are not active or in the process of being set up. Only one Time Change event message is sent to each primary RKS (if there is more than one primary RKS) regardless of how many calls may be active.

The BCID in the Event Message Header of the Time Change event message MUST be generated locally by the network element at the time of the event . The BCID is not associated with any call related BCID, it is a unique BCID for this event.

Table 28. Time_Change Event Message

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

9.17 QoS_Commit

This Event Message indicates the time at which the CMTS commits bandwidth on the PacketCable access network. The CMTS MUST also generate this event if the Committed bandwidth changes.

The originating and terminating CMTS MUST timestamp this message immediately upon:

Table 29. QoS Commit Timestamp Generation

Client initiated	CMTS initiated
Client initiated DSC-REQ or a DSA-REQ (when the CMTS reserves and commits the bandwidth in one-step).	CMTS initiated DSC-REQ or a DSA-REQ (when the CMTS reserves and commits the bandwidth in one-step).
reception of a DSA/DSC-ACK acknowledging a successful DSA-RSP/DSC-RSP (confirmation code == success).	transmission of a DSA/DSC-ACK acknowledging a successful DSA/DSC-RSP (confirmation code == success).
If a DSA/DSC-ACK is not received, the CMTS MUST NOT generate this message.	If a DSC-ACK is not transmitted, the CMTS MUST NOT generate this message.

If the DSA/DSC-RSP confirmation code is not successful, the CMTS MUST NOT generate this message.

Table 30. QoS_Commit Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	None
QoS_Descriptor	O	None
MTA_UDP_Portnum	R	None
SF_ID	R	None
Flow_Direction	R	None

9.18 RTP_Connection_Parameters Event Message

Deferred.

9.19 Media_Alive

If the PacketCable architecture is expected to support this Media_Alive Event Message, then it is recommended that all CMS, CMTS, and MGC be pre-configured with the same Media_Alive generation time.

This Event Message indicates that service is active due to the continued existence of a bearer connection. This Event Message MAY be generated by any trusted PacketCable network element (CMS, CMTS, MGC) as as defined below.

If a NE is configured to generate the optional Media_Alive event message, it must check for the status of all calls at the configured Media_Alive generation time. At the configured Media_Alive generation time, (e.g. 00:00 means midnight, 23:59 means 11:59 PM) the NE checks if any of the active calls are equal to or older than 1440 minutes. (24 hours). Only if a call is equal to or older than 1440 minutes, a Media_Alive event message for that call MUST be generated.

The call starting time for different NE types are specified by:

- CMTS: the first QoS_Commit event message EM_Header attribute Event_time for a gate.
- CMS: the Call_Answer event message EM_Header attribute Event_time. The EM_Header attribute Event_time is time stamped as per Section 9.12 Call_Answer.
- MGC: the Call_Answer event message EM_Header attribute Event_time. The EM_Header attribute Event_time is time stamped as per Section 9.12 Call_Answer.

NEs MUST (when configured to generate the Media_Alive EMs) generate the Media_Alive EMs at the Media_Alive EM generation time. Even though the Media_Alive EM generation time is configurable, the default value for the Media_Alive EM generation time MUST be midnight. Thus a service provider can have a synchronized network simply by accepting the default value from all NEs. If a service provider wants different time for Media_Alive EM generation time, it is up to the service provider to configure the different Media_Alive EM generation time.

The following diagram illustrates how a long duration call is identified.

Assumption: the Media_Alive EM generation on the NE has been configured to midnight (00:00) (the default value).

Call A is not a long duration call because its duration is less than 24 hours (or 1440 minutes) long.

Call B is not a long duration call because its duration is longer than 24 hours but it is less than 1440 minutes long at the Media_Alive EM generation time (midnight).

Call C is a long duration call because at the second midnight after the call was established, its duration is longer than 1440 minutes. (actually 2340 minutes long). Only one Media_Alive is generated because it is terminated prior to the next Media_Alive EM generation time (midnight).

Call D is also a long duration call because it meets the same criterion as Call C. Because it stays up across the midnight boundary after becoming a long duration call, two Media_Alive EMs are generated.

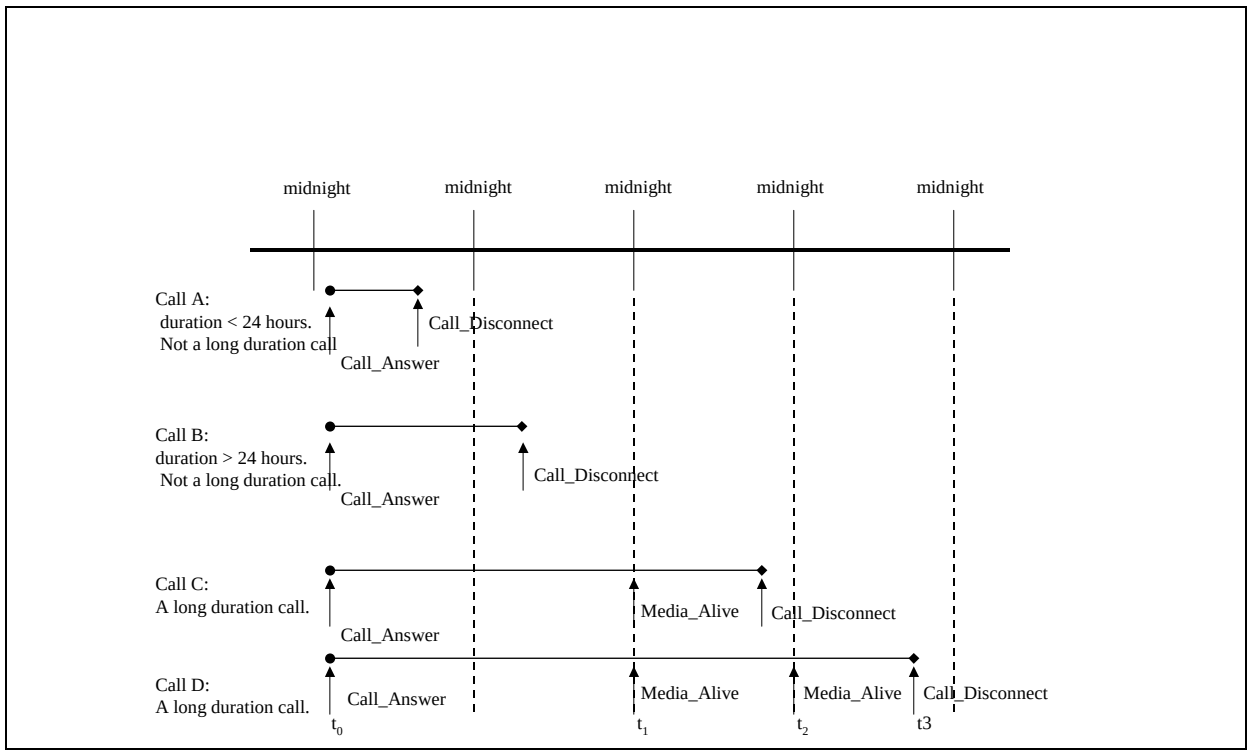

Figure 7. Long Duration Call Identification

From the above diagram, Call D will be used to illustrate the contents of the long duration call records belonging to a same call id (BCID).

In above scenario, there will be three records generated from Call D, let's identify these as record 1, 2, and 3.

The Call D starts on day 0 at 9:00:00 AM. (t0 July 27, 2001).

At first midnight crossing, the call is 900 minutes long (or 5400 seconds). So no record is generated.

At second midnight crossing (t1), the call is 2340 minutes long (or 140400 seconds). So a Media_Alive Event Message is generated with the following value:

EM Header.Event_time = 20010729000000.000

At third midnight crossing (t2), the call is 3780 minutes long (or 226800 seconds). A Media_Alive event message with the following value is generated:

EM Header.Event_time = 20010730000000.000

At 5:00pm, following the third midnight, the call is terminated. (t3). The overall duration of the call is 4800 minutes long (or 288000 seconds). A Call_Disconnect event message with the following value is generated for this call BCID.

EM Header.Event_time = 20010730170000.000

Table 31. Media_Alive Event Message

Attribute Name	Required or Optional	Comment
[Event Message Header] (Table 34)	R	None

10 PACKETCABLE EVENT MESSAGE ATTRIBUTES

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

Table 32 shows a mapping of the PacketCable Event Messages and their associated PacketCable attributes. Table 33 contains a detailed description of the PacketCable attributes.

Table 32. PacketCable Attributes Mapped to PacketCable Event Messages

EM Attribute ID	EM Attribute Name	Event Message ID																	
		1 – Signaling_Start	2 – Signaling_Stop	3 – Database_Query	4 – Deferred	5 – Deferred	6 – Service_Instance	7 – QoS_Reserve	8 – QoS_Release	9 – Service_Activation	10 – Service_Deactivation	11 – Undefined	12 – Undefined	13 – Interconnect_Start	14 – Interconnect_Stop	15 – Call_Answer	16 – Call_Disconnect	17 – Time_Change	19 – QoS_Commit
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																	
4	Calling_Party_Number	X					X			X	X								
5	Called_Party_Number	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				X									X			
14	First_Call_Calling_Party_ Number						X												
15	Second_Call_Calling_ Party_Number						X												
16	Charge_Number						X			X	X					X			
17	Forwarded_Number									X									
18	Service_Name						X			X	X								
19	Undefined																		
20	Intl_Code	X																	
21	Dial_Around_Code	X																	
22	Location_Routing_ Number	X																	

EM Attribute ID	EM Attribute Name	Event Message ID																	
		1 – Signaling_Start	2 – Signaling_Stop	3 – Database_Query	4 – Deferred	5 – Deferred	6 – Service_Instance	7 – QoS_Reserve	8 – QoS_Release	9 – Service_Activation	10 – Service_Deactivation	11 – Undefined	12 – Undefined	13 – Interconnect_Start	14 – Interconnect_Stop	15 – Call_Answer	16 – Call_Disconnect	17 – Time_Change	19 – QoS_Commit
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																		
30	SF_ID							X	X										X
31	Error_Description																		
32	QoS_Descriptor							X	X										X
33	Undefined																		
34	Undefined																		
35	Undefined																		
36	Undefined																		
37	Direction_indicator	X																	
38	Time_Adjustment																	X	
49	FEID		X													X			
50	Flow_Direction							X	X										X

Table 33 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 34 through Table 40. It should be noted that Event Message 17 it not service dependent.

Table 33. PacketCable Event Message attributes

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
0	Reserved			
1	76 bytes	EM_Header	Data structure (See Table 32)	Common data required on every PacketCable Event Message
2	Undefined			
3	variable length, maximum of 247 bytes (247 is maximum length of vendor specific attribute)	MTA_Endpoint_ Name	ASCII character string	Physical Port name (aaln/#) as defined in the PacketCable NCS Spec [1]
4	20 bytes	Calling_Party_ Number	Right justified, space padded ASCII character string	PacketCable 1.0 will use E.164 [9] 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 [9] formatted address specifying the number of the terminating party. In the future other numbering plans will be addressed.
6	Variable length, maximum of 247 bytes (247 is maximum length of vendor specific attribute)	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 2=LNPNumberLookup 3=Calling Name Delivery Lookup
8	Undefined			

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
9	20 bytes	Returned_Number	Right justified, space padded ASCII character string	PacketCable 1.0 will use E.164 [9] 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 37)	Termination code identifier
12	Undefined			
13	24 bytes	Related_Call_ Billing_ Correlation_ID	Data structure. (See Table 35)	BCID for possible use in value added services or to identify the matching originating/terminating half of the service.
14	20 bytes	First_Call_Calling_ Party_Number	Right justified, space padded ASCII character string	PacketCable 1.0 will use E.164 [9] 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 [9]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 [9] formatted address specifying the number of the 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 [9] 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	4 Bytes	Intl_Code	Right justified, space padded ASCII character string	International Country Code
21	8 Bytes	Dial_Around_Co de	Right justified, space padded ASCII character string	Dial-around code used for per-call selection of inter-exchange carrier
22	20 bytes	Location_Routing _Number	Right justified, space padded ASCII character string	For LNP uses PacketCable 1.0 will use E.164 [9] formatted address specifying the number of the terminating party. In the future other numbering plans will be addressed.

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
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 38)	Trunk group identification
25	20 bytes	Routing_Number	Right justified, space padded ASCII character string	PacketCable 1.0 will use E.164 [9] 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. Destination port field value in DQoS Gate-spec object received in DQoS Gate-Set message.
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. (See Table 36)
32	Variable; Min 8 bytes	QoS_Descriptor	Data structure See Table 39.	QoS parameters data (See Appendix C of [13])
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) clock. This time is in milliseconds, detailing the amount of the time change.
39	variable	SDP_Upstream	ASCII character string	Description of upstream packet flow
40	variable	SDP_Downstream	ASCII character string	Description of downstream packet flow

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
41	variable	User_Input	ASCII character string	Sequence of dialed digits as entered by user
42	20 bytes	Translation_Input	Right justified, space padded ASCII character string	E.164 [9]address of the input to an external translation lookup
43	42 bytes	Redirected_From _Info	Data Structure	Information about previous redirections of this call
44	variable	Electronic_ Surveillance_ Indication	Data Structure	Additional destination of CCC and CDC for redirected call
45	20 bytes	Redirected_From _Party_Number	Right justified, space padded ASCII character string	E.164 [9] address of the party initiating a redirection
46	20 bytes	Redirected_To_ Party_Number	Right justified, space padded ASCII character string	E.164 [9] address of the destination party of a redirection
47	Variable	Electronic_ Surveillance_DF _Security	Binary octet string	A pre-shared key that is used to authenticate DF-DF IKE key exchanges. The source DF receives the same key in the Electronic-Surveillance-Indication attribute, field DF-DF-Key.
48	4 bytes	CCC_ID	Unsigned integer	Call Content identifier assigned by CMTS or MGC
49	Variable length, maximum of 247 bytes	FEID	ASCII character string.	Financial Entity ID. The first 8 bytes constitute MSO defined data. By default, the first 8 bytes are zero filled. From the 9th byte on the field contains the MSO's domain name which uniquely identifies the MSO for billing and settlement purposes. The MSO's domain name is limited to 239 bytes.
50	2 bytes	Flow Direction	Unsigned integer	Flow direction: 0=Reserved 1=Upstream 2=Downstream

10.1 EM_Header Attribute Structure

Table 34 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 34. 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
BCID	Unique identifier for a transaction within a network. See following section.	Data Structure (See Table 35)	24 bytes
Event Message Type	Identifies the type of Event Message. Refer to Table 11 for a listing of Event message types.	Unsigned integer	2 bytes
Element Type	Identifies Type of Originating Element: 0 = Reserved 1 = CMS 2 = CMTS 3 = Media Gateway Controller	Unsigned integer	2 bytes
Element ID	Network wide unique identifier 5 digits (statically configured element number unique within a PacketCable domain in the range of 0-99,999)	Right justified, space padded ASCII Character String	8 bytes
Time Zone	Identifies daylight savings time and offset from universal time (UTC). Daylight Savings Time: 0 = Standard Time 1 = Daylight Savings UTC offset: ± HHMMSS The offset is reported from the network element (CMS/MGC/CMTS) point of view; not based on the subscriber point of view.	ASCII character string	 1 byte 7 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. This specifies the local time. i.e.after applying time offset to UTC time. Format: yyyymmddhhmmss.mmm	ASCII character string	18 bytes
Status	Status indicators	See Table 36	4 bytes

Field Name	Semantics	Value Type	Length
Priority	Indicates the importance to assign relative to other event messages. The processing of event message priority is defined as: -as long as there are higher priority messages within the system, lower priority messages SHOULD NOT be processed. -arrival of a higher priority message will not interrupt current lower priority message processing. Only after the completion of the message processing, the newly arrived higher message will be processed. For PacketCable Release 1.0, values for this field will be service provider assigned. 255 = highest priority 0 = lowest priority 128 = default.	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

10.1.1 Billing Correlation ID (BCID) Attribute Structure

Table 35 describes the Billing Correlation ID (BCID). The RKS, or some other back office application, uses the BCID to correlate Event Messages that are generated for a single transaction. It is one of the fields in the Event Message Header. The BCID is unique for each Transaction in the network. All Event Messages with the same BCID SHOULD be sent to the same primary RKS except in failover circumstances in which case the Event Messages MUST be sent to secondary RKS.

Table 35. BCID 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 5 digits (statically configured element number unique within a PacketCable domain in the range of 0-99,999)	Right justified, space padded ASCII character string	8 bytes
Time Zone	Identifies daylight savings time and offset from universal time (UTC). Daylight Savings Time: 0 = Standard Time 1 = Daylight Savings UTC offset: ± HHMMSS The offset is reported from the network element (CMS/MGC/CMTS) point of view; not based on the subscriber point of view.	ASCII character string	1 byte 7 bytes
Event Counter	Monotonically increasing for each Transaction	Unsigned integer	4 bytes

10.1.2 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 36 presents Status Field description.

Table 36. 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, attribute 31 MUST be included in the Event Message corresponding to this header. If Possible error, 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

10.2 Call Termination Cause Attribute Structure

Table 37 describes the data structure of the Call_Termination_Cause attribute.

Table 37. 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) [6] 2 = Future	Unsigned integer	2 bytes
Cause_Code	Cause Code Identifier. Meaning determined by Source_Document defined in previous field.	Unsigned integer	4 bytes

10.3 Trunk Group ID Attribute Structure

Table 38 describes the Trunk Group ID Data Structure.

Table 38. 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

10.4 QoS Descriptor Attribute Structure

Table 39 describes the QoS Descriptor Data Structure.

Table 39. 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	16 bytes
QoS_Parameter_Array	QoS Parameters. Contents determined by Status Bitmask.	Unsigned integer array	Variable length array of 32-bit unsigned integers

Table 40 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 [13]. QoS parameters whose definition specifies less than four bytes must be right-justified (where the 4 bytes are to be treated as an unsigned integer) in the four bytes allocated for the array element.

Table 40. QoS Status Bitmask

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	Maximum Traffic Burst	1
10	Minimum Reserved Traffic Rate	1
11	Minimum Packet Size	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

10.5 Redirected-From-Info Attribute Structure

Table 41 describes the data structure of the Redirected-From-Info.

Table 41. Data Structure of the Redirected-From-Info Attribute

Field Name	Semantics	Value Type	Length
Last-Redirecting-Party	E.164 [9] address of most recent redirecting party	ASCII string	20 bytes
Original-Called-Party	E.164 [9]address of the original called party	ASCII string	20 bytes
Number-of-Redirections	Number of times this call has been redirected	Unsigned integer	2 bytes

10.6 Electronic-Surveillance-Indication Attribute Structure

Table 42 describes the data structure of the Electronic-Surveillance-Indication.

Table 42. Data Structure of the Electronic-Surveillance-Indication Attribute

Field Name	Semantics	Value Type	Length
DF-Address	IP address of the electronic surveillance delivery function of the forwarding party	IP Address	4 bytes
CDC-Port	Port number to which to send a copy of event messages	Unsigned integer	2 bytes
CCC-Port	Port number to which to send a copy of call content packets	Unsigned integer	2 bytes
DF-DF-Key	A pre-shared key that is used to authenticate DF-DF IKE key exchanges. The destination DF receives the same key in the Electronic_Surveillance_DF_Security attribute.	Binary octet string	variable

11 TRANSPORT INDEPENDENT EVENT MESSAGE ATTRIBUTE TLV FORMAT

Every Event Message Attribute is defined by a Type Length Value (TLV) tuple. An attribute TLV tuple has the following format:

Table 43. Event Message Attribute TLV-tuple format

Field Name	Semantics	Field Length
Attribute Type	PacketCable Attribute Type	1 byte (refer to Table 33)
Attribute Length	PacketCable Attribute Length	1 byte (refer to Table 33) Note: Value is Attribute Length + 2
Attribute Value	PacketCable Attribute Value	Attribute Length bytes

12 PACKETCABLE EVENT MESSAGE FILE FORMAT

The PacketCable Event Message File Format has the following basic structure:

12.1 File Header

The following header MUST be written at the start of a file formatted using the PacketCable Event Message File Format:

Field Name	Semantics	Length	Type
Format Version	Version number of file format	4 bytes	Unsigned int
EM Count	Number of EMs in File	8 bytes	Unsigned int
File Creation Timestamp	YYYYMMDDHHMMSS.MMM	18 bytes	ASCII
File Sequence Number	Monotonically increasing	8 bytes	Unsigned int
Element ID	Network wide unique identifier 5 digits (statically configured element number unique within a PacketCable domain in the range of 0-99,999)	8 bytes	Right justified, space padded ASCII character string
Time Zone	Identifies daylight savings time and offset from universal time (UTC). Daylight Savings Time: 0 = Standard Time 1 = Daylight Savings UTC offset: ±HHMMSS	 1 byte 7 bytes	ASCII character string
File Completion Timestamp	YYYYMMDDHHMMSS.MMM	18 bytes	ASCII

Note: There is no checksum included in the file header. It is assumed that the transport mechanism is responsible for delivery of damage-free files. For example, both of the IP transport protocols, UDP and TCP, contain a checksum to protect against damaged messages.

12.2 File Naming Convention

Files created using the PacketCable Event Message File Format MUST use the following naming convention: "PKT-EM-yyyymmddhhmmss-pri-elementid-seq.bin."

12.2.1 PKT-EM-yyyymmddhhmmss-prielementid-seq.bin

The following table describes each of the components of the filename:

Component	Semantics	Type	Length
File ID	Identifies this file as containing PacketCable Event Messages	Literal string 'PKT-EM'	6 characters
Timestamp	Time at which file was opened by the network element	yyyymmddhhmmss	14 characters
Priority	Priority of this file When processing multiple files with differing priorities, files of higher priority must be processed before the lower priority files.	Integer in the range 1-4 4 is the highest 1 is the lowest	1 character
Element ID	Network wide unique identifier 5 digits (statically configured element number unique within a PacketCable domain in the range of 0-99,999) with leading zeros for padding. e.g. element id = 99 PKT-EM-yyyymmddhhmmss-pri-00099-seq.bin	Right justified, zero padded ASCII character string	5 characters
Sequence number	Monotonically increasing sequence number	Integer in the range 000001-999999, zero-filled.	6 characters

Each of the filename components is separated by a hyphen '-' character.

12.3 Configuration Items

The following items MUST be configurable by the PacketCable network element creating the file:

Name	Semantics	Type	Length
Maximum File Length	Maximum size of file, in bytes, to which flat file can grow before being closed for transport.	Unsigned integer	4 octets
Maximum Open Time	Maximum amount of time, in seconds, before file must be closed for transport.	Unsigned integer	4 octets

The PacketCable Network Element that created the file MUST close any currently open flat file at the first occurrence of either of the following events:

- The file size exceeds the Max File Length
- The file open duration exceeds the Maximum Open Time

13 TRANSPORT PROTOCOL

This section specifies the possible transport protocols used between the PacketCable network elements that generate Event Messages (CMS, CMTS, MGC) and the Record Keeping Server (RKS). These network elements MUST support RADIUS Accounting (RFC2866) with PacketCable extensions as defined in this document. The optional transport protocol is FTP as defined in this document.

The following are the PacketCable 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.
- 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

13.1 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 RFC2866 [5]. Although PacketCable 1.0 specifies RADIUS as the transport protocol, alternate transport protocols MAY be supported in future PacketCable releases.

13.1.1 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 RFC2865 [4] 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-Reponse within the configured retry interval, it MUST re-send the same Accounting Request either to the same RKS or the alternate RKS (retries may alternate between primary and secondary RKS in a vendor-specific way). The PacketCable network element MUST continue resending the Accounting-Request until it receives an acknowledgement from an RKS or the maximum number of retries is reached. The RADIUS server MUST NOT transmit any Accounting-Response reply if it fails to successfully record the Event Message.

Once a Network Element succeeds in sending event messages to the secondary RKS server, a failover to the secondary RKS should occur. This is a non-revertive failover, meaning that the secondary RKS becomes active, and is the new primary RKS. For calls in progress, all subsequent event messages should be sent to the now active secondary RKS. For all new calls, the CMS should instruct the CMTS and MGC to use the new active RKS as the primary (ie, the previous secondary RKS becomes the new primary for subsequent calls).

13.1.2 RADIUS Client Reliability

All Network Elements MUST store Event Messages until they have received an Acknowledgement (Ack) from an RKS that the data was correctly received and stored, or until the maximum number of retries has been reached. Only when an Ack is received or the maximum retries reached are the NEs allowed to delete these Event Messages.

In order to guarantee the reliable transfer of the data the Radius Client should implement a user configurable Radius message Ack interval and the number of times the client needs to retransmit the event or message. The time interval should be configurable (suggested: 10msec to 10 sec), the number of retries should be configurable (suggested: 0 to 9). The number of retries should be attempted on both the primary RKS and secondary RKS. After Exhausting the number of retries the event message should be written to an error file, and the event message can then be deleted from the network element.

Notes: 1) The Radius Client MIB (RFC2620) does *not* contain these parameters.
2) This requirement implies that the RKSes use highly reliable storage media and are also highly available.

13.1.3 Authentication and Confidentiality

Refer to the PacketCable security specification [2] 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, hardcoded to the value of 16 ASCII 0s. That is, the shared secret is "0000000000000000". 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 RFC2866.

13.1.4 Standard RADIUS Attributes

Each RADIUS message starts with the standard RADIUS header shown in Table 44.

Table 44. 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	Computed as per RADIUS Specification [4]	16 bytes

Two standard RADIUS attributes MUST follow the RADIUS Message Header: NAS-IP-Address and Acct_Status_Type. These two fields are included to improve interoperability with existing RADIUS server implementations since they are mandatory attributes in a RADIUS Accounting-Request packet.

The NAS-IP-Address indicates the originator of the Accounting-Request message and MUST contain the IP address of the originating PacketCable network element.

The Acct-Status-Type attribute 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, it could 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.

Table 45. Mandatory RADIUS Attributes

Name	Type	Length	Value
NAS-IP-Address	4	6	IP address of originating PacketCable network element
Acct-Status-Type	40	6	Interim-Update=3

Table 46. RADIUS Acct_Status_Type

Type	Length	Value
40	6 bytes	Interim-Update = 3

PacketCable attributes are defined in Section 10 of this document. PacketCable attributes are encoded in the RADIUS Vendor Specific Attributes (VSA) structure as described in this section. Additional PacketCable or vendor-specific attributes can be added to existing Event Messages by adding additional RADIUS VSAs to the message.

The Vendor-Specific attribute includes a field to identify the vendor, and the Internet Assigned Numbers 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 47. 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	1 byte (refer to Table 33)
Vendor Attribute Length	PacketCable Attribute Length	1 byte (refer to Table 33) Note: value is Vendor Length +2
Vendor Attribute Value	PacketCable Attribute Value	Vendor Length bytes

13.1.5 PacketCable Extensions

13.1.5.1 PacketCable RADIUS Accounting-Request Packet Syntax

```
<<RADIUS Accounting-Request> ::==
                <RADIUS message Header>
                <RADIUS NAS-IP-Address Attribute>
                <RADIUS Acct-Status-Type Attribute>
                <Packet Cable EM List>

<Packet Cable EM List> ::==
                <Packet Cable EM> |
                <Packet Cable EM List> <Packet Cable EM>

<Packet Cable EM> ::==
                <RADIUS VSA for PacketCable EM Header Attribute>
                <PacketCable EM Attribute List>

<PacketCable EM Attribute List> ::==
                <RADIUS VSA for PacketCable EM Attribute> |
                <PacketCable EM Attribute List>
<RADIUS VSA for Packet Cable EM Attribute>
```

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 transmit 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.

The Event Message Header MUST be the first attribute within a given Event Message. If multiple Event Messages are sent in a single RADIUS Accounting-Request, the Event Message Header attribute indicates the start of a new Event Message. The order of the Event Message attributes which follow the Event Message Header is arbitrary.

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.

13.2 File Transport Protocol (FTP)

The File Transfer Protocol (FTP) MAY be used to transport Event Messages from PacketCable network element to the RKS. If this transport protocol is used, the RKS hosts an FTP server to accept files transferred by the PacketCable network element. The PacketCable network element acts as the FTP client, pushing the files to the RKS for processing.

If FTP is used as a transport protocol, then the file MUST be formatted using the PacketCable Event Message File Format.

13.2.1 Required FTP Server Capabilities

The FTP server at the RKS MUST have the following capabilities:

- PASV Mode
- Authentication support
- File Transfer logging

Appendix A PCES Support

This section details the PacketCable Event Messages and their associated attributes that MUST be generated to support PacketCable Electronic Surveillance as defined in [8]. The following requirements apply to all PCES Event Messages:

- The appropriate network element (CMS,CMTS, MGC) MUST send the PCES Event Message to the DF in real-time as defined in [8].
- The PCES Event Message sent to the DF MUST NOT affect the monotonically increasing Sequence-Number that appears in the Event Message header sent to the RKS.

A.1 Service_Instance

If the service is under surveillance as defined in [8], the Service_Instance Event Message MUST be generated with all the standard required parameters and with the additional required electronic surveillance parameters. If the call is being forwarded or transferred by a subject under surveillance, this Event Message MUST include the Electronic-Surveillance-DF-Security object.

Table 48. Service_Instance Event Message for PCES

Attribute Name	Required or Optional	Comment
[Event Message Header]	R	
Service_Name	R	Class Service name 6 = Call_Block 7 = Call_Forward 8 = Call_Waiting 9 = Repeat_Call 10 = Return_Call
Call_Termination	O	1 = Required
Redirected_From_Party_Number	O	2 = Required
Redirected_To_Party_Number	O	2 = Required
Carrier_Identification_Code	O	2 = Required when a transit carrier is used to transport the redirected call
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

Attribute Name	Required or Optional	Comment
Routing_Number	O	4,5 = Required
Calling_Party_Number	O	4,5 = Required
Electronic_Surveillance_DF_Security	O	2 = MUST be present in events sent to DF for calls redirected by a surveillance subject. MUST NOT be present in event messages sent to RKS.

A.2 Signaling_Start

If the service is under surveillance as defined in [8], this Event Message MUST be generated with all the standard required parameters and with the additional required electronic surveillance parameters.

The MGC MUST generate, timestamp, and send this event to the DF for a terminating call under surveillance to a PSTN Gateway.

- The MGC MUST timestamp this message coincident with sending the SS7 IAM message or transmitting the dialed digits on an MF-trunk.

- For an originating call from an MTA or from a PSTN Gateway, if the MGC receives notification via signaling from the terminating CMS that the call is to be intercepted but the terminating device is unable to perform the interception, the MGC MUST timestamp and send an additional Signaling_Start event message to the Electronic Surveillance Delivery Function prior to delivering a response to the originating MTA or PSTN Gateway. This Signaling_Start event message MUST contain the Electronic Surveillance Indication object, and MUST indicate 'termination' in the Direction-Indicator.

The CMS MUST generate, timestamp, and send this event to the DF if the originating call from an MTA is under surveillance.

- The CMS MUST timestamp and send this event message DF after all translation of the dialed digits is complete, whether the translation is successful or not.

The CMS MUST generate, timestamp, and send this event to the DF. for a terminating call to an MTA under surveillance, or for a terminating call under surveillance to an MTA.

- The CMS MUST timestamp and send this event message to the Electronic Surveillance Delivery Function prior to invoking any termination features.

Table 49. Signaling_Start Event Message for PCES

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	None
Direction_indicator	R	None
MTA_Endpoint_Name	R	If the originating CMS generates this message, this attribute MUST contain the endpoint name of the originating MTA. If the terminating CMS generates this message, this attribute MUST contain the endpoint name of the terminating MTA. If the originating MGC generates this message, this attribute MAY contain the endpoint ID of the originating MG. If the terminating MGC generates this message, this attribute MAY contain the endpoint ID of the terminating MG.
Calling_Party_Number	R	None
Called_Party_Number	R	terminating address (E.164 [9] format)
Routing_Number	R	Routable number
Location_Routing_Number	R	For local number portability use
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.
User_Input	R	MUST be present for a call origination event, and MUST contain the original dialed digits received from MTA or from PSTN Gateway.
Translation_Input	R	MUST be present if an external database was consulted for translation, and the input for that external translation was different than the value of User-Input.
Redirected_From_Info	R	MUST be included for a call termination if information is available about previous redirections.
Electronic Surveillance Indication	R	MUST be present in events sent to DF for terminating calls that have been redirected by a surveillance subject. MUST NOT be present in event messages sent to RKS.

A.3 Call_Answer

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the standard required parameters and with the additional required electronic surveillance parameters.

The CMS or MGC MUST send this Event Message to the DF.

A.4 Call_Disconnect

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the standard required parameters.

The CMS or MGC MUST send this Event Message to the DF:

A.5 QoS_Reserve

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the standard required parameters. If the Session-Description-Parameters object was included in the Gate-Set message, then this message MUST include the SDP descriptions.

The CMTS MUST generate this message if:

1) the CMTS generates a Call_Disconnect event

2) the Electronic-Surveillance-Parameters object was included in the Gate-Set message to the CMTS, and the flag indicates dup-event

3) QoS is activated on a connection via a COMMIT message from the MTA

4) a DSA/DSC that includes an ActiveQoSParameterSet

5) a DSA/DSC contains an AdmittedQoSParameterSet for a gate established with the auto-commit flag

The MGC MUST generate this message if the MGC sends a CRCX or MDCX command to the Media Gateway that sets the mode to sendonly or to sendrecv.

Table 50. QoS_Reserve Event Message for PCES

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	None
QoS_Descriptor	O	None
MTA_UDP_Portnum	R	None
SDP_upstream	R	MUST be present in a QoS-Start message sent to the Electronic Surveillance Delivery Function.
SDP_downstream	R	MUST be present in a QoS-Start message sent to the Electronic Surveillance Delivery Function.
CCC_ID	R	MUST be present in a QoS-Start message sent to the Electronic Surveillance Delivery Function. For events generated by a CMTS, this MUST contain the Gate-ID.

A.6 QoS_Release

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the standard required parameters.

The CMTS MUST generate this message if:

1. the CMTS generates a Call_Disconnect event

2. the Electronic-Surveillance-Parameters object was included in the Gate-Set message to the CMTS, and the flag indicates *dup-event*

3. resources for QoS are released for a connection, via a RSVP-PATH-TEAR message from the MTA, or via a Dynamic SID Deletion

4. a QoS-Start message had previously been sent for this connection

The MGC MUST generate this message if:

- the MGC sends a DLCX command to the Media Gateway
- a MDCX command that changes the mode from sendonly or sendrecv

Table 51. QoS_Release Event Message for PCES

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	None
QoS_Descriptor	O	None
SF_ID	R	None
CCC_ID	R	MUST be present in a QoS-Stop message sent to the Electronic Surveillance Delivery Function. For events generated by a CMTS, this MUST contain the Gate-ID.

A.7 QoS_Commit

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the standard required parameters.

The CMTS MUST generate this message if:

1) the CMTS receives a Gate-Set command regarding an existing gate, and that Gate-Set includes the Session-Description-Parameters object

2) QoS is activated on a connection via a COMMIT message from the MTA, or a DSC that includes an ActiveQoSParameterSet

3) the Electronic-Surveillance-Parameters object was included in the Gate-Set message to the CMTS, and the flag indicates dup-event

Table 52. QoS_Commit Event Message for PCES

Attribute Name	Required or Optional	Comment
[Event Message Header] (see Table 32)	R	None
QoS_Descriptor	O	None
MTA_UDP_Portnum	R	None
SDP_upstream	R	MUST be present in a QoS-Start message sent to the Electronic Surveillance Delivery Function.
SDP_downstream	R	MUST be present in a QoS-Start message sent to the Electronic Surveillance Delivery Function.

A.8 Summary of Event Messages for PCES

Table 53. PacketCable Attributes Mapped to PacketCable Event Messages for PCES

EM Attribute ID	EM Attribute Name	Event Message ID						
		1 – Signaling_Start	6 – Service_Instance	7 – QoS_Reserve	8 – QoS_Release	15 – Call_Answser	16 – Call_Disconnect	19 – QoS_Commit
0	Reserved							
1	EM_Header	X	X	X	X	X	X	X
2	Undefined							
3	MTA_Endpoint_Name	X						
4	Calling_Party_Number	X	X					
5	Called_Party_Number	X	X			X		
6	Database_ID							
7	Query_Type							
8	Undefined							
9	Returned_Number							
10	Undefined							
11	Call_Termination_Cause		X				X	
12	Undefined							
13	Related_Call_Billing_ Correlation_ID		X			X		
14	First_Call_Calling_Party_Number		X					
15	Second_Call_Calling_ Party_Number		X					
16	Charge_Number		X			X		
17	Forwarded_Number							
18	Service_Name		X					
19	Undefined							
20	Undefined							
21	Undefined							
22	Location_Routing_ Number	X						
23	Carrier_Identification_ Code	X						

EM Attribute ID	EM Attribute Name	Event Message ID						
		1 – Signaling_Start	6 – Service_Instance	7 – QoS_Reserve	8 – QoS_Release	15 – Call_Answser	16 – Call_Disconnect	19 – QoS_Commit
24	Trunk_Group_ID	X						
25	Routing_Number	X	X					
26	MTA_UDP_Portnum			X				X
27	Undefined							
28	Undefined							
29	Undefined							
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						
38	Time_Adjustment							
39	SDP_Upstream			X				X
40	SDP_Downstream			X				X
41	User_Input	X						
42	Translation_Input	X						
43	Redirected_From_Inf	X						
44	Electronic_Surveillance_ Indicator	X						
45	Redirected_From_Party_Number		X					
46	Redirected_To_Party_ Number		X					
47	Electronic_Surveillance_DF_Security		X					
48	Gate_ID			X				
49	FEID					X		

Appendix B Revisions

The following Engineering Change Notices (ECNs) are incorporated in PKT-SP-EM-I02-001129:

ECN	Date Ratified	Summary
00021	6/9/00	Clarify value of authenticator field in Table 40.
00045-v2	9/25/00	Clarify syntax describing more than one Event Message carried in a single RADIUS message. Clarify RADIUS syntax for Event Messages, remove redundant Section 8.3.3 based on clarification.
00067	9/25/00	Clarify the definition of "a 16 byte, all zero value" to mean "16 ASCII 0's". Clarify that the RADIUS message "authenticator" field MUST be computed as per RADIUS.
00108	9/25/00	Clarify text it define "batch mode' as meaning multiple Event Messages carried in a single RADIUS message.
00110-v2	9/25/00	Deleted text that implied that the same physical Network Element must generate a matched-pair of Start/Stop Event Messages.
0111-v2	9/25/00	Eliminated the mechanism for the RKS to request missing Event Messages based on sequence number of timestamp. New text requiring that the CMS, CMTS, MGC use a timeout/retry mechanism to ensure that the RKS does not miss any Event Messages.
00112	9/25/00	Remove informative text recommending that the CMS, CMTS and MGC store Event Messages for a user-configurable time-period after receiving acknowledgement that the RKS has successfully received and stored the Event Message.
00113-v2	10/10/00	Clarify that the EM spec defines a transport protocol independent Event Message attribute TLV format, and RADIUS as a mandatory transport protocol. Create new Section 10 for transport protocols and Section 10.1 for RADIUS transport protocol.
00119	10/10/00	New Section 9 describes the PacketCable Event Message File Format. This file format can be used to temporarily store Event Messages on a PacketCable network and/or to transport several event messages via a transport protocol such as FTP.
00120	10/10/00	New Section 10.2 describing the optional FTP transport protocol.
00003	11/27/00	Additional support needed for Lawfully Authorized Electronic Surveillance, as per PKT-SP-ESP-I01-991229.
00114	11/27/00	Redefine Element_ID in table 34 (BCID) as 8 byte field made up of: 5 digit (statistically configured element number unique within a PacketCable domain 0-99,999); 1 digit Daylight Savings Time Flag; 2 digits time zone (0..23).
00115-v2	11/27/00	Clarify MGC timestamps for Interconnect_Start and Call_Answer.
00117	11/27/00	1) routing_number becomes a mandatory attribute in Signaling_Start 2) Remove attributes that are duplicated in Signaling_Start and Call_Answer by removing these attributes from Call_Answer (Called_Party_Number, Routed_Number, Location_Routing_Number).

ECN	Date Ratified	Summary
00125	11/27/00	Clarify that EM Attribute length of the EM header is 60 bytes.
00126	11/27/00	Clarify semantics of the PacketCable Attribute Length.
01009		Replace references to RFC2138 with RFC2865. Replace references to RFC2139 with RFC2866.
00141-v2	11/27/00	Update triggers and attributes to support single-zone, inter-domain and intra-domain scenarios.

The following Engineering Change Notices (ECNs) are incorporated in PKT-SP-EM-I03-011221:

ECN	Date Ratified	Summary
em-n-00145	2/26/01	PKT EM spec provides no long duration and/or keep-alive message.
em-n-01005	2/26/01	The current PacketCable RADIUS Accounting-Request Packet syntax is not compliant with RADIUS Accounting RFC (RFC2866) since it contains neither the NAS-IP-Address attribute nor the NAS-Identifier attribute.
em-n-01009	3/5/01	The EM spec refers to obsolete RADIUS Draft RFCs and should be updated with the new RADIUS Standards Track RFC numbers.
em-n-01044	8/6/01	The current requirements are that QoS-related messages indicating successful resource reservation and committal are sent regardless of whether the reservation/committal actually succeeded.
em-n-01045	11/5/01	Remove ambiguities in Time_Change message.
em-n-01046	8/6/01	Bring consistency to the changes made by ECN00115.
em-n-01047	8/6/01	Extend the logic of the changes made by ECN00115 to further define when Interconnect_Stop should be time stamped.
em-n-01085	8/27/01	Make Event Generation not required in the LCS System Architecture.
em-n-01128	11/5/01	It is not clear if the NodeId and Element ID are the same parameter in Event Message Header.
em-n-01129	11/5/01	There is 1 duplicate and 1 missing parameter in the QoS Descriptor Data Structure in Table 37.
em-n-01130	11/5/01	The spec is not clear on what happens when the existing reserved and/or committed bandwidth changes.
em-n-01132	11/5/01	Event Message ID number 19 (QoS_Commit) is not checked off in Tables 12, 13, and 14.
em-n-01133	11/5/01	Correct label on Table 28.
em-n-01134	11/5/01	Add missing information to MTA_UPD_ Portnum in Table 30.
em-n-01136	11/5/01	Correct length of Service_Class_Name Field in Table 36.
em-n-01135	12/3/01	The spec does not specify the possible values for the Daylight Savings Time Flag or Time zone parameter in the Element_ID field in the EM_Header Attribute Structure or BCID Description. The time zone parameter does not cover all worldwide time zones.

ECN	Date Ratified	Summary
em-n-01179	12/3/01	The DQOS spec mentions that the CMTS must generate the Call_Answer and Call_Disconnect event messages if the CMS/GC includes the appropriate objects in the COPS Gate-Set message. The Event Message spec in Appendix A discusses the CMTS generating the events. The text in the sections describing the events does not discuss the CMTS requirement.
em-n-01221	12/3/01	Need to allow FEID to be a unique value selected by the cable operator. Currently, a 3rd party organization is required to uniquely assign each MSO their "8-byte field to uniquely identify the MSO".
em-n-01223	12/3/01	Service Activation and Service Deactivation events do not have Charge Number field.
em-n-01137	12/3/01	Correct Table 40 and Table 43 - TLV format. Both Attribute Type and Attribute Length should be 1 byte.
em-n-01131	12/3/01	Clarify that QoS event messages are generated individually for both upstream and downstream bandwidth; add an attribute to indicate direction; add the SF_ID attribute to the QoS_Reserve and QoS_Commit events in order to help correlate the events for a particular flow.

The following Engineering Change Notices (ECNs) are incorporated in PKT-SP-EM-I04-021018:

ECN	Date Ratified	Summary
em-n-02036	4/29/02	Clarify the trigger condition at MGC for sending the Interconnection_Start and fix editing errors related to Call_Answer.
em-n-02047	7/1/02	Clarify Time_Change message requirement.
em-n-02052	7/1/02	Specification needs to be changed to be more clear in defining the requirements on network elements in sending event messages to the primary and secondary RKS.
em-n-02078	7/1/02	Error in the EM Attribute Length for attribute id 1 (EMS Header).
em-n-02079	7/1/02	Add enumeration - 3 (Calling Name Delivery Lookup) to the Query Type Attribute.
em-n-02080	7/1/02	Make the Location_Routing_Number attribute required to be sent for the Signaling Start event message, only when LNP is used.
em-n-02081	7/1/02	There is a mismatch between number of attributes in event messages given in different places in document.
em-n-02082	7/1/02	The long duration call indicator Event Message is referred to as both Media_Alive and Call_Alive.
em-n-02094	7/1/02	Clarify that the offset in the TimeZone is with respect to the network element, not with respect to the subscriber.

The following Engineering Change Notices (ECNs) are incorporated in PKT-SP-EM-I05-021127:

ECNs	Date Ratified	Summary
em-n-02110	11/4/02	The priority of EM is user defined.
em-n-02111	11/11/02	The file name specification in Section 12.2.1 contains 4 issues: a typo; node ID correction, time zone indicator, and file priority.
em-n-02116	11/4/02	Change Event Messaging spec to send dial-around codes and international country code as separate call attributes.
em-n-02135	11/4/02	QoS_Release EM attribute QoS_Descriptor is not needed.
em-n-02140	11/11/02	Clarify the inclusion rule of multiple Returned_Number in the Database_Query message.
em-n-02141	11/11/02	The definition for long duration call indicator Event Message Media_Alive is incomplete.
em-n-02132	11/18/02	Clarify where the Time Change Event messages are sent and the contents of the BCID.
em-n-02149	11/18/02	Clarifies/corrects language pertaining to the trigger events for some QoS Event Messages.
em-n-02182	11/18/02	Remove Call-Answer and Call-Disconnect Event Messages for CMTS.

Appendix C Acknowledgments

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:

Satish Buddhavarapu, Dave Ensign, Satish Dwarkanath, David Flanagan, Donna Fryer, Anurag Goel, Jim Harbison, Mike Heffner, Mark Jones, Keith Kelly, David McIntosh, Jean-François Mulé, Wes Porter, Paramesh Santanam, Robert Sayko, Esfira Slutsman, Jim Wilburn, Bill Willcox, Jian Zhang, SunJae Yi, and Daniel Luu.

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

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