Data-Over-Cable Service Interface Specifications

DOCSIS 3.0 OSSI Configuration Management Technical Report

CM-TR-OSSIv3.0-CM-V01-080926

RELEASED

Notice

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

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

© Copyright 2008 Cable Television Laboratories, Inc.

All rights reserved.

Document Status Sheet

Document Control Number:	CM-TR-OSSIv3.0-CM-V01-080926			
Document Title:	DOCSIS 3.0 OSSI Configuration Management Technical Report			
Revision History:	V01 - Released 9/26/2008			
Date:	September 26, 2008			
Status:	~~Work in Progress~~	~~Draft~~	Released	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	Public

Trademarks

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

Contents

Figures

Tables

This page left blank intentionally.

1 SCOPE

1.1 Introduction and Purpose

This Technical Report provides guidelines, through typical use cases, on how to apply OSSIv3.0 requirements for provisioning. This Technical Report is limited to addressing Configuration Management (flow of information from provisioning server to network devices). Configuration Management is part of the FCAPS model. Refer to the Overview section of [OSSI3.0] for details on the FCAPS model as applied to DOCSIS.

The methodology used in this Technical Report is to define how to use the object models specified in the OSSIv3.0 specification. This is accomplished through defining Use Cases for provisioning DOCSIS 3.0 features and scenarios, within a Use Case, to step through how the different options/capabilities are configured for deployment.

1.2 Limitations

The Scenarios documented in this Technical Report do not define steps to verify that configuration changes performed were properly made (beyond checking a return code for a configuration change request). This can be performed by various methods including querying MIB status objects via SNMP for verifying proper configuration. Some status objects require a CM to be registered to populate them.

The exceptions documented in each Scenario do not address run-time behavioral exceptions. The exceptions are meant to focus on error cases during configuration and provisioning.

2 REFERENCES

2.1 Normative References

This technical report does not contain any normative references.

2.2 Informative References

This specification uses the following informative references.

[CANN DHCP-Reg] CableLabs DHCP Options Registry, CL-SP-CANN-DHCP-Reg-I02-080306, March 6, 2008, Cable Television Laboratories, Inc.

[FIPS-197] Federal Information Processing Standards Publication (FIPS PUB) 197, Advanced Encryption Standard, November, 2001.

[ICMTR] DOCSIS 2.0 + IPv6 Cable Modem Technical Report, CM-TR-DOCSIS2.0-IPv6-V01-080307, March 07, 2008, Cable Television Laboratories, Inc.

[IPDR/SP] IPDR/SP Protocol Specification, Version 2.1, IPDR.org, November 2004.

[ISO 19501] ISO/IEC 19501:2005 Information technology - Open Distributed Processing - Unified Modeling Language (UML) Version 1.4.2.

[MULPI3.0] DOCSIS MAC and Upper Layer Protocols Interface Specification v3.0, CM-SP-MULPIv3.0-I08-080522, May 22, 2008, Cable Television Laboratories, Inc.

[OSSI3.0] Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification, CM-SP-OSSIv3.0-I07-080522, May 22, 2008, Cable Television Laboratories, Inc.

[RFC 3315] IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003.

[RFC 3925] IETF RFC 3925, Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4), October 2004.

[RFC 4361] IETF RFC 4361, Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4), February 2006.

[RFC 4639] IETF RFC 4639, R. Woundy and K. Marez, Cable Device Management Information Base for Data-Over-Cable Service Interface Specification (DOCSIS) Compliant Cable Modems and Cable Modem Termination Systems, December 2006.

[RFIv2.0] DOCSIS 2.0, Radio Frequency Interface Specification, CM-SP-RFIv2.0-I13-080215, February 15, 2008, Cable Television Laboratories, Inc.

[SEC3.0] DOCSIS 3.0 Security Specification, CM-SP-SECv3.0-I08-080522, May 22, 2008, Cable Television Laboratories, Inc.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- International Organization for Standardization (ISO), Internet: http://www.iso.org/iso/home.htm
- Internet Engineering Task Force (IETF) Secretariat, 46000 Center Oak Plaza, Sterling, VA 20166, Phone +1-571-434-3500, Fax +1-571-434-3535, http://www.ietf.org

- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org/
- National Institute of Standards and Technology; http://csrc.nist.gov/publications/PubsFIPS.html

3 TERMS AND DEFINITIONS

This technical report uses the following terms:

Bonded Channel Set An identified set of upstream or downstream channels among which a stream of packets is distributed.

Bonding Group A list of channels providing a means to identify the specific channels bonded together.

Cable Modem (CM) A modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system.

Cable Modem Termination System (CMTS) Cable modem termination system, located at the cable television system head-end or distribution hub, which provides complementary functionality to the cable modems to enable data connectivity to a wide-area network.

Configuration Management One of the five categories of the FCAPS model, defined by the ITU, which addresses effecting change in network devices to provision services and features.

Downstream (DS) In cable television, the direction of transmission from the head-end to the subscriber.

FCAPS A set of principles for managing networks and systems, wherein each letter represents one principle. F is for Fault, C is for Configuration, A is for Accounting, P is for Performance, S is for Security.

Hybrid Cable Modem A Pre-3.0 DOCSIS CM which may or may not support IPv6, channel bonding in one or both directions of flow, enhanced security features, or is a DOCSIS 2.0 + IPv6 CM

Media Access Control (MAC) address The "built-in" hardware address of a device connected to a shared medium.

MAC Domain A subcomponent of the CMTS that provides data forwarding services to a set of downstream and upstream channels.

MAC Domain Cable Modem Service Group The subset of a Cable Modem Service Group which is confined to the Downstream Channels and Upstream Channels of a single MAC domain. Differs from a CM-SG only if multiple MAC domains are assigned to the same CM-SGs.

Network Management 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.

Network Management System (NMS) The hardware and software components used by the Network Provider to manage its networks as a whole. The Network Management System provides an end-to-end network view of the entire network enabling management of the network elements contained in the network.

Pre-3.0 DOCSIS Versions of CableLabs Data-Over-Cable-Service-Interface-Specifications (DOCSIS) prior to the DOCSIS 3.0 suite of specifications.

Receive Channel Set The set of downstream channels assigned to an individual CM is called its Receive Channel Set, and is explicitly configured by the CMTS using the RCC encodings

Scenario In the UML, a Scenario is one particular way of reaching the goal defined by a Use Case. Several Scenarios may be generated from a single Use Case.

Simple Network Management Protocol (SNMP) A network management protocol of the IETF.

Unified Modeling Language (UML) The Unified Modeling Language (UML) is a unified model for object oriented analysis and design (OOA&D). UML is an OMG standard and is an accepted ISO specification [ISO 19501].

Upstream (US) The direction from the subscriber location toward the head-end.

Upstream Drop Classifier A set of matching criteria that the CM applies to each packet in order to determine whether to filter (drop) upstream traffic.

Use Case In the UML, a Use Case represents one particular type of a system's behavior based on stimuli from an external source (i.e., an actor). A system may have several Use Cases which define all its behavior.

4 ABBREVIATIONS AND ACRONYMS

This technical report uses the following abbreviations:

APM	Alternate Provisioning Mode
BPI+	Baseline Privacy Interface Plus
CA	Certificate Authority
CableLabs	Cable Television Laboratories, Inc.
CIFS	Common Internet File System
CLI	Command Line Interface
CM	Cable Modem
CMTS	Cable Modem Termination System
CRL	Certificate Revocation List
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data-Over-Cable Service Interface Specifications
DPM	Dual-stack Provisioning Mode
DS	Downstream
DSCP	Diff Serve Code Points
EAE	Early Authentication and Encryption
FCAPS	Fault, Configuration, Accounting, Performance, Security
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPDR	Internet Protocol Detail Record
MAC	Media Access Control
MSO	Multiple Systems Operator
MTA	Multimedia Terminal Adapter
NMS	Network Management System
OM	Object Model
OSS	Operations Support System
OSSI	Operations Support System Interface
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TLV	Type/Length/Value
TFTP	Trivial File Transfer Protocol
ToD	Time Of Day
UDC	Upstream Drop Classifier

UML	Unified Modeling Language
URL	Uniform Resource Locator

5 USE CASES

This section identifies the Use Cases, which this Technical Report will define through corresponding Scenario diagrams.

5.1 Use Case Diagram

The following Use Case diagram represents the identified Use Cases that this Technical Report focuses on. All identified Use Cases focus on provisioning and configuration management.

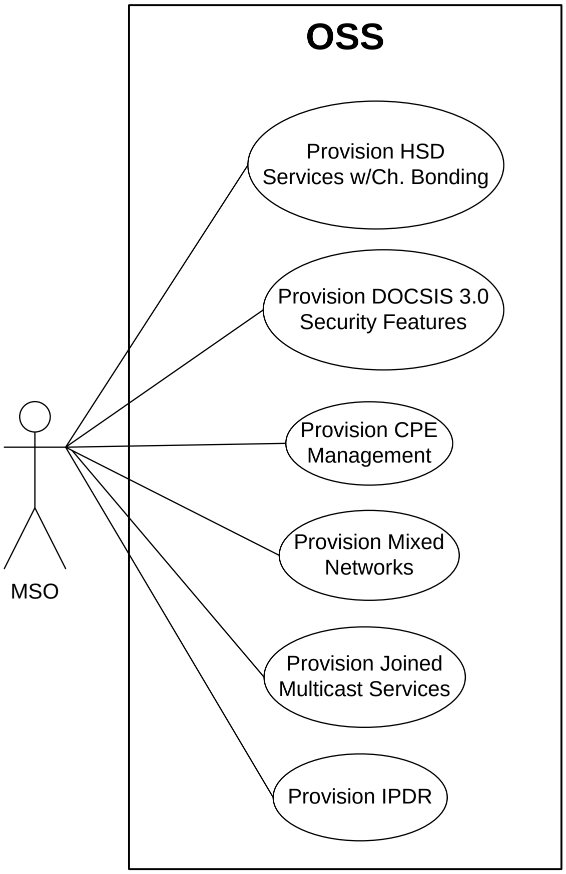

OSS
Provision HSD Services w/Ch. Bonding
Provision DOCSIS 3.0 Security Features
Provision CPE Management
Provision Mixed Networks
Provision Joined Multicast Services
Provision IPDR
MSO

Figure 1 – DOCSIS 3.0 OSS Configuration Use Case Diagram

The Multiple Systems Operator (MSO) is the actor who interacts with the system to perform certain goals (listed as Use Cases in the ovals). There may be several different MSO actors who have different roles, such as an Operator with full permissions and one with read-only permissions. This diagram only represents an Operator with full permissions.

The Operations Support System (OSS) and corresponding box represents the system and its boundaries. In this specific diagram, the OSS system may include various back office provisioning servers, software download servers, security servers, fault management servers, etc.

5.1.1 Provision HSD Services w/Channel Bonding

This Use Case encompasses Scenarios that provision Cable network elements to provide High Speed Data (HSD) services, such as higher speed Tier service plans.

Refer to Section 6 for the detailed Scenarios.

5.1.2 Provision CPE Management

This Use Case encompasses Scenarios that provision CPE management, such as packet filtering.

Refer to Section 7 for the detailed Scenarios.

5.1.3 Provision Mixed Networks

This Use Case encompasses Scenarios that provision Cable network elements in mixed network environments (e.g., a mix of CM/eMTA devices with different DOCSIS protocol versions). For example, provisioning both IPv4 and IPv6 CM/eMTAs based on their IP protocol support.

Refer to Section 8 for the detailed Scenarios.

5.1.4 Provision Joined Multicast Services

This Use Case encompasses Scenarios that focus on provisioning the CMTS for Multicast Services. The CMTS is configured to provide different Quality of Service (QoS) to different Multicast Sessions. It can also be configured to provide an Authorization feature to control access to different Multicast sessions by CMs.

Refer to Section 9 for the detailed Scenarios.

5.1.5 Provision DOCSIS 3.0 Security Features

This Use Case encompasses Scenarios that provision DOCSIS 3.0 Security Features, such as Early Authentication and Encryption.

Refer to Section 10 for the detailed Scenarios.

5.1.6 Provision IPDR

This Use Case encompasses Scenarios that focus on provisioning the Internet Protocol Detail Record (IPDR) Exporter and Collector(s). The CMTS implements the IPDR Exporter function while one or more Collectors reside in the back office for collecting IPDR records. Certain IPDR Streaming attributes require configuration in the CMTS.

Refer to Section 11 for the detailed Scenarios.

6 PROVISIONING HIGH SPEED DATA SERVICES SCENARIOS

This section defines Scenarios for provisioning High Speed Data services using channel bonding.

6.1 Configuration of Downstream Channel Bonding in a 3x1 Topology

6.1.1 Business Scenario

An MSO would like to configure a DOCSIS 3.0 CMTS for 3x1 Downstream Channel Bonding in order to provide increased bandwidth in the downstream path. With channel bonding, bandwidth is increased by combining or bonding multiple RF channels to create a Bonded Channel Set.

A Bonded Channel Set is a unique combination of downstream or upstream RF channels. The CMTS assigns a Receive Channel Set to a DOCSIS 3.0 or downstream bonding-capable Hybrid Cable Modem. The CMTS can assign many such CMs to the same Bonding Group.

This Scenario is defined independently of the type of DOCSIS 3.0 CMTS used (e.g., I-CMTS or M-CMTS) but could be applied to each deployment type.

6.1.2 Scenario Details

This scenario will detail the steps needed to create a MAC Domain that has a single Downstream Bonding Group consisting of three downstream channels and using 1 upstream channel for a specific Fiber Node. The process for creating these elements is:

- Create or configure the downstream interfaces
- Create or configure the upstream interface
- Create the MAC Domain interface
- Configure the MAC Domain using the MdCfg object [OSSI3.0]
- Create the MAC Domain Channel Configuration using the MdChCfg object [OSSI3.0]
- Create the Fiber Node topology information using the FiberNodeCfg object [OSSI3.0]
- Map the upstream and downstream interfaces to the Fiber Node using the ChFnCfg object[OSSI3.0]
- Create the Bonding Group using the BondingGrpCfg object [OSSI3.0]

For simplicity, the creation of the downstream interfaces between M-CMTS implementations and an integrated CMTS are not detailed in this Scenario. Many CMTS implementations provide CLI based commands for quickly creating interfaces rather than using SNMP. These commands will not be shown here as MSOs are very familiar with these commands and setup.

In DOCSIS 3.0, a downstream can be configured as either a Primary Capable Downstream or a secondary downstream. The difference between the two configurations is that a Primary Capable Downstream carries MAP and Sync messages and thus can support pre-3.0 DOCSIS and DOCSIS 3.0 CMs. Secondary channels do not carry MAP or Sync messages and thus are useful for DOCSIS 3.0 data. Some CMTS implementations may support the concept of channel sharing. This scenario does not address this type of configuration.

The general process above can be followed for any number of MAC Domains, upstream and downstream interfaces, Fiber Nodes and or Bonding Groups. Some CMTS implementations configure static Bonding Broups while other CMTS implementations support the dynamic or CMTS controlled Bonding Groups.

Figure 2 depicts the general topology of this Scenario.

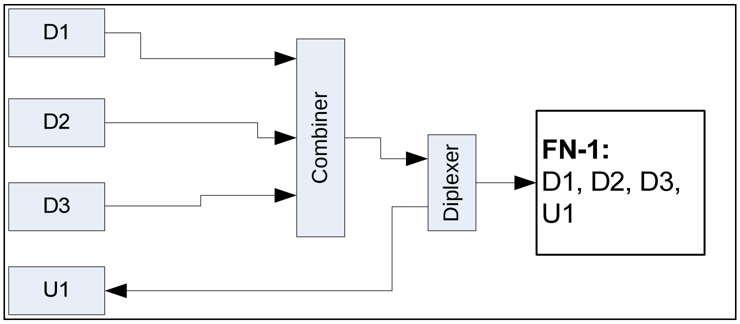


Figure 2 – General 3x1 Plant Topology

6.1.3 Assumptions:

The following assumptions are made in this Scenario

- CMTS IP configuration for the NSI and Cable interfaces are complete and operational
- The MAC Domain interface has been created using vendor specific methods
- MSO can create and configure upstream and downstream interfaces via CLI or SNMP and the method chosen is up to MSO standard operating procedures
- A DOCSIS 3.0 CMTS and DOCSIS 3.0 CM are available and all plant wiring is in place

6.1.4 5Pre-conditions

There are no additional pre-conditions that have not already been detailed previously in the Assumption and Scenario Details sections.

6.1.5 Management Objects

- CMTS MAC Domain Configuration object

Refer to the MdCfg object defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the MdCfg Object section from [OSSI3.0].

To configure a previously created MAC Domain instance (referred to as MAC Domain 1 in this Scenario) using vendor specific methods, the MdCfg object is used. Configuring the MdCfg instance will require using the CMTS determined ifIndex of the MAC Domain interface. Using the MAC Domain ifIndex, the following MdCfg attributes are configured:

- MDD interval
- Provisioning mode
- CmStatusEventControl
- Enabling use of the extended 5-85 MHz spectrum
- Enabling Multicast DSID forwarding
- Support for Multiple Receive and Multiple Transmit mode
- Enabling Early Authentication and Encryption
- Enabling TFTP proxy
- Enabling Source Address Verification
- Annex of the downstream channels

- Enabling the CM Upstream Drop Classifiers
- SendUdcRulesEnabled for aiding the CM in establishing the UDC rule set
- ServiceTypeIdList for assisting CMs to be directed to the correct downstream for configuration

Each of these attributes needs to have a specific configured value or assume the default values defined in [OSSI3.0].

- CMTS MAC Domain Channel Configuration object

Refer to the MdChCfg object defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the MdChCfg Object section from [OSSI3.0].

This object is used to map the individual upstream and downstream interfaces into a specific MAC Domain. To map these channels to MAC Domain 1 a MdChCfg instance is created for each channel (three downstreams and one upstream). The attributes of the object include the MAC Domain ifIndex, the upstream or downstream ifIndex, a designation for whether a specific downstream interface is a Primary Capable Downstream or not, an attribute for assigning the 8-bit Channel ID for this interface in the MAC Domain, and the Provisioned Attribute Mask for this interface. The IsPriCapableDs attribute is only valid when the interface being referenced is a downstream interface; it is not used when the interface is an upstream interface.

Each of these attributes needs to have a specific configured value or assume the default values defined in [OSSI3.0].

- CMTS Fiber Node Configuration object

This object is used to create a Fiber Node in the Topology data that the CMTS maintains. Refer to the FiberNodeCfg object defined in the Fiber Node Topology Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the FiberNodeCfg Object section from [OSSI3.0]. To create an instance, the Operator assigns a fiber node name and a description. The NodeName is used as reference for the ChFnCfg object. The NodeName attribute is set to "FN-1" and the NodeDescr attribute is set to "This is FN-1".

- CMTS Channel Fiber Node Configuration object

This object allows for the mapping of the upstream and downstream interfaces to specific Fiber Nodes much like the MdChCfg does for mapping these interfaces to the MAC Domain. Refer to the ChFnCfg object defined in the Fiber Node Topology Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the ChFnCfg object section from [OSSI3.0]. Creating a ChFnCfg instance requires the Operator to use a NodeName that exists in the FiberNodeCfg object and a ChIfIndex for either an upstream or downstream interface. Each of these attributes is a key for the object instance. The NodeName attribute is set to "FN-1" and the ChIfIndex attributes are set to the three ifIndexes of the downstream interface (ifType=docsCableMCmtsDownstream(229)) along with the ifIndex of the single upstream (ifType=docsCableUpstream(129)). The result of this configuration is to map the Fiber Node to the corresponding three modular downstream interfaces and one upstream interface which required creating four instances of the ChFnCfg object.

- CMTS Bonding Group Configuration object

This object allows the Operator to configure static bonding groups within a MAC Domain. Refer to the BondingGrpCfg object defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the BondingGrpCfg object section from [OSSI3.0]. A BondingGrpCfg instance is created. The instance includes values for the MdifIndex of the MAC Domain, the direction for the bonding group (downstream or upstream), a unique ID for the group, the Channel List of upstream or downstream channels that will be used in this bonding group, the SfProvAttrMask, the DsidReseqWaitTime, and the DsidReseqWarnThrshld. Each of these attributes needs to have a specific configured value or assume the default values defined in [OSSI3.0]. The attributes SfProvAttrMask, DsidReseqWaitTime, and DsidReseqWarnThrshld have default values.

6.1.6 Sequence Diagram

The following two diagrams represent the Sequence diagram. Due to the number of object instantiations, the Sequence diagram was split into two diagrams.

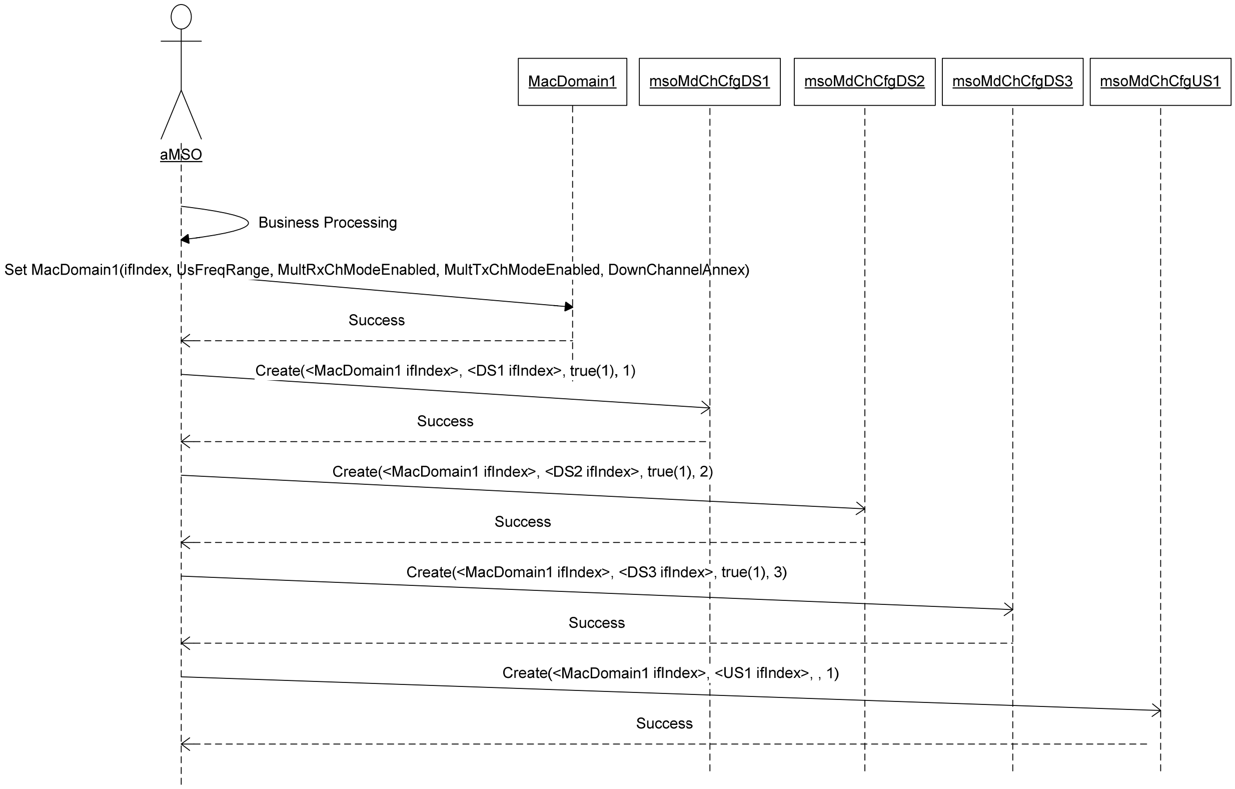

aMSO
MacDomain1
msoMdChCfgDS1
msoMdChCfgDS2
msoMdChCfgDS3
msoMdChCfgUS1
Business Processing
Set MacDomain1(ifIndex, UsFreqRange, MultRxChModeEnabled, MultTxChModeEnabled, DownChannelAnnex)
Success
Create(<MacDomain1 ifIndex>, <DS1 ifIndex>, true(1), 1)
Success
Create(<MacDomain1 ifIndex>, <DS2 ifIndex>, true(1), 2)
Success
Create(<MacDomain1 ifIndex>, <DS3 ifIndex>, true(1), 3)
Success
Create(<MacDomain1 ifIndex>, <US1 ifIndex>, , 1)
Success

Figure 3 – Sequence Diagram for Configuration of Downstream Channel Bonding in a 3x1 Topology (Part 1)

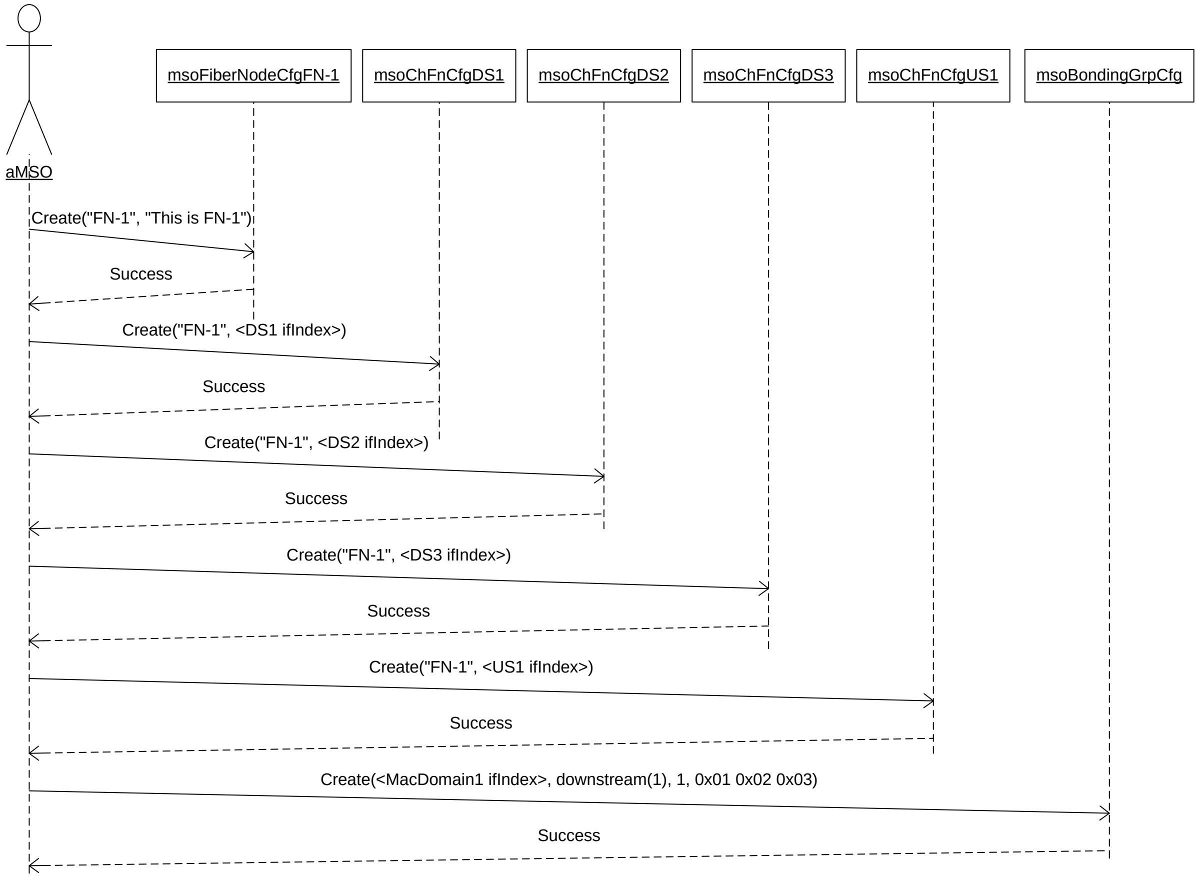
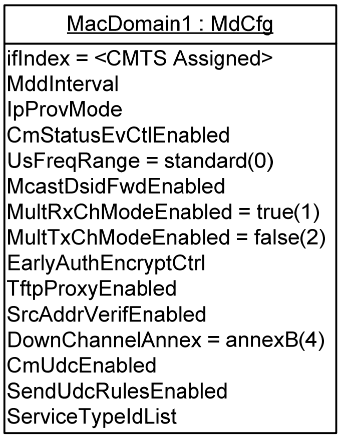

aMSO
msoFiberNodeCfgFN-1
msoChFnCfgDS1
msoChFnCfgDS2
msoChFnCfgDS3
msoChFnCfgUS1
msoBondingGrpCfg
Create("FN-1", "This is FN-1")
Success
Create("FN-1", <DS1 ifIndex>)
Success
Create("FN-1", <DS2 ifIndex>)
Success
Create("FN-1", <DS3 ifIndex>)
Success
Create("FN-1", <US1 ifIndex>)
Success
Create(<MacDomain1 ifIndex>, downstream(1), 1, 0x01 0x02 0x03)
Success

Figure 4 – Sequence Diagram for Configuration of Downstream Channel Bonding in a 3x1 Topology (Part 2)

6.1.7 Post-conditions

A DOCSIS 3.0 CMTS will be configured for a 3x1 topology with DOCSIS 3.0 CMs and downstream bonding-capable Hybrid CMs connected to a single Fiber Node consisting of three downstreams and one upstream.

The following diagram highlights the desired state for the MdCfg object (MAC Domain 1 instance) at the end of this scenario.

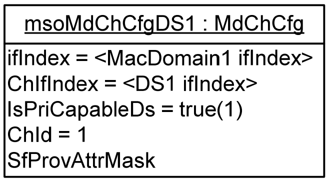

MacDomain1 : MdCfg

ifIndex = <CMTS Assigned>
MddInterval
IpProvMode
CmStatusEvCtlEnabled
UsFreqRange = standard(0)
McastDsidFwdEnabled
MultRxChModeEnabled = true(1)
MultTxChModeEnabled = false(2)
EarlyAuthEncryptCtrl
TftpProxyEnabled
SrcAddrVerifEnabled
DownChannelAnnex = annexB(4)
CmUdcEnabled
SendUdcRulesEnabled
ServiceTypeIdList

Any attribute (in the above object instances) that is left unassigned is assumed to take the default value as specified in the object model of [OSSI3.0].

The following diagram highlights the desired state for the MdChCfg object at the end of this scenario.

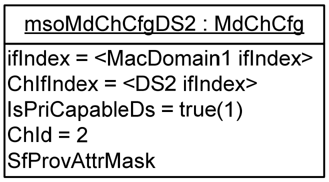
First instance which assigns downstream channel 1 (DS1) to MAC Domain 1:



msoMdChCfgDS1 : MdChCfg

ifIndex = <MacDomain1 ifIndex>
ChIfIndex = <DS1 ifIndex>
IsPriCapableDs = true(1)
ChId = 1
SfProvAttrMask

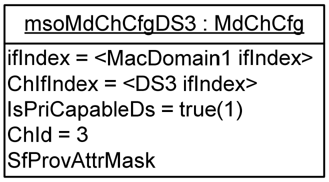
Second instance which assigns downstream channel 2 (DS2) to MAC Domain 1:



msoMdChCfgDS2 : MdChCfg

ifIndex = <MacDomain1 ifIndex>
ChIfIndex = <DS2 ifIndex>
IsPriCapableDs = true(1)
ChId = 2
SfProvAttrMask

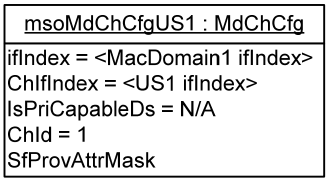
Third instance which assigns downstream channel 3 (DS3) to MAC Domain 1:



msoMdChCfgDS3 : MdChCfg

ifIndex = <MacDomain1 ifIndex>
ChIfIndex = <DS3 ifIndex>
IsPriCapableDs = true(1)
ChId = 3
SfProvAttrMask

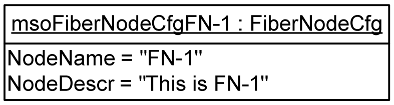
Fourth instance which assigns upstream channel 1 (US1) to MAC Domain 1:



msoMdChCfgUS1 : MdChCfg

ifIndex = <MacDomain1 ifIndex>
ChIfIndex = <US1 ifIndex>
IsPriCapableDs = N/A
ChId = 1
SfProvAttrMask

The following diagram highlights the desired state for the FiberNodeCfg object at the end of this scenario.

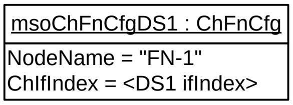


msoFiberNodeCfgFN-1 : FiberNodeCfg

NodeName = "FN-1"
NodeDescr = "This is FN-1"

The following diagram highlights the desired state for the ChFnCfg object at the end of this scenario.

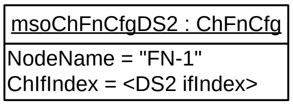
First instance which assigns downstream channel 1 (DS1) to Fiber Node FN-1:



msoChFnCfgDS1 : ChFnCfg

NodeName = "FN-1"
ChIfIndex = <DS1 ifIndex>

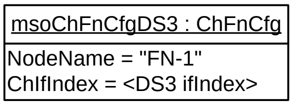
Second instance which assigns downstream channel 2 (DS2) to Fiber Node FN-1:



msoChFnCfgDS2 : ChFnCfg

NodeName = "FN-1"
ChIfIndex = <DS2 ifIndex>

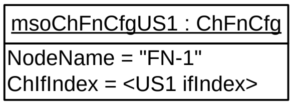
Third instance which assigns downstream channel 3 (DS3) to Fiber Node FN-1:



msoChFnCfgDS3 : ChFnCfg

NodeName = "FN-1"
ChIfIndex = <DS3 ifIndex>

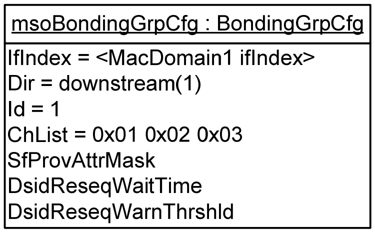
Fourth instance which assigns upstream channel 1 (US1) to Fiber Node FN-1:



msoChFnCfgUS1 : ChFnCfg

NodeName = "FN-1"
ChIfIndex = <US1 ifIndex>

The following diagram highlights the desired state for the BondingGrpCfg object at the end of this scenario.



msoBondingGrpCfg : BondingGrpCfg

IfIndex = <MacDomain1 ifIndex>
Dir = downstream(1)
Id = 1
ChList = 0x01 0x02 0x03
SfProvAttrMask
DsidReseqWaitTime
DsidReseqWarnThrshld

Any attribute (in the above object instances) that is left unassigned is assumed to take the default value as specified in the object model of [OSSI3.0].

6.1.8 Exceptions

Some exception cases might include:

- Configuring MacDomain1 with an invalid or non-existent MAC Domain ifIndex
- Specifying an invalid upstream or downstream ifIndex
- Creating an instance of ChFnCfg before the corresponding FiberNodeCfg instance is created (ChFnCfg has a dependency on the NodeName attribute of the FiberNodeCfg object)
- Creating a duplicate object instance (e.g., non-unique key values)
- Deleting an object instance that does not exist
- Configuring an invalid value for an attribute
- Omitting a required attribute when creating an instance of an object
- Omitting an attribute with a default value when creating an instance of an object when the default value is not appropriate for the Scenario

A MAC Domain cannot be created or deleted through SNMP, this is vendor specific. It is also vendor specific whether removing a MAC Domain also removes all attribute values and dependent relationships which had been previously configured.

6.1.9 Rollback Actions

Before attempting any CMTS configuration changes, a backup of the current, working running configuration should be saved as a precautionary step.

One method of rollback would include destroying instances of objects that were creating in this Scenario. For instances which are statically created and cannot be destroyed, the values would need to be set back to their prior values as captured in the backup of the running configuration which was performed.

6.2 Attribute Based Service Flow Assignment with Channel Bonding

6.2.1 Business Scenario

An MSO would like to control traffic in a channel bonded environment via service flow assignment; segregating traffic to appropriate bonding groups and channel. For instance, an MSO may seek to limit voice traffic to a channel which has high availability and low latency, while data service may have neither of these features. This will allow for appropriate traffic prioritization and service quality for a variety of services.

An MSO utilizing DOCSIS 3.0 and channel bonding configuration in a network with a variety of traffic types may require the additional granularity of attribute assignment for bonding groups and/or channels. Voice services are typically handled by Service Flows that are identified as low latency, high availability. Business class data services should be handled on high availability service flows; while residential data services may not require either of these qualifications and could be handled on a best effort basis. Additionally, metro Ethernet level business offerings might be provisioned on high availability/low latency service flows. There may also be considerations for video services, DSG devices, etc.

6.2.2 Scenario Details

Attributes should be assigned to channels and/or bonding groups defined on the CMTS. The CMTS will then assign service flows to appropriate channels/bonding groups based on the correlation between their capabilities and the attribute masks (required/forbidden/aggregate) of the service flows. Per O.2.1.5 of [OSSI3.0], bits 0, 1 and 2 of the masks indicate bonding, low latency and high availability respectively.

For example, an MSO might deploy 3 service flows, with the following attributes:

- non-bonded, low latency, high availability

  Required attribute mask: 01100000000000000000000000000000

  Forbidden attribute mask: 10000000000000000000000000000000

- bonded, high availability

  Required attribute mask: 10100000000000000000000000000000

- bonded

  Required attribute mask: 10000000000000000000000000000000

Service flows that must be on a channel bonding group, generally for bandwidth requirements, should have bit 0 of the required attribute mask set. Conversely, service flows that should explicitly not be assigned to channel bonding groups should have bit 0 of the forbidden attribute mask set. Additional requirements would be determined equivalently. Bits 16-31 can be assigned by MSOs to define their own operational constraints.

Additionally, TLV 25.17 should be used to identify whether service flows associated with a downstream bonding group is associated with a Resequencing DSID.

High level channel assignment would be as follows:

1. Config file defines service flow requirements.
2. CMTS assigns Service Flows to appropriate channel bonding groups based on bonding group capabilities and service flow required and/or forbidden attribute masks.
3. CM utilizes service flows on assigned channel bonding groups (or non-bonded channels as appropriate.

6.2.3 Assumptions

Network elements (provisioning system, CMs, CMTSs) should be capable of creating and/or utilizing config files with the appropriate TLV encodings (24/25.31,32,33 24.16 and 25.17).

6.2.4 Pre-conditions

There are no additional pre-conditions that have not already been detailed previously in the Assumption and Scenario Details sections.

6.2.5 Management Objects

- CMTS MAC Domain Channel Configuration object

Refer to the MdChCfg object defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the MdChCfg Object section from [OSSI3.0]. The SfProvAttrMask attribute represents the Provisioned Attribute Mask of non-bonded service flow assignment to this channel.

- CMTS Bonding Group Configuration object

This object allows the Operator to configure static bonding groups within a MAC Domain. Refer to the BondingGrpCfg object defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the BondingGrpCfg object section from [OSSI3.0]. The SfProvAttrMask attribute represents the Provisioned Attribute Mask encoding for the bonding group.

6.2.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

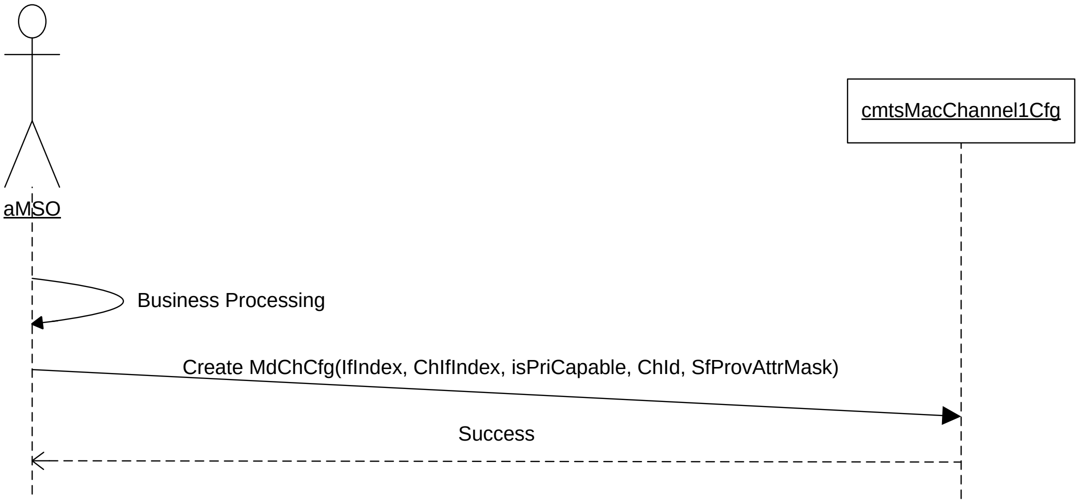

cmtsMacChannel1Cfg
aMSO
Business Processing
Create MdChCfg(IfIndex, ChIfIndex, isPriCapable, ChId, SfProvAttrMask)
Success

Figure 5 – Sequence Diagram for Attribute Based Service Flow Assignment with Channel Bonding

Model is similar for bonded channel groups, with appropriate objects.

6.2.7 Post-conditions

The following diagram highlights the desired state for the MdChCfg object at the end of this scenario. Creating the MdChCfg instance as shown defines a Mac Domain Channel Config.

6.2.8 Exceptions

PacketCable 1.5 specifications dictate that voice traffic should only be carried on non-bonded channels.

6.2.9 Rollback Actions

Before attempting any CMTS configuration changes, a backup of the current, working running configuration should be saved as a precautionary step.

The CM configuration file may need to be reviewed for errors. The last good working configuration file could be downloaded to the CM.

7 PROVISIONING CPE MANAGEMENT SCENARIOS

This section defines Scenarios for provisioning CPE management.

7.1 Configuration of Subscriber Management Group IDs for Packet Filtering

7.1.1 Business Scenario

An MSO who is preparing to assign/delegate IPv6 prefixes to customer equipment would like to maintain the ability to filter and classify IPv6 packets from customer CPE. Legacy filters [RFC 4639] do not support IPv6. Control of data traffic in the Upstream Drop Classifier (UDC)/Subscriber Management model operates differently than legacy IP filters [RFC 4639] and requires a change to configuration management. The way in which Drop Classifiers operate on the data plane differs from legacy IP filters [RFC 4639] in one fundamental way: In the upstream direction the CM performs the classification and in the downstream direction the CMTS performs the classification. Note that while UDCs are a required feature within DOCSIS 3.0, the Subscriber Management extensions are optional and may or may not be present in a particular CMTS implementation.

7.1.2 Scenario Details

This Scenario configures Subscriber Management Group IDs which will only be utilized on DOCSIS 3.0 and Hybrid CMs capable of supporting IPv6 CPEs and supporting the UDC feature. Additionally, once Subscriber Management is configured, upstream filtering groups which remain local to the CMTS (different Group IDs which affect the CMTS upstream interfaces rather than the CM via UDC rule expansion) can be configured to take effect immediately across all CMs. The Subscriber Management Group ID expansion mechanism can be automated to a significant degree, allowing a single set of changes at the CMTS to take action for the entire CM population attached to the CMTS.

This Scenario will configure Subscriber Management Group IDs on the CMTS, which expand the CM Upstream Drop Classifier rules and provide downstream filtering locally to the CMTS. The Group IDs are also populated into the Subscriber Management TLV 62 in the CM configuration file such that during CM registration, the REG-REQ message carries the unexpanded Group ID label with the CMTS responding with the REG-RSP message carrying the expanded UDC classifier rules to the CM. The use of the group ID can dramatically reduce the size of the configuration file when many drop classifier rules are required.

Scenarios include the following:

- CMTS configured for Subscriber Management Group IDs, with up to 20 rules per group:
    - Commercial customers may have special groups that tailor to their needs (RIPv2 permitted, Simple Network Management Protocol (SNMP) permitted, and Windows CIFS file sharing dropped).
    - Residential customers may have one or more groups that enforce the Acceptable Usage Policy/Terms of Service (for example, blocking common server protocols to restrict customers from operating servers).
    - CMTS downstream Group IDs filter against similar criteria to that of the upstream, enforcing the security policy in the downstream direction locally on the CMTS.
- CM configuration file profiles modified to incorporate TLVs for Subscriber Management Group IDs (one or two groups):
    - CMTS may include identical criteria for certain classes of equipment or equipment which is not sufficiently trusted. A process for incrementing or decrementing trust of a CM is outside the scope of this document, but is an important consideration in security policy development.

7.1.3 Assumptions

The MSO has developed processes for a CMTS-centric approach to managing protocol filtering at the CM (as compared to a CM configuration file centric approach). The MSO has configured Subscriber Management filters to include Group IDs for the UDC classifier rules that are to be expanded during the registration process. The MSO has configured the CM configuration files with Subscriber Management Group IDs associated with the appropriate drop classifier rules within the CMTS configuration.

With this model, the assumption is that no static drop classifier rules are directly present in the CM configuration file. One reason for using the Subscriber Management Group ID approach is to significantly reduce the size of the configuration file relative to statically configured IPv4 and IPv6 classifier rules and to provide centralized management at the CMTS. Element Management Systems control the association of the UDC rules and the UDC group IDs.

7.1.4 Pre-conditions

A DOCSIS 3.0 CMTS is required to support the enhanced Subscriber Management feature. A DOCSIS 3.0 or Hybrid CM that supports UDCs (via TLV 5.38) and IPv6 (TLV 5.39) is required. While the potential exists for Hybrid CMs that do not support UDCs, reference designs built to [ICMTR] are likely to support UDCs and IPv6, even if the manner of CPE support may differ at low level. DOCSIS 1.x/2.0 CMs do not support the UDC feature and will ignore the sub-TLVs associated with Subscriber Management Group IDs used by UDCs.

Dynamic config files can be built for CMs which advertise support of IPv6 and UDCs. Pre-3.0 DOCSIS CMs without this support will have config files built with legacy IP and LLC filters. The config file can have both, if the MSO chooses to populate the config file with legacy IP and LLC filters with UDCs.

7.1.5 Management Objects

- CMTS FilterGrp object

The FilterGrp object controls the Subscriber Management filtering criterion that is expanded within the registration response message sent from the CMTS to the CM. The Group ID (GrpId) contains the individual rules that correspond to the expansion of a UDC Group ID into individual UDC rules. The UDC Group IDs are linked to Ids of the FilterGrp object so the CMTS can signal those filter rules as UDCs to the CM during the registration process. Refer to the FilterGrp object defined in the CMTS Subscriber Management Object Model Diagram Figure in Annex P of [OSSI3.0]. This object and its associated attributes are described in Annex P.

7.1.6 Post-conditions

The desired state for the CM at the end of this scenario includes:

- CM is in an operational state.
- CM is configured with the expanded UDC rules communicated by the CMTS registration response (REG-RSP) message, populating rule criterion within the CM's PktClass object.
- CM can classify packets, dropping all packets matching criteria for a given UDC rule in its PktClass object.
- CM can alter its classifier rules upon receipt of a DSC message from the CMTS.

7.1.7 Exceptions

Some exception cases might include:

- Configuring an invalid value for any of the attributes of the FilterGrp object.
- Creating a duplicate Group ID.
- Deleting a Group ID that does not exist.
- Sending a DSC message to the CM for changing a classifier ID that does not exist.

7.1.8 Rollback Actions

TLV 62 is a single configuration setting with only two possible rollback actions possible. Of the two methods, one method requires that the CM reboot in order to take effect while the second method is dynamic and does not require the CM to reboot. The first method is to modify the CM configuration file, removing the Group ID via the TLV 62 entry and reboot the CM. The second method involves removing the classifier IDs associated with the Group ID rule expansion via a DSC message to the CM sent from the CMTS and triggered by an Element Management System.

The FilterGrp object supports creation and deletion of multiple instances. If a partial instance is created, as with a ‘createAndWait’ SNMP Set command, the device may mark this instance as 'notReady'. Once the full instance is created, the device or Operator may update the instance to 'active' such that the instance is in service, which can be performed one rule at a time within the group.

7.2 Configuration of Static UDC Rules for Packet Filtering

7.2.1 Business Scenario

Refer to Section 7.1.1.

7.2.2 Scenario Details

This Scenario configures UDCs on DOCSIS 3.0 and Hybrid CMs.

This Scenario will configure drop classifier rules in the CM configuration file. While this approach is conceptually simpler to implement, from a management perspective such drop classifier rules invoke a penalty in both configuration file size and the potential for increased complexity in order to maintain the list of upstream drop classifiers and force each CM to be rebooted in order for the change to take effect with a new configuration file. If drop classifier rules change relatively infrequently, these deficiencies may not pose a substantial detriment to configuration-file based drop rules.

7.2.3 Assumptions

The MSO has configured drop classifier rules within the provisioning system for all or a given set of configuration profiles. With this model, there is the assumption that only the drop classifier rules are present in the CM configuration file and management of these rules occurs at the provisioning servers rather than at the CMTS. On a DOCSIS 3.0 or Hybrid CM, when both legacy filters and UDC classifier rules are present in the CM configuration file, the CM will register, but the legacy filters will be disabled, and only the UDC rules will be active.

7.2.4 Pre-conditions

A DOCSIS 3.0 CM or Hybrid CM is required to support the UDC feature. DOCSIS 1.x/2.0 CMs do not support the UDC feature and will ignore the TLVs associated with UDCs. A DOCSIS 3.0 CMTS must support IPv6 for CPE management.

7.2.5 Management Objects

There are no CMTS management objects affected in this Scenario.

7.2.5.1 Configuration via CM Configuration File

The CM is configured using TLV 60 [MULPI3.0] in the CM configuration file. The configuration file will contain between 1 and as many as 255 rules. Refer to Annex F of [OSSI3.0] for further details.

7.2.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

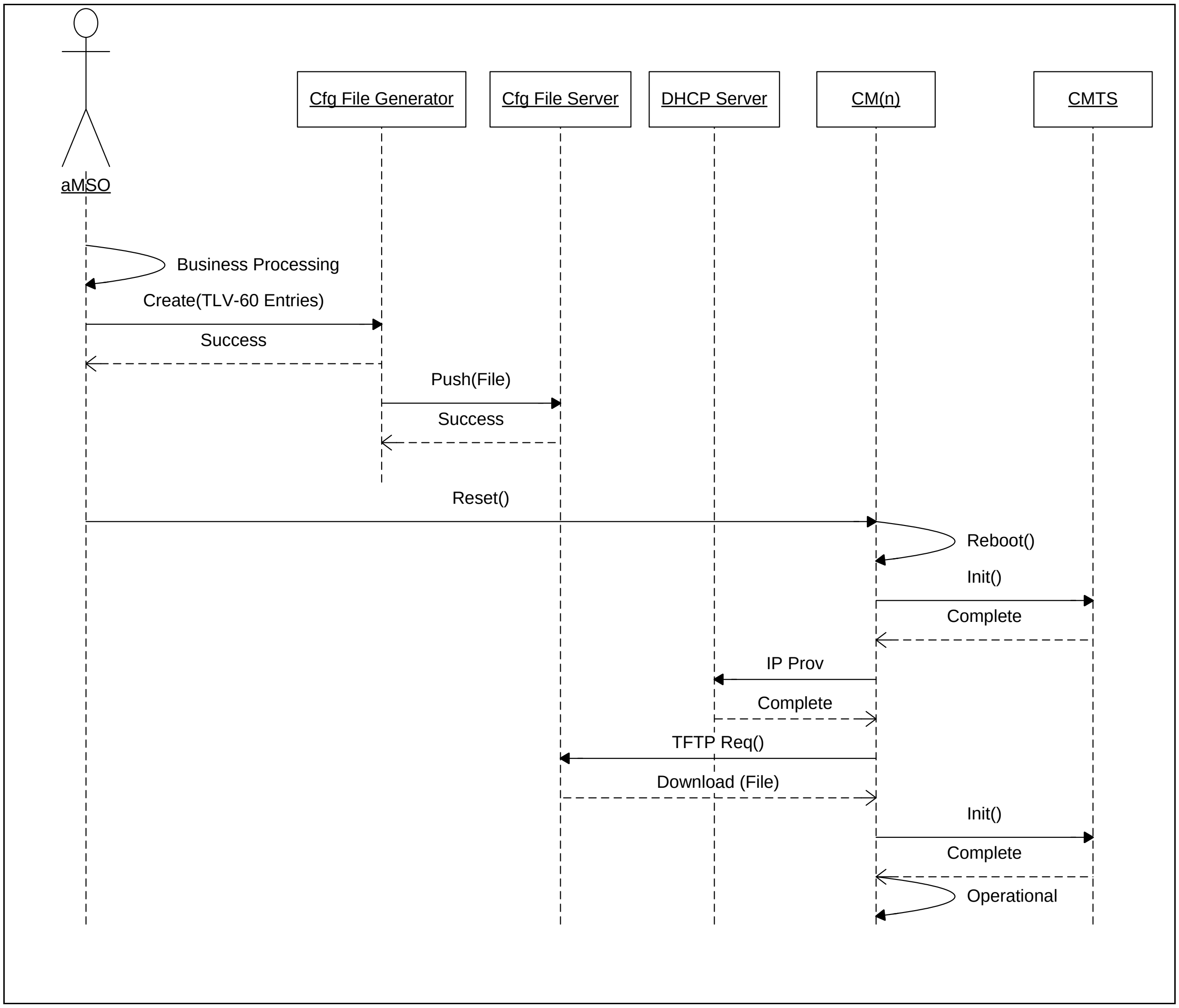


Figure 6 – Sequence Diagram for Configuration of Static UDC Rules for Packet Filtering

7.2.7 Post-conditions

The desired state for the CM after configuration includes:

- CM is in operational state.
- CM has all rules configured in the CM configuration file present in the PktClass object.
- CM is able to parse packets on the upstream and drop any packets matching rule criteria.
- CM is able to change classifier rules upon receiving a DSC message identifying the classifier ID of the rule.

7.2.8 Exceptions

The following exceptions can occur:

If any two UDC or Quality of Service rules set the same classifier priority matching the same protocol criterion, the CM will still register, but the CM's behavior will not be predictable with regards to classification behavior.

7.2.9 Rollback Actions

The following rollback actions may be taken to resolve errors:

- The configuration file should be edited to remove both UDC rules or Subscriber Management group IDs.
- If conflicting priorities are present due to misconfiguration of static UDC and/or QoS rules, the CM configuration file must be edited to avoid the conflict.

7.3 PCMM Management of UDCs

This section defines Scenarios for utilizing PCMM (Packet Cable Multi-Media) for managing Upstream Drop Classifiers (UDCs). The PCMM architecture consists of a Policy Server (acts as a policy decision point/policy enforcement point and manages relationships between application managers and cable modem termination system), an Application Manager (provides an interface to policy server(s) for the purpose of requesting services on behalf of a subscriber or a network management system), a CMTS,a CM and a CPE (Customer Premises Equipment). In a proactive mode of management, the policies are constructed and pushed to the CMTS via the Policy Server, with all CMs carrying a common set of drop classifier rules established by the MSO's security policy. The MSO will typically use packet inspection only at aggregation points to determine trends and alter the drop classification rules accordingly over relatively long periods of time.

For dynamic management of rules constructed based on changing network conditions using reactive mode management, a Deep Packet Inspection (DPI) appliance or special purpose line-card may be present in the CMTS or in one or more network access layer devices in order to perform granular packet analysis, providing timely input to the Application Manager for the purposes of building new just-in-time drop classifier rules that may apply to all CMs, a subset of CMs or a single CM. In this architecture, the CMTS/access router feature card or dedicated appliance communicate with the Application Manager, with the Application Manager parsing the input for specific events that match pre-configured thresholds, or triggers which can then create policies that the Policy Server can then communicate back to the CMTS for enforcement. Such policies might include dynamically rate-shaping or dropping a specific protocol on a specific CM, or particular protocols to or from particular networks for all CMs.

7.3.1 Business Scenario

An MSO would like to utilize their PCMM infrastructure to control UDCs in order to accelerate and automate propagation of drop classifier changes without requiring the CM to be reset. Increasingly, the need to maintain higher levels of availability at the CM/MTA requires more change management be performed by means which do not disturb primary line voice services, enhanced data services and in the near future, IPTV applications.

By making use of PCMM, the CM configuration file need not incorporate all the classifiers the security policy might deem necessary, reducing if not eliminating the number of drop classifier entries that would otherwise need to be present in the CM's configuration file at the time the CM comes online. The PCMM architecture may also be used for proactive, class-based application of UDCs, where all CMs associated with a given tier of service might receive the same drop classifier rules, or via reactive, time-sensitive drop classifier rule changes or additions in order to prevent a major viral outbreak or security threat.

7.3.2 Scenario Details

The Policy Server/Application Manager communicates via COPS (Common Open Policy Services) with the CMTS, where the CMTS communicates DSC messages to the CM in order to add or change classifier criterion.

The following high level steps are performed at the Policy Server/Application Manager.

1. Configure Policy Server with a new policy associated with CM upstream classifiers
2. Define groups
3. Define rule reference numbers
4. Define rule criterion
5. Define rule priority keeping all priorities unique
6. Configure Policy Server for communication with CMTS over COPS protocol

7. Configure CMTS to permit access via IP access lists to allow connection from Policy Server

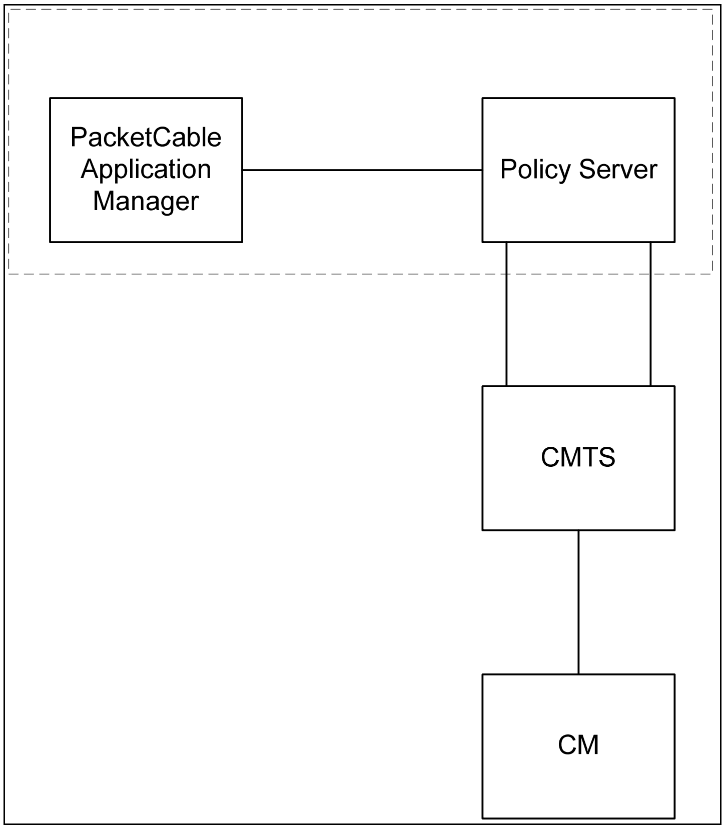


Figure 7 – General PCMM Architecture

7.3.3 Assumptions

The configuration performed in this Scenario assumes that the CMTS, Policy Server/Application Manager software are compliant with the DOCSIS and PCMM protocol specifications. The Policy Server/Application Manager and CMTS must be configured appropriately in order for this Scenario to operate.

7.3.4 Pre-conditions

The PCMM infrastructure is scaled to provide sufficient transactional performance to the meet the requirements of the number of CMTSs and the associated number of CMs per CMTS. Different CMTS makes and models will have implementation imposed constraints on their DSx transaction rate. It has been determined that the use of PCMM for the purposes of UDC automation in a proactive mode will increase DSx activity by roughly 40%, the use of PCMM in a fully dynamic, reactive mode may increase DSx activity by as much as 150%, though averaging only about 60% higher than baseline DSx activity in support of Packet Cable voice services.

A CMTS that is DOCSIS 3.0 and PCMM compliant is required for this Scenario.

7.3.5 Management Objects

7.3.5.1 Policy Server

All Policy Server/Application Manager configuration has been completed prior to this Scenario, as indicated in the Assumption section.

7.3.5.2 CMTS Configuration

7.3.5.2.1 COPS Connection

The CMTS must be configured such that the COPS connection is allowed between the CMTS and the Policy Server. Refer to individual CMTS configuration guides for CLI or SNMP commands to configure an access list permit entry.

Table 1 - CMTS Access List Example

Name	Value
ID	100
IP Address	69.124.13.1
IP Mask	255.255.254.0
Action	permit

7.3.6 Post-conditions

The CM will be configured with UDC rules that were dynamically configured via DSC exchange with the CMTS as directed by a Policy Server/Application Manager in accordance with the MSO's policies.

7.3.7 Exceptions

CMTS DSx limits may be met at the linecard or chassis level due to loads induced by Packet Cable voice services or differentiated data services (turbocharge, speedboost, etc.).

- PCMM Policy Server COPS transaction limit may be reached due to loads imposed by Packet Cable voice services or differentiated data services (turbo speedboost, etc).
- CM implementations may cause DSx transactions to be deferred until a higher priority routine is completed under certain localized high load circumstances. Implementation details differ based on CM reference design or custom development done by the CM developer.
- DOCSIS 2.0 and earlier CMs do not support the UDC feature and must use IP filters. One exception to this general rule is that Hybrid CMs may support UDCs, in such cases where IPv6 data forwarding is desired and UDCs are supported, the Hybrid CMs will operate identically to DOCSIS 3.0 CMs.

Relatively minor errors made in the configuration of the Policy Server's policies, to the individual groups or rules may result in unpredictable behavior. For example, overlapping priorities between any two classifiers, since this rulespace is shared between QoS classifiers and UDCs, may cause unpredictable behavior at the CM.

7.3.8 Rollback Actions

Before attempting any CMTS configuration changes, a backup of the current, working running configuration should be saved as a precautionary step. The PCMM Policy Server's native ability to export the working set of policies into a portable format, or backup to a database that can be restored in the event of configuration error should be utilized in advance of any additional groups or rules. Rollback can be facilitated as follows:

CMTS: Utilize a backup "known good" CMTS configuration template to restore the original configuration or any portion affected by the change. In most modern CMTSs where core management and forwarding functions are affected, the CMTS management cards may need to be set for manual fail-over, allowing the changes and rollback to be performed in a hit-less, or nearly-hitless manner.

Policy Server: Utilize the Application Manager’s product-specific backup or export functions to backup the policy rule store. In the event of misconfiguration, this backup or export may be restored or imported back into the application.

8 MIXED NETWORKS SCENARIOS

This section defines Scenarios for provisioning mixed networks.

8.1 DOCSIS 3.0 and Hybrid CM/eMTA Provisioning for IPv6

8.1.1 Business Scenario

An MSO will have DOCSIS 3.0 and Hybrid CMs present on the network for some time to come. In order to provision the CMs with the appropriate features, it will be necessary to parse the modem capabilities rather than just the DOCSIS version or Vendor Class to determine the features and capabilities of the CM. For example, a Hybrid CM might support bonding in one direction of flow only.

Features to be included in the DOCSIS 3.0 dynamic profiles are largely confined to a change in SNMP access mode via newly defined TLVs. By modularizing groups of desirable features, the DOCSIS 3.0 and Hybrid CMs will be managed in a way that addresses both capabilities unique to the device as well as features required by the tier of service to which the device will be provisioned.

The management model will change somewhat with DOCSIS 3.0 deployments, with the CMTS controlling more aspects of CM configuration (bonding, load balancing, multicast support, etc.), as compared to previous versions of DOCSIS where most configuration was done via the CM configuration file in typical scenarios.

8.1.1.1 Changes to DHCP Options

Dynamic Host Configuration Protocol (DHCP) options used during address acquisition provide helpful information to guide dynamic or class-based provisioning decisions. On the upstream from the CM/eMTA, DHCPv4 option 60 carries the DOCSIS version and CM capability string, while option 43 carries the eDOCSIS eSAFE device class, such as eMTA, eSTB, ePS, etc. For DHCPv6, on the upstream from the CM/eMTA, option 16 carries information analogous to DHCPv4 option 60, while option 17 carries the eDOCSIS eSAFE device class information, equivalent to DHCPv4 option 43. Time of Day (ToD) services must be provided for both IPv4 and IPv6 CM provisioning.

8.1.1.2 Changes to CM TLV Parameter Provisioning

Depending on the Use Case or Scenario, the CM configuration file may include new multicast encodings, Upstream Drop Classifiers (UDCs), Service Flow attribute masks and other encodings. An Extended Message Integrity Check (MIC) is generated by the provisioning system for all sub-TLVs under TLV 43 (previously only vendor-specific extensions, now includes many CableLabs DOCSIS 3.0 features). This Extended MIC is part of the DOCSIS 3.0 enhanced security features, with the generated value created by the provisioning system prior to the configuration file being sent to the CM. TLV 43 includes such features as Load Balancing, L2VPNs, Source Address Verification (SAV), Service Flow Attribute Mask, Multicast Authorization, etc.

A typical DOCSIS 3.0 CM configuration file will contain TLV 53 (SNMPv1v2c Coexistence Configuration), TLV 54 (SNMPv3 Access View Configuration), TLV 55 (SNMP CPE Access Control), TLV 60 (Upstream Drop Classifiers) and, in some cases, TLV 62 (Subscriber Management Group ID UDC management).

In cases where the provisioning server is not capable of supporting DOCSIS 3.0 TLVs, or the edge device is a Hybrid DOCSIS Cable Modem, the Operator may also be able to define certain DOCSIS 3.0-like capabilities, such as downstream channel bonding, within the configuration of the CMTS. In this case, the devices would be identified via the respective ID string containing the CM capabilities, identifying the device as Pre-3.0 DOCSIS.

8.1.1.3 Changes to SNMP Access Modes

With regard to CM configuration management, the most significant change is the migration to the SNMP Coexistence access mode from that of NmAccess mode. SNMP OpenAccess mode [OSSI3.0], which is an unrestricted mode, is unsupported by DOCSIS 3.0. The CM will not provide SNMP access if the configuration file does not contain SNMP access control TLVs such as docsDevNmAccessTable or SNMP coexistence TLV 11 or TLV 34, TLV 53 or TLV 54.

8.1.2 Scenario Details

8.1.2.1 CM Configuration Scenario Details

8.1.2.1.1 DHCPv4 Options

This section identifies the DHCPv4 options parsed by the DHCP server in order to determine DOCSIS version and CM capabilities.

Option 60 ASCII values:

- docsis1.0
- docsis1.1:xxxxxxx
- docsis2.0:xxxxxxx
- docsis3.0:

Option 125 VIVSO [RFC 3925] encoded CM capability values for DOCSIS 3.0 devices (the included list is descriptive, not comprehensive):

- UDC
- Multicast DSID Forwarding
- Multicast DSID
- IPv6
- Multiple Transmit Channel (upstream bonding)
- Multiple Receive Channel,(downstream bonding)

Option 43 ASCII values:

- eMTA
- eDVA
- ePS
- eSTB
- eTEA
- eROUTER

8.1.2.1.2 DHCPv6 Options

This section identifies the DHCPv6 options parsed by the DHCP server in order to determine DOCSIS version and CM capabilities.

Option 16 - containing a 4 octet enterprise number 4491 (CableLabs), the 2 octet value indicating a data length of 9, followed by the ASCII encoded value:

- docsis1.0
- docsis1.1:xxxxxxx
- docsis2.0:xxxxxxx
- docsis3.0:

Option 17 - containing 4 octets, the 2 octet value indicating a data length of 3-8, followed by the encoded value of the device type:

- eMTA
- eDVA
- ePS
- eSTB
- eTEA
- eROUTER

Refer to the Device Type Option section of [CANN DHCP-Reg] for additional details.

Option 17, suboption 34 - VIVSO [RFC 3925] encoded CM capability values for DOCSIS 3.0 devices (the included list is descriptive, not comprehensive):

- UDC
- Multicast DSID Forwarding
- Multicast DSID
- IPv6
- Multiple Transmit Channel
- Multiple Receive Channel

8.1.2.1.3 REG-REQ Modem Capabilities Encodings

In addition, DOCSIS 3.0 and Hybrid CMs report the following within the Modem Capabilities encodings of the Registration Request messages according to Annex C of [MULPI3.0]:

- DOCSIS version (TLV 5.2)
- Multicast DSID Support (TLV 5.32) - The number of DSIDs supported by CM
- Multicast DSID Forwarding (TLV5.33) - Ability to forward Multicast to CPEs
- Upstream bonding support MTC (TLV 5.24) - Multiple Transmit Channel
- Downstream bonding support MRC (TLV 5.29) - Multiple Receive Channel
- IPv6 support (TLV 5.39) - IP version 6 protocol support
- DOCSIS 3.0 Cable Modems include TLV-29 lists whether the client supports DS Channel Bonding

8.1.2.1.4 SNMP Access Mode Configuration

Pre-3.0 DOCSIS CMs will be provisioned with a traditional DOCSIS 1.1/2.0 style configuration file and are typically managed by SNMPv1/v2c via SNMP NmAccess mode (via TLV 11 entries). It should also be noted that Hybrid CMs must support both SNMP NmAccess and Coexistence modes, as defined in [OSSI3.0] and [ICMTR].

DOCSIS 3.0 and Hybrid CMs will be provisioned with a DOCSIS 3.0 style configuration file and are managed by SNMPv1v2c Coexistence mode (via TLV 53, TLV 54, and TLV 55 entries).

Due to the different SNMP access modes, an NMS must be able to distinguish between Pre-3.0 DOCSIS CMs and DOCSIS 3.0 and Hybrid CMs.

SNMPv1v2c Coexistence Configuration (TLV 53)

- CommunityName
- TransportAddressAccess

    - TransportAddress (IPv4 NMS address)
    - TransportAddressMask (IPv4 NMS address mask)
    - TransportAddress (IPv6 NMS prefix)
    - TransportAddressMask (IPv6 NMS prefix length)
- AccessViewType
- AccessViewName

SNMPv3 Access View Configuration (TLV 54)

SNMP CPE Access Control (TLV 55)

8.1.2.2 CMTS Configuration Scenario Details

Refer to Section 6.1 for an example CMTS configuration using a 3x1 topology.
Once configured, the DOCSIS 3.0 CMTS is then responsible for advertising MAC Downstream Descriptor (MDDs), sent periodically on all enabled DS channels, advertising the channel sets and topology ambiguity resolution lists available within the MAC domain. The MDD message provides vital information to the CM prior to registration, informing the CM of what the CMTS expects during the CM's registration exchange. For example, the MDD contains the IP provisioning mode, enables or disables security features, such as EAE, and sets the CM Status reporting.

The MDD messages include the following additions to perform IPv6 provisioning with DOCSIS 3.0 and certain Hybrid CMs which support IPv6.

- IP Initialization Parameters TLV (TLV 5): This TLV is used to communicate to the CM details about its IP services.
    - IP Version (TLV 5.1):

      0 = IPv4 Only
      1 = IPv6 Only (Required setting for this Scenario)
      2 = Alternate Provisioning Mode (APM)
      3 = Dual-stack Provisioning Mode (DPM)
      4 - 255 = Reserved

    - Pre-Registration DSID (TLV 5.2): DSID value to be used by the CM for filtering and forwarding Downstream Link-Local Multicast used for IPv6 stack initialization and Neighbor Solicitation prior to registration.

8.1.3 Assumptions

This Scenario assumes that there currently is a correctly configured and operational provisioning server capable of dynamic profile generation or, alternatively, a provisioning server capable of parsing CM DOCSIS version and associating a class-based profile accordingly. This Scenario also assumes that there are deployed and functional DOCSIS 3.0 and Hybrid CMs able to support such features as channel bonding in at least one direction of flow and/or IPv6 for management, or management and CPE traffic forwarding.

- Dynamic provisioning of CM via CM capabilities is assumed, though a scenario is provided for class-based (semi-dynamic) CM provisioning where features are more generalized and closely associated with device class (eCM, ePS, eRouter, eDVA, eMTA, eSTB, etc.) and DOCSIS version.
- DOCSIS 3.0 CMs are required for full bonding support (e.g., 4x4 topology) and are assumed to be used only in bonded configurations.

Hybrid CMs, within their capabilities, will be used in bonded configuration in whichever direction the CM might support bonding. Where bonding is not supported in a given direction of flow, load balancing will be used instead.

8.1.4 Pre-conditions

8.1.4.1 Provisioning Server

The provisioning server must be capable of parsing beyond the DOCSIS version for the individual CM capabilities and eDOCSIS device type, generating configuration files according to these attributes dynamically. Alternatively, the provisioning system must be able to parse for the DOCSIS version and eDOCSIS device type in order to provide an associated configuration file for the tier of service and device class.

8.1.4.2 CMTS

A DOCSIS 3.0 CMTS is required.

8.1.4.3 CM

Hybrid CMs, which support IPv6 and DOCSIS 3.0 CMs, are required.

Pre-3.0 DOCSIS CMs, which only support IPv4, are supported in this Scenario.

8.1.5 Management Objects

- CMTS MAC Domain Configuration object

Refer to the MdCfg object and IpProvMode attribute defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the MdCfg Object section from [OSSI3.0].

IpProvMode will be configured to ‘ipv6Only’ such that CMs/eMTAs that support IPv6 will register with the CMTS as IPv6 single stack. Any devices not supporting IPv6 will proceed with IPv4 single stack operation.

8.1.6 Sequence Diagram

This section illustrates the UML Sequence Diagrama for this Scenario. Refer to Appendix I.3 for details on the notation used.

8.1.6.1 CMTS

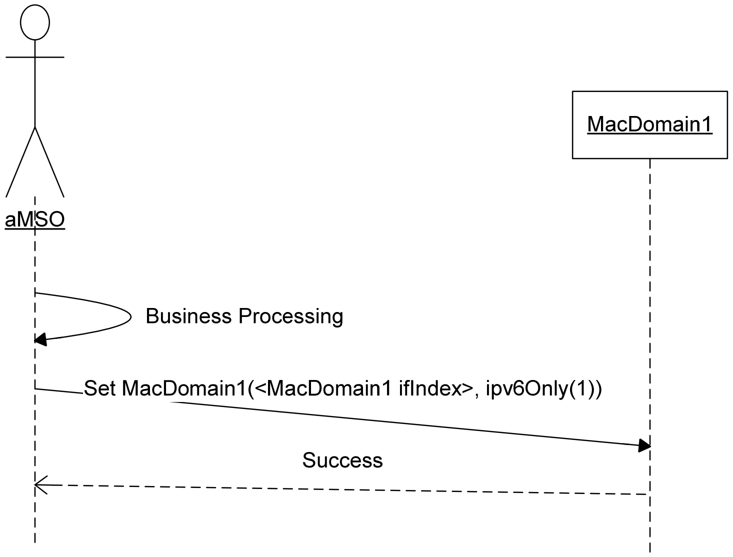


Figure 8 – CMTS Sequence Diagram for DOCSIS 3.0 and Hybrid CMTS/eMTA Provisioning for IPv6

8.1.6.2 CM

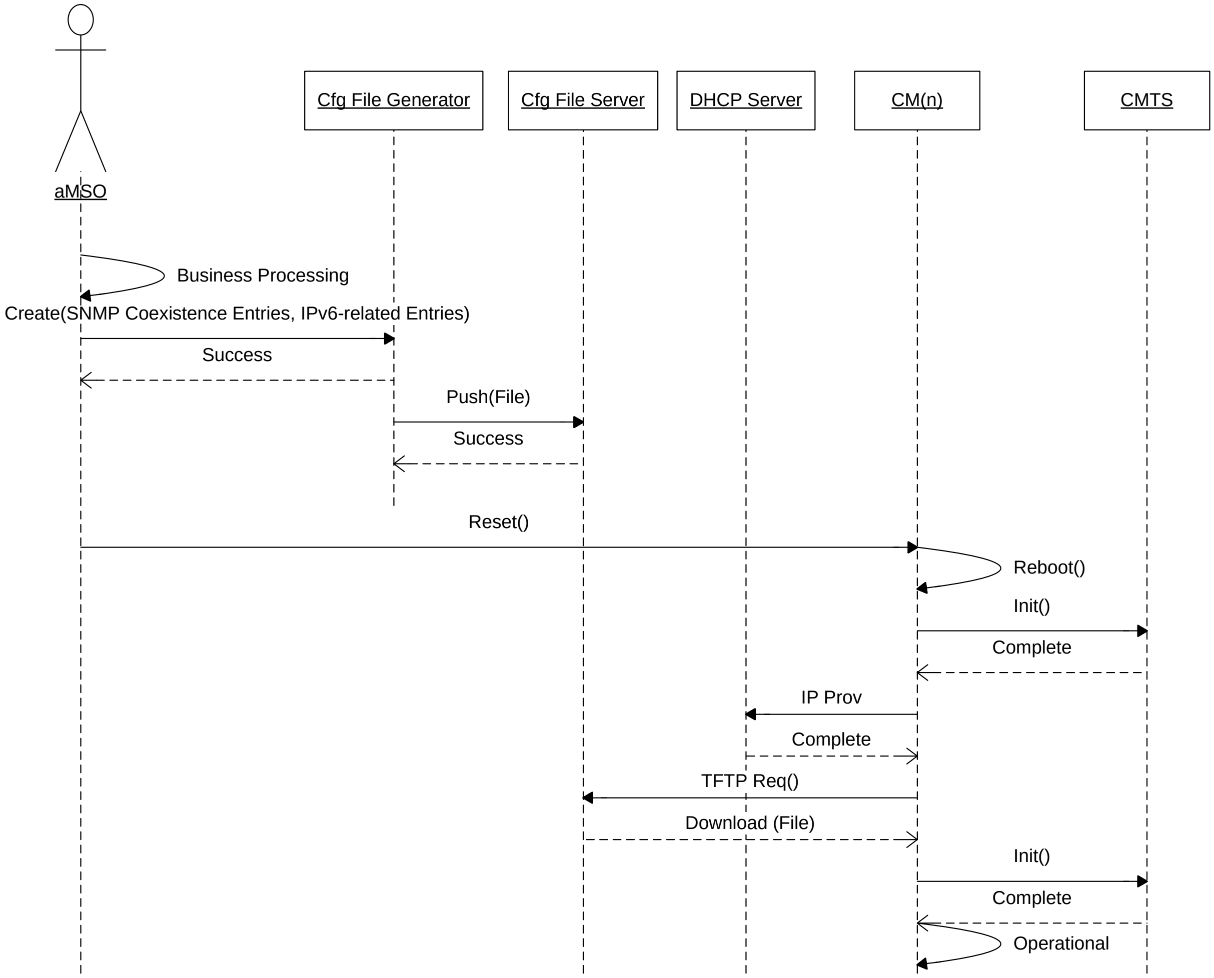


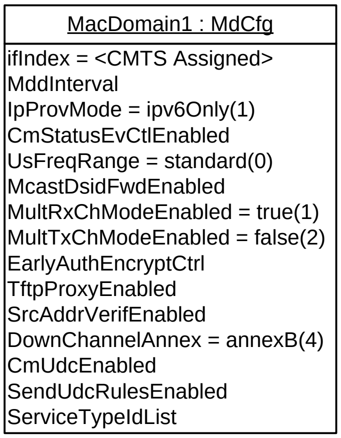
Figure 9 – CM Sequence Diagram for DOCSIS 3.0 and Hybrid CM/eMTA Provisioning for IPv6

8.1.7 Post-conditions

8.1.7.1 CMTS

A DOCSIS 3.0 CMTS may be configured for a 3x1 topology with DOCSIS 3.0 CMs and downstream bonding-capable and IPv6-capable Hybrid CMs connected to a single Fiber Node consisting of three downstreams and one upstream. Refer to Section 6.1 for details on this topology configuration including configuring MdCfg downstream bonding attributes shown in the object instance below.

The following diagram highlights the desired state for the MdCfg object (MAC Domain 1 instance) at the end of this scenario.



MacDomain1 : MdCfg

ifIndex = <CMTS Assigned>
MddInterval
IpProvMode = ipv6Only(1)
CmStatusEvCtlEnabled
UsFreqRange = standard(0)
McastDsidFwdEnabled
MultRxChModeEnabled = true(1)
MultTxChModeEnabled = false(2)
EarlyAuthEncryptCtrl
TftpProxyEnabled
SrcAddrVerifEnabled
DownChannelAnnex = annexB(4)
CmUdcEnabled
SendUdcRulesEnabled
ServiceTypeIdList

Any attribute (in the above object instances) that is left unassigned is assumed to take the default value as specified in the object model of [OSSI3.0].

8.1.7.2 CM/eMTA

DOCSIS 3.0 CMs/eMTAs and Hybrid CMs/eMTAs which support IPv6 will be in an operational state operating in SNMPv1v2c Coexistence Mode and be manageable via IPv6. Pre-3.0 DOCSIS CMs/eMTAs will be operational using SNMP NmAccess Mode and be manageable via IPv4. Devices may be provisioned depending on capabilities of the provisioning system either based on a device class or individual device capability.

8.1.8 Exceptions

Duplicate SNMP Coexistence entries using TLV-11 and TLV-53 would be detected at the CM. The CM will fail to register and will reside in a non-operational registration state as reported both at the CMTS and the CM. The CM will log a Local Log event and may send a Syslog and SNMP Notification for that event (TLV-11 Parsing Error).

8.1.9 Rollback Actions

Configuration file may need to be reviewed for errors. The last good working configuration file could be downloaded to the CM.

8.2 DOCSIS 3.0 CM and Pre-3.0 DOCSIS CM/eMTA Provisioning in a Downstream Channel Bonding Topology

8.2.1 Business Scenario

When choosing how to offer DOCSIS 3.0 features in a mixed-mode environment, an MSO may choose to provide only a subset of DOCSIS 3.0 features to the customer. For example, an MSO may choose to deploy DOCSIS 3.0 channel bonding features only, while maintaining DOCSIS 2.0 Subscriber Management and IPv4 for both DOCSIS 3.0 and Pre-3.0 DOCSIS devices. The business reasons for such a deployment center around subscriber speed increases, deployment of modular CMTS resources, and configuration flexibility while maintaining compatibility for legacy devices on the network.

8.2.2 Scenario Details

MSO offers service supporting Pre-3.0 DOCSIS devices, as well as DOCSIS 3.0 devices using 3 bonded downstreams and 1 upstream (i.e., a 3x1 topology). This scenario will provision the network devices to provide this service offering.

This Scenario is defined independently of the type of DOCSIS 3.0 CMTS used (e.g., I-CMTS or M-CMTS) but could be applied to each deployment type.

8.2.2.1 CM Configuration Scenario Details

All CMs use DOCSIS 1.1/2.0 style configuration files. The config files include TLV 11 entries for configuring SNMP NmAccess mode for SNMP management of the CMs. The config file will also contain a higher Max Sustained Traffic Rate (TLV-25.8) taking into account the bonded DS configuration.

This Scenario bypasses the need for TLV-53 (SNMPv1v2c Coexistence configuration) in the configuration file by relying on TLV 11 entries for NmAccess mode configuration.

8.2.2.2 CMTS Configuration Scenario Details

Configuring the CMTS for a 3x1 topology is required and defined in Section 6.1.

Once configured, the DOCSIS 3.0 CMTS is then responsible for advertising MAC Downstream Descriptor (MDDs), sent periodically on all enabled DS channels, advertising the channel sets and topology ambiguity resolution lists available within the MAC domain. The MDD message provides vital information to the CM prior to registration, informing the CM of what the CMTS expects during the CM's registration exchange. For example, the MDD contains the IP provisioning mode, enables or disables security features, such as EAE, and sets the CM Status reporting.

The MDD messages include the following additions to perform DS channel bonding with DOCSIS 3.0 and certain Hybrid CMs which support downstream channel bonding capabilities.

- DOCSIS MAC Management Header: Specifying type 33 (MDD), version 4.
- Configuration Change Count: Increments by 1 whenever MDD message contents change.
- Number of Fragments
- Fragment Sequence Number
- Current Channel DCID: The ID of the downstream channel on which the MDD is being sent.
- Downstream Active Channel List (TLV 1): This TLV will be present for every downstream channel in every MD-DS-SG that contains the current channel.
    - Channel ID (TLV 1.1): The ID of the channel being listed.
    - Frequency (TLV 1.2): The center frequency of the channel.
    - Modulation Order (TLV 1.3): (Optional) Bit-field describing the channel modulation and annex.
    - Primary Capable (TLV 1.4): Primary capability of channel. Always specifies primary capable.
    - CM-STATUS Event Enable (TLV 1.5): Bit-mask representing the enable/disable status of the various CM-STATUS event types.
- MAC Domain Downstream Service Group (TLV 2): This TLV will be present once for each MD-DS-SG reached by this primary downstream channel.
    - MD-DS-SG ID (TLV 2.1): One-byte identifier of the MD-DS-SG.
    - MD-DS-SG DCID List (TLV 2.2): N number of bytes, which are the DCIDs (downstream channel id) in this MD-DS-SG.
- Downstream Ambiguity Resolution Frequency List (TLV 3): List of frequencies to assist the CM in CM-SG ambiguity resolution. This will be present whenever there are more than one MD-DS-SG TLVs present.
- RCP Reporting Control TLV (TLV 4): This controls the reporting of RCPs sent by CMs in REG-REQ-MP messaging.

- RCP Center Frequency Spacing (TLV 4.1): The value will indicate either 6 or 8 MHz spacing depending on the current Annex mode of the CMTS blade.

  For Annex B, 0 is sent indicating 6 MHz spacing.
  For Annex A, 1 is sent indicating 8 MHz spacing.

- Verbose RCP Reporting (TLV 4.2)

  0 = CM MUST NOT provide verbose reporting of all its Receive Channel Profile(s) (both standard profiles and manufacturer’s profiles).
  1= CM MUST provide verbose reporting of Receive Channel Profile(s) (both standard profiles and manufacturer’s profiles).

8.2.3 Assumptions

A DOCSIS 3.0 CMTS is required for providing a 3x1 topology. A DOCSIS 3.0 CM or Hybrid CM which supports downstream channel bonding capabilities is required in order to utilize the three bonded downstream channels. Pre-3.0 DOCSIS CMs/eMTAs may also reside on a single channel in this topology.

The current generation provisioning system does not support encoding TLV-53 in the CM config files. CM firmware may be required which bypasses the need for TLV-53 inclusion in the configuration file.

It is assumed that Pre-3.0 DOCSIS devices will correctly handle TLV 25.8 Max Sustained Traffic Rate config file entries that are greater than the device capabilities, based on rates targeted for DOCSIS 3.0 CMs operating in MRC mode.

It is assumed that the current generation DHCPv4 Server will properly handle the Option 60 "docsis3.0:" entry received from a DOCSIS 3.0 CM.

Since the CMTS is configured for bonded downstream channels, DOCSIS 3.0 CMs and Hybrid CMs will register on bonded downstream channels with a 1.1/2.0 config file. Vendor specific configuration steps may be required to force DOCSIS 3.0 CMs and Hybrid CMs to use primary downstreams provided from an EQAM or I-CMTS.

The Pre-3.0 DOCSIS CMs will come up on ANY available DS (integrated or modular), as long as the CM’s tuner can tune to that frequency. Enabling load balancing would then allow the CMs to move from one primary to another.

Vendor specific configuration steps may be required to force Multimedia Terminal Adapters (MTAs) to integrated (legacy) downstream channels only.

8.2.4 Pre-conditions

8.2.4.1 Provisioning Server

A current generation provisioning server is used, which does not provide support for DOCSIS 3.0 specific TLVs.

In addition, the current generation DHCPv4 Server is used, which does not have knowledge of the Option 60 "docsis3.0:" entry received from a DOCSIS 3.0 CM.

8.2.4.2 CMTS

The CMTS must support bonding and load balancing functionality. The CMTS must support the DOCSIS 3.0 MAC Downstream Descriptor (MDD) messaging to support a mixed environment of both certified DOCSIS 3.0 and Pre-3.0 DOCSIS devices.

8.2.4.3 CM

The DOCSIS 3.0 and Hybrid CMs that support bonding in at least one direction of flow must be used whenever bonded operation is desired. In all other scenarios where a legacy CM or a Hybrid CM supporting bonding in only one direction of flow is present, the CM will be operated in load-balanced mode.

Pre-3.0 DOCSIS CMs (IPv4) supporting 1 downstream and 1 upstream are also included in the network environment.

The CMs are configured for SNMP NmAccess mode via TLV 11 config file entries.

8.2.5 Management Objects

- CMTS MAC Domain Configuration object

Refer to the MdCfg object and IpProvMode attribute defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the MdCfg Object section from [OSSI3.0].

To configure a previously created MAC Domain instance (referred to as MAC Domain 1 in this Scenario) using vendor specific methods, the MdCfg object is used. Configuring the MdCfg instance will require using the CMTS determined ifIndex of the MAC Domain interface. Using the MAC Domain ifIndex, the following MdCfg attributes are configured:

- Enable Multiple Receive mode
- Disable Multiple Transmit mode

Refer to Section 6.1.5 for further details on the 3x1 topology configuration.

8.2.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

8.2.6.1 CMTS

Refer to Section 6.1.6 for the full 3x1 topology Scenario diagram.

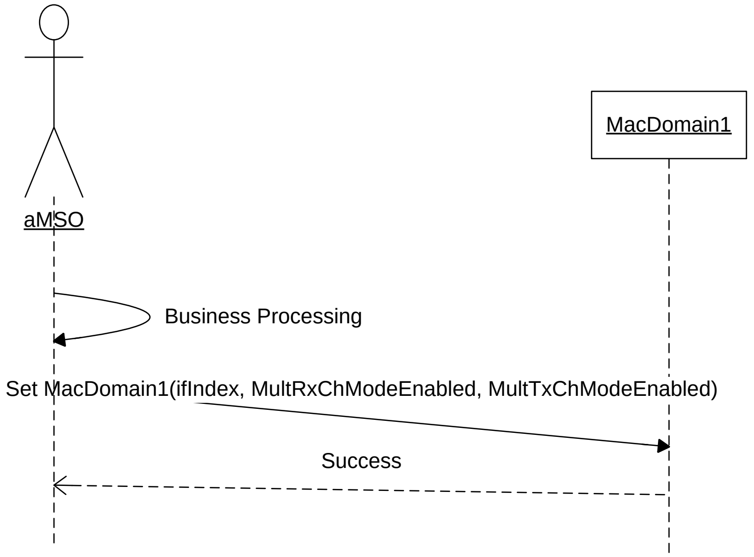

MacDomain1
aMSO
Business Processing
Set MacDomain1(ifIndex, MultRxChModeEnabled, MultTxChModeEnabled)
Success

Figure 10 – CMTS Sequence Diagram for DOCSIS 3.0 CM and Pre-3.0 DOCSIS CM/eMTA Provisioning in a Downstream Channel Bonding Topology

8.2.6.2 CM

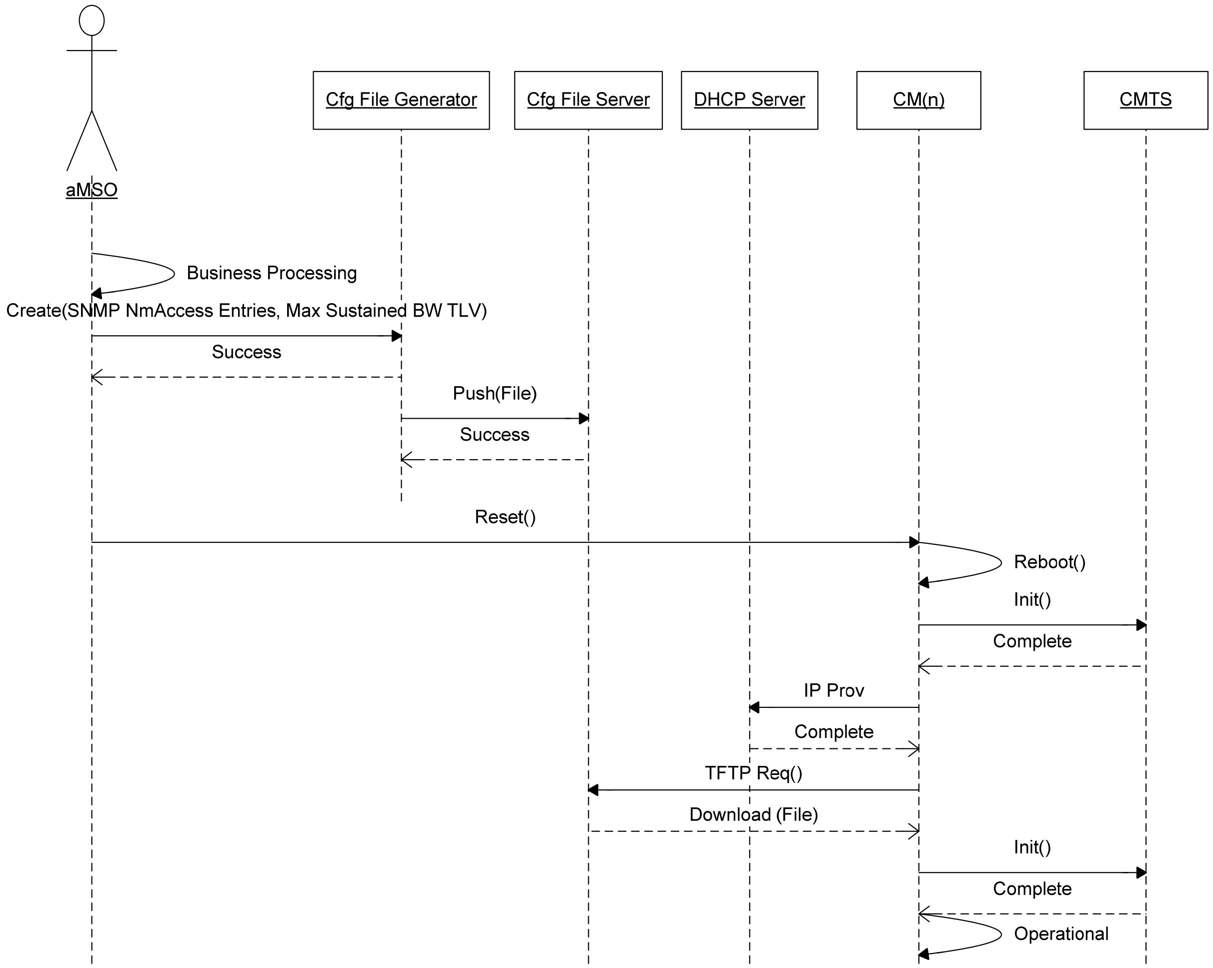


Figure 11 – CM Sequence Diagram for DOCSIS 3.0 CM and Pre-3.0 DOCSIS CM/eMTA Provisioning in a Downstream Channel Bonding Topology

8.2.7 Post-conditions

The CMs will be in an operational state operating in SNMPv1v2c NmAccess Mode and be manageable via IPv4. DOCSIS 3.0 CMs will be operating in MTC mode utilizing 3 modular downstreams and 1 upstream with a higher provisioned Max Sustained BW (TLV-25.8) rate. Pre-3.0 DOCSIS CMs/eMTAs will be operating on a single downstream and upstream as if in a DOCSIS 2.0 legacy network.

The CMTS will be operating with a 3x1 topology. Refer to Section 6.1.7 for further details.

MacDomain1 : MdCfg

ifIndex = <CMTS Assigned>
MultRxChModeEnabled = true(1)
MultTxChModeEnabled = false(2)

8.2.8 Exceptions

If the configuration file has errors the CM will not register and will reject the config file.

Refer to Section 6.1.8 for CMTS exception cases.

8.2.9 Rollback Actions

Configuration file may need to be reviewed for errors. The last good working configuration file could be downloaded to the CM.

Refer to Section 6.1.9 for CMTS rollback actions.

8.3 Migrating DHCPv4 Option Configuration to a DHCPv6 Service

8.3.1 Business Scenario

An MSO wishes to migrate DOCSIS 3.0 Cable Modems from an IPv4-only provisioning mode to any of the alternative DOCSIS 3.0 provisioning modes: IPv6-only, Alternate Provisioning Mode (APM), or Dual-stack Provisioning Mode (DPM).

8.3.2 Scenario Details

This scenario configures a DHCPv6 service with settings corresponding to the DHCPv4 option settings in order to enable a "non-IPv4Only" provisioning mode for DOCSIS3.0 Cable Modems.

8.3.3 Assumptions

This scenario assumes that there is currently a correctly configured and operational DHCPv4 service used to provision a DOCSIS Cable Modem network.

8.3.4 Pre-conditions

A DOCSIS 3.0 CMTS and an IPv6-capable Cable Modem deployment is required.

8.3.5 Management Objects

- CMTS MAC Domain Configuration object

Refer to the MdCfg object and IpProvMode attribute defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the MdCfg Object section from [OSSI3.0].

8.3.5.1 Configuring DHCP Service Settings Based on Client Data

Some DHCP services allow configuration to be based on data sent by the DHCP client to the DHCP service. For example, in DHCPv4 the version of DOCSIS supported by a cable modem can be determined by inspecting the value of the Vendor Class ID (option 60) sent by the cable modem, and the DHCP service may be configured to respond to the cable modem differently depending on the version of DOCSIS the CM supports.

Therefore, when mapping DHCPv4 configuration to DHCPv6 configuration it is useful to know how DHCPv4 data sent by the DOCSIS cable modem maps to equivalent DHCPv6 data. Additionally, some data that exists in DHCPv6 does not have an equivalent in DHCPv4, but may be useful in configuring the DHCPv6 service.

Table 2 shows all of the data sent by a DOCSIS 3.0 cable modem to the DHCP service, organized such that the DHCPv4 settings are mapped to the equivalent DHCPv6 settings.

Table 2 - DHCPv4 Client Data to DHCPv6 Client Data Mapping

Data Type	DHCPv4 Setting	DHCPv6 Setting
MAC Address	chaddr header field (client hardware address): A 16-byte field containing a 6-byte Ethernet MAC address followed by 10 zero bytes.	Option 17.36 (Device ID): A 6-byte Ethernet MAC address
Client Identifier	Option 61 Typically, but not necessarily, the htype value 1 as the first byte (indicating Ethernet), followed by the 6-byte MAC address.	Option 1 Contains a DUID (DHCP Unique ID), which can be constructed in one of three ways as described in [RFC 3315]. Note that an Operator cannot assume a particular construction of the DUID, such as the inclusion of the device MAC address. For MAC address based identification it is more appropriate to use the Option 17.36 Device ID field.
Parameter Request List	Option 55 Must include the following option codes: 1 (Subnet Mask) 2 (Time Offset) 3 (Router Option) 4 (Time Server Option) 7 (Log Server Option)	Option 17.1 (Option Request Option - ORO) Must include the following vendor-specific option codes: 37 (Time Protocol Servers) 38 (Time Offset) 32 (TFTP Server Addresses) 33 (Configuration File Name) 34 (SYSLOG Server Addresses)
Vendor Class ID	Option 60 Must have the ASCII value: docsis3.0:	Option 16 Must contain: • the 4-byte enterprise number 4491, the 2-byte value indicating a data length of 9, followed by the ASCII encoded value: docsis3.0:
TLV5 Encoding (Modem Capabilities)	Option 125.5 The DHCPv4 and DHCPv6 data for this option are the same, as specified in the "Modem Capabilities Encoding" sub-section of [MULPI3.0].	Option 17.35 The DHCPv4 and DHCPv6 data for this option are the same, as specified in the "Modem Capabilities Encoding" sub-section of [MULPI3.0].
Request Trivial File Transfer Protocol (TFTP) Servers Option	Option 125.1.2	Option 17.1.32 - see the "Parameter Request List" data type described previously in this table.
Identity Association for Non-Temporary Addresses (IA_NA)	N/A	Option 3

Data Type	DHCPv4 Setting	DHCPv6 Setting
Rapid Commit Option	N/A	Option 14 This option has no data (length = 0), its presence signals use of the two message exchange for address assignment.
Reconfigure Accept Option	N/A	Option 20 This option has no data (length = 0), its presence signals the modem's willingness to accept Reconfigure messages.
Note: PacketCable 1.5 and 2.0 put additional requirements on DHCP options for the CM when used with an embedded eMTA and eDVA.		

8.3.5.2 Configuring DHCP Service Settings Based on CMTS Inserted Data

Some DHCP services allow configuration to be based on data added by a DHCP Relay Agent, such as a DOCSIS CMTS, into the client DHCP packet.

For example, the CMTS will add the cable modem MAC address as the value of the "Remote ID" (DHCPv4 Relay Agent Information Option 82, Remote ID Sub-Option 2) to the client DHCP packet.

The DHCP service can be configured to make decisions based on the cable modem that the requesting DHCP client is behind, as identified by the Remote ID value.

Table 3 - DHCPv4 CMTS Inserted Data to DHCPv6 CMTS Inserted Data Mapping

Data Type	DHCPv4 Setting	DHCPv6 Setting
Gateway IP Address (giaddr)	giaddr header field A 4-byte network order IP address, indicating the subnet, or group of subnets, to which the device may belong.	LINK-ADDRESS field of the DHCP RELAY-FORWARD message. An identifier for the interface on which a DHCP client message was received on the CMTS.
Circuit ID	Option 82.1 The DHCP Relay Agent Information Option 82, Sub-Option 2 (Circuit ID)	Option 18 (Interface-ID)
Remote ID	Option 82.2 The DHCP Relay Agent Information Option 82, Sub-Option 2 (Remote ID), set to the 6-byte ethernet MAC address of the cable modem's RF side interface.	Option 1026 The DOCSIS Relay Agent CM MAC Address Option, set to the 6-byte ethernet MAC address of the cable modem's RF side interface.
DOCSIS Device Class	Option 82.4 The DHCP Relay Agent Information Option 82, Sub-Option 4 (DOCSIS Device Class)	N/A: No Equivalent
CMTS DOCSIS Version Number	Option 82.9.1.1 The DHCP Relay Agent Information Option 82, Sub-Option 9 (Vendor Specific Information), Sub-Sub-Option 1 (CMTS DOCSIS Version), Sub-Sub-Sub-Option 1 (CMTS DOCSIS Version Number)	Option 1025.1 The DHCPv6 Relay Agent CMTS Capabilities Option 1025, Sub-Option 1 (CMTS DOCSIS Version Number).

8.3.5.3 Configuring DHCP Settings Assigned to DOCSIS 3.0 Cable Modems

Table 4 identifies all of the DHCPv4 settings that are requested and/or required by DOCSIS 3.0 cable modems and their equivalent DHCPv6 settings. Note that some settings are considered non-critical in DHCPv4, but all of the listed settings are required for DHCPv6.

When migrating from an IPv4 Only mode to an IPv6-enabled environment, all of the following DHCPv4 settings must have their equivalent settings configured on the DHCPv6 service.

Table 4 - DHCP Settings Required by DOCSIS 3.0 Cable Modems

Data Type	DHCPv4 Setting	DHCPv4 Required?	DHCPv6 Setting
IP address	yiaddr header field	Critical	Option 3 - Identity Association for Non-Temporary Addresses (IA_NA)
TFTP servers	siaddr header field, or option 125.2	Critical	Option 17.32
Configuration file name	file header field	Critical	Option 17.33
Time Offset	Option 2	Non-Critical	Option 17.38
Time Servers	Option 4	Non-Critical	Option 17.37
Syslog Servers	Option 7	Non-Critical	Option 17.34
Subnet mask	Option 1	Non-Critical	N/A
Gateways (routers)	Option 3	Non-Critical	N/A
Lease time	Option 51	Critical	Option 3 - Identity Association for Non-Temporary Addresses (IA_NA)
Server Identifier	Option 54	Automatic	Option 2

8.3.6 Sequence Diagram

The sequence of messages exchanged in DHCPv4 is provided in the Establish IPv4 Network Connectivity section of [MULPI3.0].

The sequence of messages exchanged in DHCPv6 is provided in the Establish IPv6 Network Connectivity section of [MULPI3.0].

8.3.7 Post-conditions

Not applicable for this Scenario.

8.3.8 Exceptions

Not applicable for this Scenario.

8.3.9 Rollback Actions

Not applicable for this Scenario.

9 PROVISIONING JOINED MULTICAST SERVICES SCENARIOS

This section defines Scenarios for provisioning joined Multicast services.

9.1 Configuration of Multicast QoS

9.1.1 Business Scenario

MSOs have indicated that IP Multicast may be an increasingly important segment of the overall IP traffic to the subscriber. Applications and services like IPTV are often used as examples of applications that may require Quality of Service treatment across the DOCSIS 3.0 network. As a result of this, DOCSIS 3.0 has introduced a robust framework for configuring how IP multicast groups can be configured for QoS handling.

9.1.2 Scenario Details

There are several Scenarios and applications that can be used to illustrate the flexibility of this QoS framework. For illustration purposes, an IPTV application that uses IP multicast to transport a broadcast type channel is one where the subscriber has little interactivity (no ability to start and stop the stream). This multicast session would be transported by a Group Service Flow (GSF). A second scenario involves the digital music channels that some MSOs provide. These multicast sessions would be aggregated together into a single GSF.

9.1.3 Assumptions

An MSO who wishes to limit the total amount of unclassified IP multicast traffic on a given Downstream channel or Downstream Bonding group will use the Default Group Service Flow setup described below to configure these limits.

An MSO who wishes to provide specific QoS treatment for a single or a range of IP multicast groups based on Source Address (S), Group Address (G), or Diff Serve Code Points (DSCP)/TOS markings will use the objects detailed in this Scenario to configure these QoS attributes.

9.1.4 Pre-conditions

A DOCSIS 3.0 CMTS is required. An MSO has prior knowledge of which IP Multicast Groups they wish to manage QoS for.

9.1.5 Management Objects

The Mulitcast QoS Object Model (OM) is shown in Annex M of [OSSI3.0].

The Multicast QoS feature does not need to be specifically enabled, but it does need some basic configuration in order to be used effectively.

In order to create a default Multicast QoS configuration, a default Group Profile is built. This profile allows the MSOs to configure a Group Service Flow configuration for all non-matched Multicast traffic. This Default configuration restricts all non-matched IP multicast to a specific QoS profile (as defined in the Service Class Name object from the QoS MIB) effectively providing a specific set of QoS characteristics for all such traffic.

To accomplish this, an object is created first in the QoS MIB to create a Service Class. Next, an object is created in the DefGrpSvcClass that references the created Service Class Name object.

For configuring the QoS attributes for a specific IP Multicast group or range of groups, the process is similar. First the Group Service Flow parameters are created by instantiating an object for Service Class in the ServiceClass object in the QoS MIB. Next, an object is instantiated in the GrpQosCfg Object, which references an established ServiceClass Object and adds additional attributes, such as the type of QoS Control (Single Session or Aggregate Session). The ‘number of sessions’ attribute is applicable only when QoSCtrl is set to Aggregate Session and the ‘AppId’ attribute is a tie in to PCMM (and is not discussed in this Use Case).

At this point, a decision needs to be made by the Operator about the configuration of encryption and PHS rules for a given IP Multicast group. If either of these features are required for a specific session or range of sessions, then objects in the CmtsGrpEncryptCfg and CmtsGrpPhsCfg objects need to be instantiated. If none of these features need to be configured, the next step is to create an object in the CmtsGrpCfg object. This object is where the linkage between a single IP multicast or a range of multicast sessions and the QoS, Encryption, and PHS attributes are configured. An instantiated object here will reference the instantiated objects in the GrpQosCfg, CmtsGrpEncryptCfg, and CmtsGrpPhsCfg objects. IP Multicast sessions can be configured based on Group, Server serving the group, and DSCP/ToS markings in the IP Multicast session.

9.1.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

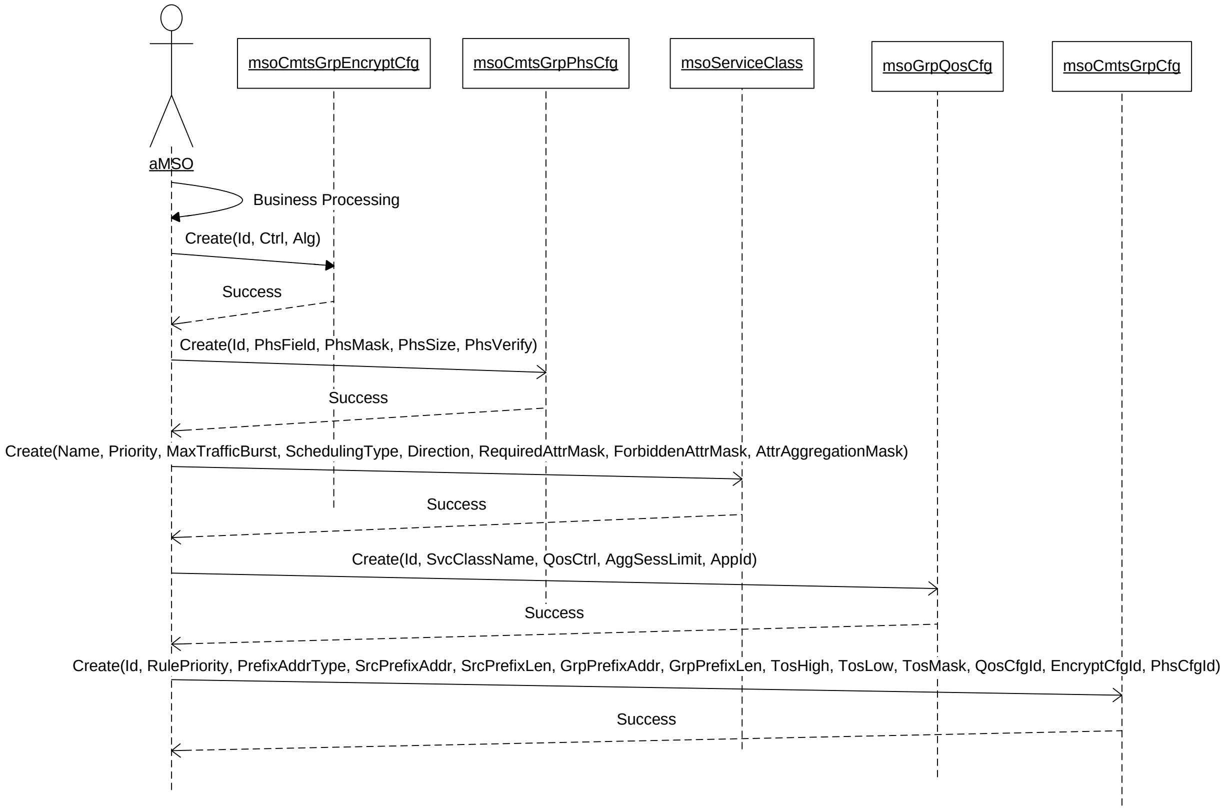

msoCmtsGrpEncryptCfg
msoCmtsGrpPhsCfg
msoServiceClass
msoGrpQosCfg
msoCmtsGrpCfg
aMSO
Business Processing
Create(Id, Ctrl, Alg)
Success
Create(Id, PhsField, PhsMask, PhsSize, PhsVerify)
Success
Create(Name, Priority, MaxTrafficBurst, SchedulingType, Direction, RequiredAttrMask, ForbiddenAttrMask, AttrAggregationMask)
Success
Create(Id, SvcClassName, QosCtrl, AggSessLimit, AppId)
Success
Create(Id, RulePriority, PrefixAddrType, SrcPrefixAddr, SrcPrefixLen, GrpPrefixAddr, GrpPrefixLen, TosHigh, TosLow, TosMask, QosCfgId, EncryptCfgId, PhsCfgId)
Success

Figure 12 – Sequence Diagram for Configuration of Multicast QoS

9.1.7 Post-conditions

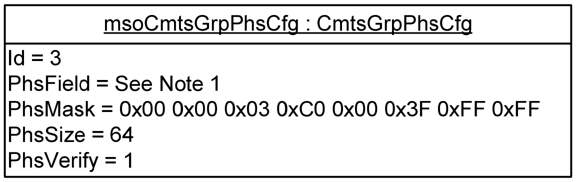
When configuration is successful, a default Group Service Flow is established in each MAC Domain for any un-matched IP Multicast traffic. For all "matched" IP Multicast traffic, a Group Classier Rule (GCR) and a Group Service Flow is created at the CMTS for the MAC Domain(s) for which a specific session or range of sessions are being forwarded (refer to "QoS Support for Joined IP Multicast Traffic" Section in [MULPI3.0]). The GSFs can be monitored by reading objects in the CmtsReplSession object from the Multicast Status Reporting object model as defined in [OSSI3.0].

The following diagram highlights the desired state for the CmtsGrpEncryptCfg object at the end of this scenario.

msoCmtsGrpEncryptCfg : CmtsGrpEncryptCfg

Id = 7
Ctrl = cmts(1)
Alg = des56CbcMode(1)

The following diagram highlights the desired state for the CmtsGrpPhsCfg object at the end of this scenario.



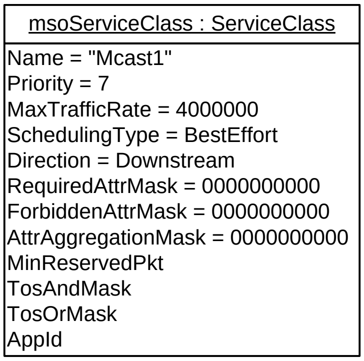
msoCmtsGrpPhsCfg : CmtsGrpPhsCfg

Id = 3
PhsField = See Note 1
PhsMask = 0x00 0x00 0x03 0xC0 0x00 0x3F 0xFF 0xFF
PhsSize = 64
PhsVerify = 1

Note 1: In Multicast QoS configuration for PHS, only the Source and Destination IP address are able to be suppressed. In these cases, the attribute PhsField takes on a value similar to the following value for an IPv4 Source and Destination IP address:

0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x000x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x03 0xE8 0x05 0xDC 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0xFF 0xFF

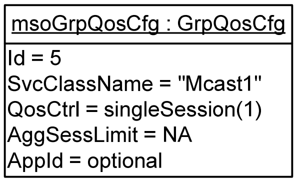
The following diagram highlights the desired state for the ServiceClass object at the end of this scenario.



msoServiceClass : ServiceClass

Name = "Mcast1"
Priority = 7
MaxTrafficRate = 4000000
SchedulingType = BestEffort
Direction = Downstream
RequiredAttrMask = 0000000000
ForbiddenAttrMask = 0000000000
AttrAggregationMask = 0000000000
MinReservedPkt
TosAndMask
TosOrMask
AppId

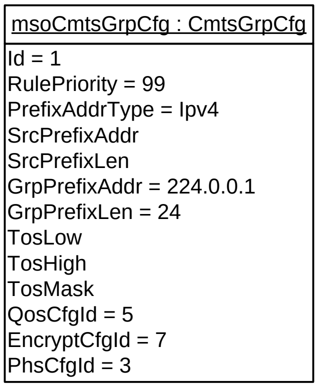
The following diagram highlights the desired state for the GrpQosCfg object at the end of this scenario.



msoGrpQosCfg : GrpQosCfg

Id = 5
SvcClassName = "Mcast1"
QosCtrl = singleSession(1)
AggSessLimit = NA
AppId = optional

The following diagram highlights the desired state for the CmtsGrpCfg object at the end of this scenario.



msoCmtsGrpCfg : CmtsGrpCfg

Id = 1
RulePriority = 99
PrefixAddrType = Ipv4
SrcPrefixAddr
SrcPrefixLen
GrpPrefixAddr = 224.0.0.1
GrpPrefixLen = 24
TosLow
TosHigh
TosMask
QosCfgId = 5
EncryptCfgId = 7
PhsCfgId = 3

Any attribute (in the above object instances) that is left unassigned is assumed to take the default value as specified in the object model of [OSSI3.0]. Default values are not required to be specified/provided during object instantiation.

9.1.8 Exceptions

This scenario defines the set of steps that are needed to create a functional QoS framework for IP Multicast sessions. These steps need to be completed in order or misconfigurations can occur. Some possibilities for these misconfigurations are:

- The removal of an SCN when that SCN is referenced by a GrpQosCfg object.
- The removal of a GrpQosCfg object when that object is referenced by a CmtsGrpCfg will leave the currently established Group Service Flow (GSF) in an undetermined state. Additionally, care should be taken when modifying the SCN parameters that are references by established GSFs as these changes are reflected in future and existing GSFs.
- Overlapping rule priorities in the CmtsGrpCfg object can lead to issues in the establishment of GSFs and Group Classifier Rules (GCR).
- Care must be taken to avoid encryption rules that call for AES encryption when clients behind non-DOCSIS 3.0 modems have the possibility of joining those configured groups.

9.1.9 Rollback Actions

To rollback a CmstGrpCfg object instance the MSO needs to only remove that object. In the case where the CmstGrpCfg object to be removed references a range of multicast sessions, the MSO can either remove the entire object or define a new object(s) with a different and higher priority than the currently instantiated object.

To roll back an object instance of GrpQosCfg, the MSO must ensure that any CmstGrpCfg objects that reference the GrpQosCfg object have been properly modified to point to a new GrpQosCfg object. Changes to an instance of existing GrpQosCfg objects are permitted, however, these changes will update not only future objects but currently instantiated objects so care must be taken when performing this action. This is also true of objects in the Service Class objects; changes here not only affect future object instances, but current instances as well.

9.2 Configuration of Multicast Authorization

9.2.1 Business Scenario

As MSOs look to deploy new services to customers, increasingly IP Multicast transport looks to provide an efficient mechanism to transport these services to multiple subscribers at the same time. In DOCSIS 3.0 a new feature called Multicast Authorization has been defined to provide a means to authorize groups of subscribers to receive traffic from various IP Multicast Groups. This feature controls only the joining of downstream IP multicast sessions; it does not control the ability of any client to transmit IP multicast traffic upstream.

9.2.2 Scenario Details

Multicast Authorization is a feature that is analogous to Access Control Lists for IP Multicast traffic. This feature is configured at the CMTS through several objects defined in the Multicast Authorization Object Model. Optionally, the DOCSIS 3.0 Specifications permit the CMTS Multicast Authorization profiles to be configured via entries in the CM config file at registration. The CMTS enforces IP Multicast join authorization by signaling or not signaling Multicast DSIDs and/or per-session Security Associations.

An MSO may choose to configure Multicast Authorization for a number of different reasons. One reason might be similar to tiers of service now for video products. A similar tiering mechanism could be configured in support of an IPTV application where a number of broadcast channels are delivered to devices in the home and only certain subsets of those channels are available to customers who have paid for that access. Thus, a basic tier of service might include a small number of IP Multicast groups and the sports tier might include only channels that are sports related. In any case, the MSO must have knowledge of the groups that are desired to be protected in this manner prior to configuring the feature.

This feature is often confused with Multicast Authorization from Pre-3.0 DOCSIS specifications, which included encryption. This feature is not related with configuring Multicast Encryption. See the Multicast QoS Scenario for information on configuring IP Multicast encryption.

Refer to the "IP Multicast Join Authorization" section of [[MULPI3.0] for additional details.

9.2.3 Assumptions

The MSO has prior knowledge of IP Multicast Groups for which they wish to manage Authorization.

9.2.4 Pre-conditions

This feature is DOCSIS version agnostic. That is, the feature can be enabled and will manage the Authorization to any downstream IP Multicast group. There are hooks into the provisioning environment to allow the Operator to signal the Multicast Authorization Profile Name or names in the CM configuration file at registration. The profile name or the static session rules need to be in the CM's config file for Authorization to work.

9.2.5 Management Objects

The components of the Multicast Authorization model are defined in Annex M of [OSSI3.0].

In order to use and configure this feature, the CMTS must be configured to enable the feature. This is accomplished by setting the scalar object enable to enable Multicast Authorization. Additionally, the MSO must configure the default Profile Name Rule Set, the Default Action (Permit or Deny), and the default number of sessions allowed to be replicated through any given CM.

Session Profiles (ProfileSessRule objects*)* are configured much like QoS classifiers. To create the Session Rules objects that are part of a profile, the Operator first configures objects in the Profile object. This object provides a mapping between a Profile Name and the Description of that profile. To create the Multicast rule, the Operator instantiates an object in the ProfileSessRule object. The attributes here include the Name, and ID, a rule priority, a set of classification parameters and an action (Permit or Deny). Multiple rules can be created for the same Profile Name.

Optionally, the CMTS can support the building of Static Multicast Authorization Session rules. These rules are communicated through the CM config file at registration in TLV-43 entries (thus allowing the Operator to configure these Session Rules for any version of DOCSIS). These rules are parsed by the CMTS and objects in the StaticSessRule object are created.

9.2.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

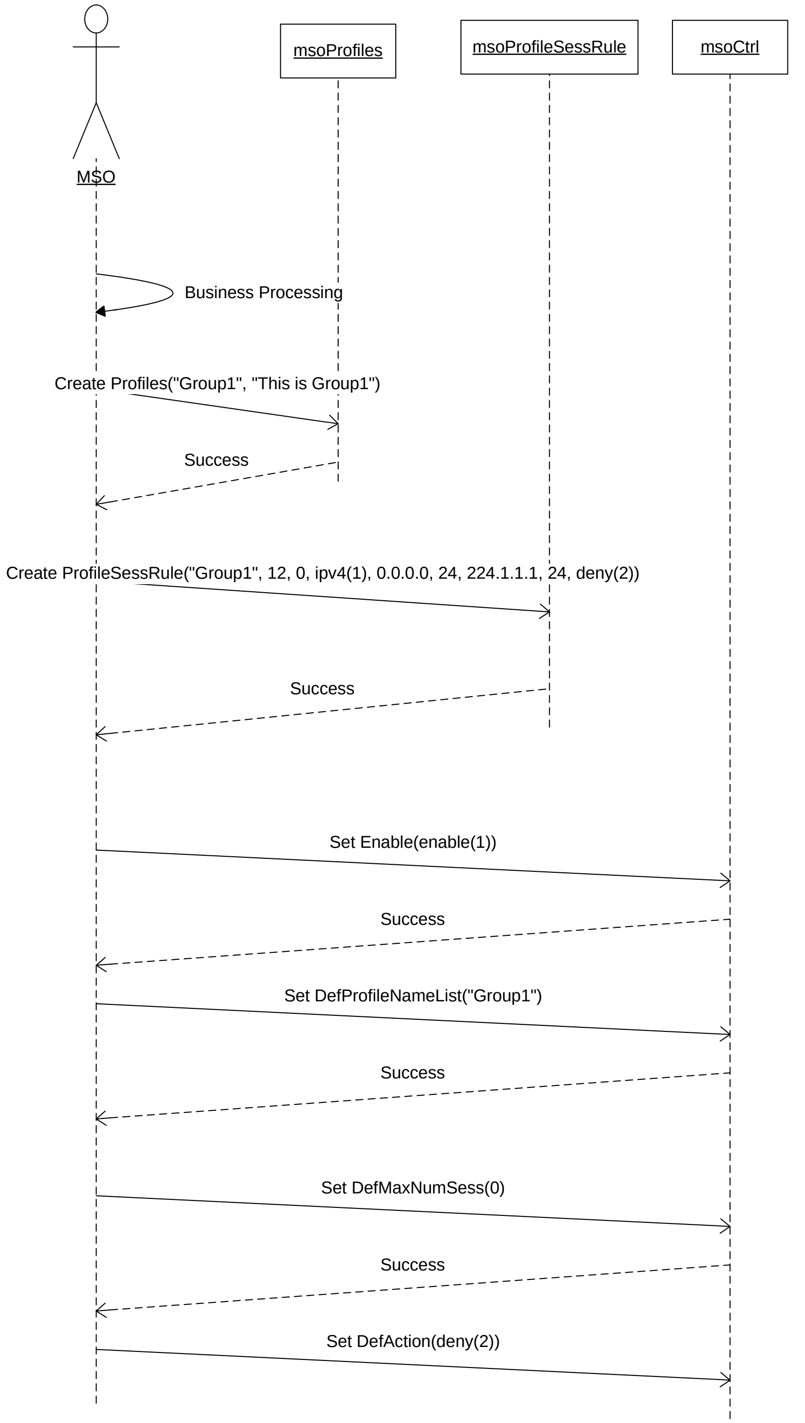

MSO
msoProfiles
msoProfileSessRule
msoCtrl
Business Processing
Create Profiles("Group1", "This is Group1")
Success
Create ProfileSessRule("Group1", 12, 0, ipv4(1), 0.0.0.0, 24, 224.1.1.1, 24, deny(2))
Success
Set Enable(enable(1))
Success
Set DefProfileNameList("Group1")
Success
Set DefMaxNumSess(0)
Success
Set DefAction(deny(2))

Figure 13 – Sequence Diagram for Configuration of Multicast Authorization

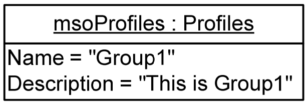
9.2.7 Post-conditions

Once Multicast Authorization is configured, the CMTS will evaluate each Multicast JOIN against the set of rules that have been configured for the Profiles associated with the CM. If a match is found in the Rules, the CMTS takes the appropriate Action and allows or denies the JOIN. In the case that the CMTS has an Action for DENY, the CMTS will not create or communicate a DSID value to a DOCSIS 3.0 CM. For Pre 3.0-DOCSIS CMs, no group will be forwarded to the CM. In these cases, and due to the IGMP protocol, the CM and CPE will continue to send JOIN requests for the multicast group over and over. Each one of these requests will be re-evaluated by the CMTS until the client either gives up or the CMTS Action is changed. Multicast Join Authorization is normally done in the CMTS prior to performing checks for Multicast QoS treatment of a specific multicast group.

For Pre 3.0-DOCSIS CMs, encryption and Baseline Privacy + must be enabled in order for a group not to be forwarded to clients that are not Authorized for a specific group. Here, control of the multicast group is maintained by use of the TEK material. If the CM is authorized for the IP multicast group, the CM will receive TEK materials via the SA MAP message. If the CM is not authorized, the CM will get an SA MAP Reject message and will not be able to decrypt the IP Multicast session.

A secondary component of this feature is the limiting of the total number of multicast sessions that can be forwarded by a specific CM or to a specific host. The value is configured using the scalar object DefNumSess. Once this value has been exceeded, the CM and/or CPE device will not be able to receive any additional IP multicast sessions until such time as the value is not exceeded.

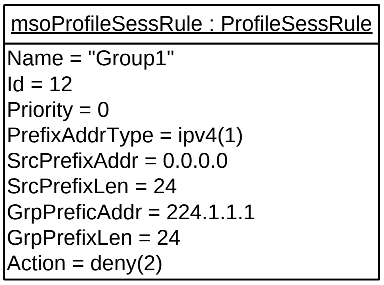
The following diagram highlights the desired state for the Profiles object at the end of this scenario.



msoProfiles : Profiles

Name = "Group1"
Description = "This is Group1"

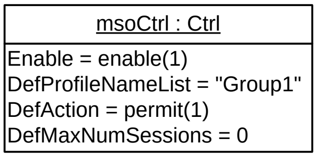
The following diagram highlights the desired state for the ProfileSessRule object at the end of this scenario.



msoProfileSessRule : ProfileSessRule

Name = "Group1"
Id = 12
Priority = 0
PrefixAddrType = ipv4(1)
SrcPrefixAddr = 0.0.0.0
SrcPrefixLen = 24
GrpPreficAddr = 224.1.1.1
GrpPrefixLen = 24
Action = deny(2)

The following diagram highlights the desired state for the Ctrl object at the end of this scenario.



msoCtrl : Ctrl

Enable = enable(1)
DefProfileNameList = "Group1"
DefAction = permit(1)
DefMaxNumSessions = 0

9.2.8 Exceptions

As with any access control list or rule-based system, there are always possible cases where overlapping rules can be created in profiles where behavior may become unpredictable. The Multicast Authorization feature also allows for the assignment of multiple profiles to a specific CM/CPE. As a result of this, it is possible that clients that should be authorized for an IP Multicast group in one profile may have that group denied in another, forcing the Operator to review all the profiles assigned to that device to determine where the misconfiguration might have occurred.

This feature does not include any exclusion lists. Any CM or CPE device can be configured for specific profiles.

CMs and CPE devices that have JOINs that are unauthorized will be recorded in the CMTS event log as NOTICE level events with the ID 89010200. There are currently no events defined for CMs/CPE devices that have exceeded the DefNumSess value.

9.2.9 Rollback Actions

There are several rollback actions associated with this use Case. Each of these cases is outlined below.

9.2.9.1 Deactivation of Multicast JOIN Authorization

In this case, the Multicast JOIN Authorization feature has been enabled and the MSO wishes to disable the feature. In this case a SNMP Set on the scalar object *enable* to disable. When this set is performed, all configuration for the feature is left intact, and subsequent CM registrations with Multicast Join Authorization TLVs will be allowed, but no enforcement of the JOINs from the CM or CPE devices behind the CM will be evaluated.

9.2.9.2 Removal or Update of ProfileName and Rule Sets

In this scenario, a specific a ProfileName or RuleSet is deleted or modified (rules added or subtracted or ProfileName instance is removed) which is associated with a single or group of CMs. In the case where a new ProfileName object is instantiated, the configuration of the CMTS is the only thing updated. There is no mechanism in the DOCSIS 3.0 specification that will allow an already registered CM to be associated with a new ProfileName object. If Rules associated with a specific ProfileName instance are updated, any JOIN from a CM that is associated with that object instance will be evaluated with the most up to date version of the Rules associated with that ProfileName object. Thus if a specific RuleSet is modified in any way, the CMs associated with that ProfileName will be evaluated with the most current set of Rules associated with that ProfileName.

ProfileName objects can also be instantiated at CM registration when the CM registers with an unknown ProfileName in the REG-REQ-(MP), the CMTS will create this new instance on the CMTS with an essentially empty RuleSet.

10 SECURITY SCENARIOS

This section defines Scenarios for provisioning DOCSIS 3.0 security features.

10.1 Configuration of Non-default Encryption Algorithm

10.1.1 Business Scenario

Current deployments are configured to support Digital Encryption Standard (DES) 56 encryption for the data traffic. In some high security applications, Government agencies are requesting MSOs to support stronger encryption techniques, specifically AES as defined in [FIPS-197]. As such, MSOs requested the addition of this encryption technique for DOCSIS 3.0 CMs.

This scenario discusses how the model in [OSSI3.0] enables the Operator to configure the encryption scheme and the associated parameters.

10.1.2 Scenario Details

This scenario configures the single prioritized list of encryption algorithms the CMTS uses when selecting the primary SAID encryption algorithm a CM supports (as indicated in the CM Auth Request message for EAE or BPI+). In this specific scenario, the MSO configures the encryption algorithm priority list for 128-bit AES followed by 56-bit DES algorithm priority (removing the 40-bit DES algorithm). Note that the default priority for this list is 128-bit AES, followed by 56-bit DES, and then 40-bit DES algorithm priority, with the strongest algorithm priority listed first (leftmost) and the weakest algorithm priority listed last (rightmost). Therefore, if a CM only supports 40-bit DES encryption, it will not be allowed to register on the 3.0 CMTS. The CM is not allowed to choose which priority to use; it is required to use the strongest supported by both the CMTS and CM.

In a 2.0+ hybrid CM, the CM may or may not support AES along with also supporting other 3.0 security features, such as EAE. AES and EAE are independent features. In the case where a CM supports AES but not EAE, the provisioning would follow the BPI+ method using AES encryption. In the case where a CM supports EAE but not AES, the provisioning would follow the EAE method using 56-bit DES encryption. Finally, if the hybrid CM does not support AES or EAE, the provisioning would follow the BPI+ method using 56-bit DES encryption.

10.1.3 Assumptions

There are no authorized CMs registered on the network, which only supports 40-bit DES encryption. The CMTS will support both 128-bit AES and 56-bit DES encryption algorithms from CMs in a mixed network (e.g., DOCSIS 3.0 CMs plus pre-3.0 DOCSIS CMs). AES-128 bit encryption can only be supported between a 3.0 CMTS and 3.0 CM.

10.1.4 Pre-conditions

The CMTS must support the DOCSIS 3.0 security feature to encrypt and decrypt data using the AES algorithm. The CMs may be either 3.0 (AES) or 2.0 (DES). Hybrid 2.0 CMs can also be supported (e.g., a CM that supports AES but not EAE, a CM that does not support AES but supports EAE, or a CM that does not support AES or EAE).

10.1.5 Management Objects

Refer to the CmtsEncrypt object defined in the Security Object Model Diagram Figure from Annex L of [OSSI3.0]. This object and its associated attribute are described in the CmtsEncrypt Object section from [OSSI3.0].

10.1.6 Scenario Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

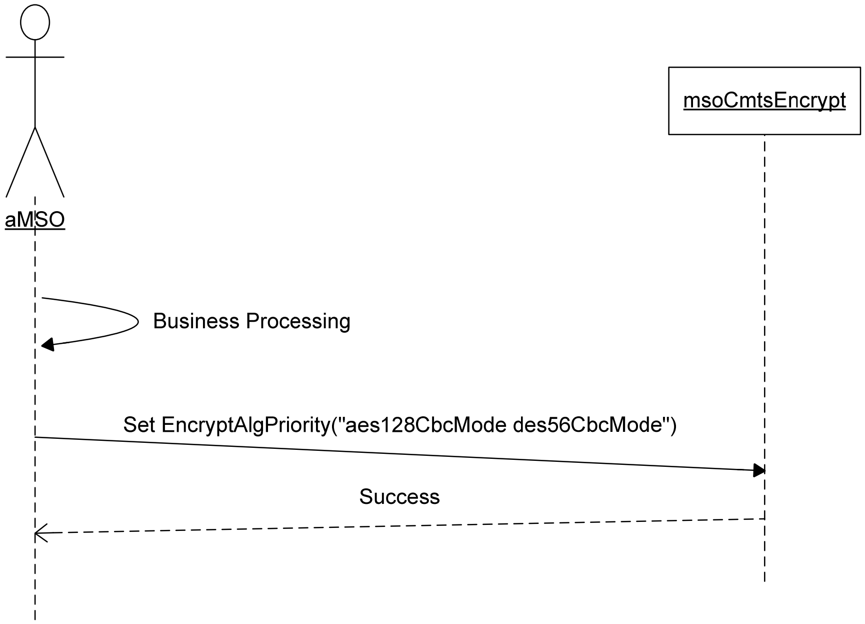


Figure 14 – Sequence Diagram for Configuration of Non-default Encryption Algorithm

10.1.7 Post-conditions

The following diagram highlights the desired state for the CmtsEncrypt object at the end of this scenario.

msoCmtsEncrypt : CmtsEncrypt
EncryptAlgPriority = "aes128CbcMode des56CbcMode"

10.1.8 Exceptions

Exception cases include malformed strings and unsupported algorithms. The sequence diagram below shows two configuration attempts. The first configuration attempts to configure AES on a CMTS that does not support this feature. The second configuration attempts to configure 56-bit DES on the CMTS; however there was an Operator error (incorrect value) in the configuration parameters.

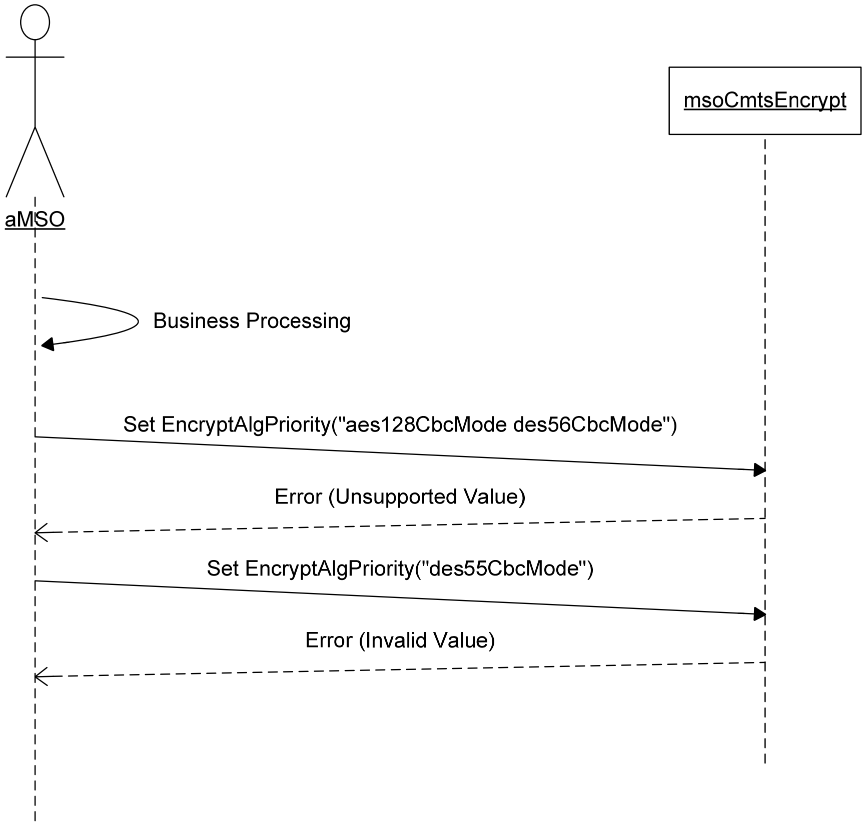

aMSO
msoCmtsEncrypt
Business Processing
Set EncryptAlgPriority("aes128CbcMode des56CbcMode")
Error (Unsupported Value)
Set EncryptAlgPriority("des55CbcMode")
Error (Invalid Value)

Figure 15 – Exception Cases for Malformed Strings and Unsupported Algorithms

10.1.9 Rollback Actions

This is not a multi-step process, so no rollback actions are necessary.

10.2 Configuration of Early Authentication and Encryption (EAE)

EAE is a DOCSIS 3.0 security feature designed to provide earlier encryption of the CM registration process.

The following EAE policies are configurable:

- Policy 1: No EAE enforcement
- Policy 2: Ranging-based EAE enforcement (a selective enforcement)
- Policy 3: Capability-based EAE enforcement (a selective enforcement)
- Policy 4: Total EAE enforcement

The following scenario will focus on configuring the CMTS for Policy 2.

10.2.1 Business Scenario

An MSO would like to enhance their provisioning security by turning on EAE to secure the CM initialization process on a modem-by-modem basis. With the DOCSIS 3.0 EAE feature enabled, only authenticated CMs are allowed to continue with their initialization process with subsequent network admission.

10.2.2 Scenario Details

This scenario configures the CMTS to enable EAE such that the CMTS uses EAE to perform network admission control by forcing CMs to authenticate before allowing them to proceed with initialization. As a result of EAE, subsequent provisioning messages are encrypted.

The following EAE policies are available:

- Policy 1: No EAE enforcement
- Policy 2: Ranging-based EAE enforcement (a selective enforcement)
- Policy 3: Capability-based EAE enforcement (a selective enforcement)
- Policy 4: Total EAE enforcement

This scenario will configure Policy 2 on the CMTS, which enforces EAE on a CM based on the CM's ranging MAC message type while it ignores the EAE capability flag in the B-INIT-RNG-REQ. Therefore, EAE is enforced on CMs, which range with B-INIT-RNG-REQ irrespective of whether the EAE capability flag is set.

If a CM is configured into the EAE Exclusion list, EAE will not be enforced on that CM. This scenario will add one CM, with MAC Address 0A:0B:0C:0D:0E:0F, to the EAE Exclusion list for diagnostic purposes (e.g., the MSO would like to disable EAE for this CM to troubleshoot problems).

10.2.3 Assumptions

This scenario assumes the MSO network does not contain any DOCSIS 2.0 hybrid CMs that support channel bonding but do not support EAE.

10.2.4 Pre-conditions

The CMTS must support the DOCSIS 3.0 EAE security feature. A DOCSIS 3.0 CM is required to support EAE. DOCSIS 1.x/2.0 CMs will be allowed to range and register because these devices do not send the B-INIT-RNG-REQ message. DOCSIS 2.0 CMs register with RNG-REQ and are authenticated after registration using BPI+.

10.2.5 Management Objects

- CMTS EAE Enforcement configuration object

Refer to the MdCfg object defined in the CMTS Bonding Object Model Diagram Figure from Annex O of [OSSI3.0]. This object and its associated attributes are described in the MdCfg Object section from [OSSI3.0].

10.2.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

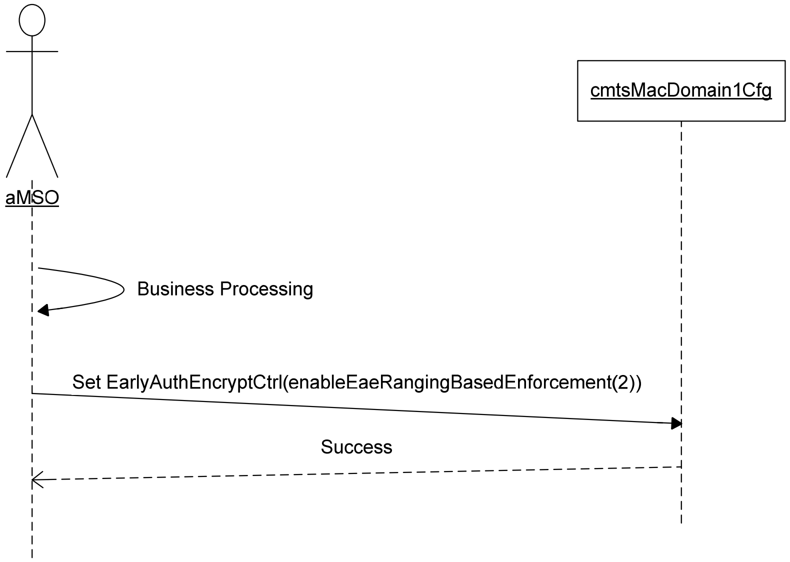
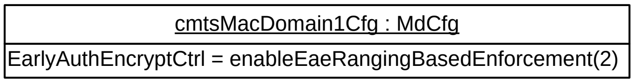

aMSO
cmtsMacDomain1Cfg
Business Processing
Set EarlyAuthEncryptCtrl(enableEaeRangingBasedEnforcement(2))
Success

Figure 16 – Sequence Diagram for Configuration of Early Authentication and Encryption (EAE)

10.2.7 Post-conditions

The following diagram highlights the desired state for the MdCfg object at the end of this scenario.


cmtsMacDomain1Cfg : MdCfg
EarlyAuthEncryptCtrl = enableEaeRangingBasedEnforcement(2)

10.2.8 Exceptions

Some exception cases might include:

- Configuring an invalid value for the EarlyAuthEncryptCtrl attribute of the MdCfg object.

10.2.9 Rollback Actions

The MdCfg is a single configuration setting and does not have a rollback requirement.

10.3 CM Registration Diagnostics using EAE Exclusion Lists

10.3.1 Business Scenario

The MSO would also like the ability to disable a CM from performing EAE in order to troubleshoot CM registration or provisioning issues. To troubleshoot the problem, an Operator may need to examine the DHCP, TFTP, and/or ToD message exchanges. Since EAE encrypts these messages, it must be disabled to analyze the provisioning messages.

The Operator has two options to investigate based on the diagnostic results:

- EAE problem
- Invalid data within provisioning messages

10.3.2 Scenario Details

If a CM is configured into the EAE Exclusion list, EAE will not be enforced on that CM. This scenario will add the target CM, with MAC Address 0A:0B:0C:0D:0E:0F, to the EAE Exclusion list for diagnostic purposes (e.g., the MSO would like to disable EAE for this CM to troubleshoot problems). A CM that maps to the exclusion rule will not perform EAE.

10.3.3 Assumptions

This scenario assumes the MSO network does not contain any DOCSIS 2.0 hybrid CMs that support channel bonding but do not support EAE.

The DOCSIS 3.0 CMTS allows EAE exclusion policy on an individual CM or group of CMs.

10.3.4 Pre-conditions

The CMTS must support the DOCSIS 3.0 EAE security feature. A DOCSIS 3.0 CM is required to support EAE. DOCSIS 1.x/2.0 CMs will be allowed to range and register because these devices do not send the B-INIT-RNG-REQ message. EAE must be enabled on the CMTS for the MAC Domain where the CM is to reside.

10.3.5 Management Objects

- CMTS CM EAE Exclusion configuration object

Refer to the CmtsCmEaeExclusion object defined in the Security Object Model Diagram Figure from Annex L of [OSSI3.0]. This object and its associated attribute are described in the CmtsCmEaeExclusion Object section from [OSSI3.0].

10.3.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

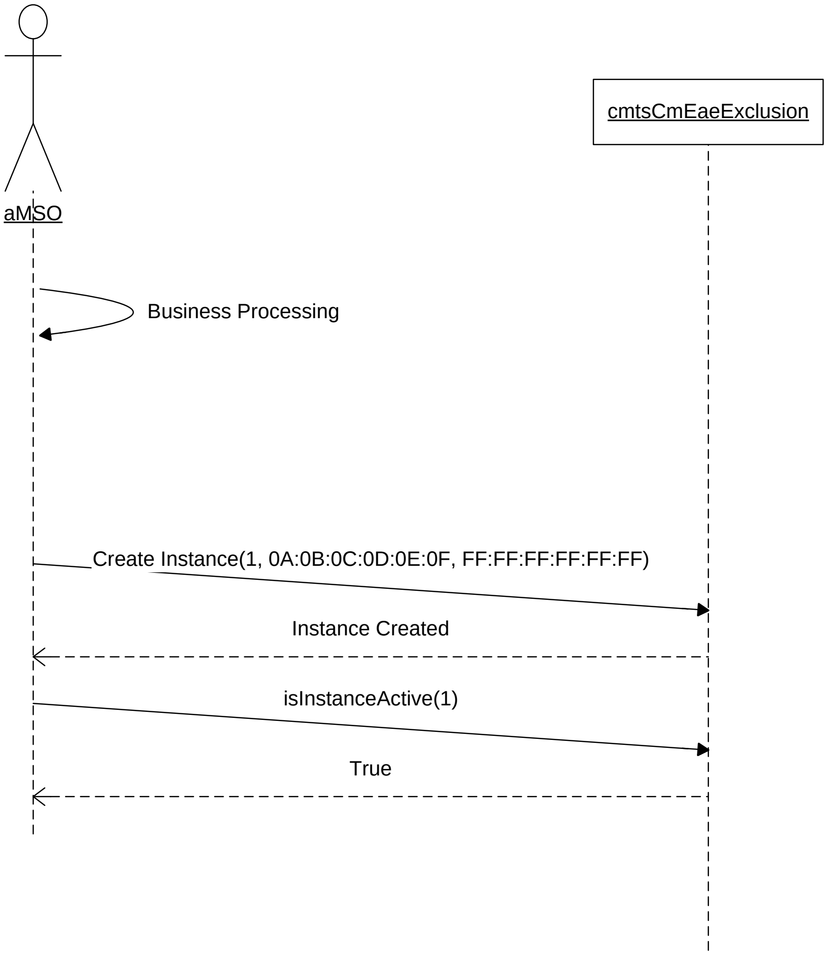
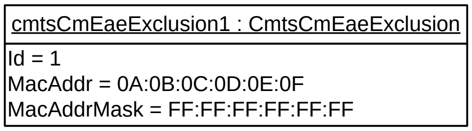


Figure 17 – Sequence Diagram for CMTS EAE Exclusion Configuration Objects

10.3.7 Post-conditions

The following diagram highlights the desired state for the CmtsCmEaeExclusion object at the end of this scenario.



cmtsCmEaeExclusion1 : CmtsCmEaeExclusion

Id = 1
MacAddr = 0A:0B:0C:0D:0E:0F
MacAddrMask = FF:FF:FF:FF:FF:FF

10.3.8 Exceptions

Some exception cases might include:

- Creating a duplicate CM EAE exclusion rule.
- Deleting a CM EAE exclusion rule that does not exist.
- Configuring an invalid value for the MacAddr or MacAddrMask attribute of the CmtsCmEaeExclusion object.

10.3.9 Rollback Actions

The CmtsCmEaeExclusion object supports creation and deletion of multiple instances. If a partial instance is created, the device may mark this instance as 'notReady'. Once the full instance is created, the device or Operator may update the instance to 'active,' such that the instance is in service.

10.4 Certificate Revocation using CRL Server

10.4.1 Business Scenario

An MSO has determined that a sub-level distributed Certificate Authority (CA) certificate has become invalid (e.g., Company XYZ is no longer in business and their distributed CA certificate may be compromised). The MSO would like to revoke the certificate at the CA level using the DOCSIS 3.0 Certificate Revocation Lists (CRLs) feature. This process will revoke all device-level certificates under the CA certificate being revoked.

10.4.2 Scenario Details

This scenario configures the CMTS to revoke an invalid distributed CA certificate using Certificate Revocation Lists (CRLs). A CRL is a list of certificate serial numbers revoked by a CA. This scenario also generalizes the configuration of a CRL server. Refer to the Certificate Revocation List Format section of [SEC3.0] for details on the CRL file format. The following configuration steps are performed:

- Configure the CRL server to provide the proper CRL file (e.g., crlFile.txt). In this scenario, the CRL file does not contain the tbsCertList.nextUpdate attribute.
- Configure the global certificate revocation method object on the CMTS to enable CRL.
- Configure the CRL list on the CMTS, including the CRL server Uniform Resource Locator (URL) (e.g., http://crl.mso.com) and CRL file refresh interval (e.g., 1000 minutes).

10.4.3 Assumptions

This scenario assumes the MSO network contains at least one CM from vendor XYZ, which contains a certificate to be revoked. The CMTS may only retrieve the CRL file from the CRL Server based on the configured CRL file refresh interval if the tbsCertList.nextUpdate attribute is missing from the CRL file. If the CRL file contains the tbsCertList.nextUpdate value, the CMTS refreshes the CRL after the specified time has passed.

10.4.4 Pre-conditions

Both the CM and CMTS carry pre-dependencies, which must be satisfied in order for the CRL feature to be enabled and utilized to enforce certificates per an MSOs' security policy.

- CMTS: The CMTS must support the DOCSIS 3.0 CRL certificate revocation security feature. Steps must be undertaken by the MSO to configure and manage the CRL feature on the CMTS using the network management objects as defined in the object models of the [OSSI3.0] specification.

- CMs and MTAs: The presence of legacy CMs without a valid certificate precludes enabling the CRL feature. When enabled, CRL enforcement causes loss of service to all affected (non-compliant) CMs and MTAs. Legacy CMs, which have a malformed certificate embedded in their software and have been subsequently abandoned by their manufacturer, must be removed from the network in a multi-step program.

Refer to the "Cable Modem Replacement Process " section detailed in Appendix II of this technical report.

10.4.5 Management Objects

- CMTS global certification revocation configuration object

  Refer to the CertificateRevocationMethod object defined in the Certificate Revocation Object Model Diagram Figure from Annex L of [OSSI3.0]. This object and its associated attribute are described in the CertificateRevocationMethod Object section from [OSSI3.0].

- CMTS CRL configuration object

  Refer to the CmtsCertRevocationList object defined in the Certificate Revocation Object Model Diagram Figure from Annex L of [OSSI3.0]. This object and its associated attribute are described in the CmtsCertRevocationList Object section from [OSSI3.0].

10.4.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

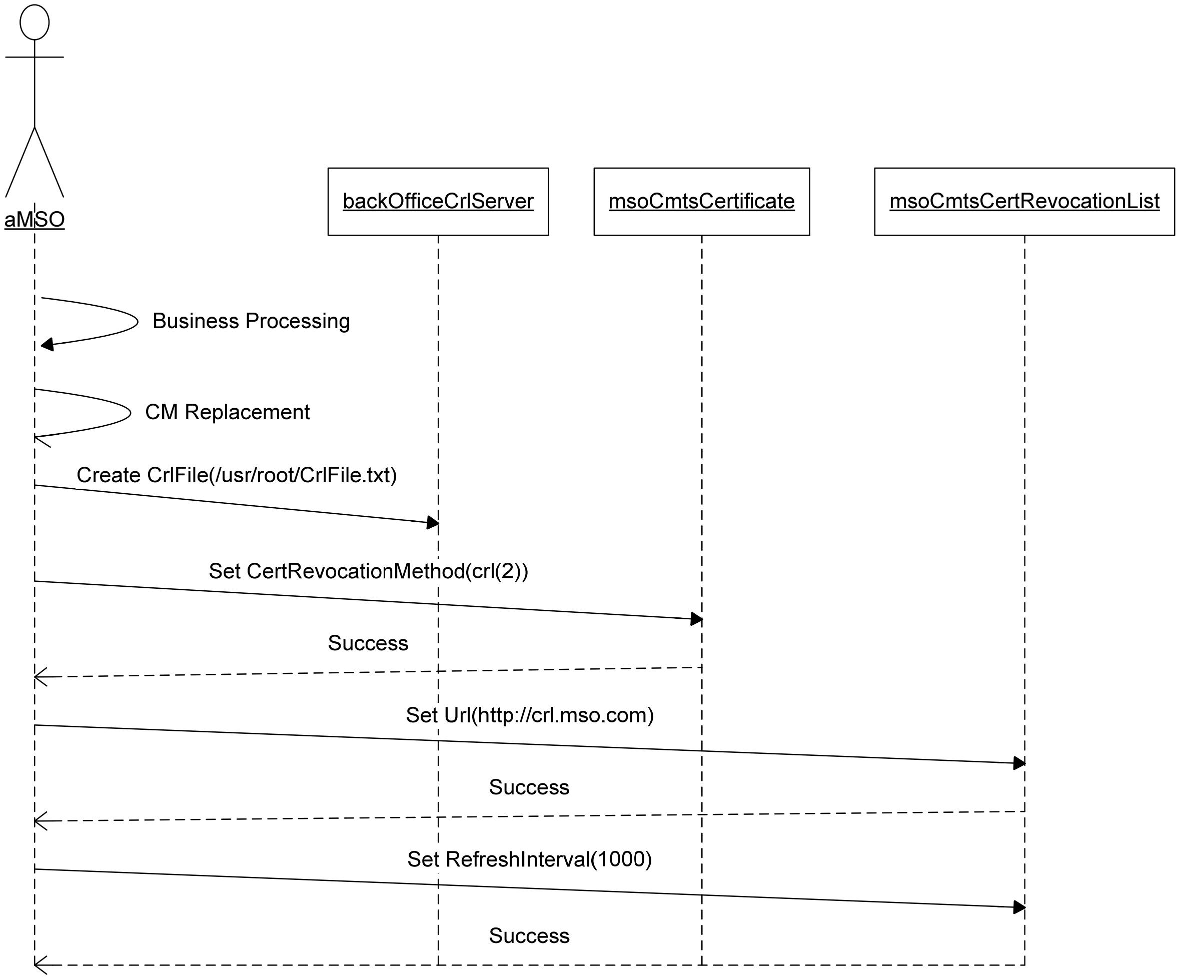

aMSO
backOfficeCrlServer
msoCmtsCertificate
msoCmtsCertRevocationList
Business Processing
CM Replacement
Create CrlFile(/usr/root/CrlFile.txt)
Set CertRevocationMethod(crl(2))
Success
Set Url(http://crl.mso.com)
Success
Set RefreshInterval(1000)
Success

Figure 18 – Sequence Diagram for Certificate Revocation using CMTS CRL Server

10.4.7 Post-conditions

The following diagram highlights the desired state for the CertificateRevocationMethod object at the end of this scenario.

msoCmtsCertificate : CmtsCertificate
CertRevocationMethod = crl(2)

The following diagram highlights the desired state for the CmtsCertRevocationList object at the end of this scenario.

msoCmtsCertRevocationList : CmtsCertRevocationList

Url = http://crl.mso.com
RefreshInterval = 1000

10.4.8 Exceptions

Some exception cases might include:

- Configuring an invalid value for the URL attribute of the CmtsCertRevocationList object.
- The CRL Server does not respond to the CMTS CRL query.
- CertificateRevocationMethod set incorrectly as ocsp(3) or none(1).

10.4.9 Rollback Actions

The CertificateRevocationMethod is a single configuration setting and does not have a rollback requirement. The CmtsCertRevocationList object provides default values for the URL (empty string) and refresh interval (10080 minutes). If one or the other attributes failed configuration, the default value is still in place. When the URL attribute is set to an empty string, the CTMS will not attempt to retrieve the CRL file from the server.

10.5 TFTP Configuration File Security

10.5.1 Business Scenario

An MSO would like to strengthen the security of the CM provisioning process to help prevent theft-of-service, including theft of different service levels than intended, and denial-of-service attacks. The DOCSIS 3.0 TFTP Proxy, Configuration File Name Authorization and Configuration File Learning security features are configured in the CMTS to provide this level of CM provisioning security and are configured independently.

10.5.2 Scenario Details

The TFTP Proxy feature will be provisioned in the CMTS to secure the CM provisioning process by abstracting the configuration file server address from the CM and other devices on the cable network. The abstraction reduces the likelihood of denial of service, or of unauthorized access to the TFTP server's configuration files. The CM is provisioned with the CMTS IP address in place of the configuration file server IP address and the CMTS proxies all TFTP messages between the CM and configuration file server.

The Configuration File Learning feature will be provisioned in the CMTS in order to secure the CM provisioning process by verifying the CM registers with the correct parameters that were set in the configuration file downloaded to the CM.

Finally, the Configuration File Name Authorization feature will be provisioned in the CMTS, via an authorized DHCP server list and Configuration File Learning, to secure the CM provisioning process by enforcing the CM to download the correct configuration file according to the DHCP configurations offered to the CM.

10.5.3 Assumptions

This scenario assumes that the configuration file download process uses TFTP and that the CMTS acts as a proxy for the TFTP server address [SEC3.0]. A single address does not limit the MSO to a singular TFTP server, rather round robin or virtual IP load balancing server farms which may present a different TFTP server address during IP acquisition depending on algorithm.

Configuring the authorized DHCP servers within the CMTS is vendor-specific, refer to vendor's configuration guide for more details (e.g., IPv6 Relay and/or Cable Helper).

10.5.4 Pre-conditions

The CMTS must support the DOCSIS 3.0 security features:

- TFTP Proxy
- Configuration File Name Authorization
- Configuration File Learning

There are no pre-conditions for the CM, DHCPv4/v6 server or configuration file server since this is a CMTS feature and is transparent to those entities.

10.5.5 Management Objects

- CMTS TFTP Proxy Enabled configuration object

Refer to the MdCfg object defined in the CMTS Bonding Object Model Diagram Figure from Annex O of the DOCSIS 3.0 OSSI Specification. This object and its associated attributes are described in the MdCfg Object section.

- CMTS Configuration File Server configuration object

Refer to the CmtsServerCfg object defined in the Security Object Model Diagram Figure from Annex L of the DOCSIS 3.0 OSSI Specification. This object and its associated attribute are described in the CmtsServerCfg Object section.

10.5.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

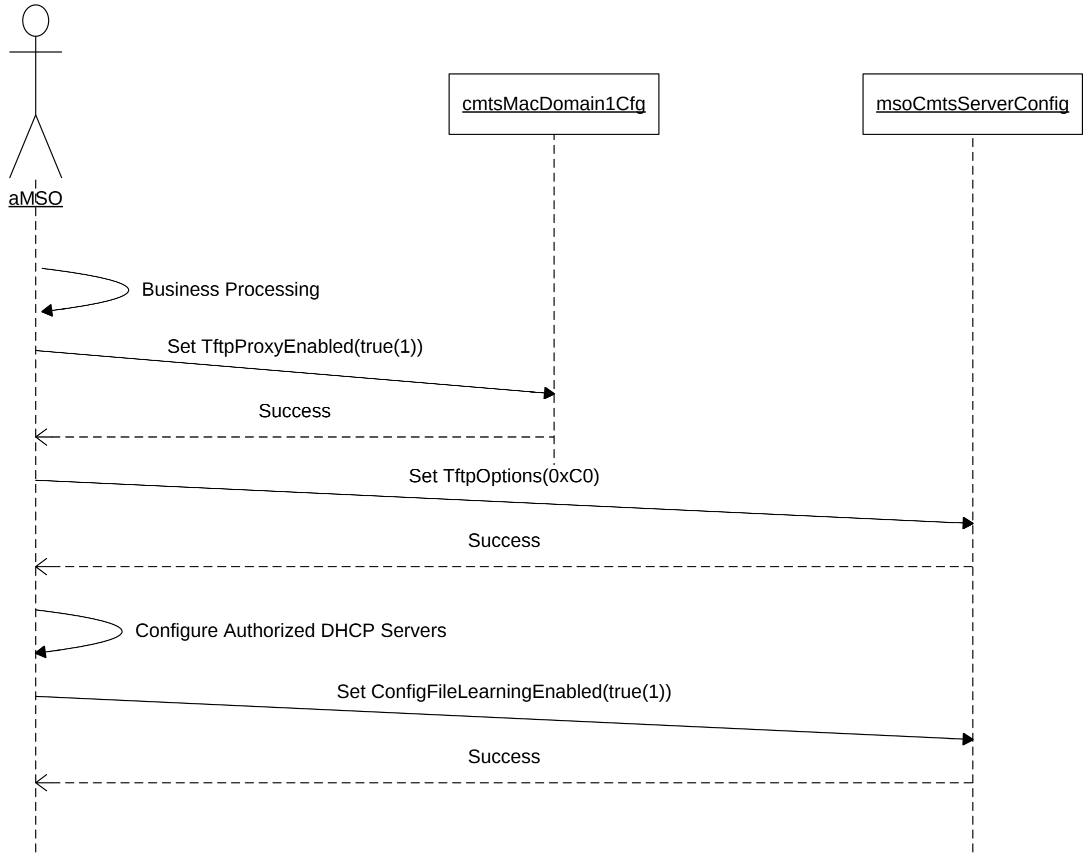
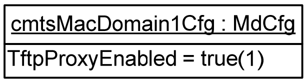


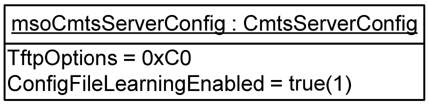
Figure 19 – Sequence Diagram for TFTP Configuration File Security

10.5.7 Post-conditions

The following diagram highlights the desired state for the MdCfg object at the end of this scenario.



The following diagram highlights the desired state for the CmtsServerCfg object at the end of this scenario.


msoCmtsServerConfig : CmtsServerConfig
TftpOptions = 0xC0
ConfigFileLearningEnabled = true(1)

The value 0xC0 assigned to the TftpOptions attribute instructs the CMTS to insert the source IP address and MAC address of received TFTP packets into the TFTP option fields before forwarding the packets to the Configuration File server.

10.5.8 Exceptions

There is a dependency between the CmtsServerConfig object and the TftpProxyEnabled attribute of the MdCfg object. The attributes defined in CmtsServerConfig are meaningless if the TftpProxyEnabled attribute is set to false(2). Even if the TftpOptions and ConfigFileLearningEnabled attributes are configured properly, the CMTS will ignore those attributes until the TftpProxyEnabled attribute is set to true(1).

Because the TftpOptions and ConfigFileLearningEnabled attributes have defined default values, if TftpProxyEnabled is set to true(1) without configuring the TftpOptions and ConfigFileLearningEnabled, their default values will be used.

10.5.9 Rollback Actions

No rollback actions are necessary since each attribute can be configured independently of the others.

10.6 Source Address Verification Security

10.6.1 Business Scenario

An MSO would like to strengthen their network security by enforcing Source Address Verification (SAV) to ensure that CMs as well as CPEs located behind CMs cannot successfully spoof addresses in order to obtain access to services or to disrupt services to other users on their network. SAV will be performed against Operator assigned IP addresses including those obtained through DHCP messaging as well as static IP addresses identified through parameters defined in the CM config file. Business customers may require a static range of IP addresses assigned by the Operator for the CPEs. An MSO is likely to create SAV Group IDs for assigning static ranges of IP addresses.

10.6.2 Scenario Details

This scenario will configure SAV within the CMTS to enable the following:

- Verification of DHCP assigned IP addresses
- Verification of static IP addresses using an SAV named group to define a configured list of prefixes

When the SAV feature is enabled, the CMTS drops any received upstream packets whose IP source address has not been assigned by the Operator. This includes packets whose source IP address is an IP address that has been assigned to another device. Source IP addresses are considered assigned by the Operator when they are provisioned via DHCP messaging or identified by parameters in the configuration file.

In addition, The CMTS may be configured to enable and disable the use of the SAV Group ID Encoding and Static SAV Prefix Encoding for identification of Operator assigned static ranges of IP addresses. This scenario will detail the use of SAV Group ID Encoding for statically assigned IP addresses.

The CM configuration file contains the following TLV encodings that are used to indicate IP addresses that have been assigned by the Operator, but are not issued by a DHCP server:

- An SAV Prefix Group ID Encoding that identifies a list of prefixes configured at the CMTS

  DOCSIS General Extension Information TLV 43.8 = 0xFF 0xFF 0xFF (reserved Vendor ID indicating general info)

  SAV Authorization Encoding TLV 43.7.1 = "OneSubnet" (ASCII string of SAV Group Name)

10.6.3 Assumptions

This scenario applies in deployment scenarios where CPEs are directly connected to a CM and where CPEs are behind a router (embedded eRouter or standalone router) that is connected to a CM.

Configuring the authorized DHCP servers within the CMTS is vendor-specific; refer to vendor's configuration guide for more details (e.g., IPv6 Relay and/or Cable Helper).

The CMTS will learn the DHCP assigned IP addresses in a vendor specific manner (e.g., snoop DHCP messages, perform DHCP Lease Queries, etc).

10.6.4 Pre-conditions

The CMTS must support the DOCSIS 3.0 Source Address Verification security feature.

The CM must support forwarding TLV 43 to the CMTS in the REG-REQ or REG-REQ-MP messages during registration.

There are no pre-conditions for DHCP server or configuration file server since this is a CMTS feature and is transparent to those entities.

The DHCPv4 and DHCPv6 servers have been configured as authorized DHCP servers on the CMTS using vendor specific methods.

10.6.5 Management Objects

- CMTS SAV Enabled configuration object

Refer to the MdCfg object defined in the CMTS Bonding Object Model Diagram Figure from Annex O of the DOCSIS 3.0 OSSI Specification. This object and its associated attributes are described in the MdCfg Object section. The SrcAddrVerifEnabled attribute enables or disables the top level SAV feature at the Mac Domain.

- CMTS Global SAV Control configuration object

Refer to the CmtsSavCtrl object defined in the Security Object Model Diagram Figure from Annex L of the DOCSIS 3.0 OSSI Specification. This object and its associated attributes are described in the CmtsSavCtrl Object section. The CmAuthEnable attribute enables or disables SAV for CM configured policies. In this scenario, the SAV Group Name is configured as a CM SAV policy. This policy is checked whenever the CMTS has not resolved an address as assigned through DHCP messaging.

- CMTS SAV Group Subnet Prefix configuration object

Refer to the SavCfgList object defined in the Security Object Model Diagram Figure from Annex L of the DOCSIS 3.0 OSSI Specification. This object and its associated attributes are described in the SavCfgList Object section. This object allows an Operator to configure an SAV Group Name policy.

- CMTS SAV CM Authorization Policy status object

Refer to the SavCmAuth object defined in the Security Object Model Diagram Figure from Annex L of the DOCSIS 3.0 OSSI Specification. This object and its associated read-only attributes are described in the SavCmAuth Object section. This object defines a read-only set of SAV policies associated with a CM that the CMTS will use in addition to the CMTS verification of an Operator assigned IP Address being associated with a CM.

10.6.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

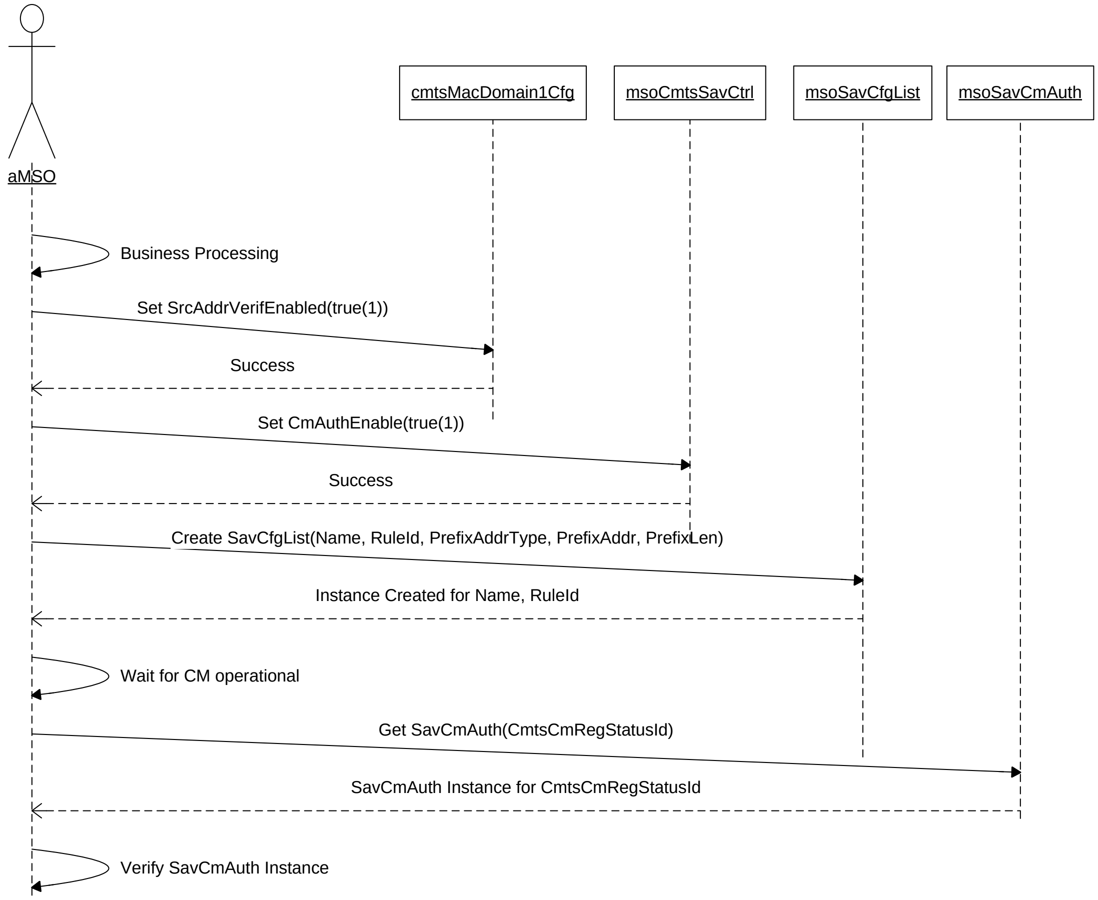

aMSO
cmtsMacDomain1Cfg
msoCmtsSavCtrl
msoSavCfgList
msoSavCmAuth
Business Processing
Set SrcAddrVerifEnabled(true(1))
Success
Set CmAuthEnable(true(1))
Success
Create SavCfgList(Name, RuleId, PrefixAddrType, PrefixAddr, PrefixLen)
Instance Created for Name, RuleId
Wait for CM operational
Get SavCmAuth(CmtsCmRegStatusId)
SavCmAuth Instance for CmtsCmRegStatusId
Verify SavCmAuth Instance

Figure 20 – Sequence Diagram for Source Address Verification Security

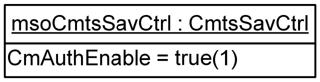
The SavCmAuth instance is created by the CMTS when the CM (identified by the CmtsCmRegStatusId) registers with the CMTS and includes the SAV Group Name in the REG-REQ or REG-REQ-MP.

10.6.7 Post-conditions

The following diagram highlights the desired state for the MdCfg object at the end of this scenario. The global SAV configuration setting is at the Mac Domain level.

cmtsMacDomain1Cfg : MdCfg
SrcAddrVerifEnabled = true(1)

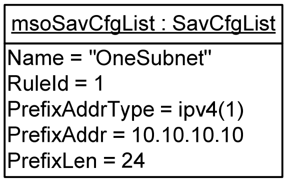
The following diagram highlights the desired state for the CmtsSavCtrl object at the end of this scenario. The CmAuthEnable set to true(1) will enable SAV for CM configured policies as defined in the SavCmAuth object instances (e.g., SAV Group ID Encoding and/or Static SAV Prefix Encoding.)



msoCmtsSavCtrl : CmtsSavCtrl

CmAuthEnable = true(1)

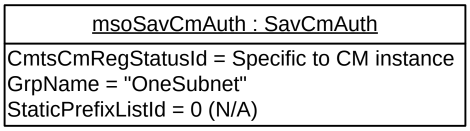
The following diagram highlights the desired state for the SavCfgList object at the end of this scenario. Configuring the SavCfgList instance as shown defines a SAV Group ID Encoding CM policy.



msoSavCfgList : SavCfgList

Name = "OneSubnet"
RuleId = 1
PrefixAddrType = ipv4(1)
PrefixAddr = 10.10.10.10
PrefixLen = 24

The following diagram highlights the desired state for the SavCmAuth object at the end of this scenario. This instance includes a single SAV Group ID Encoding CM policy as configured by the SavCfgList instance and signaled by the CM during registration.



msoSavCmAuth : SavCmAuth

CmtsCmRegStatusId = Specific to CM instance
GrpName = "OneSubnet"
StaticPrefixListId = 0 (N/A)

10.6.8 Exceptions

There is a dependency between the CmtsSavCtrl object and the SrcAddrVerifEnabled attribute of the MdCfg object. The attribute defined in CmtsSavCtrl is meaningless if the SrcAddrVerifEnabled attribute is set to false(2). The SavCmAuth object is dependent on the CmtsSavCtrl object. If the CmAuthEnable attribute of the CmtsSavCtrl object is set to false(2), the CM policies defined in SavCmAuth will be ignored by the CMTS. Even if the CmAuthEnable attribute and SavCfgList object attributes are configured properly, the CMTS will ignore those attributes until the SrcAddrVerifEnabled attribute is set to true(1).

Creating an instance of the SavCfgList object via CMTS configuration requires the Operator to specify the PrefixAddrType and PrefixAddr attributes. The PrefixLen attribute has a default value of 0 if not specified during instance creation. A CMTS may reject an object instance creation if either PrefixAddrType and/or PrefixAddr attributes are omitted during the instance creation.

If the CM signals an SAV Group Name during registration in which the CMTS has no knowledge (i.e., the SAV Group was not configured in the CMTS), the CMTS will ignore the Name attribute in the SavCfgList object and the CM registration is not denied for this reason.

The CM config file cannot include SAV Authorization Encoding TLVs which define both a SAV Group Name encoding (TLV 43.7.1) and a SAV Static Prefix encoding (TLV 43.7.2). This scenario does not address the SAV Static Prefix case.

10.6.9 Rollback Actions

Since SrcAddrVerifEnabled and CmAuthEnable attributes are configured independently, there is no rollback action required. Refer to the Exceptions section for dependency details of these attributes.

If the CMTS rejects an SavCfgList instance creation, the CMTS should not create a partial instance that is not ready. If a partial instance is created for some reason, it can be destroyed and recreated, or updated and set active. If the Operator creates an instance of SavCfgList that is incorrect, they can destroy the instance and start over, or updated the instance and set it active.

11 PROVISION IPDR SCENARIOS

This section defines Scenarios for provisioning Cable network elements and back office servers for supporting IPDR/SP streaming of data.

11.1 IPDR/SP Configuration for SAMIS-TYPE-1 Service Definition

11.1.1 Business Scenario

MSOs are now challenged with trying to monitor per subscriber data consumption. DOCSIS 3.0 IPDR feature for Subscriber Account Management Information Systems (SAMIS) can be leveraged to extract the subscriber consumption data at a periodic interval. The SAMIS IPDR Service Definition will provide data consumption per subscriber per service flow. Periodic collection of this data can be used by back office applications to process usage-based billing.

11.1.2 Scenario Details

This Scenario configures the CMTS for IPDR/SP streaming of SAMIS-TYPE-1 Service Definition. The following configuration steps are performed:

- Identify the IP address of the Primary and Backup IPDR/SP collector in the MSO back office system.
- Configure the CMTS with the IP address and port of primary and backup IPDR/SP collector.
- Configure global IPDR/SP parameters associated to Service Definition, streaming interval, timeout, keep Alive.
- Configure other optional IPDR/SP parameters like ackSequenceInterval and ackTimeInterval [IPDR/SP].

11.1.3 Assumptions

This Scenario assumes that IPDR/SP session parameters such as ackSequenceInterval and ackTimeInterval [IPDR/SP] are configurable on the CMTS.

The MSO has a backup collector available to handle IPDR streaming protocol redundancy.

The CMTS provides CLI commands to show the status of IPDR/SP connection and collection status.

CMTS IPDR Configuration is a one-shot CLI command where there is no possibility of partial configuration.

11.1.4 Pre-conditions

The CMTS must support the IPDR/SP protocol and the SAMIS-TYPE-1 Service Definition as defined in [OSSI3.0]. The CMTS must provide vendor specific methods for configuring IPDR/SP parameters.

11.1.5 Management Objects

There are no IPDR/SP configuration management objects currently defined in [OSSI3.0]. Refer to the "IPDR Exporter Configuration" section of [OSSI3.0] for details.

11.1.6 Sequence Diagram

This section illustrates the UML Sequence Diagram for this Scenario. Refer to Appendix I.3 for details on the notation used.

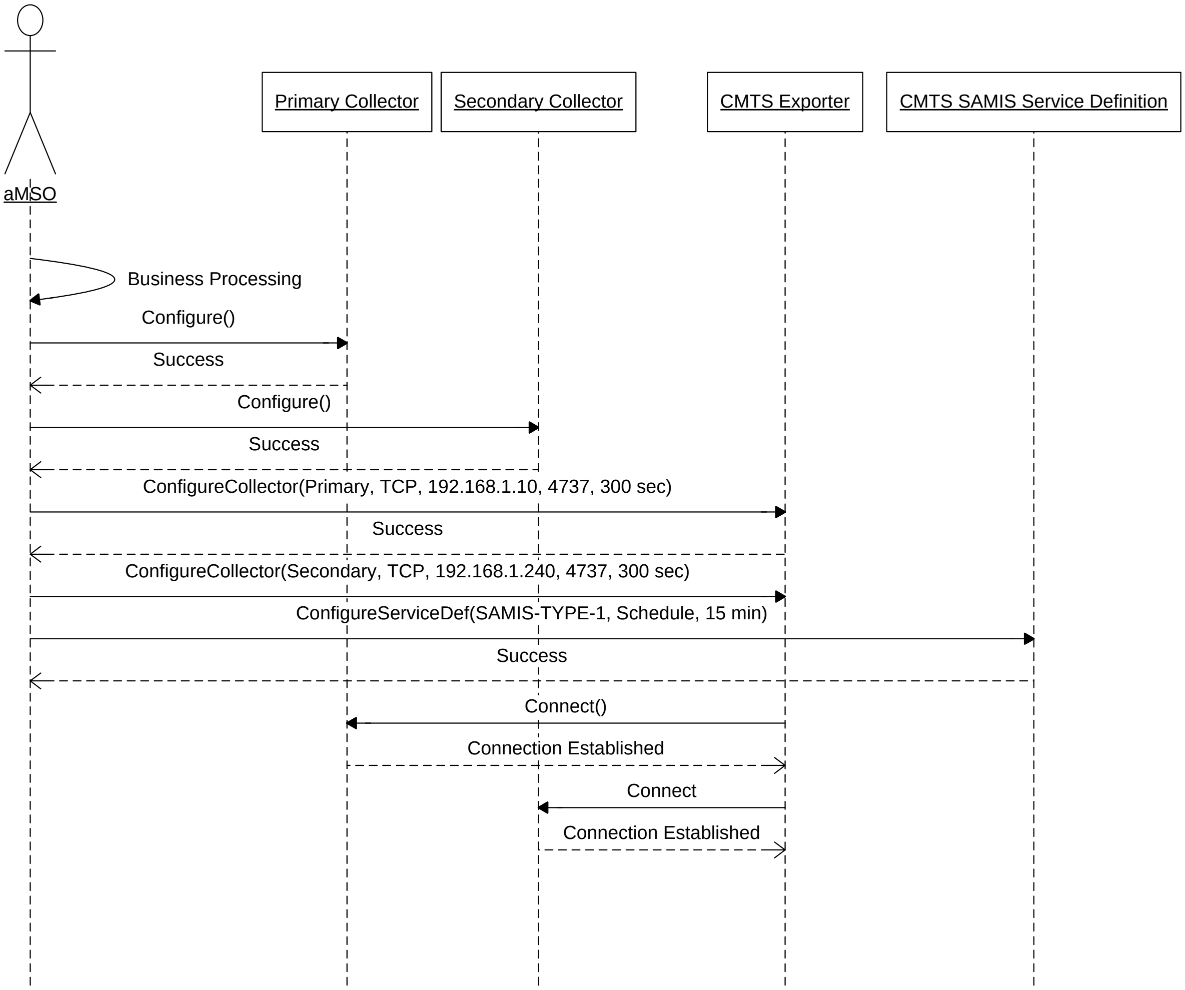

Primary Collector
Secondary Collector
CMTS Exporter
CMTS SAMIS Service Definition
aMSO
Business Processing
Configure()
Success
Configure()
Success
ConfigureCollector(Primary, TCP, 192.168.1.10, 4737, 300 sec)
Success
ConfigureCollector(Secondary, TCP, 192.168.1.240, 4737, 300 sec)
ConfigureServiceDef(SAMIS-TYPE-1, Schedule, 15 min)
Success
Connect()
Connection Established
Connect
Connection Established

Figure 21 – Sequence Diagram for IPDR/SP Configuration for SAMIS-TYPE-1 Service Definition

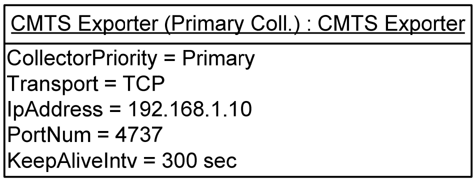
11.1.7 Post-conditions

The CMTS provides the CLI commands to list the collector instances and their collection status.

Most IPDR/SP collectors provide an application interface to verify the connection and collection status.

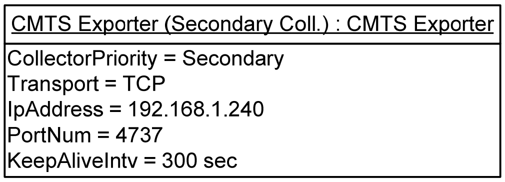
The CMTS, the primary collector, and the backup collector have established a connection and are successfully exchanging IPDR/SP protocol messages. The CMTS is successfully streaming SAMIS-TYPE-1 instance data at the pre-configured time intervals.

The CMTS Exporter must be configured with primary and secondary collector information as shown below:



CMTS Exporter (Primary Coll.) : CMTS Exporter

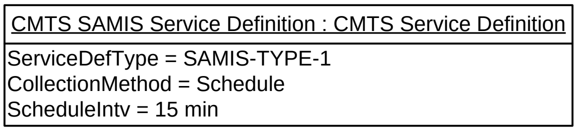
CollectorPriority = Primary
Transport = TCP
IpAddress = 192.168.1.10
PortNum = 4737
KeepAliveIntv = 300 sec



CMTS Exporter (Secondary Coll.) : CMTS Exporter

CollectorPriority = Secondary
Transport = TCP
IpAddress = 192.168.1.240
PortNum = 4737
KeepAliveIntv = 300 sec

The CMTS Exporter may also require configuring which IPDR Service Definition to stream, which collection methodology to use and what the collection interval is. An example is shown below:



CMTS SAMIS Service Definition : CMTS Service Definition

ServiceDefType = SAMIS-TYPE-1
CollectionMethod = Schedule
ScheduleIntv = 15 min

Since there are no standard configuration objects or attributes defined in [OSSI3.0], the above are merely examples. CMTS implementations may vary based on vendor implementation.

11.1.8 Exceptions

Since CMTS IPDR/SP configuration is a one-shot CLI command, there are no exception cases of a partial configuration state within the CMTS.

11.1.9 Rollback Actions

No rollback is required.

Appendix I Unified Modeling Language (UML) Notation

This appendix illustrates the Unified Modeling Language (UML) notation used throughout this technical report to define Use Case diagrams, Scenario diagrams, and Object Instance diagrams.

Refer to the Object Model Notation Appendix of [OSSI3.0] for a detailed explanation of the UML Object Model Diagram. Although Object Model diagrams are not defined in this Technical Report, they are referenced from [OSSI3.0]. This Technical Report does define Object Instance diagrams based on the Object Model diagrams defined in [OSSI3.0].

I.1 Overview

The Unified Modeling Language (UML) is a unified model for object-oriented analysis and design (OOA&D). UML is an OMG standard and is an accepted ISO specification [ISO 19501].

UML defines a general-purpose, graphical modeling language that can be applied to any application domain (e.g., communications) and implementation platforms (e.g., J2EE).

I.2 Use Case Diagram

The Technical Report Use Case diagram is represented by the UML Use Case Diagram. The Use Case diagram is used to show what functions are performed in a system by which actors (e.g., how an actor with a specific role interacts with a system to perform certain goals).

I.2.1 Diagram Notation

An actor (i.e., Cook or Waitress) is represented as a stick figure icon and may have a name or description of their role. Each Use Case is listed in an oval with an action statement for the actor(s) to perform a goal (i.e., Make Breakfast). A system boundary is included in the diagram.

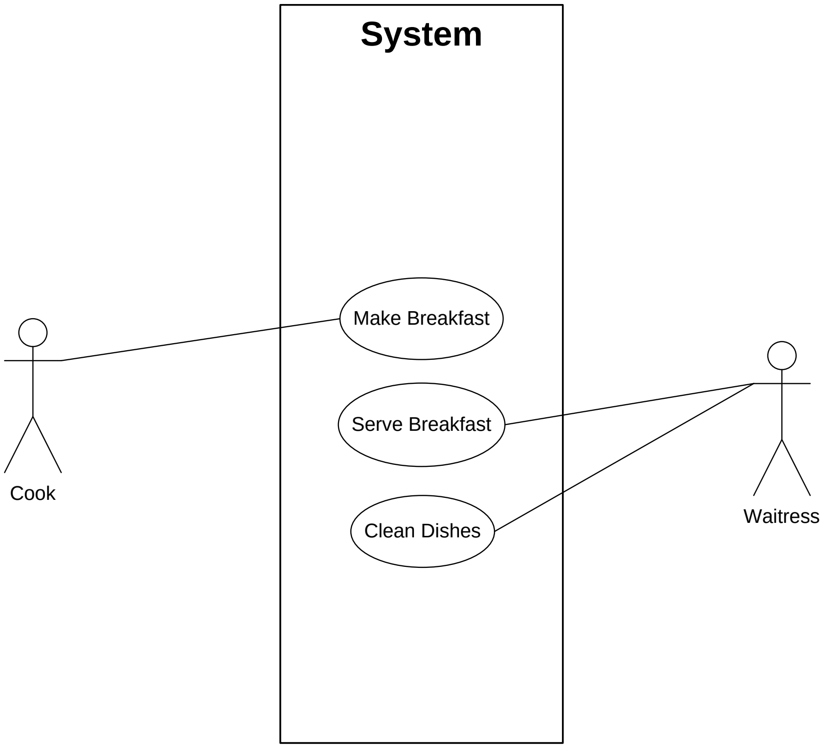


Figure I-1 - Example Use Case Diagram

I.3 Sequence Diagram

The Technical Report Sequence diagram is represented by the UML Sequence Diagram. The Sequence diagram describes the message interactions between an Actor and the objects in a system (or between objects in a system) in a given time/sequence order. Time increases downward in a Sequence diagram. Sequence diagrams are often called Scenario diagrams or Message Sequence Charts.

I.3.1 Diagram Notation

In a Sequence diagram, object instances (i.e., myObjectA and myObjectB) are shown as boxes along the top of the diagram. The vertical dashed lines extending downward from the object instances are lifelines and represent the lifetime of an object instance. Messages are shown as solid arrows between the lifelines of two object instances. A return (represented by a dashed line) is not a new message, but a return from a previous message. A self-call is a message that is looped back on the same object lifeline.

Procedure calls (i.e., Set AttributeA1()) with parameters passed (i.e., 20) appear above messages. Common procedures include a Get function, which is often realized as an SNMP GET message, and a Set function, which is often realized as an SNMP SET message. In addition, Create (or Add) and Delete (or Remove) procedures are often realized in SNMP as row creation or deletion actions in MIB tables which support dynamic row creation and deletion.

Figure I-2 shows a Sequence Diagram for an interaction between ObjectA (instantiated as myObjectA) and ObjectB (instantiated as myObjectB).

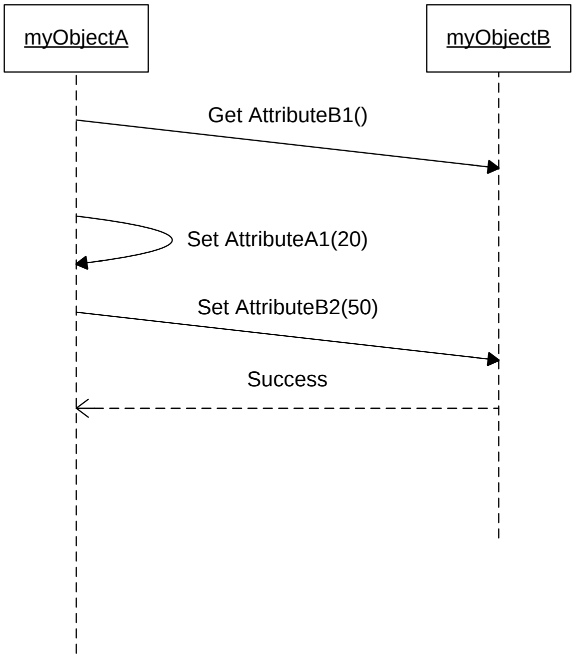


Figure I-2 - Example Sequence Diagram for ObjectA Interacting with ObjectB

I.4 Object Instance Diagram

An Object Instance Diagram represents the objects in a system during one snapshot in time. In this diagram, the class objects (defined in an Object Model diagram) are instantiated.

I.4.1 Diagram Notation

Figure I-3 shows an Object Instance Diagram for an instantiation (myObjectA) of ObjectA.

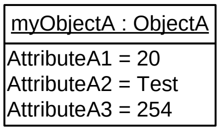


Figure I-3 - Example Object Instance Diagram for ObjectA

Appendix II Cable Modem Replacement Process

CM replacement consists of equipment identification, signal level pre-qualification for self-install, customer notifications, per System/Headend warehouse process changes and staff notifications, shipping logistics, self-install/equipment replacement processes in the OSS, reclamation to non-reuse category of inventory (disposal) and where applicable, establishment of end-of-life equipment disposal program. These same processes can be re-used for any and all equipment that is replaced, either due to feature requirements for a new service profile, or due to defects that cannot be resolved via software update.

1. All CMs are cataloged by their sysDescr, providing valuable information on vendor, hardware, and software revision. This is often maintained in CM software management systems to upgrade CM software whenever such software is available and has been tested in the MSOs lab. Regular reports are produced from a central location (firmware management is often a centralized vs. local function) to identify the CMs/MTAs to be targeted for replacement and progress of those replacements throughout the project's time frame.
2. Build and maintain a regular report correlating targeted CMs/MTAs with the last 30 days of its recorded signal levels in order to categorize and qualify the CM/MTA installations prior to shipping equipment for self-install equipment replacement
   a. For targeted CMs having signal levels below nominal, equipment replacements are to be scheduled with the local dispatch in much the same manner as a new install.
   b. All signal levels will be corrected and the customer will be educated about use of splitters and the necessary quality of cable to be used for any and all extensions, making the customer aware that MSO will generally come out to perform such installs (new TVs, other equipment, etc.) for free.
   c. Installer will use a technician equipment swap page in the web provisioning tools for the OSS instead of completing the new install process flow.
3. Decisions must be made at a local level as to how to allocate resources to the program for the duration of the project. All execution occurs at a local level and the processes developed must be tailored to the unique circumstances of the locale.
   a. Methods of communicating intentions to the customer, for example, via another page in the cable bill or via some other direct mailing must be decided.
   b. Allocation of staff for equipment installations in customer locations that are not classified as new installs can be problematic to run-rates (installs per day/week/month) and may increase new install time frames from a few days to a week in some cases.
   c. Rescue installs, where self-installs could not be completed by the customer, have to be anticipated and a certain number of staff allocated for such rescues.
   d. Timing of a particular group of nodes (or the entire head-end) equipment replacement is locally determined and staged accordingly.
   e. A protocol for customers who do not respond to their equipment replacement schedule notifications with call-ins to confirm their appointments (or change the time block/date), or receive the equipment for self-install but take no action, must be dealt with. Trucks should not be rolled to locations where no contact can be made.
   f. Decisions have to be made about handling of service for customer's whose equipment replacements have not taken place and could not otherwise be scheduled with the customer (customer out of town, etc.). At a certain date after all installs were scheduled to be complete, these customers may lose service. The Customer Care teams generally must maintain their program until several months after the majority of customer's have been migrated.
4. Correlation is performed between the targeted CMs/MTAs and the MAC address along with its association with a billing account number, account name, and service address.
5. Notice that equipment is to be replaced is mailed to all affected customers by billing account. In some cases, they may notice that an extra page is included in their bill, which is usually sent at least two billing cycles before the intended equipment rollover is supposed to occur. Each bill (if that is the route chosen) will include further information on the CM/MTA (or other equipment) replacement program and any incentives for returning old equipment.

6. Equipment is shipped at least two weeks in advance of the desired equipment replacement by UPS or Fedex (depending on local rates) from the local warehouse. Packaging includes a box to be sent by USPS back to the warehouse.

   If equipment returns are not at least half of what is sent out, an incentive program may need to be created (if not already established) or modified. Common incentives include credits on bill, or turning on new features unique to the new equipment only upon return of old equipment into inventory.

7. For qualified customer installs that were deemed possible to complete as self-installed equipment replacement, the customer will follow a five-step instruction sheet that physically attaches equipment in the same manner as the outdated equipment. The new MAC address will prompt an installation process via a webpage (any URL typed will navigate to this page) to replace equipment. Generally, the installs flows are built such that the CM/MTA MAC address does not need to be known at time of shipping, simplifying logistics and avoiding pre-authorized equipment bypassing flow-through provisioning.

8. The new MAC address is then read off the CM label by the customer (per the instruction supplied with the CM/MTA), typing this MAC address into the equipment replacement provisioning flow and replacing the old MAC address in the billing record. The CM will reset and be provisioned with a configuration profile consistent with the tier of service to which the customer has subscribed. Installation/replacement of equipment will usually take several hours to complete propagation through the provisioning and monitoring systems.

9. The equipment replacement formally completes when the old CM has been returned to inventory and categorized as "do not reuse." The inventory process should avoid equipment that is reclaimed for this purpose being sent out on the next install at another customer location.

10. A report of all reclaimed CMs/eMTAs and all the equipment that has not yet been returned will be supplied periodically to Regional and Corporate to report on the status of the reclamation.

11. Local warehouses will be required to arrange disposal. In most cases, the CMs can be sent to a recycling facility (locations are certified by the EPA and other state-level protection agencies) where precious metals, plastics, and other materials can be reclaimed and re-used instead of being deposited in a landfill.

12. CM and MTA equipment owned by the customer will be similarly replaced, customer may be notified as part of the initial and subsequent notifications of a URL to go to for the recommended equipment list if they wish to purchase their own CM/MTA. If the customer calls in with their MAC address and the equipment does not match the CM recommended list, the CM will not be allowed to be provisioned, and the original MAC address will be retained. Customers will be encouraged to take the CM provided by the MSO.

Appendix III DHCP Options

III.1 DHCPv6 Options Used by DOCSIS 3.0 Clients

The following table lists the DHCPv6 options used by a DOCSIS 3.0 client.

Table III-1 - DHCPv6 Options Used by DOCSIS 3.0 Clients

DHCP Option Number	Description	Normative Reference	Comments
1	Client Identifier	[RFC 3315]	Included in the DHCP SOLICIT, DHCP REQUEST, and DHCP DECLINE messages sent by the DHCP client to the DHCP server. Included in the DHCP ADVERTISE and DHCP REPLY messages sent by the DHCP server to the DHCP client.
2	Server Identifier	[RFC 3315]	Included in the DHCP ADVERTISE and DHCP REPLY messages sent by the DHCP server to the DHCP client. Included in the DHCP REQUEST messages sent by the DHCP client to the DHCP server.
3	Identity Association for Non-Temporary Addresses (IA_NA)	[RFC 3315]	Included in the DHCP SOLICIT, DHCP REQUEST, and DHCP DECLINE messages sent by the DHCP client to the DHCP server. Included in the DHCP ADVERTISE and DHCP REPLY messages sent by the DHCP server to the DHCP client.
14	Rapid Commit	[RFC 3315]	Included in the DHCP SOLICIT message sent by the DHCP client to the DHCP server.
16	Vendor Class ID	[RFC 3315]	Included in the DHCP SOLICIT, DHCP REQUEST, and DHCP DECLINE messages sent by the DHCP client to the DHCP server.
17	Vendor-specific Information Option	[RFC 3315]	Included in the DHCP SOLICIT and DHCP REQUEST messages sent by the DHCP client to the DHCP server. Included in the DHCP ADVERTISE and DHCP REPLY messages sent by the DHCP server to the DHCP client.
Option 17 Sub-Options			
1	Option Request Option (ORO) Sub-Option	[CANN DHCP-Reg]	Included in the DHCP SOLICIT and DHCP REQUEST messages sent by the DHCP client to the DHCP server.
32	TFTP Servers Sub-Option	[CANN DHCP-Reg]	Included in the DHCP ADVERTISE and DHCP REPLY messages sent by the DHCP server to the DHCP client.
33	Configuration file name Sub-Option	[CANN DHCP-Reg]	Included in the DHCP ADVERTISE and DHCP REPLY messages sent by the DHCP server to the DHCP client.

34	Syslog Servers Sub-Option	[CANN DHCP-Reg]	Included in the DHCP ADVERTISE and DHCP REPLY messages sent by the DHCP server to the DHCP client.
35	TLV5 Encoding (Modem Capabilities) Sub-Option	[CANN DHCP-Reg]	Included in the DHCP SOLICIT and DHCP REQUEST messages sent by the DHCP client to the DHCP server.
36	Device ID Sub-Option	[CANN DHCP-Reg]	Included in the DHCP SOLICIT and DHCP REQUEST messages sent by the DHCP client to the DHCP server.
37	Time Servers	[CANN DHCP-Reg]	Included in the DHCP SOLICIT and DHCP REQUEST messages sent by the DHCP client to the DHCP server.
38	Time Offset	[CANN DHCP-Reg]	Included in the DHCP SOLICIT and DHCP REQUEST messages sent by the DHCP client to the DHCP server.
Standard DHCP Options			
18	Interface-ID	[RFC 3315]	Included in the DHCP RELAY-FORWARD message sent by the DHCP Relay Agent to the DHCP server. Included in the DHCP RELAY-REPLY message sent by the DHCP server to the DHCP Relay Agent.
19	Reconfigure Message	[RFC 3315]	Included in the DHCP RECONFIGURE message sent by the DHCP server to the DHCP client.
20	Reconfigure Accept	[RFC 3315]	Included in the DHCP ACCEPT message sent by the DHCP client to the DHCP server.
1025	DHCPv6 Relay Agent CMTS Capabilities Option	[CANN DHCP-Reg]	Included in the DHCP RELAY-FORWARD message sent by the DHCP Relay Agent to the DHCP server.
Option 1025 Sub-Options			
1	CMTS DOCSIS Version Number	[CANN DHCP-Reg]	Included in the DHCP RELAY-FORWARD message sent by the DHCP Relay Agent to the DHCP server.
1026	DOCSIS Relay Agent CM MAC Address Option	[CANN DHCP-Reg]	Included in the DHCP RELAY-FORWARD message sent by the DHCP Relay Agent to the DHCP server.

III.2 Differences in DHCPv4 Options Used by DOCSIS 2.0 Cable Modems vs. DOCSIS 3.0 Cable Modems

DOCSIS 2.0 cable modems and DOCSIS 3.0 cable modems use virtually the same set of DHCPv4 options as pre-3.0 DOCSIS with only minor differences in the values of some DHCP options indicating DOCSIS version and modem capabilities, as indicated in Table III-2 below.

Table III-2 - DHCPv4 Option Differences between DOCSIS 2.0 and DOCSIS 3.0

Option Number	Description	DOCSIS 2.0 Value	DOCSIS 3.0 Value
60	Vendor Class ID	Contains the ASCII value "docsis2.0:xxxxxxx", where xxx… encoding is as specified in [RFIv2.0].	Contains the ASCII value "docsis3.0:".
125.5	TLV5 Encoding (Modem Capabilities)	Not supported in DOCSIS 2.0.	As specified in the Modem Capabilities Encoding sub-section of [MULPI3.0].
125.1.2	Request TFTP Servers Option	Uses standard DHCPv4 options.	Request for TFTP servers data.
61	Client Identifier	Not supported in DOCSIS 2.0.	A Client Identifier option containing the DUID (DHCP Unique Identifier) for this CM as specified by [RFC 4361].

III.3 Differences in DHCPv6 Options Used by DOCSIS 2.0 Cable Modems that support IPv6 vs. DOCSIS 3.0 Cable Modems

Note that DOCSIS 2.0 CMTS’ do not support DHCPv6. A DOCSIS 2.0 cable modem operating in a DHCPv6 environment must operate with a DOCSIS 3.0 CMTS.

As described in [ICMTR], DOCSIS 2.0 cable modems operating in a DHCPv6 environment use the same procedures and settings as DOCSIS 3.0 cable modems with only minor differences in the values of some DHCP options indicating DOCSIS version and modem capabilities, as indicated in Table III-3 below.

Table III-3 - DHCPv6 Option Differences between DOCSIS 2.0 and DOCSIS 3.0

Option Number	Description	DOCSIS 2.0 Value	DOCSIS 3.0 Value
17.35	TLV5 Encoding (Modem Capabilities)	As specified in Modem Capabilities and Vendor Class Reporting section of [ICMTR].	As specified in the Modem Capabilities Encoding sub-section of [MULPI3.0].
16	Vendor Class ID	Contains the 32-bit number 4491 (the Cable Television Laboratories, Inc. enterprise number) and the string "docsis2.0:".	Contains the 32-bit number 4491 (the Cable Television Laboratories, Inc. enterprise number), and the string "docsis3.0:".

Appendix IV Acknowledgements

On behalf of the cable industry and our member companies, CableLabs would like to thank the following individuals for their contributions to the development of this technical report.

Contributor	**Company Affiliation**
Nick Brown	Cox Communications, Inc.
Patrick Cosmo	Incognito Software Inc.
Kirk Erichsen	Time Warner Cable
Deepak Gargeshwari	ARRIS
Eric Hasenstab	BigBand
Brian Hedstrom	CableLabs
Robert Lund	Cisco
Dan Torbet	ARRIS