PacketCable™ OSS Overview Technical Report

PKT-TR-OSSI-V02-991201

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.

Document Status Sheet

Document Control Number:	PKT-TR-OSSI-V02-991201
Document Title:	PacketCable™ OSS Overview Technical Report
Revision History:	V01 – Released October 30, 1999 V02 – Released December 1, 1999
Date:	December 1, 1999

Contents

1 INTRODUCTION....1

1.1 Purpose....1

1.2 Background....2

1.3 Scope....3

1.4 Document Overview....4

1.5 Requirements Syntax....4

2 ARCHITECTURAL OVERVIEW....6

2.1 Typical Network Elements....8

2.1.1 PacketCable Network Elements....8

2.1.2 DOCSIS Network Elements....8

2.1.3 Standard Internet Elements....8

2.2 PacketCable Element Management System (EMS)....9

2.3 PacketCable Network Management System (NMS)....9

2.4 DOCSIS Element Management System (EMS)....10

2.5 DOCSIS Network Management System (NMS)....11

2.6 Internet Management System....11

2.7 Policy Services....11

2.8 Telephone Number (TN) Admin Database....12

2.9 Network Inventory / Topology Database....12

2.10 Name Server Database....12

2.11 Customer Records Database....13

2.12 Device Provisioning....13

2.13 Customer Interface....13

2.14 3rd Party Interconnect (Bonding Gateway)....13

2.15 Asset and Work Force Management....13

2.16 Customer Care....14

2.17 Customer Service Management....14

2.18 Trouble Management....14

2.19 Billing....14

2.20 Network Planning and Engineering....15

2.21 Field Technician....15

3 MAPPING INTO THE TMN MODEL....16

3.1 Business Management Layer 16
3.2 Service Management Layer 17
3.3 Network Management Layer 17
3.4 Element Management Layer 17
3.4.1 SNMPv3 18
3.4.2 PacketCable MIBs 18
3.5 Network Element Layer 18
4 OPERATIONAL PROCESSES 19
4.1 Phase 1 Processes 20
4.1.1 Device Provisioning 20
4.1.2 Customer Service Provisioning (*a.k.a.* Order Handling) Process 20
4.1.3 Accounting (aka Invoicing and Collections) Process 25
4.2 Phase 2 Processes 27
4.2.1 Network Planning & Development 27
4.2.2 Network Provisioning 27
4.2.3 Network Inventory Management 28
4.2.4 Network Testing, Maintenance & Restoration 28
4.3 Out of Scope Processes 28
4.3.1 Customer Care and Contact Management 28
4.3.2 Sales Process 28
4.3.3 Problem Handling Process 28
4.3.4 Customer QoS Management 29
4.3.5 Service Planning and Development Process 29
4.3.6 Service Problem Resolution Process 29
4.3.7 Service Quality Management Process 29
4.3.8 Rating and Discounting Process 29
4.3.9 Content Provider Management 29
5 CONCLUDING REMARKS 30
APPENDIX A. ACKNOWLEDGEMENTS 31
APPENDIX B. REFERENCES AND BIBLIOGRAPHY 32
APPENDIX C. GLOSSARY 34
APPENDIX D. REVISIONS 45

Figures

Figure 1-1. PacketCable Network Component Reference Model (partial) 2
Figure 4-1.TM Forum's High Level Process Breakdown 19
Figure 4-2. Billing – Process Flow Diagram 26

1 INTRODUCTION

1.1 Purpose

The primary purpose of this overview document is to introduce a high-level Operations Support System (OSS) framework for PacketCable™ products and services. This document describes at a very high level the key processes involved in an end-to-end Operations Support System / Backoffice Support System (OSS/BSS) management system for a PacketCable network.

Strictly speaking, the terms OSS and BSS refer to different types of management functions. The term OSS refers to facilities management or network management functions and typically includes fault management, performance management, and security management. The term BSS refers to business management functions and typically includes accounting management and configuration management.

A number of organizations have proposed frameworks for conceptually organizing OSS/BSS management functions in an attempt to clearly identify interfaces both internal to and between these management functions. Both the ITU and the TeleManagement Forum (formerly the NMF) have developed frameworks that organize combined OSS/BSS functions into the following areas: business management, service management, network management and element management. In these frameworks, the separation of OSS and BSS functions are no longer strictly enforced, and all of these functions are generally classified as OSS functions. Throughout the remainder of this document, the term OSS will be used to refer to all OSS/BSS functionality.

It is the intent of this document to facilitate discussions among the CableLabs® member companies and other interested parties concerning PacketCable OSS requirements. The reference architecture for the PacketCable Network is shown in Figure 1-1 below:

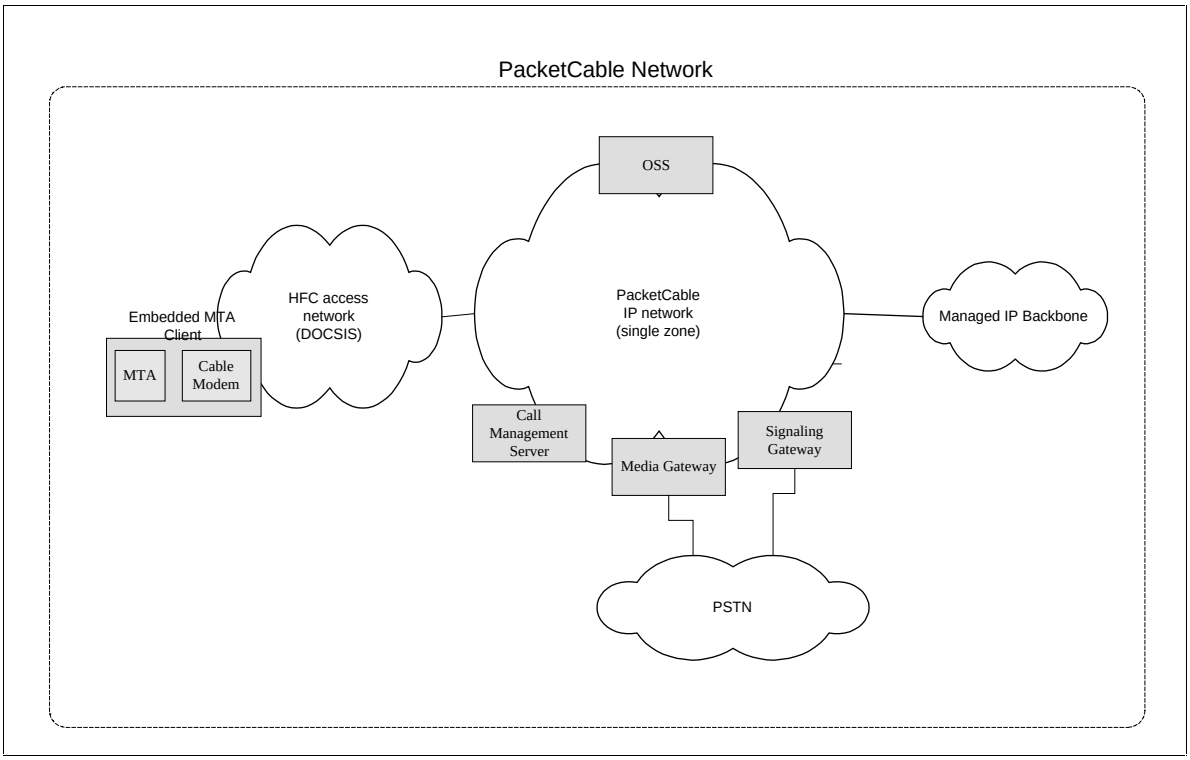

Figure 1-1. PacketCable Network Component Reference Model (partial)

1.2 Background

This section describes a typical OSS environment from the viewpoint of three traditional service providers: telco, data network, and cable operator. Some level of convergence must occur within these three environments in order to gain a common understanding of the OSS requirements of a PacketCable network. This document discusses OSS functions in terms of the operational processes that are required to deliver voice, video and other multimedia services on a PacketCable network.

It is difficult to define a "typical" OSS for a traditional telephone company environment. Some telcos have very large, very well integrated OSSs. Other telco OSS environments may contain several completely independent and stand-alone systems. Back-office management systems may focus on high-level processes such as order entry and billing. Operations management systems may require manual entry of information such as customer telephone number and other configuration parameters. These manual systems tend to be difficult to incorporate into newer, more automated systems. The large, very well integrated telephony OSSs are optimally designed to support telephony services and cannot be easily extended to support mixed services such as voice, video and data.

A traditional IP data network OSS environment typically relies on information generated by routers, switches, or other network elements. Most routers are capable of logging usage, fault, security, accounting, performance and other information. Often this data is written to log files stored on the network equipment or accessed via a network management system.

It is difficult to define the typical OSS for a traditional cable environment. Typical cable OSSs are centered around the billing system. The billing system tends to incorporate all the provisioning, customer care, and trouble ticket functions. Experience has shown that these monolithic billing systems are not easily extensible to support new mixed services such as voice, video and data. Provisioning functions, such as activating pay-per-view, tend to be reasonably simple and more easily automated. Commonly available HFC network management and monitoring tools for network inventory and topological mapping are available.

In an effort to provide a common understanding of a PacketCable OSS environment, this document will provide both a top-down and bottom-up view of an OSS. The top-down approach is best described in the process-based OSS framework currently used by the TeleManagement Forum. The bottom-up approach is best described in the ITU's layer-based TMN framework. A combined approach using key concepts from both frameworks has been selected to best describe the PacketCable OSS while keeping current with industry-accepted OSS frameworks in a rapidly converging service provider environment.

1.3 Scope

A number of documents and specifications describe the PacketCable project. The "PacketCable Architecture Framework" [17] is the starting point for understanding the PacketCable project and the various PacketCable Interface Specifications, technical reports and other PacketCable documents.

The main areas of concern for any OSS are fault management, performance management, security management, accounting management, and configuration management. These topics will not be addressed in detail in this OSS overview document, but will be addressed in PacketCable documents and/or specifications developed by the PacketCable Primary Line, Security, and Billing focus teams.

The scope of this PacketCable OSS overview document is limited to providing the starting point for understanding the PacketCable OSS at a high level. This document defines terminology, architecture, operational processes, interfaces and data flows. It also introduces a plausible range of operational processes that a cable operator might employ to launch and manage PacketCable products and services. The operational processes contained in the architectural model identified in this document are not intended to be prescriptive—they comprise one possible OSS model. It is understood that each cable operator may use the architectural model described in this document as a guideline. Each cable operator may then determine which operational processes are required and the timeframe in which these processes will be phased into their OSS to best meet their specific business needs.

The operational processes and interfaces examined in detail in section 4 of this document have been identified by CableLabs member companies as critical to the operation of a PacketCable network. For this reason, these interfaces warrant further specification to ensure multi-vendor interoperability. Interface specification details are described in PacketCable PKT-OSSI specification documents. The ultimate

objective of the PKT-OSSI Specifications is to enable prospective PacketCable vendors to address the OSS requirements in a uniform and consistent manner necessary for the commercial deployment of PacketCable products and services.

In an effort to keep pace with the larger PacketCable project and interface specification development effort, the OSS operational processes and interfaces are addressed in a phased approach. Phase one processes are required to support interface specifications developed for phase one of the PacketCable project. It should also be understood that not every operational process or interface within an operational process requires detailed analysis.

For a complete list of PacketCable specifications, please refer to URL http://www.packetcable.com.

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.

1.4 Document Overview

Section 1 - Introduction

Section 2 - Architectural overview

Section 3 - Mapping into the TMN model

Section 4 - Operational Processes

1.5 Requirements Syntax

Throughout this document, words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word or the adjective "REQUIRED" means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.

"SHOULD"	This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

Other text is descriptive or is explanatory.

2 ARCHITECTURAL OVERVIEW

This section provides an overview of the functional components required to implement a PacketCable capable OSS. The functional components listed in this section are considered the minimum set required to efficiently and effectively manage a PacketCable network to provide services to a customer. These functional components may be performed by manual and/or automated procedures. They may be resident on a single piece of hardware or distributed across multiple pieces of hardware.

Figure 2-1 depicts the functional components of the PacketCable OSS and the interaction with the typical PacketCable network elements. The typical PacketCable network elements are described in the PacketCable Architecture document [17] and will not be discussed in detail in this document. Shaded components in the diagram are part of the PacketCable OSS. Each component is described in detail in the sections following the diagram.

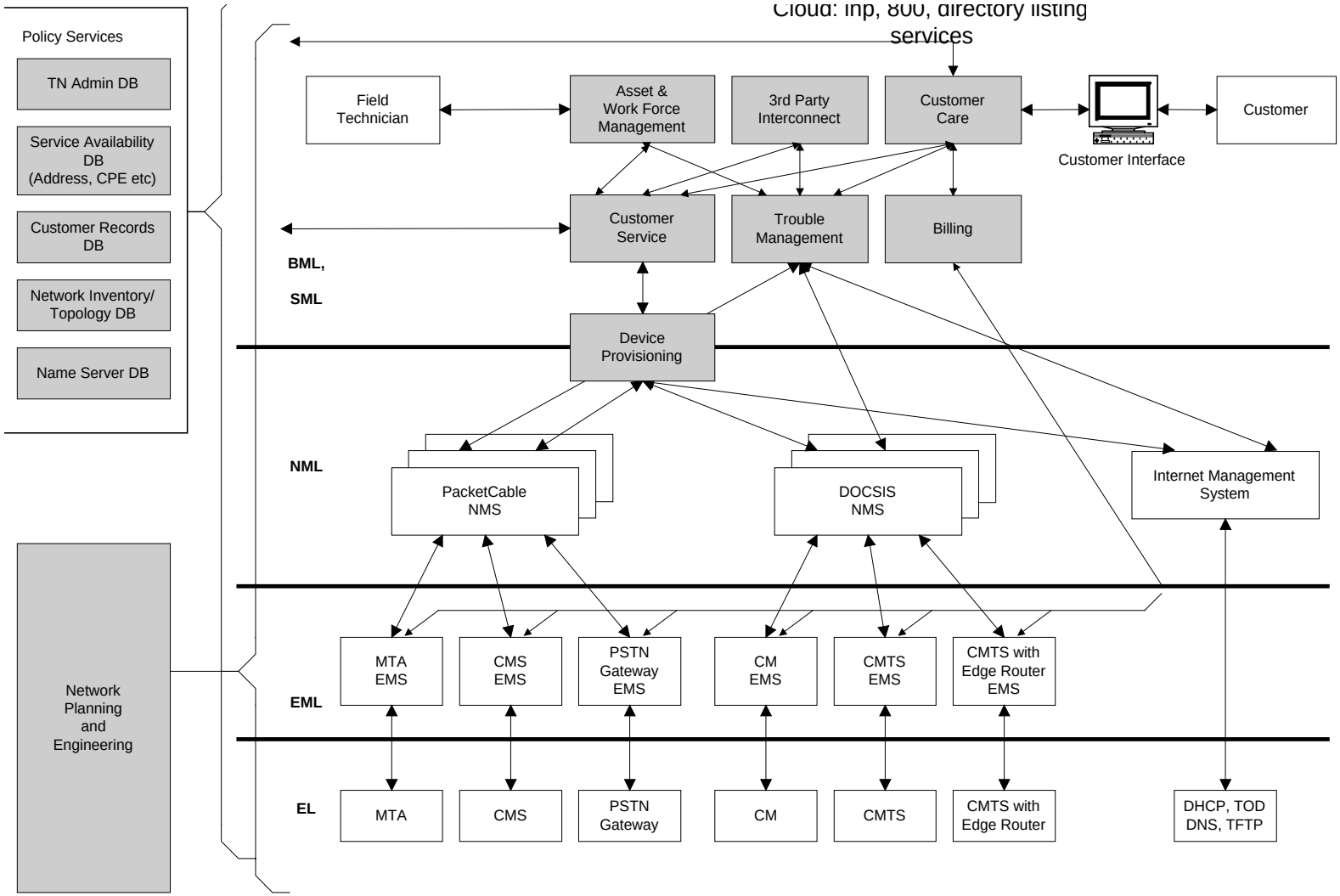

Figure 2.1 PacketCable Network Elements and OSS Components

Figure 2-1 shows the interaction between the logical OSS components. The figure shows both Policy Services as well as Network Planning and Engineering spanning all layers.

This figure does not explicitly show redundant components. In order to provide carrier-grade service, many key OSS and PacketCable components must be redundant. Carrier-grade requirements are addressed in the PacketCable Primary Line focus team documents.

This figure does not explicitly show security or other authentication servers. These issues will be addressed in the PacketCable Security focus team documents.

2.1 Typical Network Elements

2.1.1 PacketCable Network Elements

The PacketCable network elements are described in detail in the PacketCable Architecture document [17]. A brief explanation is included in this section for completeness.

MTA – multimedia terminal adapter (MTA) which contains the media interface to voice and/or video devices. Two types of MTAs exist – a standalone MTA with a subscriber LAN interface to access the PacketCable service (e.g. ethernet), or an embedded MTA with an embedded DOCSIS CM MAC and PHY.

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

PSTN Gateway – The PSTN gateway provides access from the subscriber network into the PTSN network.

2.1.2 DOCSIS Network Elements

The DOCSIS network elements are described in detail in the DOCSIS Radio Frequency Interface Specification [20].

2.1.3 Standard Internet Elements

- DNS – Domain Name System Server maps IP addresses to ASCII domain names
- DHCP – Dynamic Host Configuration Protocol Server dynamically allocates IP addresses and client configuration information to IP devices.
- TOD – Time of Day Server
- TFTP – Trivial File Transfer Protocol Server transfers files to client devices.

2.2 PacketCable Element Management System (EMS)

The PacketCable Element Management System is made up of SNMPv3 managers for agents at the element layer. Other processes may transfer data from the PacketCable network elements up to processes in higher layers. The SNMPv3 agent typically handles fault, configuration and provisioning, accounting, performance and security data for the element it is managing.

Please refer to the PacketCable MIB framework document [28] for more information on PacketCable's use of SNMPv3.

Element fault management can be defined as the processes used to manage and repair or temporarily work around faults (hardware and software) within a network element. This includes such things as device alarm reporting/suppression, and routine or on-demand diagnostic testing. The element management system must forward fault indications (these may be correlated and filtered indications rather than the original indications) to the network management system for the network management system to determine the impact the element fault will have on the network.

Element configuration and provisioning management can be defined as the processes used to configure network element. This includes such things as component management and device provisioning.

Element accounting management can be defined as the processes that monitors device usage. This includes such things as how much of a device's resources are used on a per call and/or per customer basis.

Element performance management can be defined as the processes that monitor the network element. Information collected should include device utilization, transmission faults, packet loss and/or delay and, for voice communications applications, such things as dropped or blocked calls. Monitoring of network element may also be used to determine marginal network components and in conjunction with fault management schedule maintenance before failures occur.

Element security management can be defined as the processes that police access to network elements. Element security management determines who or what has access to the device it manages and the breadth of access. For example, a service technician may be allowed to monitor the status of a particular device, where as the policy management system may be given complete access to configure or update the device.

2.3 PacketCable Network Management System (NMS)

The PacketCable Network Management System functional component is responsible for interfacing to one or more PacketCable Element Management Systems. The PacketCable NMS typically handles network-wide fault, configuration and provisioning, accounting, performance and security issues for the EMS or collection of EMS to which it interfaces. A single PacketCable NMS may interface with a single or multiple PacketCable EMSs. For example, a single PacketCable NMS may interface with multiple MTA EMSs and/or multiple CMS EMSs and/or other EMSs such as announcement servers. Alternatively, one NMS may handle the CMS EMSs

in a geographic region while a different NMS may handle the HFC cable plant EMSs for that same region. Many different logical configurations can be envisioned and will not be enumerated in this document.

It's possible that a PacketCable NMS may interface with zero or more DOCSIS EMSs. It's possible that a PacketCable NMS would interface with a larger Network Management System or a "Manager of Managers".

Network fault management can be defined as the processes used to manage and repair or temporarily work around faults in the network. This includes such things as alarm filtering and correlation as well as network diagnostic testing. The Network Fault management system must be able to handle faults reported either automatically by the network element managers or from external human interfaces (e.g. customer-reported faults). The correlation of faults and alarms reported within a system, especially multiple faults may be either manual or automatic but does require access to some type of network inventory and topological map of the network. This topic includes redundancy management, protection schemes, routine maintenance, trouble tickets and trouble tracking.

Network configuration and provisioning management can be defined as the processes used to configure network resources. This includes such things as path/link management and call provisioning.

Network accounting management can be defined as the processes that monitors network usage. This includes such things as the volume and duration of network resources used per call and/or per customer.

Network performance management can be defined as the processes that monitor the network. Information collected should include network devices, network utilization. The information collected can be used to plan network evolution and ensure service level agreements and customer service contracts (QoS) are being met. Network performance management also includes capacity monitoring, and performance planning.

Network security management can be defined as the processes that restricts access to network services. Network security management determines who or what has access to which sections of the network. Network security management can also provide various levels of control to different sections of the network on a per user or per system basis.

2.4 DOCSIS Element Management System (EMS)

A DOCSIS 1.0 EMS typically is an SNMPv1 or SNMPv2 agent that communicates directly with the DOCSIS network elements. A DOCSIS 1.1 EMS requires the use of SNMPv3 agents.

The DOCSIS element management systems (EMS) are described in detail in the DOCSIS Radio Frequency Interface Specification [20].

2.5 DOCSIS Network Management System (NMS)

The DOCSIS network management systems (NMS) are described in detail in the DOCSIS Radio Frequency Interface Specification [20].

2.6 Internet Management System

The Internet Management Server manages the IP servers required to provision the PacketCable MTA and the DOCSIS CM. The typical components managed by the Internet management system are the ToD, TFTP, DNS and DHCP servers.

Please refer to the PacketCable MTA provisioning spec [4] for a detailed description of device provisioning.

This system may allow creation and modification of the configuration files that are sent to the MTA and CM using TFTP. This component may support both the DOCSIS and PacketCable provisioning requirements. This would also manage the IP address ranges.

The Internet Management System functionality may be performed manually by a network administrator using the standard interfaces to the ToD, TFTP, DNS and DHCP servers.

2.7 Policy Services

The policy services system(s) contain(s) information about a service provider's physical network, service capabilities of these physical elements, and customer information such as services to which a customer is allowed. A policy services system is critical for QoS because it defines the priorities used by the CMS and CMTS for the DOCSIS upstream and downstream service class names. Routing policies may be defined that pertain to congestion conditions which would allow traffic routing to alternative routes based on traffic conditions.

Seamless integration of the policy system databases into a single end-to-end OSS architecture is a complicated task. In practice, pieces of the policy services system functionality are often found in multiple parts of the overall OSS, and often redundantly. For example, the information required to describe a new service may need to be stored in an order entry system in one format and again in the billing system in a different format. Ideally, both the order entry system and the billing system would both access a single logical database to obtain the information describing the new service. The Policy Services System, when used effectively, should allow complete centralized administration of all common data and service details which would otherwise have to be manually entered or duplicated in multiple other OSS components.

In general, the policy services system has significant impact on network configuration/provisioning and service deployment.

2.8 Telephone Number (TN) Admin Database

The Telephone Number (TN) Admin Database contains the service provider's block of available numbers, information describing which customer is assigned to which number, which blocks of numbers are reserved for particular services such as residential use or PBX use, TN aging schedules, etc.

This data is typically accessed by the customer service and customer care systems. Service Availability Database

The Service Availability Database contains mapping of services that can be presented to a customer based on network topology and CPE. (for example, CMS#1 supports 3-way calling, CMS#2 and CMS#3 support caller-id, Bob Smith's CPE only supports G.711 and we can't offer CD-quality sound). This implies a relationship with the Network Inventory/Topology database.

This information defines the services or features the provider may offer. This data is typically accessed by the customer services and customer care systems.

2.9 Network Inventory / Topology Database

The Network Inventory/Topology Database typically contains HFC network inventory information such as a description of headend equipment, fiber nodes, amplifiers, as well as physical location of these devices. HFC network configuration information such as RF bandwidth allocation may also be included. A description of subscriber CPE equipment may be stored in this database. Although not depicted on this picture, access to this database is required by both "fault/performance management" and "customer service management".

The Network Inventory database can be a static representation of the physical inventory currently deployed in the field as well as additional inventory on-hand for upgrades, etc.

Network inventory can be differentiated into physical and assignable inventory. Physical inventory is created at network provisioning and tends be static. Assignable inventory is derived from the physical inventory and is the dynamic state of that equipment with relationship to the services that have been activated.

The topology database describes how the physical inventory is interconnected. Network management topology is derived from the physical topology and used to reflect the real-time state of the network. The existence of physical inventory may be obtained by auto-discovery mechanisms.

2.10 Name Server Database

The Name Server Database is the IP equivalent of the TN Admin database. It contains the unique Fully Qualified Domain Name (FQDN) name for customer names which will be used to do the dynamic IP address allocation. An example of a FQDN might be a tuple such as (3035551212@mycable.com, Joe User).

2.11 Customer Records Database

The Customer Records Database contains customer profile information such as: customer name; billing address; service address; customer telephone number; fully qualified domain name; make, model, SN of CPE; list of subscribed services and all selected feature parameters (e.g., voicemail with pickup after 3 rings and PIN code); special programs (e.g., bundled programs, reduced rates, etc.).

This database may also contain personal preferences for services, such as preferred email web browser.

2.12 Device Provisioning

Device Provisioning is the actual programming of the CPE equipment. This is explained in detail in the provisioning spec [4]1. It should be understood that device provisioning is different than subscriber provisioning or customer service provisioning. Customer service provisioning is described in detail in section 4.1 of this document.

2.13 Customer Interface

The Customer Interface is the entry point for customer input and may be human or automated. Based on customer input information, an order entry is established. The customer interface may be a web site, IVR system, or a customer service representative. This interface may allow customers to access their billing information or any other information in the customer care domain.

2.14 3rd Party Interconnect (Bonding Gateway)

The 3rd party Interconnect or Bonding Gateway allows internal/external capabilities exchange and activation of services provided by a 3rd party such as E911, operator services, LNP, directory listings, trouble ticketing to external systems, ordering services from external systems (e.g,. PSTN), and access to an SS7 database or calling card database. This component also allows interconnection to an RBOC and inter-exchange accounting and account settlements

2.15 Asset and Work Force Management

The Asset and Work Force Management System coordinates consolidation of multiple orders to effectively and efficiently schedule truck rolls. This function is sometimes performed manually, although automated systems are available. Asset and Work Force Management activities typically make use of the network inventory database.

If automated systems are being used for workforce management, the systems must take into account the type of repair or installation being scheduled so that the appropriate type and level of technician is dispatched. The workforce management system should also recognize when multiple orders for a single location are being

processed to ensure that all of the orders will be processed via a single truck roll rather than multiple truck rolls. An even more sophisticated feature would support least-cost routing of truck rolls. Some systems may support a geographic or roadmap display.

2.16 Customer Care

The functions that are considered customer care and customer service management may vary depending on how the backoffice is organized. The Customer Care System is typically responsible for ensuring the customer's service is maintained at the highest possible level. Anything that interfaces with the customer, such as taking an order, taking info for a trouble ticket, responding to billing questions is handled as part of this process.

2.17 Customer Service Management

The functions that are considered customer care and customer service management may vary depending on how the backoffice is organized. The Customer Service Management system includes the Order Entry System that processes orders based on customer requests such as adds/modifications/deletes of services for a subscriber. This function typically includes product or service promotions, marketing, sales, etc. This system tracks the high-level state of an order throughout the duration of its provisioning lifecycle.

2.18 Trouble Management

Trouble management provides the service level functionality of service assurance. At this level, customer-reported trouble tickets, service level and QoS agreements are managed. This system is also responsible for trouble report generation and the interface to customer care. The degree of integration with the network management layer determines the visibility of the state of the network at the service layer. A good system design will allow the service provider to manage service assurance effectively without having to know all of the details of the underlying network.

2.19 Billing

The billing system is responsible for processing and/or calculating charges and discounts in both a real time and batch mode for all types of transactions. These transactions may include but are not limited to the following: Event Message Records; Call Detail Records; Expanded Message Interface (EMI) Records; Recurring Monthly Transactions; One-Time Charge or Credit Transactions; Pay-Per View Transactions; Packet Transactions.

The billing system is responsible for calculating and applying discounts in multiple modes such as but not limited to: Volume Based Discounting; Cross-Product Discounting; Usage Base Discounting; Promotional Discounting; One-Time Discounting.

The billing system will also be responsible for the calculating and applying all taxes based on rules and regulations of the appropriate taxing jurisdiction.

The billing system will also be responsible for handling all collection activities. These include but are not limited to the following: Payment Processing; Pre-Payment Processing; Debit Card Processing; Credit Card Processing; Electronic Fund Transfer System (EFTS) Processing; Automatic Check Handling (ACH) Processing; Adjustment Processing; Balance Aging; Disconnect Processing; Reconnect Processing. Mediation and settlement are typically included in the billing system. The billing system needs to be billing independent.

2.20 Network Planning and Engineering

The Network Planning and Engineering System is much-encompassing and ranges from concept to offering services. This function spans all the layers of the architecture model from BML down to the physical network elements. The process starts with the concept of what services and products you want to offer. Then you determine what network resources that are required by doing projections of take rates, homes passed, geographic locations, etc. Based on the anticipated services and products, the network deployment is planned, appropriate equipment is ordered and purchased, all appropriate provisioning is accomplished and all management systems are configured to support the network. This function also makes use of performance data and asset allocation data.

2.21 Field Technician

Technician responsible for equipment installation when not possible for customer to perform their own installation.

3 MAPPING INTO THE TMN MODEL

The ITU's TMN model is a framework used to group various OSS operational processes into functional layers. The 5 TMN functional layers are Business Management Layer (BML), Service Management Layer (SML), Network Management Layer (NML), Element Management Layer (EML), and the Element Layer (EL). When layering OSS operational processes using the TMN model, it is instructive to be aware of the evolution of the use of the TMN model by other standards bodies such as the TeleManagement Forum (formerly the Network Management Forum). Although one of the leading champions of the use of the TMN model in helping promote consistent and standards-based OSS implementations, the TeleManagement Forum is starting to focus more attention on a top-down view of operational processes that are required to support an OSS, rather than rigid adherence to TMN layering. This document will take a similar approach to applying TMN layering where it is clear and helpful, but focusing on the PacketCable OSS components and systems that are required regardless of which layer they may belong.

Rigid adherence to standards-defined TMN layers will not be part of this document. The categorizing of systems or processes against TMN layers in this section are purely suggested groupings not mandatory. It is recognized that arbitrary TMN positioning of all or part of various OSS operational functions or systems would be difficult to apply or gain a consensus on by either vendors or the MSOs for the following reasons:

- each MSO has or will have unique operational OSS requirements and implementations
- vendor solutions and products often include functionality which needs to work closely together and is therefore delivered in a single product or system but may span multiple layers of the TMN model.
- vendors and service providers have traditionally had trouble identifying solutions rigidly along the TMN model.
- most traditional TMN classifications would position the OSSs of service providers at the business management layer and certainly no further down than the service management layer.

This document will discuss OSS interaction with all relevant systems regardless of their appropriate TMN level. This approach is intended to help deliver clear and relevant recommendations and quickly identify and detail the required standard interfaces, MIBs, protocols, and interactions between the OSS functional systems and processes.

3.1 Business Management Layer

This layer is made up of a number of business processes such as billing systems and customer care or help desk systems. Generally, in a traditional OSS environment, systems would have with little or no direct interaction with the operational support

systems. It is recognized, however, that vendor solutions have evolved and often perform multiple functions that may span both business and service management layers. For example, Billing Systems, Policy Management Systems, and Order Entry Systems often provide Customer Care support, and are seldom restricted to just these functions and often perform provisioning functions, and customer service representative (CSR) interfaces as well.

Business Management Layer and Service Management Layer processes are shown in a combined BML/SML layer in Section 4 - Operational Processes of this document. Protocols at this layer will be addressed only for interfaces within the scope of the PacketCable project.

3.2 Service Management Layer

This layer is made up of a number of service processes such as policy management, call management, and order entry. As at the Business Management Layer, many policy management systems, and order entry systems offer other functions such as billing support, or customer care support.

Business Management Layer and Service Management Layer processes are shown in a combined BML/SML layer in Section 4 - Operational Processes of this document. Protocols at this layer will be addressed only for interfaces within the scope of the PacketCable project.

3.3 Network Management Layer

This layer is made of up of potentially multiple management systems ranging from hybrid fiber-coax management systems, SONET management systems, cable plant management, RF management, microwave management, and FR or ATM management systems, depending on the cable operator.

As a greater use of the IP protocol takes hold, more management systems or products will become available at this layer. However, other less traditional systems such as Call Agent Management Systems, IP-based IN management systems, and policy management systems have started performing some of the network access management within this layer. Components within this layer will generally be vendor specific and subject to the specific requirements of the individual cable operators.

Generally the OSS framework defined in this document will interface to this layer but not rigidly define the components or requirements at this layer. Protocols at this layer will be addressed only for interfaces within the scope of the PacketCable project.

3.4 Element Management Layer

The DOCSIS OSS is primarily focused on the element management layer and the element layer. To the extent possible, PacketCable OSS at these layers will be complementary with the DOCSIS OSSI approach.

This layer is made up primarily of element management systems such as DOCSIS element management systems, and PacketCable Element management systems used to interface and configure the cable modems, cable modem termination systems, and MTA's. Other systems at this level could include call agent management systems, or cable plant element management systems.

Other systems such as billing systems, policy management systems, or provisioning systems may include some element management components or will interface with these systems.

Generally the PacketCable OSSs defined in this document will interface to this layer but not rigidly define the components or requirements at this layer. Protocols at this layer will be addressed only for interfaces within the scope of the PacketCable project.

3.4.1 SNMPv3

PacketCable requires support of SNMPv3. SNMPv3 offers definite advantages that make it the preferred choice but the actual rollout of the SNMPv3 specific attributes or MIBs may be subject to vendor and industry availability of SNMPv3 support in test equipment and products.

3.4.2 PacketCable MIBs

PacketCable will generate detailed MIB definitions for appropriate interfaces and functional areas. PacketCable specifications for these MIB definitions will be included in separate PacketCable OSS specification documents.

3.5 Network Element Layer

DOCSIS OSS is primarily focused on the element management layer and the element layer. To the extent possible, PacketCable OSS at these layers will be complementary with the DOCSIS OSSI approach.

This layer is made up of components such as call management servers, PSTN gateways, DOCSIS cable modems and CMTS, cable plant, DHCP servers, etc.

Generally, the PacketCable OSS framework defined in this document will interface to this layer but not rigidly define the components or requirements at this layer. Protocols at this layer will be addressed only for interfaces within the scope of the PacketCable project.

4 OPERATIONAL PROCESSES

In order to develop the PKT-OSSI specification it is necessary to consider the operational processes common to cable operators. As a framework, the work published by the TeleManagement Forum (formerly the NMF) will be used as a template for defining the relevant processes. The SMART TMN Telecom Operations Map [3] provides a blueprint for process definition. According to the TM Forum, the SMART TMN Telecom Operations Map delivers to Service Providers a neutral reference point when considering internal processes. It should be understood that business process terminology used by the TM Forum and by cable operators, and between cable operators for that matter, may vary. As much as possible, clarification and reconciliation of the different terminology is included in this document in an attempt to minimize confusion.

Figure 4-1 shows the overall Telecom Operations Map, defined by the TM Forum, that can be used as a framework for understanding the relationship among individual process flows.

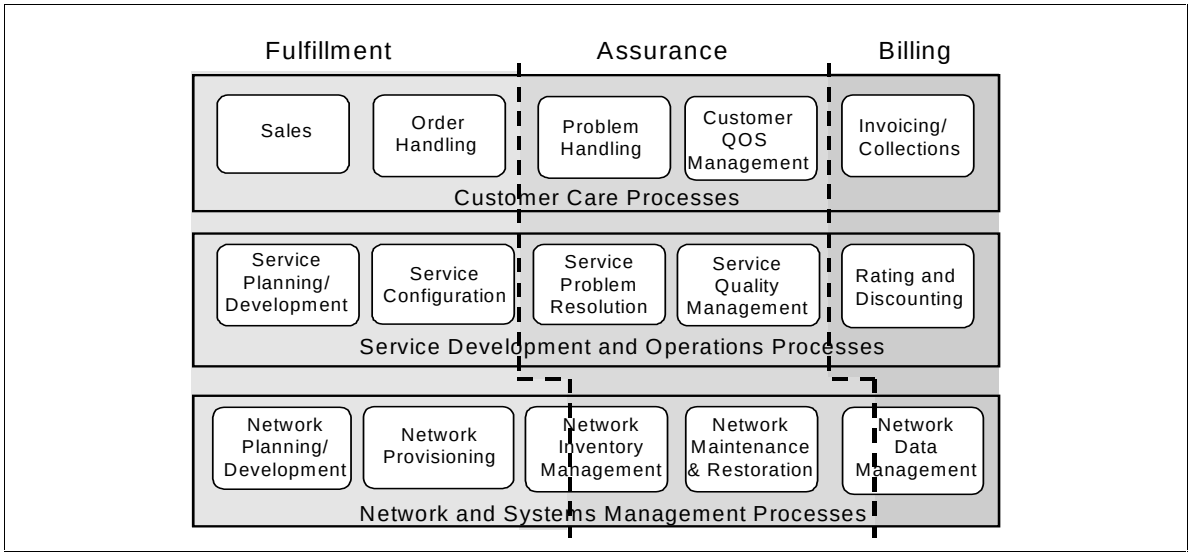

Figure 4-1.TM Forum's High Level Process Breakdown

The Telecom Operations Map uses the layers of the TMN model in defining its map. The Customer Care layer corresponds to the "customer-facing part of the service management" layer of the TMN model, the Service Development and Operations layer corresponds to the "service management" layer of the TMN model, and the Network and Systems Management layer corresponds to the "network-facing part of the service management" layer of the TMN model.

It is not the purpose of this document to reiterate the description of each of the business processes within the Telecom Operations Map, nor the linkages nor the interfaces. For complete details on the Telecom Operations Map the reader is referred to the SMART TMN Telecom Operations Map document published by the TM Forum.

The purpose of this document is to look at each of the processes identified by the TM Forum and explore their applicability to a PacketCable Service Provider. Having established a framework of processes the remainder of this section will explore in more details the issues surrounding each process as it applies to PacketCable.

The remainder of this section has been divided into two major subsections: In Scope Processes and Out of Scope Processes. Not all of the processes defined by the TM Forum are of immediate concern to PacketCable. Those processes which are of immediate concern are addressed in the "In Scope Processes" section. All others are classified in the "Out of Scope Processes" section. Nothing precludes the migration of "Out of Scope" processes to the "In Scope" section, or vice versa, as need warrants or wanes.

4.1 Phase 1 Processes

4.1.1 Device Provisioning

The PacketCable MTA Device Provisioning Specification [4] describes the process flow for PacketCable device provisioning.

4.1.2 Customer Service Provisioning (*a.k.a.* Order Handling) Process

This section will examine the typical process of bringing up a new subscriber service. The OSS primarily gets involved in customer service provisioning which, when working in conjunction with the "plug&play" capabilities outlined in the PacketCable device provisioning document, allows for streamlined and highly automated implementations.

Figure 2 shows the interacting sub-processes typically required to perform customer service provisioning. A short description of each of the sub-processes and information flows is described below. These sub-processes are described in "Section 2 - Architectural overview" of this document.

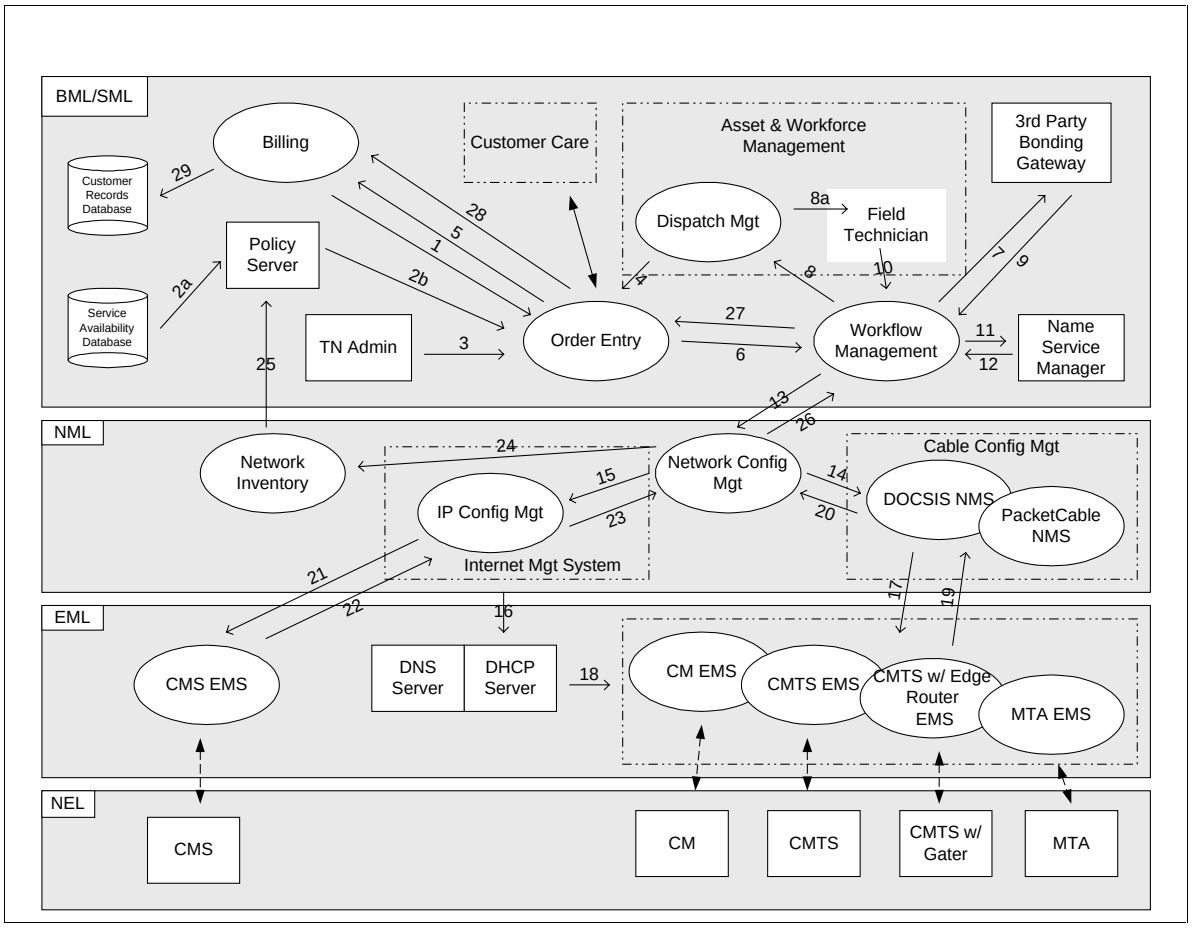

Figure 2: Example Customer Service Provisioning Flows

4.1.2.1 Business/Services Management Layer Sub-Processes

The Business and Services Management layers perform billing, customer care, order entry and order management tasks. A list of the sub-processes are described below or in section 2 of this document.

- **Order Entry Process** – Collection point for customer input. A process that builds a customer work order based on customer information.
- **Work Flow Management** – A process that breaks a customer work order into individual tasks that are then tracked and monitored for completion.
- **Dispatch Management Process** – Process that coordinates truck roll schedules based on many individual orders for the most efficient dispatch.
- **Name Service Manager** – Service responsible for generating unique Fully Qualified Domain Name (FQDN).

4.1.2.2 Network Management Layer

The Network Management layer performs the network inventory and management tasks. The functional blocks and sub-processes within the Network Management Layer below or in section 2 of this document.

- **Network Inventory Process** – Maintains a current and accurate representation of the network components.
- **IP Configuration Management Process** – Contains specific knowledge about the IP domain and is responsible for IP domain configuration control. This process interfaces to DNS and DHCP servers.
- **Network Configuration Management Process** – Maintains a current and accurate representation of the network topology and thus knowledge of network connectivity. Coordinates network activities into device specific activities to deliver or amend network services.
- **Cable Configuration Management Process** – Contains specific knowledge about the cable domain and is responsible for cable domain configuration control. This is composed of two parts, DOCSIS and PacketCable, which could be separate or combined based on individual vendor implementation.

4.1.2.3 Customer Service Provisioning Process Flows

An explanation of the step by step flow for provisioning voice communications service for a customer is described below.

Assumptions:

This flow assumes that CM activation follows the provisioning flow that is specified in the PacketCable MTA Device Provisioning Specification [4]. According to this specification PacketCable specific configuration parameters are downloaded to the CM in a configuration file. It is not the intention of the flow that is being defined here to describe a method for creation, initialization and modification of this configuration file. The creation and maintenance of the configuration file is implementation specific and will be left to the individual vendors to define. The flow is intended to describe the interaction of processes that are required for the activation of service in packet voice networks. It should be noted that these processes may be manual, automatic or a combination of manual and automated processes.

The PacketCable MTA Device Provisioning Specification also provides a mechanism for identification of the cable modem MAC address, device type including manufacturer ID and serial number through an SNMP trap. This flow assumes the existence of such a trap. The trap allows the subscriber provisioning systems to identify the CM automatically and without any need for human intervention.

This flow is based on the assumption that a customer gets in touch with the Customer Service Representative at the provisioning center using a regular phone that is

connected to a CM at the customer premises. While this assumption does not hold in all cases, it does provide a worst case situation. Other possible scenarios are:

- Customer does not have cable service, uses an ordinary phone to call the provisioning center and request service. In this case a truck roll might be necessary for installation of basic cable service and subsequent activation of voice communications service.
- Customer does have cable service, uses existing cable modem and a PC to enter the provisioning web site where he can request service by going through the steps specified in a provisioning web page..

In all cases there might be a time delay between the time that service is requested and the time that service is activated. The delay may be due to LNP processing, physical cable installation, etc. This flow takes this delay into account.

Subscriber Provisioning Flow:

Customer calls Customer Service Representative (CSR) using CPE connected to the PacketCable compliant CM. When this CM is powered on it goes through the default device provisioning process that is specified in the PacketCable MTA Device Provisioning Specification [4]. This default provisioning process configures the CM with some temporary capabilities one of which is to allow a phone off of the CM to go off-hook and connect to the CSR which might be a person or an IVR script.

Flow	Flow Description
1	Using Order Entry Process, CSR obtains blank customer billing record. This record will have among other fields, the following: Customer name; Customer billing address; Customer service address; MTA manufacturer; MTA model number; MTA serial number; Desired TN; Flag indicating if TN exists or does not exist; List of services that can be provisioned. Typically the CSR obtains all customer info at this time with the exception of desired features. Collection of customer information is a two step process: • Basic customer information related to billing. This is information that is needed to generate a bill. This process should be done as early in the flow as possible, in order to prevent running the risk of providing service without having the ability to bill. This information also includes anything that needs to be known in relation to the type of service that a customer can request, for example, location where service is to be deployed, quality of service being requested, type of service being requested, desired TN, any special rates that are in effect, etc. The reason for collecting this info early is to decide if deployment of this type of service is possible as well as to present the customer with a selection of possible services. • Once it is determined what types of service a customer can have, the customer can be given the choice of selecting from available service categories.
2	Order Entry obtains service availability info by consulting the policy manager which in turn consults the Service Availability Database and exercises any policies that are in place for the requested service.

3	Order Entry obtains TN number for service if this is request for new service with no existing number.
4	Order Entry retrieves information from Dispatch Management in the event that a truck roll will be required in order to coordinate truck roll with times which are acceptable to customer.
CSR updates customers billing record with information obtained from customer based on set of desired features from set available.	
5	Order Entry sends updated billing record to Billing Process as inactive.
6	Order Entry builds work order and forwards work order to Work Flow Manager
Work Flow Manager breaks down work into component pieces.	
7	Work Flow Manager forwards requests for LNP phone number to 3rd Party Gateway if required.
8	If truck roll required, send request to dispatch manager which will coordinate truck roll (8a) if required. (optional)
9	Telephone Number (TN) info received from 3rd Party Gateway.
10	Field Technician reports that work is completed. (Occurs only if Steps 8 and 8a are executed.)
11	Naming Service Manager is passed TN and will create the FQDN based on some predefined naming policy.
12	FQDN returned to Workflow Manager.
13	Note that by this time the provisioning center will have to have all relevant information needed for creation of the requested service. These are: CM MAC address; TN; FQDN; Call agent name for the port that being activated. The above mentioned 4 attributes are passed to Network Configuration Management.
Network Configuration Manager will have two series of work to do, one that relates to configuration of cable infrastructure, and one that relates to configuration of the IP and voice communications infrastructure. Cable configurations are handled by the Cable configuration manager, and IP and voice communications configurations are done by the IP Configuration Manager. ***Steps 14 to 20 involve the setting of FQDN and MAC addresses in the DHCP database. This will complete IP initialization of the CM. To initialize the voice communications feature the following need to be done:*** **1) Create PacketCable configuration file for this modem** **2) Set PacketCable MIB attributes that are required for the service**	
14	FQCDN and MAC address passed to Cable Configuration Management where they are eventually entered into the DHCP database.
15	TN and FQDN passed to IP Configuration management.
16	IP Configuration Management registers FQDN with DHCP server. The DHCP to DNS updates are not described here but some vendor specific mechanism must exist to perform this coordination.
17	Cable Configuration Management passes info to Cable EMS. There are actually two types of management systems here. One is for DOCSIS and the other is for PacketCable. DOCSIS will talk to CM, CMTS and CMTS w/ Gate EMS systems. PacketCable will be responsible for talking to CMTS, CMTS w/ Gate and the MTA EMS systems.

18	Cable EMS requests IP address through DHCP handshake and associates it with FQDN via DHCP server/DNS server. It should be noted that both the CM and MTA EMS systems may be requesting dynamic IP addresses.
19	Cable EMS systems acknowledge completion of task to Cable Configuration Management.
20	Cable Configuration Management notifies Network Configuration Management of task completion.
Steps 21-23 involve initialization of the call agent and it's associated databases.	
21	FQDN and TN passed to CMS EMS. This is where the CMS must update any internal tables which it uses to map the TN to the FQDN. The reader is advised to remember that PacketCable uses dynamic addressing. It is therefore assumed that a DNS lookup with the FQDN is required for all call originations or terminations.
22	CMS EMS notifies IP Configuration Management of task completion.
23	IP Configuration Management notifies Network Configuration Management of task completion.
24	Network Configuration Management updates Network Inventory.
25	Network Inventory updates Service Availability Database via the policy server.
26	Network Configuration Management notifies Work Flow Manager of task completion.
27	Work Flow Manager notifies Order Entry of task completion (returns assigned TN and FCDN).
28	Order Entry notifies Billing Process to activate billing record passing assigned TN/FQDN.
29	Billing Process updates TN/FQDN in customer billing record and activates it.

4.1.3 Accounting (aka Invoicing and Collections) Process

This section will examine the typical process of performing accounting. The accounting process typically encompasses sending invoices to customers, processing their payments and performing payment collections. In addition, this process handles customer inquiries about bills, and is responsible to resolve billing problems to the customer's satisfaction. The aim is to provide a correct bill and, if there is a billing problem, resolve it quickly with appropriate status to the customer. An additional aim is to collect monies due the service provider in a professional and customer supportive manner. This process also typically includes customer billing, content provider billing, advertising management billing, and billing distribution.

Figure 4-3 Shows the interacting sub-processes typically required to perform customer service provisioning. A short description of each of the sub-processes and information flows is described below.

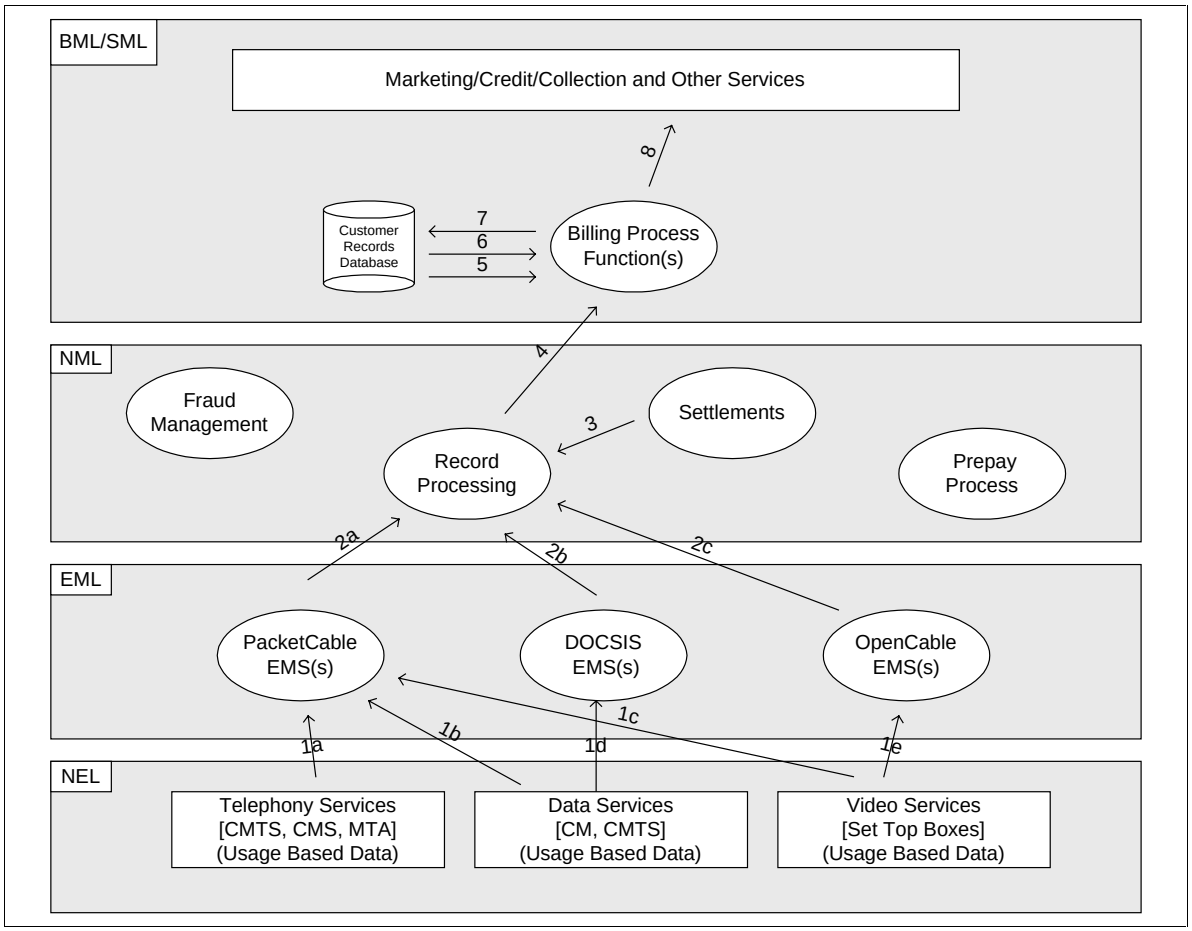

Figure 4-3. Example Billing Flows

4.1.3.1 Network Management Layer

The Network Management layer performs fraud management, accounting settlements among providers, prepay services and record maintenance tasks.

- Fraud Management – Detection and prevention of fraudulent use of services.
- Record Processing – Collects service usage information from network element EMS system. Based on settlements and other information, formats data into correct form for transmittal to billing process.
- Settlements – Process that is used to allocate fractional payment to the individual entities utilized in providing end-to-end services across multiple domains (e.g. different MSOs).
- Prepay Process – The process used to control/administer prepaid services in a network.

4.1.3.2 Billing Process Flows

An example process flow for the invoicing process is outlined below. This figure shows the information flow in the context of PacketCable functional entities. This figure shows the sequence of information transfers that may be followed for proper call usage billing for a subscriber.

Flow	Flow Description
1	The individual EMS systems retrieve usage based information from network elements.
2	Record processing collects usage data from the EMS systems.
3	Record processing retrieves settlement information from Settlements process.
4	Record processing builds billing record based on service usage and settlement info and forwards formatted billing record to billing process.
5	Billing process retrieves customer rate info (and other data as needed) from Customer Records Database and determines charges based on rate, customer info and service usage record.
6	Billing process retrieves any flat rate billing info for this customer and adds charges to bill being processed.
7	Billing process writes updated info to Customer Records Database.
8	Billing process transmits customer charge info to bill rendering service.

4.1.3.3 *Billing CDR*

Many PacketCable components, such as the CMS, CMTS, PSTN Gateway, contain state information or other information that may be required for a billing CDR. Each of these devices may generate event messages containing information about a portion of the call. For example, the CA may generate a call-start event message and a separate call-end event message. For the same call, the CMTS may generate a QoS event message to indicate a change in the quality of service during the call.

For complete details of the PacketCable Event Messages the reader is refer to PacketCable Event Messages specification.

4.2 Phase 2 Processes

4.2.1 Network Planning & Development

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

4.2.2 Network Provisioning

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

4.2.3 Network Inventory Management

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

Engineering and network inventory (Tracks inventory of cable operator's network components to monitor capacity exhaust and support engineering and installation field forces.)

4.2.4 Network Testing, Maintenance & Restoration

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

Fault and performance management (Integrated across domains and integrated with trouble management)

4.3 Out of Scope Processes

All processes outlined in the TeleManagement Forum's Telecom Operations Map, except Order Handling process and Invoicing/Collections process are beyond the scope of PacketCable's attention at this time. The processes are, however, each given their own section below as a placeholder for any and all issues which may warrant attention at a future date.

4.3.1 Customer Care and Contact Management

4.3.1.1 The TeleManagement Forum refers to these functions as "Customer Interface Management"

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

4.3.2 Sales Process

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition. Examples of functions considered part of the sales process are:

- Wholesale/retail gateway capability
- Leads and sales
- Marketing
- Acct/Receivable Credit/Coll/Refunds

4.3.3 Problem Handling Process

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

Trouble management (Directs automated functions and keeps current order status information during the service provisioning and activation.)

4.3.4 Customer QoS Management

This process covers the scenarios for monitoring, managing and reporting service as defined by SLA's. This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

4.3.5 Service Planning and Development Process

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

4.3.6 Service Problem Resolution Process

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

4.3.7 Service Quality Management Process

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

4.3.8 Rating and Discounting Process

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

4.3.9 Content Provider Management

This process is expected to be operator specified. The PacketCable OSS framework assumes no universal definition.

5 CONCLUDING REMARKS

The business processes and operational scenarios outlined in this document are only an illustration of how a cable operator may launch and manage PacketCable services. The expectation is that establishing a certain operations support system framework for such services should facilitate engaging interested equipment vendors in discussions about practical, implementable OSS solutions and OSS interfaces. This framework allows for examining those interfaces in the context of plausible, but not prescriptive, service and business models.

Appendix A. Acknowledgements

This technical reference is the result of the expertise and vision of many different companies and organizations. The PacketCable project wishes to recognize the following individuals for their ongoing involvement and contributions to this document: David Ensign (MediaOne), Keith Kelly (NetSpeak), Azita Kia (Cisco), Kirby Koster (Bridgewater Systems), Roger Loots (Lucent), Malcolm McDonald (NetSpeak).

Maria Stachelek, CableLabs

Appendix B. References and Bibliography

[1]. *Operations Support System Framework for Data Over Cable Services*, TR-DOCS-OSSIW08-961016, Cable Television Laboratories Inc., October 16, 1996.

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

[3]. *SMART TMN™ Telecom Operations Map*, GB910, Evaluation Version Release 1.1, TeleManagement Forum, April, 1999.

[4]. *PacketCable MTA Device Provisioning Specification*, PKT-SP-PROV-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[5]. DHCP: Dynamic Host Configuration Protocol, IETF RFC 2131, March 1997.

[6]. DHCP Options and BOOTP Vendor Extensions, IETF, RFC 2132, March 1997.

[7]. ASSIGNED NUMBERS, IETF (contains ARP/DHCP parameters), RFC 1340, July 1992.

[8]. The TFTP Protocol (Revision 2), STD 33, RFC 1350, MIT, July 1992.

[9]. LDAP: Lightweight Directory Access Protocol (v3), RFC 2251, August 1997.

[10]. Domain Names—Concepts and Facilities, IETF, RFC 1034, STD 13, November 1987.

[11]. Domain Names—Implementation and Specifications, IETF RFC 1035, November 1987.

[12]. Domain Name System Structure and Delegation, IETF, RFC 1591, March 1994.

[13]. *PacketCable Vendor specific DHCP option*, a PacketCable proposal to the IETF DHCP Committee. Primary Author Burcak Baser 3COM.

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

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

[16]. *PacketCable Distributed Call Signaling Specification*, PKT-SP-DCS-D02-991007, October 10,1999, Cable Television Laboratories, Inc.

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

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

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

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

[21]. SNMPv2-TM, RFC1449.

[22]. SNMPv2-TC, RFC1903.

[23]. *PacketCable Audio/Video Codecs Specification*, PKT-SP-CODEC-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[24]. *PacketCable Provisioned QoS Specification*, PKT-SP-PQoS-D02-990603, June 18, 1999, Cable Television Laboratories, Inc.

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

[26]. PacketCable Event Messages White Paper, PKT-TR-OSS-D01-990329.

[27]. *PacketCable Event Messages*, PKT-SP-EM-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./.

[28]. *PacketCable MIB Framework*, PKT-SP-MIBS-I01-991201, Cable Television Laboratories, Inc., December 1, 1999. http://www.PacketCable.com./

[29]. *PacketCable NCS MIB*, PKT-SP-MIBS-NCS-I01-991201, Cable Television Laboratories, Inc., December 1, 1999. http://www.PacketCable.com./

[30]. *PacketCable MTA MIB*, PKT-SP-MIBS-MTA-I01-991201, Cable Television Laboratories, Inc., December 1, 1999. http://www.PacketCable.com./

[31]. ITU's m.3400

[32]. ITU's m.3010

[33]. ITU's m.3200

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
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information.
Authorization	The act of giving access to a service or device if one has the permission to have the access.
BAF	Bellcore AMA Format, another way of saying AMA
BPI+	Baseline Privacy Interface Plus is the security portion of the DOCSIS 1.1 standard which runs on the MAC layer.
CBC	Cipher block chaining mode is an option in block ciphers that combine (XOR) the previous block of ciphertext with the current block of plaintext before encrypting that block of the message.
CBR	Constant Bit Rate.
CA	Certification Authority - a trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CA	Call Agent. In this specification "Call Agent" is part of the CMS that maintains the communication state, and controls the line side of the

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

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

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

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

MGCP	Media Gateway Control Protocol. Protocol follow on to SGCP.
MIB	Management Information Base
MIC	Message integrity code, a fixed length data item that is sent together with a message to ensure integrity, also known as a MAC.
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSO	Multi-System Operator, a cable company that operates many head-end locations in several cities.
MSU	Message Signal Unit
MTA	Media Terminal Adapter – contains the interface to a physical voice device, a network interface, CODECs, and all signaling and encapsulation functions required for VoIP transport, class features signaling, and QoS signaling.
MTP	The Message Transfer Part is a set of two protocols (MTP 2, 3) within the SS7 suite of protocols that are used to implement physical, data link and network level transport facilities within an SS7 network.
MWD	Maximum Waiting Delay
NANP	North American Numbering Plan
NANPNAT	North American Numbering Plan Network Address Translation
NAT Network Layer	Network Address Translation Layer 3 in the Open System Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.
Network Layer	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
Network Management	The functions related to the management of data across the network.
Network Management OSS	The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.
NCS	Network Call Signaling
Nonce	A random value used only once which is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP)
NTP	Network Time Protocol, an internet standard used for synchronizing clocks of elements distributed on an IP network
NTSC	National Television Standards Committee which defines the analog color television, broadcast standard used today in North America.
Off-Net Call	A communication connecting a PacketCable subscriber out to a user on the PSTN
On-Net Call	A communication placed by one customer to another customer entirely on the

	PacketCable Network
One-way Hash	A hash function that has an insignificant number of collisions upon output.
OSP	Operator Service Provider
OSS-D	OSS Default – Network Provider Provisioning Server
OSS	Operations Systems Support. The back office software used for configuration, performance, fault, accounting and security management.
PAL	Phase Alternate Line – the European color television format which evolved from the American NTSC standard.
PDU	Protocol Data Unit
PKCS	Public Key Cryptography Standards, published by RSA Data Security Inc. Describes how to use public key cryptography in a reliable, secure and interoperable way.
PKI	Public Key Infrastructure - a process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
PKINIT	The extension to the Kerberos protocol that provides a method for using public key cryptography during initial authentication.
PHS	Payload Header Suppression, a DOCSIS technique for compressing the Ethernet, IP and UDP headers of RTP packets.
Plaintext	The original (unencrypted) state of a message or data.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to any one other then the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves.
PSC	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
PSFR	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
PSTN	Public Switched Telephone Network.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A users private key is kept secret and is the only key which can decrypt messages sent encrypted by the users public key.
PCM	Pulse Code Modulation – A commonly employed algorithm to digitize an

	analog signal (such as a human voice) into a digital bit stream using simple analog to digital conversion techniques.
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service, guarantees network bandwidth and availability for applications.
RADIUS	Remote Access Dial-In User Service, an internet protocol (RFC 2138 and RFC 2139) originally designed for allowing users dial-in access to the internet through remote servers. Its flexible design has allowed it to be extended well beyond its original intended use
RAS	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
RC4	A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in PacketCable.
RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
RKS	Record Keeping Server, the device which collects and correlates the various Event Messages
Root Private Key	The private signing key of the highest level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures that it generated with the corresponding root private key.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
RSVP	Resource reSerVation Protocol
RTCP	Real Time Control Protocol
RTO	Retransmission Timeout
RTP	Real Time Protocol, a protocol defined in RFC 1889 for encapsulating encoded voice and video streams.
S-MTA	Standalone MTA – a single node which contains an MTA and a non DOCSIS MAC (e.g. ethernet).
SA	Security Association - a one-way relationship between sender and receiver offering security services on the communication flow .
SAID	Security Association Identifier - uniquely identifies SAs in the BPI+ security protocol, part of the DOCSIS 1.1 specification.
SCCP	The Signaling Connection Control Part is a protocol within the SS7 suite of protocols that provides two functions in addition to those that are provided within MTP. The first is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	A Service Control Point is a Signaling Point within the SS7 network,

	identifiable by a Destination Point Code, that provides database services to the network.
SCTP	Simple Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information that is delivered as a unit between peer service access points.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.
Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
SF	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
SFID	Service Flow ID, a 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. Any 32-bit SFID must not conflict with a zero-extended 14-bit SID. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). USFIDs and DSFIDs are allocated from the same SFID number space.
SFR	Service Flow Reference, a 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
SG	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1 - a one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
Signed and Sealed	An “envelope” of information which has been signed with a digital signature and sealed by using encryption.
SIP	Session Initiation Protocol is an application layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants.
SIP+	Session Initiation Protocol Plus is an extension to SIP.
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SPI	Security Parameters Index - a field in the IPSEC header that along with the destination IP address provides a unique number for each SA.
SS7	Signaling System Number 7. SS7 is an architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Signal Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
STP	Signal Transfer Point. An STP is a node within an SS7 network that routes signaling messages based on their destination address. It is essentially a packet

	switch for SS7. It may also perform additional routing services such as Global Title Translation.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and source and destination UDP/TCP port.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.
Systems Management	Functions in the application layer related to the management of various open systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.
TCAP	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling Control Point.
TCP	Transmission Control Protocol
TD	Timeout for Disconnect
TFTP	Trivial File Transfer Protocol
TFTP-D	Default – Trivial File Transfer Protocol
TGS	Ticket Granting Server used to grant Kerberos tickets.
TGW	Telephony Gateway
TIPHON	Telecommunications & Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value tuple within a DOCSIS configuration file.
TN	Telephone Number
ToD	Time of Day Server
TOS	Type of Service. An 8-bit field of every IP version 4 packet. In a Diffserv domain, the TOS byte is treated as the Diffserv Code Point, or DSCP.
Transit Delays	The time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.
Trunk	An analog or digital connection from a circuit switch which carries user media content and may carry voice signaling (MF, R2, etc.).
TSG	Trunk Subgroup
Tunnel Mode	An IPSEC (ESP or AH) mode that is applied to an IP tunnel, where an outer IP packet header (of an intermediate destination) is added on top of the original, inner IP header. In this case, the ESP or AH transform treats the inner IP header as if it were part of the packet payload. When the packet reaches the intermediate destination, the tunnel terminates and both the outer IP packet header and the IPSEC ESP or AH transform are taken out.
UDP	User Datagram Protocol, a connectionless protocol built upon Internet Protocol (IP).
Upstream	The direction from the subscriber location toward the head-end.
VAD	Voice Activity Detection
VBR	Variable bit-rate
VoIP	Voice over IP
WBEM	Web-Based Enterprise Management (WBEM) is the umbrella under which the DMTF (Desktop Management Task Force) will fit its current and future

	specifications. The goal of the WBEM initiative is to further management standards using Internet technology in a manner that provides for interoperable management of the Enterprise. There is one DMTF standard today within WBEM and that is CIM (Common Information Model). WBEM compliance means adhering to the CIM. See www.dmtf.org
X.509 certificate	a public key certificate specification developed as part of the ITU-T X.500 standards directory

Appendix D. Revisions

Engineering Change Numbers

ECN	Date Ratified	Summary