

**PacketCable™**

# **Security, Monitoring, and Automation Architecture Framework Technical Report**

**PKT-TR-SMA-ARCH-V01-081121**

**RELEASED**

## **Notice**

This PacketCable technical report is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein.

© Copyright 2008 Cable Television Laboratories, Inc.  
All rights reserved.

## Document Status Sheet

**Document Control Number:** PKT-TR-SMA-ARCH-V01-081121

**Document Title:** PacketCable™ Security, Monitoring, and Automation  
Architecture Framework Technical Report

**Revision History:** V01 - Released 11/21/08

**Date:** November 21, 2008

### Trademarks

CableLabs®, DOCSIS®, EuroDOCSIS™, eDOCSIS™, M-CMTS™, PacketCable™, EuroPacketCable™, PCMM™, CableHome®, CableOffice™, OpenCable™, OCAP™, CableCARD™, M-Card™, DCAS™, tru2way™, and CablePC™ are trademarks of Cable Television Laboratories, Inc.

## Abstract

This technical report describes the Security, Monitoring, and Automation (SMA) architecture, including all major system components and the network interfaces. The intended audience for this document includes developers of equipment who intend to conform to the CableLabs SMA specifications and network architects who need to understand the overall SMA architecture framework.

This technical report describes the SMA release. It contains the following information:

- A reference architecture;
- Description of the various functional groupings within the architecture;
- Detailed description of specific architectural components;
- Interface definitions.

The SMA specifications take precedence over this technical report if the technical report contradicts any specification requirements.

# Table of Contents

<b>1</b>	<b>OVERVIEW</b> .....	<b>1</b>
<b>2</b>	<b>REFERENCES</b> .....	<b>2</b>
2.1	NORMATIVE REFERENCES .....	2
2.2	INFORMATIVE REFERENCES .....	2
2.3	REFERENCE ACQUISITION.....	2
<b>3</b>	<b>TERMS AND DEFINITIONS</b> .....	<b>3</b>
<b>4</b>	<b>ABBREVIATIONS AND ACRONYMS</b> .....	<b>4</b>
<b>5</b>	<b>PACKETCABLE SMA</b> .....	<b>5</b>
5.1	OVERVIEW.....	5
5.2	PACKETCABLE SMA DESIGN GOALS .....	6
5.2.1	<i>Generic Architecture Goals</i> .....	6
5.2.2	<i>SMA Signaling</i> .....	6
5.2.3	<i>Media Transport and Encoding</i> .....	6
5.2.4	<i>Quality of Service</i> .....	7
5.2.5	<i>Security</i> .....	7
5.2.6	<i>Provisioning and Management</i> .....	7
5.3	PACKETCABLE SMA DEPLOYMENT MODELS.....	7
<b>6</b>	<b>PACKETCABLE SMA ARCHITECTURE AND FUNCTIONAL COMPONENTS</b> .....	<b>8</b>
6.1	HOME DOMAIN.....	8
6.1.1	<i>SMA Gateway</i> .....	8
6.1.2	<i>Security Panel</i> .....	8
6.1.3	<i>Sensor and Controller Network</i> .....	8
6.1.4	<i>User Interface</i> .....	9
6.1.5	<i>Home IP Network</i> .....	9
6.2	ACCESS DOMAIN .....	9
6.2.1	<i>Cable Modem (CM)</i> .....	9
6.2.2	<i>Cable Modem Termination System (CMTS)</i> .....	9
6.2.3	<i>Home Router</i> .....	9
6.3	OPERATOR DOMAIN .....	10
6.3.1	<i>Event Server</i> .....	10
6.3.2	<i>Portal Server</i> .....	10
6.3.3	<i>Notification Server</i> .....	10
6.3.4	<i>STUN and TURN Servers</i> .....	10
6.4	CENTRAL STATION DOMAIN.....	11
6.4.1	<i>Central Station</i> .....	11
6.5	QOS AND PACKETCABLE MULTIMEDIA.....	11
6.5.1	<i>Policy Server</i> .....	12
6.5.2	<i>Application Server</i> .....	12
6.5.3	<i>Application Manager</i> .....	12
6.6	OPERATIONAL SUPPORT SYSTEMS.....	12
6.6.1	<i>Dynamic Host Configuration Protocol (DHCP) Server</i> .....	12
6.6.2	<i>Domain Name System (DNS) Server</i> .....	12
6.6.3	<i>Provisioning Server</i> .....	12
6.6.4	<i>Element and Network Management Systems (EMS and NMS)</i> .....	12
6.6.5	<i>Configuration Server</i> .....	12
6.6.6	<i>Time Server</i> .....	13

**7 PACKETCABLE SMA INTERFACES .....14**

7.1 SIGNALING .....14

    7.1.1 *Instructions* .....14

    7.1.2 *Events*.....15

7.2 MEDIA .....15

7.3 QUALITY OF SERVICE .....16

7.4 PROVISIONING AND MANAGEMENT .....17

    7.4.1 *DHCP- and SNMP-based mechanism* .....17

    7.4.2 *SMA Signaling based mechanism* .....19

7.5 SECURITY .....19

    7.5.1 *Signaling*.....19

    7.5.2 *Media* .....20

    7.5.3 *QoS*.....20

    7.5.4 *Provisioning and Management*.....20

**APPENDIX I ACKNOWLEDGEMENTS .....21**

## Figures

FIGURE 1 - SMA REFERENCE ARCHITECTURE.....5

FIGURE 2 - SMA SIGNALING INTERFACE.....14

FIGURE 3 - SMA INTERFACES FOR MEDIA (SMA GATEWAY IS BEHIND A NAT).....15

FIGURE 4 - SMA QoS INTERFACES .....16

FIGURE 5 - SMA PROVISIONING AND MANAGEMENT INTERFACES.....18

FIGURE 6 - SMA PROVISIONING AND MANAGEMENT INTERFACES.....19

## Tables

TABLE 1 - SMA SIGNALING INTERFACE.....14

TABLE 2 - NAT AND FW TRAVERSAL INTERFACE DESCRIPTIONS.....16

TABLE 3 - QoS INTERFACE DESCRIPTIONS .....17

TABLE 4 - PROVISIONING AND MANAGEMENT INTERFACE DESCRIPTIONS .....18

TABLE 5 - PROVISIONING AND MANAGEMENT INTERFACE DESCRIPTIONS .....19

This page left blank intentionally.

# 1 OVERVIEW

The SMA architecture is a CableLabs effort designed to facilitate deployments to address the following areas.

- Security - The ability to protect lives and property through professional monitoring, notifying first responders (e.g., fire, police, and medical), and providing emergency alerts to authorized individuals like home occupants. For example, fire and smoke sensors alert monitoring agencies, who can notify and provide critical information to local emergency personnel.
- Monitoring - The ability to self-monitor the status and activity in the home so that a user can be made aware of any desired state changes. For example, when motion is detected by a motion sensor, real-time alerts and associated data, such as video or photo clips, can be sent to a user.
- Automation - The ability to automate and remotely control lifestyle conveniences such as lighting, heating, cooling, and appliances. For example, a user can remotely use a web portal to verify and control conditions such as lighting or temperature in the home.

## 2 REFERENCES

### 2.1 Normative References

There are no normative references in this document.

### 2.2 Informative References

This technical report uses the following informative references.

- [MM-ARCH-TR] PacketCable Multimedia Architecture Framework Technical Report, PKT-TR-MM-ARCH-V02-051221, December 21, 2005, Cable Television Laboratories, Inc.
- [RFC 2616] IETF RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, June 1999.
- [RFC 2617] IETF RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999.
- [RFC 2818] IETF RFC 2818, HTTP Over TLS, May 2000.
- [RFC 4566] IETF RFC 4566, SDP: Session Description Protocol, July 2006.
- [W3 XML1.0] Extensible Markup Language (XML) 1.0 (Fourth Edition), W3C Recommendation, August 16, 2006.
- [W3 XSD1.0] XML Schema Part 1: Structures, Second Edition, W3C Recommendation, October 28, 2004.

### 2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; Internet: [www.packetcable.com/http:///](http://www.packetcable.com/http:///) or <http://www.cablemodem.com/>
- Internet Engineering Task Force (IETF), Internet: <http://www.ietf.org/>
- World Wide Web Consortium, [www.w3c.org](http://www.w3c.org), c/o MIT, 32 Vassar Street, Room 32-G515 Cambridge, MA 02139

### 3 TERMS AND DEFINITIONS

This technical report uses the following terms and definitions:

<b>ICE</b>	Internet Connectivity Establishment
<b>PacketCable Multimedia</b>	An application agnostic QoS architecture for services delivered over DOCSIS networks
<b>RESTful webservice</b>	Use of REST design principles via HTTP as the protocol

## 4 ABBREVIATIONS AND ACRONYMS

This technical report uses the following abbreviations and acronyms:

<b>AS</b>	Application Server
<b>AM</b>	Application Manager
<b>CM</b>	Cable Modem
<b>CMTS</b>	Cable Modem Termination System
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DOCSIS</b>	Data-Over-Cable Service Interface Specifications
<b>DNS</b>	Domain Name System
<b>EMS</b>	Element Management System
<b>HFC</b>	Hybrid Fiber-Coax
<b>HTTP</b>	Hyper Text Transport Protocol
<b>IP</b>	Internet Protocol
<b>NAT</b>	Network Address Translation
<b>NMS</b>	Network Management System
<b>PCMM</b>	PacketCable Multimedia
<b>PS</b>	Policy Server
<b>QoS</b>	Quality of Service
<b>REST</b>	REpresentational State Transfer
<b>SMA</b>	Security, Monitoring and Automation
<b>TLS</b>	Transport Layer Security
<b>XML</b>	eXtensible Markup Language

## 5 PACKETCABLE SMA

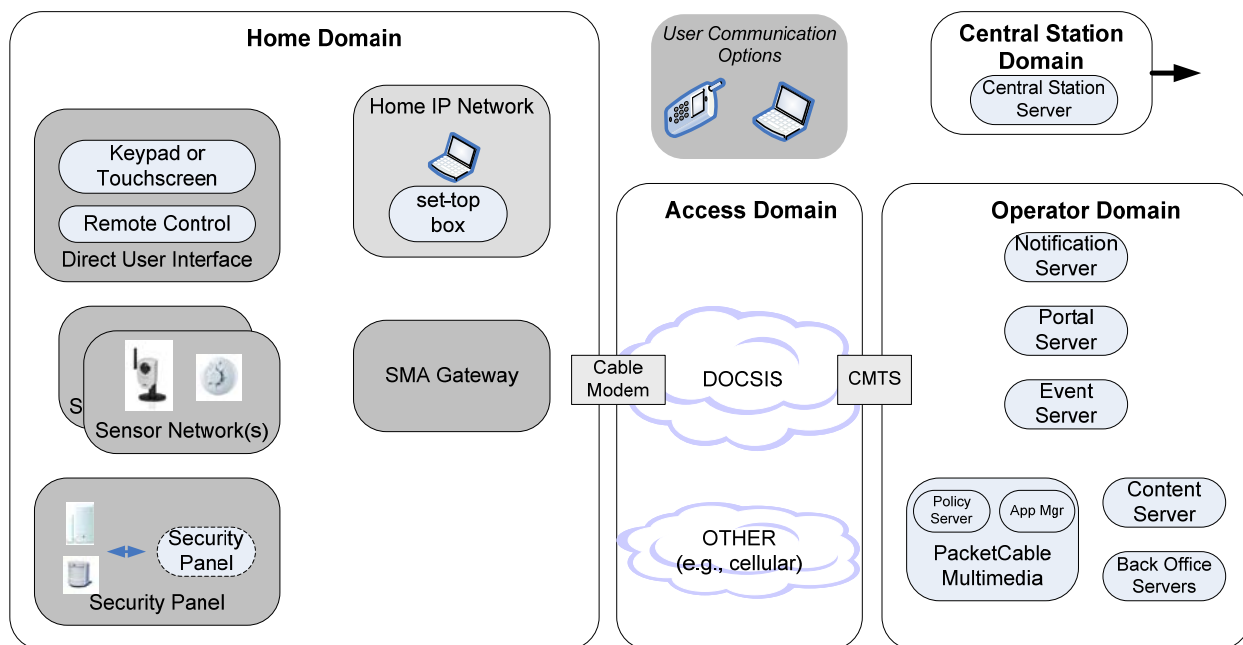
The PacketCable SMA architecture describes a set of functional groups and logical entities, as well as a set of interfaces that support the information flows exchanged between the entities.

This section provides:

- An overview of the architecture, including a description of the main functional groupings (e.g., home domain, MSO domain) and logical entities (e.g., SMA Gateway, Event Server) within those groupings;
- A set of design goals for the PacketCable SMA architecture;
- A set of SMA deployment models.

### 5.1 Overview

Figure 1 shows the logical domains of the SMA reference architecture, with each domain containing a set of logical or physical components.



**Figure 1 - SMA Reference Architecture**

The architecture is divided into several logical areas or functional groupings:

- **Home Domain:** The home domain refers to the logical collection of SMA network elements and interfaces within the user's home. SMA network elements are the sensor, control, and security panel devices that interface with an SMA Gateway. The SMA Gateway is an Operator-managed SMA component that acts as an interface between the Home Domain and the Operator Domain via the Access Domain.
- **Access Domain:** The access network elements that allow for communication between the SMA Gateway and the Operator Domain form the access domain. As shown, the DOCSIS access network is one example, and is the only access network considered by this version of the document. The diagram also acknowledges the presence of other access types, such as cellular. The access domain is also responsible for controlling any QoS establishment between the home domain and the Operator domain.

- **Operator Domain:** The Operator Domain encompasses the functional network elements and the interfaces in the operator's network that configure, manage, and control SMA elements within the home domain. Examples of elements include the Event Server, QoS, and management entities.
- **Central Station Domain:** The Central Station domain receives critical alarms and processes them according to established processes and procedures, such as attempts to alert authorities or homeowners. Elements within this domain are not within the scope of this version of the document.

## 5.2 PacketCable SMA Design Goals

In order to enable SMA deployments across the cable network infrastructure, PacketCable SMA defines interfaces in the following areas:

- SMA Signaling;
- Media Session Establishment;
- Quality of Service;
- Security;
- Provisioning and Management.

### 5.2.1 Generic Architecture Goals

The design goals of the PacketCable SMA architecture:

- Provide extensible architecture that provides a uniform set of interfaces to allow for the deployment of SMA services without impacting the underlying signaling and management platform;
- Support IPv4 and IPv6 operation;
- Leverage existing standards and open protocols whenever possible.

### 5.2.2 SMA Signaling

PacketCable SMA Signaling design goals:

- Specify the signaling requirements between the SMA Gateway and the Event Server within the Operator Domain. Specifically, this includes support for SMA events that provide information such as state changes and SMA instructions that affect state changes;
- Specify the capability to establish signaling channels between the network elements, plus they recognize, report, and recover from any interruptions.

### 5.2.3 Media Transport and Encoding

PacketCable media transport and encoding goals:

- Specify requirements to facilitate media session establishment between SMA devices and media clients via signaling between the SMA Gateway and the Event Server;
- Define a minimal set of codecs and associated media transmission protocols that may be supported;
- Specify mechanisms to facilitate media sessions when the SMA Gateway is behind a NAT device.

#### 5.2.4 Quality of Service

PacketCable QoS design goals:

- Leverage the PacketCable Multimedia specification to provide QoS when a subscriber is accessing service through the DOCSIS network;
- Support packet marking and classification from the access network such that a QoS mechanism like Differentiated Services (DiffServ) can be used in the backbone.

#### 5.2.5 Security

PacketCable security design goals:

- Support confidentiality, authentication, integrity, and access control mechanisms;
- Protect the network from various denial-of-service, network disruption, theft-of-service attacks;
- Protect the Home Domain from denial-of-service attacks, security vulnerabilities, and unauthorized access;
- Provide mechanisms for SMA Gateway authentication, secure provisioning, secure signaling, secure media, and secure software download.

#### 5.2.6 Provisioning and Management

PacketCable Provisioning design goals:

- Specify provisioning flows for an SMA Gateway to initialize in IP networks and obtain configuration;
- Specify configuration and management protocols and data models for SMA Gateways;
- Support secure software download for embedded and standalone SMA Gateways.

### 5.3 PacketCable SMA Deployment Models

PacketCable SMA supports the following deployment models:

- The SMA Gateway connects directly via a DOCSIS network;
- The SMA Gateway connects via a home router, which may or may not be managed by the Operator.

In the case of the former, the SMA Gateway can either be standalone or embedded with a DOCSIS Cable Modem. In the case of the latter, an NA(P)T (Network Address and Port Translator) and a Firewall may be present between the local network and the access network. Since NAT may modify IP addresses and ports, and a firewall restricts access, provisioning and media planes need to behave differently when these elements are inserted between the SMA Gateway and the Event Server.

## 6 PACKETCABLE SMA ARCHITECTURE AND FUNCTIONAL COMPONENTS

This section provides additional details on each of the functional areas within the PacketCable SMA architecture.

### 6.1 Home Domain

The home domain refers to the logical collection of SMA network elements and interfaces within the user's home.

#### 6.1.1 SMA Gateway

The SMA Gateway is a Customer Premise Equipment (CPE) device that works in conjunction with server counterparts in the operator domain to perform functions required for security, monitoring, and automation. The SMA gateway bridges the sensor network, the control network, and security panel network to the broadband IP network, and it uses IP protocols to carry the alarm and activity events to the operator domain servers for processing. This IP connection also carries configuration information, provisioning commands, management and reporting information, security authentication, and any real-time media such as video or audio.

The SMA gateway architecture integrates current security control panel capabilities into the gateway, creating a single unit that interconnects with widely available sensors and devices.

The SMA Gateway encompasses the following functionality:

- Sensor network adaptors: Enable communications with the sensor networks. The state of the sensor network is communicated to other components in the system through the adaptors.
- Control network adaptors: Enable communications with home control device networks. The states of home control devices are communicated to other components in the system through the adaptors.
- Security panel support: Provide interfaces for alarm panels to enable communication, including receiving events from security panel sensors.
- Network connectivity: Depending on the deployment model, the gateway includes interfaces to access technologies such as DOCSIS and Ethernet.

#### 6.1.2 Security Panel

The security panel domain includes security panels in the home and the sensors and devices connected to the security panel. The architecture supports systems to the home that include security panel systems and associated sensors, or it may utilize existing security panels in the home.

#### 6.1.3 Sensor and Controller Network

Sensors and devices in the home connected to the SMA gateway are joined together to create a sensor network in the home. There are many different sensor network technologies that use transport, including wireless, wireline, home electrical wiring, and home coax wiring. Most of the wireless technologies use a mesh network topology to provide redundancy and routing. Other devices such as IP video cameras, are also supported.

Binary sensors and devices in the sensor network, such as motion sensors and contact closures, send alarms based on built-in states relevant to the devices (e.g., motion detectors send alarms when motion is detected). Other devices, such as video cameras, are capable of sending complex data formats, such as MPEG4 and Motion JPEG. Home Control components will also be capable of both send and receive operations to perform their intended tasks (e.g., turn a light on and off, or control a thermostat).

#### **6.1.4 User Interface**

Key pads, touch screens, remote controls, and OCAP applications on a set-top box are all examples of interfaces for users to interact with the gateway while in the home. An in-home user interface will allow users to perform command and control functions such as arm and disarm, environment settings (e.g., lights, thermostat), locking doors, etc. User Interface devices capable of rendering more complex data to the user may also act as third party content screens to complement existing screens in the home.

#### **6.1.5 Home IP Network**

The home network includes existing networked components in the home, such as existing cable modems, routers, and network devices such as personal computers and IP video cameras.

### **6.2 Access Domain**

The SMA Gateway connects to the Operator Domain via the existing cable access network or other available access networks, such as cellular. The Access Network elements provide the IP connectivity and QoS resources needed by the SMA Gateway to provide PacketCable SMA services. The SMA architecture specified in this document considers only the cable access network, i.e., DOCSIS.

#### **6.2.1 Cable Modem (CM)**

The CM is the Customer Premise Equipment (CPE) used in conjunction with the CMTS to provide broadband data transport service over the Cable HFC Access Network. Based on the deployment model, the SMA Gateway can be embedded with a CM or be a standalone device that is directly connected via a CM. It can also be connected via a home router.

The DOCSIS access network needs to support full IPv6 operations with network access QoS using PacketCable Multimedia.

#### **6.2.2 Cable Modem Termination System (CMTS)**

The CMTS resides in the cable operator's headend, and, in conjunction with the CM, provides broadband data transport service over the Cable HFC Access Network. Beginning with version 1.1, DOCSIS defines a means to provide QoS on the access network. PacketCable Multimedia defines a means for IP-enabled services to request QoS from the DOCSIS network.

#### **6.2.3 Home Router**

As indicated in Section 5.3, an SMA Gateway may be connected via a home router that interfaces with the Access Domain. This has some implications for signaling, provisioning, and management. Specifically, this requires protocols to support SMA Gateways behind NAT devices.

## 6.3 Operator Domain

This section provides additional detail on each of the functions in the Operator Domain.

### 6.3.1 Event Server

The event server in the operator network provides the functionality to:

- Receive events from the gateway over access technologies, and, based on configured rules, forward these events to the Notification Server for processing (e.g., send SMS text messages or email/call the user);
- Route approved content to the SMA gateway in the home for rendering to users;
- Monitor connectivity of gateways and, based on configured rules, forward connectivity events to the Notification Server for processing (e.g., email the user).

### 6.3.2 Portal Server

The portal server, through an interface to the event server, enables user web-based control and management of the SMA system via PCs, cell phones, and other portable devices. The functions enable these interfaces to:

- Arm and disarm the system;
- Check the status of the system;
- Manage security zones (sensors);
- Configure user alerts (events, who to contact, how to contact, etc.);
- Manage/update device settings (e.g., increase temperature of house).

### 6.3.3 Notification Server

Notifications to disparate devices are managed by the notification server. It is responsible for receiving user defined alerts from the event and alarm servers and notifying the appropriate device(s) using the appropriate protocol or technology, including:

- Phone Outbound IVR (alerts via voice call generation);
- Text Messaging, including mobile SMS messaging;
- Email;
- Pager;
- Software Clients on PC and Cell phone;
- Personal Web Portal;
- IM.

### 6.3.4 STUN and TURN Servers

STUN and TURN servers are required only when an SMA Gateway is behind a NAT device and needs to establish media sessions with other media clients that may or may not be behind NAT devices. The STUN server determines one of several possible candidate media addresses using the STUN protocol. The TURN server is an extended STUN server that receives STUN Allocate requests and sends STUN responses. The TURN server is capable of acting as a data relay, receiving data on the address it provides to SMA Gateways, and forwarding it to the SMA Gateways. This data relay functionality allows media to traverse NATs in cases when other NAT traversal techniques are insufficient.

## 6.4 Central Station Domain

The central station domain contains the central station software and servers that receive critical alarms from the alarm server and forward them to emergency dispatch. Central station staff manage the incoming alarms and may interact with the SMA system by utilizing two-way audio and video or validating alarm logs. This may be accomplished through the use of an SMA application or web portal for central station personnel.

### 6.4.1 Central Station

The Central Station performs the following functions in the SMA Reference Architecture:

- Receives emergency events, such as burglary, smoke detection, or medical emergency;
- Participates in viewing upstream media paths - such as audio and video - to verify that an emergency is taking place ("look and listen into the home");
- Sends live media back to the SMA Gateway, in order to (for example) engage in a two-way voice conversation with the customer on supported equipment;
- Makes calls to notify people on the customer's call list that an emergency is taking place;
- Calls the Police, Fire Department, or Medical Personnel in the locality of the customer, to have them dispatch to the home.

It is important to note that the current SMA Working Group is not defining an interface to the central stations. This is left to the individual vendor implementations. Each vendor may implement this connection point in any of the following ways:

- Connecting from home security equipment directly to central station (bypassing SMA Gateway);
- Connecting from SMA Gateway directly to central station;
- Connecting from Operator Network (Event Server) directly to central station.

Furthermore, it is likely that each central station participating in the monitoring of alarm accounts will have a different style or preference for receiving alarm event data. These mechanisms may include:

- POTS-based telephone event reception;
- IP-based event reception over the public Internet;
- IP-based event reception over a private dedicated T1 (or other Broadband pipe) between Central Station and Operator Network.

## 6.5 QoS and PacketCable Multimedia

PacketCable Multimedia defines an IP-based platform for delivering QoS-enhanced multimedia services over DOCSIS access networks. This platform allows the core capabilities of PacketCable (e.g., QoS authorization and admission control, event messages for billing and other back-office functions, and security) to support a wide range of IP-based services. PacketCable Multimedia components offer a general-purpose platform for cable operators to deliver a variety of IP-based multimedia services that require QoS treatment.

The PacketCable Multimedia architecture defines the interactions between a CMTS, a Policy Server, and an Application Manager. The CMTS is included as part of the Access Network. The Application Manager is specific to each application. The Policy Server, which is a unique PacketCable Multimedia element that may communicate with a variety of Application Managers, and the Application Server, which is an element specific to each application, are described below.

For more information about the PCMM architecture, please refer to the [MM-ARCH-TR].

### **6.5.1 Policy Server**

The Policy Server primarily acts as an intermediary between Application Manager(s) and CMTS(s) for QoS session management. It applies network policies to Application Manager requests and proxies messages between the Application Manager and CMTS.

### **6.5.2 Application Server**

An Application Server (AS) provides application-specific services. An AS may influence SMA operations based on its supported services. It may also host and execute services. An AS may initiate services or terminate services on behalf of an SMA gateway.

### **6.5.3 Application Manager**

The Application Manager (AM) plays a coordinating role involving application signaling and semantics and as well as interactions with the PacketCable Multimedia policy framework. The Application Manager receives service requests from an Application Server.

## **6.6 Operational Support Systems**

The Operational Support Systems manage functions such as billing, provisioning, customer care, and network management that are required to support PacketCable SMA services.

### **6.6.1 Dynamic Host Configuration Protocol (DHCP) Server**

A DHCP server is used when the SMA Gateway's local network is under the control of the Operator. It provides information, such as an IP address, that allows the SMA Gateway to connect to the Operator's IP network. SMA Gateways that connect via a home router may obtain this information from the Home Router's DHCP server, if available.

### **6.6.2 Domain Name System (DNS) Server**

A DNS server is used to resolve DNS entities (e.g., Fully Qualified Domain Name or FQDNs) into network addresses and vice-versa. An Operator's DNS service is expected to be utilized by SMA Gateways and SMA devices for locating network entities or routing of messages.

### **6.6.3 Provisioning Server**

The Provisioning Server is a PacketCable-defined component responsible for authenticating the SMA Gateway, providing the configuration details (e.g., configuration server address), and for the establishment of management communications with the SMA Gateway.

### **6.6.4 Element and Network Management Systems (EMS and NMS)**

EMS and NMSs perform the monitoring and management of the SMA functional components. While the PacketCable SMA architecture specifies the monitoring and management requirements for the SMA Gateway, EMS and NMSs control and manage components such as SMA devices and Operator Domain elements.

### **6.6.5 Configuration Server**

The configuration server is responsible for providing the configuration to the SMA Gateway.

### **6.6.6 Time Server**

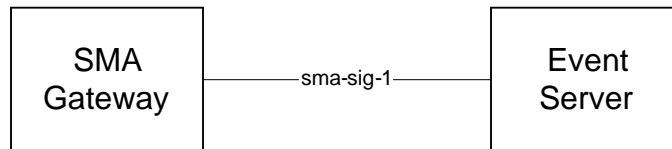
The time server is responsible for providing the time to the SMA Gateway.

## 7 PACKETCABLE SMA INTERFACES

PacketCable SMA specifies functional entities and protocol interfaces between them. This section provides an overview of the interfaces in the areas of Signaling, QoS, Security, and provisioning and management.

### 7.1 Signaling

The PacketCable SMA Signaling interface is illustrated in Figure 2.



**Figure 2 - SMA Signaling Interface**

The interface, sma-sig-1, is specified between the SMA Gateway and the Event Server. It allows for the communication of messages between the two entities. The interface illustrated in Figure 2 is described in Table 1.

**Table 1 - SMA Signaling Interface**

Interface	PacketCable Network Elements	Interface Description
sma-sig-1	SMA Gateway - Event Server	<p>Enables the SMA Gateway to exchange messages to, and from, the Event Server.</p> <p>The interface is realized using a RESTful web service approach using HTTP 1.1 ([RFC 2616]) as the communication protocol and W3C XML 1.0 ([W3 XML1.0]) for data. The data models will be created using W3C XML Schema Definition 1.0 ([W3 XSD1.0]).</p>

The communication between the entities is via a stateless messaging framework, i.e., the signaling messages are exchanged asynchronously and do not follow a request-response paradigm. Any state changes are reflected via further asynchronous messages.

The messages exchanged can be classified into two types: instructions and events. The message types are explained in the following sub-sections.

#### 7.1.1 Instructions

The Event Server can send across messages that control the state of the SMA services provided by the SMA Gateway and the SMA network elements in the Home Domain. Such messages are termed instructions. A non-exhaustive list of instruction messages follows:

- Create SMA Device: adds a new SMA Device to the SMA Gateway;
- Remove SMA Device: removes an SMA Device from the SMA Gateway;
- Set Property: sets an SMA Device property;
- Get Property: gets an SMA Device property;
- Query Home Domain: returns the queried properties (e.g., connection status) for SMA devices that are connected to the SMA Gateway in the home domain;

- Create Logical Directive: a new directive (e.g., filters, triggers, schedules) is added;
- Modify Logical Directive: a previously configured logical directive is updated;
- Delete Logical Directive: removes a previously configured directive.

### 7.1.2 Events

Events are messages that report the state of a particular entity or action on the originating entity. Events can be generated as a result of modification to SMA services, but they do not modify the SMA services. They are transmitted from the SMA Gateway to the Event Server and, optionally, the other way around. Examples of events include:

- SMA device connectivity: for example, new SMA device found;
- SMA device state change: for example, the motion sensor was triggered.

## 7.2 Media

PacketCable SMA supports both video and audio streams, also referred to as media sessions. Media sessions can be requested by users who are within the home domain or outside of the home domain connecting through the Event Server.

Media session establishment is supported via the SMA Signaling interface, sma-sig-1, and the use of the Session Description Protocol (SDP) as specified in [RFC 4566]. For SMA Gateways that can reside behind NAT devices, PacketCable SMA architecture specifies the use of ICE methodology using STUN and TURN servers to support media sessions. Figure 3 provides the interfaces required for media transport.

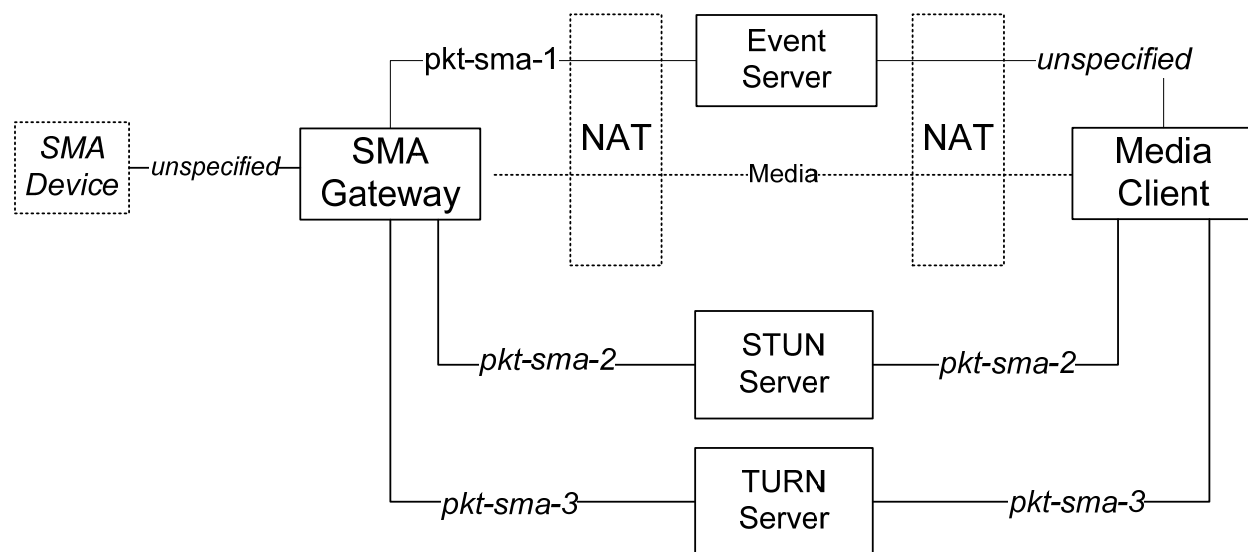


Figure 3 - SMA Interfaces for Media (SMA Gateway is behind a NAT)

The interfaces shown in Figure 3 are described in Table 2.

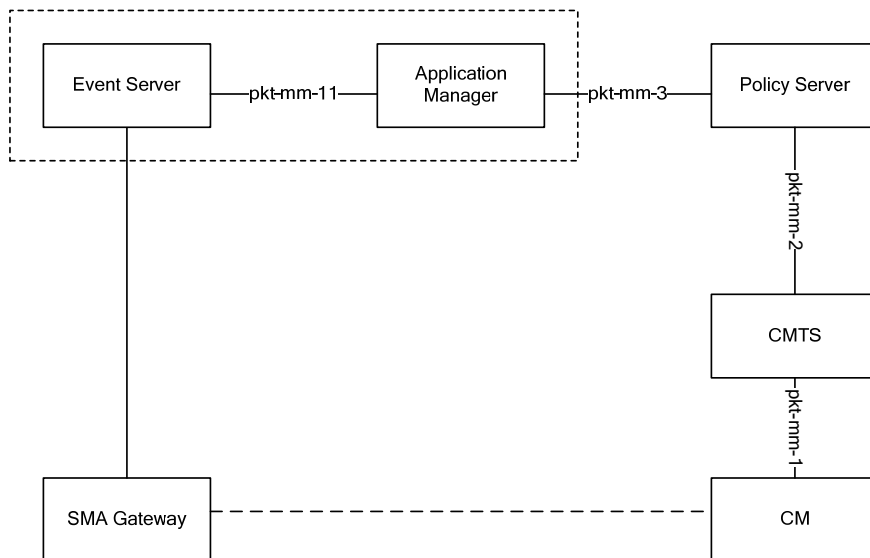
**Table 2 - NAT and FW Traversal Interface Descriptions**

Interface	PacketCable Network Elements	Interface Description
pkt-sma-1	SMA Gateway - Event Server	Refer to Table 1.
pkt-sma-2	SMA Gateway - STUN Server Media Client - STUN Server	Enables the SMA Gateway to determine one of several possible candidate media addresses using STUN, in support of the ICE methodology. Only SMA Gateways that can reside behind NAT devices need this interface.  This interface can also be used by media clients that may reside behind NAT devices.
pkt-sma-3	SMA Gateway - TURN Server Media Client - STUN Server	Allows the SMA Gateway to access a TURN server in order to support the traversal of a NAT that does not perform Address Independent Mapping. Only SMA Gateways that can reside behind NAT devices need this interface.  This interface can also be used by media clients that may reside behind NAT devices.

### 7.3 Quality of Service

The Quality of Service approach for SMA is based on PacketCable Multimedia. For the purposes of providing Quality of Service, an Application Manager (AM) serves as the interface between the PacketCable SMA architecture and the PacketCable Multimedia architecture. Its function is to receive QoS messages from the SMA Event Server and to formulate appropriate messages to the PacketCable Multimedia Policy Server.

Figure 4 illustrates the relationship between the Application Manager, the SMA Gateway, and the PacketCable Multimedia Policy Server. Note also that the Application Manager shown here as a distinct function may be packaged along with an SMA Event Server.



**Figure 4 - SMA QoS Interfaces**

The interfaces shown in Figure 4 are described in Table 3.

**Table 3 - QoS Interface Descriptions**

<b>Interface</b>	<b>PacketCable Network Elements</b>	<b>Interface Description</b>
pkt-mm-1	CM - CMTS	The Cable Modem (CM) may request QoS from the CMTS via DOCSIS 1.1 DSx signaling. Alternatively, the CMTS may instruct the CM to setup, tear down, or change a DOCSIS service flow in order to satisfy a QoS request, again via DSx signaling.
pkt-mm-2	Policy Server - CMTS	This interface is fundamental to the policy-management framework. It controls policy decisions, which may be: (a) pushed by the Policy Server (PS) onto the CMTS, or (b) pulled from the PS by the CMTS. The interface also allows for proxied QoS requests on behalf of a client. In some scenarios, this interface may also be used to inform the PS when QoS resources have become inactive.
pkt-mm-3	Application Manager - Policy Server	The Application Manager (AM) may request that the PS install a policy decision on the CMTS on behalf of the client. This interface may also be used to inform the AM of changes in the status of QoS resources.
pkt-mm-11	Application Server (Event Server) - Application Manager	The Application Server uses this interface to send network resource requests on behalf of the client to the AM.  This interface may also be used to notify the AS of changes in the status of the network resources.

Refer to [MM-ARCH-TR] for more information.

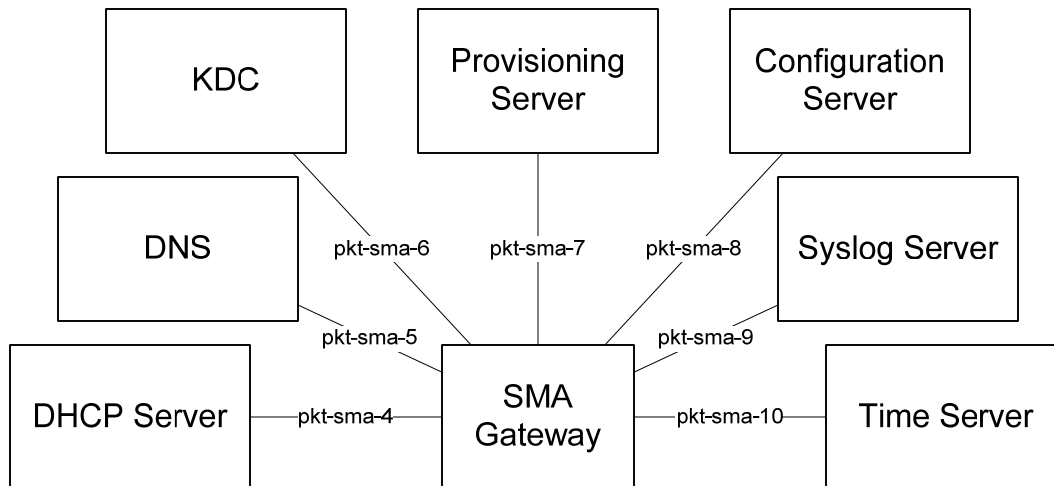
## 7.4 Provisioning and Management

The SMA Architecture addresses the provisioning and management of the SMA Gateway. Provisioning refers to the processes involved in the initialization of the SMA Gateway to establish connectivity with the MSO's network and to obtain the necessary configuration to provide SMA Services. Management refers to the protocols, methodologies, and interfaces that enable monitoring, controlling, and ensuring availability of offered SMA services.

To support the two deployment models - clients that connect directly via a DOCSIS network and clients that can connect via home routers - PacketCable SMA specifies two provisioning mechanisms. For the former deployment model, the use of DHCP and SNMP-based mechanisms is specified. For the latter, the re-use of the SMA Signaling Interface, pkt-sma-1, is specified.

### 7.4.1 DHCP- and SNMP-based mechanism

Figure 5 illustrates the DHCP- and SNMP-based provisioning and management interfaces required for SMA.



**Figure 5 - SMA Provisioning and Management Interfaces**

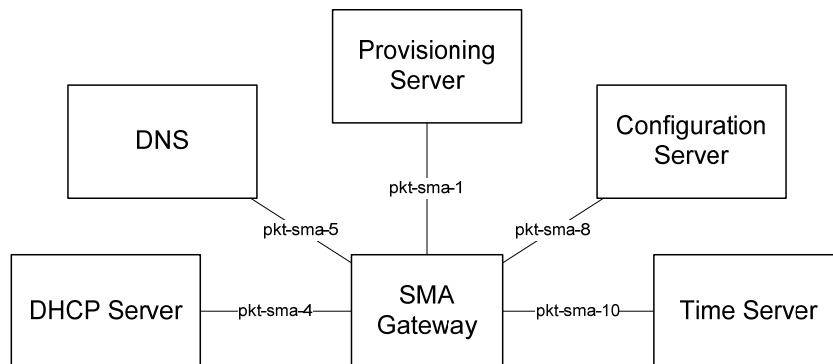
The interfaces depicted in Figure 5 are described in Table 4.

**Table 4 - Provisioning and Management Interface Descriptions**

Interface	PacketCable SMA Network Components	Interface Description
pkt-sma-4	SMA Gateway - DHCP	Allows the SMA Gateway to obtain IP parameters for IP communication (e.g., IP address, DNS server addresses).
pkt-sma-5	SMA Gateway - DNS	Allows the SMA Gateway to resolve DNS names for location of network elements or routing of messages.
pkt-sma-6	SMA - KDC	Allows the SMA Gateway to authenticate itself to the Key Distribution Center (KDC) using the Kerberos protocol.
pkt-sma-7	SMA Gateway - Provisioning Server	Allows the SMA Gateway to authenticate and exchange device capabilities with the Provisioning Server. Once authenticated, the SMA Gateway uses this interface to obtain configuration information, such as the configuration server and configuration filename. This is an optional element that is used in certain provisioning flows.
pkt-sma-8	SMA Gateway - Configuration Server	Allows the SMA Gateway to obtain its configuration file.
pkt-sma-9	SMA Gateway - Syslog Server	Allows the SMA Gateway to report management events via Syslog.
pkt-sma-10	SMA Gateway -Time Server	Allows the SMA Gateway to obtain its time information to ensure accuracy during SMA signaling, e.g., events.

### 7.4.2 SMA Signaling based mechanism

The SMA Signaling based mechanism re-uses the SMA Signaling interface, pkt-sma-1, and some of the interfaces from the DHCP- and SNMP-based mechanism. The main differences between the DHCP- and SNMP-based mechanisms is that the provisioning messages are transmitted via pkt-sma-1. The Provisioning Server in this case is either a logical element that can be collocated within the Event Server, or a separate entity, in which case the SMA Gateway needs to establish multiple HTTP 1.1 connections (one to the Provisioning Server and one to the Event Server).



**Figure 6 - SMA Provisioning and Management Interfaces**

The interfaces depicted in Figure 6 are described in Table 5.

**Table 5 - Provisioning and Management Interface Descriptions**

Interface	PacketCable SMA Network Components	Interface Description
pkt-sma-4	SMA Gateway - DHCP	Refer to Table 4.
pkt-sma-5	SMA Gateway - DNS	Refer to Table 4.
pkt-sma-1	SMA Gateway - Provisioning Server	Refer to Table 1.
pkt-sma-8	SMA Gateway - Configuration Server	Refer to Table 4.
pkt-sma-10	SMA Gateway -Time Server	Refer to Table 4.

## 7.5 Security

The PacketCable SMA Security architecture requires security for all the specified interfaces. This includes signaling, QoS, provisioning, and management. The security requirements include authentication of the entities involved: integrity protection and optional privacy.

### 7.5.1 Signaling

Given that sma-sig utilizes HTTP for transport, the architecture uses HTTP over TLS ([RFC 2818]) for integrity protection and, optionally, privacy. Furthermore, HTTP over TLS sessions should be "mutually authenticated" - in other words, both the Gateway, and the Event Server, must authenticate to each other. Authentication of the Event Server is accomplished by verifying the Server certificate during TLS establishment. SMA Gateway authentication can be accomplished either via certificates stored on clients or by using digest authentication ([RFC 2617]).

### **7.5.2 Media**

Media session establishment is facilitated via the signaling interface, pkt-sma-1, which is secured as specified in Section 7.5.1. The media sessions themselves are secured using the utilized media transport protocols.

### **7.5.3 QoS**

The SMA Architecture reuses the PacketCable Multimedia Architecture for QoS, along with the security recommendations. No additional considerations are added.

### **7.5.4 Provisioning and Management**

The SMA Architecture requires provisioning mechanisms to provide the security considerations. Specifically, it supports mutual authentication between the components and integrity protection. For sensitive configuration data, privacy is supported.

Within the DHCP- and SNMP-based provisioning, the security requirements are met using Kerberized SNMPv3 with authentication facilitated by the device's X.509 certificate. When the SMA Signaling interface, pkt-sma-1, is used for provisioning, it is secured as specified in Section 7.5.1.

## Appendix I      Acknowledgements

This technical report was developed and influenced by numerous individuals representing many different vendors and organizations. CableLabs hereby wishes to thank everybody who participated directly or indirectly in this effort.

CableLabs wishes to recognize the following individuals for their significant involvement and contributions this technical report (in alphabetical order):

- Bryan Field-Elliot, NextAlarm
- Jerry Mahler, Motorola
- Michel Kohanim, Universal Devices
- Wade Cohn, uControl

CableLabs also wishes to thank the members of the CableLabs SMA Vendor Focus Team and Roy Perry (CableLabs) for reviews and comments.

*Kevin Johns and Sumanth Channabasappa, CableLabs*

---

---