# Building a PacketCable™ Network: A Comprehensive Design for the Delivery of VoIP Services

SCTE Cable Tec-Expo® 2002

David McIntosh
Cable Television Laboratories
Project Manager, Telecommunication Architectures
400 Centennial Parkway
Louisville, CO  80027
303-664-8184
d.mcintosh@cablelabs.com

# Table of Contents



# Table of Figures

## Introduction

The cable plant has experienced significant upgrades in the past several years allowing for the delivery of advanced broadband services. Two CableLabs® projects played an important role in the development of these upgrades. The DOCSIS™ specification laid the groundwork for the delivery of advanced broadband services. PacketCable™ defines an IP-based service delivery architecture that overlays the DOCSIS 1.1 infrastructure. While Voice over IP (VoIP) is the first service considered for the PacketCable platform, a wide variety of beyond-voice services will also be supported, including services such as unified messaging, interactive gaming, and videoconferencing. The end-to-end architecture as designed[1][6], offers a complete system that includes: provisioning, signaling, event messaging, configuration management, quality of service (QoS), and security. These functions are managed by specific servers and network endpoints that when combined, collectively build a PacketCable network.

This paper is centered on what it takes to build a PacketCable network, with a focus on the variety of headend servers that manage all aspects of service delivery for on-net as well as off-net IP sessions. It will also profile the architecture designed for event messages.

Headend servers serve as the core of a PacketCable network, configured to interoperate through the use of open and standardized interfaces. The collection of servers overlayed on the DOCSIS 1.1 infrastructure brings together the HFC access network's PacketCable subscriber; the cable operator's managed IP network; and gateways that interface public switched telephone network (PSTN) trunks and the signaling system number 7 (SS7) network.

The PacketCable interfaces are specified and standardized to give vendors and cable operators maximum flexibility in the design and interoperability of products and networks. A prime example of such an interface is the one used for event messaging (EM). An operator has a keen interest in billing for service, and consequently the EM protocol describes several mechanisms between key components that permit the capture and storage of network activity for service billing.

The paper concludes with a short description of security, an acknowledgement of the North American and International standardization of PacketCable, and a look at the evolution of the network.

## PacketCable Architectural Overview

The PacketCable architecture started out as a multimedia service delivery platform with an early focus on optimizations to support an IP emulation of the PSTN for delivery of residential VoIP services. This focus on residential services can be seen as the logical progression of cable operator's initial cable television penetration into the residential market and the opportunity presented by the rollout of the cable modem. VoIP for the local access market focused on residential customers as opposed to small office-home office (SOHO) or business customers can be viewed as an appropriate evolution of the broadband capabilities of cable operator's service offerings. PacketCable in its initial form is a phone-to-phone service offering rather than a personal computer-based telephony. Also, just as in the same way when a cell phone battery goes dead, some configurations of PacketCable may not work when the power goes out. Whether the service includes the lifeline, always-on capability of the PSTN is a business decision of the provider.

A key function of service delivery in PacketCable is billing. The architecture is designed to accommodate mechanisms that track and record access network resource usage information that ultimately generates billing revenue for the cable operator.

The PacketCable architecture, pictured in Figure 1, leverages the services of DOCSIS 1.1 to integrate three networks: the Hybrid Fiber Coaxial (HFC) access network, the managed IP network, and the PSTN. The cable modem termination system (CMTS) uses the Data Over Cable Service Interface Specification (DOCSIS) 1.1 protocol on the shared HFC access network to manage sessions with cable modems. The multimedia terminal adapter (MTA), PacketCable's adjunct to the cable modem, provides the services on top of IP and is designed to be either a separate standalone device or to be embedded within the cable modem. The CMTS also provides connectivity between the HFC access network and the managed IP network. The managed IP network provides interconnection between the basic PacketCable functional components responsible for signaling, media, provisioning, and QoS establishment. In addition, the managed IP network provides long-haul IP connectivity between other managed IP and DOCSIS HFC networks or the gateways to the PSTN.

The advantages of DOCSIS 1.1 for this architecture include two key improvements over DOCSIS 1.0: first, there are now tiered services for quality of service delivery, and second, there is enhanced security in the form of device authentication of a cable modem (CM) on the net, secure software download, and privacy on the HFC between the CMTS and each CM

## *Prepare the Network*

The PacketCable network builds on top of the cable operators HFC plant, specifically the DOCSIS 1.1 infrastructure and associated endpoints of the CM via the cable operator's managed IP network. By adding PacketCable functionality to the subscribers CM and the cable operators IP network, a new range of service are opened up; e.g., Voice over IP or videoconferencing to name two. This is accomplished through the deployment of a PacketCable-ready CM at the subscribers home and the addition of IP servers in the cable headend for call processing, provisioning, quality of service, security, record-keeping, and PSTN access.

## *Upgrade the Access Network*

The HFC network must be upgraded for two-way interactive communication; however, this overhaul is largely complete, allowing for rapid penetration of CM and PacketCable services. The subscriber's CM will be upgraded either through a swap out with one that now includes DOCSIS 1.1 and an embedded PacketCable MTA or a DOCSIS 1.1 CM and a standalone MTA. The cable operator's CMTS is upgraded to DOCSIS 1.1 allowing for tiered services and a more secure access network environment.

### *Install Gateways*

PacketCable allows MTAs to interoperate with the legacy PSTN through gateways. This interconnection to the PSTN is a combination of a media gateway controller (MGC), media gateway (MG), and signaling gateway (SG). The SG exchanges ISUP (ISDN User Part) and transaction capabilities applications part (TCAP) messages with the PSTN SS7 network.

There also is a hybrid gateway solution that takes advantage of the legacy PSTN switch. This architecture uses PacketCable on the access side of the network and circuit switch call control derived from a PSTN local digital switch location. The crossover between the packet- and circuit-based communications takes place at the IP digital terminal (IPDT) hosted by the MSO. The advantage of this solution is that is serves as a bridge to a full IP based network allowing for the PSTN switch as presently configured to handle the lions share of provisioning, billing, operator, and emergency services. It also allows the switch to be fully amortized in the process of migration to a PacketCable network.

## Building the Headend for Distributed Call Processing

The PacketCable architecture is defined in terms of functional components and protocol interfaces which may be combined to create differentiated product offerings. These components, shown below in Figure 1, build a fully functioning PacketCable network.

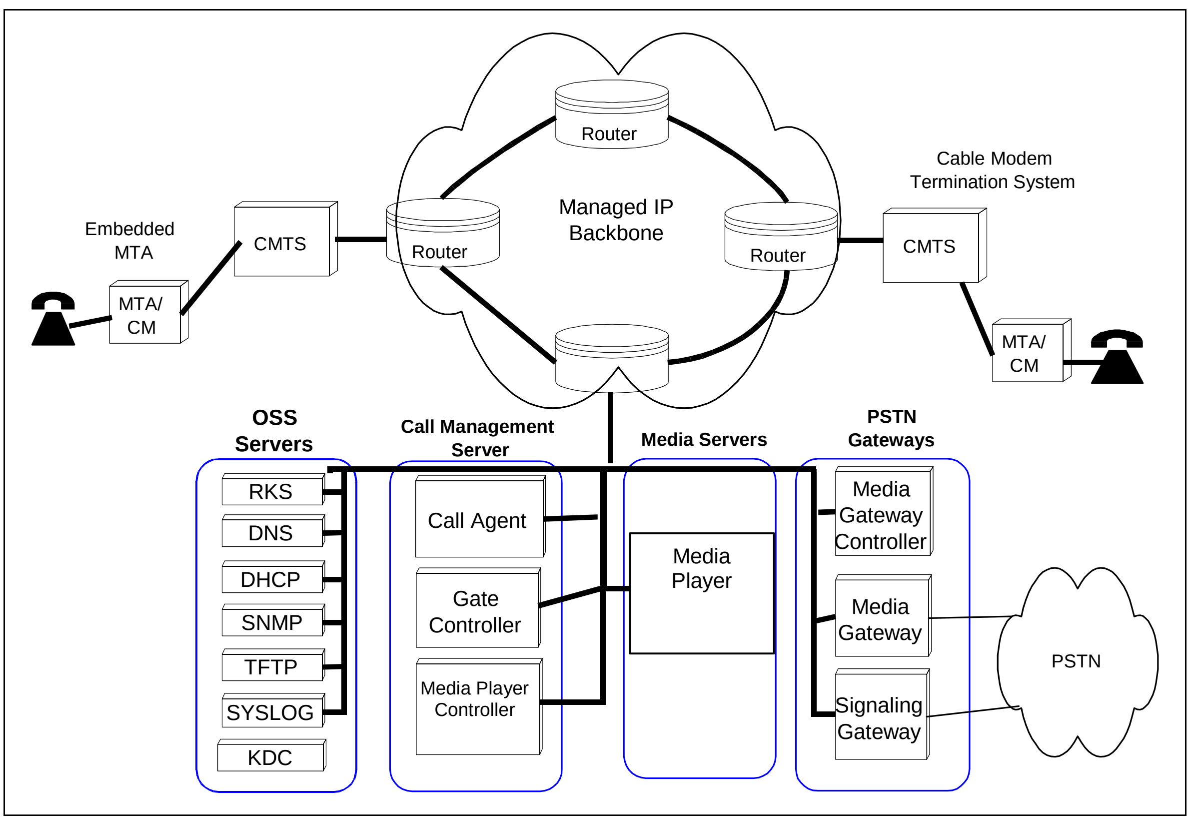


***Figure 1: PacketCable Network Component Reference Model***

### *Call Management Server*

The Call Management Server (CMS) is a key component that provides call control and signaling related services for the MTA, CMTS, and PSTN gateways in the PacketCable network. The CMS is composed of a call agent (CA) and a gate controller (GC). The CA instructs the MTA to look for certain events, such as off-hook, or to play certain signals such as dialtone. The GC component performs QoS admission control. It communicates with the CMTS to either admit or deny requests for QoS generated by the MTA.

### *Operational Support Systems*

Operational support systems (OSS) contain a variety of supporting servers and infrastructure functions that build a fully functioning PacketCable network. The OSS's main functional areas are fault management, performance management, security management, accounting management, and configuration management. Associated components include provisioning servers, record keeping servers (RKS) for billing, key distribution center (KDC) for security, and domain name service (DNS) for name resolution, etc. Here are brief descriptions of some of the more prominent OSS components as shown in Figure 1:

#### Provisioning Servers

There are two kinds of provisioning in PacketCable, one on the IP side of the network and one for PacketCable specific components. PacketCable defines a limited set of OSS functional components and interfaces to support, e.g., MTA device provisioning, event messaging to carry billing information, and security for authentication and key management.

On the IP side, the dynamic host configuration protocol server (DHCP) is used during the MTA device provisioning process, DNS is used to map between IP addresses and ASCII domain names. The trivial file transfer protocol server (TFTP) or the hypertext transfer protocol server (HTTP) is used during the MTA device provisioning process to download configuration files to the MTA. Additionally, a SYSLOG server is used to collect events, such as traps and errors, from an MTA.

#### Security Servers

Security management touches the PacketCable architecture at each component and at each interface. Security services build on top of DOCSIS 1.1 security for the PacketCable applications. The key headend server responsible for security is the KDC. It is utilized as a Kerberos server to manage component authentication, key exchange, and encryption.

#### Record Keeping Servers

The RKS receives PacketCable event messages from the CMS, CMTS, and MGC. It assembles the event messages into coherent sets, or call detail records (CDRs), which are then made available to other back office systems, such as billing, fraud detection, and other systems.

## *Media Servers*

The media server (also known as an audio server) is a logical entity that holds media content for a specific multimedia service. In PacketCable, the media server delivers a subscriber a messages such as; "*the number you have called is no longer in service…*". The media player controller (MPC) requests the media player (MP) to play these network announcements based on call state as determined by the CMS.

## *Additional Architectural Capabilities*

To round out the construction of a PacketCable network, the architecture incorporates capabilities that are fundamental for the delivery of VoIP services. Described below are two of these: dynamic QoS and security. Event messages, also a core capability, are described in detail in the following section.

### Dynamic QoS

An IP-based network is by default a best-effort service. When packets are dropped or delayed in a multimedia architecture that defines acceptable packet loss, latency, and jitter the result is unpredictable end-to-end throughput. QoS is the mechanism that manages the PacketCable service flows[3].

PacketCable splits the resource management of the QoS model into access network and backbone network segments. This approach allows for different bandwidth provisioning and signaling mechanisms for different network segments: the origination side, the far end, and the backbone network. Additionally it allows for resource-constrained segments to manage resource usage and maintain per-flow reservations carefully[5].

### Security

PacketCable security spans all interfaces in the PacketCable architecture[4]. It provides confidentiality for media packets and for signaling communication across the network via authentication, encryption, and key management. It ensures that unauthorized message modification, insertion, deletion and replays anywhere in the network are easily detectable without affecting network operation. Security is interface specific, but the majority of signaling interfaces are secured using IP security (IPSec). The media stream is secured by encrypting and authenticating the payload directly.

PacketCable also defines a corresponding key management mechanism in addition to defining the security protocol that will be applied to each interface. There are three basic key management mechanisms defined for use in PacketCable: Kerberized Key Management, internet key exchange (IKE) with either pre-shared keys or X.509 digital certificates, and randomly generated keys exchanged within secured signaling messages.

# Event Messages in the PacketCable Network

PacketCable uses an event-based approach to the process of capturing information to be used for billing and session accounting[2]. Network elements generate event messages across specified interfaces for the portion of the communication pertaining to them. These interfaces are shown in Figure 2. An event message is a data record containing information about usage and activities. An event-based format is necessary to accommodate the distributed architecture where complete "session state" no longer resides in one or two network elements, but is instead spread across many, e.g. CMS, CMTS, and MGC. For example, the CMTS generates a "start of QoS" message when the CMTS commits access network resources to a PacketCable service.

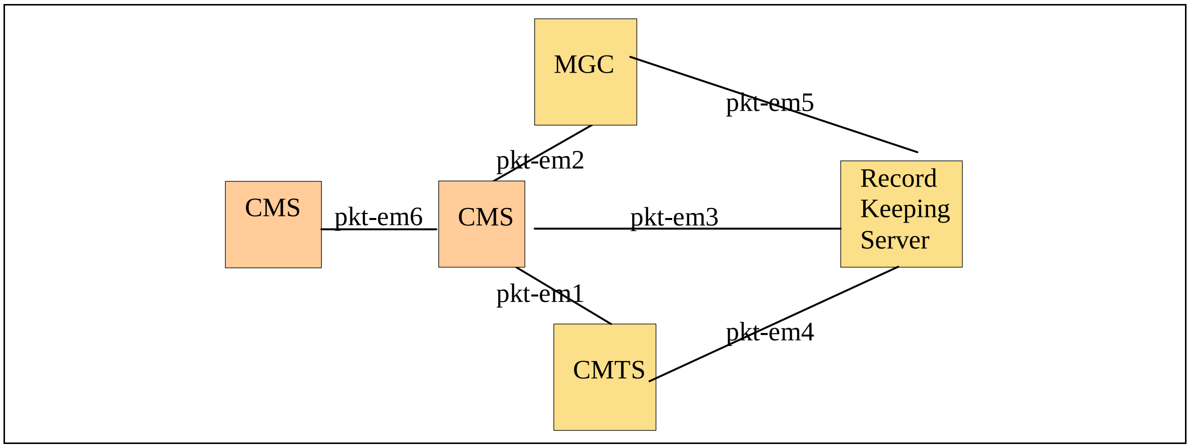


***Figure 2: Event Messages Interfaces***

The PacketCable architecture provides a QoS-enabled IP-based service delivery platform for voice and other multimedia services. The framework of PacketCable Event Messages provides a mechanism for tracking access network resources that have been requested and consumed by these services. This tracking or usage information can be used by back office systems for many purposes including billing, settlements, network usage monitoring, and fraud management.

A single EM framework has been defined to support a variety of service-delivery scenarios and network topologies. For example, the framework supports tracking information for services that either originate or terminate on the PSTN, as well as services that stay on the cable operator's network. This framework is designed to be flexible and extensible enough to support not only the initial suite of PacketCable voice services but also to accommodate beyond-voice services anticipated in the future.

## *Event Message Concepts*

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 RKS, information contained in multiple event messages provides a complete record of the service. Event messages are collected and are sent to one or more back office applications such as a billing system, a fraud detection system, or a pre-paid services processor.

*Originating/Terminating Model* - PacketCable makes use of an "originating/terminating model" based on the PSTN "half-call model." In this model, the originating party's service provider is responsible for tracking information sufficient to bill the originating party for service, and to settle with the terminating provider.  The terminating party's service provider has the same responsibility for the terminating party.  This "originating/terminating model" supports the various PacketCable network topologies.

*Batch vs. real time* - PacketCable allows Event Messages to be sent to the RKS as they are generated.  Alternatively, once generated, Event Messages may be stored on the CMS/CMTS/MGC and sent to the RKS in a single file.

*Call Detail Records* - Using the unique billing correlation ID (BCID) assigned to a given call, the RKS collects all the individual Event Messages for that call, and assembles them into a single call detail record.  The format of the CDR may be AMA, BAF, IPDR, or any format appropriate for the billing and other back-office servers that will make use of the information.

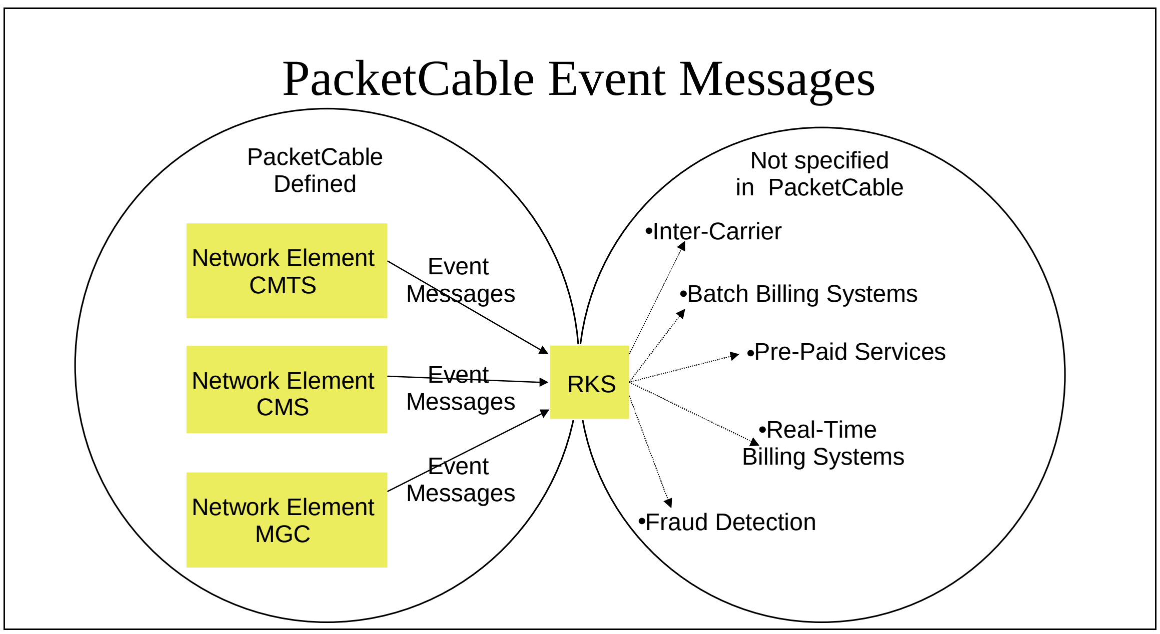


***Figure 3:  Event Messages Architecture***

Figure 3 depicts the PacketCable Event Message architecture. By standardizing the transport, syntax, and collection of appropriate Event Message attributes from a distributed set of network elements (CMS, CMTS, MGC), this architecture provides a single repository (RKS) to interface with billing, settlement, reconciliation, and other systems.

## Multimedia Evolution

Multimedia services will move PacketCable beyond the charter of its initial set of VoIP specifications.  Multimedia will specify an architecture and service delivery platform that extracts the QoS and policy infrastructure of the initial PacketCable specifications.  It will make these capabilities available in a standard way to non-voice services requiring better-than-best-effort treatment on the access network. The full voice architecture will not be a prerequisite to the deployment of multimedia services, but rather a cable operator may choose to deploy either voice or multimedia services, with the assurance that both architectures will seamlessly coexist.

## Specifications and Standards

The comprehensive nature of the PacketCable network is the result of a suite of Technical Reports and Specifications that delineate the end-to-end architecture and associated interfaces for a complete IP applications system. These Technical Reports and Specifications (available at www.packetcable.com) have been accepted as standards by several North American and International standards organizations including the Society of Cable Telecommunications Engineers (SCTE), American National Standards Institute (ANSI), and the International Telecommunications Union (ITU)

## Conclusion

The PacketCable architecture described in this paper leverages improvements made in the cable plant to build an advanced IP platform for the delivery of VoIP services. The architecture has been framed as three networks coordinated through a collection of headend servers. and supported by core capabilities such as dynamic QoS and security. This construction is guided by a comprehensive and advanced set of interoperable specifications that outline functions and capabilities fundamental to the reliable, efficient delivery of IP-based services.

The PacketCable Event Messages framework has been detailed as a flexible and extensible model that enables VoIP billing, settlements, and other back office functions. This event messages framework will be expanded along with other PacketCable capabilities to keep pace with IP services beyond VoIP.

## References


[1] *"PacketCable 1.0 Architecture Framework Technical Report*", PKT-TR-ARCH-V01-991201, December 1, 1999, CableLabs, www.packetcable.com

[2] *"PacketCable Event Messages Specification,*" PKT-SP-EM-I03-011221, December 21, 2001, CableLabs, www.packetcable.com

[3] "*PacketCable Dynamic Quality-of-Service Specification*,"PKT-SP-DQOS-I03-020116, January 16, 2002, CableLabs, www.packetcable.com

[4] *"PacketCable Security Specification,"* PKT-SP-SEC-I05-020116 January 16, 2002, CableLabs, www.packetcable.com

[5] *"Quality-of-Service: A DOCSIS/PacketCable™ Perspective"*, Venkatesh Sunkad and Majid Chelehmal, Proceedings of SPIE Volume: 4522, pgs. 87-98, July 2001.

[6] *"The PacketCable Architecture"*, Ed Miller, Flemming Andreasen, and Glenn Russell, IEEE Communications Interactive, June 2001, www.ieee.org