PacketCable™ 1.0 Architecture Framework Technical Report

PKT-TR-ARCH-V01-991201

Notice

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

Abstract

This technical report describes the architecture framework for PacketCable™ networks including all major system components and network interfaces necessary for delivery of PacketCable services. The intended audience for this document includes developers of equipment intended to be conformant to PacketCable specifications, and network architects who need to understand the overall PacketCable architecture framework.

Document Status Sheet

Document Control Number:	PKT-TR-ARCH-V01-991201
Document Title:	PacketCable™ 1.0 Architecture Framework Technical Report
Revision History:	D01-991201: release
Date:	December 1, 1999

TABLE OF CONTENTS

Figures

Tables

1 INTRODUCTION

1.1 PacketCable Overview

PacketCable™ is a project conducted by Cable Television Laboratories, Inc. (CableLabs®) and its member companies. The PacketCable project is aimed at defining interface specifications that can be used to develop interoperable equipment capable of providing packet-based voice, video and other high-speed multimedia services over hybrid fiber coax (HFC) cable systems utilizing the DOCSIS protocol. PacketCable utilizes a network superstructure that overlays the two-way data-ready broadband cable access network. While the initial PacketCable offering will be packet-based voice communications for existing and new cable subscribers, the long-term project vision encompasses a large suite of packet-based capabilities.

The objective of the PacketCable Architecture Technical Report is to provide a high level reference framework that identifies the functional components and defines the interfaces necessary to implement the capabilities detailed in the individual PacketCable specifications as listed in section 2.3.

1.2 PacketCable Motivation

The emergence of the Internet Protocol (IP) as the standard transport for packet data networks has enabled a revolution in communications service and applications. This online revolution is evidenced by the widespread use of email, chat groups, music, video, and the exponential growth of the World Wide Web, for entertainment, information exchange, online commerce, and a wide range of the new and innovative services. New classes of IP based information appliances are also emerging, including multimedia personal computers, IP based set top boxes, and IP based voice and video phones.

In recent years the growth of a worldwide IP based data network, coupled with the exponential growth in the number of households that have online access, have resulted in an enabling environment for offering integrated voice and data services over a common broadband cable access network and IP transport backbone. While the initial application of IP voice technology was for toll bypass services, particularly high-cost international toll service, the technology has now matured to the point where it is feasible to offer IP-based voice communications services comparable to those offered by telecommunications carriers on the PSTN.

With the success of the DOCSIS standardization effort, the QoS enhancements of DOCSIS 1.1, and the acceleration of major cable system upgrades for two way capacity, the infrastructure is in place for development and deployment of packetized voice and video applications. These applications can be deployed with minimal incremental cost, providing a technically distinctive and cost-effective alternative for subscribers' voice communications needs, as well as a platform for introducing the next generation of voice and other real time multimedia services.

1.3 PacketCable Project Phasing

The PacketCable architecture is designed to be a robust, complete, end-end broadband architecture that supports voice, video, and other multimedia services. The architecture is capable of supporting millions of subscribers over multiple cable operator networks.

It is understood that the initial focus of the PacketCable architecture must support the time-to-market business considerations of CableLabs Member Companies for deploying packet-based services. Going forward, the PacketCable architecture must continue to evolve to meet Member business requirements and to accommodate advances resulting from the maturing of IP-based technology. The PacketCable project will release specifications that define this architecture in a phased approach according to technical feasibility and business priority. As new PacketCable specifications are released, they will complement the previously released specifications.

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 flow," "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.

2 PACKETCABLE 1.0

'PacketCable 1.0' is a CableLabs definition for the first release of specifications that define the PacketCable reference architecture.

In this version of the architecture framework, the emphasis is on specification of the subscriber environment and its interface requirements to the PacketCable network including the DOCSIS HFC access network, Call Management Server, media servers, PSTN gateway, and MTA device provisioning components. The requirements for these functional components and the standardized interfaces between components are defined in detail in the PacketCable 1.0 specifications. In later versions, additional component interfaces will be defined.

PacketCable 1.0 consists of a variety of functional components, each of which must work in harmony to create a consistent and cost-effective delivery mechanism for packet-based services. This distributed architecture allows incremental development and deployment of new features and services, leaving room for implementation flexibility and product innovation. A key focus of the initial PacketCable release is the definition of low-cost subscriber equipment and a network architecture that supports low cost packet-based services. Follow-on phases of this project will continue to add support for advanced subscriber-side functionality. This may require evolution in the PacketCable call signaling, QoS security, provisioning, and billing protocols.

PacketCable allows the use of proprietary vendor-specific solutions for interfaces not defined in specifications. Over time, as additional PacketCable interface protocols are defined, these proprietary interfaces will need to be updated in order to be compliant with PacketCable specifications.

2.1 PacketCable Architecture Framework

At a very high level, the PacketCable 1.0 architecture contains three networks: the "DOCSIS HFC Access Network", the "Managed IP Network" and the PSTN. The Cable Modem Termination System (CMTS) provides connectivity between the "DOCSIS HFC Access Network" and the "Managed IP Network". Both the Signaling Gateway (SG) and the Media Gateway (MG) provide connectivity between the "Managed IP Network" and the PSTN. The reference architecture for PacketCable 1.0 is shown in Figure 1.

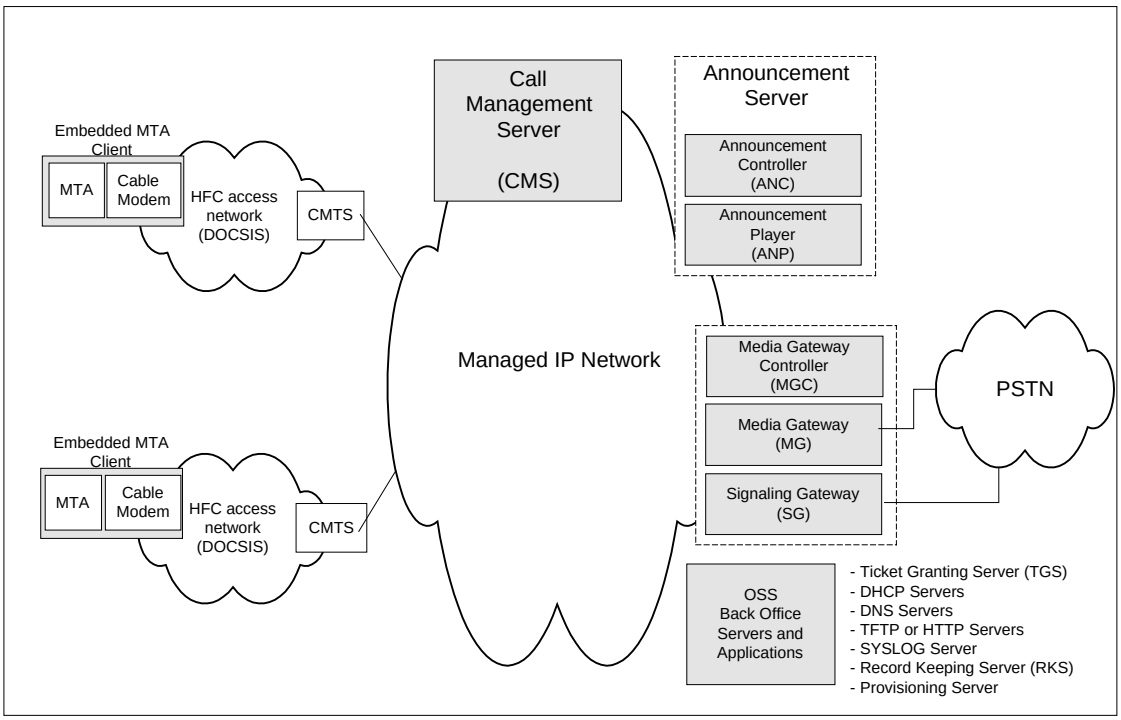

Figure 1. PacketCable Reference Architecture

The DOCSIS HFC access network provides high-speed, reliable, and secure transport between the customer premise and the cable headend. This access network may provide all DOCSIS 1.1 capabilities including Quality of Service. The DOCSIS HFC access network includes the following functional components: the Cable Modem (CM), Multi-media Terminal Adapter (MTA), and the Cable Modem Termination System (CMTS).

The Managed IP network serves several functions. First, it provides interconnection between the basic PacketCable functional components responsible for signaling, media, provisioning, and quality of service establishment. In addition, the managed IP network provides long-haul IP connectivity between other Managed IP and DOCSIS HFC networks. The Managed IP network includes the following functional components: Call Management Server (CMS), Announcement Server (ANS), several Operational Support System (OSS) back-office servers, Signaling Gateway (SG), Media Gateway (MG), and Media Gateway Controller (MGC).

The individual network components that are shown in Figure 1 are described in detail in Section 3.

2.2 PacketCable Zones and Domains

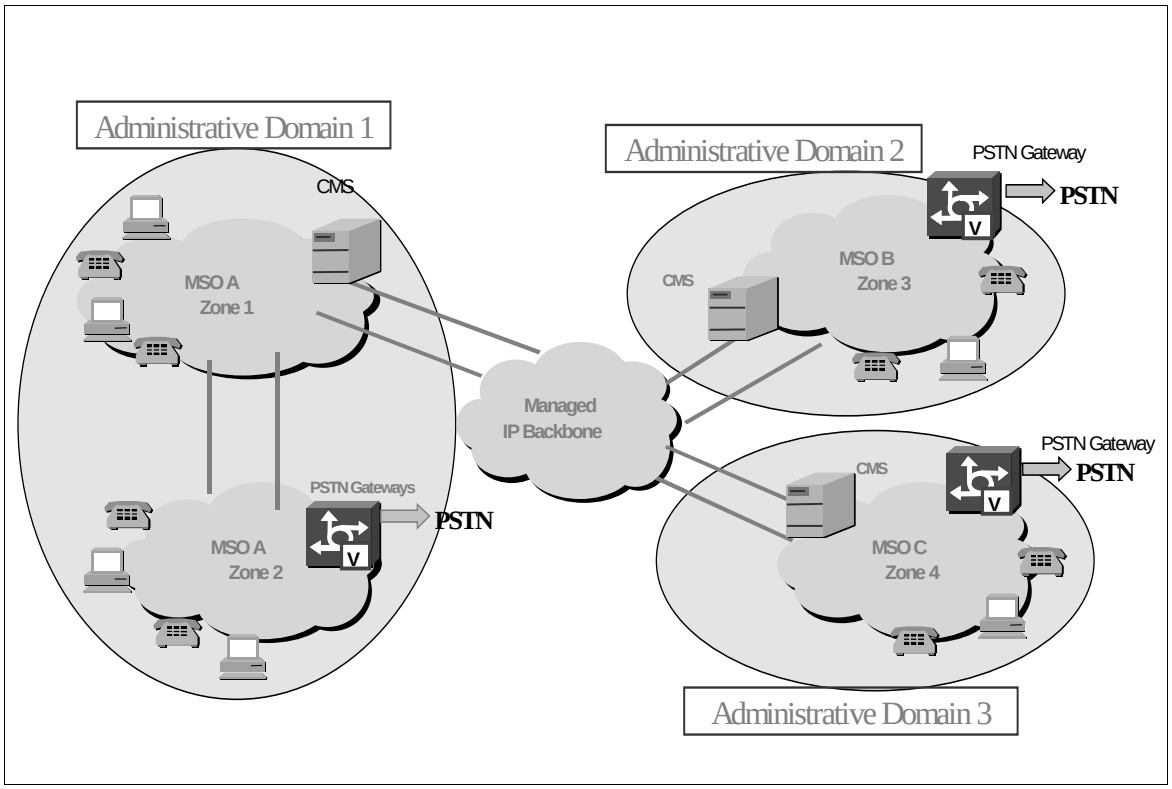

Figure 2. Zones and Administrative Domains

A PacketCable zone consists of the set of MTAs in one or more DOCSIS HFC access networks that are managed by a single functional CMS as shown in Figure 2. Interfaces between functional components within a single zone are defined in the PacketCable 1.0 specifications. Interfaces between zones (e.g., CMS-CMS) have not been defined and will be addressed in future phases of the PacketCable architecture.

A PacketCable domain is made up of one or more PacketCable zones that are operated and managed by a single administrative entity. A PacketCable domain may also be referred to as an administrative domain. Interfaces between domains have not defined in PacketCable 1.0 and will be addressed in future phases of the PacketCable architecture.

2.3 PacketCable 1.0 Specifications

PacketCable 1.0 consists of the eleven Specifications and three Technical Reports shown in Table 1.

Table 1 PacketCable 1.0 Specifications and Reports

PacketCable Specification Reference Number	Specification Name
PKT-SP-CODEC	Audio/Video Codecs
PKT-SP-DQOS	Dynamic Quality-of-Service
PKT-SP-EC-MGCP	Network-Based Call Signaling (NCS)
PKT-SP-EM	Event Messages
PKT-SP-ISTP	Internet Signaling Transport Protocol (ISTP)
PKT-SP-MIBS	MIB Framework
PKT-SP-MIBS-MTA	MTA MIB
PKT-SP-MIBS-NCS	NCS MTA MIB
PKT-SP-PROV	MTA Device Provisioning
PKT-SP-SEC	Security
PKT-SP-TGCP	PSTN Gateway Call Signaling Protocol
PacketCable Technical Report Reference Number	**Technical Report Name**
PKT-TR-CF	Call Flows
PKT-TR-ARCH	Architecture Framework
PKT-TR-OSS	OSS Overview

2.4 PacketCable 1.0 Design Considerations

In order to enable real-time multimedia communications across the cable network infrastructure, PacketCable specifications define protocols in the following areas:

- Call Signaling
- Quality of Service
- Media Stream Transport and Encoding
- Device Provisioning
- Event Messaging
- Security and Privacy
- Operational Support Systems

This section provides an overview of the high-level design goals and concepts used in developing the specifications that define the PacketCable 1.0 reference architecture. Individual PacketCable specifications should be consulted to obtain detailed protocol requirements for each of these areas.

2.4.1 General Architectural Goals

- Enable voice quality capabilities comparable to or better than the PSTN as perceived by the end-user.
- Provide a network architecture that is scalable and capable of supporting millions of subscribers.
- Ensure the one-way delay for local IP access and IP egress (i.e. excluding the IP backbone network) is less than 45ms.
- Support primary and secondary line residential voice communications capabilities.
- Leverage existing protocol standards. PacketCable strives to specify open, approved industry standards that have been widely adopted in other commercial communication networks. This includes protocols approved by the ITU, IETF, IEEE, Telcordia and other communications standards organizations.
- Leverage and build upon the data transport and Quality of Service capabilities provided by DOCSIS.
- Define an architecture that allows multiple vendors to rapidly develop low-cost interoperable solutions to meet Member time-to-market requirements.
- Ensure that the probability of blocking a call can be engineered to be less than 1% during the High Day Busy Hour (HDBH)
- Ensure that call cutoffs and call defects can be engineered to be less than 1 per 10,000 completed calls.
- Support modems (up to V.90 56 kb/s) and fax (up to 14.4 kbps)
- Ensure that frame slips due to unsynchronized sampling clocks or due to lost packets occur less than 0.25 per minute.

2.4.2 Call Signaling

- Define a network-based signaling paradigm.
- Provide end-to-end call signaling for the following call models:
    - calls that originate from the PSTN and terminate on the cable network
    - calls that originate on the cable network and terminate on the cable network within a single PacketCable zone
    - calls that originate from the cable network and terminate on the PSTN
- Provide signaling to support custom calling features such as:
    - Call Waiting
    - Cancel Call Waiting
    - Call Forwarding (no-answer, busy, variable)
    - Three-way Calling

- Voice mail Message Waiting Indicator

- Provide signaling to support Custom Local Area Signaling Services (CLASS) features such as:
  - Calling Number Delivery
  - Calling Name Delivery
  - Calling Identity Delivery On Call Waiting
  - Calling Identity Delivery Blocking
  - Anonymous Call Rejection
  - Automatic Callback
  - Automatic Recall
  - Distinctive Ringing/Call Waiting
  - Customer Originated Trace
- Support a signaling paradigm consistent with existing IP telephony standards for use within a cable operator's PacketCable network and when connecting to the PSTN.
- Ability to direct dial any domestic or international telephone number (E.164 address)
- Ability to receive a call from any domestic or international telephone number supported by the PSTN.
- Ensure that a new subscriber retains current phone number via Local Number Portability (LNP)
- Ability to use the IXC of choice for intra-LATA toll (local toll) and inter-LATA (long distance) calls. This includes pre-subscription and "dial-around" (10-1X-XXX).
- Support Call Blocking/Call Blocking Toll restrictions, (e.g. blocking calls to 900-, 976-, etc.)

2.4.3 Quality of Service

- Provide a rich set of policy mechanisms to provide and manage QoS for PacketCable services over the access network.
- Provide admission control mechanisms for both upstream and downstream directions.
- Allow dynamic changes in QoS in the middle of PacketCable calls.
- Enable transparent access to all of the QoS mechanisms defined in DOCSIS 1.1. PacketCable clients need not be aware of specific DOCSIS QoS primitives and parameters.

- Minimize and prevent abusive QoS usage including theft-of and denial-of service attacks. Ensure QoS policy is set and enforced by trusted PacketCable network elements.
- Provide a priority mechanism for 911 and other priority based signaling services.

2.4.4 CODEC and Media Stream

- Minimize the effects that latency, packet-loss, and jitter have on voice-quality in the IP telephony environment.
- Define a minimum set of audio codecs that must be supported on all PacketCable endpoint devices (MTAs). Evaluation criteria for mandatory codecs are selected as those most efficient with respect to voice quality, bandwidth utilization, and implementation complexity.
- Accommodate evolving narrow-band and wide-band codec technologies.
- Specify echo cancellation and voice activity detection mechanisms.
- Support for transparent, error-free DTMF transmission and detection.
- Support terminal devices for the deaf and hearing impaired.
- Provide mechanisms for codec switching when fax and modem services are required.

2.4.5 Device Provisioning and OSS

- Support dynamic and static provisioning of customer premise equipment (MTA and Cable Modem).
- Provisioning changes should not require reboot of MTA.
- Allow dynamic assignment and management of IP addresses for subscriber devices
- Ensure that real-time provisioning and configuration of MTA software does not adversely affect subscriber service.
- Define SNMP MIBs for managing customer premise equipment (MTA).

2.4.6 Security

- Enable residential voice capabilities with the same or higher level of perceived privacy as in the PSTN.
- Provide protection against attacks on the MTA.
- Protect the MSO from various denial of service, network disruption and theft of service attacks.
- Design considerations include confidentiality, authentication, integrity, non-repudiation and access control.

3 PACKETCABLE FUNCTIONAL COMPONENTS

This section describes the functional components present in a PacketCable network. Component descriptions are not intended to define or imply product implementation requirements but instead to describe the functional role of each of these components in the reference architecture. Note that specific product implementations may combine functional components as needed. Not all components are required to be present in a PacketCable Network.

The PacketCable architecture contains trusted and untrusted network elements. Trusted network elements are typically located within a Cable Operator's managed backbone network. Untrusted network elements, such as the CM and MTA, are typically located within the subscriber's home and outside of the MSO's facility.

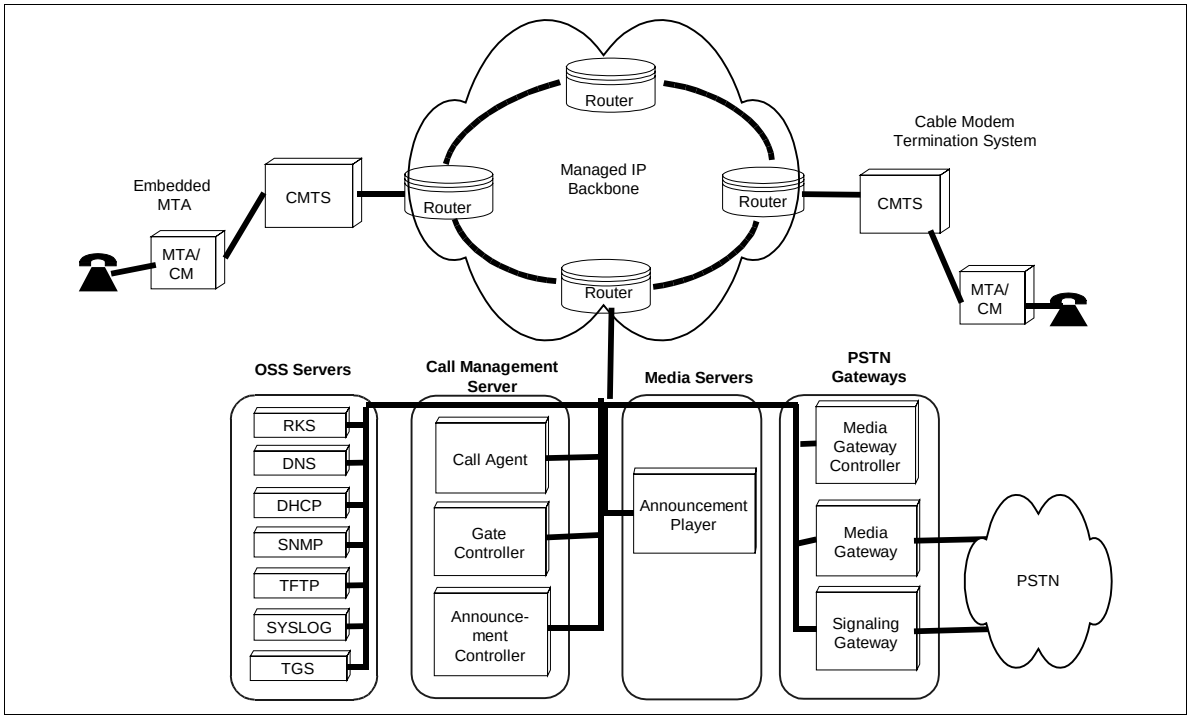

Figure 3. PacketCable Component Reference Model

3.1 Multimedia Terminal Adapter (MTA)

An MTA is a PacketCable client device that contains a subscriber-side interface to the subscriber's CPE (e.g., telephone) and a network-side signaling interface to call control elements in the network. An MTA provides codecs and all signaling and encapsulation functions required for media transport and call signaling.

MTAs reside at the customer site and are connected to other PacketCable network elements via the HFC access network (DOCSIS). PacketCable 1.0 MTAs are required to support the Network Call Signaling (NCS) protocol.

An embedded MTA (E-MTA) is a single hardware device that incorporates a DOCSIS 1.1 cable modem as well as a PacketCable MTA component. Figure 4 shows a representative functional diagram of an E-MTA.

PacketCable 1.0 specifications only require support for embedded MTAs. Throughout this report, unless otherwise noted, the term MTA refers to an embedded MTA.

3.1.1 MTA Functional Requirements

An MTA is responsible for the following functionality:

- NCS call signaling with the CMS
- QoS signaling with the CMS and the CMTS
- Authentication, confidentiality and integrity of some messages between the MTA and other PacketCable network elements
- Mapping media streams to the MAC services of the DOCSIS access network
- Encoding/decoding of media streams
- Providing multiple audio indicators to phones, such as ringing tones, call-waiting tones, stutter dial tone, dial tone, etc.
- Standard PSTN analog line signaling for audio tones, voice transport, caller-id signaling, DTMF, and message waiting indicators
- The G.711 audio codec
- One or more RJ11 analog interface(s) as defined by Bellcore TR-909

Additional MTA functionality is defined in other PacketCable specifications such as NCS Signaling [5], Dynamic Quality-of-Service [4], Audio-Video Codecs [3], MIBS [8][9], and MTA Device Provisioning [12].

3.1.2 MTA identifiers

The following identifiers characterize the E-MTA:

- An embedded MTA has two MAC addresses, one for the cable modem and one for the MTA.
- An embedded MTA has two IP addresses, one for the cable modem and one for the MTA.
- An embedded MTA has two Fully Qualified Domain Names (FQDN), one for the cable modem and one for the MTA
- At least one telephone number per configured physical port
- Device capabilities
- The MTA's associated CMS

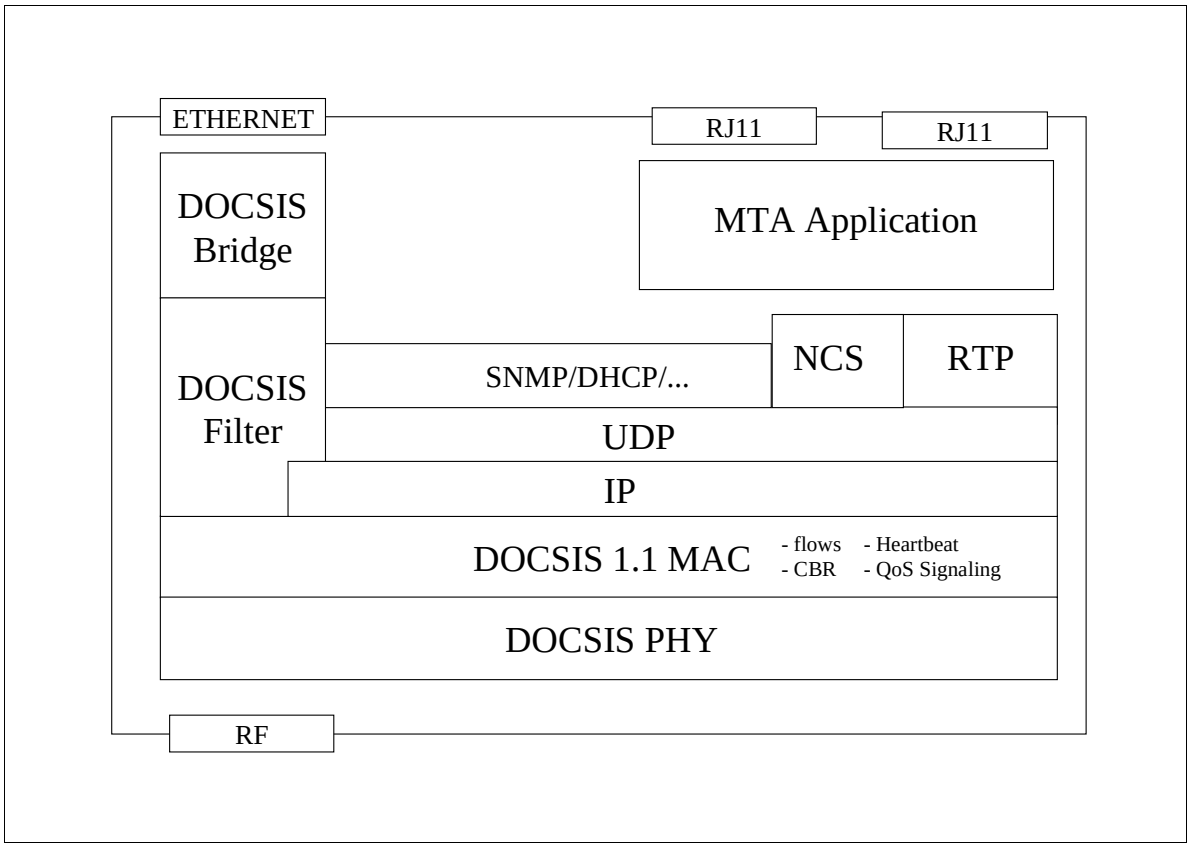

Figure 4. E-MTA Conceptual Functional Architecture

3.2 Cable Modem (CM)

The cable modem (CM) is a network element that is defined in the DOCSIS [19]. The CM is a modulator/demodulator residing on the customer premise that provides data transmission over the cable network using the DOCSIS protocol. In PacketCable, the CM plays a key role in handling the media stream and provides services such as classification of traffic into service flows, rate shaping, and prioritized queuing.

3.3 HFC Access Network

PacketCable-based services are carried over the Hybrid Fiber/Coax (HFC) access network. The access network is a bi-directional, shared-media system that consists of the Cable Modem (CM), the Cable Modem Termination System (CMTS), and the DOCSIS MAC and PHY access layers.

3.4 Cable Modem Termination System (CMTS)

The CMTS provides data connectivity and complimentary functionality to cable modems over the HFC access network (DOCSIS). It also provides connectivity to wide area networks. The CMTS is located at the cable television system head-end or distribution hub.

The CMTS is responsible for the following functions:

- Providing the required QoS to the CM based upon policy configuration.
- Allocating upstream bandwidth in accordance to CM requests and network QoS policies.
- Classifying each arriving packet from the network side interface and assigning it to a QoS level based on defined filter specifications.
- Policing the TOS field in received packets from the cable network to enforce TOS field settings per network operator policy.
- Altering the TOS field in the downstream IP headers based on the network operator's policy.
- Performing traffic shaping and policing as required by the flow specification.
- Forwarding downstream packets to the DOCSIS network using the assigned QoS.
- Forwarding upstream packets to the backbone network devices using the assigned QoS.
- Converting and classifying QoS Gate parameters into DOCSIS QoS parameters.
- Signaling and reserving any backbone QoS necessary to complete the service reservation.
- Recording usage of resources per call using PacketCable Event Messages.

3.4.1 CMTS Gate

The CMTS Gate is a functional component of the CMTS that performs traffic classification and enforces QoS policy on media streams as directed by the Gate Controller (GC).

3.5 Call Management Server (CMS)

The Call Management Server provides call control and signaling related services for the MTA, CMTS, and PSTN gateways in the PacketCable network. The CMS is a trusted network element that resides on the managed IP portion of the PacketCable network.

A PacketCable 1.0 CMS consists of the following logical PacketCable components.

Call Agent (CMS/CA) – Call Agent is a term that is often used interchangeably with CMS, especially in the MGCP. In PacketCable, the Call Agent (CA) refers to the control component of the CMS that is responsible for providing signaling services using the NCS protocol to the MTA. In this context, Call Agent responsibilities include but are not limited to:

- Implementing call features
- Maintaining call progress state
- The use of codecs within the subscriber MTA device

- Collecting and pre-processing dialed digits
- Collecting and classifying user actions

Gate Controller (CMS/GC) – The Gate Controller (GC) is a logical QoS management component within the CMS that coordinates all quality of service authorization and control. Gate Controller functionality is defined in the Dynamic Quality of Service specification.

The CMS may also contain the following logical components:

Media Gateway Controller - The MGC is logical signaling management component used to control PSTN Media Gateways. The MGC function is defined in detail later in this section.

Announcement Controller - The ANC is a logical signaling management component used to control network announcement servers. The ANC function is defined in detail in Section 3.8.

The CMS may also provide the following functions:

- Call management and CLASS features
- Directory Services and Address translation
- Call routing
- Record usage of local number portability services
- Zone-to-Zone call signaling and QoS admission control

For the purposes of this specification, protocols that implement the functionality of the CMS are specified as terminating at the CMS – actual implementations may distribute the functionality in one or more servers that sit "behind" the Call Management Server.

3.6 PSTN Gateway

PacketCable allows MTA's to inter-operate with the current PSTN through the use of PSTN Gateways.

In order to enable operators to minimize cost and optimize their PSTN interconnection arrangements, the PSTN Gateway is decomposed into three functional components:

- **Media Gateway Controller (MGC)** – The MGC maintains the call state and controls the overall behavior of the PSTN gateway.
- **Signaling Gateway (SG)** – The SG provides a signaling interconnection function between the PSTN SS7 signaling network and the IP network.
- **Media Gateway (MG)** – The MG terminates the bearer paths and transcodes media between the PSTN and IP network.

3.6.1 Media Gateway Controller (MGC)

The Media Gateway Controller (MGC) receives and mediates call-signaling information between the PacketCable network and the PSTN. It maintains and controls the overall call state for calls requiring PSTN interconnection.

The MGC controls the MG by instructing it to create, modify, and delete connections that support the media stream over the IP network. The MGC also instructs the MG to detect and generate events and signals such as continuity test tones for ISUP trunks, or MF signaling for MF trunks. Each trunk is represented as an endpoint.

The following is a list of functions performed by the Media Gateway Controller:

- **Call Control Function** – maintains and controls the overall PSTN Gateway call state for the portion of a call that traverses the PSTN Gateway. The function interfaces with external PSTN elements as needed for PSTN Gateway call control, e.g., by generating TCAP queries.
- **PacketCable Signaling** – terminates and generates the call signaling from and to the PacketCable side of the network.
- **MG Control** – The MG Control function exercises overall control of endpoints in the Media Gateway:
  - Event Detection instructs the MG to detect events, e.g., in-band tones and seizure state, on the endpoint and possibly connections.
  - Signal Generation instructs the MG to generate in-band tones and signals on the endpoint and possibly connections.
  - Connection Control instructs the MG on the basic handling of connections from and to endpoints in the MG.
  - Attribute Control instructs the MG regarding the attributes to apply to an endpoint and/or connection, e.g., encoding method, use of echo cancellation, security parameters, etc.
- **External Resource Monitoring –** maintains the MGC's view of externally visible MG resources and packet network resources, e.g. endpoint availability.
- **Call Routing –** makes call routing decisions.
- **Security –** ensures that any entity communicating with the MGC adheres to the security requirements.
- **Usage Recording via Event Messages –** records usage of resources per call.

3.6.2 Media Gateway (MG)

The Media Gateway provides bearer connectivity between the PSTN and the PacketCable IP network. Each bearer is represented as an endpoint and the MGC instructs the MG to set-up and control media connections to other endpoints on the PacketCable network. The MGC also instructs the MG to detect and generate events and signals relevant to the call state known to the MGC.

3.6.2.1 Media Gateway Functions

The following is a list of functions performed by the Media Gateway:

- Terminates and controls physical circuits in the form of bearer channels from the PSTN.
- Discriminates between media and Channel Associated In-band signaling information from the PSTN circuit.
- Detects events on endpoints and connections as requested by the MGC. This includes events needed to support in-band signaling, e.g., MF.
- Generates signals on endpoints and connections, e.g., continuity tests, alerting, etc. as instructed by the MGC. This includes signals needed to support in-band signaling.
- Creates, modifies, and deletes connections to and from other endpoints as instructed by the MGC.
- Controls and assigns internal media processing resources to specific connections upon receipt of a general request from the Media Gateway Controller.
- Performs media transcoding between the PSTN and the PacketCable network. This includes all aspect of the transcoding such as codecs, echo cancellation, etc.
- Ensures that any entity communicating with the MG adheres to the security requirements.
- Determines usage of relevant resources and attributes associated with those resources, e.g., number of media bytes sent and received.
- Reports usage of resources to the MGC.

3.6.3 Signaling Gateway (SG)

The Signaling Gateway function sends and receives circuit-switched network signaling at the edge of the PacketCable network. For PacketCable 1.0, the signaling gateway function only supports non-facility associated signaling in the form of SS7. Facility associated signaling in the form of MF is supported by the MG function directly.

3.6.3.1 SS7 Signaling Gateway Functions

The following is a list of functions performed by the Signaling Gateway function:

- Terminates physical SS7 signaling links from the PSTN (A, F links).
- Implements security features, to ensure that the Gateway security is consistent with PacketCable and SS7 network security requirements.
- Terminates Message Transfer Part (MTP) level 1, 2 and 3.
- Implements MTP network management functions as required for any SS7 signaling point.

- Performs ISUP Address Mapping to support flexible mapping of Point Codes (both Destination Point Code and Origination Point Code) and/or Point Code/CIC code combination contained within SS7 ISUP messages to the appropriate Media Gateway Controller (MGC) (either a domain name or an IP address). The addressed MGC will be responsible for controlling the Media Gateway, which terminates the corresponding trunks.
- Performs TCAP Address Mapping to map Point Code/Global Title/SCCP Subsystem Number combinations within SS7 TCAP messages to the appropriate Media Gateway Controller or Call Management Server.
- Provides mechanism for certain trusted entities ("TCAP Users") within the PacketCable network, such as Call Agents, to query external PSTN databases via TCAP messages sent over the SS7 network.
- Implements the transport protocol required to transport the signaling information between the Signaling Gateway and the Media Gateway Controller.

3.7 OSS Back Office Components

The OSS back office contains business, service, and network management components supporting the core business processes. As defined by the ITU TMN framework, the main functional areas for OSS are fault management, performance management, security management, accounting management, and configuration management. These topics are covered in detail in the PacketCable OSS Framework Technical Report [15].

PacketCable 1.0 defines a limited set of OSS functional components and interfaces to support MTA device provisioning and Event Messaging to carry billing information.

3.7.1 TGS

For PacketCable, the term TGS (Ticket Granting Server) is utilized for a Kerberos server. The Kerberos protocol with the public key PKINIT extension is used for key management on the MTA-CMS interface [37].

The TGS grants Kerberos tickets to the MTA. A ticket contains information used to set up authentication, privacy, integrity and access control for the call signaling between the MTA and the CMS. This ticket is issued in three different scenarios.

- During device provisioning, the MTA requests a ticket from the TGS. It is strongly recommended that the MTA save Kerberos tickets in persistent storage. In the case when the MTA reboots, if the saved ticket is still valid, then the MTA will not need to execute the PKINIT to request a new ticket from the TGS.
- In normal operation, each time a ticket expires, the MTA will request a new ticket during the grace period from the TGS. Note: In the case of power failure in the CMS, the MTA will no longer be associated with this CMS. When this CMS restarts it will request "wake up" information from the MTA. If the ticket the MTA currently holds is beyond the expiration time, often referred to as a stale ticket, the MTA will request a new ticket from the TGS. If the MTA is still

holding a valid ticket then it should send this ticket to the CMS without requesting a new one from the TGS.

- When the TGS is not available on the network and the MTA can not get a new ticket during the grace period, the MTA must hold on to the current, but stale ticket until a TGS is available to grant a new ticket. The request from the MTA during this condition is specified in the PacketCable Security specification [13].

3.7.2 Dynamic Host Configuration Protocol Server (DHCP)

The DHCP server is a back office network element used during the MTA device provisioning process to dynamically allocate IP addresses and other client configuration information.

3.7.3 Domain Name System Server (DNS)

The DNS server is a back office network element used to map between ASCII domain names and IP addresses.

3.7.4 Trivial File Transfer Protocol Server or HyperText Transfer Protocol Server (TFTP or HTTP)

The TFTP Server is a back office network element used during the MTA device provisioning process to download configuration files to the MTA. An HTTP Server may be used instead of a TFTP server to download configuration files to the MTA.

3.7.5 SYSLOG Server (SYSLOG)

The SYSLOG server is a back office network element used to collect events such as traps and errors from an MTA.

3.7.6 Record Keeping Server (RKS)

The RKS is a trusted network element component that receives PacketCable Event Messages from other trusted PacketCable network elements such as the CMS, CMTS, and MGC. The RKS also, at a minimum, is a short-term repository for PacketCable Event Messages. The RKS may assemble 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.

3.8 Announcement Server (ANS)

An Announcement Server is a network component that manages and plays informational tones and messages in response to events that occur in the network. An Announcement Server (ANS) is a logical entity composed of an Announcement Controller (ANC) and an Announcement player (ANP).

3.8.1 Announcement Controller (ANC)

The ANC initiates and manages all announcement services provided by the Announcement Player. The ANC requests the ANP to play announcements based on call state as determined by the CMS. When information is collected from the end-user by the ANP, the ANC is responsible for interpreting this information and manage the session accordingly. Hence, the ANC may also manage call state.

3.8.2 Announcement Player (ANP)

The Announcement Player is a media resource server. It is responsible for receiving and interpreting commands from the ANC and for delivering the appropriate announcement(s) to the MTA. The ANP also is responsible for accepting and reporting user inputs (e.g., DTMF tones). The ANP functions under the control of the ANC.

4 PROTOCOL INTERFACES

Protocol specifications have been defined for most of the component interfaces in the PacketCable architecture. An overview of each protocol interface is provided within this section. The individual PacketCable specifications should be consulted for the complete protocol requirements.

It is possible that some of these interfaces may not exist in a given vendor's product implementation. For example, if several functional PacketCable components are combined then it is possible that some of these interfaces are internal to that component.

4.1 Call Signaling Interfaces

Call signaling requires multiple interfaces within the PacketCable architecture. These interfaces are identified in Figure 5. Each interface in the diagram is labeled, and further described in the subsequent Table 2.

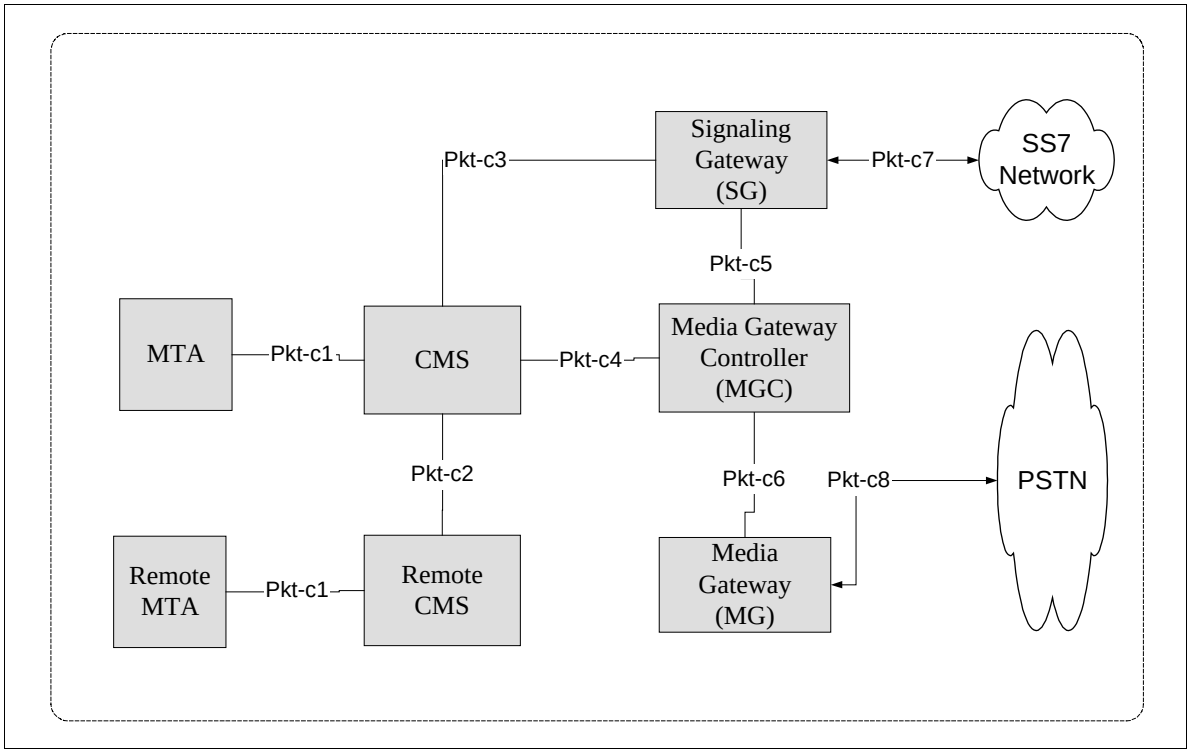

Figure 5. Call Signaling Interfaces

Table 2. Call Signaling Interfaces

Interface	PacketCable Functional Components	Description
Pkt-c1	MTA – CMS	Call signaling messages exchanged between the MTA and CMS using the NCS protocol, which is a profile of MGCP.
Pkt-c2	CMS-CMS	Call signaling messages exchanged between CMS's. The protocol for this interface is undefined in PacketCable 1.0.
Pkt-c3	CMS – SG	Call signaling messages exchanged between CMS and SG using the ISTP/TCAP protocol.
Pkt-c4	CMS – MGC	Call signaling messages exchanged between the CMS and MGC. The protocol for this interface is undefined in PacketCable 1.0
Pkt-c5	SG – MGC	Call signaling messages exchanged between the MGC and SG using the ISTP/ISUP and ISTP/TCAP protocol
Pkt-c6	MGC – MG	Interface for media control of the media gateway and possibly in-band signaling using the TGCP protocol, which is a profile of MGCP, similar to NCS.
Pkt-c7	SG – SS7	The SG terminates physical SS7 signaling links from the PSTN (A, F links). The following protocols are supported: • ISUP User Interface. Provides an SS7 ISUP signaling interface to external PSTN carriers. • TCAP User Interface. Provides mechanism for certain trusted entities ("TCAP Users") within the PacketCable network, such as Call Agents, to query external PSTN databases via TCAP messages sent over the SS7 network.
Pkt-c8	MG – PSTN	This interface defines bearer channel connectivity from the Media Gateway to the PSTN and supports the following call signaling protocols: • In-Band MF Signaling A future version of PacketCable may support ISDN PRI[1].

4.1.1 Network-based Call Signaling (NCS) Framework

The PacketCable Network-Based Call Signaling (NCS) protocol (Pkt-c1) is an extended variant of the IETF's MGCP call signaling protocol. The NCS architecture places call state and feature implementation in a centralized component, the Call Management Server (CMS), and places device control intelligence in the MTA. The MTA passes device events to the CMS, and responds to commands issued from the CMS. The CMS, which may consist of multiple geographically or administratively distributed systems, is responsible for setting up and tearing down calls, providing advanced services [CLASS and custom calling features], performing call authorization, and generating billing event records, etc.

Examples of the partition of function would be for the CMS to instruct the MTA to inform the CMS when the phone goes off hook, and seven DTMF digits have been entered. When this sequence of events occur, the MTA notifies the CMS. The CMS

[1] This function may be viewed as belonging in the Signaling Gateway function.

may then instruct the MTA to create a connection, reserve QoS resources through the access network for the pending voice connection, and also to play a locally generated ringback tone. The CMS in turn communicates with a remote CMS (or MGC) to setup the call. When the CMS detects answer from the far end, it instructs the MTA to stop the ringback tone, activate the media connection between the MTA and the far-end MTA, and begin sending and receiving media stream packets.

By centralizing call state and service processing in the CMS, the service provider is in a position to centrally manage the reliability of the service provided. In addition the service provider gains full access to all software and hardware in the event that a defect that impacts subscriber services occurs. Software can be centrally controlled, and updated in quick debugging and resolution cycles that do not require deployment of field personnel to the customer premise. Additionally, the service provider has direct control over the services introduced and the associated revenue streams associated with such services.

4.1.2 PSTN Signaling Framework

PSTN signaling interfaces are summarized in Table 2 (Pkt-c3 through Pkt-c8). These interfaces provide access to PSTN-based services and to PSTN subscribers from the PacketCable network.

The PacketCable PSTN signaling framework consists of a PSTN gateway that is subdivided into three functional components:

- Media Gateway Controller (MGC)
- Media Gateway (MG)
- Signaling Gateway (SG)

The Media Gateway Controller and Media Gateway are analogous to, respectively, the CMS and MTA in the NCS framework. The Media Gateway provides bearer and in-band signaling connectivity to the PSTN. The Media Gateway Controller implements all the call state and intelligence and controls the operation of the Media Gateway through the TGCP protocol (pkt-c6). This includes creation, modification and deletion of connections as well as in-band signaling information to and from the MG. TGCP is an extended variant of the IETF's MGCP call signaling protocol. The TGCP variant is closely aligned with NCS.

The CMS and the MGC may each send routing queries (e.g., 800 number lookup, LNP lookup) to an SS7 Service Control Point (SCP) via the SG (pkt-c3 and pkt-c5). The MGC, via the SG, also exchanges ISUP signaling with the PSTN's SS7 entities for trunk management and control. The ISTP protocol provides the signaling interconnection service between the PacketCable network call control elements (Call Management Server and Media Gateway Controller) and the PSTN SS7 Signaling network through the SS7 Signaling Gateway. ISTP contains features for initialization; address mapping from the SS7 domain to the IP domain; message delivery for SS7 ISUP and TCAP; congestion management, fault management, maintenance operations; and redundant configuration support. ISTP bridges the gap between basic IP transport mechanisms and application level signaling. Although not a translation of

the SS7 MTP3 and SCCP protocols, ISTP implements analogues to some of the MTP3 and SCCP functions in a fashion appropriate to distributed systems communicating over an IP network. These capabilities allow the IP network to interact with and receive all the services of the PSTN. As service capabilities evolve over time, these same signaling capabilities may be used to support PSTN access to the PacketCable network's own routing and service databases.

4.2 Media Streams

The IETF standard RTP (RFC 1899 - Real-Time Transport Protocol) is used to transport all media streams in the PacketCable network[32]. PacketCable utilizes the RTP profile for audio and video streams as defined in RFC 1990[35].

The primary media flow paths in the PacketCable network architecture are shown in Figure 6 and are further described below.

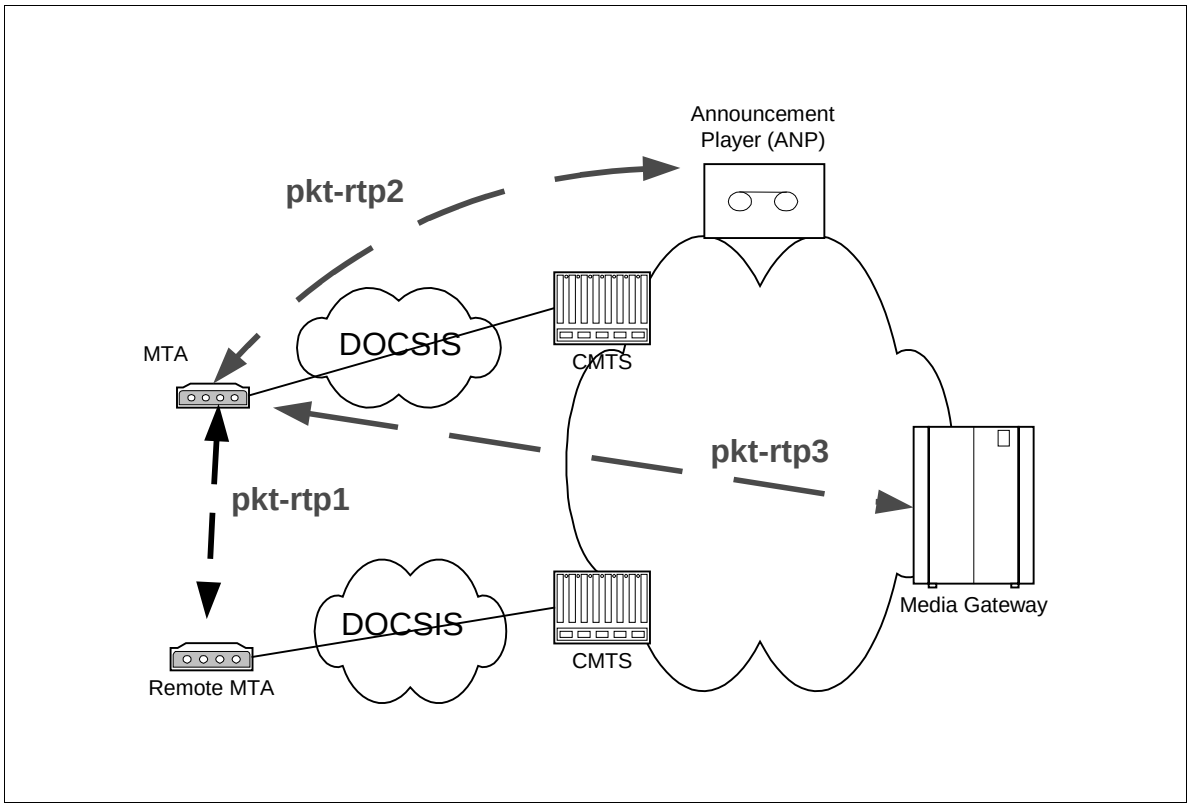

Figure 6. RTP Media Stream Flows in a PacketCable Network

pkt-rtp1: Media flow between MTAs. Includes, for example, encoded voice, video, and fax.

pkt-rtp2: Media flow between the ANP and the MTA. Includes, for example, tones and announcements sent to the MTA by the Announcement Player.

pkt-rtp3: Media flow between the MG and the MTA. Includes, for example, tones, announcements, and PSTN media flow sent to the MTA from the Media Gateway.

RTP encodes a single channel of multimedia information in a single direction. The standard calls for an 8-byte header with each packet. An 8-bit RTP "Payload Type" is defined to indicated which encoding algorithm is used. Most of the standard audio and video algorithms are assigned to particular PT values in the range 0 through 95. The range 96 through 127 is reserved for "dynamic" RTP payload types. The range 128 through 255 is reserved for private administration.

The packet format for RTP data transmitted over IP over Ethernet is depicted in Figure 7 below.

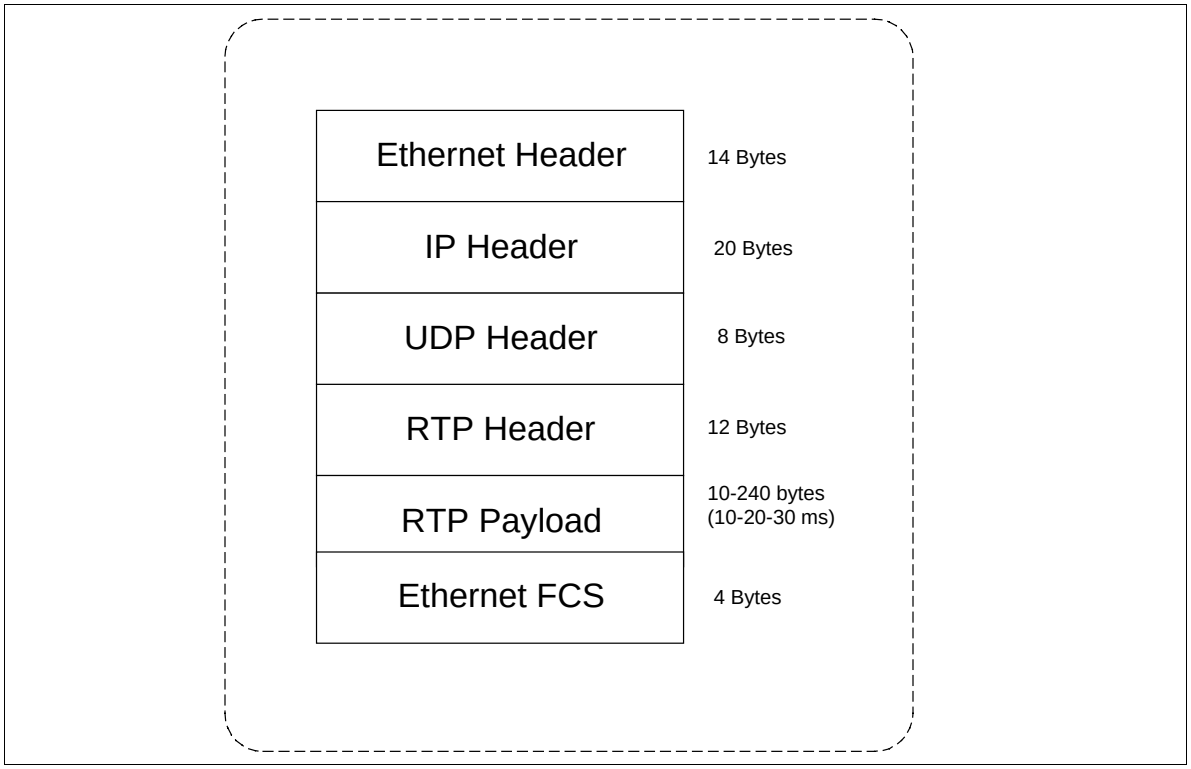

Figure 7. RTP Packet Format

The length of the RTP Payload as well as the frequency with which packets are transmitted depends on the algorithm as defined by the Payload Type field.

RTP sessions are established dynamically by the endpoints involved, so there is no "well-known" UDP port number. The Session Description Protocol (SDP) was developed by the IETF to communicate the particular IP address and UDP port an RTP session is using.

The packet header overhead of Ethernet, IP, UDP, and RTP is significant when compared to a typical RTP Payload size, which can be as small as 10 bytes for packetized voice. The DOCSIS 1.1 specification addresses this issue with a Payload Header Suppression feature for abbreviating common headers.

4.3 MTA Device Provisioning

The scope of MTA Device Provisioning is to enable a MTA to register and provide subscriber services over the HFC network. Provisioning covers initialization, authentication, and registration functions required for MTA device provisioning. The Provisioning Specification [12] also includes attribute definitions required in the MTA configuration file.

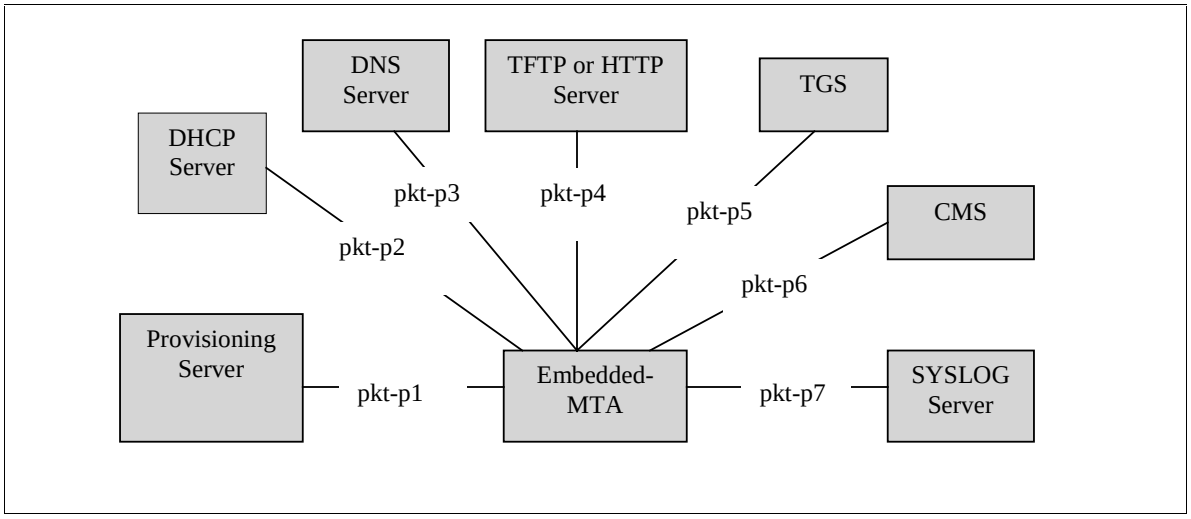

Figure 8. PacketCable Provisioning Interfaces

Table 3 describes the provisioning interfaces shown in the above diagram.

Table 3. Device Provisioning Interfaces

Interface	PacketCable Functional Components	Description
Pkt-p1	MTA-PROV Server	Interface to exchange device capability as well as MTA device and endpoint information between the MTA and Provisioning Server using the SNMP protocol. The MTA also sends notification that provisioning has completed along with a pass/fail status using the SNMP protocol.
Pkt-p2	MTA- DHCP Server	DHCP interface between the MTA and DHCP Server used to assign an IP address to the MTA. If a DNS server is required during provisioning, then the address of this server is also included.
Pkt-p3	MTA – DNS Server	DNS interface between the MTA and DNS Server used to obtain the IP address of a PacketCable server given its fully qualified domain name.
Pkt-p4	MTA – HTTP or TFTP Server	MTA configuration file is downloaded to the MTA from the TFTP Server or HTTP Server.
Pkt-p5	MTA – TGS	MTA obtains a Kerberos ticket from the Ticket Granting Server using the Kerberos protocol.
Pkt-p6	MTA – CMS	MTA establishes an IPSec Security Association with the CMS using the Kerberos protocol.
Pkt-p7	MTA – SYSLOG	MTA sends notification that provisioning has completed along with a pass/fail status to the SYSLOG server via UDP.

4.4 SNMP Element Management Layer Interfaces

PacketCable requires SNMPv3 to interface the MTA to element management systems for MTA device provisioning. SNMPv3 ”traps” and “informs” are supported for event handling, as well as “sets” and “gets” for provisioning. PacketCable MIBs are defined in the MTA MIB specification [8] and the NCS MIB specification [9].

The PacketCable NCS MIB contains Network Call Signaling information for provisioning on both a device and a per endpoint basis. The MTA MIB contains data for device provisioning and for supporting provisioned functions such as event logging. More detailed information on the MIBs framework can be found in the PacketCable MIBs framework specification [10].

4.5 Event Messages Interfaces

4.5.1 Event Message Framework

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

This PacketCable Event Messages specification defines the structure of the Event Message data record and defines RADIUS as the transport protocol. 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. Additional transport protocols may be recommended in future releases of this specification. Although the scope of the specification is limited to defining Event Messages for basic residential voice capabilities, it is expected that this specification will be expanded to support additional PacketCable-based services. Figure 9 shows a representative Event Message architecture.

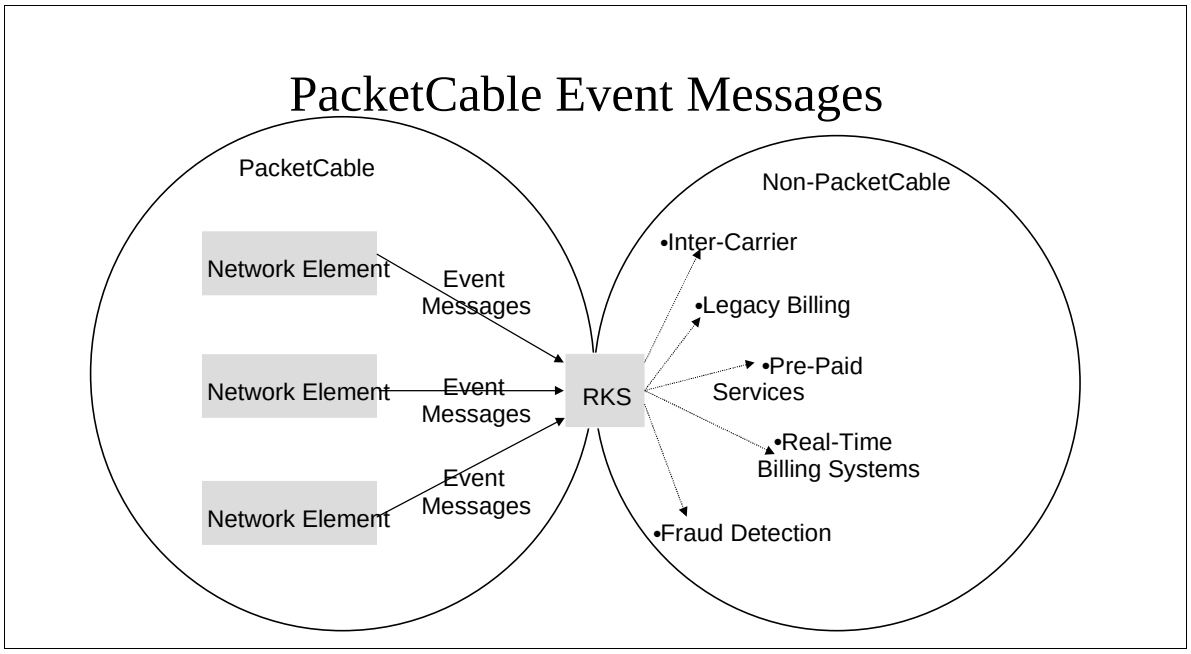

Figure 9. Representative Event Messages Architecture

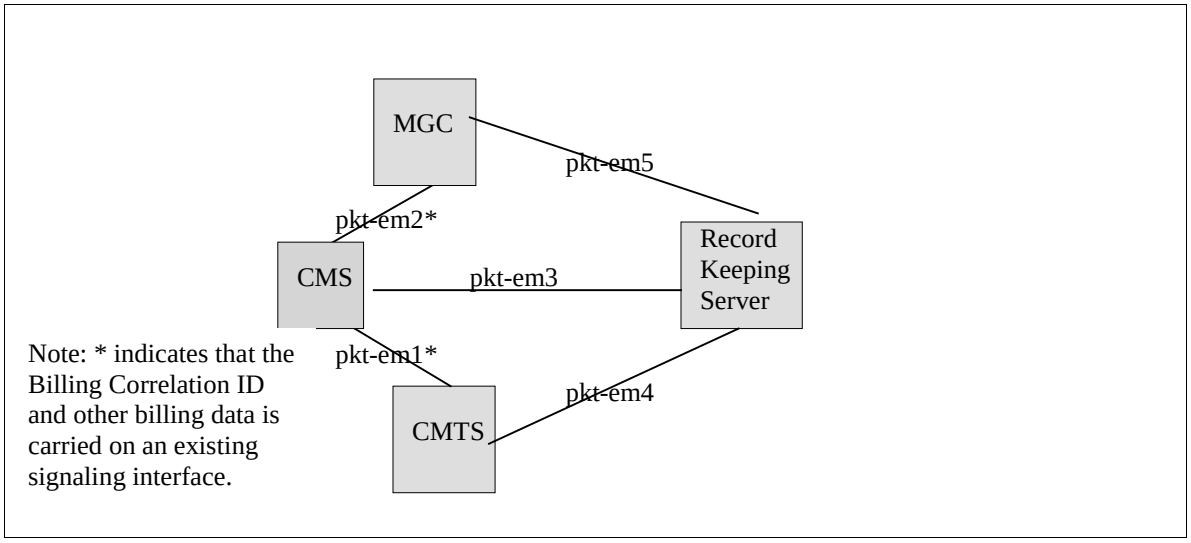

Figure 10. Event Message Interfaces

The following table describes the Event Message interfaces shown in Figure 9.

Table 4. Event Message Interfaces

Interface	PacketCable Functional Component	Description
pkt-em1	CMS-CMTS	DQoS Gate-Set message carrying Billing Correlation ID and other data required for CMTS to send Event Messages to an RKS.
Pkt-em2	CMS-MGC	Vendor-proprietary interface carrying Billing Correlation ID and other data required billing data. Either the CMS or MGC

Interface	PacketCable Functional Component	Description
		may originate a call and therefore need to create the Billing Correlation ID and send this data to the other.
Pkt-em3	CMS-RKS	RADIUS protocol carrying PacketCable Event Messages.
Pkt-em4	CMTS-RKS	RADIUS protocol carrying PacketCable Event Messages.
Pkt-em5	MGC-RKS	RADIUS protocol carrying PacketCable Event Messages.

4.6 Quality-of-Service (QoS)

4.6.1 QoS Framework

Quality of Service signaling interfaces are defined between many of the components of the PacketCable network. Signaling may be handled at the application layer (e.g. SDP parameters), network layer (e.g. RSVP), or the data-link layer (e.g. DOCSIS 1.1 QoS).

From the perspective of the MTA and its access network the PacketCable QoS Framework is represented in Figure 11:

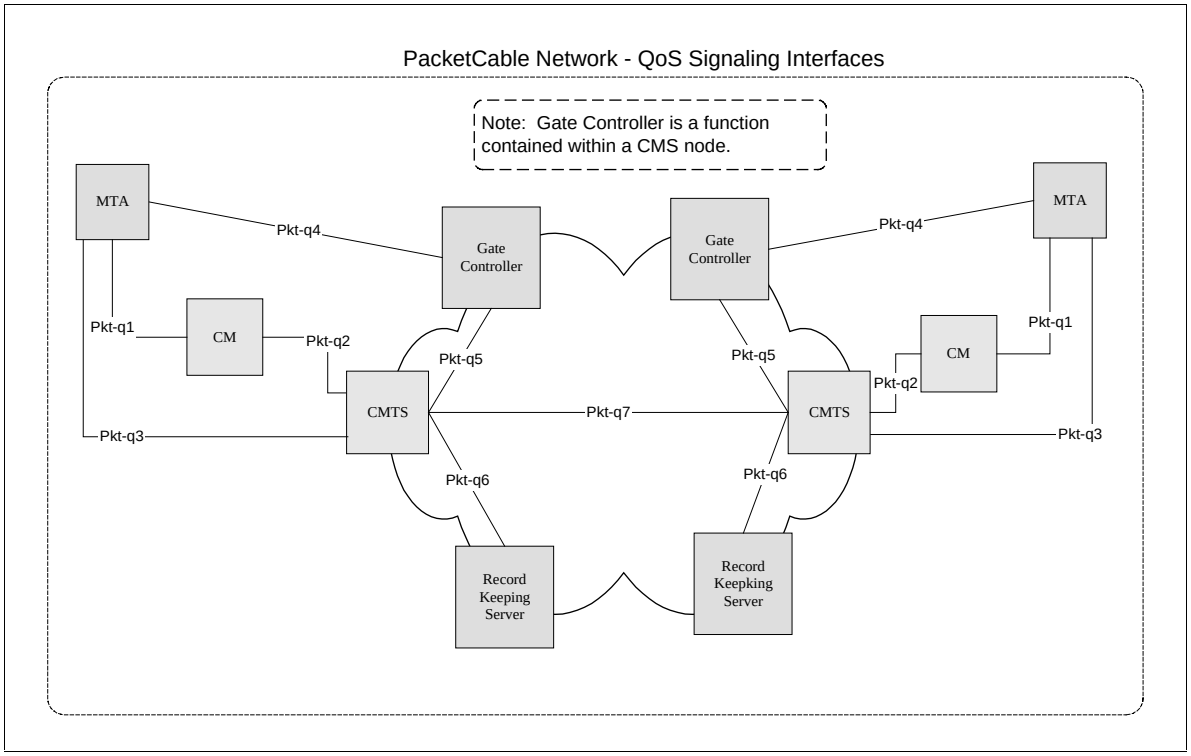

Figure 11. PacketCable QoS Signaling Interfaces

Table 5 briefly identifies each interface and how each interface is used in the Dynamic QoS Specification (DQoS). Two alternatives are shown for this specification: first a general interface that is applicable to either embedded or

standalone MTAs; and second, an optional interface that is available only to embedded MTAs.

Table 5. QoS Interfaces for Standalone and Embedded MTAs

Interface	PacketCable Functional Components	DQoS Embedded/ Standalone MTA	D-QoS Embedded MTA
Pkt-q1	MTA – CM	N/A	E-MTA, MAC Control Service Interface
Pkt-q2	CM – CMTS (DOCSIS)	DOCSIS, CMTS-initiated	DOCSIS, CM-initiated
Pkt-q3	MTA – CMTS	RSVP+[2]	N/A
Pkt-q4	MTA – GC/CMS	NCS/DCS	NCS
Pkt-q5	GC – CMTS	Gate Management	Gate Management
Pkt-q6	CMTS – RKS	Billing	Billing
Pkt-q7	CMTS – CMTS	Gate Management	Gate Management

The function of each QoS interface is further described is defined in Table 6 below.

Table 6. QoS Interfaces

Interface	PacketCable Functional Components	Description
Pkt-q1	MTA – CM	This interface is only defined for the embedded MTA. The interface decomposes into three sub-interfaces: *Control*: used to manage DOCSIS service-flows and their associated QoS traffic parameters and classification rules. *Synchronization*: used to synchronize packet and scheduling for minimization of latency and jitter. *Transport*: used to process packets in the media stream and perform appropriate per-packet QoS processing. The MTA/CM interface is conceptually defined in Appendix E of the DOCSIS RFI specification.
Pkt-q2	CM – CMTS	This is the DOCSIS QoS interface (control, scheduling, and transport). It should be noted that, architecturally, control functions can be initiated from either the CM or the CMTS. However the CMTS is the final policy arbiter and granter of admission into the DOCSIS access network. The following capabilities of the DOCSIS MAC are used within PacketCable: ▪ Multiple service flows, each with its own class of upstream traffic, both single and multiple voice connections per DOCSIS service flow ▪ Prioritized classification of traffic streams to service flows. ▪ Guaranteed minimum/constant bitrate scheduling service ▪ Constant bit rate scheduling with traffic activity detection service

[2] For PacketCable 1.0, only the embedded MTA interfaces as defined in Section 4 of the Dynamic Quality of Service specification are required. The CMTS is not required to support RSVP across the MTA-CMTS interface as defined in DQoS Section 3 [4].

Interface	PacketCable Functional Components	Description
		(slow down, speed up, stop, and restart scheduling) ▪ DOCSIS packet header suppression for increased call density ▪ DOCSIS classification of voice flows to service flow ▪ DOCSIS synchronization of CODEC to CMTS clock and Grant Interval ▪ Two-phase activation of QoS resources ▪ TOS packet marking at network layer ▪ Guarantees on latency and jitter. ▪ Internal sub-layer signaling between PacketCable MTA and DOCSIS (embedded MTA) ▪ This interface is further defined in the DOCSIS RFI specification.
Pkt-q3	MTA – CMTS	The interface is used for request of bandwidth and QoS resources related to the bandwidth. The interface runs on top of layer 4 protocols that bypass the CM. As a result of message exchanges between the MTA and CMTS, service flows are activated using CMTS-originated signaling on interface PKT-Q2. An enhanced version of RSVP is utilized for this signaling.
Pkt-q4	MTA – CMS/GC	Signaling interface between the MTA and CMS/GC. Many parameters are signaled across this interface such as media stream, IP addresses, and Codec selection, but it is possible for certain protocols to either derive QoS semantics from the signaling, or to extend the application layer signaling protocol to contain explicit QoS signaling parameters.
Pkt-q5	CMS/GC – CMTS	This interface is used to manage the dynamic Gates for media stream bearer channels. This interface enables the PacketCable network to request and authorize QoS changes without requiring any layer two DOCSIS access network QoS control functions in MTA. When supporting standalone MTAs no new client-side QoS signaling protocol needs to be designed. The GC/CMS takes responsibility for requesting policy, and the CMTS takes responsibility for access control and quickly setting up QoS on the DOCSIS access link.
Pkt-q6	CMTS – RKS	This interface is used by the CMTS to signal to the RKS all changes in call authorization and usage. This interface is defined in the Event Messages specification.
Pkt-q7	CMTS – CMTS	This interface is used for coordination of resources between the CMTS of the local MTA and the CMTS of the remote MTA. The CMTS is responsible for the allocation and policing of local QoS resources.

4.6.2 Layer Two vs. Layer Four MTA QoS Signaling

QoS signaling from the MTA can be performed either at layer two (DOCSIS) or layer four (RSVP). Layer two signaling is accessible to CM and CMTS devices that exist at the RF boundary of the DOCSIS access network. Layer four signaling is required for devices that are one or more hops removed from the RF boundary of the DOCSIS access network.

If layer two QoS signaling is initiated by the MTA, the MTA must be an embedded MTA. The MTA utilizes the implicit interface for controlling the DOCSIS MAC service flows as suggested by Appendix E of the DOCSIS 1.1 RFI specification.

Layer four QoS signaling is initiated by the MTA; the MTA may be either an embedded MTA or standalone MTA. Enhanced RSVP is used for this signaling and is intercepted by the CMTS. The CMTS utilizes layer two QoS signaling to communicate QoS signaling changes to the CM.

4.6.3 Dynamic Quality-of-Service

PacketCable Dynamic QoS (D-QoS) utilizes the call signaling information at the time that the call is made to dynamically authorize resources for the call. Dynamic QoS prevents various theft of service attack types by integrating the QoS messaging with other protocols and network elements. The network elements that are necessary for a Dynamic QoS control are shown in Figure 11.

The function within the CMTS that performs traffic classification and enforces QoS policy on media streams is called a Gate. The Gate Controller element manages Gates for PacketCable media streams. The following key information is included in signaling between the GC and the CMTS:

- **Maximum Allowed QoS Envelope** – The maximum allowed QoS envelope enumerates the maximum QoS resource (e.g., "2 grants of 160 bytes per 10ms") the MTA is allowed to admit for a given media stream bearer flow. If the MTA requests a value greater than the parameters contained within the envelope the request will be denied.
- **Identity of the media stream endpoints** – The GC/CMS authorizes the parties that are involved in a media stream bearer flow. Using this information the CMTS can police the data stream to ensure that the data stream is destined and originated from the parties that are authorized.
- **Billing Information** – The GC/CMS creates opaque billing information that the CMTS does not have to decode. The information might be as simple as billing identity or the nature of the call. The CMTS forwards this billing information to the RKS as the call is activated or terminated.

The role of each of the PacketCable components in implementing D-QoS is as follows:

Call Management Server/Gate Controller – The CMS/GC is responsible for QoS authorization. The QoS authorization might depend on the type of call, type of user or other parameters defined by policy.

CMTS – Using information supplied by the GC/CMS the CMTS performs admission control on the QoS requests and at the same time polices the data stream to make sure that the data stream is originated and sent to authorized-media stream parties. The CMTS interacts with CM, RKS, MTA, and Terminating CMTS. The responsibilities of CMTS with respect to each of these elements is:

- CMTS to CM – The CMTS is responsible of setting up and tearing down service flows in such a way that the service level agreement it made with the MTA is met. Inasmuch as the CMTS does not trust the CM it polices the traffic from the CM such that the CM works in the way CMTS requested.
- CMTS to Record Keeping Server – The CMTS updates the Record Keeping Server (RKS) each time there is a change in the QoS Service Level Agreement between CMTS and MTA. It uses the Billing Information that is given by GC/CMS to identify each authorized QoS link. The CMTS puts timing information in the message it sends and also buffers the messages if the connection to RKS is severed.
- CMTS to MTA – The MTA makes dynamic requests for modification of QoS traffic parameters. When the CMTS receives the request it makes an authorization check to find out whether the requested characteristics are within the authorized QoS envelope and also whether the media stream endpoints are authorized. Then it provisions the QoS attributes for the RFI link on the CMTS and activates the appropriate QoS traffic parameters via signaling with the CM. When all the provisioning and authorization checks succeed the CMTS sends a success message to the GC/CMS indicating that MTA and CMTS are engaged in a Service Level Agreement.
- CMTS to Terminating CMTS – The CMTS sends messages to the terminating end CMTS (or other terminating access networking device) to ensure that the committed bandwidth on both sides is the same. If the committed bandwidth is not the same then both sides close the connection.

Cable Modem (CM) – Even though the CM is an untrusted entity the CM is responsible for the correct operation of the QoS link between itself and the CMTS. The CMTS makes sure that the CM cannot abuse the RFI link, but it is the responsibility of the CM to utilize the RFI link to provide services that are defined by the DOCSIS 1.1 specification.

Record Keeping Server (RKS) – The RKS acts as a database and stores each event as sent by the CMTS. The RKS stores the messages by attaching received time and network element information. The RKS has to have sufficient interface and/or processing power to allow additional processing to be done.

MTA – The MTA is the entity to which the Service Level Agreement is provided by the access network. The MTA is responsible for the proper use of the QoS link. If it exceeds the traffic authorized by the SLA than it the MTA will not receive the QoS characteristics that it requested. The MTA uses two stage QoS bandwidth allocation – while the call origination is proceeding the QoS resources are admitted, then when the call is answered the resources are activated.

4.7 Announcement Services

Announcements are typically needed for calls that do not complete. Additionally, they may be used to provide enhanced information services to the caller (e.g., calling card, n11 services, etc.). The signaling interfaces to support PacketCable Announcement Services are shown in Figure 12 and are summarized in Table 7 below.

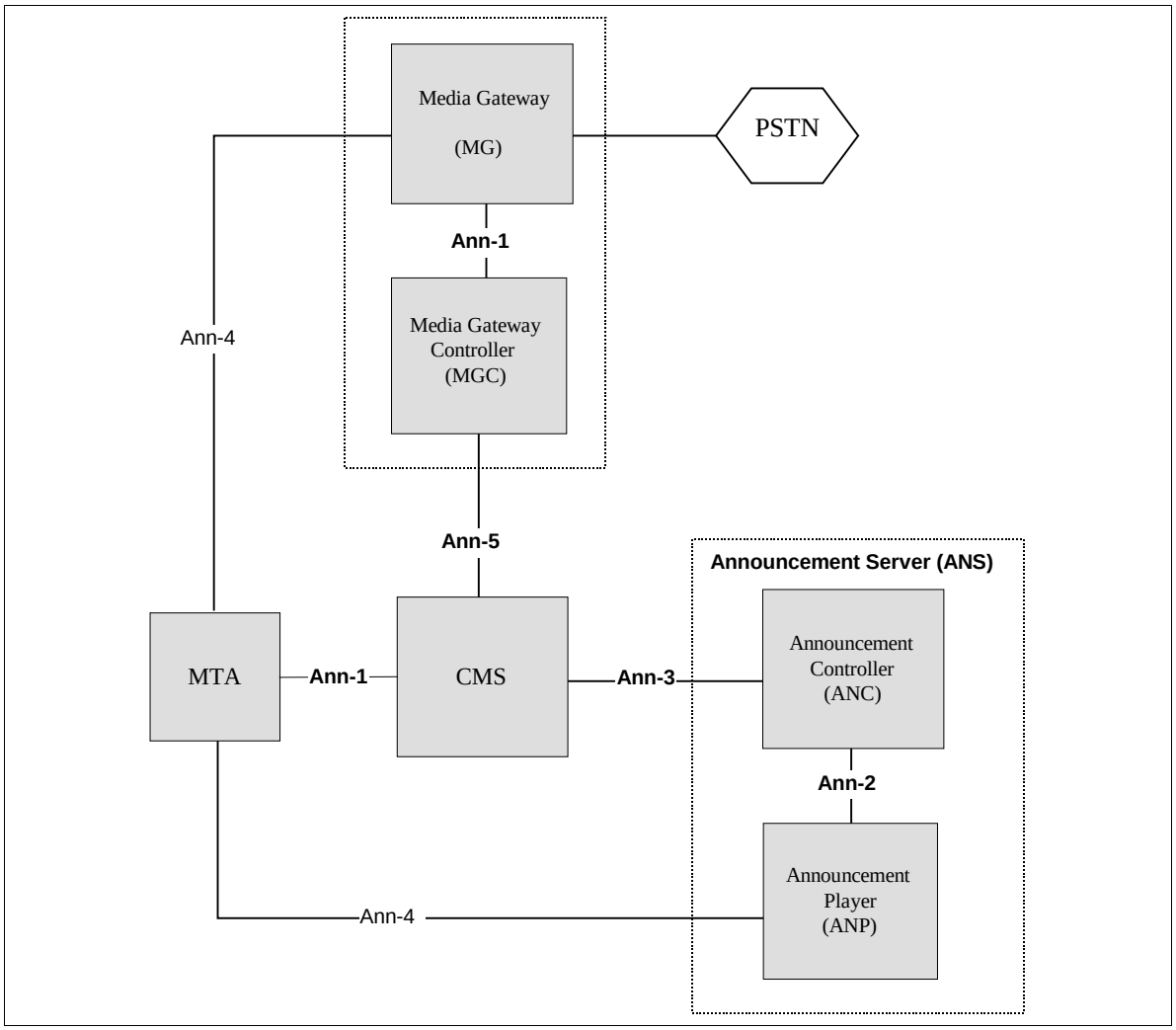

Figure 12. Annoucement Services Components and Interfaces

Table 7. Announcement Interfaces

Interface	PacketCable Functional Components	Protocol
Pkt-ann1	MTA – CMS MGC – MG	The CMS to MTA interface provides a mechanism for the CMS to signal the MTA to play locally stored announcements. Storing announcements in the MTA allows for providing informative progress tones to the end user independently of the network state (e.g., congestion). An NCS-based announcement package has been defined that can be used for both the CMS-MTA and MGC-MG interfaces. Simple, fixed-content announcements (e.g., all-lines-busy) may also be stored at the Media Gateway to provide announcements to PSTN users. The MGC to MG interface provides a mechanism for the MG to play fixed-content announcements to PSTN end-users involved in off-net to on-net calls.
Pkt-ann2	ANC – ANP	The signaling protocol for the ANC to ANP interface is NCS with an announcement package. When the CMS identifies a need for an ANS-based announcement, it sends a request to the ANC over interface Ann-3. Upon receiving a request from the CMS, the ANC opens a session with the Announcement Player using the NCS package.
Pkt-ann3	CMS – ANC	The protocol for the Ann-3 interface is undefined for PacketCable 1.0
Pkt-ann4	ANP-MTA	Defines the media stream format (RTP) for delivery of the announcement from the Announcement Player to the MTA using the RTP protocol.
Pkt-ann5	CMS-MGC	The Ann-5 protocol interface is undefined for PacketCable 1.0.

4.7.1 ANS Physical vs. Logical configuration

The ANC and ANP are logical components that may reside in the same physical entities. When logical components reside in the same physical entity, interfaces between these components become optional. In addition, standalone components using the Ann-2 and Ann-3 interfaces MAY be shared by many network entities.

4.8 Security

4.8.1 Overview

Each of PacketCable's protocol interfaces is subject to threats that could pose security risks to both the subscriber and service provider. The PacketCable architecture addresses these threats by specifying, for each defined protocol interface, the underlying security mechanisms (such as IPSec) that provide the protocol interface with the security services it requires, e.g., authentication, integrity, confidentiality.

For example, the media stream path may traverse a large number of potentially unknown Internet service and backbone service providers' wires. As a result, the media stream may be vulnerable to malicious eavesdropping, resulting in a loss of communications privacy. PacketCable core security services include a mechanism for

providing end-to-end encryption of RTP media streams, thus substantially reducing the threat to privacy.

The security services available through PacketCable's core service layer are authentication, access control, integrity, confidentiality and non-repudiation. A PacketCable protocol interface may employ zero, one or more of these services to address its particular security requirements.

PacketCable security addresses the security requirements of each constituent protocol interface by:

- identifying the threat model specific to each constituent protocol interface
- identifying the security services (authentication, authorization, confidentiality, integrity, and non-repudiation) required to address the identified threats.
- specifying the particular security mechanism providing the required security services.

The security mechanisms include both the security protocol (e.g., IPSec, RTP-layer security, and SNMPv3 security) and the supporting key management protocol (e.g., IKE, PKINIT/Kerberos).

Figure 13 provides a summary of all the PacketCable security interfaces.

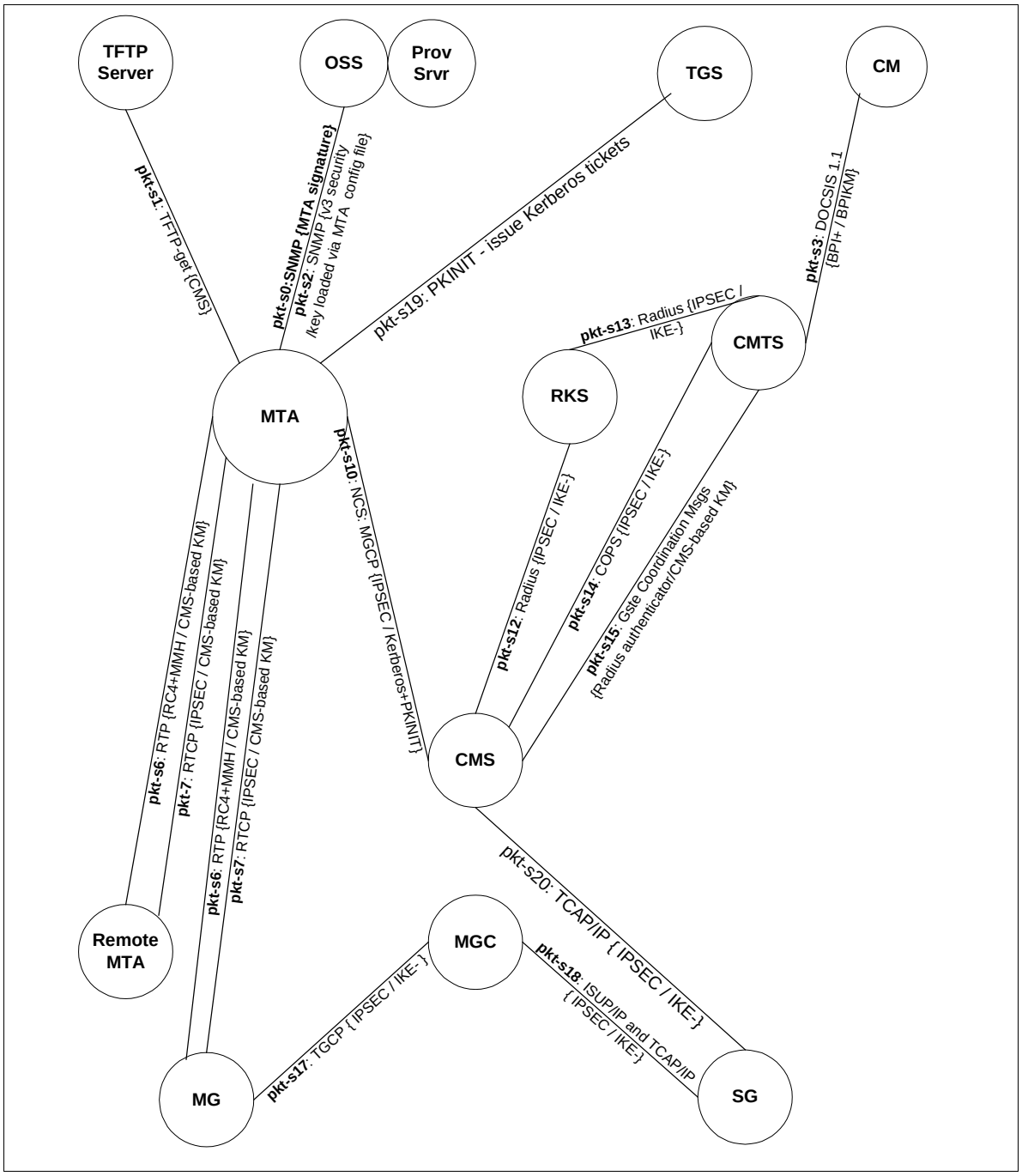

Figure 13. PacketCable Security Interfaces

In Figure 13, each interface is labeled as:

<**label**>: **<protocol> { <security protocol> / <key management protocol> }**

If the key management protocol is missing, it means that it is not needed for that interface. PacketCable interfaces that do not require security are not shown on this diagram.

The following abbreviations are used in the above diagram:

- **IKE-:** IKE with pre-shared keys
- **IKE+:** IKE requires public key certificates
- **CMS-based KM:** Keys randomly generated and distributed by CMS

The following table describes each of the interfaces shown in the above diagram.

Table 8. Security Interfaces

Interface	PacketCable Functional Components	Description
pkt-s0	MTA – Provisioning App	SNMPv3 INFORM from the MTA to the SNMP Manager, followed by optional SNMP GET(s) by the SNMP Manager are used to query MTA device capabilities. This occurs at the time where SNMPv3 keys may not be available, and security is provided with an RSA signature, formatted according to CMS (Cryptographic Message Syntax).
Pkt-s1	MTA – TFTP or HTTP Server	MTA Configuration file download. The MTA downloads a configuration file (with TFTP-get) that is signed by the TFTP server and sealed with the MTA public key, with a CMS (Cryptographic Message Syntax) wrapper. This flow occurs right after an SNMPv3 INFORM followed by an optional SNMP GET(s) – see flow pkt-s0
pkt-s2	MTA – Provisioning App	Standard SNMPv3 security. The SNMPv3 keys are downloaded with the MTA configuration file, using interface pkt-s1.
Pkt-s3	CM – CMTS	BPI+ privacy layer on the HFC link. Both security and key management are defined by DOCSIS 1.1.
pkt-s6	MTA – MTA	End-to-end media packets between two MTAs, or between MTA and MG. RTP packets are encrypted directly with RC4, without any additional security layers. An MMH-based MAC (Message Authentication Code) optionally provides message integrity. Keys are distributed by the CMS to the two endpoints.
Pkt-s7	MTA – MTA	RTCP control protocol for RTP, defined above. Message integrity and encryption provided with IPSEC. Key management is same as for RTP – keys are distributed by CMS.
Pkt-s10	MTA-CMS	MTA-CMS signaling for NCS. Message integrity and privacy via IPSEC. Key management is with Kerberos with PKINIT (public key initial authentication) extension.
Pkt-s12	CMS – RKS	Radius billing events sent by the CMS to the RKS. Radius authentication keys are hardcoded to 0. Instead, IPSEC is used for message integrity as well as privacy. Key management is IKE-.

Interface	PacketCable Functional Components	Description
Pkt-s13	CMTS – RKS	Radius events sent by the CMTS to the RKS. Radius authentication keys are hardcoded to 0. Instead, IPSEC is used for message integrity, as well as privacy. Key management is IKE-.
Pkt-s14	CMS – CMTS	COPS protocol between the GC and the CMTS, used to download QoS authorization to the CMTS. Message integrity and privacy provided with IPSEC. Key management is IKE-.
Pkt-s15	CMS – CMTS	Gate Coordination messages for DQoS. Message integrity is provided with an application-layer (Radius) authenticator. Keys are distributed by local CMS over COPS.
Pkt-s16	N/A	N/A
pkt-s17	MGC – MG	PacketCable interface to the PSTN Media Gateway. IPSEC is used for both message integrity and privacy. Key management is IKE-.
Pkt-s18	MGC – SG	PacketCable interface to the PSTN Signaling Gateway. IPSEC is used for both message integrity and privacy. Key management is IKE-.
Pkt-s19	MTA – TGS	Kerberos/PKINIT key management protocol, where the TGS issues CMS tickets to the MTAs.
Pkt-s20	CMS – SG	CMS queries the PSTN Gateway for LNP (Local Number Portability) and other telephony services. IPSEC is used for both message integrity and privacy. Key management is IKE-.

4.8.2 Device Provisioning Security

The PacketCable security architecture divides device provisioning into three distinct activities: subscriber enrollment, device provisioning and device authorization.

4.8.2.1 Subscriber Enrollment

The subscriber enrollment process establishes a permanent subscriber billing account that uniquely identifies the MTA to the CMS via the MTA's serial number or MAC address. The billing account is also used to identify the services subscribed to by the subscriber for the MTA.

Subscriber enrollment may occur in-band or out-of-band. The actual specification of the subscriber enrollment process is out of scope for PacketCable and may be different for each Service Provider.

4.8.2.2 Device Provisioning

The MTA device verifies the authenticity of the configuration file it downloads from the boot server. Privacy of the configuration data is also provided. The configuration data will be "signed and sealed" by packaging it into a PKCS #7 sealed object.

4.8.2.3 Dynamic Provisioning

SNMPv3 security will be used for dynamically provisioning voice communications capabilities on an embedded-MTA.

4.8.2.4 Device Authorization

Device authorization is when a provisioned MTA Device authenticates itself to the Call Management Server, and establishes a security association with that server prior to becoming fully operational. Device authorization allows subsequent call signaling to be protected under the established security association.

4.8.2.5 Signaling Security

All signaling traffic, which includes QoS signaling, call signaling, and signaling with the PSTN Gateway Interface, will be secured via IPSec. IPSec security association management will be done through the use of two key management protocols: Kerberos/PKINIT and IKE. Kerberos/PKINIT will be used to exchange keys between MTA clients and their CMS server; IKE will be used to manage all other signaling IPSec SAs.

4.8.2.6 Media Stream Security

Each media RTP packet is encrypted for privacy. The MTAs have an ability to negotiate a particular encryption algorithm, although the only one that is currently specified is RC4. Encryption is applied to the packet's payload but not to its header.

Each RTP packet may include an optional message authentication code (MAC). The MAC algorithm can also be negotiated, although the only one that is currently specified is MMH. The MAC computation spans the packet's unencrypted header and encrypted payload.

Keys for the encryption and MAC calculation are derived from the End-End secret, which is exchanged between sending and receiving MTA as part of the call signaling. Thus, the key exchanges for media stream security are secured themselves by the call signaling security.

4.8.2.7 OSS and Billing System Security

The SNMP agents in PacketCable devices implement SNMPv3. The SNMPv3 User Security Model [RFC 2274] provides authentication and privacy services for SNMP traffic. SNMPv3 view-based access control [RFC 2275] may be used for access control to MIB objects.

The IKE key management protocol is used to establish encryption and authentication keys between the Record Keeping Server (RKS) and each PacketCable network element that generates Event Messages. When the network IPSec Security Associations are established, these keys must be created between each RKS (primary, secondary, etc) and every CMS and CMTS. The key exchange between the MGC and RKS may exist and is left to vendor implementation in PacketCable 1.0. The Event

Messages are sent from the CMS and CMTS to the RKS using the RADIUS transport protocol, which is in turn secured by IPSec.

5 NETWORK DESIGN CONSIDERATIONS

5.1 Time Keeping and Reporting Issues

In order to maintain service quality, it is highly recommended that all network equipment clocks be maintained to within 200 milliseconds of Universal Time Coordinated (UTC).

It is recommended that PacketCable networks maintain a timeserver that is accurate to within a specified interval of Universal Time Coordinated (UTC). It is recommended that the server be able to exchange time information with other network equipment such that the receiving equipment is able to be synchronized to the time server clock at the completion of the synchronization protocol exchange.

NTP [38] is the recommended protocol for PacketCable time synchronization.

All systems that generate billing event messages must synchronize their clocks to a network clock source. Synchronization should be done to ensure that the reporting device's own clock remains within ±100 milliseconds of the last synchronization value.

5.2 Timing for Playout Buffer Alignment with Coding Rate

Packet generating and packet handing equipment generally operate with free-running clocks. Problems may arise in the offering of isochronous services due to the plesiochronous nature of these clocks. The difference in clock speed between these plesiochronous entities are generally exhibited as overrun or underrun of the playout buffers.

In order to minimize the occurrence of these conditions, all CMTS' should lock their downstream transmission rate to a clock derived from a source that reflects a Stratum-3 clock. Embedded MTAs should use the downstream transmission rate to derive the clock used to determine packetization period. MTAs should also use this clock to determine the rate of playout from the receive buffer. Non-embedded MTAs should use the average packet arrival interval[3] as the basis for determining their packetization and playout clock.

5.3 IP Addressing

An embedded MTA is a multi-function entity with one function required for CM administration and the second function being the MTA function itself. All IP addresses in a PacketCable network are IPV4.

All PacketCable 1.0 embedded MTAs are required to have 2 IP addresses - one for the CM and one for the MTA. All PacketCable 1.0 embedded MTAs are required to have 2 MAC addresses - one for the CM and one for the MTA.

The following requirements can be met using the dual IP address configuration:

[3] I.e., the interval from arrival of the first bit of packet N to the arrival of the first bit of packet N+1, ignoring intervals where a packet does not arrive within 5 ms of the expected periodicity.

- An embedded MTA containing a dual IP address can assign a private IP address for the CM host function, in the case where NAT translation is not provided elsewhere in the PacketCable network.
- With two IP addresses per MTA, the PacketCable operator can route the voice service packets over a voice backbone and all other packets (data) over a data backbone. Essentially the routing backbone must be configured such that different routing paths are followed for each of the two destination IP addresses.
- The PacketCable operator can simplify network side administration and management functions using separate IP addresses. For example, policy filters can be instantiated that block or permit traffic from the MTA component of the node. In addition, network service providers can provide source address screening services, and network traffic statistics and diagnostics can be collected based upon the IP address of the MTA.

Dual IP addresses result in special considerations that affect the following:

- IP protocol stack implementation of the MTA,
- Implementation of PacketCable OSS and device provisioning protocols,
- Network routing implementations.

5.4 Dynamic IP Addressing Assignment

An operational issue exists regarding the dynamic IP addresses assignment for MTAs. The NCS model specified in PacketCable 1.0 is based on a Call Management Server mapping a subscriber's service to an endpoint identifier and an IP address. Therefore, call processing operations would be affected if the MTA's IP address changed during an active call. However, there are some recommendations that network operators and MTA vendors can employ to eliminate this situation.

1. When configuring DHCP options for an MTA, the network operator should configure the IP Address Lease Time (Option Code 51) to specify a very long lease time. This option is detailed in "Dynamic Host Configuration Protocol" [RFC2131] and "DHCP Options and BOOTP Vendor Extensions" [RFC2132]. Per paragraph 3.3 of RFC2131, a lease time setting of "0xffffffff" represents an infinite lease. Use of long lease times will minimize the possibility that an active MTA would be unable to renew its assigned IP address lease.
2. Network operators should also configure an MTA's DHCP Timer T1 and T2 values (Option Codes 58 and 59, respectively) to be no more than the default values specified in paragraph 4.4.5 of RFC2131. Configuring an MTA to begin it's IP address lease time renewal process at no more than 50% of the assigned lease time, combined with the use of very long lease time values, will further ensure that an MTA will be able to renew its IP address lease.
3. MTA vendors should implement mechanisms to prevent an MTA from entering the RENEWING state (as specified in RFC2131) while call

processing is active. It is left to vendor implementation to determine exactly how this capability might best be implemented in their product.

5.5 FQDN Assignment

The following are potential operational issues that are expected to be resolved through vendor-specific implementations:

It is assumed that the OSS back office will generate the appropriate FQDNs for all PacketCable devices, and pass this data to the appropriate PacketCable devices and other network elements. These interfaces are not defined in PacketCable 1.0.

An operational issue exists regarding synchronization of databases within the provisioning domain. Specifically the DHCP database, and the DNS table's require concurrent updates when a subscriber record changes (this includes creation). RFC2131 provides a mechanism by which a host (a DHCP client) could acquire certain configuration information, specifically its IP address(es). However, DHCP does not provide any mechanisms to update the DNS Resource Records that contain the information about mapping between the host's FQDN and its IP address(es) (i.e., the Address and Pointer Resource Records). Thus the information maintained by DNS for a DHCP client may be incorrect – a host (the client) could acquire its address by using DHCP, but the Address Resource Record for the host's FQDN wouldn't reflect the address that the host acquired, and the Pointer Resource Record for the acquired address wouldn't reflect the host's FQDN.

The problem has two main issues. One, how do you update the DNS system when a new IP address is dispensed, and two, how long do you make time out values for RR's. Both of these issues are vendor implementation issues and therefore lie outside of the scope of PacketCable specifications. However, some recommendations on 'best practices' are outlined in RFC 2131.

5.6 Priority Marking of Signaling and Media Stream Packets

Both the media stream and the signaling stream for PacketCable-based services require methods for properly marking and transporting packets at a sufficiently high level of quality of service, both in the DOCSIS access network and in the managed IP backbone.

The primary mechanism for providing low-latency quality of service for media streams in the access network is the DOCSIS 1.1 flow classification service. This service classifies packets into specific flows based upon packet fields such as IP source and destination addresses and UDP port number parameters. In the upstream such classified packets are transported via an appropriate constant bit rate service (for current codecs) as dynamically scheduled by the CMTS. In the downstream the packets are transported via an appropriate high priority queuing and scheduling mechanism. DQoS (between CMS and CMTS) and DOCSIS (between CMTS and CM) signaling mechanisms are used to dynamically setup the media stream flow classification rules and service flow QoS traffic parameters.

In addition to flow classification, it is useful to mark media stream packets with appropriate priority markings. Such priority markings can be utilized within CMTS/CM queuing systems and also within Diff-serv managed QoS backbones (which may not contain flow classification mechanisms) in order to provide high priority QoS treatment of such packets. It should be noted that while no definition is provided as to how QoS is managed in the Managed IP backbone in the current architecture, it is expected that the mechanisms defined for PacketCable QoS will be usable within such a managed backbone.

Signaling packets may also benefit from prioritized QoS services. In particular as an access network becomes loaded to capacity, it may be important to forward signaling packets at a higher priority than data packets in order to avoid excessive signaling latency. It should be noted that from a network traffic-engineering point of view it has not yet been determined whether high priority treatment of signaling packets is required. If signaling prioritization is desired, then the method for providing prioritized QoS is based upon two mechanisms. First mark all signaling packets with a high priority marking, and second provide a DOCSIS Classifier that classifies such packets to be transported on a higher priority service flow. The Classifier can be as simple as mapping all upstream packets with this priority to the high priority SID, or can be more complex and also identify the IP address of the MTA(s) which originate the signaling. The higher priority service flow may be either statically provisioned or dynamically created by the administrator of the CMTS. It should be noted that if the administrator is concerned about theft of service of the high priority service flow, then he may configure the service flow for high priority (low latency) but low bandwidth.

Marking of packets for both the media stream and the signaling stream (NCS) is performed by the MTA and the CMS. The marking is performed at the IP layer using a field that has alternately been called the TOS byte or the Diff-serv Code Point (DSCP). The TOS byte was the original definition of the byte while DSCP is the new definition of the byte as used by the IETF Diff-serv architecture. Because two formats for this byte exist, the configuration of the values should be done in a format and type independent way (in the MIBs for the MTA and Call Agent).

Management Information Bases (MIBS) are defined in PacketCable for assigning the provisioned and default values for media stream priority marking and signaling stream priority marking (e.g. a value of ‘3’ for signaling and a value of ‘5’ for media). It should be noted that in NCS the signaled SDP parameters may contain overrides for the configured media stream priority marking value on a connection by connection basis. No mechanism currently exists for dynamically overriding the provisioned priority marking value of the signaling stream on a call by call basis.

5.7 Fax Support

PacketCable supports real-time fax transmission. Fax is ‘best’ accomplished using the G.711 standard for audio encoding/decoding. If a call is established using a compressed codec, the embedded MTA will have to be instructed to look for fax tones. If fax tones are detected, the CMS will have to be notified and the MTA will be

instructed to switch to using G.711. Note that this places a requirement on the embedded device to monitor the media stream and detect fax tones.

Support for switching over to fax from a voice call is required; however, switching back to voice from fax is not required (*i.e.*, monitoring the fax media stream for an ending signal and then switching back to a low bandwidth codec).

Local termination of fax and translating the fax stream to an IP fax relay data stream is not required in this version of the architecture.

5.8 Analog Modem Support

Analog modems are supported in a similar fashion to fax—a MTA will be asked to detect modem tones and, when such tones are detected, the CMS will instruct the MTA to switch over to the G.711 codec if it is not already in use. Note that this places a requirement on the embedded device to monitor the voice stream and to detect analog modem tones.

Switching over to G.711 to support analog modem signaling from a voice call will be supported; however, switching back to voice from modem signaling will not be required to be supported (*i.e.*, monitoring the modem media stream for an ending signal and then switching back to a low-bandwidth codec).

Local termination of modems and translating the modem stream to an IP modem relay data stream is not required in this version of the architecture.

6 FUTURE CONSIDERATIONS

The goal of PacketCable is to enable full-featured, robust, wide-scale deployment for global cable IP networks. To meet this goal, the PacketCable project will continue to evolve to support ground-breaking services, features, and functionality. The project evolution is accompanied by an architecture evolution as new features are added and old ones are re-designed. Continuing the design evolution allows cutting-edge techniques to be added to optimize access, maximize bandwidth utilization and provide for advanced multimedia features.

Future PacketCable network capabilities will likely include but are not limited to, inter-zone and inter-domain signaling, tools for client power management, primary line support, fault management and performance management**.** Additional equipment types such as standalone MTAs (S-MTAs) and new media servers are also planned for specification.

Potential changes in other areas could address enhanced QoS, provisioning and security capabilities. For example, QoS could add layer four QoS signaling (for providing service to standalone MTAs via RSVP with enhancements) and a specific protocol for backbone networks. Provisioning for subscriber installed and dynamically provisioned MTAs (out-of-box registration and activation of service) may be possible in the near future on PacketCable networks. Security could include support for new network devices, and interfaces to those devices. Additionally, security would be added for the MTA-CMTS interface (RSVP) for QoS signaling, and for any newly defined provisioning and signaling protocols. Also, an increased choice in the number of cryptographic algorithms may be made available.

Appendix A. Acknowledgements

Many contributors are to be acknowledged for the development of the PacketCable architecture framework specification. Certainly all of the participants in the various technical task forces have made a contribution through their contribution to the working groups. In particular, the following individuals are recognized by their contributions and review of this specification – Flemming Andreasen (Telcordia), Burcak Beser (3COM), Chet Birger (YAS Corp.), David Bukovinsky (CableLabs), John Chapman (Cisco), Frank Christofferson (CableLabs), Nancy Davoust (CableLabs), Raj Deshpande (Motorola), Jonathan Fellows (General Instrument), Bill Foster (Cisco), Keith Kelly (Netspeak), William Marshall (AT&T), Sasha Medvinsky (General Instrument), Ed Miller (CableLabs), Rick Morris (Arris Interactive), John Pickens (Com21), Michael Patrick (Motorola), Stephane Proulx (Broadsoft), K. K. Ramakrishnan (AT&T), Glenn Russell (CableLabs), Maria Stachelek (CableLabs), Don Stanwyck (IPUnity), Andrew Sundelin (CableLabs), and Venkatesh Sunkad (CableLabs).

Appendix B. References

[1] "PacketCable Product Specification," Cable Television Laboratories, Inc. /MCNS, November 25, 1998.

[2] "PacketCable Specification Overview – Version 1.0," Cable Television Laboratories, Inc. /MCNS, July 29, 1998.

[3] "PacketCable Audio/Video Codecs Specification,"PKT-SP-CODEC-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[4] "PacketCable Dynamic Quality-of-Service Specification,"PKT-SP-DQOS-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[5] "PacketCable Network-Based Call Signaling Protocol specification," PKT-SP-EC-MGCP-I02-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[6] "PacketCable Event Messages Specification," PKT-SP-EM-I01-991201, December 01, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[7] "PacketCable Internet Signaling Transport Protocol (ISTP) Specification,"PKT-SP-ISTP-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[8] "PacketCable MTA MIB Specification,"PKT-SP-MIB-MTA-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[9] "PacketCable NCS MIB Specification," PKT-SP-MIB-NCS-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[10] "PacketCable MIBs Framework Specification,"PKT-SP-MIBS-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[11] "PacketCable PSTN Gateway Call Signaling Protocol Specification,"PKT-SP-TGCP-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[12] "PacketCable MTA Device Provisioning Specification,"PKT-SP-PROV-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[13] "PacketCable Security Specification,"PKT-SP-SEC-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[14] "PacketCable Call Flows," PKT-TR-CF-991201, CableLabs, December 01, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[15] "PacketCable OSS Overview," PKT-TR-OSSI-V01-990730, July 30, 1999, Cable Television Laboratories, Inc., available at www.PacketCable.com.

[16] "PacketCable Functional Requirements PSTN Gateway Architecture Description and Functional Requirements," PKT-FR-PSTNGWARCH-990305, March 5, 1999, Cable Television Laboratories, Inc.

[17] "PacketCable Event Messaging White Paper," PKT-OSS-TD01-990329

[18] "Distributed Open System Architecture," ATT.

[19] "Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification," SP-RFIv1.1-I03-991105. Cable Television Laboratories, Inc. Available at www.cablemodem.com.

[20] "DOCSIS QoS Management Information Base," draft-ietf-ipcdn-qos-mib-00.txt. Cable Television Laboratories, Inc. Available at www.cablemodem.com.

[21] "Data-Over-Cable Service Interface Specifications," Cable Modem Termination System – Network Side Interface Specification," SP-CMTS-NSII01- 960702. Cable Television Laboratories, Inc. Available at www.cablemodem.com.

[22] "Data-Over-Cable Service Interface Specifications, Cable Modem to Subscriber Premise Equipment Interface Specification," SP-CMCI-I03-991115. Cable Television Laboratories, Inc. Available at www.cablemodem.com.

[23] "Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification," SP-OSSI-I02-990113. Cable Television Laboratories, Inc. Available at www.cablemodem.com.

[24] "Data-Over-Cable Service Interface Specifications, Cable Modem Telephony Return Interface Specification," SP-CMTRI-I01-970804. Cable Television Laboratories, Inc. Available at www.cablemodem.com.

[25] "Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification," SP-BPI+-I03-991105. Cable Television Laboratories, Inc. Available at www.cablemodem.com.

[26] "COPS Usage for RSVP," IETF (Boyle, et. al.), Internet Draft, draft-ietf-rap-cops-rsvp-05.txt, June 1999 (expires December 1999).

[27] "An Architecture for Differentiated Services," IETF RFC 2475.

[28] "Definition of the Differentiated Services Field (DS Field) in the Ipv4 and Ipv6 Headers," IETF RFC 2474.

[29] "The COPS (Common Open Policy Service) Protocol," IETF (J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry), Internet Draft, draft-ietf-rap-cops-08.txt, Nov. 6, 1999 (expires April 2000).

[30] "Resource reSerVation Protocol – Version 1 Functional Specification," IETF RFC 2205.

[31] "CANOE – Cable Access Network Operations Extensions for DOCSIS PacketCable Networks," 3Com, August 17, 1998.

[32] "RTP: A Transport Protocol for Real-Time Application," IETF RFC 1889.

[33] "SDP: Session Description Protocol," IETF RFC 2327.

[34] "Dynamic Host Configuration Protocol", IETF RFC 2131.

[35] "RTP Profile for Audio and Video Conferences with Minimal Control," IETF RFC 1890.

[36] "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links," draft-ietf-avt-crtp-05.txt

[37] "The Kerberos Network Authentication Service (V5)", IETF Draft (Clifford Neuman, John Kohl, Theodore Ts'o), draft-ietf-cat-kerberos-revisions-04.txt, July, 1999.

[38] "Network Time Protocol" IETF RFC 1119.

Appendix C. Glossary

AAA	Authentication, Authorization and Accounting
Access Control	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes or other system resources on a network.
Active	A service flow is said to be "active" when it is permitted to forward data packets. A service flow must first be admitted before it is active.
Admitted	A service flow is said to be "admitted" when the CMTS has reserved resources (e.g. bandwidth) for it on the DOCSIS network.
AF	Assured Forwarding. A Diffserv Per Hop Behavior.
AH	Authentication header is an IPSec security protocol that provides message integrity for complete IP packets, including the IP header.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access".
Announcement Server	An announcement server plays informational announcements in PacketCable network. Announcements are needed for communications that do not complete and to provide enhanced information services to the user.
AMA	Automated Message Accounting., a standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies)
Asymmetric Key	An encryption key or a decryption key used in a public key cryptography, where encryption and decryption keys are always distinct.
AT	Access Tandem. A switching point in PSTN networks that allows access to an entire calling area.
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information.
Authorization	The act of giving access to a service or device if one has the permission to have the access.
BAF	Bellcore AMA Format, another way of saying AMA
BPI+	Baseline Privacy Interface Plus is the security portion of the DOCSIS 1.1 standard which runs on the MAC layer.
CBC	Cipher block chaining mode is an option in block ciphers that combine (XOR) the previous block of ciphertext with the current block of plaintext before encrypting that block of the message.
CBR	Constant Bit Rate.
CA	Certification Authority - a trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CA	Call Agent. In this specification "Call Agent" is part of the CMS that maintains call state, and controls the line side of calls.
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. A coding format for digital signals.
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set which must contain both an encryption algorithm and a message authentication algorithm (e.g. a MAC or an HMAC). In general, it may also contain a key management algorithm, which does not apply in the context of PacketCable.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
CIR	Committed Information Rate.
Cleartext	The original (unencrypted) state of a message or data.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax
CMS	Call Management Server. Controls the audio call connections. Also called a Call Agent in MGCP/SGCP terminology.
CMTS	Cable Modem Termination System, the device at a cable head-end which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
Codec	COder-DECoder
Confidentiality	A way to ensure that information is not disclosed to any one other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
COPS	Common Open Policy Service Protocol is currently an internet draft which describes a client/server model for supporting policy control over QoS Signaling Protocols and provisioned QoS resource management.
CoS	Class of Service. The type 4 tuple of a DOCSIS 1.0 configuration file.
CSR	Customer Service Representative
Cryptoanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
DA	Directory Assistance
DE	Default. A Diffserv Per Hop Behavior.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default - Network Provider DHCP Server
Digital certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate

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

H.323	An ISO standard for transmitting and controlling audio and video information. The H.323 standard calls for the use of the H.225/H.245 protocol for call control between a "gateway" audio/video endpoint and a "gatekeeper" function.
Header	Protocol control information located at the beginning of a protocol data unit.
HFC	Hybrid Fiber/Coax(ial [cable]), HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the head-end and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.
H.GCP	A protocol for media gateway control being developed by ITU.
HMAC	Hashed Message Authentication Code – a message authentication algorithm, based on either SHA-1 or MD5 hash and defined in RFC 2104.
HTTP	Hyper Text Transfer Protocol. Refer to IETF RFC 1945 and RFC 2068.
IANA	Internet Assigned Numbered Authority. See www.ietf.org for details.
IC or IXC	Inter-exchange Carrier. A long distance carrier.
IETF	Internet Engineering Task Force. A body responsible, among other things, for developing standards used in the Internet.
IKE	Internet Key Exchange is a key management mechanism used to negotiate and derive keys for SAs in IPSec.
IKE–	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
IKE+	A notation defined to refer to the use of IKE, which requires digital certificates for authentication.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access Transport Area
IP	Internet Protocol. An Internet network-layer protocol.
IPSec	Internet Protocol Security, a collection of Internet standards for protecting IP packets with encryption and authentication.
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part is a protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ISTP	Internet Signaling Transport Protocol
ISTP – User	Any element, node, or software process that uses the ISTP stack for signaling communications.
ITU	International Telecommunication Union
IVR	Interactive Voice Response System
Jitter	Variability in the delay of a stream of incoming packets making up a flow such as a voice call
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.

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

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

PKI	Public Key Infrastructure - a process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
PKINIT	The extension to the Kerberos protocol that provides a method for using public key cryptography during initial authentication.
PHS	Payload Header Suppression, a DOCSIS technique for compressing the Ethernet, IP and UDP headers of RTP packets.
Plaintext	The original (unencrypted) state of a message or data.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to any one other then the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves.
PSC	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
PSFR	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
PSTN	Public Switched Telephone Network.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A users private key is kept secret and is the only key which can decrypt messages sent encrypted by the users public key.
PCM	Pulse Code Modulation – A commonly employed algorithm to digitize an analog signal (such as a human voice) into a digital bit stream using simple analog to digital conversion techniques.
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service, guarantees network bandwidth and availability for applications.
RADIUS	Remote Access Dial-In User Service, an internet protocol (RFC 2138 and RFC 2139) originally designed for allowing users dial-in access to the internet through remote servers. Its flexible design has allowed it to be extended well beyond its original intended use
RAS	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
RC4	A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in PacketCable.

RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
RKS	Record Keeping Server, the device which collects and correlates the various Event Messages
Root Private Key	The private signing key of the highest level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures that it generated with the corresponding root private key.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
RSVP	Resource reSerVation Protocol
RTCP	Real Time Control Protocol
RTO	Retransmission Timeout
RTP	Real Time Protocol, a protocol defined in RFC 1889 for encapsulating encoded voice and video streams.
S-MTA	Standalone MTA – a single node which contains an MTA and a non DOCSIS MAC (e.g. ethernet).
SA	Security Association - a one-way relationship between sender and receiver offering security services on the communication flow .
SAID	Security Association Identifier - uniquely identifies SAs in the BPI+ security protocol, part of the DOCSIS 1.1 specification.
SCCP	The Signaling Connection Control Part is a protocol within the SS7 suite of protocols that provides two functions in addition to those that are provided within MTP. The first is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	A Service Control Point is a Signaling Point within the SS7 network, identifiable by a Destination Point Code, that provides database services to the network.
SCTP	Simple Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information that is delivered as a unit between peer service access points.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.
Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
SF	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
SFID	Service Flow ID, a 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. Any 32-bit SFID

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

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

Appendix D. Example Delay Budgets

A model that estimates delay and jitter for PacketCable networks is shown in the following charts. This information is for informative purpose only.

VoIP over DOCSIS Delay & Jitter Model

John T. Chapman, jchapman@cisco.com V2.1, 9/8/99 (v1.0 5/3/98)

Scenario:	A	B	C	D	E	F	G	H	I	J	K	L	
Voice Coding:	G.711T	G.728T	G.729T	G.711T	G.728T	G.729T	G.711	G.728	G.729	G.711	G.728	G.729	
Voice per Packet (ms):	10	10	10	20	20	20	10	10	10	20	20	20	
Delay Round Trip													
Codec:													
No Grant Sync:	25	30	39	35	40	49	32	45	50	42	55	60	ms
Grant Sync:	25	30	39	35	40	49	32	45	50	42	55	60	ms
Cable Plant:													
No Grant Sync:	15	15	15	25	25	25	15	15	15	25	25	25	ms
Grant Sync:	9	9	9	9	9	9	9	9	9	9	9	9	ms
Backbone:	210	210	210	210	210	210	210	210	210	210	210	210	ms
BTI <-> BTI													
No Grant Sync:	290	300	318	331	340	358	304	330	340	345	370	380	ms
Grant Sync:	278	288	306	299	308	326	292	318	328	313	338	348	ms
PSTN <-> BTI													
No Grant Sync:	275	285	303	305	315	333	289	315	325	319	345	355	ms
Grant Sync:	269	279	297	289	299	317	283	309	319	303	329	339	ms
Jitter One Way													
Coder:	0	0	0	0	0	0	0	0	0	0	0	0	ms
Cable Plant Upstream:													
No Grant Sync:	3	3	3	3	3	3	3	3	3	3	3	3	ms
Grant Sync:	3	3	3	3	3	3	3	3	3	3	3	3	ms
Backbone:	10	10	10	10	10	10	10	10	10	10	10	10	ms
Cable Plant Downstream:	1	1	1	1	1	1	1	1	1	1	1	1	ms
Decoder:	0	0	0	0	0	0	0	0	0	0	0	0	ms
BTI -> BTI													
No Grant Sync:	14	14	14	14	14	14	14	14	14	14	14	14	ms
Grant Sync:	14	14	14	14	14	14	14	14	14	14	14	14	ms
BTI -> PSTN													
No Grant Sync:	13	13	13	13	13	13	13	13	13	13	13	13	ms
Grant Sync:	13	13	13	13	13	13	13	13	13	13	13	13	ms
PSTN -> BTI	11	11	11	11	11	11	11	11	11	11	11	11	ms

Jitter Model Used: Case 1: Correlated

Delay Analysis:

Scenario:	A	B	C	D	E	F	G	H	I	J	K	L		Variable?
Voice Coding:	G.711T	G.728T	G.729T	G.711T	G.728T	G.729T	G.711	G.728	G.729	G.711	G.728	G.729		
Voice per Packet (ms):	10	10	10	20	20	20	10	10	10	20	20	20		c/v
Coder														
Codec Tx Look Ahead:	0.0	0.0	5.0	0.0	0.0	5.0	5.0	0.0	5.0	5.0	0.0	5.0	ms	
Tx Processing Delay:	0.0	2.5	4.0	0.0	2.5	4.0	1.0	10.0	10.0	1.0	10.0	10.0	ms	
Packetization:	10.0	10.0	10.0	20.0	20.0	20.0	10.0	10.0	10.0	20.0	20.0	20.0	ms	
Sub-Total:	**10.0**	**12.5**	**19.0**	**20.0**	**22.5**	**29.0**	**16.0**	**20.0**	**25.0**	**26.0**	**30.0**	**35.0**	**ms**	
CM -> CMTS														
Bytes per Frame:	109.0	49.0	39.0	189.0	69.0	49.0	109.0	49.0	39.0	189.0	69.0	49.0	bytes	
Upstream Rate:	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	Mbps	
CM prop Time:	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	ms	v
Upstream Playout Time:	0.3	0.2	0.1	0.6	0.2	0.2	0.3	0.2	0.1	0.6	0.2	0.2	ms	
Grant Arrival Uncertainty:														
-> no Grant Sync:	8.0	8.0	8.0	18.0	18.0	18.0	8.0	8.0	8.0	18.0	18.0	18.0	ms	
-> with Grant Sync:	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	ms	
Grant Window:	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	ms	v
uBR prop time:	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	ms	v
Cable Plant prop time:	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	ms	
Sub-Total no GS:	**12.3**	**12.1**	**12.0**	**22.5**	**22.1**	**22.1**	**12.3**	**12.1**	**12.0**	**22.5**	**22.1**	**22.1**	**ms**	
Sub-Total with GS:	**6.3**	**6.1**	**6.0**	**6.5**	**6.1**	**6.1**	**6.3**	**6.1**	**6.0**	**6.5**	**6.1**	**6.1**	**ms**	
Backbone														
# Switching Nodes:	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	nodes	
Delay per Node:	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	ms	
Node Prop Time:	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	ms	v
Specified Plant Delay:	95.0	95.0	95.0	95.0	95.0	95.0	95.0	95.0	95.0	95.0	95.0	95.0	ms	
Sub-Total:	**105.0**	**105.0**	**105.0**	**105.0**	**105.0**	**105.0**	**105.0**	**105.0**	**105.0**	**105.0**	**105.0**	**105.0**	**ms**	
CMTS -> CM														
Bytes per Frame:	149.0	89.0	79.0	229.0	109.0	89.0	149.0	89.0	79.0	229.0	109.0	89.0	bytes	
Downstream Rate:	27.0	27.0	27.0	27.0	27.0	27.0	27.0	27.0	27.0	27.0	27.0	27.0	Mbps	
uBR propagation time:	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	ms	v

Codec Parameters

	Row	G.711T	G.711	G.729T	G.729	G.728T	G.728	SC-10	G.723.1	G.722T	
Bit Rate	2	64	64	8	8	16	16	10	5.6	64	kbps
Frame Size	3	0	0	10	10	2.5	2.5	20	30	0	ms
Tx Look Ahead	4	0	5	5	5	0	0	18.5	7.5	0	ms
Tx Processing Delay	5	0	1	4	10	2.5	10	10	10	0	ms
Rx Processing Delay	6	0	1	5	10	2.5	10	10	10	0	ms

Global Variables

OH Bytes in u/s Frame:	29	bytes	Header Suppression On
OH Bytes in d/s Frame:	69	bytes	Header Suppression Off
Cable Plant Radius:	100	miles	
Minimum Jitter Buffer:	15	ms	
Jitter Model for Calculation	1	1,2,3	1 = correlated, 2 = only backbone correlated, 3 = uncorrelated

Notes:

=> Delay design goal is <= 300 ms

=> data input fields are marked in yellow with a black border

=> The CODEC "T" suffix refers to an optimized implemention with minimized processing delay

=> Non-T versions are a conservative implementation. "T" versions are an aggressive implementaiton and require development effort.

=> G.711 uses 5 ms look ahead for VAD

=> G.711T moves VAD look ahead into the packetization time, and optimizes DSP processing

=> G.729 assumes 5 ms of DSP power per channel for both rx and tx, a two channel implementation, and no process interleaving

=> G.729T assumes interleaving of packets

=> G.728 assumes 5 ms of DSP power per channel for both rx and tx, a two channel implementation, and no process interleaving

=> G.728T assumes optimized processing. Theoretical delay is 0.625. An extra 125 us was added for design margin

=> The processing delay of the DSP codec ~~*must*~~ be the worst case delay when handling multiple channels.

=> Over time as DSP horsepower increases, processing delay will decrease. Values are for DSP product of 1999.

=> The jitter buffer values are set equal to the max of measured jitter or minimum buffer size.

=> Jitter buffer is based upon CM to CM model, not PSTN to CM model.

=> Backbone budget may be 200 ms instead of 210 ms. This would free up 10 additional ms.

=> Jitter has been calculated 3 different ways:

1) correlated: All max jitter values are added together. This provides a worst case, but is not realistic

2) uncorrelated except the backbone: This allows a fixed jitter buget in the backbone to be added to the rest of the uncorrelated delays

3) uncorrelated: All jitter sources are considered uncorrelated.