SCTE · ISBE

STANDARDS

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 106 2018

DOCSIS Set-top Gateway (DSG) Specification

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at http://www.scte.org.

140 Philips Road
Exton, PA 19341

Note: DOCSIS® and CableCARD™ are registered trademarks of Cable Television Laboratories, Inc., and used in this document with permission.

Contents

Figures

Tables

1 SCOPE

1.1 Executive Summary

The DOCSIS Set-top Gateway (DSG) specification defines an interface and associated protocol that introduces additional requirements on a DOCSIS CMTS and DOCSIS CM to support the configuration and transport of a class of service known as "Out-Of-Band (OOB) messaging" between a Set-top Controller (or application servers) and the customer premise equipment (CPE). In general, the CPE is intended to be a digital Set-top Device, but may include other CPE devices, such as Residential Gateways or other electronic equipment. Figure 1–1 provides the context for this standard in relation to the data-over-cable reference architecture and the other interface specifications in the family.

1.2 Introduction and Overview

Traditionally, the physical transport of this Out-Of-Band messaging has been carried over dedicated channels, as specified by [SCTE 55-1] and [SCTE 55-2]. This standard defines the applicable communications standards and protocols needed to implement an Out-Of-Band messaging interface to the Set-top Device using DOCSIS as a transport. It applies to cable systems employing HFC and coaxial architectures. Specifically, the scope of this standard is to:

- Describe the communications protocols and standards to be employed.
- Specify the data communication requirements and parameters that will be common to all units.

The intent of this document is to specify open protocols, with a preference for existing, well-known, and well-accepted standards. This interface standard is written to provide the minimal set of requirements for satisfactory communication between the Set-top Controller and the Set-top Device over the DOCSIS transport. "DOCSIS Set-top Gateway" (DSG) shall be the general term used to describe this interface.

The present document corresponds to and is the technical equivalent of the CableLabs [DOCSIS DSG] specification.

1.3 Purpose of Document

Cable operators have deployed millions of digital set-top boxes enabling broadcast and interactive services. They have also deployed millions of DOCSIS cable modems with the associated infrastructure, CMTS, routers, and network connectivity. There is significant interest in enabling digital set-top boxes to leverage the existing infrastructure of digital video and DOCSIS networks. This document is one of a series of interface specifications that will permit the early definition, design, development, and deployment of digital cable systems on a uniform, consistent, open, non-proprietary, multi-vendor interoperable basis.

The intended service will allow transparent uni-directional and bi-directional transport of Out-Of-Band messaging over Internet Protocol (IP), between the cable system headend and customer locations, over an all-coaxial or hybrid-fiber/coax (HFC) cable network. This is shown in simplified form in Figure 1–1.

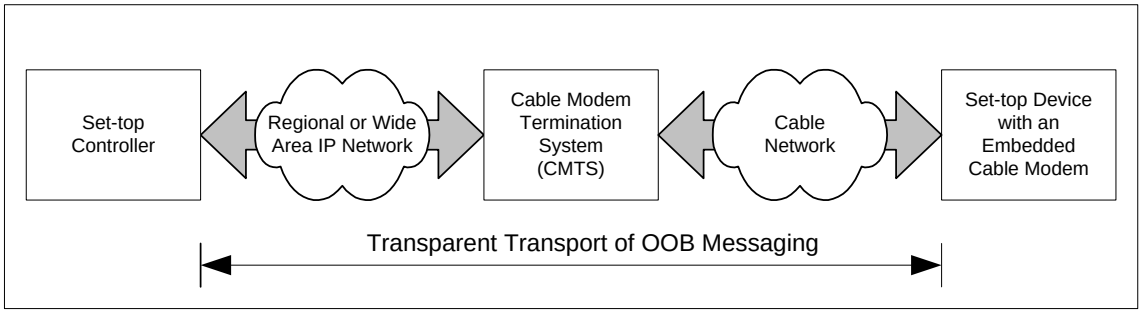


Figure 1–1 - Transparent Out-Of-Band Messaging Via DOCSIS

The transmission path over the cable system is realized at the headend by a Set-top Controller that is responsible for managing the Set-top Devices, a regional or wide area IP network connecting the Set-top Controller to the Cable Modem Termination System (CMTS), and, at each customer location, a Set-top Device with an embedded Cable Modem. At the headend (or hub), the interface to the data-over-cable system is called the Cable Modem Termination System - Network-Side Interface [DOCSIS-CMTS-NSI].

The intent is for the cable operators to transparently transport OOB messaging traffic between these interfaces, including but not limited to UDP over IP datagrams in either unicast, broadcast, or multicast forms. DSG addresses several issues:

- DSG allows the DOCSIS downstream transport to be used for Out-of-Band signaling.
- DSG allows delivery of Out-of-Band messages through the DOCSIS downstream without requiring return path functionality between the Set-top Devices and the CMTS.
- DSG allows legacy non-IP addressing of Set-top Devices by a Set-top Controller to be transported over a tunnel on an IP network.

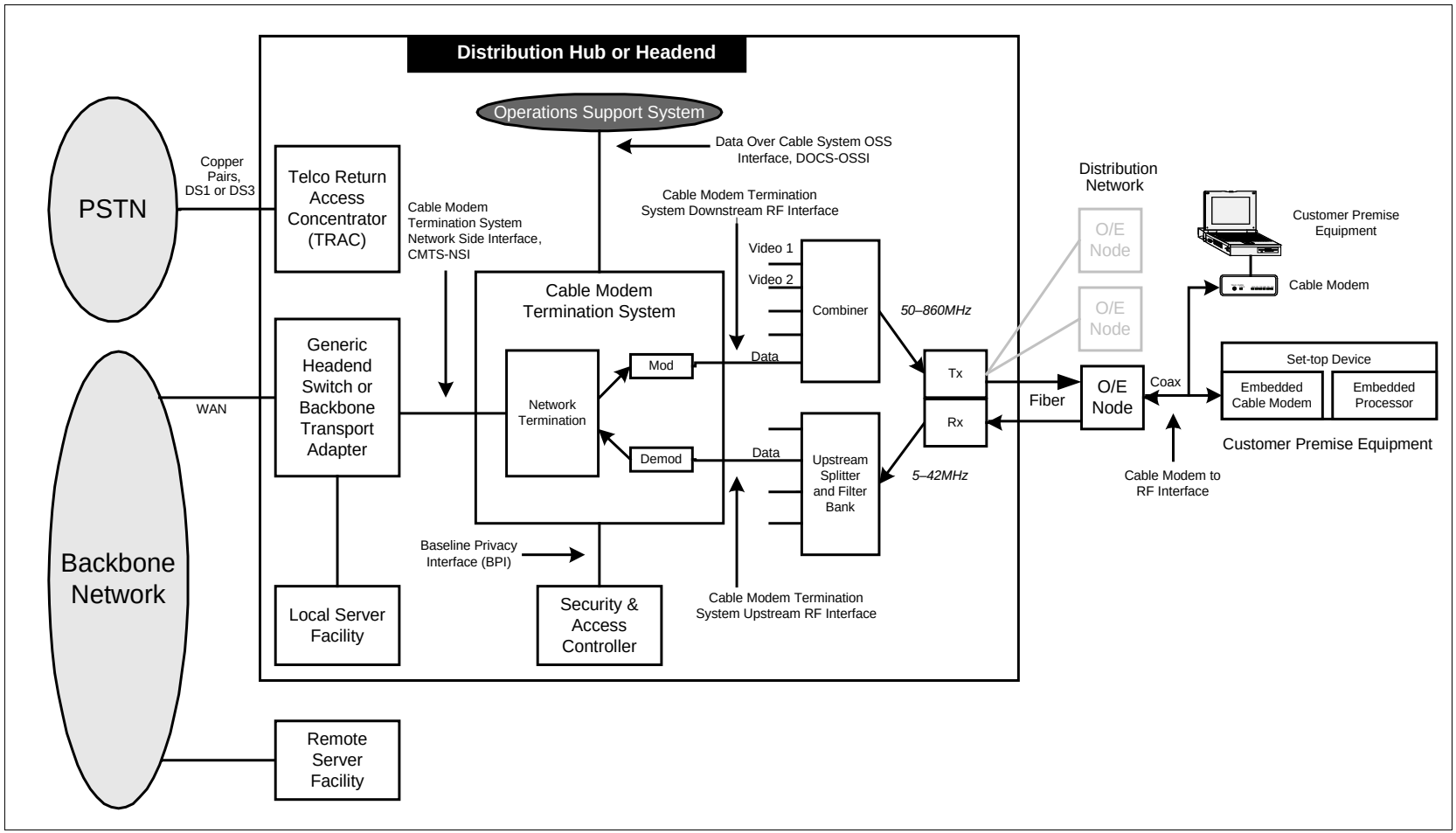


Figure 1–2 - Data-Over-Cable Reference Architecture

1.4 Requirements

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

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

2 REFERENCES

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1 Normative References

2.1.1 SCTE References

[DOCSIS2.0-IPv6]	ANSI/SCTE 79-3 2017 DOCSIS 2.0 + IPv6 Cable Modem Standard.
[DOCSIS-RFIv1.1]	ANSI/SCTE 23-1 2010, DOCSIS 1.1 Part 1: Radio Frequency Interface.
[DOCSIS-RFIv2.0]	ANSI/SCTE 79-1 2016, DOCSIS 2.0 Part 1: Radio Frequency Interface.
[DOCSIS-MULPI]	ANSI/SCTE 135-2 2013, DOCSIS 3.0 Part 2: MAC and Upper Layer Protocols.

2.1.2 Standards from other Organizations

[DOCSIS-RFI]	Refers to both [DOCSIS-RFIv1.1] and [DOCSIS-RFIv2.0].
[DOCSIS RFI/MULPI]	Refers to [DOCSIS-RFI] and [DOCSIS-MULPI].
[DOCSIS-CMTS-NSI]	DOCSIS Cable Modem Termination System - Network Side Interface Specification, SP-CMTS-NSI-I01-960702, July 2, 1996, Cable Television Laboratories, Inc.
[DOCSIS-PNMP]	DOCSIS Best Practices and Guidelines, Proactive Network Maintenance Using Pre-equalization, CM-GL-PNMP-V03-160725, July 25, 2016, Cable Television Laboratories, Inc.
[DSG-IF-MIB]	DOCSIS Set-top Gateway Agent MIB, DSG-IF-MIB, http://mibs.cablelabs.com/MIBs/DOCSIS/.
[DSG-IF-STD-MIB]	DOCSIS Set-top Gateway Set-top Device MIB, DSG-IF-STD-MIB, http://mibs.cablelabs.com/MIBs/DOCSIS/.
[UPNP-DA]	UPnP™ Device Architecture 1.0, Version 1.0.1, 2 December 2003. http://www.upnp.org/download/UPnPDA10_20000613.htm.

2.2 Informative References

The following documents might provide valuable information to the reader but are not required when complying with this document.

2.2.1 SCTE References

[SCTE 18]	ANSI/SCTE 18 2013, "Emergency Alert Message for Cable".
[SCTE 23-3]	ANSI/SCTE 23-3 2010 “DOCSIS 1.1 Part 3: Operations Support System Interface.”
[SCTE 55-1]	ANSI/SCTE 55-1 2009, "Digital Broadband Delivery System: Out-of-Band Transport Part 1: Mode A".
[SCTE 55-2]	ANSI/SCTE 55-2 2008, "Digital Broadband Delivery System: Out-of-Band Transport Part 2: Mode B".
[SCTE 65]	SCTE 65 2016, "Service Information Delivered Out-Of-Band For Digital Cable Television".

[SCTE 79-2] ANSI/SCTE 79-2 2016 “DOCSIS 2.0 Part 2: Operations Support System Interface.”

2.2.2 Standards from other Organizations

[CAS ID] "Conditional Access System Identifier," CA_system_ID, administered by DVB, www.dvb.org.

[DOCSIS-OSSIv3.0] Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification, CM-SP-OSSIv3.0-I30-170111, January 11, 2017, Cable Television Laboratories, Inc.

[DOCSIS-OSSI] Refers to [, [SCTE 79-2], and [DOCSIS-OSSIv3.0].

[eDOCSIS] eDOCSIS Specification, CM-SP-eDOCSIS-129-170906, September 6, 2017, Cable Television Laboratories, Inc.

[IANA] "Internet Multicast Addresses," Internet Assigned Numbers Authority, http://www.iana.org/assignments/multicast-addresses.

[IEEE 802.3] IEEE Std 802.3 Part 3: Carrier sense multiple address with collision detection (CSMA/CD) access method and physical layer specifications, IEEE, March 8, 2002.

[GRE 1] IETF RFC 1701, Generic Routing Encapsulation (GRE), S. Hanks, T. Li, D. Farinacci, P. Traina. October 1994.

[GRE 2] IETF RFC 2784, Generic Routing Encapsulation (GRE). D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, March 2000.

[MPEG-SI] Information Technology - Generic Coding of Moving Pictures and Associated Audio: Systems, Recommendation H.222.0, ISO/IEC 13818-1, Section 2.6.17.

[OC-CC] OpenCable CableCARD™ Interface 2.0 Specification, OC-SP-CCIF2.0-I27-150330, March 30, 2015, Cable Television Laboratories, Inc.

[OC-CDL] OpenCable Common Download 2.0 Specification, OC-SP-CDL2.0-I13-120531, May 31, 2012, Cable Television Laboratories, Inc.

[OC-HOST2.1] OpenCable Host Device 2.1 Core Functional Requirements, OC-SP-HOST2.1-CFR-I17-130418, April 18, 2013, Cable Television Laboratories, Inc.

[OCAP] OpenCable Application Platform Specification, (OCAP), OC-SP-OCAP1.3.1-130530, May 30, 2013, Cable Television Laboratories, Inc.

[OUI] Organizationally Unique Identifier, IEEE, http://standards.ieee.org/regauth/oui.

[RFC 1112] IETF RFC 1112, Host Extensions for IP Multicasting, Steve E. Deering, August 1989.

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

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

[RFC 3171] IETF RFC 3171, IANA Guidelines for IPv4 Multicast Address Assignments, Z. Albanna, K. Almeroth, D. Meyer, M. Schipper, August 2001.

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

[RFC 3447] IETF RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003.

[RFC 3569] IETF RFC 3569, An Overview of Source-Specific Multicast (SSM), S. Bhattacharyya, July 2003.

[RFC 3927] IETF RFC 3927, Dynamic Configuration of IPv4 Link-Local Addresses, B. Aboba, S. Cheshire, E. Guttman, May 2005.

[RFC 4279]	IETF RFC 4279, Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), P. Eronen, H. Tschofenig, December 2005.
[RFC 5246]	IETF RFC 5246, The Transport Layer Security (TLS) Protocol, T. Dierks, E. Rescorla, August 2008.
[DOCSIS DSG]	DOCSIS Set-top Gateway (DSG) Interface Specification, CM-SP-DSG-I25-170906, September 06, 2017, Cable Television Laboratories, Inc.

3 DEFINITIONS AND ABBREVIATIONS

3.1 Terms and Definitions

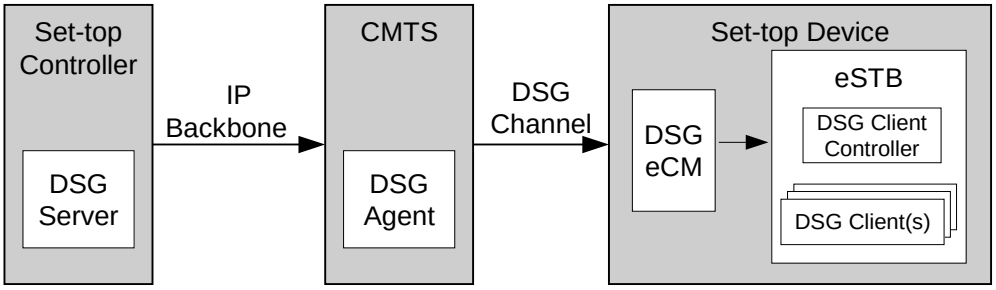


Figure 3–1 - DSG Terminology

This standard defines the following terms:

Application ID	This is a 16-bit field indicating a numeric ID for an application running on the Set-top Device. The Application ID is typically assigned through a Source Name Sub-table (SNS) from [SCTE 65] carried in the Broadcast DSG Tunnel.
CA_system_ID	This is a 16-bit field indicating the type of CA system applicable for either the associated ECM and/or EMM streams. The CA_system_ID may be used as a DSG Client ID in DSG Advanced Mode.
Card	A detachable CableCARD™ device defined in OpenCable and distributed by cable providers that connects to the cable receiver and manages Conditional Access.
DOCSIS 2.0+IPv6 DSG eCM	A DSG eCM that supports IPv6 Provisioning and Management and connected IPv6 eSAFEs.
DOCSIS Set-top Gateway	The DOCSIS Set-top Gateway (DSG) defines functionality on a DOCSIS CMTS and DOCSIS CM to support the configuration and transport of a class of service known as "Out-Of-Band (OOB) messaging" between a Set-top Controller (or application servers) and the customer premise equipment (CPE). The DSG is not intended for the delivery of programming content.
DSG Address Table	The collection of DSG Rules and DSG Classifiers contained within the DCD message. The DSG Client uses its DSG Client ID as an index into the DSG Address Table to determine what DSG Tunnel Address to receive.
DSG Advanced Mode	Operation with the DCD message. Address assignment is dynamic. The DSG Tunnel Address is determined by the DSG Agent and learned by the DSG Client through the DSG Address Table in the DCD message.
DSG Agent	The DSG Agent is the implementation of the DSG protocol within the CMTS. The DSG Agent creates the DSG Tunnel, places content from the DSG Server into the DSG Tunnel, and sends the DSG Tunnel to the DSG Client.

DSG Basic Mode	A deprecated mode of DSG operation without the DCD message. Address assignment was static in this mode. The DSG Tunnel Address was determined by the DSG Client and learned by the DSG Agent through configuration. This mode provided backwards compatibility with earlier versions of the DSG specification. This mode is not required to be supported by DSG eCMs.
DSG Channel	Any DOCSIS downstream channel that contains one or more DSG Tunnels.
DSG Classifier	A description of layer 3 and layer 4 filtering applied to DSG Tunnel traffic. DSG Classifiers may be specified in the DSG Agent and sent as a component of the DSG Address Table in the DCD Message.
DSG Client	The DSG Client terminates the DSG Tunnel and receives content from the DSG Server. There may be more than one DSG Client within a Set-top Device.
DSG Client Controller	The portion of the Set-top Device that handles the processing of DCD messages and makes decisions regarding the forwarding of DSG Tunnels within the Set-top Device.
DSG Client ID	This is an identifier that uniquely identifies a DSG Client. The DSG Client ID is unique per DSG Client, but is not unique per Set-top Device as the same DSG Client which provides the same function may exist in multiple Set-top Devices. In DSG Advanced Mode, the DSG Client ID may be an Application ID, a CA_system_ID, a DSG Well-Known MAC Address, or a broadcast ID.
DSG eCM	A DOCSIS Cable Modem that has been embedded into a Set-top Device and includes DSG functionality.
DSG Rule	A row entry within the DSG Address Table that assigns a DSG Client ID to a DSG Tunnel Address.
DSG SEB Client	DSG capable device that cannot establish a DOCSIS upstream connection, which therefore uses a DSG SEB Server to obtain DOCSIS interactive capabilities.
DSG SEB Server	DSG capable device that provides DOCSIS interactive capabilities to DSG SEB Clients residing on a shared home network interface, where the services include exposing of the DSG SEB Server's eCM such that the DSG SEB Client is able to acquire IP connectivity by way of the DSG SEB Server.
DSG Server	The DSG Server refers to any server such as an Application Server or other network attached device that provides content that is transported through the DSG Tunnel to the DSG Client.
DSG Tunnel	A stream of packets sent from the CMTS to the Set-top Terminal. In DSG Advanced Mode, a DSG Tunnel might be identified solely by its DSG Tunnel Address, or it might be identified by a combination of the DSG Tunnel Address along with other DSG Rule parameters: Classifier IP addresses, and UDP port numbers.
DSG Tunnel Address	This specifically refers to the destination MAC address of the DSG Tunnel. If the source MAC address, the destination IP address, or the source IP address is to be referenced, then that reference must be explicitly stated.
Embedded Set-top Box	An embedded Set-top Box is an embedded Service Application Functional Entity (eSAFE) defined in [eDOCSIS]. It includes the DSG Client(s), a DSG Client Controller, an embedded processor for an application environment, and either an embedded or removable module for Conditional Access.
One-way	This expression infers that the downstream path (from the network to the subscriber) is operational, and that the upstream path (from the subscriber to the network) is not operational. This may occur because the upstream path is not available, the Set-top Device is not registered, or the Set-top Device does not support a two-way mode of operation.

Out-Of-Band Messaging	The control and information messages sent from the Set-top Controller (or Application Server or similar device for legacy Out-Of-Band (OOB) messaging) to one or more Set-top Devices. Specifically, OOB infers the use of a dedicated channel for signaling which is separate from the video channels. This includes the following types of messages: • Conditional Access (CA) messages including entitlements • Service Information (SI) messages • Electronic Program Guide (EPG) messages • Emergency Alert System (EAS) messages • Other control or information messages
QoS Parameter Set	The set of Service Flow Encodings that describe the Quality of Service attributes of a Service Flow or a Service Class.
Service Class	A set of queuing and scheduling attributes that is named and that is configured at the CMTS. A Service Class is identified by a Service Class Name. A Service Class has an associated QoS Parameter Set.
Set-top Controller	This is the computer system responsible for managing the Set-top Devices within a cable system. It manages Set-top Devices through control and information messages sent via the Out-Of-Band channel.
Set-top Device	A cable receiver that contains an embedded Cable Modem for DOCSIS connectivity and an embedded Set-top Box. In OpenCable, this definition refers to the combination of an OpenCable Host Device 2.1 and a Card.
Set-top Extender Bridge	A client/server architecture that allows DSG Set-tops, incapable of establishing a DOCSIS upstream connection thru the eCM, to forward IP traffic over an alternate connection utilizing a Home Network Interface.
Two-way	This expression infers that the downstream path and the upstream path are operational.
UDP Stream	A sequence of packets with the same source IP address, source port number, destination IP address, and destination port.
Well-Known MAC Address	This refers to the MAC address of the DSG Client within the Set-top Device. This MAC address has been assigned by the manufacturer of a removable Card and/or embedded Conditional Access system, and has been made known to the MSO for use in configuring the DSG Agent.

3.1.1 Terms for DOCSIS DSG Device Versions

This standard defines the following terms when addressing different versions of DOCSIS DSG devices:

Pre-3.0 DOCSIS DSG eCM: A DOCSIS 1.x, 2.0 or other non-3.0 DSG eCM
Pre-3.0 DOCSIS DSG CMTS: A DOCSIS 1.x, 2.0 or other non-3.0 DSG CMTS
DOCSIS 3.0 DSG eCM: A DSG eCM which implements the DOCSIS 3.0 requirements
DOCSIS 3.0 DSG CMTS: A DSG CMTS which implements the DOCSIS 3.0 requirements

3.2 Abbreviations and Acronyms

This standard uses the following abbreviations:

AES-CBC	Advanced Encryption Standard – Cipher Block Chaining
CA	Conditional Access
CM	Cable Modem

CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
DCC	Dynamic Channel Change
CVT	Code Version Table (Common Download)
DCD	Downstream Channel Descriptor
DOCSIS®	Data-Over-Cable Service Interface Specifications
DS	Downstream
DSG	DOCSIS Set-top Gateway
DVS	Digital Video Subcommittee
EAS	Emergency Alert System
eCM	Embedded Cable Modem
EPG	Electronic Program Guide
eSTB	Embedded Set-top Box
FOM	Figure of Merit
HFC	Hybrid Fiber Coax
IP	Internet Protocol
MAC	Media Access Control
MSO	Multi System Operator
MTA	Multimedia Terminal Adaptor
MTU	Maximum Transmission Unit
OCAP	OpenCable Application Platform
OOB	Out-Of-Band
SCTE	Society of Cable Telecommunications Engineers
SEB	Set-top Extender Bridge
SEBC	DOCSIS Set-top Gateway SEB Client
SEBS	DOCSIS Set-top Gateway SEB Server
SI	Service Information
SNS	Source Name Sub-Table
SSD	Secure Software Download
STD	Set-top Device
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type-Length-Value
UCID	Upstream Channel ID
uimsbf	unsigned integer, most significant bit first
UDP	User Datagram Protocol
US	Upstream

VSP	Vendor-Specific Parameter
XAIT	Extended Application Information Table (OCAP)

4 REFERENCE ARCHITECTURE

The reference architecture for the data-over-cable services and interfaces is shown in Figure 1–2.

The DOCSIS Set-top Gateway architecture is an adaptation of the DOCSIS reference architecture shown in Figure 1–1. Figure 4–1 below shows how the DOCSIS Set-top Gateway layers on the DOCSIS reference architecture. As shown in this figure, there are potentially multiple servers (1 to K) that function as the Set-top Controller, a regional IP network or IP backbone that connects these servers to potentially multiple CMTSs (1 to M) located in distribution hubs or headends, and an HFC/Cable Network that connects the CMTS to the Set-top Devices located in the subscriber's home. The DOCSIS Set-top Gateway as shown in this diagram is implemented in the CMTS.

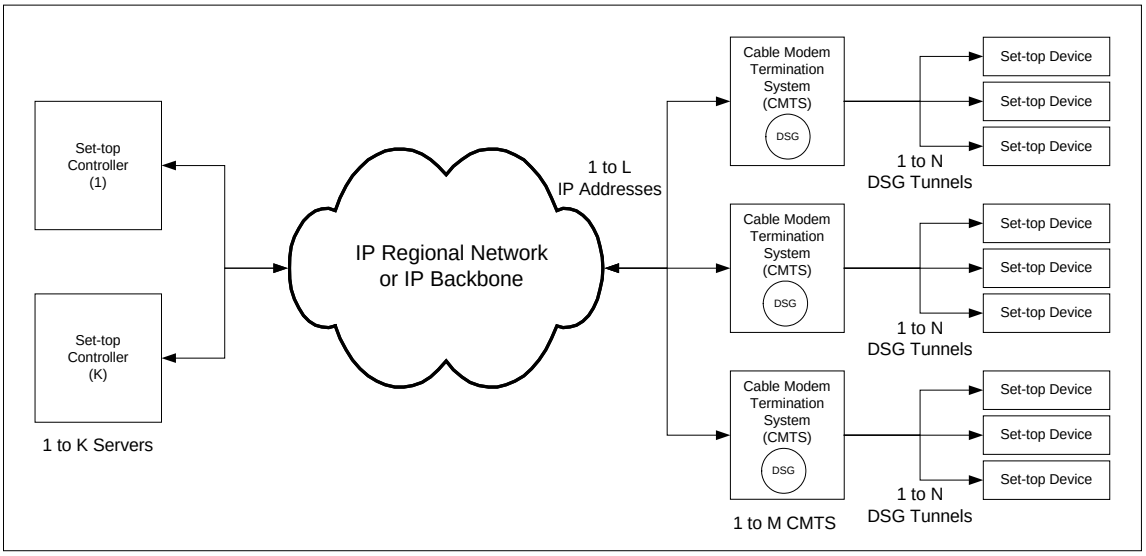


Figure 4–1 - DOCSIS Set-top Gateway System Physical Diagram

The DSG Agent maps IP datagrams received on its IP Network Interface to N DSG Tunnels on the DOCSIS transport. In particular, the DSG Agent:

- Receives IP Multicast datagrams on potentially multiple IP addresses (1 to L).
- It then maps these datagrams to one of potentially multiple DSG Tunnels on the DOCSIS transport and forwards them on to the DSG Clients.

Networking solutions are available for either legacy DSG Servers or legacy IP networks that do not support IP Multicast. Refer to Section 5.7.8.

The instantiation of the DSG Protocol within the Set-top Device is referred to as the DSG Client. The instantiation of the DSG Protocol within the CMTS is referred to as the DSG Agent. The Set-top Controller or application server which sources content is referred to as the DSG Server. Thus the OOB messages originate at the DSG Server, pass through the DSG Agent, onto the DSG Tunnel, and terminate at the DSG Client. The expression DSG Tunnel Address implicitly refers to the destination MAC address of the DSG Tunnel.

The logical view of the DOCSIS Set-top Gateway is shown in Figure 4–2.

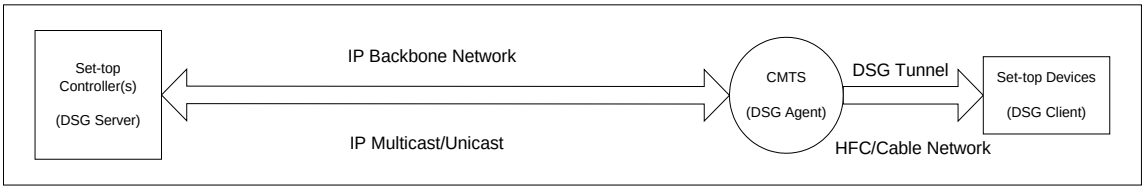


Figure 4–2 - DOCSIS Set-top Gateway Logical Diagram

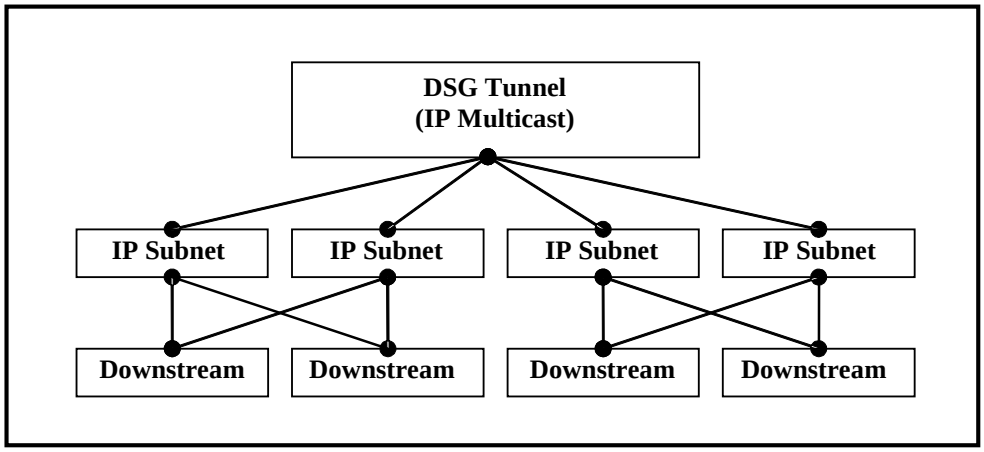


Figure 4–3 - DSG Tunnel within the DSG Agent

The DSG Agent has to define the uniqueness of a DSG Tunnel in relation to an IP Multicast destination address, IP subnets, and DOCSIS downstreams. This relationship is shown in Figure 4–3 above and is described below.

The following conditions exist at the DSG Agent:

- A DSG Agent may have one or more DOCSIS downstream channels and one or more IP subnets.
- An IP subnet may span one or more DOCSIS downstream channels.
- A DOCSIS Downstream Channel may be a member of one or more IP Subnets.
- There is one instantiation of the DSG Tunnel per DSG Agent and each IP subnet requiring the DSG Tunnel joins the IP Multicast session. The IP address associated with the DSG Tunnel is the IP address of the IP Multicast connection from the DSG Server to the DSG Agent.

4.1 DSG Basic Mode

The term DSG Basic Mode was previously used in this standard to refer to a method of delivering DSG Tunnels without using a DCD message. This mode of operation is now deprecated. There may still be legacy units operating in DSG Basic mode deployed in some systems.

4.2 DSG Advanced Mode

In DSG Advanced Mode, the DSG Tunnel Address is determined dynamically by an entry in the DSG Address Table. The DSG Address Table is located in the DOCSIS MAC Management Message called Downstream Channel Descriptor (DCD). The DSG Address Table is indexed by the DSG Client with its DSG Client ID. The following features may be achieved by performing an appropriate DSG Client ID to DSG Tunnel Address association and the concept of regionalization:

- Multiple DSG Clients can be assigned to a single DSG Tunnel. This would be a one-to-many scenario.
- A DSG Client can be given different DSG Tunnels based upon downstream or upstream associations.
- The uniqueness of a DSG Tunnel for a particular DSG Client is per downstream on a one-way HFC plant, and per upstream on a two-way HFC plant.

DSG Advanced Mode uses a multicast (group) MAC address for the DSG Tunnel Address. Since more than one IP multicast address may map to the same multicast MAC address when using IP Multicast [RFC 1112], the DSG Client should use both the destination MAC address and the destination IP address to receive the DSG Tunnel.

A multicast (group) MAC address is used for DSG Advanced Mode since DSG Tunnels are multicast in nature. Use of DSG Advanced Mode presumes that the DOCSIS 1.0 CMs have been configured to disable the IP Multicast forwarding of DSG traffic.

4.3 DSG and IP Multicast

DSG is intended as an extension to IP Multicast. In the general case, the addressing of the IP Multicast packet and the DSG Tunnel are the same. The DSG Tunnel encapsulates the IP Multicast datagram in a DOCSIS frame. The one exception to the addressing is that under certain circumstances, DSG allows the MAC address to be re-written to another multicast MAC address.

The signaling protocols for the two are different. The fundamental reason for this is the need for DSG to work on a one-way plant. IP Multicast has several different protocols which allow end points to join an IP Multicast session. In DSG, the CMTS assigns end points to DSG Tunnels using a DOCSIS MAC management message.

5 DOCSIS SET-TOP GATEWAY

The DSG Agent is intended to provide transparent transport of Out-Of-Band messaging over a DOCSIS channel that is traditionally carried on dedicated channels, specifically those defined in [SCTE 55-1] and [SCTE 55-2]. The following sections detail the requirements and normative behavior of the DSG Server, DSG Agent, and DSG Client for this service.

5.1 Assumptions and Constraints

The DSG Agent will exist within a constrained environment. This section details the assumptions regarding the environment that is required in order to enable this service.

- Any implementation of the DOCSIS Set-top Gateway will work with DOCSIS 1.0, DOCSIS 1.1, DOCSIS 2.0, and DOCSIS 3.0 networks.
- Any implementation of the DOCSIS Set-top Gateway will work for both embedded and removable security implementations within a Set-top Device.
- Any implementation of the DOCSIS Set-top Gateway will not impact the security of the CA systems negatively.
- The DSG Agent will support the transport of multiple simultaneous Conditional Access systems.
- The DSG Agent will provide one-way downstream transport for Out-Of-Band messaging.
- Since the DSG Agent provides a one-way stream of Out-Of-Band messages, DOCSIS Baseline Privacy Interface (BPI) and Baseline Privacy Plus Interface (BPI+) do not apply to the DSG transport.
- The Set-top Device will use an IP session over DOCSIS for all return traffic. For example, if an Out-Of-Band polling message is sent from the DSG Server to the Set-top Device via the DSG Agent within the CMTS, the Set-top Device response to the message is returned to the headend via IP over DOCSIS.
- The Set-top Device will operate in a one-way environment. Examples of the limited functionality available to a Set-top Device in a one-way environment might be:
    - Analog NTSC audio-visual programming (clear, non-scrambled).
    - Digital audio-visual programming using MPEG-2 transport including, but not limited to, standard and high definition MPEG-2 Main Profile @ Main Level video and Dolby AC-3 audio.
    - Broadcast (in-the-clear), subscription-based (scrambled or encrypted), and call-ahead Pay-Per-View (PPV) (scrambled or encrypted) services. (Call-ahead Pay-Per-View is a paid service in which the viewer pre-subscribes selected programming via telephone.)
    - Processing and enforcement of Copy Protection.
    - Pass through of digital high definition audio-visual programming.
- Considerations for DOCSIS 3.0:
    - DSG Tunnels will not contain IPv6 data unless it is encapsulated.
    - DSG Agents, DSG Client Controllers and DSG eCMs will not support IPv6 DSG classifiers.
    - A DSG Client Controller will not be affected by DOCSIS 3.0 operation; no new messages will be used between the DSG Client Controller and the eCM.

5.2 Requirements - General

5.2.1 DSG Server

- For DSG Basic Mode only, the DSG Server MUST maintain a minimum data rate of one packet per second on at least one DSG Tunnel within each unique group of DSG Tunnels which serve a CPE device. This requirement is to keep the acquisition time of the appropriate DOCSIS channel to less than one second. The intent is that the data be present at a sufficiently high rate such that in the process of searching for and trying to acquire a DOCSIS channel, no exorbitant amount of time needs to be spent on any DOCSIS channel that does not carry OOB data.
- The DSG Server MUST support either IP Multicast or IP Unicast.
- The DSG Server MUST NOT send packets of a size that would cause IP fragmentation to occur.

NOTE: The calculation of payload size should allow for the 20 byte IP protocol overhead, the 8 byte UDP overhead, and any VPN/IPSec or other IP protocol overhead that may be in use. Fragmented IP/UDP packets would not contain the port number in every fragment. For the eCM classifiers to successfully filter fragments by port, the filters would have to be stateful filters; a complication to be avoided. Annex D was added to provide for the orderly segmentation of MPEG tables by the DSG Server.

- A DSG Server that produces an industry-standard data stream among those listed in Table 5–2 MUST NOT include in this stream any data other than that allowed by the indicated standard. The DSG Server MUST emit the data stream such that a DSG Rule and its optional Classifiers can distinctly describe a tunnel containing only this stream. For instance, distinct UDP port numbers or distinct destination IP addresses, sometimes in combination with source IP addresses, are adequate to distinguish streams.
- A DSG Server that produces an Object or Data Carousel data stream associated with an Application Client ID MUST NOT include in this stream any other data including non-carousel related MPEG sections or unspecified data formats. Annex E was added to provide for the encapsulation of such data.

5.2.2 DSG Agent

The following are the normative requirements for the DSG Agent within a CMTS.

5.2.2.1 General Operation

- The DSG Agent MUST be implemented on a CMTS.
- The DSG Agent MUST implement the MIB defined in Annex A of this standard and be configurable through this MIB.
- The DSG Agent SHOULD allow SNMP access to the DSG MIBs on the same IP address it allows access to the DOCSIS MIBs.

5.2.2.2 Network Side Operation

- The DSG Agent MUST NOT forward frames with Ethertypes other than 0x0800, corresponding to IP, onto the DSG Tunnel.
- The DSG Agent MUST be able to filter packets based on the UDP port number and the IP protocol type, after de-encapsulation of any IP tunneling protocols that may have been used between the DSG Server and the DSG Agent. This requirement should be interpreted as an input access list on a CMTS. This requirement should not be interpreted as the CMTS using the UDP ports to route packets to different DSG Tunnels.
- The DSG Agent MAY use source IP address verification to prevent forwarding of packets originating from other than a trusted DSG Server.
- The DSG Agent MAY use dedicated links, Secure Sockets Layer (SSL/TLS), virtual private networks (VPN), IPSec, or other means to provide secure connections between it and the DSG Server. The specifics of how this may be implemented are beyond the scope of this document.

5.2.2.3 RF Side Operation

- The DSG Agent MUST support a one-way (downstream) transport without requiring return path functionality from the DSG Client.
- The DSG Agent MUST be able to support forwarding on one or more DOCSIS downstream channels.
- The DSG Agent MUST simultaneously support STDs operating in DSG Basic Mode and STDs operating in DSG Advanced mode.
- The downstream DOCSIS PDUs encapsulating the DSG OOB messages MUST have Frame Control bits set to the Packet PDU code point by the CMTS.
- The CMTS MUST NOT send standard DOCSIS MAC Management messages to the DSG Tunnel Address.
- The DSG Agent MUST be able to support at least 32 DSG Rules per DCD Message.

NOTE: Since a single DSG Rule represents a single DSG Tunnel on a particular downstream channel, in effect this requires the DSG Agent to support at least 32 DSG Tunnels per downstream channel.

- The DSG Agent MUST be capable of rate limiting or rate shaping each DSG Tunnel, as described in [DOCSIS-RFI]. The rate limiting parameters MUST be configurable per DSG Tunnel and are determined by the QoS Parameter Set associated with the Service Class assigned to the DSG Tunnel. The DCD MAC Management Message is not included in this calculation.

NOTE: One application in which rate-limiting functionality may be used is an OpenCable Host. The buffer capacity contained in the OpenCable Host is limited and data rates in excess of 2.048 Mbps can potentially overflow this buffer. Thus, the maximum sustained traffic rates for all DSG Tunnels that cross the Card interface for a particular OpenCable host device should be chosen such that the total traffic crossing the Card interface for that host—including DCD message fragments, DSG Tunnels, and any other data—does not exceed 2.048 Mbps. Note that encapsulation overhead and the size of the packets traversing this interface could reduce the available bandwidth. Refer to [OC-CC] for additional information.

- The DSG Agent MUST forward the IP packets received at its configured IP address(es) by performing a MAC level rewrite by replacing the destination MAC address with the DSG Tunnel Address and the source MAC address with the DSG HFC-side MAC address. The DSG Agent MUST NOT modify the IP Source Address, IP Destination Address, or IP Protocol Type of the IP header. The CMTS containing the DSG Agent MUST NOT modify the IP Source Address or IP Protocol Type of the IP header. The CMTS containing the DSG Agent MUST NOT modify the IP Destination Address of the IP header except in the context of supporting IP Unicast message streams as defined in Section 5.2.2.4. The DSG Agent or containing CMTS MAY modify other fields of the IP header. The payload of the IP packet, including the UDP port numbers, MUST remain unchanged.

5.2.2.4 IP Addressing for DSG Tunnels

- The DSG Agent MUST allow the mapping of an IP Multicast address to a DSG Tunnel Address. The DSG Agent MUST NOT allow one IP Multicast address to be mapped to more than one DSG Tunnel Address.

NOTE: Many DSG Servers may send content to the same IP Multicast stream which would be associated to one DSG Tunnel. This scenario is referred to as "many-to-one" in this standard.

- The DSG Agent MUST be configured so that each interface requiring the DSG Tunnel is a member of the appropriate multicast group. An IP Multicast address to DSG Tunnel Address association MAY span one or more IP subnets. An IP Subnet MAY span one or more downstreams.

NOTE: A DSG Rule with a Broadcast Client ID among those listed in Table 5–2 can have one and only one Broadcast client ID. When configuring the DSG Agent the operator needs to ensure that the eSTB behind the DSG eCM will be able to uniquely identify data from the different Broadcast tunnel data streams. For this reason when configuring a DSG Rule with a Broadcast Client ID, if the Client ID and the DSG Tunnel Address are not enough to uniquely identify the different data streams, then the operator needs to define for that DSG Rule a single DSG classifier with at least the Destination IP address and a single UDP destination port number. The combination of DSG MAC Address, Source IP address/mask, IP destination address and UDP destination port number needs to be unique across all rules in a DCD containing Broadcast Client IDs. A given DCD may contain multiple rules for a given Broadcast Client ID. The DSG Client Controller is expected to select at most one rule to use for a given Broadcast Client ID.

The use of an IP Unicast address to transport DSG Tunnel information is intended only to support legacy DSG servers and networks that do not support multicast IP routing. Otherwise, the binding of an IP Unicast address to a DSG Tunnel is explicitly deprecated. If the message stream from the DSG Server to the DSG Agent is IP Unicast, then the CMTS that hosts the DSG Agent MUST support that IP Unicast message stream by at least one of the following three methods:

- The CMTS supports IP Multicast tunneled over IP Unicast. The DSG Server or a router external to the DSG Server would encapsulate the IP Multicast packet within an IP Unicast packet. The CMTS would de-encapsulate the IP Unicast tunnel and forward the IP Multicast packet to the DSG Agent [GRE 1] [GRE 2]. In this case, the DSG Agent receives an IP Multicast packet, and so the DSG Classifier is configured with the appropriate IP Multicast destination address.
- The CMTS translates the IP Unicast address to an IP Multicast address. The new multicast packet would be forwarded to the DSG Agent. In this case, the DSG Agent receives an IP Multicast packet, and so the DSG Classifier is configured with the appropriate IP Multicast destination address.
- The CMTS forwards the IP Unicast packet directly onto the DOCSIS downstream. This option may cause an IP Unicast packet with the provisioned DSG Tunnel MAC address to be forwarded in a multicast fashion on multiple DOCSIS downstream channels. In this case, the DSG Agent receives an IP Unicast packet, and so the DSG Classifier is configured with the appropriate IP Unicast destination address.

5.2.2.5 MAC Addressing for DSG Tunnels

- The destination MAC address of the DSG Tunnel is known as the DSG Tunnel Address. The DSG Agent MUST be configurable to use a multicast (group) MAC address as the DSG Tunnel Address. The use of a unicast MAC address is explicitly deprecated.
- A multicast (group) MAC address may be derived by taking a unicast (individual) MAC address, and setting the I/G bit to a one. The I/G bit is the Individual/Group bit, and it is the LSB of the first byte of the MAC address [IEEE 802.3].
- A DSG Client Controller would use a DSG Client ID as an index into the DSG Address Table in the DCD MAC management message to discover the DSG Tunnel Address. The DSG Client ID could be a DSG Broadcast ID, a Well-Known MAC Address, an Application ID, or a CA_system_ID.
- In certain cases, an operator may want DSG Clients that support DSG Advanced Mode to receive DSG Basic Mode Tunnels. To support such a configuration, and to provide consistency of provisioning, a DSG Basic Mode Tunnel is defined as a DSG Tunnel in which both the DSG Tunnel Address and the DSG Client ID match the Well-Known MAC Address provided by the Set-top Device manufacturer.

5.2.2.6 DOCSIS 3.0 DSG Agent Considerations

DOCSIS 3.0 introduces new concepts which are relevant to DSG Agent operation including downstream channel bonding and enhanced multicast.

5.2.2.6.1 Downstream Bonding Considerations

The DSG Agent is to be configured such that all DSG tunnels are sent on primary-capable downstream channels. A DSG eCM discards DCD messages or DSG tunnel traffic received on non-Primary Downstream channels.

The DSG Agent MUST transmit each instance of a DSG Tunnel on a single downstream channel, as non-bonded traffic.

In DOCSIS 3.0, a downstream channel may be shared by multiple CMTS MAC domains. A downstream channel shared by multiple MAC domains contains multiple MDD messages with different source MAC addresses. A DOCSIS 3.0 eCM parses the source MAC address of the MDD and DCD messages to ensure that the CMTS MAC domain of the MDD message is the same as that of the DCD message. However, a Pre-3.0 DOCSIS DSG eCM does not parse the source MAC address of the DCD message and would be confused if it received multiple DCDs from different MAC Domains on a downstream channel. The DSG Agent MUST NOT insert DCD messages from more than one MAC Domain on any downstream channel.

5.2.2.6.2 Multicast Considerations

In DOCSIS 3.0, the DSG Agent labels all multicast traffic with a DSID to be used by the eCM for filtering and forwarding purposes. The DSG Agent broadcasts the DSID(s) to be used for DSG tunnel traffic in the DSG DA-to-DSID Association Entry TLV in the MDD message. Exactly one DSID value is assigned for each DSG Tunnel Address, and as each DSG Tunnel can have multiple classifiers associated with it, multiple IP Multicast streams can be associated with a single DSID. Thus, forwarding of DSG Tunnel traffic is different from standard DOCSIS 3.0 Multicast forwarding where each IP Multicast Session is assigned and labeled with its own DSID. The DSG Agent is not permitted to modify the DSID that is associated with a Destination Address once it has been added to the MDD message; as such, entries in the DSG DA-to-DSID Association Entry TLV can only be added or deleted, but never modified. The DSG Agent can only modify the DSG DA-to-DSID Association Entry TLV in the MDD message when it modifies the DCD message due to the addition or deletion of DSG rules.

The DSG Agent is responsible for ensuring that the DSG eCM continues to receive DSG tunnel traffic labeled with DSIDs known to the DSG eCM. The DSG Agent is also responsible for ensuring that DSG tunnel traffic is not sent to any eCM interface other than the DSG tunnel interface.

The DSG Agent is not permitted to add or delete any multicast DSIDs associated with the DSG tunnel interface in the Registration Response message. This includes any static multicast sessions erroneously created via the CMTS Static Multicast Session Encodings in which the Static Multicast CMIM indicates the DSG tunnel interface. The DSG Agent MUST NOT signal any multicast DSIDs used to label DSG tunnel traffic in the Registration Response message.

The DSG Agent is not permitted to initiate a DBC transaction to add or delete a multicast DSID associated with the DSG tunnel interface. The DSG Agent MUST NOT initiate a DBC transaction to signal any multicast DSIDs used to label DSG tunnel traffic.

The Downstream Multicast QoS mechanisms described in [DOCSIS-MULPI] do not apply to DSG tunnels.

5.2.3 DSG eCM

- The DSG eCM MUST coexist with other DOCSIS devices on the same DOCSIS channel (Standalone Cable Modem, Embedded MTA, Embedded PS, etc.).
- The DSG eCM component MUST implement the MIB module DSG-IF-STD-MIB defined in Annex B of this standard to indicate the eCM and DSG Client Controller interactions for DSG operations in a Set-top Device.
- The DSG eCM MUST support the DOCSIS Event extensions defined in Annex C of this standard.
- The DSG eCM MUST be able to function in either a one-way or two-way environment.
- The DSG eCM MUST support the bridging of 8 simultaneous DSG Tunnel MAC addresses.

NOTE: An MDF-capable DSG eCM with MDF-enabled [DOCSIS-MULPI] will use a DSID in place of the DSG Tunnel MAC address for purposes of forwarding DSG tunnel traffic.

- The DSG eCM MUST support at least twelve simultaneous DSG Classifiers per DSG Tunnel MAC Address, and MUST support at least thirty-two simultaneous DSG Classifiers in total.
- The DSG eCM MUST NOT perform any DSG operations if a DSG Client Controller is not present in the Set-top Device. DSG operations include but are not limited to: the hunt for a DOCSIS downstream channel with a valid DSG tunnel identifier (DCD and/or well-known CA MAC addresses); acquisition of the DCD; acquisition and forwarding of any DSG tunnels; etc. As a result, the provisions of this standard only apply to a DSG eCM when DSG is active.
- The DSG eCM MUST follow the standard DOCSIS initialization and registration process, with the following specific exceptions:
    - In acquiring the appropriate DOCSIS downstream channel in DSG Advanced Mode, the DSG eCM MUST search for the first DOCSIS channel that contains a DCD message, and pass the contents of the DCD message (including fragment information) to the DSG Client Controller. The DSG Client Controller will make a determination on the suitability of the DCD.

- The DSG eCM MUST only attempt to register on the network after acquiring the appropriate DOCSIS downstream channel.
- The DSG eCM MUST NOT reboot under circumstances in which the upstream channel is impaired. Instead of rebooting, the DSG eCM MUST continue to receive and process the DOCSIS downstream channel.
- The DSG eCM MUST periodically attempt to re-register after loss of the upstream channel (except when the upstream transmitter has been disabled).
- The state transition between the one-way and two-way modes of operation MUST be as shown in Figure 5–1.

The specifics of how these requirements are implemented are detailed in Section 5.4.

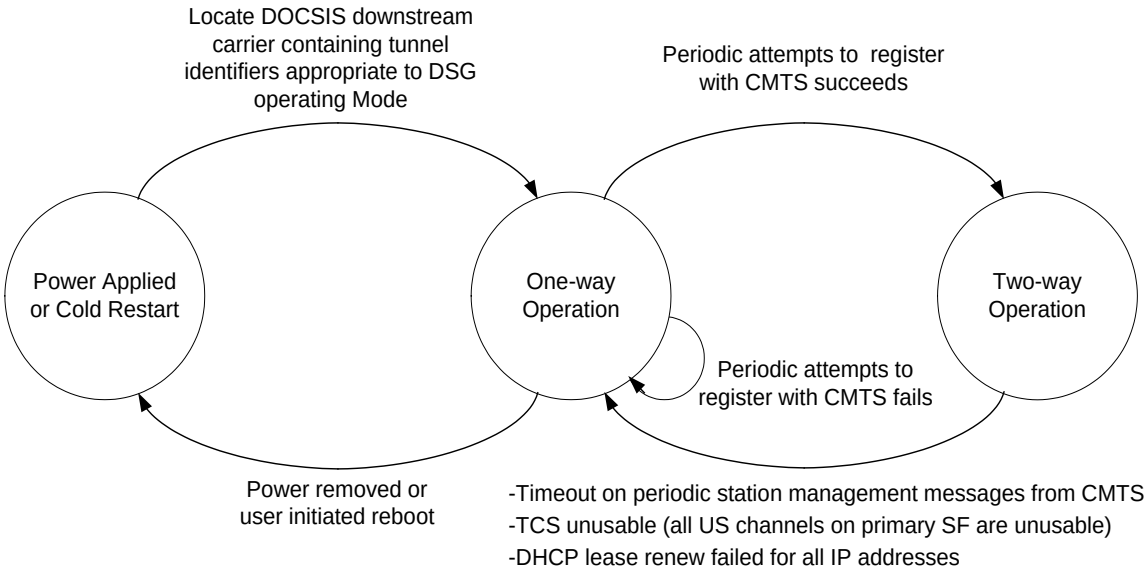


Figure 5–1 - DSG eCM State Transition Diagram

5.2.3.1 DA-to-DSID Association of DSG Tunnels when MDF is Enabled

DOCSIS 3.0 introduces several new concepts which are relevant to DSG operation: downstream service group resolution, and upstream channel bonding.

Upon initialization, the DOCSIS 3.0 DSG eCM searches for a DSG downstream channel which carries both DOCSIS SYNC messages and a DCD message. The DOCSIS downstream channel on which the DSG eCM finds a DCD message may be considered a DOCSIS 3.0 primary-capable downstream channel if it additionally contains an MDD message containing ambiguity resolution TLVs. If no MDD messages are detected, the DSG eCM reverts to DOCSIS 2.0 operation, continues to gather upstream parameters, then ranges before continuing on to establish IP connectivity and then registers with the CMTS.

If the DSG eCM finds a DCD message on a primary-capable downstream channel which also contains an MDD message, the eCM ensures that the MDD message has a source MAC address matching the source MAC address of the DCD message. This ensures that the MAC domain of the DCD message is the same as the MAC domain of the MDD message. If the source MAC address of the MDD message differs from the source MAC address of the DCD message, the DSG eCM discards the MDD message and reverts to DOCSIS 2.0 operation.

If the DOCSIS downstream channel on which the eCM finds a DCD message contains an MDD message with a source MAC address matching that of the DCD message, the eCM determines the MD-DS-SG (MAC domain downstream service group) prior to forwarding the DCD message to the DSG Client Controller. This is to maintain consistency in tuner usage in downstream ambiguity resolution for both CMs and DOCSIS 3.0 DSG eCMs. If the DSG client controller considers the DCD message to be invalid, the DOCSIS 3.0 DSG eCM searches all primary-

capable downstream channels within the MAC domain for a valid DSG downstream before scanning other downstream channels. This increases the chance that the DSG eCM will register as a DOCSIS 3.0 DSG eCM. The DSG eCM uses the 'Downstream Active Channel List TLV' in the MDD message to get the list of primary-capable downstream channels in the MAC domain.

Neither DCD messages nor DSG tunnel traffic are sent bonded across multiple downstreams. The DOCSIS 3.0 DSG eCM forwards DCD messages and DSG tunnels received on the Primary Downstream Channel to the DSG Client Controller. The DOCSIS 3.0 DSG eCM discards DCD messages and DSG tunnels not received on the Primary Downstream Channel.

In the case of a failure in the upstream path, the DOCSIS 3.0 DSG CM operating in Multiple Transmit Channel (MTC) Mode enters one-way mode when the CM loses all of the upstream channels on which the primary upstream service flow is assigned. (This includes the case in which the DOCSIS 3.0 DSG eCM maintains upstream connectivity with one or more upstream channels not associated with the primary upstream service flow.) If a failure occurs in the upstream path that causes it to switch from an operational state to one-way mode, the DOCSIS 3.0 DSG eCM in MTC Mode periodically attempts to restart the upstream ambiguity resolution process after the expiration of the Tdsg3 timer.

5.2.3.2 DOCSIS 3.0 MDF-capable DSG eCM Considerations

The enhanced multicast operation introduced in DOCSIS 3.0 additionally impacts DSG operation. DOCSIS 3.0 introduces the concept of Multicast DSID Forwarding (MDF) in which the CMTS labels all downstream multicast traffic with a DSID, which is communicated to the eCM to be used for filtering and forwarding purposes. MDF can be enabled on DOCSIS 3.0 CMs and on DOCSIS 2.0+IPv6 CMs that indicate they are MDF-capable by reporting a value of 1 or 2 in the MDF Modem Capability.

When MDF is enabled on the MAC Domain, DSG tunnel traffic is to be labeled with a DSID that the CMTS advertises in the DSG DA-to-DSID Association Entry in the MDD message. If the DSG DA-to-DSID Association Entry is present in the MDD message, the MDF-capable DSG eCM filters and forwards DSG tunnel traffic based on the DSID communicated in the DSG DA-to-DSID Association Entry in the MDD message.

When MDF is enabled, it may be necessary for the MDF-capable DSG eCM to update its DSIDs in response to an indication of a change to its DSG tunnels such as a DCD message with an updated change count or message from the DSG Client Controller altering a DSG tunnel. When MDF is enabled, the MDF-capable DSG eCM re-learns the DSG DA-to-DSID Association Entries in the MDD message after it completes a DBC or DCC transaction that changes the primary downstream channel.

5.3 Requirements - DSG Tunnel Definition

DSG Advanced Mode Tunnels use a DOCSIS MAC management message called the Downstream Channel Descriptor (DCD), which provides dynamic provisioning of DSG Tunnels and allows the implementation of several additional features:

Consolidated Keep-Alive: The one DCD message provides a consolidated keep-alive function for all the DSG Tunnels on a downstream. This keep-alive is provided by the DSG Agent rather than the DSG Server.

Enhanced Security: This is achieved through a combination of techniques. First, the destination MAC address of the DSG Tunnel may be replaced dynamically. If the DSG Client ID were to ever become widely known, it may provide the opportunity for a PC to assume that MAC address and snoop the DSG Tunnel. This problem is reduced by substituting the known DSG Tunnel Address with a MAC addresses assigned by the DSG Agent. DSG Advanced Mode also allows the DSG Tunnel to be further qualified by the destination IP address, source IP address, and destination UDP port.

One-to-Many: With the ability to re-assign the DSG Tunnel Address, it is possible to have one DSG Tunnel service more than one distinct DSG Client.

Regionalization: DSG Advanced Mode allows the DSG Tunnels to be unique per downstream on a one-way plant, and unique per upstream on a two-way plant.

Layer 4 Multiplexing: In DSG Advanced Mode, a DSG Server may use destination UDP ports to distinguish content, and then combine all the content onto one IP session. This reduces the number of IP Unicast or IP Multicast

addresses required for the configuration of DSG Tunnels. Specifically, the DSG Server would do the multiplexing of UDP ports into an IP stream, the DSG Agent would forward that IP stream to a DSG Tunnel, and the DSG Client would de-multiplex the stream based upon UDP port number.

5.3.1 Downstream Channel Descriptor (DCD)

DSG Advanced Mode uses a DSG Address Table within a DOCSIS MAC Management Message called the Downstream Channel Descriptor (DCD) to manage the DSG Tunnel. The DCD message provides several functions:

- It provides a consolidated keep-alive mechanism for all DSG Tunnels on a particular downstream, even if the IP network has been interrupted. The keep-alive for a particular DSG Tunnel is based upon the existence of a series of DCD messages and upon the inclusion of that DSG Tunnel within those DCD messages.
- It provides an address substitution and classification mechanism to increase the flexibility and security of the DSG Tunnel.
- It allows the use of multicast addresses. Specifically, multicast sessions from the IP backbone based upon [RFC 1112] addressing may be passed through the DSG Agent as a DSG Tunnel without address translation.
- It allows the MSO to assign any Set-top Device to any DSG Tunnel.
- It allows global changes to the DSG Client timers to allow operator driven changes in DSG eCM performance.
- It provides a list of downstream frequencies which contain DSG Tunnels.

The DCD Message contains a group of DSG Rules and DSG Classifiers. This collection of DSG Rules and DSG Classifiers in the DCD message is known as the DSG Address Table. The DSG Address Table contains information relevant to the tunnels on the current downstream that allows a DSG Client Controller to discover the presence of applicable tunnels, their DSG Tunnel Addresses and associated DSG Classifiers. The DSG Agent MUST include all DSG Tunnels on the current downstream in the DSG Address Table in the DCD message. The DCD message is unique per downstream. When necessary, the DCD message is broken into a number of DCD message fragments.

The DSG Agent MUST insert at least one DCD message fragment per second. The DSG Agent SHOULD send a complete DCD message at least once per second on each DOCSIS downstream that contains a DSG Tunnel. Since a DCD message containing a single TLV cannot be fragmented, the DSG Agent MUST be capable of inserting a DCD message containing only a DSG Configuration TLV at least once per second on each DOCSIS downstream that does not contain a DSG Tunnel. It is expected that the DSG Client Controller will accept the inclusion of a DSG Client ID in the DSG Address Table as an indication that a DSG Tunnel exists on this downstream for a DSG Client corresponding to that DSG Client ID.

The DCD message fragments MUST be LLC unnumbered information frames and be compatible with the format of a DOCSIS MAC Management Message. The DCD message fragments MUST NOT exceed 1522 bytes in length, as measured from the beginning of the Ethernet destination MAC address to the end of the CRC. The MAC Management Message Header and the values of the Version field and the Type field for DCD in the MAC Management Message Header are defined in [DOCSIS-RFIv2.0].

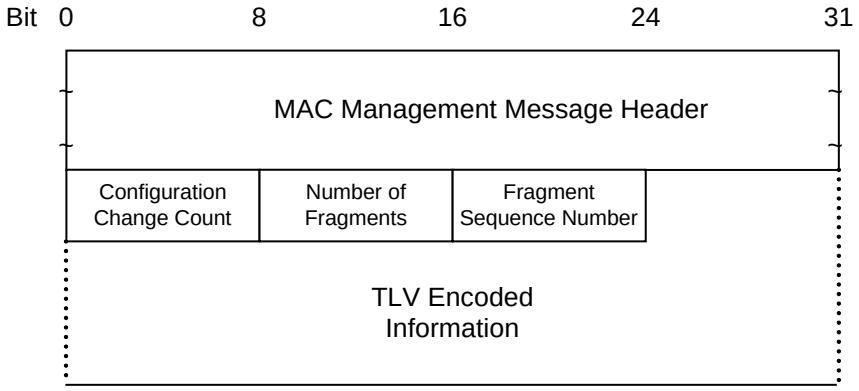


Figure 5–2 - DCD Message Fragment Structure

A DSG Agent MUST generate Downstream Channel Descriptors in the form shown in Figure 5–2, including the following parameters:

Configuration Change Count: Incremented by one (modulo the field size) by the DSG Agent whenever any of the values of the Downstream Channel Descriptor change. The configuration change count MUST be the same value across DCD message fragments.

Number of Fragments: Fragmentation allows the DCD TLV parameters to be spread across more than one DOCSIS MAC Frame, thus allowing the total number of DCD TLV parameters to exceed the maximum payload of a single DCD MAC management frame. The value of this field represents the number of DCD MAC management frames that a unique and complete set of DCD TLV parameters are spread across to constitute the DCD message. This field is an 8-bit unsigned integer. The default value for this field is 1.

Fragment Sequence Number: This field indicates the position of this fragment in the sequence that constitutes the complete DCD message. Fragment Sequence Numbers MUST start with the value of 1 and increase by 1 for each fragment in the sequence. Thus, the first DCD message fragment would have a Fragment Sequence Number of 1 and the last DCD message fragment would have a Fragment Sequence Number equal to the Number of Fragments. The DSG Agent MUST NOT fragment within any top level or lower level TLVs. Each DCD message fragment is a complete DOCSIS frame with its own CRC. Other than the Fragment Sequence Number, the framing of one DCD message fragment is independent of the framing of another DCD message fragment. This allows the potential for the Set-top Device to process fragments as they are received rather than reassembling the entire payload. This field is an 8-bit unsigned integer. The default value for this field is 1.

NOTE: A change in the structure of any of the fields that are not TLVs could cause backward compatibility issues for deployed devices, and therefore should be avoided.

All other parameters are coded as TLV tuples. The DSG Agent MUST be capable of changing these parameters dynamically during normal operation in response to configuration changes. If these parameters are changed, the DSG Agent MUST increment the configuration change count (modulo the field size). In some events (for example failover, hot swap, etc.,) discontinuities in the value of configuration change count may occur. After any event that can cause a discontinuity in the configuration change count, the DSG Agent MUST ensure that the configuration change count is incremented (modulo the field size) between two subsequent DCD messages (even if the DCD message does not change). This is done to ensure that, after a failover or hot-swap, the new configuration change count does not match the configuration change count used before the failover event. When the configuration change count is changed, all DSG Rules and DSG Classifiers from the previous DCD message are considered invalid and are replaced by the DSG Rules and DSG Classifiers from the current DCD message. The DSG eCM MUST NOT re-initialize if any of these operational parameters are changed.

NOTE: DSG Tunnels are not guaranteed to provide reliable transport to DSG clients. In particular, there could be some packet loss when DSG Tunnel parameters are changed, while the DSG clients adapt to the new parameters.

DSG Vendor-Specific Parameters: Vendor-specific information for DSG Clients, if present, MUST be encoded in the vendor specific information field (VSIF) (code 43) using the Vendor ID field (code 8) to specify which TLV tuples apply to which vendor's products. Vendor-Specific Parameters may be located inside or outside of a DSG Rule. Vendor-Specific Parameters are coded as TLV tuples and are defined in Annex C of [DOCSIS-RFI].

DSG Classification Parameters: The DSG Classifier is used to provide additional layer 3 and layer 4 filtering for the DSG Tunnel.

DSG Rules: These parameters are used by the DSG Client Controller to determine which DSG Tunnel to receive and if there are any DSG Classifiers to apply.

DSG Configuration: These include various operating parameters for the DSG eCM, including timer values for the DSG eCM state machines and a list of the downstream frequencies containing DSG Tunnels.

The DSG Agent MUST support the above TLVs through the MIB defined in Annex A. DOCSIS 1.0 CMTSs that implement DSG Advanced Mode MUST support these parameters on the DOCSIS signaling interface, but are not obligated to use the same data structures in their internal implementation. The DSG eCM MUST pass all TLVs in a DCD message to the DSG Client Controller without processing. It is expected that the DSG Client Controller will

reject, without failure, any TLV that it does not recognize while accepting the remaining TLVs that it does recognize.

These TLVs used by the DSG Agent and the DSG Client Controller are summarized in Table 5–1 and then described in the subsequent sections. A check mark beneath the DSG Agent column indicates that the corresponding TLV is intended for use when processing packets received by the DSG Agent. A check mark beneath the DSG Client Controller column indicates that the corresponding TLV may be included in the DCD message and is intended for use when processing packets received by the DSG eCM. The Mandatory/Optional in DCD column indicates whether or not the TLV MUST be included by the DSG Agent in order for the DCD message to be considered valid. Note that a sub-TLV that is labeled Mandatory does not override the fact that its parent TLV is optional, i.e., the sub-TLV is only required if the optional parent TLV is present. The Repeatable in DCD column indicates whether or not a TLV may be included multiple times in the DCD message. Note that the Repeatability of a sub-TLV is specified only in the context of its parent TLV, i.e., a non-repeatable sub-TLV may be included at most once within each instance of its parent TLV. Note that, as per [DOCSIS-RFI], the maximum value for the length octet in any TLV is 254. This places limitations on the number of repeated sub-TLVs that can be included within any TLV.

Table 5–1 - Summary of DCD TLV Parameters

Type	Length	Name	DSG Agent	DSG Client Controller	Mandatory/ Optional in DCD	Repeatable in DCD
23	-	Downstream Packet Classification Encoding	√	√	O	√
23.2	2	Classifier Identifier	√	√	M	
23.5	1	Classifier Priority	√	√	M	
23.9	-	IP Packet Classification Encodings	√	√	M	
23.9.3	4	Source IP Address	√	√	O	
23.9.4	4	Source IP Mask	√	√	O	
23.9.5	4	Destination IP Address	√	√	M	
23.9.9	2	Destination TCP/UDP Port Start		√	O	
23.9.10	2	Destination TCP/UDP Port End		√	O	
50	-	DSG Rule		√	O	√
50.1	1	DSG Rule Identifier		√	M	
50.2	1	DSG Rule Priority		√	M	
50.3	n	DSG UCID List (Deprecated)		√	O	
50.4	-	DSG Client ID		√	M	
50.4.1	2	DSG Broadcast		√	O	
50.4.2	6	DSG Well-Known MAC Address		√	O	√
50.4.3	2	CA System ID		√	O	
50.4.4	2	Application ID		√	O	√
50.5	6	DSG Tunnel Address	√	√	M	
50.6	2	DSG Classifier Identifier	√	√	O	√
50.43	-	DSG Rule Vendor-Specific Parameters		√	O	√
51	-	DSG Configuration		√	O	
51.1	4	DSG Channel List Entry		√	O	√
51.2	2	DSG Initialization Timeout (Tdsg1)		√	O	
51.3	2	DSG Operational Timeout (Tdsg2)		√	O	
51.4	2	DSG Two-way Retry Timer (Tdsg3)		√	O	

Type	Length	Name	DSG Agent	DSG Client Controller	Mandatory/ Optional in DCD	Repeatable in DCD
51.5	2	DSG One-way Retry Timer (Tdsg4)		√	O	
51.43	-	DSG Config Vendor-Specific Parameters		√	O	√

5.3.1.1 DSG Classifier

DSG Classifiers are for classifying packets and are coded as TLV tuples. The definitions of the TLV values are defined in section "Packet Classification Encodings" in Annex C of [DOCSIS-RFI]. The DSG Classifier parameters are set through the DSG MIB. They are not intended to be configured via a CM Configuration File. When a DSG Classifier is configured to be included in the DCD, the DSG Agent MUST include the DSG Classifier in the DCD message on the downstream channel to which the Classifier applies. The DSG Classifier ID is unique per DSG Agent.

The DSG Agent applies the DSG Classifier parameters to incoming packets from the DSG Server in order to assign the packet to the appropriate DSG Tunnel. The DSG Agent MUST classify incoming packets based upon the Classification Parameters listed in Table 5–1 with the exception of the UDP Port.

The DSG Client Controller will use the DSG Classifier parameters to establish a packet filter on the DSG eCM for the downstream DSG Tunnel packet flow. DSG Tunnel packets which match filters established by the DSG Client Controller MUST be forwarded by the DSG eCM.

The DCD message, which is intended for use by the DSG Client Controller, may include any of the Classification Parameters in Table 5–1. The DCD message MUST NOT include any classification parameters not listed in Table 5–1. The DSG Agent MUST NOT include any Ethernet LLC Packet Classification Encodings as these might interfere with the DSG Rule parameters.

Type	Length	Value
23	n	

5.3.1.2 DSG Rule

The DSG Agent MUST support all DSG Rule TLVs.

The DSG Rule is only intended to be included in the DCD message and is not intended to be included in the CM Configuration File.

Type	Length	Value
50	n	

5.3.1.2.1 DSG Rule Identifier

The value of the field specifies an identifier for the DSG Rule. This value is unique per DCD Message. The DSG Agent assigns the DSG Rule Identifier.

Type	Length	Value
50.1	1	1-255

5.3.1.2.2 DSG Rule Priority

The value of the field specifies the priority for the DSG Rule, which is used for determining the order of application of the DSG Rule. A higher value indicates higher priority. The default value is 0 which is the lowest priority.

Type	Length	Value
50.2	1	0-255

5.3.1.2.3 DSG UCID List

The DSG UCID list was previously used in this standard for regionalization of the DSG Tunnels. This concept is now deprecated.

5.3.1.2.4 DSG Client ID

The value of the field specifies the matching parameters for the DSG Client ID for which the DSG Rule applies. A DSG Rule will apply to a DSG Client if there is a match on one of the DSG Client ID fields.

The DSG Client ID recognizes that IDs may originate from different address spaces. Each of those address spaces are coded as sub-TLVs within the DSG Client ID TLV. These sub-TLVs MAY be repeated within the DSG Client ID TLV to include additional DSG Client IDs. The same DSG Client ID MAY be listed in more than one DSG Rule. If the same DSG Client ID is listed in more than one DSG Rule, the expected behavior of the DSG Client Controller is to take the DSG Rule Priority field into account when applying DSG Rules.

The DSG Agent MUST support all ID types.

Type	Length	Value
50.4	n	

5.3.1.2.4.1 DSG Broadcast ID

Traffic for a DSG Client ID of this type conforms to specific industry standards. This traffic is received by a DSG Client that operates with standard data. A DSG Client ID of this type should not have a Length of zero (0). If the Length is 0 then the DSG Client Controller should disregard the rule if a Length of zero is not supported by the DSG Client Controller (the use of this subtype with Length 0 is deprecated). If the Length is 2 and the Value is non-zero, a specific type of industry-standard data is denoted per Table 5–2. The DCD MUST NOT contain a DSG Broadcast ID TLV of Length 2 and Value 0.

NOTE: Client behavior is not defined if data streams for multiple standards are mixed into a single tunnel, and provisioning by the operator is expected to prevent such mixing.

NOTE: The DCD can contain multiple rules with a DSG Broadcast ID, each to indicate the presence of a specific industry-standard data stream.

Subtype	Length	Value
50.4.1	0	unspecified broadcast; the use of this subtype with Length 0 is deprecated
50.4.1	2	as defined in Table 5–2

Table 5–2 - DSG Broadcast ID Value Definitions

Value	Definition
0	Prohibited.
1	Contains [SCTE 65] - Delivery as defined in Annex D of this document.
2	Contains [SCTE 18] - Delivery as defined in Annex D of this document.
3	Contains OCAP Object Carousel [OCAP]; the use of this Value is deprecated.*
4	Contains OpenCable Common Download Carousel [OC-CDL]; the use of this Value is deprecated.*
5	Contains XAIT and/or CVT data as specified in [OC-CDL] - Delivery as defined in Annex D of this document.
6-55534	Reserved for future use.
55535-65535	Reserved for MSO specific use.

* Carousel data will be carried in tunnels labeled with Application Client IDs.

5.3.1.2.4.2 DSG Well-Known MAC Address

A DSG Client ID of this type is received by a DSG Client that has been assigned a MAC Address. The first three bytes of the MAC address are known as the Organizationally Unique Identifier (OUI) as defined in [OUI]. The MAC address is assigned by the DSG Client Controller. While the DSG Tunnel MAC address is restricted to being a Group MAC Address, no such restriction applies to this encoding.

Subtype	Length	Value
50.4.2	6	dst1, dst2, dst3, dst4, dst5, dst6

NOTE: The Well-Known MAC address can be used as a transition from the DSG Basic mode deployment to DSG advanced mode deployment.

5.3.1.2.4.3 CA System ID

A DSG Client ID of this type is received by a DSG Client that has been assigned a CA_system_ID as defined by [MPEG-SI] and assigned by [CAS ID]. The CA_system_ID is sent "uimsbf" (unsigned integer most significant bit first).

Subtype	Length	Value
50.4.3	2	CA_system_ID

5.3.1.2.4.4 Application ID

A DSG Client ID of this type is received by a DSG Client that has been assigned an Application ID. The Application ID is sent "uimsbf" (unsigned integer most significant bit first). The Application ID would be taken from a private address space managed by the MSO. The Application ID can be assigned to the DSG Client from a table contained within the DSG Broadcast Tunnel such as the Source Name Sub-table (SNS) as defined in [SCTE 65]. (Refer to Annex D for information on the delivery of SCTE 65 tables.)

There may be one or more applications per DSG Tunnel. There may be one or more DSG Tunnels that are used for carrying application traffic.

Subtype	Length	Value
50.4.4	2	Application_ID

5.3.1.2.5 DSG Tunnel Address

This is the destination MAC address that will be used for the DSG Tunnel. This TLV allows the DSG Tunnel Address to be dynamically remapped to another MAC address. An MDF-capable DSG eCM with Multicast DSID forwarding enabled only uses the DSG Tunnel address to identify the DSID for the DSG tunnel Data from the DA to DSID Association Entry TLV.

Type	Length	Value
50.5	6	Destination MAC Address of the DSG Tunnel

5.3.1.2.6 DSG Classifier Identifier

The value of the field specifies a Classifier Identifier that identifies the corresponding DSG Classifier to be used with this DSG Rule. The Classifier Identifier MUST correspond to a DSG Classifier included in the same DCD message.

This TLV may be repeated within a DSG Rule to include additional DSG Classifiers.

Type	Length	Value
50.6	2	1 - 65535

5.3.1.2.7 DSG Rule Vendor-Specific Parameters

This allows vendors to encode vendor-specific DSG parameters within a DSG Rule. The Vendor ID MUST be the first TLV embedded inside Vendor-Specific Parameters. If the first TLV inside Vendor-Specific Parameters is not a Vendor ID, then the TLV will be discarded. Refer to [DOCSIS-RFI] for the definition of Vendor ID.

This TLV may be repeated within a DSG Rule to include additional DSG Rule Vendor-Specific Parameters. The length (n) of this TLV can be between 5 and 55 bytes (5 bytes for the Vendor ID, and up to 50 bytes for the subsequent values).

Type	Length	Value
50.43	n	

5.3.1.3 DSG Configuration

This group of TLVs contains parameters for configuration and operation of the DSG eCM. The DSG Channel List allows a DSG Agent to advertise which downstreams contain DSG Tunnels. This is intended to reduce the Set-top Device initial scan time.

The state machines of the DSG eCM in the Set-top Device have several timer values which define the operation of DSG. The set of DSG Timer TLVs allows those timer values to be dynamically provisioned from the DSG Agent.

Type	Length	Value
51	n	

5.3.1.3.1 DSG Channel List Entry

The value of this field is a receive frequency that is available to be used by the Set-top Device for receiving DSG Tunnels. This TLV MAY be repeated to create a DSG Channel List which would be a list of downstreams containing DSG Tunnels. This DSG Channel List may be transmitted on any DOCSIS downstream channel, regardless of the presence or absence of DSG Tunnels on that channel. This TLV may be the only TLV present in the DCD message, or it may co-exist with other TLVs within the DCD Message.

This is the center frequency of the downstream channel in Hz stored as a 32-bit binary number. The receive frequency assigned by the CMTS MUST be a multiple of 62500 Hz.

NOTE: The intent of the DSG Channel List is to contain a list of all the downstream frequencies that contain DSG Tunnels.

Type	Length	Value
51.1	4	Rx Frequency

5.3.1.3.2 DSG Initialization Timeout (Tdsg1)

This is the timeout period for the DSG packets during initialization of the DSG eCM defined in seconds. The default value is 2 seconds. If this sub-TLV is present, it is intended to overwrite the default value of Tdsg1 in the DSG eCM initialization state machine. If the DSG Initialization Timeout sub-TLV is not present, then the DSG eCM MUST utilize the default value. The valid range of values is 1 to 65535.

Type	Length	Value
51.2	2	Tdsg1 (in seconds)

5.3.1.3.3 DSG Operational Timeout (Tdsg2)

This is the timeout period for the DSG packets during normal operation of the DSG eCM defined in seconds. The default value is 600 seconds. If this sub-TLV is present, it is intended to overwrite the default value of Tdsg2 in the DSG eCM operational state machine. If the DSG Operational Timeout sub-TLV is not present, then the DSG eCM MUST utilize the default value. The valid range of values is 1 to 65535.

Type	Length	Value
51.3	2	Tdsg2 (in seconds)

5.3.1.3.4 DSG Two-way Retry Timer (Tdsg3)

This is the retry timer that determines when the DSG eCM attempts to reconnect with the CMTS and establish two-way connectivity defined in seconds. The default value is 300 seconds. If this sub-TLV is present, it is intended to overwrite the default value of Tdsg3 in the DSG eCM operational state machine. If the DSG Two-way Retry Timer sub-TLV is not present, then the DSG eCM MUST utilize the default value. The valid range of values is 0 to 65535. A value of zero (0) indicates that the DSG client must continuously retry two-way operation.

Type	Length	Value
51.4	2	Tdsg3 (in seconds)

5.3.1.3.5 DSG One-way Retry Timer (Tdsg4)

This is the retry timer that determines when the DSG eCM attempts to rescan for a downstream DOCSIS channel that contains DSG packets after a Tdsg2 timeout defined in seconds. The default value is 1800 seconds. If this sub-TLV is present, it is intended to overwrite the default value of Tdsg4 in the DSG eCM operational state machine. If the DSG One-way Retry Timer sub-TLV is not present, then the DSG eCM MUST utilize the default value. Valid range of values is 0 to 65535. A value of zero (0) indicates the DSG client must immediately begin scanning upon Tdsg1 or Tdsg2 timeout.

Type	Length	Value
51.5	2	Tdsg4 (in seconds)

5.3.1.3.6 DSG Configuration Vendor-Specific Parameters

This allows vendors to encode vendor-specific parameters outside the DSG Rule but within the DCD message. The Vendor ID MUST be the first TLV embedded inside Vendor-Specific Parameters. If the first TLV inside Vendor-Specific Parameters is not a Vendor ID, then the TLV will be discarded. Refer to [DOCSIS-RFI] for the definition of Vendor ID.

This TLV may be repeated within a DSG Rule to include additional DSG Configuration Vendor-Specific Parameters. The length (n) of this TLV can be between 5 and 55 bytes (5 bytes for the Vendor ID, and up to 50 bytes for the subsequent values).

Type	Length	Value
51.43	n	

5.3.2 DSG Service Class

The DSG Service Class is used to manage the Quality of Service of the DSG Tunnels within the DSG Agent. The DSG Service Class is identified with a Service Class Name and has an associated QoS Parameter Set. The DSG Service Class parameters are set through the DSG MIB. Multiple DSG Tunnels may reference the same DSG Service Class. Each DSG Tunnel MUST only have one Service Class reference. The DSG Service Class parameters are not intended to be included in the DCD message or the CM Configuration File.

The DSG Agent MUST recognize the following DSG Service Class Parameters. These parameters are defined in the section "Service Flow Encodings" in Annex C of [DOCSIS-RFI]:

- Service Class Name
- Traffic Priority
- Downstream Maximum Sustained Traffic Rate (R)
- Maximum Traffic Burst (B)

- Minimum Reserved Traffic Rate
- Assumed Minimum Reserved Rate Packet Size

5.4 DSG eCM Operation

This section describes the behavior of DSG eCMs for two different versions of DOCSIS:

- Section 5.4.3 describes the behavior of Pre-3.0 DOCSIS DSG eCMs.
- Section 5.4.4 describes the behavior of DOCSIS 3.0 DSG eCMs. A DOCSIS 3.0 DSG eCM follows the initialization sequence outlined in these sections even if it is registering on a Pre-3.0 DOCSIS DSG CMTS.

5.4.1 DSG Modes

The DSG Client Controller, acting on behalf of a Client (or Clients), instructs the eCM to begin DSG operation. In DSG Advanced Mode the DSG Client Controller becomes aware of MSO-defined tunnel MAC addresses by indexing into the DSG Address Table in the DCD message.

The following requirements apply to the DSG eCM:

- The DSG eCM MUST NOT begin DSG operation unless explicitly instructed to do so by the DSG Client Controller (Figure 5–11 - DSG Operation and Figure 5–30 - DOCSIS 3.0 DSG Operation).
- The DSG eCM MUST forward the unaltered contents of each DCD fragment that comprises the first DCD message received to the DSG Client Controller.
- After any change in the DCD message (as indicated by the change count), the DSG eCM MUST forward the unaltered contents of each DCD fragment that comprises the new DCD message to the DSG Client Controller.
- The DSG eCM MUST scan additional downstream channels for a DCD message if the DSG Client Controller indicates that the DCD message was in error or invalid.
- If the DSG eCM has been unable to identify a downstream channel with an appropriate DCD message after a complete downstream scan, it MUST inform the DSG Client Controller that it could not locate a DCD message and continue scanning.

5.4.2 DSG eCM Initialization and Operation

The DSG eCM will have an initialization sequence that differs from the standard DOCSIS cable modem, primarily related to how the DSG eCM responds to the various timeouts and error conditions. The DSG eCM will remain tuned to a DOCSIS downstream containing DSG packets and continue to process the IP packets carried in the DSG tunnel even when the return channel is impaired or two-way connectivity is lost. This is necessary to enable the delivery of downstream OOB messages regardless of two-way capabilities.

The Pre-3.0 DOCSIS DSG eCM initialization sequence is based on the CM initialization sequence defined in the "Cable Modem Initialization" section of [DOCSIS-RFI]. The DOCSIS 3.0 DSG eCM initialization sequence is based on the CM initialization sequence defined in the "Cable Modem Initialization and Reinitialization" section of [DOCSIS-MULPI]. The differences from the DOCSIS standard are detailed in the following sections as well as highlighted in gray in the accompanying figures. The DSG eCM initialization sequence introduces two new timers and two new retry timers. These are:

- Tdsg1 - The timeout period for the DSG channel during initialization of the DSG eCM.
- Tdsg2 - The timeout period for the DSG channel during normal operation of the DSG eCM.
- Tdsg3 - Two-way retry timer - The retry timer that determines when the DSG eCM attempts to reconnect with the CMTS and establish two-way connectivity.
- Tdsg4 - One-way retry timer - The retry timer that determines when the DSG eCM attempts to rescan for a downstream DOCSIS channel that contains DSG packets after a Tdsg2 timeout.

When operating in DSG Advanced mode, the DSG eCM MUST use the default timer values as specified in Sections 5.3.1.3.2 through 5.3.1.3.5, unless they are overridden by the DSG Client Controller in response to an override from

a DCD message. If the default timer values are overridden by the DSG Client Controller, the DSG eCM MUST use those updated values until it is rebooted or another override is received.

In general, the intent of this initialization sequence is to avoid rebooting the DSG eCM if at all possible and continue to receive downstream OOB messages via DSG in all cases. To achieve this the DSG Specification introduces a one-way mode of operation that is distinguished from normal two-way DOCSIS operation by remaining tuned to and processing the DOCSIS downstream during periods when the upstream channel is impaired or other timeout conditions occur. As shown in the following sections, this is achieved by modifying all instances that would result in re-initializing the MAC layer in DOCSIS to go to the one-way mode of operation. The DSG eCM recovers from these error conditions by periodically attempting to reacquire the upstream channel and establish two-way connectivity.

When a DSG eCM loses its upstream channel capability, either through upstream channel impairment or other reasons, it will no longer respond to periodic ranging requests from the CMTS. The CMTS will eventually de-register the DSG eCM. Consequently, when the DSG eCM attempts to reacquire two-way connectivity it will begin the Upstream Acquisition process by collecting UCD messages or by resolving MD-US-SG (3.0 DSG eCM only).

Further, since the DSG tunnel is not guaranteed to be present on all downstream DOCSIS channels, the initialization sequence is also modified to make certain that a valid DOCSIS downstream is acquired that is deemed by the DSG Client Controller as a Valid DSG channel.

The DSG Client Controller needs to be made aware of any eCM limitations that may impact 2-way data forwarding, so it can provide the proper reactions on such limitations. If data forwarding to any or all of the eSTB MAC addresses cannot be supported, the eCM MUST report these limitations to the DSG Client Controller.

5.4.2.1 DCC considerations for DSG eCMs

The DSG Client Controller needs to be made aware of DCC operations so it can track DCC progress, provide the proper reactions to upstream and downstream channel changes, and maintain a valid DSG channel. Such DCC operations are bracketed in time between two CM generated messages: DCC-RSP (Depart) and DCC-RSP (Arrive) [DOCSIS-RFI].

- When the CM sends a "DCC-RSP (Depart)" message, the eCM MUST also send a "DCC Depart, Initialization Type <IT> " (where IT = "DCC initialization type") message to the DSG Client Controller.
- When the CM sends a "DCC-RSP (Arrive)" message, the eCM MUST also send a "2-way OK, UCID <P1>" (where P1 = 255) message to the DSG Client Controller. The reserved value 255 is used for the UCID to maintain compatibility with legacy DSG Client Controller implementations that expect a UCID value.

5.4.2.2 DBC considerations for DOCSIS 3.0 DSG eCMs

In a set-top box containing a DOCSIS 3.0 DSG eCM, the DSG Client Controller needs to be made aware of DBC operations so it can track DBC progress, provide the proper reactions to upstream and downstream channel changes, and maintain a valid DSG channel. On a DOCSIS 3.0 DSG eCM, if the DBC changes the primary downstream channel, the eCM sends the "DCC depart message" to the DSG Client Controller. The intent here is to reuse the DCC Depart message from the Pre-3.0 DOCSIS eCMs for the DBC case as well, so that the DSG Client Controller does not see any differences with respect to DOCSIS 3.0 or pre-3.0 DOCSIS DSG eCMs. The eCM MUST send the "DCC Depart Message" before it sends the DBC-RSP. The eCM SHOULD send the "DCC Depart Message" prior to implementing the changes indicated in the DBC-REQ.

After a successful DBC operation affecting the primary downstream, when the eCM sends a "DBC-RSP " message, the eCM MUST also send a "2-way OK, UCID <P1>" (where P1 = 255) message to the DSG Client Controller. The reserved value 255 is used for the UCID to maintain compatibility with legacy DSG Client Controller implementations that expect a UCID value.

The DSG eCM MUST initialize and operate as described in the following subsections and their state transition diagrams. Note that the eCM MUST be prepared to receive instruction from the DSG Client Controller at any time and act upon that instruction.

5.4.3 Pre-3.0 DOCSIS DSG eCM Operation

This section only applies to Pre-3.0 DOCSIS DSG eCMs.

5.4.3.1 DSG eCM State Transition Diagrams

The operation of a DSG eCM is described here by two separate state machines. The first, "DSG eCM Initialization and Operation," is covered by the state transition diagrams in Figure 5–3 through Figure 5–10 (and described in Section 5.4.2.2 to Section 5.4.3.8), and the second, "DSG Operation," is covered by the state transition diagram in Figure 5–11 (and described in Section 5.4.3.9). These two different state machines operate in parallel, and the "DSG Operation" state machine provides inputs into the "DSG eCM Initialization and Operation" state machine.

These state transaction diagrams apply only to the eCM. The messages sent between the two state machines, and to and from the DSG Client Controller, are provided in the following sections.

5.4.3.1.1 Messages sent/received by "DSG eCM Initialization and Operation"

Inputs from the DSG Operation state machine:

- Valid DSG Channel
- Invalid DSG Channel
- DCD Present (DSG Advanced Mode only)

Inputs from the DSG Client Controller:

- Disable upstream transmitter
- Enable upstream transmitter

Outputs to DSG Client Controller:

- Downstream Scan Completed
- 2-way OK, UCID. (The reserved value 255 is used for the UCID to maintain compatibility with legacy DSG Client Controller implementations that expect a UCID value.)
- Entering One-way Mode
- Cannot forward 2-way traffic, NACO <val>, Max CPE <val>
- DCC Depart, Initialization Type <IT> (where IT = "DCC initialization type")

5.4.3.1.2 Messages sent/received by "DSG Operation"

Inputs from the DSG Client Controller:

- Start DSG Advanced Mode
- Filter these MAC Addresses and Classifiers
- Not Valid. Hunt for new DSG Channel

Outputs to DSG Client Controller:

- DCD Message information
- eCM MAC reinitialization

5.4.3.2 DSG eCM Initialization Overview

The following figure corresponds to the "CM Initialization Overview" figure in [DOCSIS-RFI]. The difference in the initialization of the DSG eCM is scanning for the downstream DSG channel and going to Two-way Operation as opposed to just becoming Operational. This process is described in detail in the following sections.

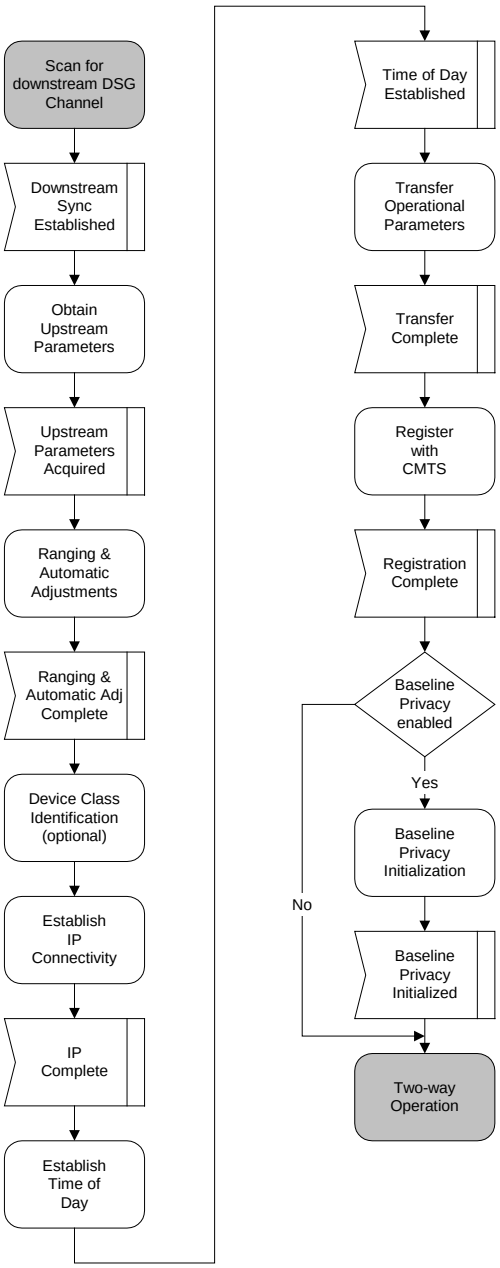


Figure 5–3 - DSG eCM Initialization Overview

5.4.3.3 DSG eCM Scan For Downstream Channel

This section corresponds to the "Scanning and Synchronization to Downstream" section in [DOCSIS-RFI] although the figure does not have a corresponding figure in either specification. In addition to the steps required to acquire a valid downstream channel, it is necessary that the downstream channel contain appropriate DSG tunnels. If a DOCSIS downstream channel containing the appropriate DSG tunnels cannot be found, then the DSG eCM MUST continue scanning.

The DSG eCM MUST have its DSG Mode set to Advanced at startup before scanning for a downstream channel.

When operating in DSG Advanced mode, the DSG Client Controller may provide the DSG eCM with a list of downstream frequencies which have been derived from the DSG Channel List portion of the DCD message. This list

is meant to aid the DSG eCM in acquiring an appropriate downstream rapidly. Note that once the DSG eCM receives a configuration file via the registration process, the requirements relating to the Downstream Frequency Configuration Setting (TLV-1) and the Downstream Channel List (TLV-41) as described in [DOCSIS-RFI] still apply.

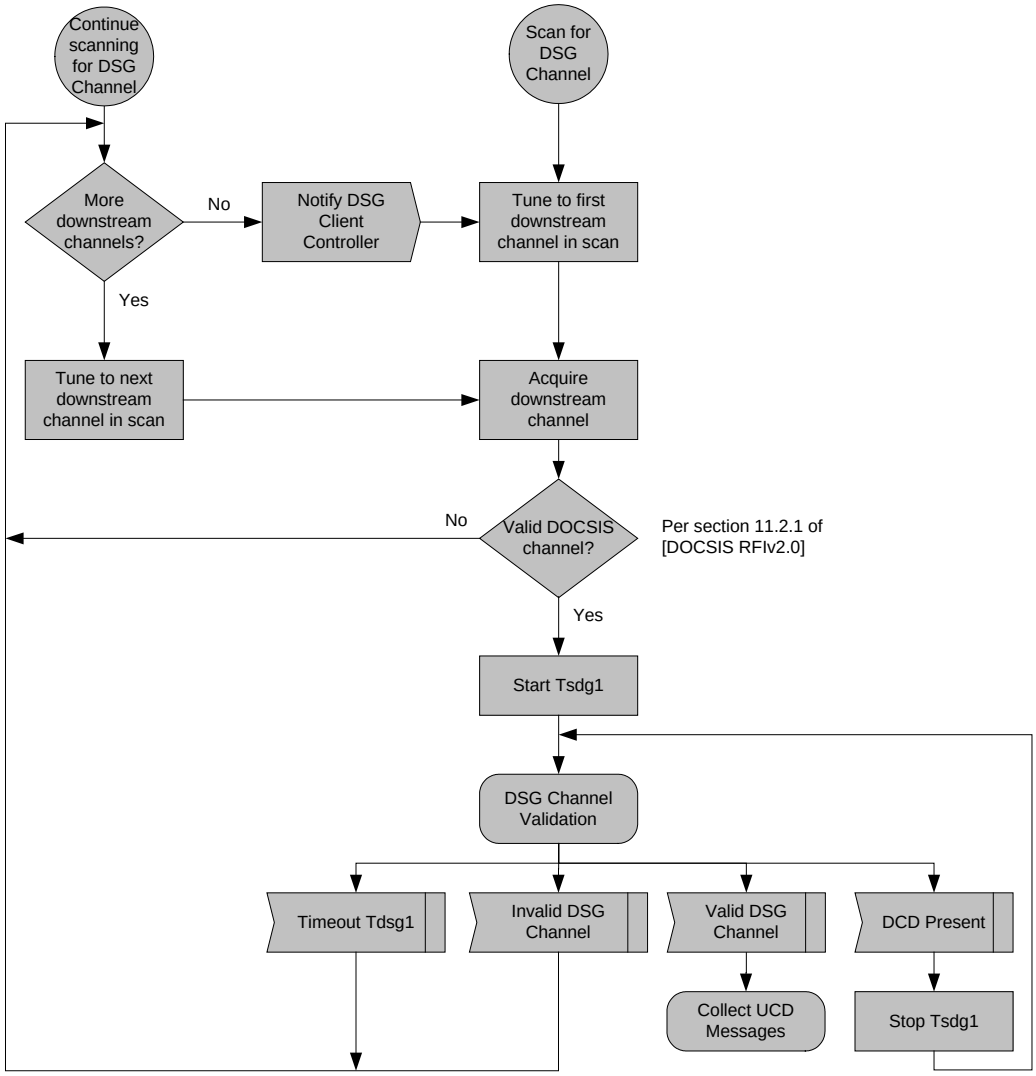


Figure 5–4 - DSG eCM Scan for Downstream DSG Channel

5.4.3.4 DSG eCM Obtain Upstream Parameters

This section corresponds to the "Obtain Upstream Parameters" section in [DOCSIS-RFI]. The difference in this case is that in the case of a T1 timeout, the DSG eCM will Start One-way mode of operation.

If the T1 timer expires, the eCM MUST enter One-way mode. This requirement also covers T1 timer activity as mentioned in [DOCSIS-RFIv2.0] related to unusable UCDs.

It should be noted that a DSG modem that does not comply with TLV19 [DOCSIS-RFIv2.0] will move to One-way mode of operation if the CMTS issues an intentional Range Abort to kick the DSG modem off an upstream that is 'reserved' via TLV19. In this case, the DSG modem will take Tdsg3 seconds (default 300 seconds) to begin another search for another upstream. The expectation is that most DSG modems will comply with TLV19.

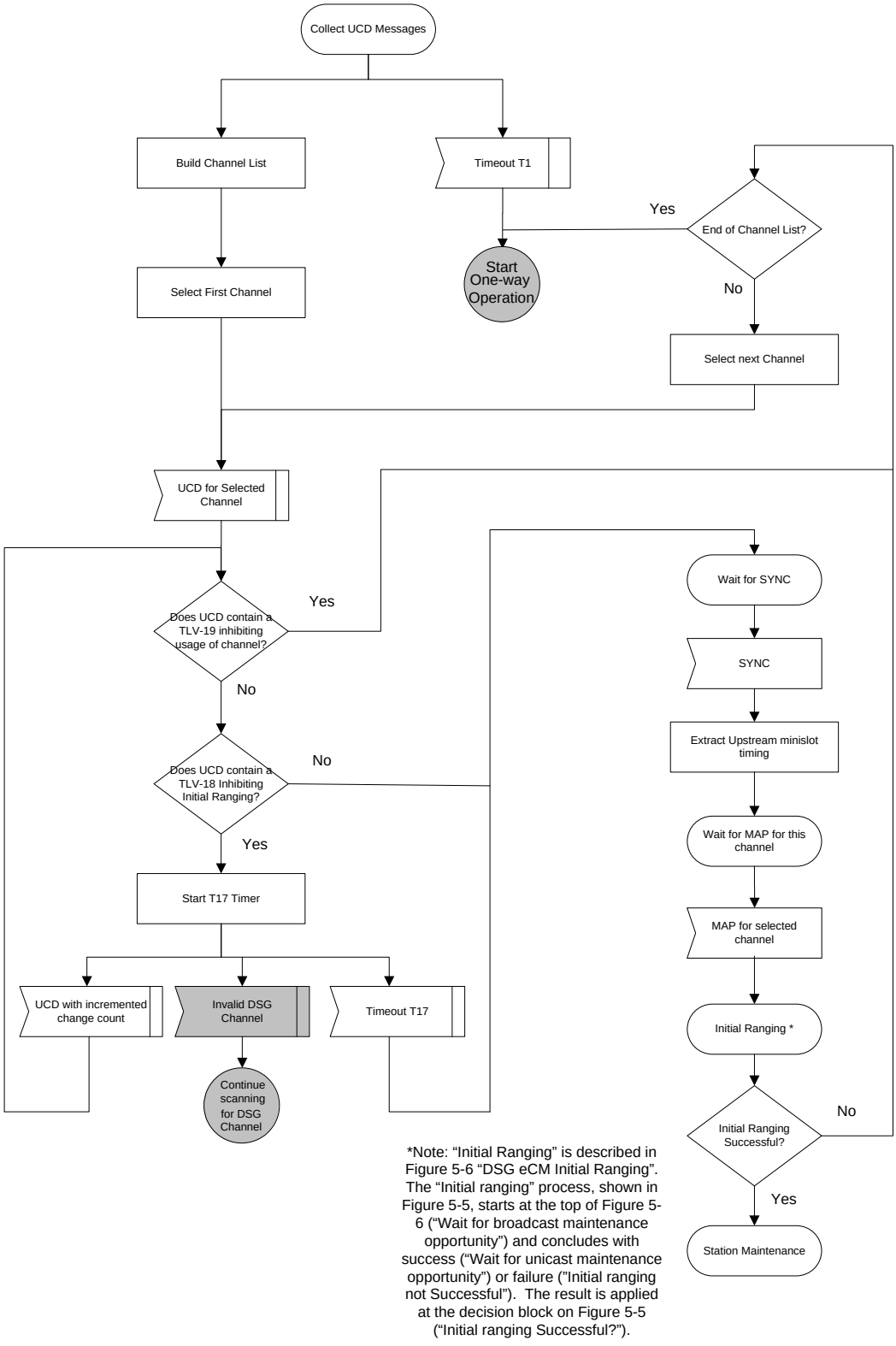
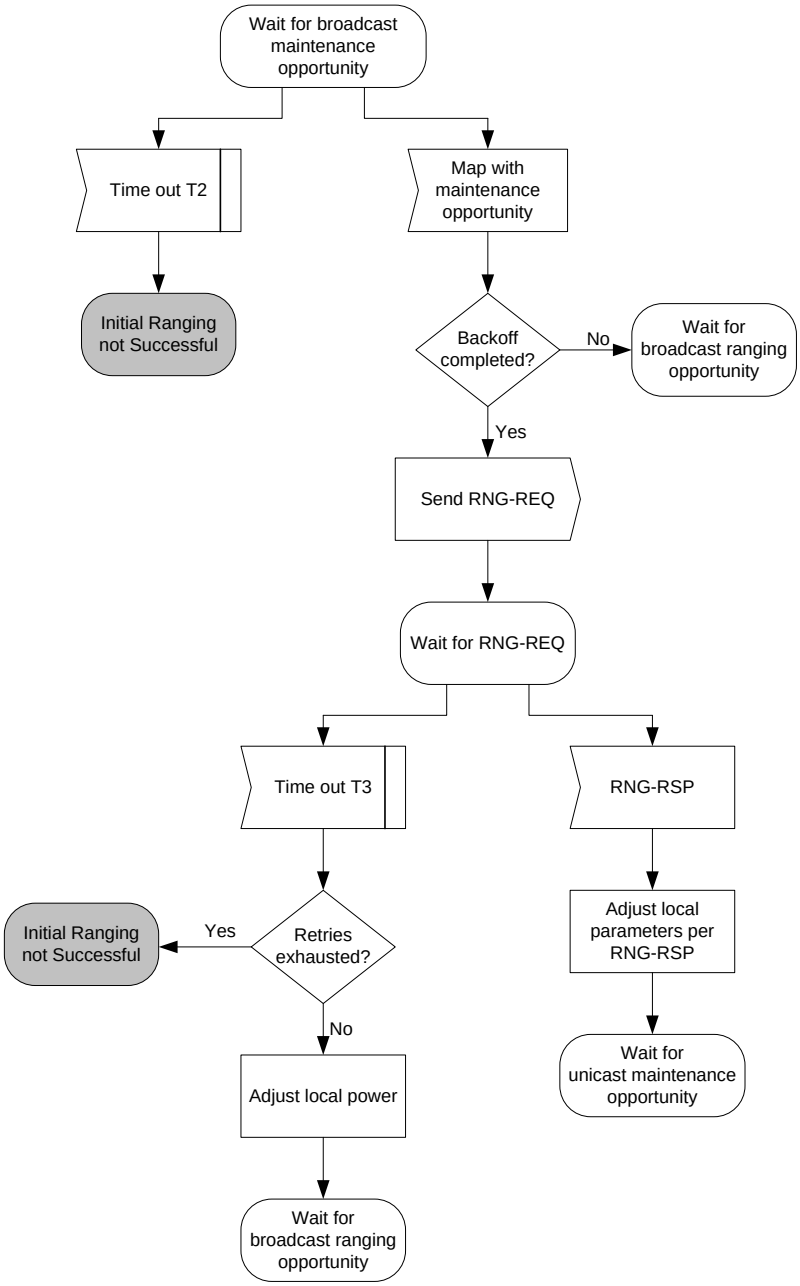


Figure 5–5 - DSG eCM Obtaining Upstream Parameters

5.4.3.5 DSG eCM Ranging and Automatic Adjustments

This section corresponds to the "Ranging and Automatic Adjustments" section in [DOCSIS-RFI]. The differences in this case are that conditions which would have caused the CM to reinitialize the MAC layer - such as a T2 or T4 timeout, or other error conditions - will instead cause either the initial ranging to fail or the eCM to start One-way mode of operation. In addition, successful ranging enables bidirectional data transfer, as opposed to just enabling data transfer, since downstream tunnel forwarding will already have been enabled.



Note: Timeout T3 may occur because the RNG-REQs from multiple modems collided. To avoid these modems repeating the loop in lockstep, a random backoff is required. This is a backoff over the ranging window specified in the MAP. T3 timeouts can also occur during multi-channel operation. On a system with multiple upstream channels, the CM attempts initial ranging on every suitable upstream channel before moving to One-way Operation.

Figure 5–6 - DSG eCM Initial Ranging

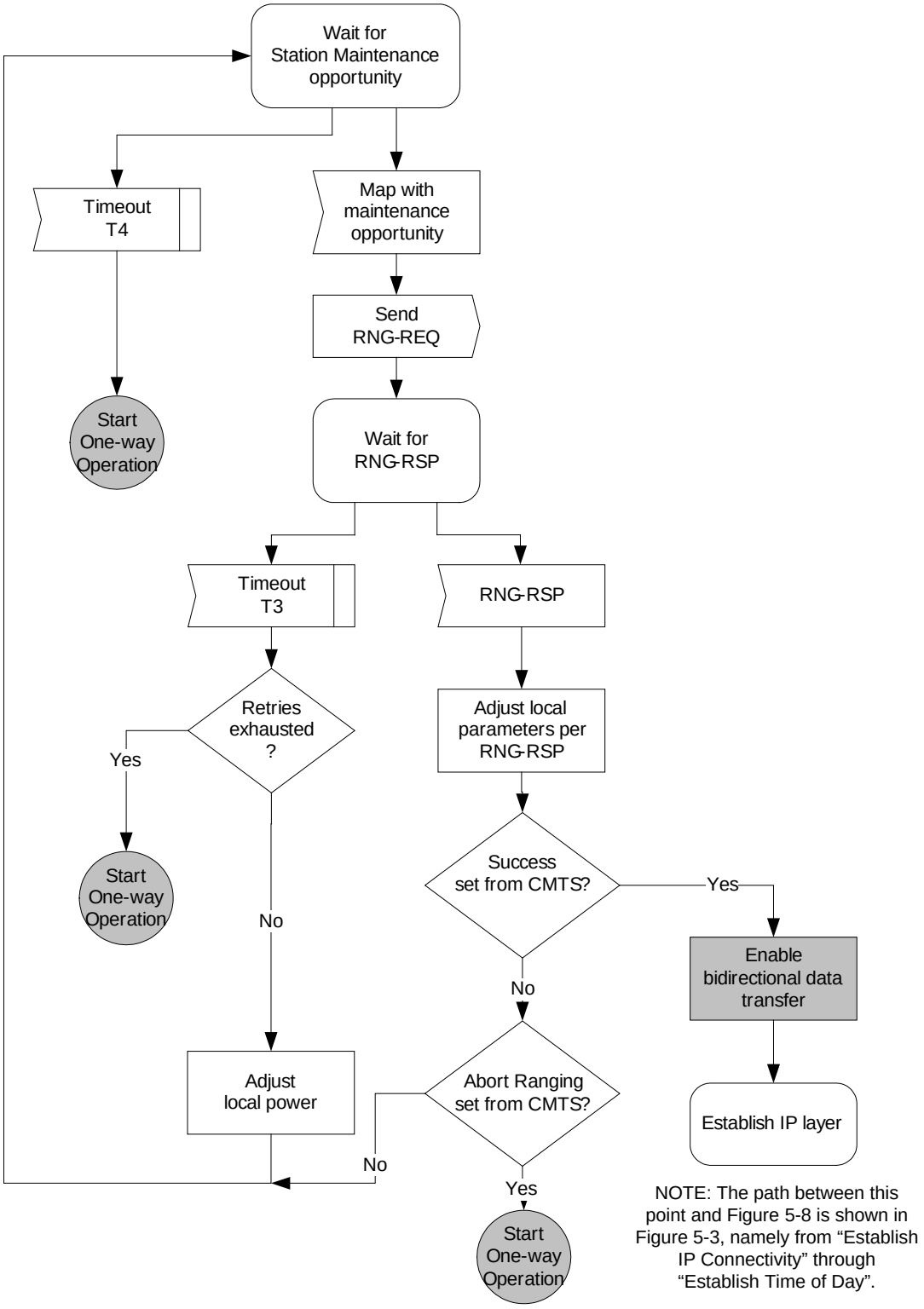


Figure 5–7 - DSG eCM Unicast Station Maintenance Ranging

5.4.3.6 DSG eCM Establish IP Connectivity

This section describes the steps the eCM performs to acquire a management IP address for itself. For the DSG eCM without IPv6 support, this section corresponds to the "Establishing IP connectivity" section in [DOCSIS2.0-IPv6]. For the DOCSIS 2.0+IPv6 DSG eCM, this section corresponds to the "Establishing IP connectivity" section in [DOCSIS2.0-IPv6].

The DOCSIS 2.0+IPv6 DSG eCM will read the MDD to read the IP Provisioning Mode, the Pre-Registration DSID, and possibly other parameters. The DOCSIS 2.0+IPv6 DSG eCM MUST discard all cached MDD TLV encodings and collect new MDD messages each time it attempts to establish IP connectivity. The DOCSIS 2.0+IPv6 DSG eCM MUST NOT use an MDD message whose source MAC address does not match that of the DCD message.

If the IP connectivity step fails the eCM enters the One-way Operation state.

5.4.3.7 DSG eCM Registration

This section corresponds to the "Registration" section in [DOCSIS-RFI]. The difference in this case is that, when retries for the Config File are exhausted, T6 timeout retries are exhausted, there are TLV type 11 errors, or the registration response is not OK, the DSG eCM will Start One-way mode of operation. There is also a notification to the DSG Client Controller when Two-way Operation has been established.

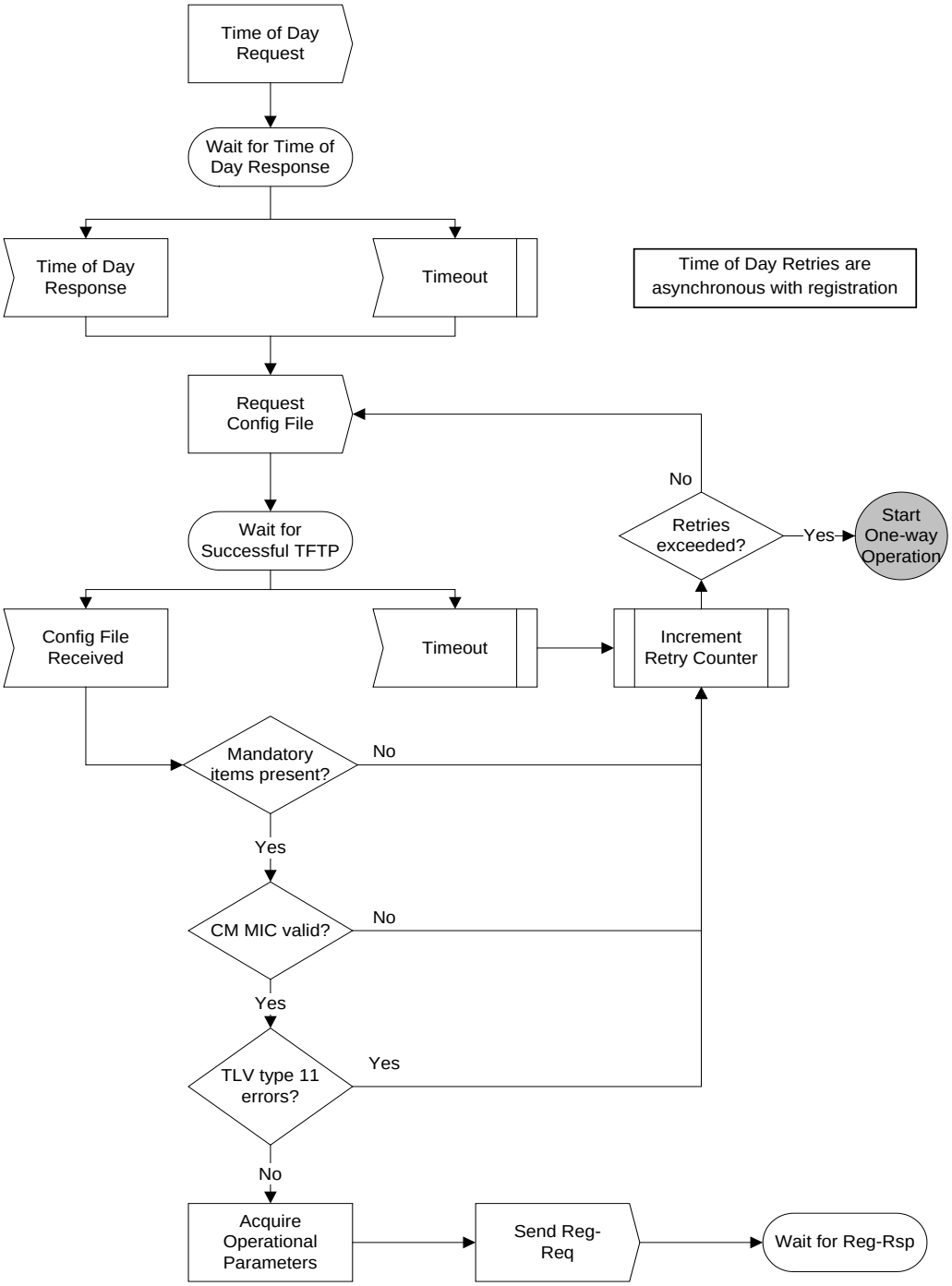


Figure 5–8 - DSG eCM Registration

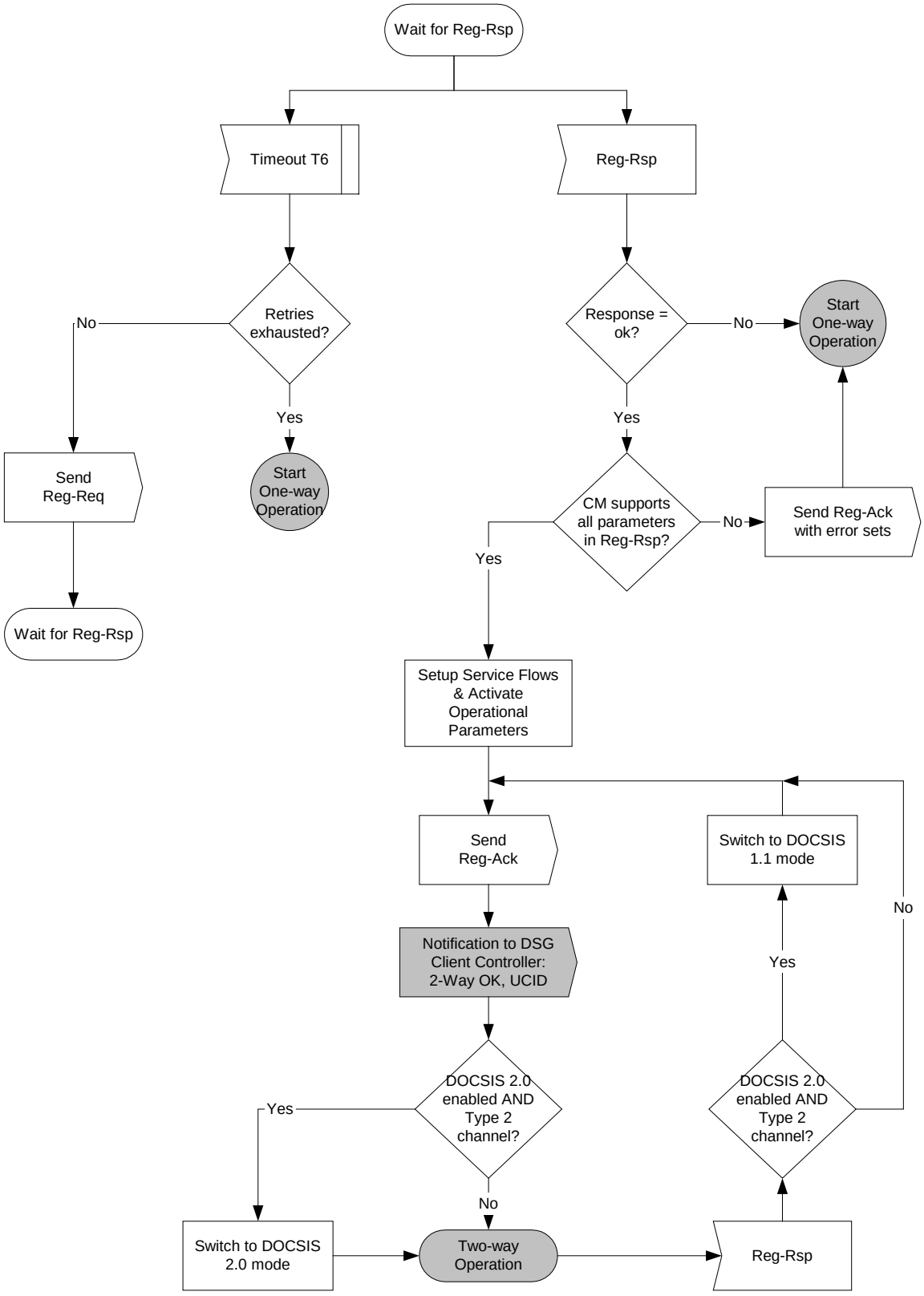


Figure 5–9 - DSG eCM Wait for Registration Response

5.4.3.8 DSG eCM Operation

This section corresponds in part to the "Periodic Signal Level Adjustment" section in [DOCSIS-RFI], although it also introduces several completely new concepts. The differences include One-way mode of operation, Two-way Operation Disabled, and the reception of an Invalid DSG Channel notification. The messages sent between the DSG Client Controller and the DSG eCM are detailed in Section 5.4.3.1.1.

When the DSG eCM enters One-way mode of operation as a consequence of any of the timeouts or error conditions indicated in the preceding sections, it MUST remain tuned to and process DSG traffic on the DOCSIS downstream channel. If the eCM enters One-way mode of operation as a result of loss of downstream sync, the eCM MUST NOT disable the Tdsg3 timer. If the CM loses downstream sync temporarily, the eCM can still receive DSG tunnel data, but will be unable to transmit on the upstream. As long as the CM receives the DCD messages and DSG tunnel data, eCM stays on the downstream, unless there is loss of DCD messages or DSG tunnel data on that downstream channel.

When a Tdsg3 timeout occurs, the DSG eCM behavior will depend on the value of the dsgIfStdOneWayRecovery MIB. If this MIB is set to scan(2), the eCM will scan for a new downstream channel. If this MIB is set to retryUp(1), the eCM will attempt to re-establish the upstream on the current downstream.

When the DSG eCM enters two-way disabled operation as a consequence of being told by the DSG Client Controller to disable its upstream transmitter, it MUST remain tuned to and process DSG traffic on the DOCSIS downstream channel. At any point in its initialization or operational sequences, when the DSG eCM receives notification from the DSG Client Controller to disable its upstream transmitter, the DSG eCM MUST immediately cease using its upstream transmitter. The DSG eCM MUST then enter DSG Two-way Disabled operation as described in Figure 5–10.

If the eCM is unable to renew its IP address [DOCSIS-RFI], then the eCM MUST move to One-way mode of operation.

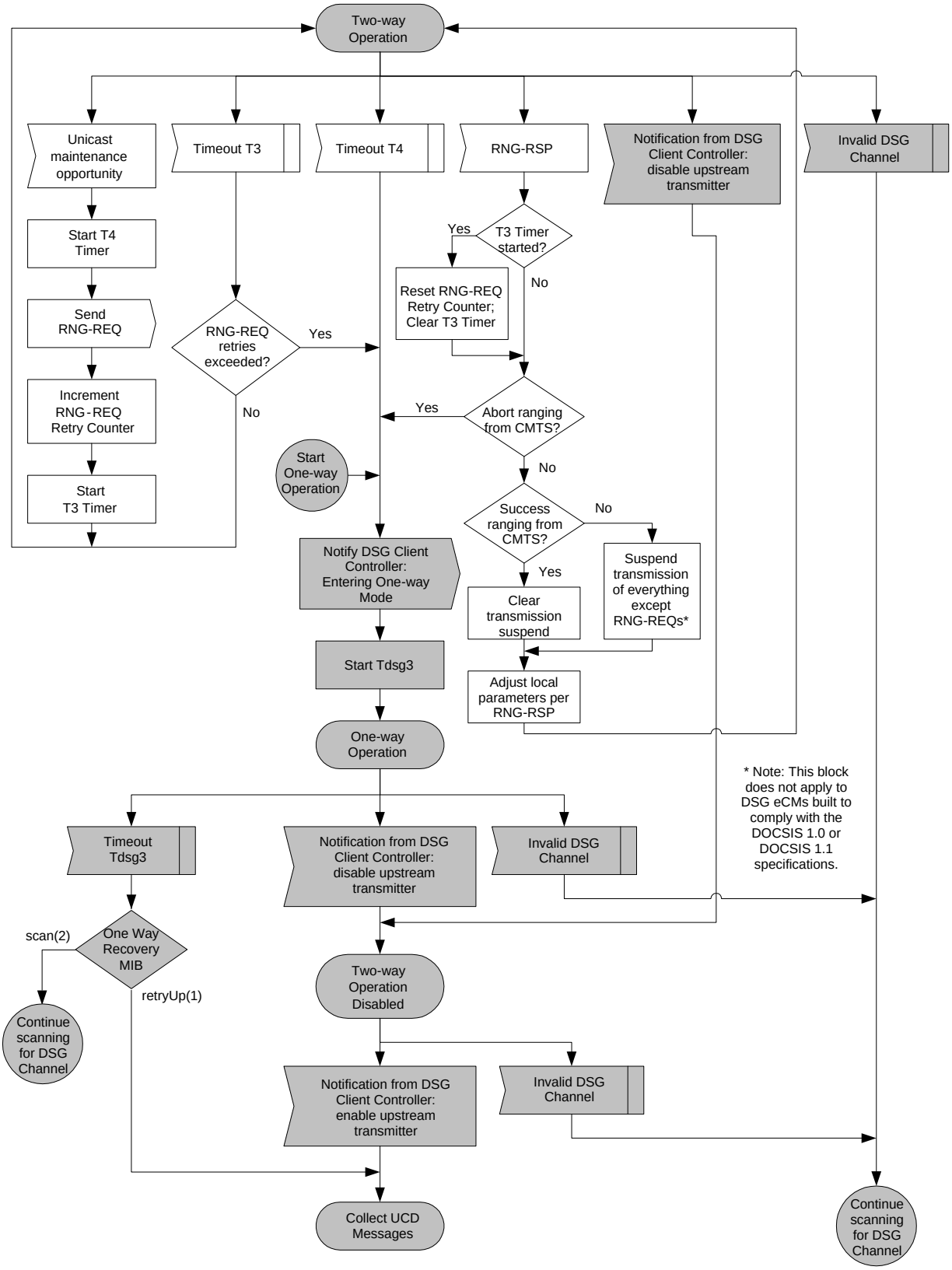


Figure 5–10 - DSG eCM Operation

5.4.3.9 DSG Operation

The DSG tunnel provides OOB information to the DSG Client(s) within the Set-top Device. Multiple DSG tunnels are permitted, each identified by a MAC address. To acquire data from one or more tunnels, the DSG Client Controller must be able to understand the addresses in use to define the tunnels, and must be able to request the appropriate filtering for the DSG Client.

When DSG is operational, the DSG eCM MUST operate as described in Figure 5–11.

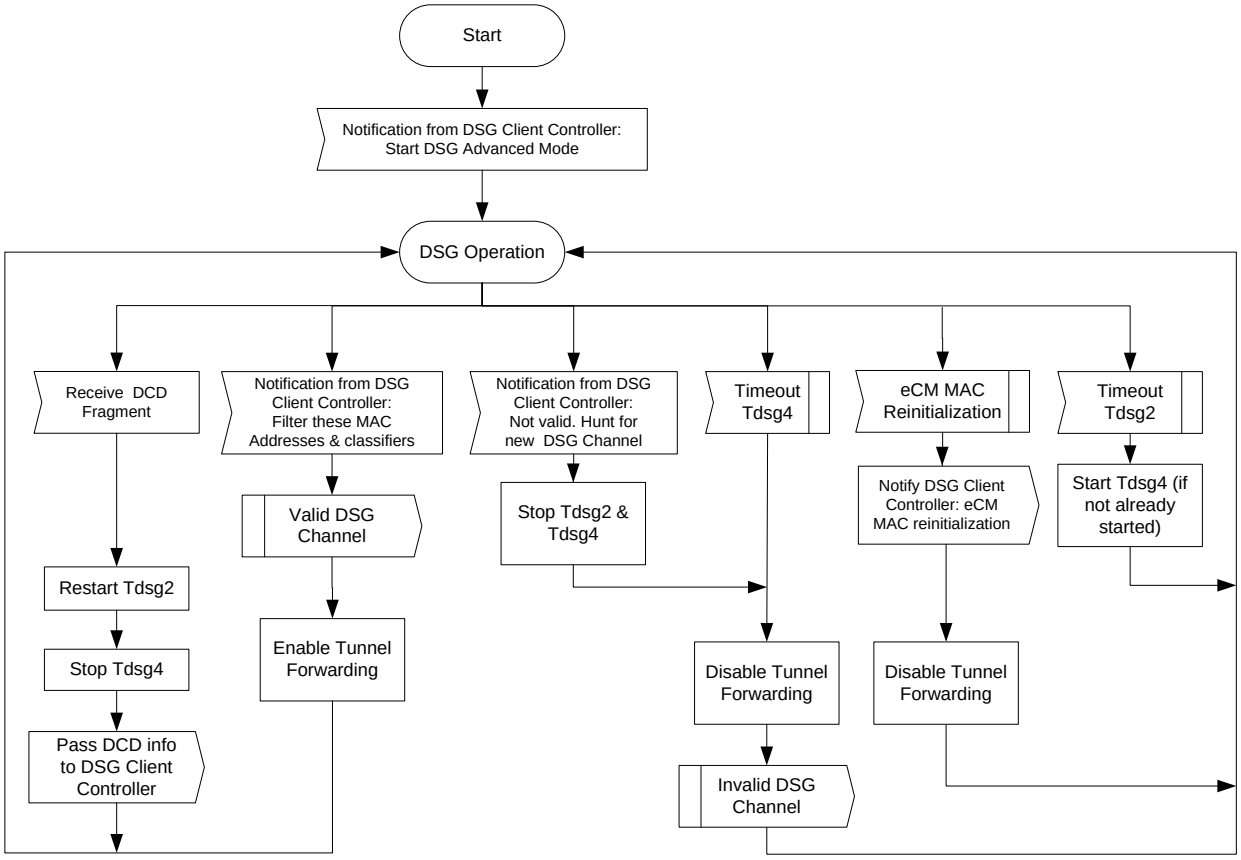


Figure 5–11 - DSG Operation

5.4.4 DOCSIS 3.0 DSG eCM Operation

This section only applies to DOCSIS-3.0 DSG eCMs.

5.4.4.1 DOCSIS 3.0 DSG eCM State Transition Diagrams

The operation of a DOCSIS 3.0 DSG eCM is described here by two separate state machines that operate in parallel. These state transaction diagrams apply only to the eCM.

The first state machine, "DSG 3.0 eCM Initialization and Operation," is covered by the state transition diagrams in Figure 5–12 through Figure 5–28 (and described in Sections 5.4.4.2 to 5.4.4.7).

The second state machine "DSG Operation" is covered by the state transition diagram in Figure 5–30 (and described in Section 5.4.4.8). This state machine provides inputs into the "DSG eCM Initialization and Operation" state machine.

The messages sent between the two state machines, and to and from the DSG Client Controller, are provided in the following sections. There are no messages defined to and from the DSG Client Controller other than the ones already defined in the Pre-3.0 DOCSIS DSG eCM Case.

5.4.4.1.1 Messages sent/received by "DSG eCM Initialization and Operation"

Inputs from the DSG Operation state machine and the Channel Presence validation diagram are:

- Valid DSG Channel
- Invalid DSG Channel
- DSG-Channel Found
- Continue DS Scan.

The Continue DS Scan and the DSG-Channel Found messages are only for DOCSIS 3.0 DSG eCMs but are internal to eCM state machines and do not reach the DSG Client Controller.

Inputs from the DSG Client Controller:

- Disable upstream transmitter
    - When the eCM is operating with Multiple Transmit Channel Mode, this message requires the CM to disable all its upstream transmissions.
- Enable upstream transmitter

Outputs to DSG Client Controller:

- Downstream Scan Completed
- 2-way OK, UCID
    - The reserved value 255 is used for the UCID to maintain compatibility with legacy DSG Client Controller implementations that expect a UCID value.
- Entering One-way Mode
- Cannot forward 2-way traffic, NACO <val>, Max CPE <val>
- DCC Depart, Initialization Type <IT> (where IT = "DCC initialization type")

5.4.4.1.2 Messages sent/received by "DSG Operation"

Inputs from the DSG Client Controller:

- Start DSG Advanced Mode
- Filter these MAC Addresses and Classifiers
- Not Valid. Hunt for new DSG Channel

Outputs to DSG Client Controller:

- DCD Message information
- eCM MAC reinitialization

5.4.4.2 DOCSIS 3.0 DSG eCM Initialization Overview

The following figure corresponds to the "Cable Modem Initialization Overview" figure in [DOCSIS-MULPI]. The difference in the initialization of the DOCSIS 3.0 DSG eCM is scanning for the downstream DSG channel and going to Two-way Operation as opposed to just becoming Operational. This process is described in detail in the following sections.

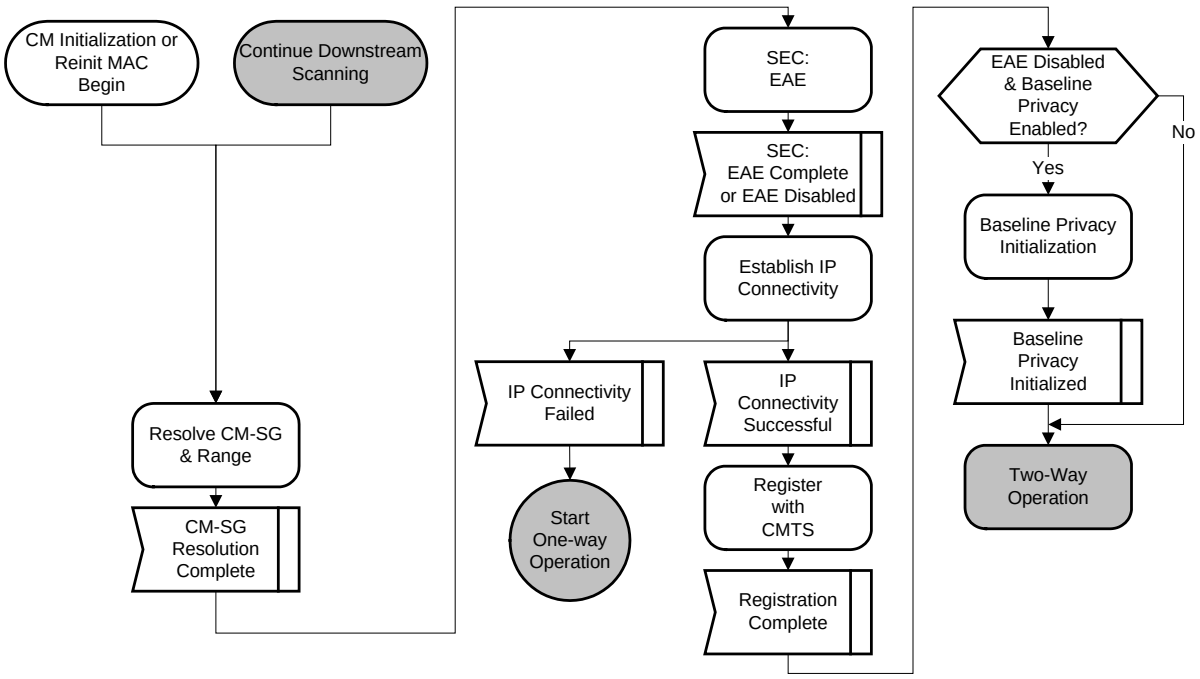


Figure 5–12 - DOCSIS 3.0 DSG eCM Initialization Overview

The DOCSIS 3.0 DSG eCM follows the initialization sequence described below.

The eCM powers up and starts scanning for a primary-capable DOCSIS Downstream channel after its DSG Mode is set to 'DSG Advanced Mode' at startup by the DSG Client Controller. The eCM tries to find a DCD message on the downstream channel on which it locks. If it does not find any DCD messages, it tunes to the next primary capable downstream channel. If the eCM finds DCD messages on the downstream channel, it looks for an MDD message with a source MAC address matching that of the DCD message.

If the eCM does not find an MDD message with the source address matching that of the DCD message, it starts the initialization process as a DSG eCM would on a DOCSIS 2.0 CMTS.

If the eCM finds MDD messages on the downstream channel then it starts the process of Downstream Ambiguity resolution to determine know which MD-DS-SG it belongs to. The MDD provides the different active downstream channels which exist in that MAC Domain.

After DS Ambiguity resolution the eCM sends the DCD message to the DSG Client Controller. If the DSG Client Controller accepts the DCD and signals that the downstream channel is a valid DSG channel, the eCM continues with the rest of the Initialization and registration process. If the DSG Client Controller, signals that the downstream channel is an invalid DSG channel, the eCM scans the other downstream channels in the MD-DS-SG for DCD messages within the MAC domain. The eCM discards any DCD messages that do not have a source MAC address matching that of the MAC domain. The eCM sends any DCD messages it finds within the MAC domain to the DSG Client Controller. If none of the DCDs on the downstream channels within the MAC domain are acceptable to the DSG Client Controller, then the eCM continues with the downstream channel scan to find the next channel with a DCD.

During the Upstream parameter acquisition and ranging process, if the eCM is unable to communicate with the CMTS, then the eCM goes into One-way mode of operation. The same happens for failure to establish IP connectivity or registration failure.

Details of each of the steps above are described in the sections below.

5.4.4.3 DSG eCM Scan For Downstream Channel

The DOCSIS 3.0 DSG eCM will follow the initialization sequence as described in the "Scan for Downstream Channel," and "Continue Downstream channels" sections in [DOCSIS-MULPI].

In addition to acquiring a valid downstream channel, it is necessary that the downstream channel contain appropriate DSG tunnels. If a DOCSIS downstream channel containing the appropriate DSG tunnels cannot be found, then the DSG eCM MUST continue scanning.

The DOCSIS 3.0 DSG eCM MUST NOT start scanning for Downstream Channels before the DSG Client Controller sets the DSG Mode to Advanced.

When operating in DSG Advanced mode, the DSG Client Controller may provide the DSG eCM with a list of downstream frequencies which have been derived from the DSG Channel List portion of the DCD message. This list is meant to aid the DSG eCM in acquiring an appropriate downstream rapidly. Note that once the DSG eCM receives a configuration file via the registration process, the requirements relating to the Downstream Frequency Configuration Setting (TLV-1) and the Downstream Channel List (TLV-41) as described in [DOCSIS-MULPI] still apply.

5.4.4.4 DSG eCM Service Group Discovery and Initial Ranging

This section corresponds to the "Service Group Discovery and Initial Ranging" section in [DOCSIS-MULPI]. The details of the SDL is described in the below sub-sections.

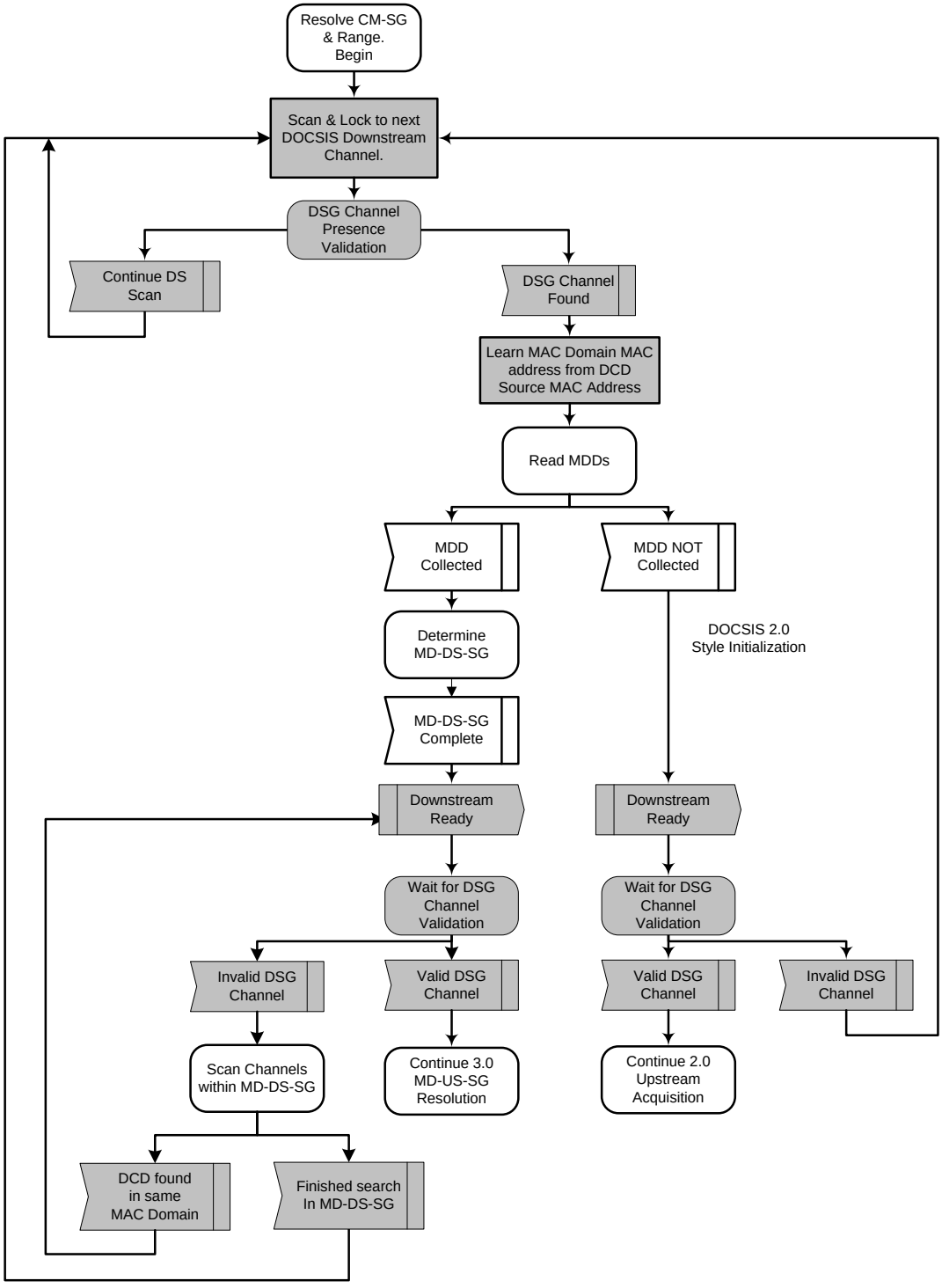


Figure 5–13 - DOCSIS 3.0 DSG eCM Scan and MD-DS-SG-Resolution

The following diagram describes the steps the eCM performs to complete US acquisition and ranging when connected to a DOCSIS 3.0 downstream channel or to acquire an upstream when connected to a DOCSIS 2.0 downstream.

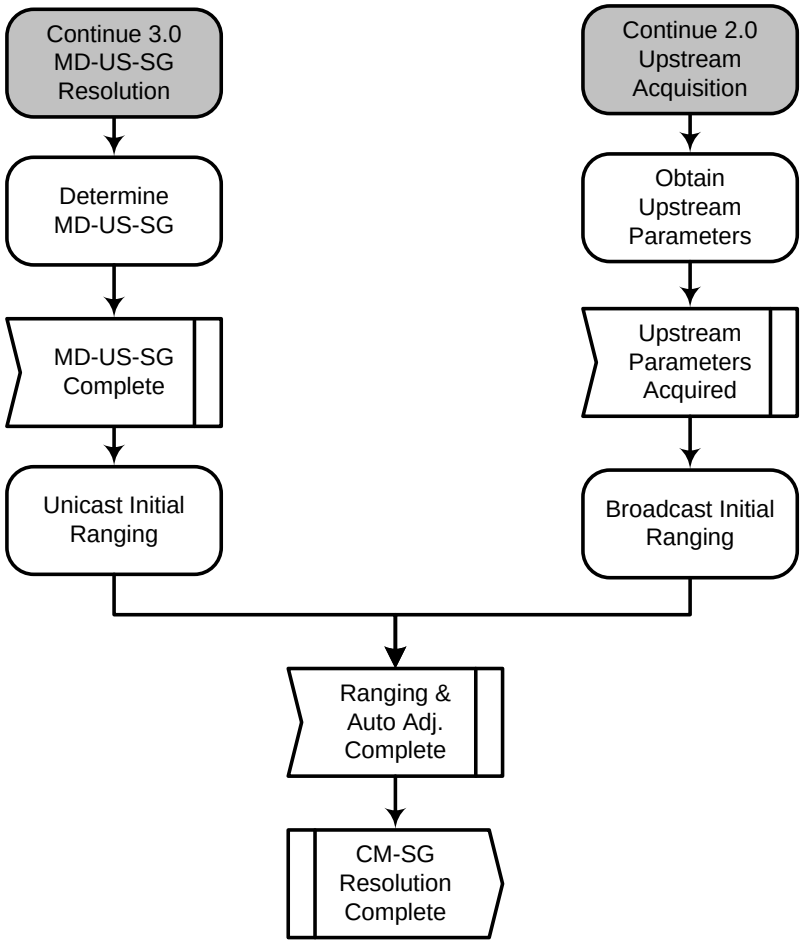


Figure 5–14 - Continue Upstream Acquisition

5.4.4.4.1 DOCSIS 3.0 DSG Channel Presence Validation

This section describes the process by which a DOCSIS 3.0 DSG eCM determines the presence of a valid DSG channel. This was part of the DSG operation State machine for the Pre-3.0 DOCSIS DSG eCMs, but was separated out for DOCSIS 3.0 as there was a need to complete the DSG channel validation prior to completing the Downstream Ambiguity Resolution. The DOCSIS 3.0 DSG eCM starts the Tdsg1 timer and waits to find a DCD message fragment. If the Tdsg1 timer times out the eCM continues downstream scanning. If the eCM finds a DCD message it stops the Tdsg1 timer and sends a 'DSG channel found' message to the downstream scan state machine.

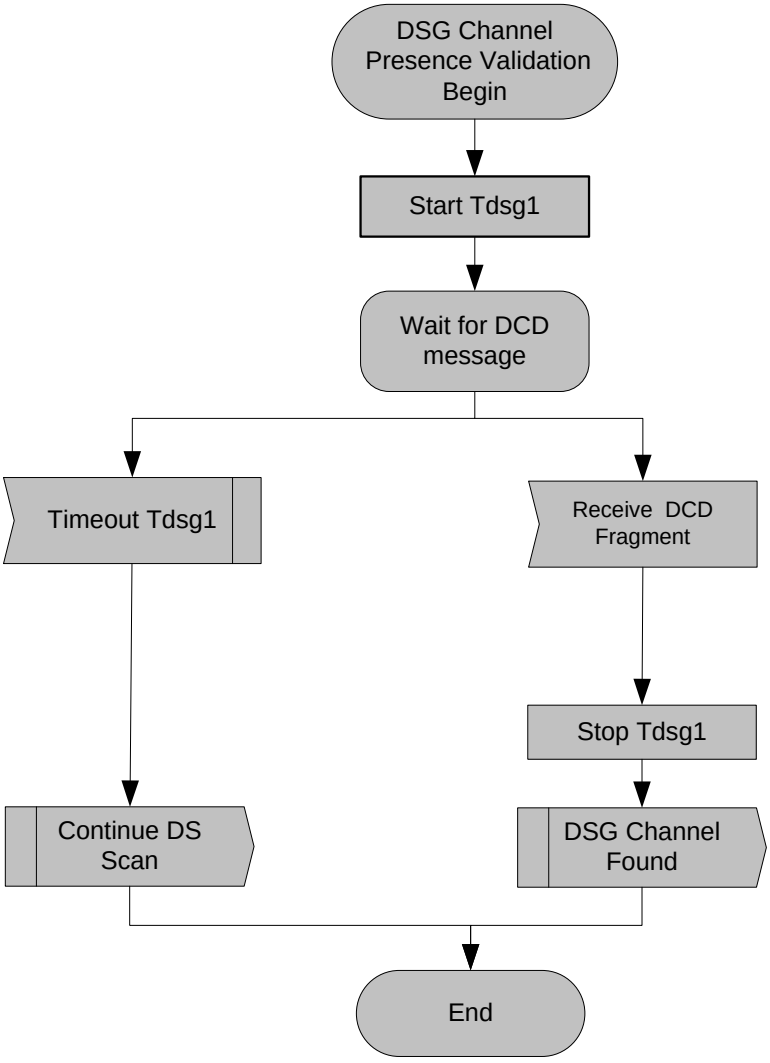


Figure 5–15 - DSG Channel Presence Validation

5.4.4.4.2 Read MAC Domain Descriptor (MDD)

This section corresponds to the "Read MAC Domain Descriptor (MDD)" section in [DOCSIS-MULPI]. This describes how the eCM looks for MDD messages on a downstream. The process is a little different from what is in [DOCSIS-MULPI]. As the eCM sees MDD message fragments on the downstream, it compares the Source MAC Address of the newly collected fragment to the MAC domain Address of the DCD message. Only if the address matches does the eCM collect the MDD fragment. A DOCSIS 3.0 DSG eCM MUST NOT use an MDD message whose source MAC address does not match that of the DCD message.

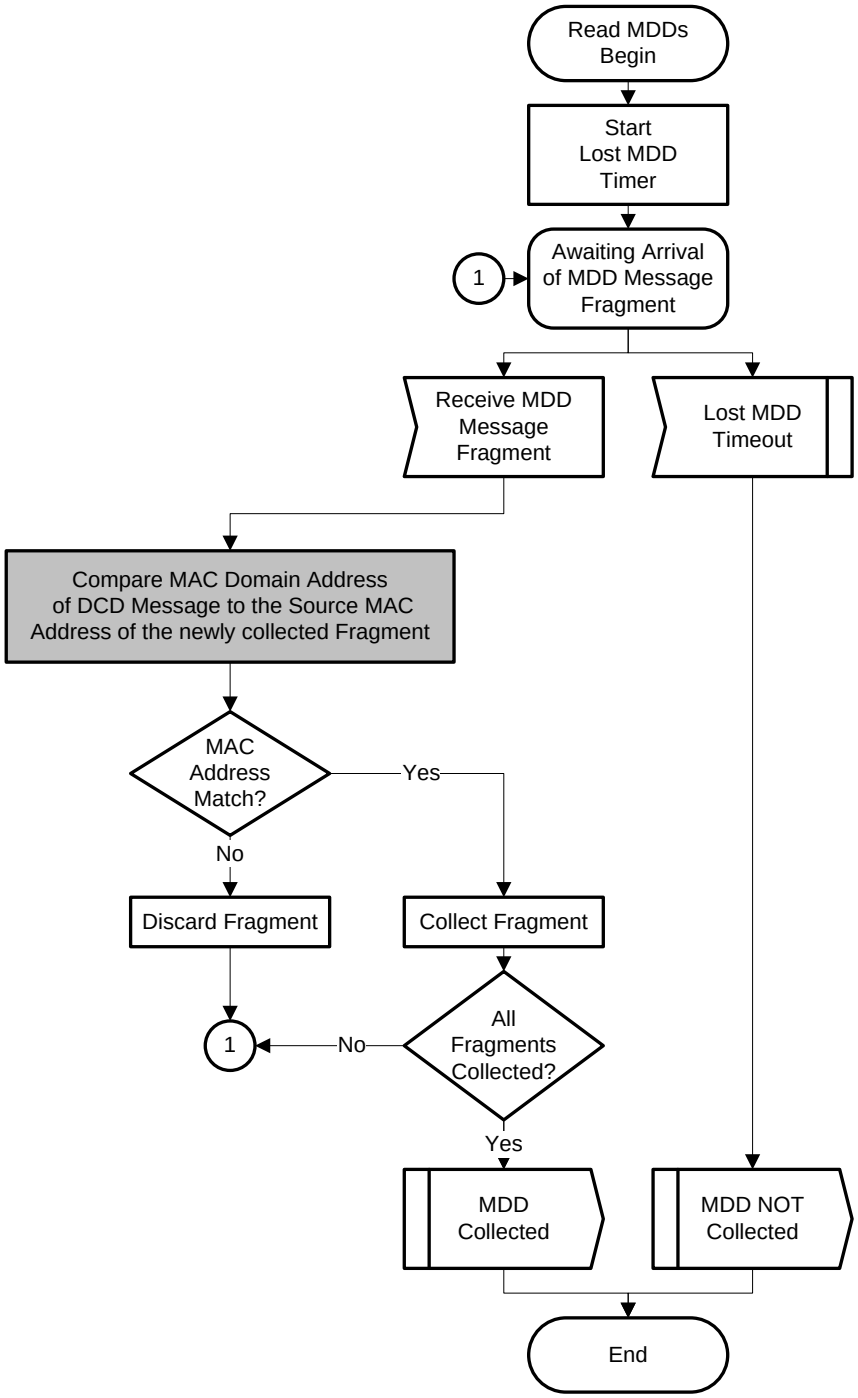


Figure 5–16 - Read MDD

5.4.4.4.3 Determination of MD-DS-SG

This section corresponds to the "Determination of MD-DS-SG (MDD)" section in [DOCSIS-MULPI]. This describes how the eCM determines its downstream Service group and this process is unchanged from as defined in MULPI. This Downstream Ambiguity resolution needs to be completed prior to sending the stream of DCD messages to the DSG Client Controller.

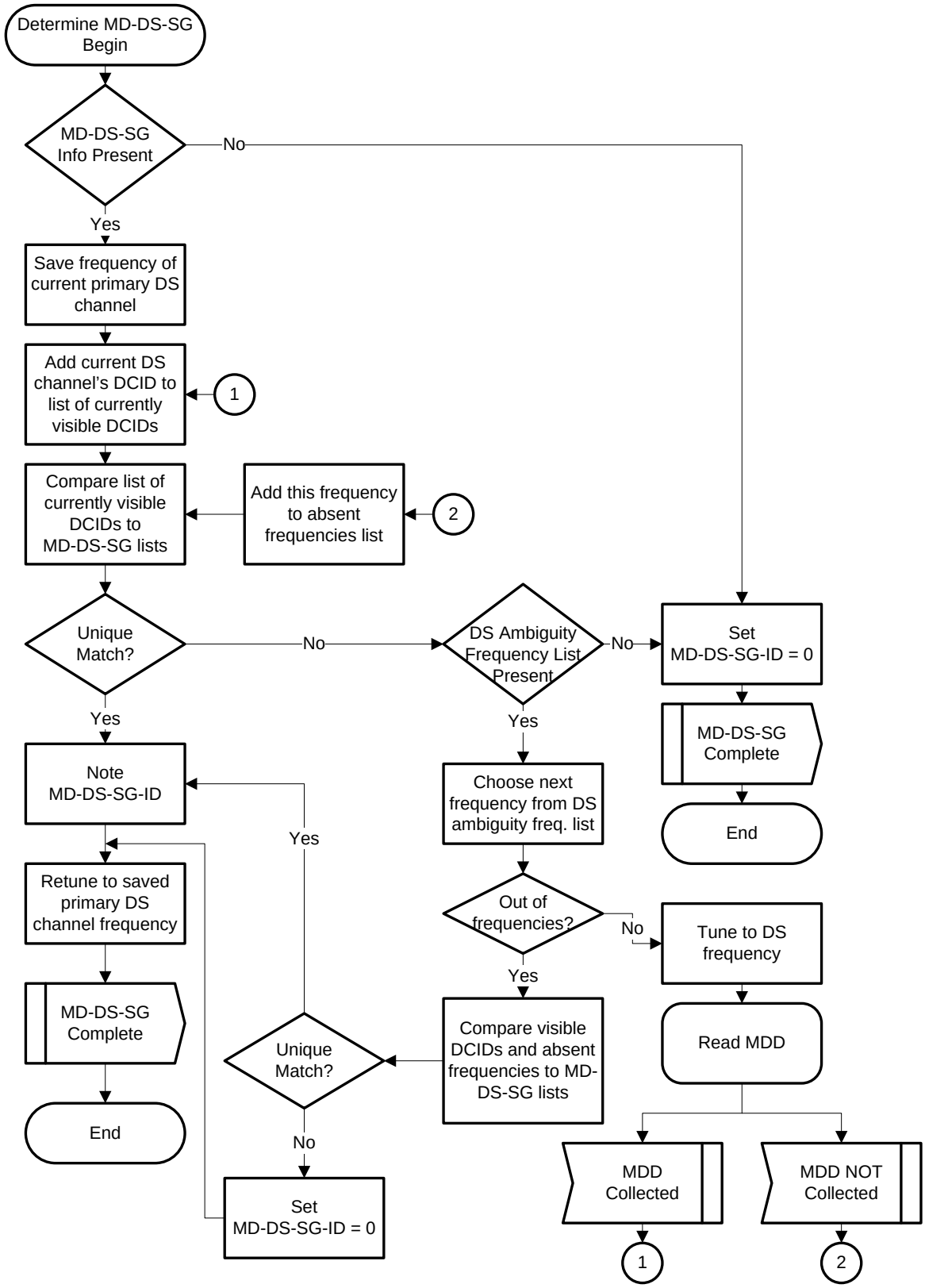


Figure 5–17 - Determine MD-DS-SG

5.4.4.4.4 Wait for DSG channel Validation

The "Wait for DSG channel Validation" is an DSG eCM wait state where the DSG eCM waits till it gets a message from the DSG Client Controller specifying if the DSG channel was a valid one or not.

5.4.4.4.5 Scan DS channels within MD-DS-SG

If the DSG Client Controller signals that the downstream channel is an invalid DSG channel then the eCM first scans to other downstream channels in the MD-DS-SG. When scanning for channels within the MAC Domain the eCM first chooses channels in common with the channels present in the DSG Channel List (from the DCD). If there is a DSG Channel List present and it does not include any channels in the MAC Domain, the eCM is not required to try every single channel within MD-DS-SG.

For each of the downstream channels, if the eCM finds DCDs (within the same MAC Domain), it forwards the DCD on to the DSG Client Controller. The eCM discards DCDs received from different MAC domains and continues scanning to other downstream channels.

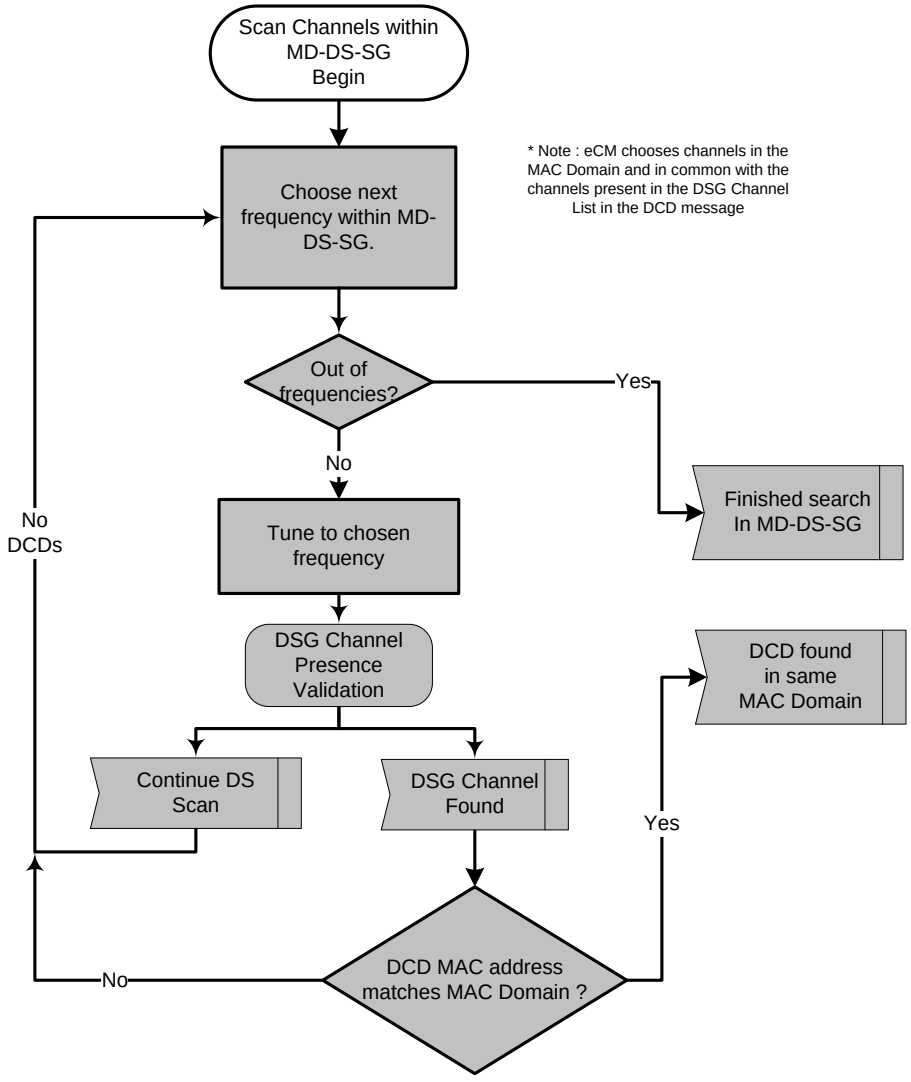


Figure 5–18 - Scan Channels within MD-DS-SG

5.4.4.4.6 Determine MD-US-SG

This section corresponds to the "Determination of MD-US-SG" section in [DOCSIS-MULPI]. This describes the steps the eCM needs to perform to complete MD-US-SG resolution. The behavior here is the same as in MULPI except when the eCM is out of candidate UCIDs, the DSG eCM starts One-way mode of operation. The eCM also checks for ranging Hold-off direction per [DOCSIS-MULPI].

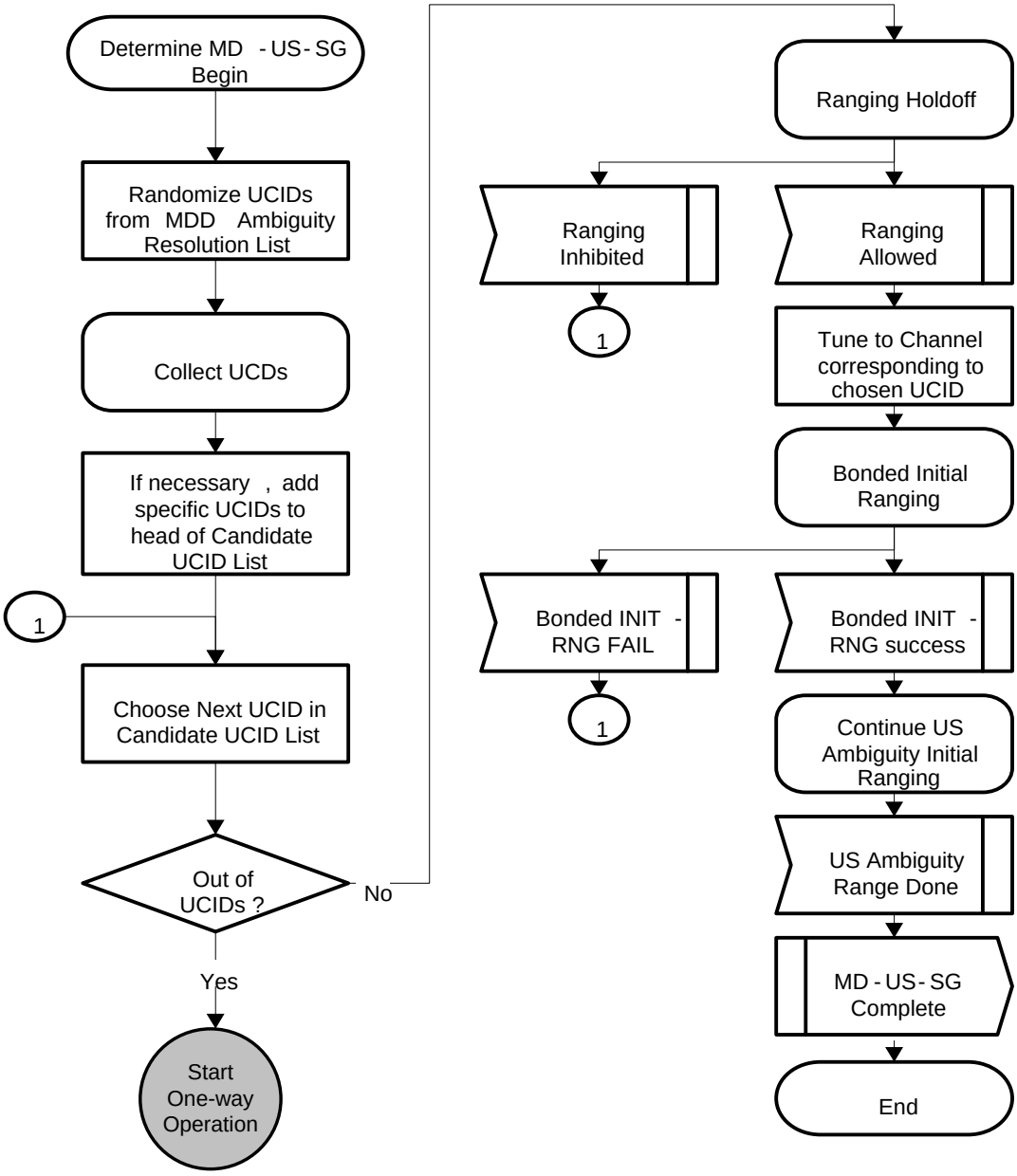


Figure 5–19 - Determine MD-US-SG

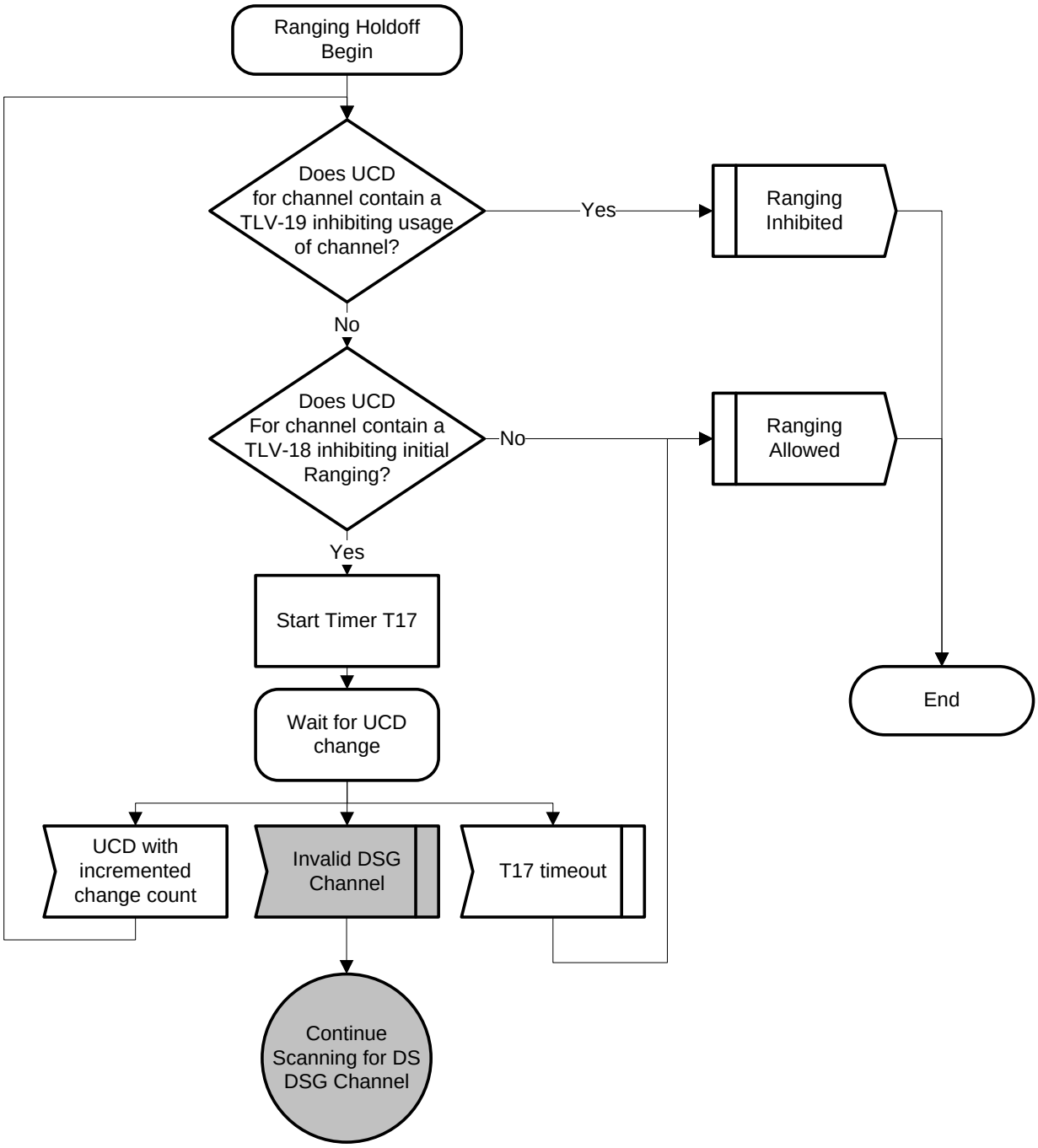


Figure 5–20 - Determine Ranging Hold-Off

5.4.4.4.6.1 Bonded Initial Ranging

This section corresponds to the "Bonded Initial Ranging" section in [DOCSIS-MULPI]. This describes how the eCM performs Bonded Initial Ranging. The behavior here is the same as in MULPI except when the eCM receives a Ranging Abort, the DSG eCM starts One-way mode of operation.

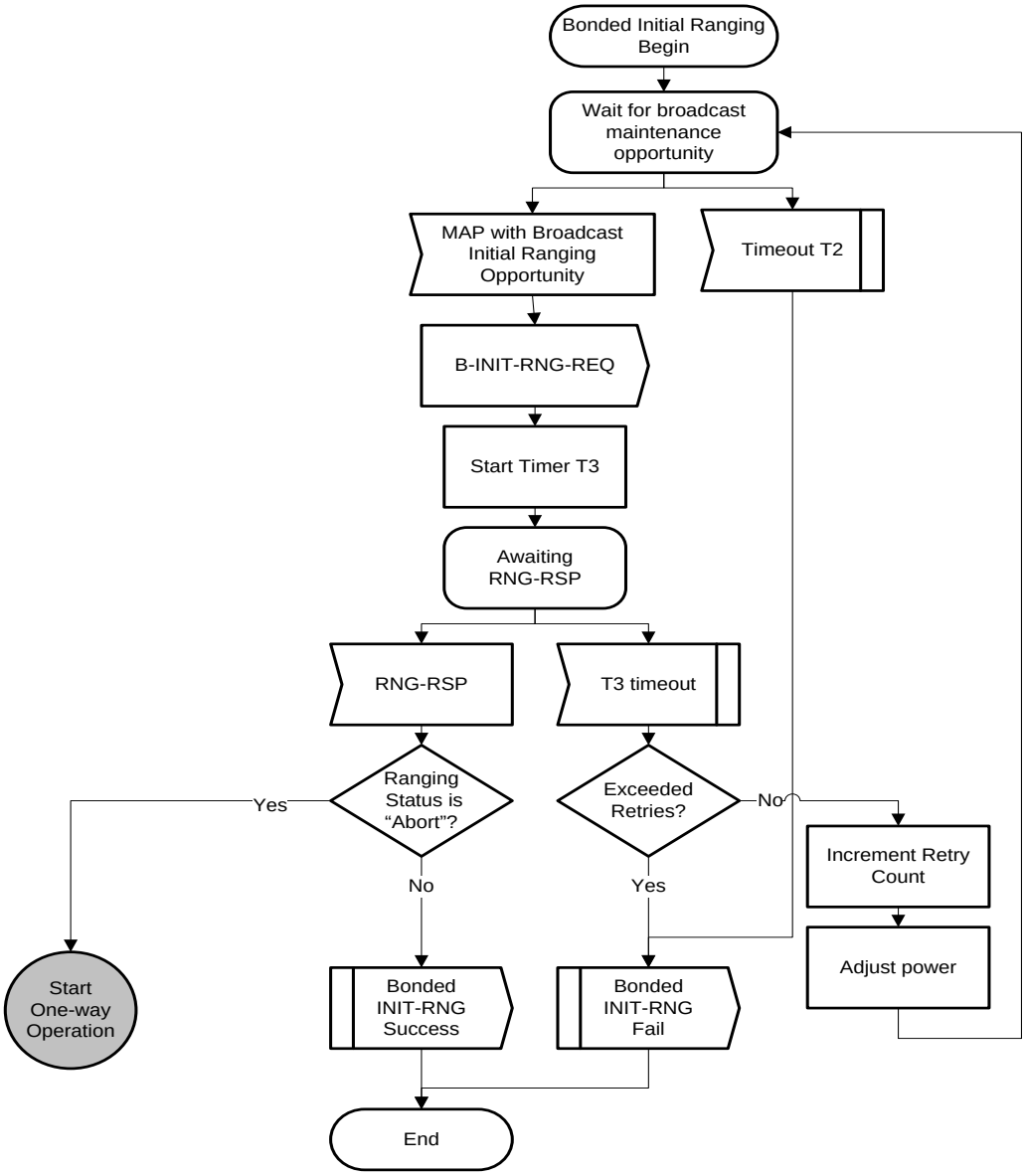
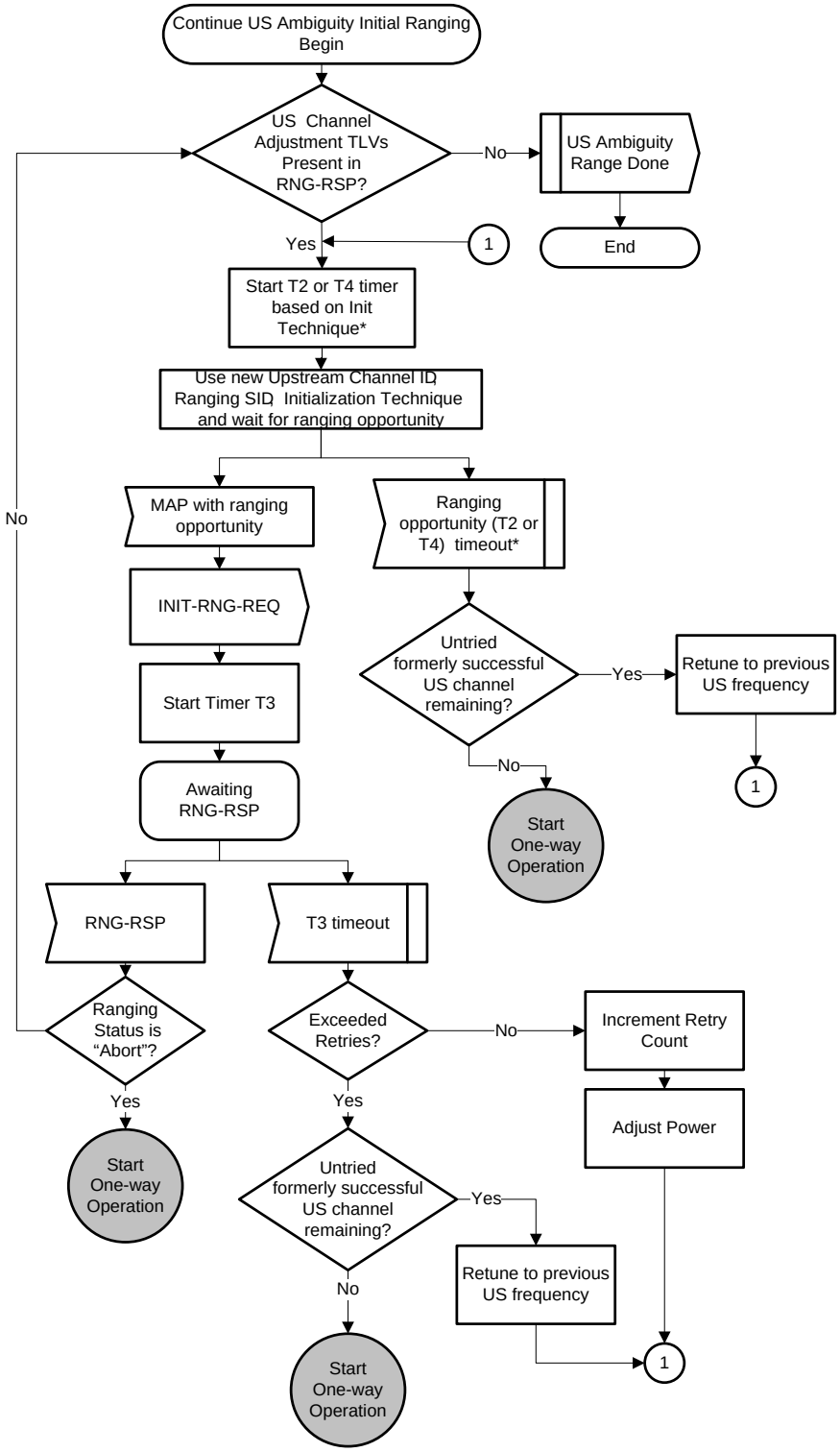


Figure 5–21 - Determine MD-US-SG

5.4.4.4.6.2 Continue US Ambiguity Initial Ranging

This section corresponds to the "Continue US Ambiguity Initial Ranging" section in [DOCSIS-MULPI]. This describes how the eCM performs upstream Ambiguity Initial Ranging. The behavior here is the same as in MULPI except when the eCM is unable to range and no more untried US channels remain and on a Ranging Abort, the DSG eCM starts One-way mode of operation.



***Note:** The ranging opportunity timeout is dependent on the Initialization Technique attribute in the current adjustment request. If Technique 1 is used then the timeout value is T2. If Initialization Techniques 2 or 3 are used the timeout value is T4.

Figure 5–22 - Continue US Ambiguity Initial Ranging

5.4.4.4.7 Obtain Upstream Parameters

This section corresponds to the "Obtain Upstream Parameters / Try Next Upstream (DOCSIS 2.0 Initialization)" section in [DOCSIS-MULPI]. This describes the steps the eCM needs to perform to complete upstream acquisition when connected to a 2.0 downstream channel. The behavior here is the same as in MULPI except on a T1 timeout, the DSG eCM starts One-way mode of operation.

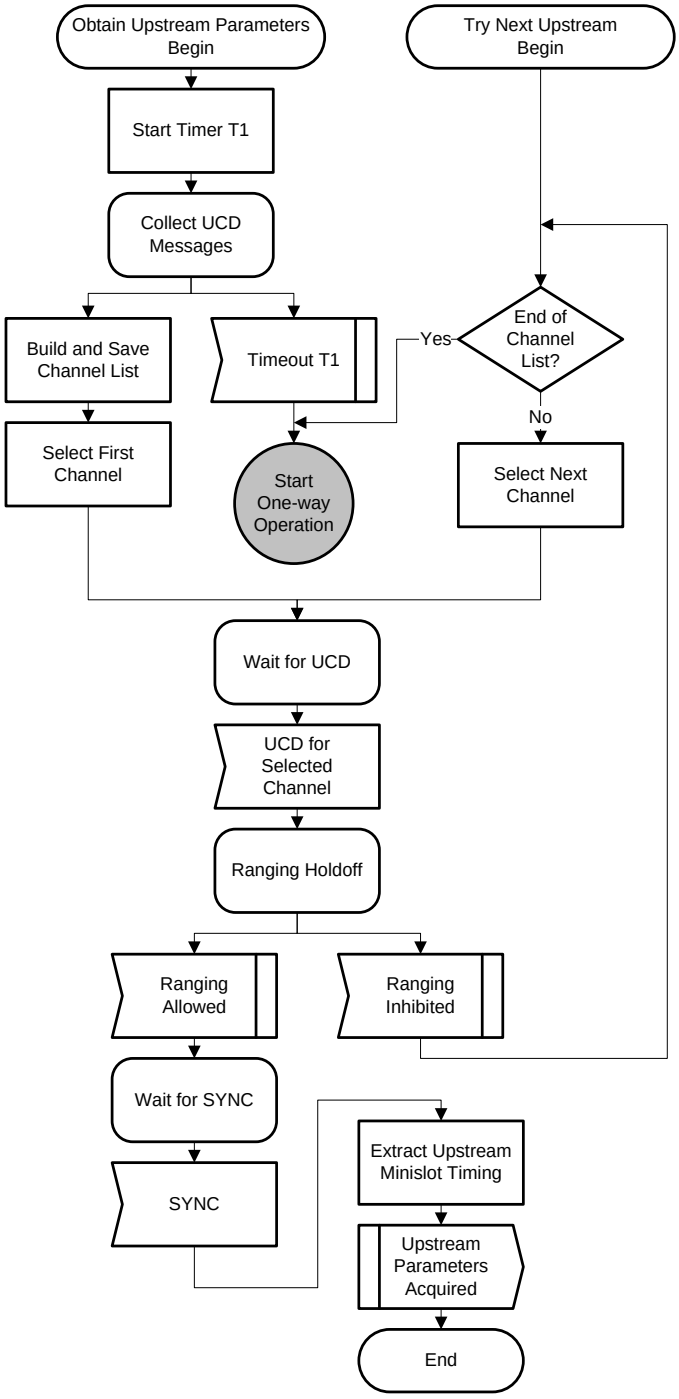


Figure 5–23 - Obtain Upstream Parameters

5.4.4.4.8 Broadcast Initial Ranging

This section corresponds to the "Ranging and Automatic Adjustments" section in [DOCSIS-MULPI]. This describes the steps the eCM needs to perform to complete ranging and adjustment of transmitting parameters. The behavior here is the same as in MULPI except on a Range Abort from the CMTS, the DSG eCM starts One-way mode of operation.

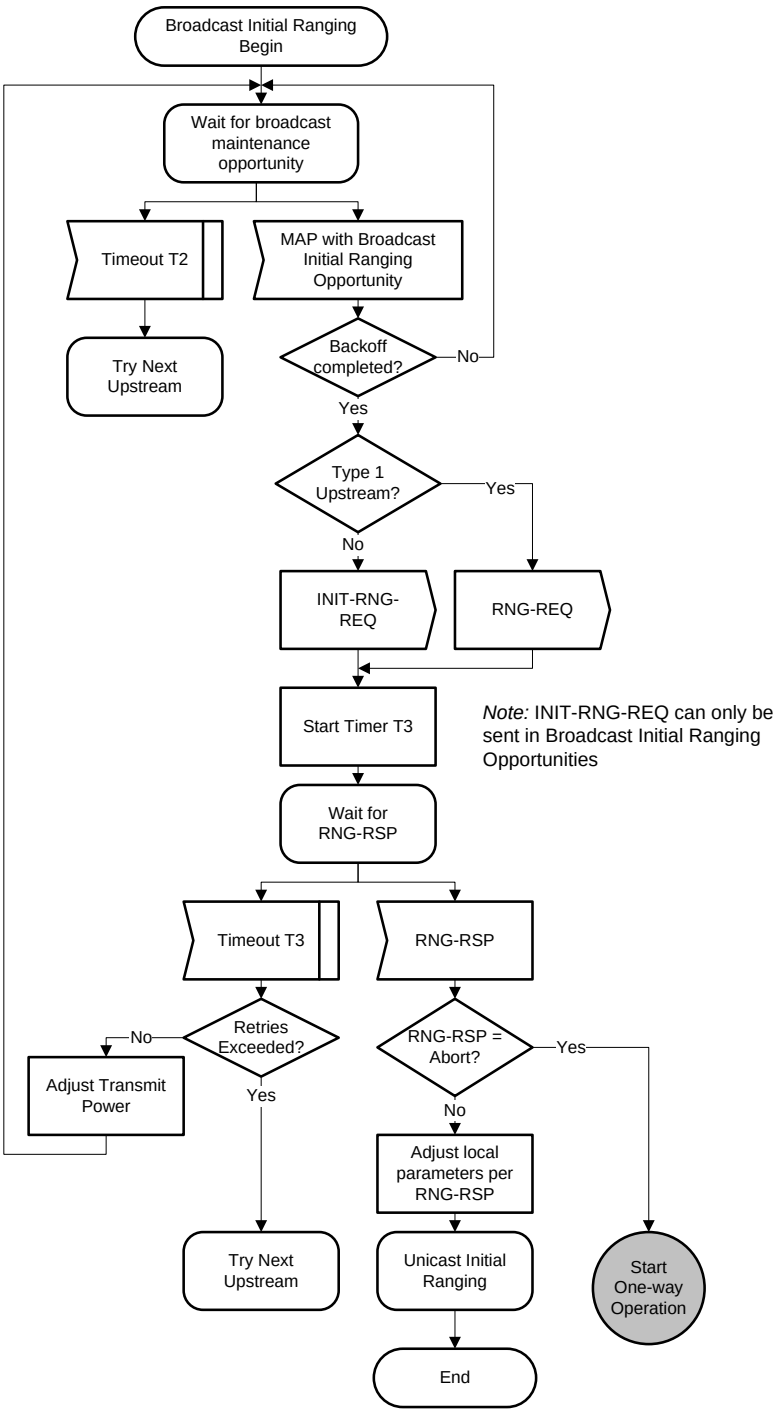


Figure 5–24 - Broadcast Initial Ranging

5.4.4.4.9 Unicast Initial Ranging

This section corresponds to the "Ranging and Automatic Adjustments" section in [DOCSIS-MULPI]. This describes the steps the eCM needs to perform during Unicast Initial Ranging. The behavior here is the same as in MULPI except on T4 timeouts, Retires exceeded after T3 timeouts and a Range Abort from the CMTS, the DSG eCM starts One-way mode of operation.

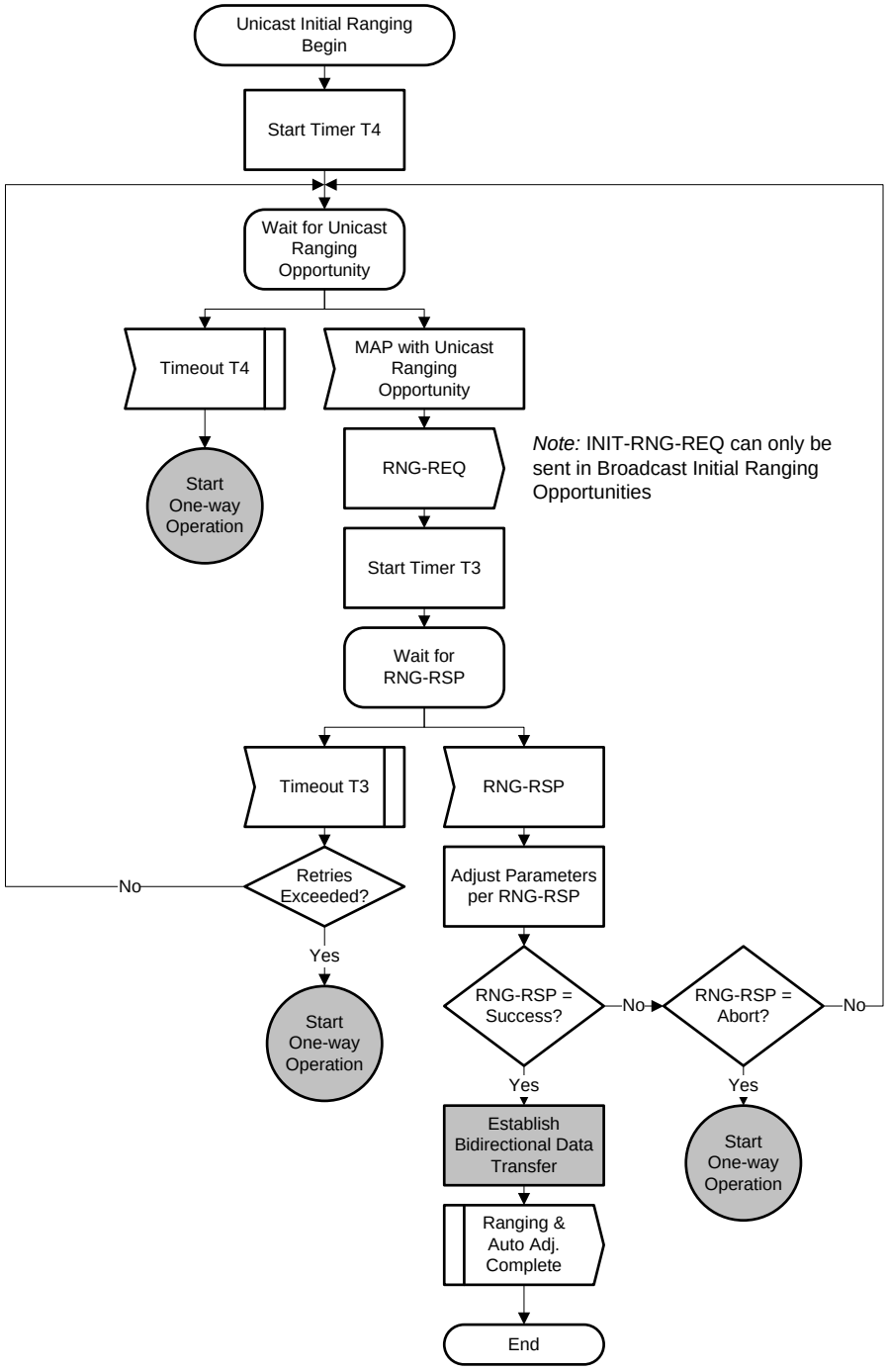


Figure 5–25 - Unicast Initial Ranging

5.4.4.5 Establishing IP Connectivity

This section corresponds to the "Establishing IP connectivity" section in [DOCSIS-MULPI]. This describes the steps the eCM performs to acquire a management IP address for itself. The eCM can obtain an IPv4 or IPv6 management address. The behavior here is the same as in MULPI.

If the IP connectivity step fails the eCM goes into One-way mode of operation (Figure 5–12).

5.4.4.6 Registration with the CMTS

This section corresponds to the "Registration with the CMTS" section in [DOCSIS-MULPI]. This describes the steps the eCM needs to perform during registration with a CMTS. The behavior here is the same as in MULPI except where noted below and in the diagrams in this section. When acquiring CM transmit channels, if a failure occurs on all the upstreams or the number of retires is exhausted after a T6 timeout then the eCM begins One-way mode of operation.

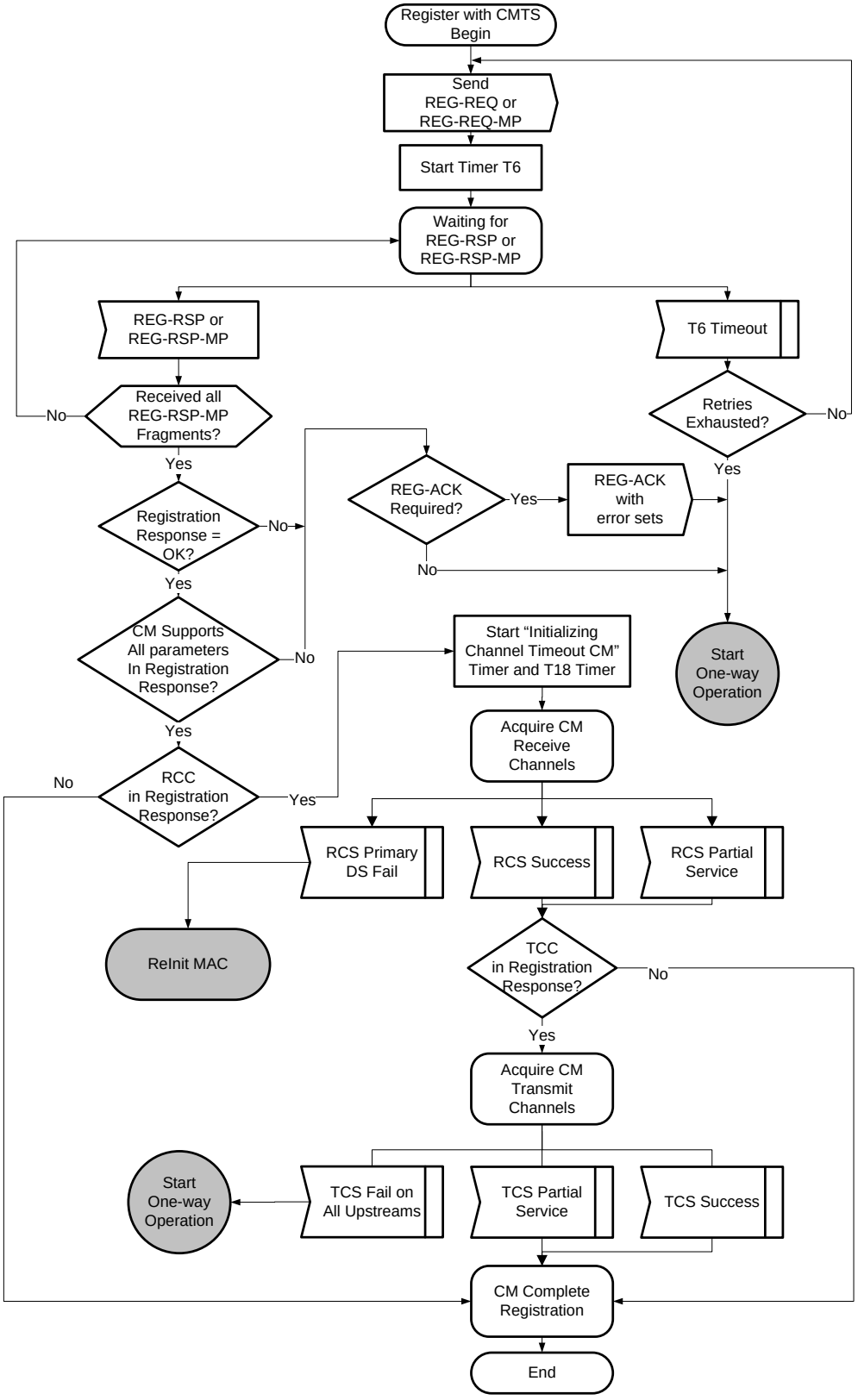


Figure 5–26 - CM Registration with CMTS

5.4.4.6.1 CM Acquire Receive and Transmit Channels

This section corresponds to the "Registration with the CMTS" section in [DOCSIS-MULPI]. This describes the steps the eCM performs during registration when the CM starts to acquire all the Receive and Transmit Channels as directed by the CMTS. The behavior here is the same as defined in MULPI.

5.4.4.6.2 CM Completes Registration

This section corresponds to the "Registration with the CMTS" section in [DOCSIS-MULPI]. This describes the steps the eCM performs during registration after the CM completes Receive and Transmit Channel acquisition. The behavior here is the same as in [DOCSIS-MULPI] except if the REG-ACK retries are exceeded or if the primary upstream service flow cannot be established the eCM Starts One-way mode of operation. Also, after registration is complete the eCM sends a Notification message to the DSG Client Controlled that "Two-way operation" is OK.

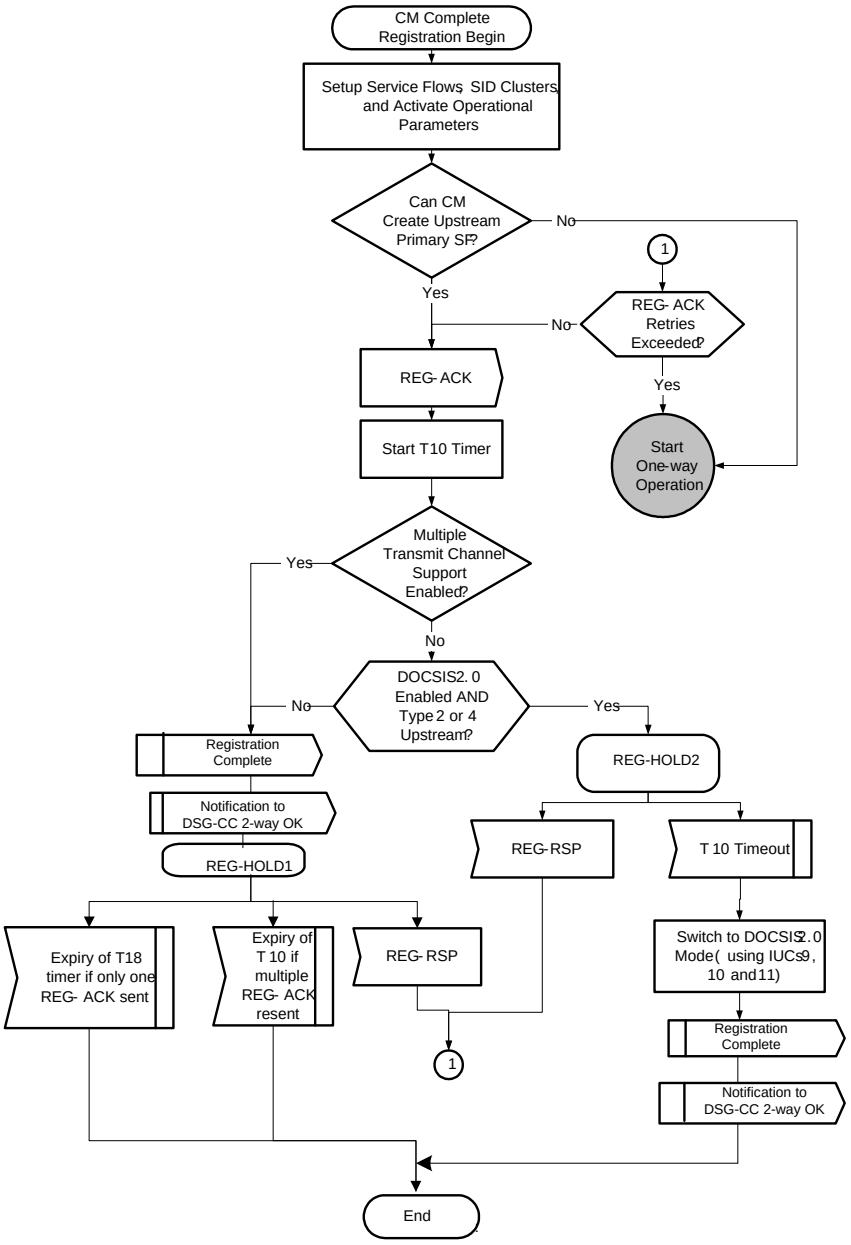


Figure 5–27 - CM Completes Registration

5.4.4.7 DOCSIS 3.0 DSG eCM Operation

This section corresponds to the "Periodic Maintenance" section in [DOCSIS-MULPI]. Like the DOCSIS Pre-3.0 DSG eCM, the 3.0 DSG eCM uses the same the concepts of One-way Operation, Two-way Operation Disabled, and the reception of an Invalid DSG Channel notification. The messages sent between the DSG Client Controller and the DSG eCM are detailed in Section 5.4.4.1.1.

When the DSG eCM enters One-way mode of operation as a consequence of any of the timeouts or error conditions indicated in the preceding sections, it MUST remain tuned to and process DSG traffic on the primary downstream channel. If the eCM enters One-way mode of operation as a result of loss of downstream sync, the eCM MAY disable the Tdsg3 timer and refrain from attempting two-way operation until downstream sync is re-established. If the CM loses downstream sync temporarily, the eCM can still receive DSG tunnel data, but will be unable to transmit on the upstream. As long as the CM receives the DCD messages and DSG tunnel data, eCM stays on the downstream, unless there is loss of DCD messages or DSG tunnel data on that downstream channel.

When the DSG eCM enters two-way disabled operation as a consequence of being told by the DSG Client Controller to disable its upstream transmitter, it MUST remain tuned to and process DSG traffic on the DOCSIS downstream channel. At any point in its initialization or operational sequences, when the DSG eCM receives notification from the DSG Client Controller to disable its upstream transmitter, the DOCSIS 3.0 DSG eCM MUST immediately cease using all of its upstream transmitters. The DSG eCM MUST then enter DSG Two-way Disabled operation as described in Figure 5–28 below.

When the eCM is in One-way mode of operation, and the Tdsg3 timer times out, the resulting behavior depends on the value of the dsgIfStdOneWayRecovery MIB. If this MIB is set to retryUp(1), the eCM will "Attempt to Reestablish Upstream" (Figure 5–29) and attempt to collect the MDD to ensure that no parameters have changed. If the eCM successfully collects an MDD, then it will compare the Configuration Change Count field to the value of this field in the previously collected MDD, if any. The eCM MUST reinitialize its MAC if the Configuration Change Count field has changed. This procedure ensures consistent behavior with non-DSG devices.

When any of the following occur:

- the eCM is in One-way mode of operation and the eCM receives an "Invalid DSG channel message" from the DSG Client Controller, or
- the eCM is in Two-way operation disabled and the eCM receives an "Invalid DSG channel message" from the DSG Client Controller, or
- dsgIfStdOneWayRecovery is set to scan(2)

then the eCM resumes the scan for new Downstream channels. In addition, when dsgIfStdOneWayRecovery is set to scan(2), the "eCM MAC Reinitialization" message is sent to the state machine in Figure 5–30, resulting in a transition to the DSG HOLD state.

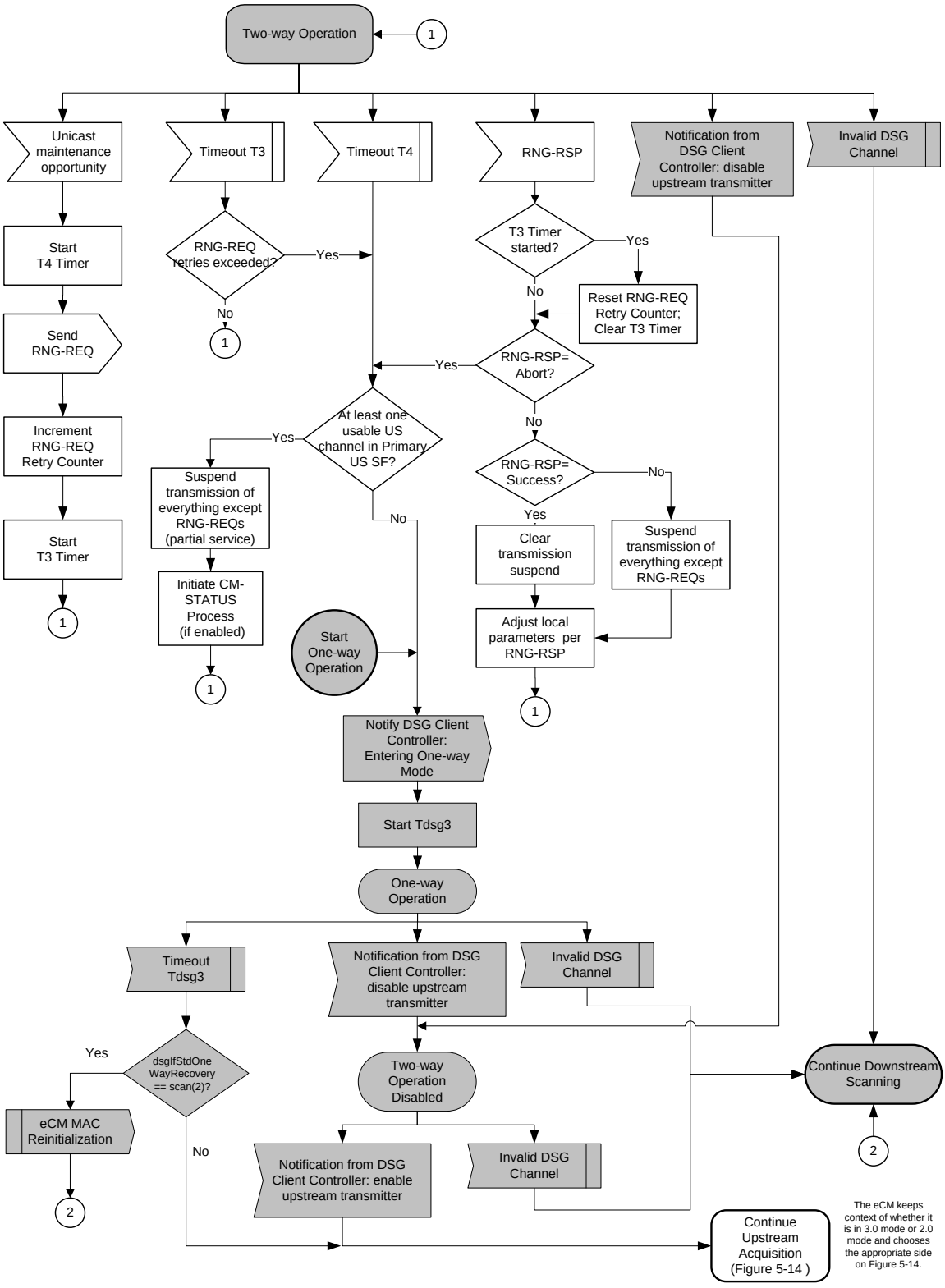


Figure 5–28 - eCM Operation

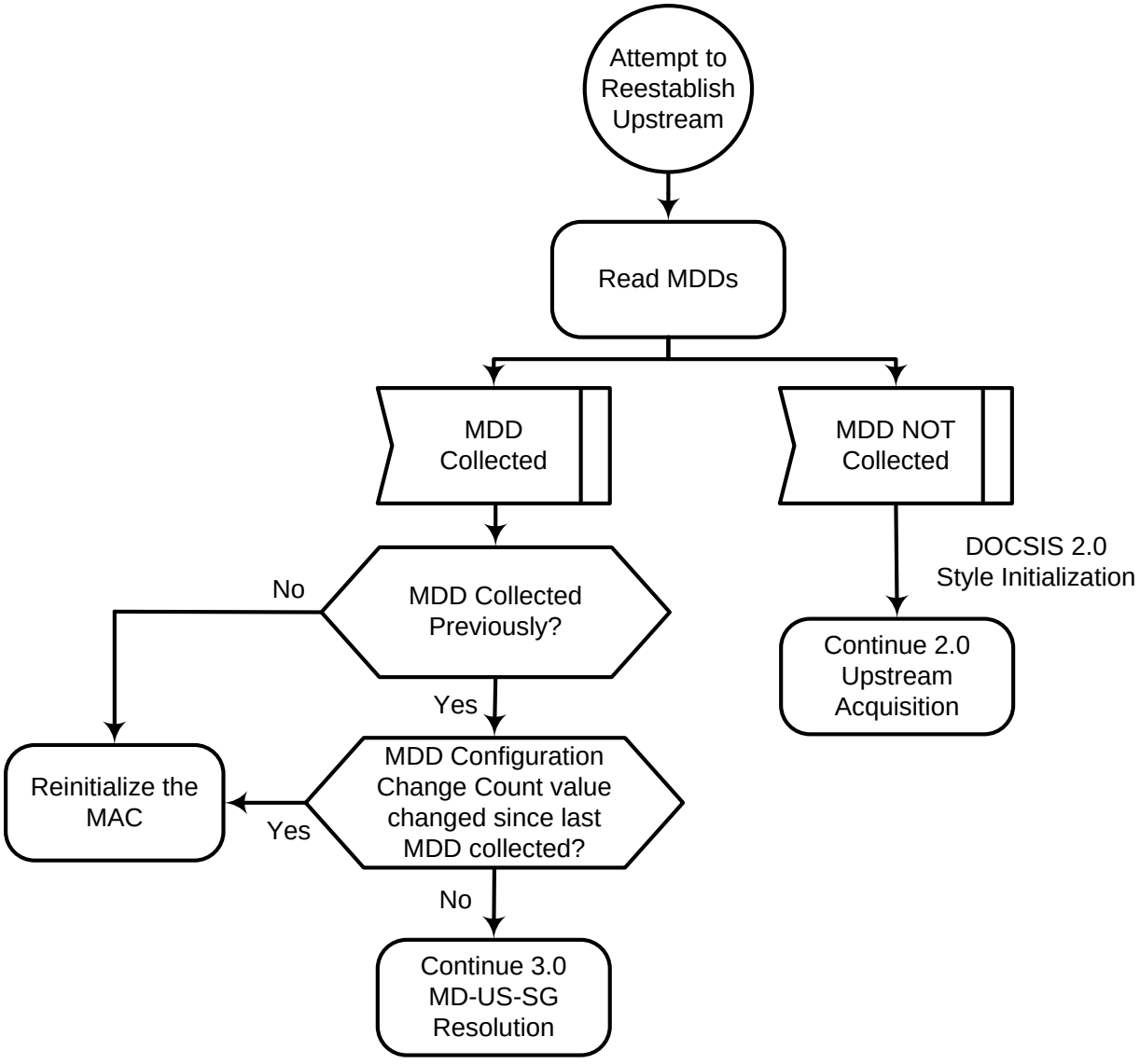


Figure 5–29 - Attempt to Reestablish Upstream

If the eCM is unable to renew its IP address then the eCM MUST move to One-way mode of operation.

NOTE: When the eCM is configured to provision in APM or DPM, it should not enter One-way mode of operation unless it cannot obtain either an IPv4 or an IPv6 address ([DOCSIS-MULPI]).

5.4.4.7.1 Multiple Transmit Channel (MTC) mode and Partial Service considerations

In DOCSIS 3.0, Multiple Transmit Channel Mode (MTC Mode) provides mechanisms and capabilities that enable Upstream Channel Bonding. If a CM is operating in MTC Mode, all of its service flows, whether assigned to a single channel or to an upstream bonding group, operate with the mechanisms that are supported in MTC Mode.

Whenever one or more channels in the Transmit Channel Set (TCS) and/or the Receive Channel Set (RCS) are unusable, that CM is said to be operating in a "partial service" mode of operation in the upstream and/or downstream respectively. A channel is deemed to be unusable when the CM is unable to acquire one or more channels during registration and/or DBC, or if a CM lost an upstream and/or downstream channel during normal operation.

If the eCM loses all of the upstream channels on which the primary upstream service flow is assigned, the eCM enters the One-way mode of operation.

5.4.4.8 DOCSIS 3.0 DSG Operation

The DSG tunnel provides OOB information to the DSG Client(s) within the Set-top Device. Multiple DSG tunnels are permitted, each identified by a MAC address. To acquire data from one or more tunnels, the DSG Client Controller must be able to understand the addresses in use to define the tunnels, and must be able to request the appropriate filtering for the DSG Client.

The DOCSIS 3.0 DSG eCM MUST discard DCD messages and DSG tunnel packets not received on its Primary Downstream channel. The DOCSIS 3.0 DSG eCM MUST discard DCD messages and message fragments whose source MAC address does not match that of the MDD that the eCM is using on its Primary Downstream.

When DSG is operational, the DOCSIS DSG eCM MUST operate as described in Figure 5–30.

This DSG operational diagram is similar to the one defined for Pre-3.0 DOCSIS DSG eCMs, but with differences as defined below.

The diagram introduces a 'DSG HOLD' state because the eCM completes Downstream Ambiguity resolution prior to sending a DCD message to the DSG Client Controller. When the eCM receives a notification from the DSG Client Controller, to start Advanced mode, it moves into this DSG Hold state. It waits there until it receives the "Downstream Ready" message from the "DSG 3.0 eCM DS scan and MD-DS-SG Resolution" portion of the eCM Initialization sequence. The "Downstream Ready" message communicates that the eCM has successfully acquired a DOCSIS 2.0 downstream channel or acquired a DOCSIS 3.0 downstream channel and completed the downstream ambiguity resolution process for that downstream. Once it receives the "Downstream Ready" message, the eCM moves to the DSG-Operation state.

When in the DSG Operation state, either on notification from the DSG Client Controller that the DSG channel is invalid or if the Tdsg4 timer times out, then the eCM sends out the Invalid DSG Channel message to the "DSG eCM operation" state machine and goes to the DSG HOLD state. It waits there until the eCM finds another valid Downstream Channel. This way the eCM will not forward the new DCD messages from a particular downstream unless the DS ambiguity resolution process has been completed from that new downstream channel since the DS ambiguity resolution process could potentially break the flow of DCD messages to the DSG Client Controller.

Another change from the Pre-3.0 DOCSIS DSG Operation diagram is that the eCM does not signal the "DCD present" message to the DSG 3.0 eCM DS scan and MD-DS-SG Resolution part of the Initialization sequence. This has been replaced by the DOCSIS 3.0 DSG Channel Presence Validation [Section 5.4.4.4.1].

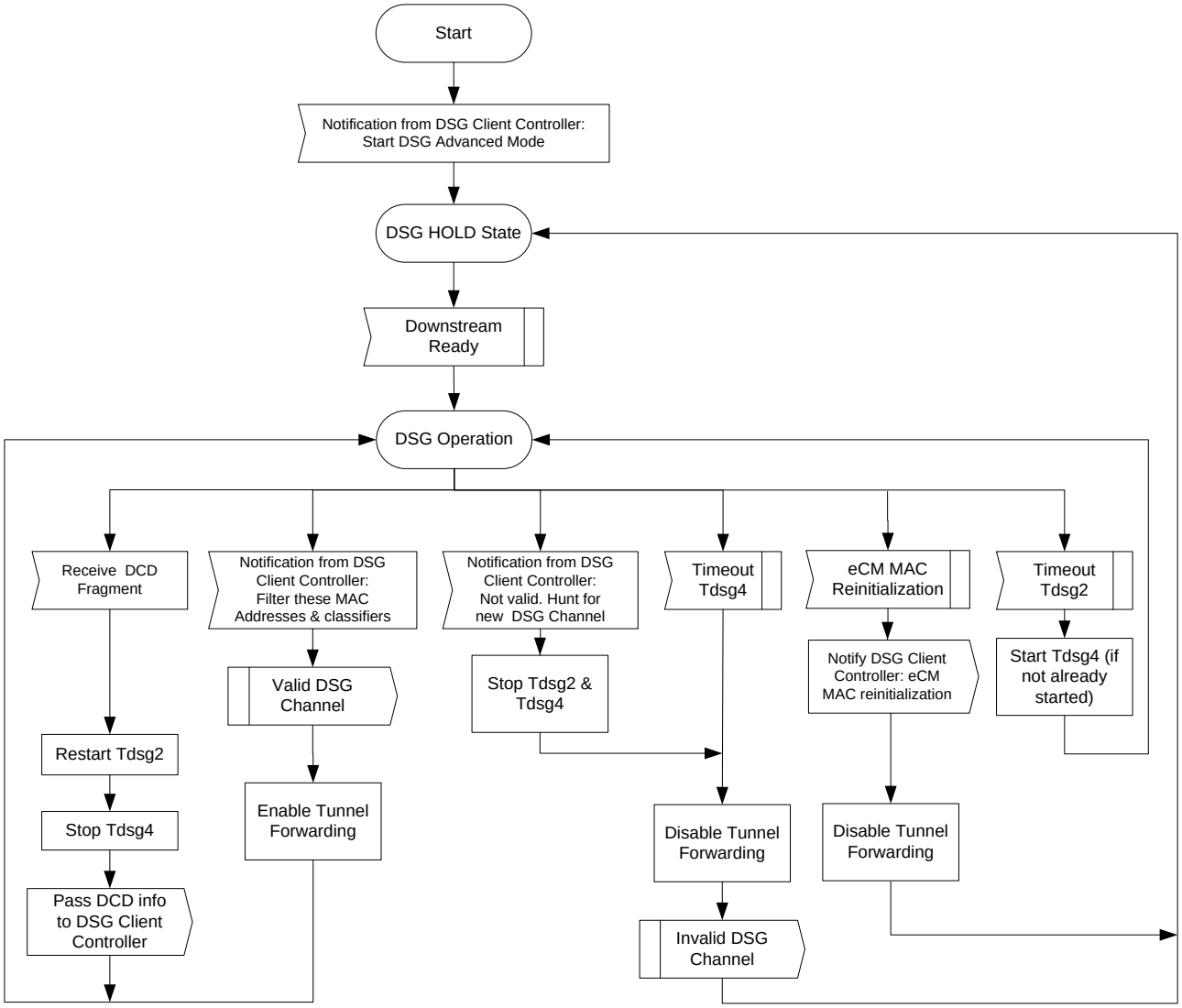


Figure 5–30 - DOCSIS 3.0 DSG Operation

5.4.5 Tunnel Acquisition and Handling

5.4.5.1 DSG Advanced Mode Tunnel Acquisition and Handling

When operating in DSG Advanced Mode, the DSG eCM MUST comply with the following DSG tunnel acquisition requirements:

- The DSG eCM MUST pass the contents of the DCD to the DSG Client Controller and allow the DSG Client Controller to determine the appropriateness of the current downstream channel.
- The DSG eCM MUST NOT forward DSG Tunnel data to the DSG Client(s) until the appropriate filters have been set based upon information received from the DSG Client Controller. When MDF is enabled, the MDF-capable DSG eCM uses the DSID from the DSG DA-to-DSID Association Entry TLV in the MDD message to forward the appropriate DSG. The DSG Tunnel Address is not used as a filtering criterion.
- If MDF is enabled, the MDF-capable DSG eCM MUST re-learn the DSG Tunnel DSID(s) in the DSG DA-to-DSID Association Entry TLVs of the MDD message after a DBC or DCC transaction that changes the primary downstream channel. If the DSID used to carry DSG tunnel traffic is unknown to it, the MDF-capable DSG eCM will not be able to forward DSG Tunnel frames.

- Once these filters have been set, the DSG eCM MUST begin forwarding DSG Tunnel data to the DSG Client(s), whether it is operating in One-way mode or Two-way mode.
- The DSG eCM MUST only forward DSG Tunnel data to the DSG Client that matches these filters.
- The DSG eCM MUST dynamically replace these filters if instructed to do so by the DSG Client Controller.
- If the DSG eCM transitions from a Two-way to a One-way mode of operation, it MUST continue to forward the same DSG Tunnels to the DSG Client(s) unless instructed to do otherwise by the DSG Client Controller.

5.4.5.2 DA-to-DSID Association of DSG Tunnels in DOCSIS 3.0

DOCSIS 3.0 defines the DSG DA-to-DSID Association Entry TLV in the MDD message to convey the association between a DSID and a Group MAC Address used for DSG tunnel traffic [DOCSIS-MULPI].

The DSG Agent MUST include one instance of the DSG DA-to-DSID Association Entry TLV for each DSG Tunnel address in the MDD message unless it has been configured to disable Multicast DSID Forwarding on a Global or MAC Domain basis. The DSG Agent MUST NOT use a given DSID value in more than one instance of the DSG DA-to-DSID Association Entry TLV. The DSG Agent MUST NOT modify DSID values in the DSG DA-to-DSID Association Entry TLV in the MDD message. The only time that the DSG Agent modifies the DSG DA-to-DSID Association Entry TLV in the MDD message is when it modifies the DCD message due to the addition or deletion of DSG rules. The DSG Agent MUST add new DA-to-DSID mappings to the DSG DA-to-DSID Association Entry TLV in the MDD message when it adds new DSG tunnels to the DCD message. The DSG Agent MUST delete existing DA-to-DSID mappings from the DSG DA-to-DSID Association Entry TLV in the MDD message when it deletes DSG tunnels from the DCD message. When it includes the DSG DA-to-DSID Association Entry TLV in the MDD message, the DSG Agent MUST label DSG tunnel traffic with the associated DSID which is communicated in the DSG DA-to-DSID Association Entry.

If it has been configured to disable Multicast DSID Forwarding on a Global or MAC Domain basis, the DSG Agent MUST NOT include the DSG DA-to-DSID Association Entry TLV in the MDD message. The DSG Agent MUST NOT disable Multicast DSID forwarding on individual DSG eCMs when it includes the DSG DA-to-DSID Association Entry TLV in the MDD message.

Prior to registration, the presence or absence of the DSG DA-to-DSID Association Entry TLV in the MDD message indicates whether Multicast DSID Forwarding is enabled on the DSG eCM. If the MDD message contains the DSG DA-to-DSID Association Entry TLV, the MDF-capable DSG eCM MUST perform DSID based filtering and forwarding of DSG tunnel traffic. An MDF-capable DSG eCM uses the information in the DSG DA-to-DSID Association Entry TLV to ascertain the DSIDs to use for each multicast group MAC address for which it needs to forward DSG Tunnel data.

The absence of either the MDD message or the DSG DA-to-DSID Association Entry TLV in the MDD message indicates that Multicast DSID Forwarding is disabled on the MDF-capable DSG eCM. If no MDD is present on the downstream channel or the MDD message does not contain the DSG DA-to-DSID Association Entry TLV, the MDF-capable DSG eCM MUST filter and forward DSG tunnel traffic based on the DSG Tunnel address.

After registration, the value returned by the CMTS in the Multicast DSID Forwarding capability encoding in the Registration Response message indicates whether Multicast DSID Forwarding is enabled on the MDF-capable DSG eCM. A DSG eCM with MDF-enabled continues to use its previously learned DA-to-DSID mappings to forward DSG Tunnel data.

When MDF is enabled, it may be necessary for the MDF-capable DSG eCM to update its DSIDs. When it receives an indication of a change to its DSG tunnels, the MDF-capable eCM MUST update its application of the DSG DA-to-DSID Association Entry TLV in the MDD message to DSG tunnel filters.

Because a DSG Agent might use distinct DA-to-DSID mappings on each primary-capable downstream channel within a MAC Domain, the MDF-capable DSG eCM re-learns the DSG DA-to-DSID Association Entries in the MDD message after it completes a DBC or DCC transaction that changes the primary downstream channel when MDF is enabled.

5.5 Security Considerations

Since DSG must be capable of working on a one-way plant, the BPI or BPI+ protocols as currently defined are not available for use.

Security considerations for a DSG system that include DSG Servers, DSG Agents, and DSG Clients can be grouped into two categories: receiver based and sender based.

5.5.1 Receiver Based

Receiver based broadly refers to ensuring the content is received by the desired end points and no others.

The MAC address for the DSG Tunnel provides a basic but unsecured way of choosing which end points will receive the content from the DSG Tunnel. Should the DSG Client IDs be placed in the public domain, then it may be possible for a subscriber to adopt that MAC address and begin receiving DSG Tunnel content.

In DSG Advanced Mode, this mode of operation is enhanced by allowing the DSG Agent to substitute new values for the DSG Tunnel Address.

Since none of these techniques are fully secure, the Set-top Device Manufacturer is expected to provide application layer encryption which would run between the DSG Server and the DSG Client, and would protect any sensitive DSG Tunnel content.

5.5.2 Sender Based

Sender based broadly refers to ensuring the content that is received by the Set-top Device originated from the correct sender. This can be accomplished by specifying operating procedures at the Set-top Device and the CMTS.

In DSG Advanced Mode, a packet filter may be installed in the DSG Client which further qualifies the packets in the DSG Tunnel by adding access control based upon the source IP address, destination IP address, and destination UDP port. If the CMTS and the IP network can prevent packets from illegally entering the Head End IP Network with these fields set to the values of the DSG Tunnel, then an enhanced layer of security can be achieved.

Since none of these techniques are fully secure, the Set-top Device Manufacturer is expected to provide an application layer protocol that will allow the Set-top Device to authenticate the sender of the content of the DSG Tunnel.

The CMTS which hosts the DSG Agent MUST ensure that other network protocols (such as ARP, DHCP, DOCSIS Registration, BPKM signaling, etc.) do not associate the destination MAC address of the DSG Tunnel with a non-DSG IP Address, or do not disassociate the destination MAC address of the DSG Tunnel from its designated DSG IP Address.

NOTE: This provision is to prevent a security threat in which an external entity sends in a packet or signaling message on any inbound CMTS interface which infers ownership by that external entity of a MAC address in use by a DSG Tunnel. In such a scenario, unless specifically prevented, other protocols in the CMTS could create false associations of DSG Tunnel MAC Addresses to other IP addresses. It is worth noting that most of these security concerns can be negated by using a multicast (group) MAC address for the DSG Tunnel (see DSG Advanced Mode), since the above protocols generally operate in conjunction with IP flows with unicast (individual) MAC addresses.

The CMTS which hosts the DSG Agent MUST NOT allow any packets sourced from the DOCSIS upstream to be retransmitted to a DSG Tunnel or to prevent the operation of the DSG Tunnel.

NOTE: This provision is to prevent a security threat in which an external entity connected to a DOCSIS CM sends a packet which imitates a packet from the DSG Server with the intent of having that packet be retransmitted to the DSG Tunnel. This provision also identifies and disallows a Denial-of-Service scenario where packets sent from a single entity on a DOCSIS Upstream are not allowed to shut down the operation of a DSG Tunnel.

5.6 Interoperability

5.6.1 DSG and IP Multicast

On the DSG Agent Network Side Interface (NSI) the DSG Agent MUST advertise, via a multicast routing protocol, the multicast routes/groups that are configured in the DSG Agent.

On the DSG Agent RF Side Interface (RFI), IP Multicast Addresses that are associated with DSG Tunnels via the DCD message MUST NOT be managed by IGMP. As such, the downstream channel carrying the DCD message MUST be considered to be "statically joined" to each multicast group included in the DCD message. For these associated multicast groups, the DSG Agent MUST ignore any IGMP messages (membership queries, membership reports, leave messages) on the RF interface. Also, the DSG Agent MUST not generate IGMP messages (group-specific queries, membership reports, leave messages) on the RF interface.

In accordance with [RFC 3171] and [IANA], the DSG Agent is not required to support IP Multicast Addresses in the ranges indicated as RESERVED in [RFC 3171]. These addresses should not be used for DSG Tunnels.

In the case of IP Multicast, where the destination IP address is multicast and the DSG Tunnel Address has been derived from [RFC 1112], then the DSG Rule MUST include a DSG Classifier with an entry for the destination IP address. This is required because the addressing algorithm in [RFC 1112] allows up to 32 IP addresses to map to the same MAC address.

By including a source IP address and source IP mask in the DSG Classifier, Source-Filtered Multicast, and Source-Specific Multicast [RFC 3569] like operations can be used. The DSG Agent is not required to support source IP mask values other than 255.255.255.255 in DSG Classifiers that include a destination IP address in the range indicated for source-specific multicast [RFC 3171].

NOTE: When using a [RFC 1112] derived MAC address, the format of a DSG Tunnel will be identical to that of a standard IP Multicast packet over DOCSIS. The difference between a DSG Tunnel and an IP Multicast over DOCSIS session is the signaling protocol for setting up the session. The DSG Tunnel uses the DCD Message, while the standard multicast session over DOCSIS would be using IGMP.

NOTE: By default, DOCSIS 1.0 cable modems forward multicast traffic onto the home network. This can be avoided by programming the downstream address filters in the CM (through SNMP) to reject the DSG Multicast traffic. Refer to [RFC 4639] for details on the CM filters. Refer to Section 5.2.2.5, MAC Addressing for DSG Tunnels, for further considerations about the use of unicast DSG tunnel addresses.

5.6.2 DSG Basic Mode and DSG Advanced Mode

This section discusses issues with interoperability between DSG Basic Mode and DSG Advanced Mode, and the expected behavior of the DSG Agent and DSG Client.

In the deprecated DSG Basic Mode, the DSG Tunnel Address (the destination MAC address of the DSG Tunnel) is set equal to the DSG Client ID (which is a MAC address for DSG Basic Mode), while in DSG Advanced Mode, the DSG Agent assigns the DSG Tunnel Address with the DSG Address Table which is located in the DCD message.

The DSG Agent will always generate DCD messages for its DSG Tunnels, but would be able to support DSG Clients that are operating either in DSG Basic Mode or DSG Advanced Mode by proper choice of the DSG Tunnel Addresses.

In general, the operator might configure the DSG Agent to use different DSG Tunnels for STDs operating in DSG Basic Mode and STDs operating in DSG Advanced mode since the DSG Tunnels may carry slightly different content. If the same content can be sent to both, then a single DSG Tunnel can be configured with the DSG Client ID appropriate for the STDs operating in DSG Advanced Mode, and the DSG Tunnel Address set to the Well-Known MAC Address that the STDs operating in DSG Basic Mode are expecting. In this case, the operator should not arbitrarily change the DSG Tunnel Address as this would disconnect the STDs operating in DSG Basic Mode.

A Set-top Device which supports both Modes can use the presence of the DCD message to determine which mode the DSG Agent supports. If the DCD message is present, the Set-top Device would assume DSG Advanced Mode of operation. If the DCD message is absent, the Set-top would assume DSG Basic Mode of operation. For an example of an algorithm for switching between the two modes at the Set-top Device, refer to [OC-HOST2.1].

5.7 DSG Operation

This section discusses a variety of ways that DSG may be used in deployment. This section is not inclusive of all scenarios.

5.7.1 DSG Advanced Mode Tunnels

The DCD message is supported by DSG Client Controllers that support DSG Advanced Mode. The DSG Client Controller will forward the DSG Tunnel to the DSG Client based upon the criteria in the DSG Address Table. The DSG Address Table consists of series of DSG Rules and DSG Classifiers.

The DSG Client Controller searches the DSG Address Table for DSG Rules that match. When a match is found, the DSG Client Controller uses the DSG Rule to obtain the destination MAC address of the DSG Tunnel to receive (known as the DSG Tunnel Address), and it uses the DSG Classifiers to determine what Layer 3 and/or Layer 4 parameters to filter on. This information is then passed to the DSG eCM.

This is demonstrated in Figure 5–31, Example #1.

5.7.2 DSG Tunnel Address Substitution

The destination IP address of the DSG Tunnel is always a multicast address. The DSG Tunnel Address (destination MAC Address) is always a multicast (group) MAC address. As a result, the destination MAC address of the DSG Tunnel may be unrelated to the destination IP address of the DSG Tunnel.

This ability to substitute destination MAC addresses may be useful for increasing the security of the DSG Tunnel should the DSG Client ID or the DSG Tunnel Address become publicly known.

This is demonstrated in Figure 5–31, Example #1.

5.7.3 Many to One

In this scenario, one DSG Server may be supplying content to multiple DSG Clients over a larger area, while another DSG Server may be supplying directed content to a smaller serving area. Within a downstream, however, the content from both the DSG Servers are going to the same DSG Client.

DSG Advanced Mode allows multiple IP flows from the Backbone to merge into one DSG Tunnel. This is indicated to the DSG Client Controller by including multiple DSG Classifiers within one DSG Rule. Note that the multiple IP flows could be IP Unicast, IP Multicast, or both.

This is demonstrated in Figure 5–32, Example #5.

5.7.4 One to Many

The ability to have multiple entries within the DSG Client ID TLV within a DSG Rule would allow one DSG Server to send common content with a single IP stream to the DSG Agent and use a shared DSG Tunnel to DSG Clients from different manufacturers, each of which have their own DSG Client ID. This allows a one-to-many connectivity of DSG Server to DSG Clients, while maintaining the requirement that one IP address must be resolvable to only one MAC address.

This is demonstrated in Figure 5–32, Example #5.

5.7.5 Regionalization

An operator may want to send different content to different Set-top Devices from the same manufacturer on different HFC network segments.

In DSG Advanced Mode, a DSG Tunnel Address substitution may be made on a per downstream basis. For example, there could be multiple IP flows from the DSG Server to the DSG Agent. These flows may be intended for the same function - such as EAS information - but the content differs across downstreams within the same subnet. Each of these flows would get mapped to a different DSG Tunnel Address on each downstream or group of downstreams, depending upon geographical requirements. Each downstream would have a unique DCD message which would contain the same DSG Client ID, but would contain the unique DSG Tunnel Address. This is demonstrated in Figure 5–31, Example #2.

5.7.6 Layer 4 Multiplexing

One of the fields of the DSG Classifier is the destination UDP port. This provides more flexibility for how the DSG Server creates content and how the network delivers that content.

With DSG Advanced Mode, the DSG Server could assign different content to different destination UDP ports. There would then be one IP session from the DSG Server to the DSG Agent which would continue onto the DOCSIS downstream as a single DSG Tunnel. This DSG Tunnel would then feed multiple DSG Clients based upon the destination UDP ports.

The DSG Address Table would contain a series of DSG Rules which pointed all participating DSG Clients to the same DSG Tunnel, but each of which contained a different pairing of destination UDP port and a DSG Client ID.

This is useful as there are fewer IP addresses on the DSG Agent to be reserved, and it permits DSG configurations to scale without impacting any IP address space limitations. This would also simplify the networking configuration of multicast by reducing the number of multicast sessions required and by pushing the management of different DSG Tunnel content to layer 4.

Care must be taken to not place too much content into one DSG Tunnel such that the combined content would exceed the rate limits chosen for the DSG Tunnel, or that the content would overwhelm the DSG eCM since the packet filter specified by the DSG Classifier is typically executed in software.

This mode of operation requires that the DSG Client Controller not only use the DSG Classifier as part of a accept/discard filter, but also to forward the correct content based upon UDP Port to the correct destination within the Set-top Device.

5.7.7 DSG Channel List

A DSG Channel is a downstream channel that contains one or more DSG Tunnels. A DSG Channel List is therefore a list of downstreams that contain DSG Tunnels. Set-top Devices are responsible for picking a DSG Channel from the DSG Channel List based upon some criteria that they own. The DSG Channel List is not intended to indicate which Set-top Device should go on which downstream.

Typically, the DSG Channel List will contain a list of all the DSG Channels, and the DSG Channel List will be advertised on all DOCSIS downstream channels, regardless if the DOCSIS downstream channel is a DSG Channel. This typical scenario has exceptions. Each DOCSIS downstream serves different physical areas of the plant. A single CMTS may actually span two regions of the plant which have different frequencies for their DOCSIS downstreams. Thus, the DSG Channel List would be different for each of those regions.

As an example of operation, if the DSG Tunnels for Vendor A were on downstream A, the DSG Tunnels for Vendor B were on downstream B, and downstreams C and D had no DSG Tunnels, then the DSG Channel List would exist on downstreams A through D, but only list downstreams A and B. The Set-top Device would decide whether to transition between downstream A and B based upon whether all its DSG Clients were able to find their appropriate DSG Tunnels.

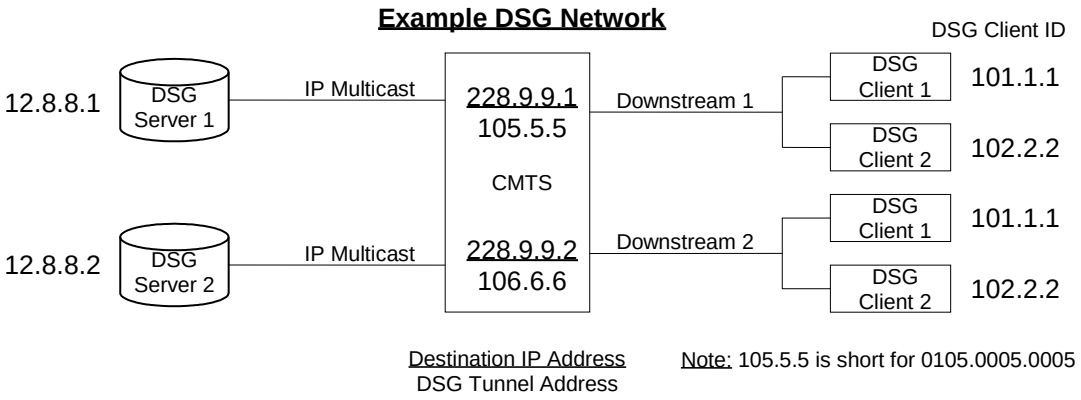
5.7.8 Support for Legacy DSG Servers and Legacy IP Networks

Legacy DSG Servers may not support IP Multicast. Likewise, legacy IP networks may not support IP Multicast. These two facts create four operational scenarios, each of which have different solutions. These solutions are described in Table 5–3. Note that tunneling of IP Multicast over IP Unicast is a preferred solution over Address Translation as it is a more common and efficient practice when dealing with IP Multicast.

Table 5–3 - Support Strategies for Legacy Network Equipment

DSG Server Capability	Network Capability	Strategy
Multicast	Multicast	The DSG Server generates an IP Multicast packet. The IP network delivers an IP Multicast packet to the CMTS. The CMTS passes the packet to the DSG Agent. This solution is the preferred solution.

DSG Server Capability	Network Capability	Strategy
Multicast	Unicast	The DSG Server tunnels an IP Multicast packet in an IP Unicast tunnel through the IP Network to each CMTS. The CMTS terminates the IP tunnel and delivers the IP Multicast packet to the DSG Agent. This solution compensates for a legacy IP network that does not support IP Multicast.
Unicast	Multicast	The DSG Server generates an IP Unicast packet. An external router to the DSG Server provides a Network Address Translation (NAT) function which translates the IP Unicast packet to IP Multicast. This router supports IP Multicast routing protocols and sends the IP Multicast packets to one or more CMTSs through the IP network. The CMTS passes the packet to its DSG Agent. This solution compensates for a legacy DSG Server which does not support IP Multicast. This solution allows the DSG Server to support multiple CMTSs.
Unicast	Unicast	The DSG Server generates an IP Unicast packet for each CMTS. The IP network delivers the IP Unicast packet to the CMTS. Either address translation is done to convert the IP Unicast packet to an IP Multicast packet or the IP Unicast packet is forwarded in a multicast fashion on multiple DOCSIS downstream channels. This solution results from both a legacy DSG Server and a legacy IP network.



Example #1: Two DSG Tunnels with MAC DA substitution. (DS = Downstream)

DSG Rule (DS1 & DS2)	
DSG Rule ID	1
DSG Client ID	101.1.1
DSG Tunnel Address	105.5.5

DSG Rule (DS1 & DS2)	
DSG Rule ID	2
DSG Client ID	102.2.2
DSG Tunnel Address	106.6.6

Example #2: Regionalization per Downstream

DSG Rule (DS1)	
DSG Rule ID	1
DSG Client ID	101.1.1
DSG Tunnel Address	105.5.5

DSG Rule (DS2)	
DSG Rule ID	2
DSG Client ID	101.1.1
DSG Tunnel Address	106.6.6

Example #3: This example is now deprecated.

Figure 5–31 - Example DSG Configurations

Example #4: Two DSG Tunnels with Full Classifiers with MAC DA substitution.

DSG Rule (DS1 & DS2)	
DSG Rule ID	1
DSG Client ID	101.1.1
DSG Tunnel Address	105.5.5
DSG Classifier ID	10

DSG Rule (DS1 & DS2)	
DSG Rule ID	2
DSG Client ID	102.2.2
DSG Tunnel Address	106.6.6
DSG Classifier ID	20

DSG Classifier	
DSG Classifier ID	10
IP SA	12.8.8.1
IP DA	228.9.9.1
UDP DP	8000

DSG Classifier	
DSG Classifier ID	20
IP SA	12.8.8.2
IP DA	228.9.9.2
UDP DP	8000

Example #5: One DSG Tunnel, supporting both IP Multicast flows from multiple DSG Servers (many-to-one) to multiple DSG Clients (one-to-many) with full classification and MAC substitution.

DSG Rule (DS1 & DS2)	
DSG Rule ID	1
DSG Client ID	101.1.1 102.2.2
DSG Tunnel Address	105.5.5
DSG Classifier ID	10 20

DSG Classifier	
DSG Classifier ID	10
IP SA	12.8.8.1
IP DA	228.9.9.1
UDP DP	8000

DSG Classifier	
DSG Classifier ID	20
IP SA	12.8.8.2
IP DA	228.9.9.2
UDP DP	8000

Figure 5–32 - Example DSG Configurations

(Continued from previous page)

5.7.9 DCC Considerations

Dynamic Channel Change (DCC) operations [DOCSIS-RFI] allow the opportunity to move CMs, including DSG eCMs, to new US and/or DS channels. DCC operations can be triggered manually or autonomously for load-balancing purposes. If DCC is implemented and used to change downstream channels, then an operator needs to ensure that the content of the DSG Tunnels are forwarded onto the old and new DOCSIS downstream channels that are impacted by the DCC message. If not, the Set-top Device will not be able to receive DSG tunnel information on the downstream. Whenever a DSG eCM is subject to DCC operations, care must be taken to provide the proper provisioning and configuration of the DSG Agent and the DSG eCM. When MDF is enabled, the MDF-capable DSG eCM re-reads the DSG DA-to-DSID Association Entry TLV from the MDD message after completing a DCC transaction that changes the primary downstream channel.

If MDF is enabled on the DSG eCM and the DCC moves the DSG eCM to a new MAC Domain, initialization technique zero (reinitialize the MAC) should be used when the MDF mode is different between the old and new

MAC Domains. If MDF is enabled on the DSG eCM and the DCC moves the DSG eCM to a new MAC domain, initialization techniques other than re-initialize the MAC can be utilized only when the MDF mode is aligned between MAC domains (either both MAC domains enable MDF or both MAC domains disable MDF).

5.7.10 DBC Considerations for DOCSIS 3.0 DSG eCMs

Dynamic Bonding Change (DBC) operations [DOCSIS-MULPI] allow the CMTS an opportunity to change upstream and/or downstream bonding parameters or channels within a MAC domain on CMs including DSG eCMs operating in Multiple Receive Channel mode. At any time after registration, the CMTS uses the DBC command to change any combination of the following parameters in a CM: the receive channel set, the transmit channel set, DSID(s) or DSID associated attributes (including Multicast Rules), Security association(s) for encrypting downstream traffic, and Service Flow SID Cluster Assignments.

DBC operations can be triggered manually or autonomously for load-balancing purposes. If DBC is implemented and used to change the Primary Downstream Channel, then an operator needs to ensure that the content of the DSG Tunnels are forwarded onto the old and new DOCSIS downstream channels that are impacted by the DBC message. If not, the Set-top Device will not be able to receive DSG tunnel information on the downstream.

DBC messaging is not intended to change the Multicast DSIDs of the DSG tunnels in any fashion. The DSIDs for the DSG tunnels are signaled via the MDD and the DBC messaging is not used to change those DSIDs. The use of DBC messaging to signal or change Multicast DSIDs for non-DSG tunnel traffic is permitted in DOCSIS 3.0 devices.

In all cases, if a DSG eCM is subject to DBC operations, then care must be taken to provide the proper provisioning and configuration of the DSG Agent and the DSG eCM.

5.7.11 Load Balancing Considerations

DOCSIS 2.0 and 3.0 CMTSs support autonomous load balancing of CMs using DCC and/or DBC. Also when a DOCSIS 3.0 CM registers with a DOCSIS 3.0 CMTS, the CMTS performs a channel assignment (RCC and TCC) [DOCSIS-MULPI] based on the load balancing configuration for the CM. Since the DSG Agent is unaware of the DSG tunnels being received by a particular DSG eCM, autonomous load balancing and DSG operation could conflict unless specifically configured otherwise.

One option to avoid this conflict is to disable load balancing on DSG eCMs. Alternatively, the MSO could configure a restricted load balancing group that only contains downstream channels that are carrying identical DSG tunnels. Finally, the CMTS vendor could implement a load balancing policy which allows load balancing of upstream channels and/or non-primary downstream channels, but does not allow a change to the DSG eCMs Primary Downstream Channel.

Annex A DOCSIS Set-top Gateway Agent MIB Definition (Normative)

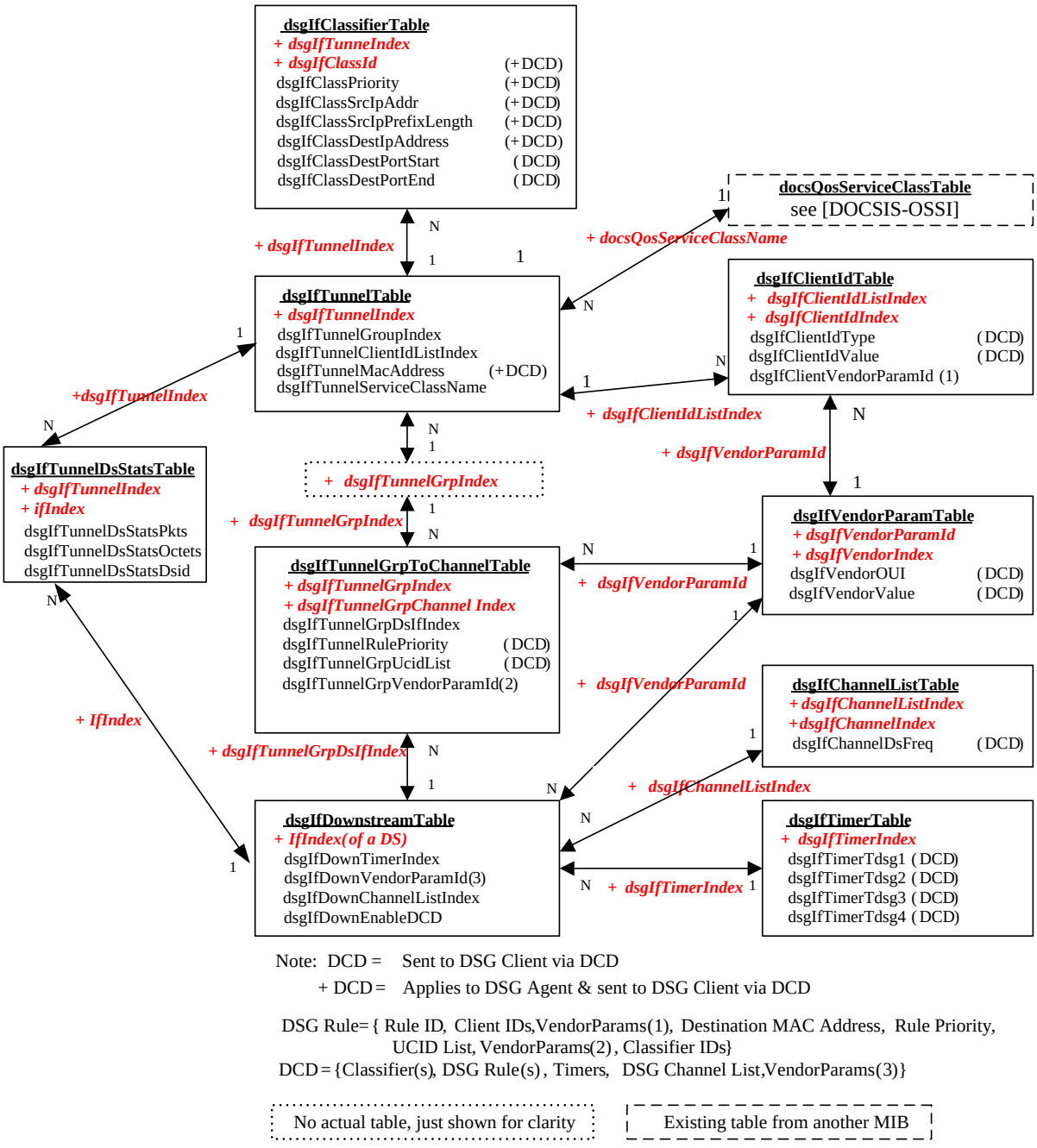


Figure A–1 - DSG MIB Module Objects Relationships

For the full text of the [DSG-IF-MIB], see http://mibs.cablelabs.com/MIBs/DOCSIS/.

Annex B DOCSIS Set-top Gateway Set-top Device MIB Definition (Normative)

For the full text of the [DSG-IF-STD-MIB], see http://mibs.cablelabs.com/MIBs/DOCSIS/.

Annex C Format and Content for DSG eCM Event, SYSLOG, and SNMP Trap Extensions (Normative)

To facilitate device provisioning and fault management, the DSG eCM MUST support the DOCSIS Event extensions defined in this section.

This section is an extension of Annex D "Format and Content for Event, SYSLOG, and SNMP Trap (normative)" of [SCTE 79-2] for DOCSIS 2.0 and [DOCSIS-OSSIv3.0] for DOCSIS 3.0. The eCM MUST conform to the requirements of [SCTE 79-2] the section "Fault Management," pertaining to these events, unless otherwise explicitly indicated in this section.

C.1 DSG eCM Event Extensions Description

"CM event" is used in this part to reference Annex D [SCTE 79-2] for DOCSIS 2.0 and [DOCSIS-OSSIv3.0] for DOCSIS 3.0.

The DSG eCM Events are based on the DSG notifications described in Sections 5.4.2.1 and 5.4.2.2, which can be categorized into the following types:

- DSG eCM to DSG Client Controller (CC) Events: (DSG eCM -> CC). The eCM communicates to the DSG Client Controller information such as the eCM operational mode and conditions on the RFI side of the CMTS.
- DSG Client Controller to DSG eCM Events: (DSG CC -> eCM). The DSG Client Controller uses DSG channel /DCD information to notify the eCM of operational requirements or actions.
- DSG eCM Internal Events: The DSG eCM State Transition Diagrams indicate various events that affect operation of the eCM.

Other DSG eCM events are specific to DSG operations. One example is the event generated when operators trigger DOCSIS Secure Software Download (SSD) for a DSG eCM when the eCM does not support this DOCSIS feature (see Section C.1.2).

NOTE: Herein, the abbreviation CC is used to refer to the Client Controller.

Table C–1 indicates the relationship between the DSG eCM events and the DSG Client control/eCM notifications. The Event definitions are in Section C.2.

Table C–1 - DSG Notifications and eCM Events relations

Notification Direction	Notification	DSG eCM Event Error Code Set
DSG CC → eCM	Start DSG Advanced Mode	G01.1
DSG CC → eCM	Disable upstream transmitter	G01.2
DSG CC → eCM	Enable upstream transmitter	G01.3
DSG CC → eCM	Not Valid. Hunt for new DSG Channel	G01.4
DSG eCM internal	Tdsg1 Timeout	G02.1
DSG eCM internal	Tdsg2 Timeout	G02.2
DSG eCM internal	Tdsg3 Timeout	G02.3
DSG eCM internal	Tdsg4 Timeout	G02.4
DSG eCM internal	eCM MAC reinitialization	G02.5
DSG eCM → CC	Downstream Scan Completed	G03.0
DSG eCM internal	Valid DSG Channel	G03.1
DSG eCM internal	DCD Present	G03.2
DSG eCM → CC	2-way OK, UCID	G04.0

Notification Direction	Notification	DSG eCM Event Error Code Set
DSG eCM → CC	Entering One-way Mode	G04.1
DSG eCM → CC	Cannot forward 2-way traffic, NACO <val>, Max CPE <val>	G04.2

C.1.1 DSG eCM event processes

All but one of the DOCSIS DSG event extensions are associated with the processes discussed in the following subsections.

C.1.1.1 DSG eCM event process "dsgOper"

The DSG Event extensions herein designated as "dsgOper" cover events generated during either initialization or operation. These event processes are divided into two sub-processes: DSG OPERATION and DSG TIMEOUT. The Error Code Set used for these events are G01 and G02.

C.1.1.2 DOCSIS event process "dsgInit"

In DOCSIS the event process "Init" refers to the CM initialization and registration processes. The DSG Event extensions associated with the "dsgInit" process are divided into three DOCSIS sub-processes, DOWNSTREAM ACQUISITION, OBTAIN UPSTREAM PARAMETERS, and REGISTRATION.

The DSG extensions for DOWNSTREAM ACQUISITION use Error Code Set G03, while the DSG extensions for OBTAIN UPSTREAM PARAMETERS and REGISTRATION use Error Code Set G04.

Note that DOCSIS OSSI specs need to be aware of the usage of Error Code Set G when extending DOCSIS Event Error Code Sets.

C.1.2 eCM event processes

Events in this category may reuse DOCSIS standard Events Process and sub-process and are assigned to Error Code Set G05.

C.2 DSG DOCSIS Events Extensions

Table C–2 - DSG DOCSIS Events Extensions

Process	Sub-Process	CM Priority	Event Message	Message Notes And Details	Error Code Set	Event ID	Trap Name
eCM STB OPERATION							
dsgOper	DSG OPERATION	Informational	Start DSG Advanced Mode		G01.1	71000101	
dsgOper	DSG OPERATION	Warning	Disable upstream transmitter	send event before disabling upstream	G01.2	71000102	DsgIfStdUpstreamDisabledNotify
dsgOper	DSG OPERATION	Warning	Enable upstream transmitter	send event upon successful re-registration	G01.3	71000103	dsgIfStdUpstreamEnabledNotify
dsgOper	DSG OPERATION	Warning	Not valid, Hunt for new DSG channel		G01.4	71000104	
dsgOper	DSG TIMEOUT	Warning	Tdsg1 Timeout		G02.1	71000201	

Process	Sub-Process	CM Priority	Event Message	Message Notes And Details	Error Code Set	Event ID	Trap Name
dsgOper	DSG TIMEOUT	Warning	Tdsg2 Timeout		G02.2	71000202	dsgIfStdTdsg2TimeoutNotify
dsgOper	DSG TIMEOUT	Informational	Tdsg3 Timeout		G02.3	71000203	
dsgOper	DSG TIMEOUT	Critical	Tdsg4 Timeout		G02.4	71000204	
dsgOper	DSG OPERATION	Warning	eCM MAC Reinitialization		G02.5	71000205	
eCM DOWNSTREAM ACQUISITION							
dsgInit	DOWNSTREAM ACQUISITION	Warning	Downstream Scan Completed		G03.0	71000300	
dsgInit	DOWNSTREAM ACQUISITION	Informational	Valid DSG Channel	only logged when in DSG Channel Validation State	G03.1	71000301	
dsgInit	DOWNSTREAM ACQUISITION	Informational	DCD Present, DS	only logged when in DSG Channel Validation State	G03.2	71000302	
eCM UPSTREAM PARAMETERS							
dsgInit	REGISTRATION	Informational	2-way OK, UCID <P1>	P1 = 255	G04.0	71000400	
dsgInit	OBTAIN UPSTREAM PARAMETERS	Critical	Entering One-way Mode		G04.1	71000401	
dsgInit	REGISTRATION	Warning	Cannot forward 2-way traffic, NACO <P1>, Max CPE <P2>	P1 = NACO value, P2 = Max CPE value from configuration file	G04.2	71000402	
Deprecated Events (See Annex C of [eDOCSIS] for new Events)							
SW Upgrade (Deprecated)	SW UPGRADE GENERAL FAILURE	Notice	DOCSIS SSD not supported		G05.1	71000500	

Annex D Delivery of MPEG-2 Sections in the Broadcast Tunnel (Normative)

The Broadcast Tunnel is intended to carry data for consumption by all devices regardless of manufacturer and CA vendor. To achieve this, a standardized encapsulation must be used on all Broadcast Tunnels where MPEG-2 sections are delivered. This Annex specifies an encapsulation for the carriage of MPEG-2 sections over all Broadcast Tunnels.

D.1 MPEG-2 Section Encapsulation

If MPEG-2 sections (e.g., SCTE 65) are sent on the DSG Broadcast Tunnel, then these sections MUST be encapsulated by the DSG Server in UDP (RFC 768) over IPv4 (RFC 791) utilizing a new header (BT Header) embedded within the UDP datagram. The Broadcast Tunnel (BT) Header is defined in Table D–1. Sections MUST be packed by the DSG Server as one section per UDP datagram. A section packed by the DSG Server MUST NOT exceed a size of 4096 bytes.

Figure D–1 depicts the MPEG-2 section encapsulated within a UDP over IPv4 packet.

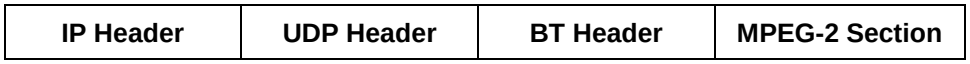


Figure D–1 - Section Encapsulation

Table D–1 - BT Header

Bt_header () {	Bits	Bit Number/ Description
header_start	8	uimsbf
version	3	uimsbf
last_segment	1	bslbf
segment_number	4	uimsbf
id_number	16	uimsbf
}		

Where:

- header_start = this shall have a fixed value of 0xff. This identifies the presence of the BT Header allowing systems based on UDP section encapsulation to be migrated to the encapsulation defined here. ISO 13818-1 defines 0xff to be a forbidden table id.
- version = defines the version number of the BT Header. This shall be 0x01.
- last_segment = defines whether this segment is the last segment of a segmented section. When set, the segment is the last one for the given id_number.
- segment_number = defines the number of the current segment for the given id_number. A value of 0 indicates this is the first segment. If the segment_number = 0 and the last_segment is set, then the section has not been segmented and the UDP datagram contains a complete section.
- id_number = number assigned to each section delivered thus allowing the device to correlate segments that are applicable to a particular section in the event that segmentation of the section was required. The id_number is defined within the context of the UDP stream. Therefore, all segments belonging to the same section are

identified by having the same source IP address, source port number, destination IP address, destination port, and id_number.

If the resultant IP datagram will exceed the network MTU, the DSG Server MUST perform segmentation of the MPEG-2 table at the UDP layer and populate the segmentation values of the BT header accordingly. When segmenting the section, all segments except the last MUST be of equal size and SHOULD be the maximum size possible without exceeding the MTU. The DSG Server MUST emit the segments in order (i.e., with the segment_number field monotonically increasing). The DSG Server MUST NOT have more than one incomplete MPEG-2 section outstanding on a UDP stream.

The DSG Client is responsible for reassembling each segmented MPEG-2 section. The DSG Client MUST be capable of simultaneously reassembling four segmented MPEG-2 sections on each Broadcast Tunnel without data loss.

NOTE: In some cases, multiple DSG Servers will generate UDP streams intended for a single DSG Rule with a single DSG Broadcast ID. For example, separate DSG Servers can be used to generate XAIT and CVT data for the Broadcast Tunnel with DSG Broadcast ID 5. In such cases, the operator is responsible for ensuring that the aggregate number of segmented UDP streams is four or less at all times for this Broadcast Tunnel. The client behavior is undefined if this constraint is violated.

The DSG Server SHOULD minimize segmentation where possible.

NOTE: Many tables based on the MPEG-2 section syntax can be split across multiples sections. Therefore, by restricting the section size to below the MTU and creating multiple sections to carry the data, it is possible to minimize segmentation.

D.2 Layer 4 Multiplexing

Typically, MPEG-2 sections are encapsulated within MPEG-2 transport packets. These packets contain a PID which is used for demultiplexing the transport stream. When the MPEG-2 sections are encapsulated as described above, the association between Table Id (contained in the section) and the PID is lost as no PID information is carried within the datagram. If such an association is required, Table Ids can be assigned specific multicast IP addresses and/or specific UDP ports within the Broadcast Tunnel where the addresses/ports conceptually represent PIDs. It is not within scope of DSG to define how the DSG Client Controller is provisioned with this information.

For example, if the DSG Client Controller is provisioned accordingly and the DSG Client requests SI/EAS tables from the DSG Client Controller using PID and Table Id to identify the SCTE 65 and SCTE 18 traffic flows, the DSG Client Controller is required to map between the PID and Table Id and the multicast address/port on which the requested flow is located and pass the applicable flow(s) to the DSG Client.

Annex E Delivery of MPEG-2 Sections in Application Tunnels (Normative)

[OCAP] and OpenCable Common Download define an encapsulation for the carriage of MPEG-2 sections over certain DSG application tunnels. This header is required by the implementation to support the carriage of DSMCC object and data carousels (as defined in [OCAP]) over DSG application tunnels.

If MPEG-2 sections are sent on a DSG application tunnel as part of a carousel, then the DSG Server MUST encapsulate and send the sections within UDP over IPv4 utilizing the DSG_Carousel_Header. The consumer of these sections will expect this header to be present at the beginning of every UDP datagram within DSG application tunnels that carry DSMCC object or data carousels. This header should be immediately followed by a complete MPEG section. Each UDP packet should contain the DSG_Carousel_Header and a complete MPEG section. Since IP datagram fragmentation is not allowed, this necessarily limits the MPEG-2 section length to less than the DOCSIS MTU.

Table E–1 - DSG Carousel Header

Syntax	Bits	Type	Value	Comment
DSG_Carousel_Header() {				
version	2	bslbf	0x1	The version number of the DSG_Carousel_Header. This shall be 0x1.
reserved	1	bslbf	0x1	
MPEG_transport_PID	13	uimsbf	+	This field carries the MPEG transport stream PID information for the MPEG section. DSG tunnels that use this header do not contain full MPEG TS encapsulation; however, the PID information is carried on the DSG stream. This allows for a DSG stream that carries MPEG sections to be filtered by MPEG PID value.
}				

Annex F DOCSIS Set-top Gateway (DSG) Set-top Extender Bridge (SEB) (Normative)

This Annex defines the architecture and requirements necessary to support the DSG SEB capabilities. Support for DSG SEB is optional for DSG capable devices, however, if the device supports the DSG SEB architecture, then the device MUST support DSG SEB as defined in this Annex. In addition the Annex also provides additional optional functionality that layers on top of the mandatory elements, as explained in this Annex.

DSG SEB is built on the UPnP architecture as defined in [UPNP-DA].

Devices that support DSG SEB are required to support functionality based on these high level design constraints:

1. DSG capable devices that fail to complete DOCSIS registration attempt to locate and use a DSG SEB Server (SEBS) for upstream IP traffic
2. The DSG SEB Client (SEBC) MUST not forward any DSG traffic to the home network.
3. The eCM of the SEBS is only accessible by the SEBC devices on the home network. PCs, gaming consoles, and other non-OpenCable IP devices are not allowed access to the MSO's network through the eCM of the SEBS. Therefore, the SEBS MUST NOT forward any packets received on its home network interface not addressed with a MAC address of a known SEBC.
4. SEBC eSTB devices must be addressed in the same address space as the eSTB of the SEBS such that the SEBC devices can successfully communicate with the service provider's conditional access system, VOD servers, etc. Thus, the SEBC's must receive their IP address from the same source as the SEBS (i.e., the DHCP server in the service provider's headend).
5. DSG capable devices that are able to complete DOCSIS provisioning must use the eCM for provisioning of the eSTB. If the device completes DOCSIS registration and does not commit to the role of SEBS (e.g., a SEBS already resided on the home network), then the device does not act as a SEBC, until such time as it loses upstream/downstream and is not able to re-provision its eCM.
6. DSG capable devices that satisfy the SEBS eligibility criteria (see Section F.2.6, SEBS Requirements, and Section F.5, Determining Server Figure of Merit) will advertise their presence using SSDP and wait for connections from SEB Clients. All SEB Clients on the Home Network will establish SEB Tunnels with a single SEB Server. However, the other SEBS will continue to listen for SEB Client connections in case the currently selected SEBS becomes unavailable or ineligible.

F.1 DSG_SEB_Server:1 Device Template

F.1.1 Overview and Scope

This device template is compliant with the UPnP Device Architecture version 1.0. It defines a device type referred to herein as DSG_SEB_Server:1.

DSG_SEB_Server:1 is a device (e.g., OpenCable Host Device), henceforth referred to as SEBS, equipped with a DSG compliant cable modem, capable of providing DSG services to other devices, henceforth referred to as SEBC, connected to the SEBS via a local area network (e.g., MoCA). DSG services consist of bi-directional IP connectivity (i.e., the SEBS exposes it's upstream/downstream DOCSIS resource allowing the connected SEBC to obtain access to the service provider's DOCSIS network).

DSG_SEB_Server:1 enables the following functions, as illustrated in Figure F–1.

- Provides IP connectivity to the service provider's DOCSIS network.

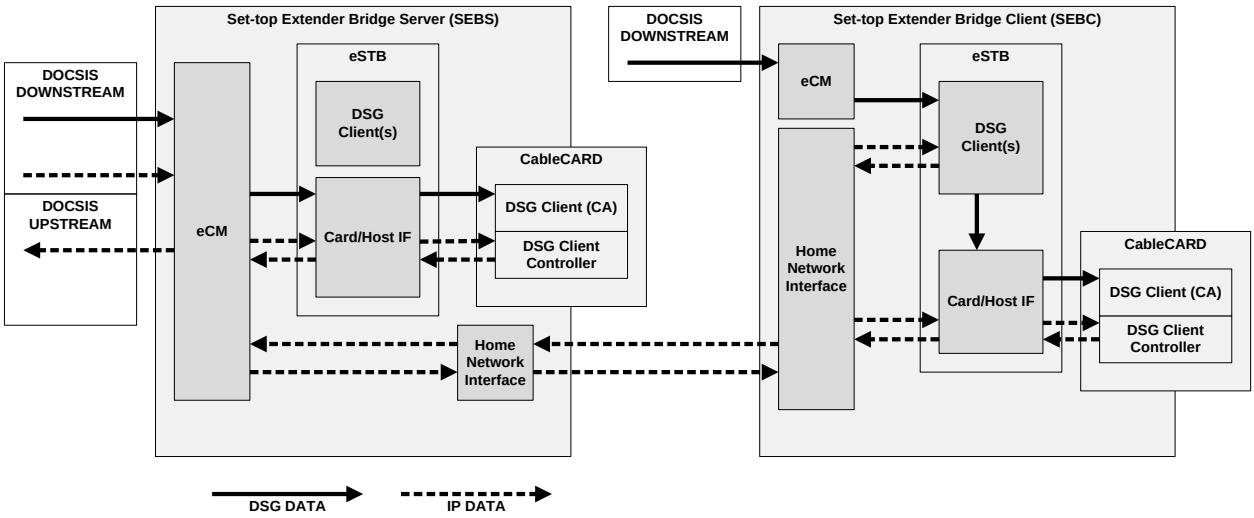


Figure F–1 - Block diagram of DSG SEB Solution

F.1.2 Device Type

The following device type identifies a device that is compliant with this template:

- urn:schemas-cablelabs-com:device:DSG_SEB_Server:1

The shorthand DSG_SEB_Server:1 is used herein to refer to this device type.

F.1.3 Device Model

The DSG capable device that supports DSG SEB MUST implement minimum version numbers of all required embedded devices and services specified in the table below.

Table F–1 - DSG SEB Device Requirements

Device Type	Root	Req. or Opt. [1]	Service Type	Req. or Opt. [1]	Service ID [2]
DSG_SEB_Server:1	yes	R	DSG_SEB:1	R	DSGSEB

[1] R = Required, O = Optional, X = Non-standard.

[2] Prefixed by urn:cablelabs-com:serviceId:

F.1.4 Description of Device Requirements

All service types are required exactly once.

F.1.5 Relationships Between Services

None.

F.1.6 XML Device Description

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <URLBase>base URL for all relative URLs</URLBase>
  <device>
    <deviceType> urn:schemas-cablelabs-com:device:DSG_SEB_Server:1</deviceType>
    <friendlyName>short user-friendly title</friendlyName>
```

```
    <manufacturer>manufacturer name</manufacturer>
    <manufacturerURL>URL to manufacturer site</manufacturerURL>
    <modelDescription>long user-friendly title</modelDescription>
    <modelName>model name</modelName>
    <modelNumber>model number</modelNumber>
    <modelURL>URL to model site</modelURL>
    <serialNumber>manufacturer's serial number of the eSTB </serialNumber>
    <UDN>uuid:UUID</UDN>
    <UPC>Universal Product Code</UPC>
    <iconList>
      <icon>
        <mimetype>image/format</mimetype>
        <width>horizontal pixels</width>
        <height>vertical pixels</height>
        <depth>color depth</depth>
        <url>URL to icon</url>
      </icon>
      XML to declare other icons, if any, go here
    </iconList>
    <serviceList>
      <service>
        <serviceType>urn:schemas-cablelabs-com:service:DSG_SEB_Server:1</serviceType>
        <serviceId>urn:cablelabs-com:serviceId:DSGSEB</serviceId>
        <SCPDURL>URL to service description</SCPDURL>
        <controlURL>URL for control</controlURL>
        <eventSubURL>URL for eventing</eventSubURL>
      </service>
    </serviceList>
    <presentationURL>URL for presentation</presentationURL>
  </device>
</root>
```

F.2 DSG_SEB:1 Service Template

F.2.1 Overview and Scope

This service template is compliant with the UPnP Device Architecture [UPNP-DA]. It defines a service type referred to herein as DSG_SEB:1.

DSG_SEB:1 provides control for the establishing of IP connectivity between the SEBS and the SEBCs on the home network.

DSG_SEB:1 enables the following functions:

- Providing IP connectivity to SEBCs via the service provider's DOCSIS network
- Notification that SEBC has left the home network

F.2.2 Data Forwarding Model

The SEBS offers a layer 2 forwarding service to devices connected to a SEBC, as illustrated in Figure F–2. The forwarding service uses a distinct SEB Tunnel for each connected SEBC. In general, each SEBC is connected to CPE devices which utilize the layer 2 forwarding service. These devices include eSAFEs, the SEB eCM, and possibly external CPE devices.

To facilitate the forwarding process, the SEBS implements a forwarding database with information about all devices connected through the various SEB Tunnels. The forwarding database also contains information about the multicast groups that each device is subscribed to. Database updates are made using UPnP actions.

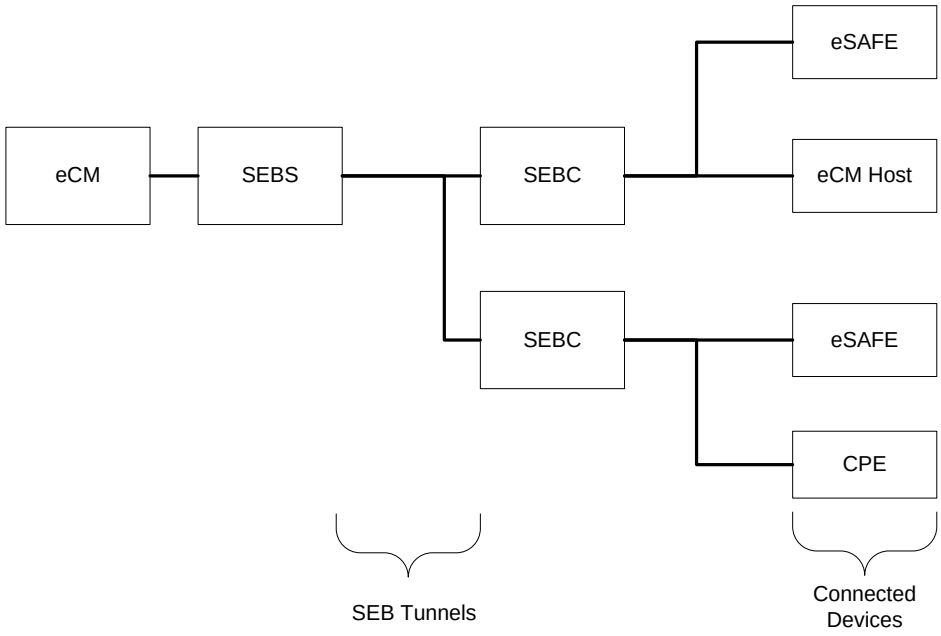


Figure F–2 - SEB data forwarding model components

F.2.3 Addressing

To ensure that a SEBC eSTB device gets an IP address sufficient to allow the eSTB of the SEBC to communicate with the service provider's management systems, conditional access system, VOD servers, etc., the SEBS simply forwards DHCP discover requests from the SEBC to the WAN. The SEBC DHCP broadcasts are never exposed to the home network outside of the TCP tunnel between the SEBC and the SEBS. Similarly, to ensure that the SEBC eCM device gets an IP address that allows the eCM of the SEBC to communicate with the service provider's DOCSIS provisioning and management system, the SEBS simply forwards all DHCP messaging from clients toward the WAN.

Since the SEBC does not utilize DHCP until it has established the TCP tunnel, the SEBC utilizes link-local addressing as per [RFC 3927] for the DSG SEB provisioning. UPnP defines that link-local is to be used when DHCP addressing fails; however in this case, since the SEBC's are not using DHCP until after they establish the TCP tunnel. As such, the SEBS is required to maintain its link-local address to facilitate the provisioning of new SEBCs that enter the network.

F.2.4 Encryption on Home Network Interface

To provide protection to SEB Tunnel traffic, the forwarded layer 2 frames are encrypted in both directions using TLS. This includes, unicast, multicast, and broadcast frames.

F.2.5 Transport Layer Security (TLS) Requirements

The following are mandatory requirements for DSG capable devices that support DSG SEB protocol:

1. The DSG capable device that supports DSG SEB protocol MUST support version 1.2 of the Transport Layer Security (TLS) Protocol as defined in [RFC 5246].
2. The DSG capable device that supports DSG SEB protocol MUST support the following Cipher Suites [RFC 5246]:
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_NULL_SHA (null cipher suite for debugging support)

3. The DSG capable device that supports DSG SEB protocol MUST use TLS_RSA_WITH_AES_128_CBC_SHA as the default Cipher Suite.
4. The DSG capable device that supports DSG SEB protocol MUST implement the optional device authentication process defined within TLS, for both server and client.
5. The DSG capable device that supports DSG SEB protocol MUST implement the SHA-1 hash algorithm and RSASSA-PKCS1-v1_5 [RFC 3447] for the TLS signature/hash algorithm pair, utilized during the TLS Handshake Protocol [RFC 5246].
6. The DSG capable device that supports DSG SEB protocol MUST implement the RSA_PSK [RFC 4279] key exchange algorithm, utilized during the TLS Handshake Protocol [RFC 5246].

F.2.5.1 Data Encapsulation

Each layer 2 frame forwarded over the SEB Tunnel will be carried in a TLS Record with a ContentType value of application_data(23). Each TLS Record will contain exactly one layer 2 frame. Layer 2 frames are not fragmented across multiple TLS Records.

The TLS Record will include the Ethernet header and the 32-bit Ethernet CRC.

F.2.6 SEBS Requirements

The following are mandatory requirements for devices that support the SEBS functionality.

1. A DSG capable device MUST only attempt to operate as a SEBS, if the device completes DOCSIS registration, acquires an IP address for the eSTB, DSG mode = two-way advanced, ifAdminStatus for Home Network interface is set to UP, the eCM's Network Access Control Object = 1 and the DSG SEB Control Object = TRUE.
2. A DSG capable device MUST NOT attempt to operate as a SEBS unless its eCM can support at least one additional CPE based on the Maximum Number of CPEs configuration file parameter and the implementation limits of the eCM.
3. The DSG capable device MUST utilize link-local [RFC 3927] to acquire an IP address that is to be used on the home network interface for the initial provisioning of SEBC devices that enter the network.
4. The SEBS MUST transmit UPnP:Discovery:Advertisement:Notify-Alive messages at least once every 120 seconds (i.e., CACHE-CONTROL set to 1800).
5. The DSG capable device MUST terminate SEBS operation, if the device is taken out of two-way advanced DSG mode.
6. The DSG capable device MUST terminate SEBS operation, if the eCM's ifAdminStatus for Home Network interface is set to DOWN.
7. The DSG capable device MUST terminate SEBS operation, if the eCM's Network Access Control Object = 0.
8. The DSG capable device MUST terminate SEBS operation if the eCM's DSG SEB Control Object = FALSE.
9. The DSG capable device MUST terminate SEBS operation if the eCM exits the Two-way Operation state.
10. The SEBS MUST use TLS [RFC 5246] for all DSG SEB non-SSDP UPnP Actions and Queries (Notifies do not use TLS as these are broadcast)
11. The SEBS MUST use its CableLabs certificates for DSG SEB TLS sessions.
    a. Device first attempts to authenticate with DOCSIS certificates, if this fails (e.g., SEBC is not a DOCSIS device), then it attempts to authenticate with OpenCable certificates.
12. The SEBS MUST reject any UPnP DSG SEB Action received from an unauthenticated device.
13. The SEBS MUST reject any UPnP DSG SEB Query received from an unauthenticated device.

14. The SEBS will respond to SEB Tunnel requests as described in Section F.3

F.2.6.1 Downstream Forwarding and Control

1. The SEBS MUST update its forwarding database based on the UPnP ClientConnect, ClientAddDevice, ClientRemoveDevice, ClientJoin, and ClientLeave actions.
2. The SEBS MUST remove all entries in its forwarding database for a SEB Tunnel if that tunnel is closed for any reason (e.g., the TCP session for that SEB Tunnel is closed.)
3. Using a proprietary mechanism, the SEBS MUST provision the eCM with the MAC addresses of all devices in the forwarding database.
4. Upon receiving a layer 2 frame with a unicast destination MAC address, the SEBS will examine its forwarding database to determine if any SEB Tunnels are associated with that destination MAC address. If a matching SEB Tunnel is found, the SEBS MUST forward the frame to that SEB Tunnel.
5. The SEBS MUST silently discard any frame with an unknown destination MAC address.
6. Upon receiving a layer 2 frame with a broadcast destination MAC address, the SEBS MUST forward the frame to all SEB Tunnels within its forwarding database.
7. Upon receiving a layer 2 frame with a multicast destination MAC address, the SEBS will examine its forwarding database to determine which SEB Tunnels have requested this multicast flow. If matching SEB Tunnels are found, the SEBS MUST forward the frame to those SEB Tunnel(s).
8. The SEBS MUST forward multicast packets according to the packet's destination MAC address. when making multicast forwarding decisions.
9. When forwarding layer 2 frames on a SEB Tunnel, the SEBS MUST encrypt the header and payload using TLS with an approved ciphersuite.

F.2.6.2 Upstream Forwarding

1. Upon receiving a layer 2 frame from a SEB Tunnel, the SEBS will examine its forwarding database to determine if the source MAC address of the frame is associated with that tunnel. If the source MAC address is valid, the SEBS MUST forward the frame to the eCM. Note that this requirement applies to unicast, multicast, and broadcast frames.
2. The SEBS MUST silently discard any frame with an unknown source MAC address.
3. The SEBS MUST silently discard any frame with a source MAC address belonging to a different SEB Tunnel than the one the frame was received on.

F.2.7 SEBC Requirements

The following are requirements for the SEBC.

1. The SEBC MUST use link-local [RFC 3927] for the home network interface to acquire an IP address that is to be used for the establishment of the TCP connection for IP connectivity.
2. The SEBC MUST terminate SEBC operation, if the SEBC loses connection with the SEBS and is not able to locate a replacement DSG SEB Server.

   After terminating SEBC operation, the SEB Server Selection Process MUST be re-initiated unless a DOCSIS upstream channel can be established.
3. The SEBC MUST use its CableLabs certificates for DSG SEB TLS sessions.
   a. If the device has both DOCSIS and OpenCable certificates, then it first attempts to authenticate with DOCSIS certificates, if this fails (e.g., SEBC is not a DOCSIS device), then it attempts to authenticate with OpenCable certificates.
4. The SEBC MUST reject any UPnP DSG SEB Action received from an unauthenticated device.
5. The SEBC will establish a SEB Tunnel as described in Section F.3.

6. The SEBC MUST utilize a value of 0xFF for UCID when providing UCID values to the DSG Client Controller.

F.2.7.1 Downstream Forwarding

1. Upon receiving a layer 2 frame with a unicast destination MAC address from its SEB Tunnel, the SEBC MUST forward the frame to the connected device with that MAC address (if one exists.)
2. The SEBC MUST silently discard any frame with an unknown unicast destination MAC address.
3. Upon receiving a layer 2 frame with a broadcast destination MAC address from its SEB Tunnel, the SEBC MUST forward the frame to all connected devices.
4. Upon receiving a layer 2 frame with a multicast destination MAC address from its SEB Tunnel, the SEBC will examine the destination MAC address to determine the identity of the multicast flow. The SEBC MUST forward this frame to any connected devices which have previously requested this flow.

F.2.7.2 Upstream Forwarding and Control

1. The SEBC MUST generate a UPnP ClientConnect action to initially establish a connection with the SEBS.
2. After the SEBC establishes a connection with the SEBS it MUST use a UPnP ClientAddDevice action for each connected device (i.e., eSTB) that requires layer-2 forwarding.
3. The SEBC MUST generate a UPnP ClientJoin action for each connected device that requires a multicast flow. Note that all IPv6 devices will require Solicited Node Multicast flows, which will need to be explicitly requested using this method.
4. The SEBC SHOULD generate a UPnP ClientLeave action if it determines that a multicast flow is no longer required by any of its connected devices.
5. Upon receiving a layer 2 frame from a connected device, the SEBC MUST forward this frame on its SEB Tunnel.
6. When forwarding layer 2 frames on an SEB Tunnel, the SEBC MUST encrypt the header and payload using TLS with an approved ciphersuite.

F.2.8 Service Modeling Definitions

F.2.8.1 Service Type

The following service type identifies a service that is compliant with this template:

urn:schemas-cablelabs-com:service:DSGSEB:1

The shorthand DSGSEB:1 is used herein to refer to this service type.

F.2.8.2 State Variables

Defines state variables.

Table F–2 - State Variables

Variable Name	Req. Opt.1	Data Type	Allowed Value	Default Value	Eng. Units
ServiceFigureOfMerit	R	ui4	>=0	(none)	n/a
MaxConnectedDevices	R	i4	>=1, <= 256, +/-1	1	n/a
NumConnectedDevices	R	i4	>=0, <= MaxConnectedDevices	0	n/a
ConnectedDevices	R	CSV string	(bin:hex, ui1, ui1, string) See below	(none)	n/a)
GroupJoins	R	CSV string	See below	(none)	n/a
UpstreamChannelHeadroom	R	ui1	>=1, <=17, =/-1	1	dBmV
DownstreamChannelPower	R	i4	see below	(none)	n/a
UpstreamChannelPower	R	i4	see below	(none)	n/a

Variable Name	Req. Opt.1	Data Type	Allowed Value	Default Value	Eng. Units
ChannelChange	R	ui1	see below	(none)	n/a
A_ARG_TYPE_MacAddress	R	bin:hex	00:00:00:00:00:00 to ff:ff:ff:ff:ff:ff	(none)	n/a
A_ARG_TYPE_DeviceType	R	ui1	>=1, <=4	(none)	n/a
A_ARG_TYPE_TunnelPort	R	ui4	>=0, <=65534		
A_ARG_TYPE_IpAddress	R	string	IPv4 address in dotted decimal format or IPv6 address in colon-separated hex format	(none)	n/a
A_ARG_TYPE_IpAddressType	R	ui1	0 = IPv4, 1=IPv6	(none)	n/a
A_ARG_TYPE_Result	R	string	See below	(none)	n/a

1 R = Required, O = Optional.

F.2.8.2.1 ServiceFigureOfMerit

A number calculated by a device as a measure of its eligibility to perform as a DSG SEB server. See Section F.5, MaxConnectedDevices.

The maximum number of connected devices that this DSG SEB Server is capable of serving.

F.2.8.2.2 NumConnectedDevices

The number of connected devices currently serviced by this DSG SEB Server.

F.2.8.2.3 ConnectedDevices

Lists the DSG SEB Client devices that are connected to the DSG SEB Server. Each entry in the list is a CSV string consisting of the client device MacAddress, DeviceType, IpAddressType and IpAddress, in that order. Note that multiple devices may be connected through a single SEB Tunnel (e.g., an eSTBSAFE and an eCM connected using a single SEB Tunnel.)

F.2.8.2.4 GroupJoins

Lists the multicast groups that this server has joined, and with each multicast group, identifies which served DSG SEB Client devices are receiving the group.

F.2.8.2.5 UpstreamChannelHeadroom

Indicates that allowable power level, below maximum upstream transmit power, that is acceptable for this device to make itself available to client devices as a DSG SEB Server. When the device's upstream power transmit level is GREATER than the maximum transmit power less headroom, then the device MUST NOT advertise itself as a DSG SEB Server.

F.2.8.2.6 DownstreamChannelPower

Indicates the power level of the primary downstream channel that the device is locked to expressed in dBmV. Units are in tenths of a dBmV; for example, 5.1 dBmV will be represented as 51. This value is equivalent to the value reported via the docsIfDownChannelPower object of the DOCS-IF-MIB.

F.2.8.2.7 UpstreamChannelPower

Indicates the power level of the upstream channel that the device is transmitting on expressed in dBmV. Units are in tenths of a dBmV; for example, 5.1 dBmV will be represented as 51. This value is equivalent to the value reported via the docsIfCmStatusTxPower object of the DOCS-IF-MIB.

F.2.8.2.8 ChannelChange

Indicates the eCM of the DSG SEB Server has entered a state (e.g., DCC or DBC related) where it is preparing to switch to a new upstream channel. The DSG SEB Server sets the value of this field as indicated below based on the action it takes when initiating a channel change. A value of 0xFF indicates that the DSG SEB Server has just completed a channel change and is back to normal operation. The other values are set as applicable when the DSG SEB Server performs the channel change:

- 0x00 = Reinitialize the MAC.
- 0x01 = Perform broadcast initial ranging on new channel before normal operation.
- 0x02 = Perform unicast initial ranging on new channel before normal operation.
- 0x03 = Perform either broadcast initial ranging or unicast initial ranging on new channel before normal operation.
- 0x04 = Use the new channel(s) directly without re-initializing or initial ranging.
- 0x05 = Re-initialization method not specified.
- 0x06 = DBC operation.
- 0x07 – FE = Reserved for future use
- 0xFF = Channel change complete

F.2.8.2.9 A_ARG_TYPE_MacAddress

This state variable is introduced to provide type information for the MacAddress argument in various actions The MacAddress argument indicates the MAC address of a device residing in the SEBC, such as an eSAFE or an upstream-impaired SEB eCM.

F.2.8.2.10 A_ARG_TYPE_DeviceType

This state variable is introduced to provide type information for the DeviceType argument in various actions. When used in action ClientConnect(), it indicates either the eCM is requesting a TCP port in order to open a tunnel with the SEBS. When used in the action ClientAddDevice it indicates the eSTB is requesting the IP address information. In both actions, the DSG SEB Server uses this to determine if the MAC address being provided is for the eCM or eSTB. This allows the DSG SEB to indicate in its diagnostics what type of devices it is serving.

Valid values are:

- eSTB(2)
- eCM(3)
- other(4)

F.2.8.2.11 A_ARG_TYPE_TunnelPort

This state variable is introduced to provide type information for the TunnelPort argument in various actions. The TunnelPort argument provides the client devices with the TCP port selected by the DSG SEB Server for the client's use in establishing the TCP/IP tunnel for client-server IP traffic. Tunnel port assignments are server implementation dependent.

F.2.8.2.12 A_ARG_TYPE_Result

This state variable is introduced to provide type information for the Result argument from the GetConnectedDevices action. The structure of the Result argument is a DIDL-Lite XML Document:

- Optional XML declaration <?xml version="1.0" ?>
- <DIDL-Lite> is the root element
- <connecteddevice> is the element representing each connected device with these nested elements, obtained from the state variable ConnectedDevices:
    - <macaddress>
    - <devicetype>
    - <ipaddrtype>
    - <ipaddress>

Note that since the value of Result is XML, it needs to be escaped (using normal XML rules before embedding in a SOAP message. In addition, when a value of type A_ARG_TYPE¬ Result is employed in a CSV list, as it is here, commas (",") that appear within the XML are escaped as "\,", as required for strings embedded in other strings.

F.2.8.2.13 A_ARG_TYPE_IpAddress

This state variable is introduced to provide type information for the IpAddress argument in various actions. When used as an argument to an action, this state variable represents an IPv4 or IPv6 address, for example: 192.168.0.1 in the case of IPv4.

F.2.8.2.14 A_ARG_TYPE_IpAddressType

This state variable is introduced to provide type information for the IpAddressTypes argument in various actions.

F.2.8.3 Relationships Between State Variables

There are no relationships

F.2.9 Eventing and Moderation

As the table below summarizes, DSG_SEB:1 defines eventing and moderation for its state variables.

Table F–3 - DSG SEB Event Moderation

Variable Name	Evented	Moderated Event	Max Event Rate[1]	Logical Combination	Min Delta per Event[2]
ServiceFigureOfMerit	no	no	n/a	n/a	n/a
MaxConnectedDevices	no	no	n/a	n/a	n/a
NumConnectedDevices	no	no	n/a	n/a	n/a
ConnectedDevices	no	no	n/a	n/a	n/a
GroupJoins	no	no	n/a	n/a	n/a
UpstreamChannelHeadroom	no	no	n/a	n/a	n/a
DownstreamChannelPower	no	no	n/a	n/a	n/a
UpstreamChannelPower	no	no	n/a	n/a	n/a
ChannelChange	yes	yes	2	n/a	n/a

[1] Determined by N, where Rate = (Event)/(N seconds).

[2] (N) * (allowedValueRange Step).

F.2.9.1 Event Model

The ChannelChange value is used to keep the SEBC informed of DCC and DBC events occurring at the SEBS. In some cases the SEBC needs to be aware of the channel change state so as to be able take action on messages/connections that are in place that may be impacted by the downtime associated with the channel change.

The SEBC MUST subscribe to these events and maintain the subscription for the entire duration that it is utilizing the services of the SEBS.

F.2.10 Actions

Immediately following Table F–4 is detailed information about the defined actions, including short descriptions of the actions, the effects of the actions on state variables, and error codes defined by the actions.

Except where noted, if an action is an error, calling the action will have no effect on state.

Table F–4 - DSG SEB Actions

Name	Req. or Opt.[1]
ClientConnect	R
ClientAddDevice	R
ClientRemoveDevice	R

ClientJoin	R
ClientLeave	R
GetServiceState	R
GetConnectedDevices	R

[1] R = Required, O = Optional

F.2.10.1 ClientConnect

The SEBC uses this action to request layer 2 frame forwarding for a connected device. The SEBS creates an SEB Tunnel for this purpose and returns tunnel's TCP port.

F.2.10.2 Arguments

Table F–5 - ClientConnect Arguments

Argument(s)	Direction	relatedStateVariable
AddMacAddress	IN	A_ARG_TYPE_MacAddress
AddDevType	IN	A_ARG_TYPE_DeviceType
SetTunnelPort	OUT	A_ARG_TYPE_TunnelPort

F.2.10.2.1 Dependency on State

None

F.2.10.2.2 Effect on State

None

F.2.10.2.3 Errors

Table F–6 - ClientConnect Error Codes

errorCode	errorDescription	Description
402	Invalid Args	See UPnP Device Architecture section on Control.
501	Action Failed	See UPnP Device Architecture section on Control.
606	Action not authorized	See UPnP Device Architecture section on Control.
801	Max Number Of Devices	See Common Error Codes below
802	SEBS service terminated	See Common Error Codes below

F.2.10.3 ClientAddDevice

The SEBC uses this action to request layer 2 frame forwarding for a connected device.

F.2.10.3.1 Arguments

Table F–7 - ClientAddDevice Arguments

Argument(s)	Direction	relatedStateVariable
AddMacAddress	IN	A_ARG_TYPE_MacAddress
AddDevType	IN	A_ARG_TYPE_DeviceType

F.2.10.3.2 Dependency on State

None

F.2.10.3.3 Effect on State

None

F.2.10.3.4 Errors

Table F–8 - ClientAddDevice Error Codes

errorCode	errorDescription	Description
402	Invalid Args	See UPnP Device Architecture section on Control.
501	Action Failed	See UPnP Device Architecture section on Control.
606	Action not authorized	See UPnP Device Architecture section on Control.
801	Max Number Of Devices	See Common Error Codes below
802	SEBS service terminated	See Common Error Codes below

F.2.10.4 ClientRemoveDevice

The SEBC uses this action to discontinue layer 2 frame forwarding for a connected device.

F.2.10.4.1 Arguments

Table F–9 - ClientRemoveDevice Arguments

Argument(s)	Direction	relatedStateVariable
RemoveMacAddress	IN	A_ARG_TYPE_MacAddress

F.2.10.4.2 Dependency on State

None

F.2.10.4.3 Effect on State

None

F.2.10.4.4 Errors

Table F–10 - ClientRemoveDevice Error Codes

errorCode	errorDescription	Description
402	Invalid Args	See UPnP Device Architecture section on Control.
501	Action Failed	See UPnP Device Architecture section on Control.
606	Action not authorized	See UPnP Device Architecture section on Control.
802	SEBS service terminated	See Common Error Codes below
803	Unknown Device	See Common Error Codes below

F.2.10.5 GetServiceState

This action requests that the SEBS return service state information to the requesting client device. Service state information is used by client devices to select an SEBS.

F.2.10.5.1 Arguments

Table F–11 - GetServiceState Arguments

Argument(s)	Direction	relatedStateVariable
GetServiceFigureOfMerit	OUT	ServiceFigureOfMerit
GetNumConnectedDevices	OUT	NumConnectedDevices

F.2.10.5.2 Dependency on State

None

F.2.10.5.3 Effect on State

None

Table F–12 - GetServiceState Error Codes

errorCode	errorDescription	Description
501	Action Failed	See UPnP Device Architecture section on Control.
606	Action not authorized	See UPnP Device Architecture section on Control.
802	SEBS service terminated	See Common Error Codes below

F.2.10.6 ClientJoin

This action requests that the SEBS join a multicast group and start forwarding the group to the requesting SEBC over the SEB tunnel.

F.2.10.6.1 Arguments

Table F–13 - ClientJoin Arguments

Argument(s)	Direction	relatedStateVariable
AddMulticastDstMacAddress	IN	A_ARG_TYPE_MacAddress
AddClientMacAddress	IN	A_ARG_TYPE_MacAddress

F.2.10.6.2 Dependency on StateClientLeave

None

F.2.10.6.3 Effect on State

None

F.2.10.6.4 Errors

Table F–14 - ClientJoin Error Codes

errorCode	errorDescription	Description
402	Invalid Args	See UPnP Device Architecture section on Control.
501	Action Failed	See UPnP Device Architecture section on Control.
606	Action not authorized	See UPnP Device Architecture section on Control.

F.2.10.7 ClientLeave

This action requests that the SEBS stop forwarding the group to the requesting SEBC over the SEB tunnel. If no other SEBC has joined this multicast group, the SEBS MAY leave the group, as well.

F.2.10.7.1 Arguments

Table F–15 - ClientLeave Arguments

Argument(s)	Direction	relatedStateVariable
RemoveMulticastDstMacAddress	IN	A_ARG_TYPE_MacAddress
RemoveClientMacAddress	IN	A_ARG_TYPE_MacAddress

F.2.10.7.2 Dependency on State

None

F.2.10.7.3 Effect on State

None

F.2.10.7.4 Errors

Table F–16 - ClientLeave Error Codes

errorCode	errorDescription	Description
402	Invalid Args	See UPnP Device Architecture section on Control.
501	Action Failed	See UPnP Device Architecture section on Control.
606	Action not authorized	See UPnP Device Architecture section on Control.
803	Unknown Device	See Common Error Codes below

F.2.10.8 GetConnectedDevices

This action allows a DSG SEB Client to request the list of client devices connected to the service.

F.2.10.8.1 Arguments

Table F–17 - GetConnected Devices Arguments

Argument(s)	Direction	relatedStateVariable
ListConnectedDevices	OUT	A_ARG_TYPE_Result

F.2.10.8.2 Effect on State

None

F.2.10.8.3 Errors

None

F.2.10.9 Relationships Between Actions

The actions defined herein may be called in any order.

F.2.10.10 Common Error Codes

The following table lists error codes common to actions for this service type. If an action results in multiple errors, the most-specific error should be returned.

Table F–18 - DSG SEB Common Error Codes

errorCode	errorDescription	Description
401	Invalid Action	See UPnP Device Architecture section on Control.
402	Invalid Args	See UPnP Device Architecture section on Control.
404	Invalid Var	See UPnP Device Architecture section on Control.
501	Action Failed	See UPnP Device Architecture section on Control.
801	Max Number of Devices	The number of SEBC devices serviced by the SEBS has reached the limit of the Max Number of CPE devices provisioned for the SEBS.
802	SEBS Service Terminated	The SEBS has terminated its SEBS services.
803	Unknown Device	The specified device identifier (typically a MAC address) is not recognized by the SEBS.

F.2.11 XML Service Description

```
<?xml version="1.0"?>
<scpd xmlns="urn:schemas-upnp-org:service-1-0">
  <specVersion> <!-- UPnP version 1.0 -->
    <major>1</major>
```

```
    <minor>0</minor>
  </specVersion>
  <actionList>
    <action> <!—ClientConnect to Server-->
      <name>ClientConnect</name>
      <argumentList>
        <argument>
          <name>AddMacAddress</name>
          <relatedStateVariable>MacAddress</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
  <argument>
          <name>AddDevType</name>
          <relatedStateVariable>DeviceType</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
         <argument>
          <name>SetTunnelPort</name>
          <relatedStateVariable>TunnelPort</relatedStateVariable>
          <direction>out</direction>
          <retval />
        </argument>
      </argumentList>
    </action>
    <action> <!—GetServiceState from Server-->
      <name>GetServiceState</name>
      <argumentList>
        <argument>
          <name>GetServiceFigureOfMerit</name>
          <relatedStateVariable>ServiceFigureOfMerit</relatedStateVariable>
          <direction>out</direction>
          <retval />
        </argument>
        <argument>
          <name>GetNumConnectedDevices</name>
          <relatedStateVariable>NumConnectedDevices</relatedStateVariable>
          <direction>out</direction>
          <retval />
        </argument>
      </argumentList>
    </action>
    <action> <!—Acquire ClientJoin multicast group-->
      <name>ClientJoin</name>
      <argumentList>
  <argument>
          <name>AddMulticastDstAddress</name>
          <relatedStateVariable>MacAddress</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
  <argument>
          <name>AddClientMacAddress</name>
          <relatedStateVariable>MacAddress</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
      </argumentList>
    </action>
    <action> <!—Add device on client's tunnel-->
      <name>ClientAddDevice</name>
      <argumentList>
```

```
        <argument>
          <name>AddMacAddress</name>
          <relatedStateVariable>MacAddress</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
        <argument>
          <name>AddDevType</name>
          <relatedStateVariable>DeviceType</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
      </argumentList>
    </action>
    <action> <!—Remove device from client's tunnel-->
      <name>ClientRemoveDevice</name>
      <argumentList>
        <argument>
          <name>RemoveMacAddress</name>
          <relatedStateVariable>MacAddress</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
      </argumentList>
    </action>
    <action> <!—Acquire ClientLeave multicast group-->
      <name>ClientLeave</name>
      <argumentList>
  <argument>
          <name>RemoveMulticastDstAddress</name>
          <relatedStateVariable>MacAddress</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
  <argument>
          <name>RemoveClientMacAddress</name>
          <relatedStateVariable>MacAddress</relatedStateVariable>
          <direction>in</direction>
          <retval />
        </argument>
      </argumentList>
    </action>
    <action> <!-Request list of connected devices ->
      <name>GetConnectedDevices</name>
      <argumentList>
        <argument>
          <name>ListConnectedDevices</name>
          <relatedStateVariable>ConnectedDevices</relatedStateVariable>
          <direction>out</direction>
        </argument>
      </argumentList>
    </action>
  </actionList>
  <serviceStateTable>
<stateVariable sendEvents="no">
      <name>ServiceFigureOfMerit</name>
      <dataType>ui4</dataType>
      <allowedValueRange>
        <minimum>0</minimum>
        <maximum>65536</maximum>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="no">
```

```
      <name>MacAddress</name>
      <dataType>bin:hex</dataType>
      <allowedValueRange>
        <minimum>00:00:00:00:00:00</minimum>
        <maximum>ff:ff:ff:ff:ff:ff</maximum>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>MaxConnectedDevices</name>
      <dataType>i4</dataType>
      <allowedValueRange>
        <minimum>0</minimum>
        <maximum>256</maximum>
        <step>+/-1</step>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>NumConnectedDevices</name>
      <dataType>i4</dataType>
      <allowedValueRange>
        <minimum>0</minimum>
        <maximum>256</maximum>
        <step>+/-1</step>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>ConnectedDevices</name>
      <dataType>CSV string</dataType>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>GroupJoins</name>
      <dataType>CSV string</dataType>
    </stateVariable>
   <stateVariable sendEvents="no">
      <name>UpstreamChannelHeadroom</name>
      <dataType>ui1</dataType>
      <allowedValueRange>
        <minimum>1</minimum>
        <maximum>17</maximum>
        <step>+/-1</step>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>DownstreamChannelPower</name>
      <dataType>i4</dataType>
      <allowedValueRange>
        <minimum>-999</minimum>
        <maximum>999</maximum>
        <step>+/-1</step>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>UpstreamChannelPower</name>
      <dataType>i4</dataType>
      <allowedValueRange>
        <minimum>-999</minimum>
        <maximum>999</maximum>
        <step>+/-1</step>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="yes">
      <name>DynamicChannelChange</name>
      <dataType>ui1</dataType>
```

```
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>DeviceType</name>
      <dataType>ui1</dataType>
      <allowedValueRange>
        <minimum>1</minimum>
        <maximum>4</maximum>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>TunnelPort</name>
      <dataType>ui4</dataType>
      <allowedValueRange>
        <minimum>0</minimum>
        <maximum>65534</maximum>
      </allowedValueRange>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>IpAddress</name>
      <dataType>string</dataType>
    </stateVariable>
   <stateVariable sendEvents="no">
      <name>IpAddressType</name>
      <dataType>ui1</dataType>
      <allowedValueRange>
        <minimum>0</minimum>
        <maximum>1</maximum>
      </allowedValueRange>
    </stateVariable>
</serviceStateTable>
</scpd>
```

F.3 DSG Set-top Extender Bridge (SEB) Theory Of Operation

The following use cases are provided to aid the developer in the implementation of the DSG SEB solution and are not meant to be an exhaustive set of use cases.

F.3.1 Server Discovery

F.3.1.1 One DSG Capable Device Completes DOCSIS Registration

This use case examines the very basic behavior of one DSG-capable device on a home network (e.g., MoCA), serving as an SEBS for one upstream-impaired DSG-capable device operating as an SEBC. Both of the DSG Capable Devices boot up, initialize DOCSIS and attempt to provision. One DSG Capable Device completes registration and assumes the role of SEBS, while the other devices become the SEBC. This use case applies equally to multiple upstream-impaired DSG Capable Devices becoming SEB client devices.

1. "n" DSG capable devices configured for two-way DSG mode where eCM bridging capabilities are enabled, where configured is defined as follows:
   a. DSG mode = two-way advanced
   b. ifAdminStatus for Home Network interface is set to UP
   c. Maximum Number of CPEs assigned to the eCM > 2 (one for the SEBS eSAFE and one for a connected device.)
   d. eCM's Network Access Control Object = 1.
   e. DSG SEB Control Object = TRUE.
2. DSG capable devices acquire DSG Tunnel(s).
3. DSG capable devices attempt to provision DOCSIS and establish Home Network (not necessarily in this order),

4. One of the "n" DSG capable devices completes DOCSIS registration
    a. provisions DHCP IP address for the eCM and eSTB as per [eDOCSIS]
    b. provisions link-local IP address for the eSTB as per [RFC 3927] for use on the Home Network.
        i. Link-local IP address used for DSG SEB communications
5. DSG capable device that completes DOCSIS registration measures its DOCSIS channel performance and verifies that the channel characteristics meet the minimum requirements for becoming an SEBS.
6. DSG capable device that completes DOCSIS registration calculates the Figure of Merit value, reflecting the quality of its DOCSIS channel.
7. DSG capable device that completes DOCSIS registration assumes role of SEBS and issues UPnP:Discovery:Advertisement:Notify-Alive as per [UPNP-DA].
8. DSG capable devices that fail to complete registration assume role of SEBC and gather SEBS service advertisements.
9. After waiting for further advertisements and receiving none, the SEBC queries the description of the SEBS (issues HTTP GET on the root URL provided in the UPnP:Discovery:Search:Response from the SEBS as per "retained" Alive message).
10. SEBS responds providing the Root Description of the SEBS.
11. SEBC parses content of Root Description and requests a description of the DSG SEB services of the SEBS (issues HTTP GET on the services URL, i.e., the SCPDURL, provided in the root description of the SEBS)
12. SEBS responds with its DSG SEB services information
13. SEBC posts GetServiceState service action request to SEBS to retrieve the candidate server's Figure of Merit and number of connected devices. (NOTE: when only one (1) SEBS advertisement has been received, SEBC could omit this query.)
14. Assuming that there is just one SEBS advertisement available to this SEBC, the SEBC posts a ClientConnect service action request to the SEBS, passing the eCM-MAC and eCM-Type and receiving back the TCP port assigned for the client's use.
15. SEBC opens a TLS-secured SEB tunnel to the SEBS, using the port assigned by the SEBS.
16. SEBC posts ClientAddDevice service actions with the MAC addresses of the SEB eSTB.
17. SEBC initiates DHCP in an effort to acquire an IP address, using normal DHCP discovery and request over the SEB tunnel. The SEBS forwards DHCP traffic in both directions between the SEBS tunnel and the WAN connection using its DOCSIS upstream and downstream channels.
18. SEBC receives Offers/Solicits from DHCP servers, and selects an appropriate DHCP offer according to its normal DHCP procedures.
19. SEBS and SEBC configured.

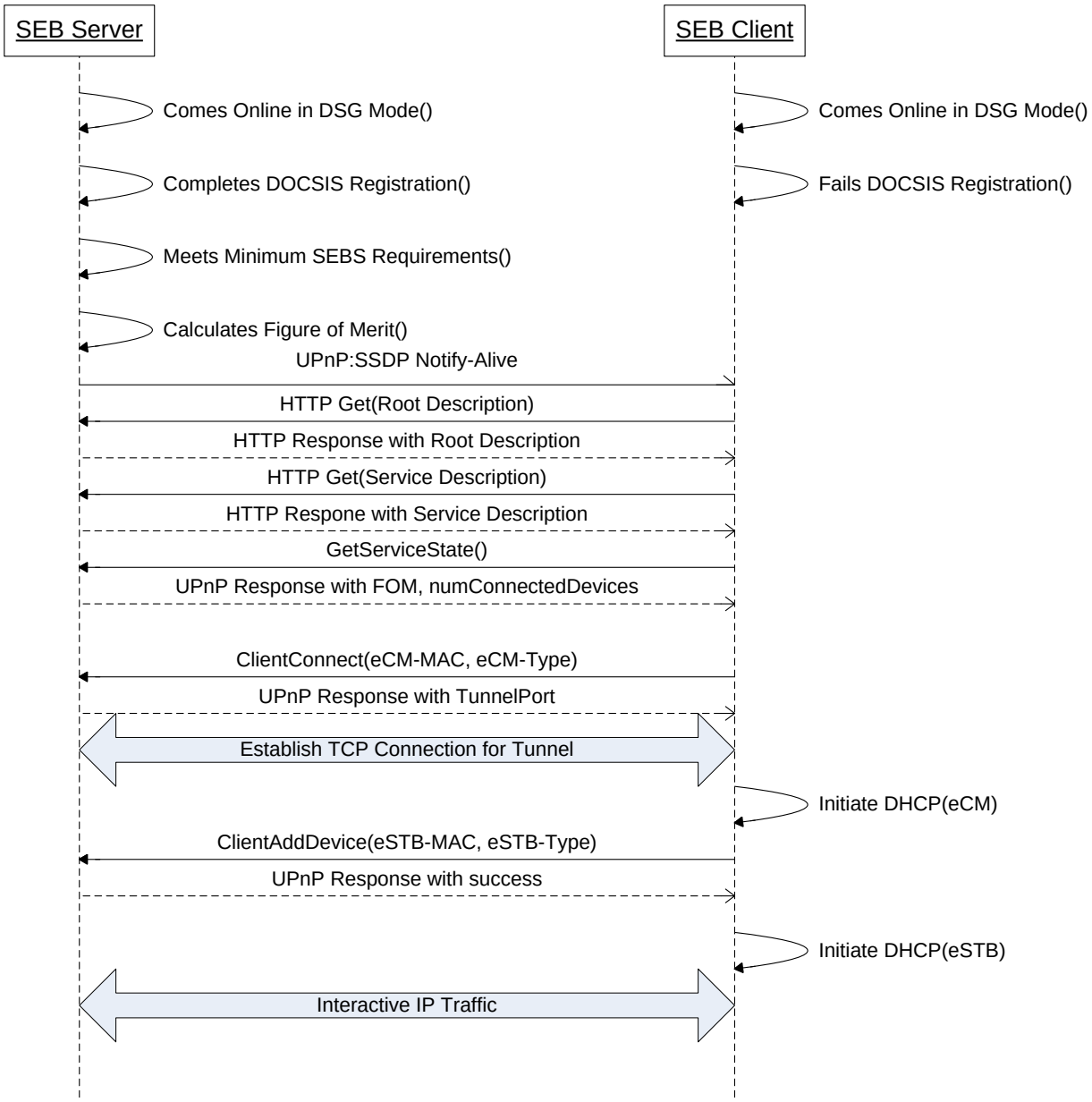


Figure F–3 - Basic SEBS and SEBC configuration

F.3.1.2 Multiple DSG Capable Devices Complete DOCSIS Registration

This use case examines SEB Client selection of a candidate SEB Server when more than one DSG-capable device on a home network (e.g., MoCA), completes DOCSIS registration. The DSG Capable Devices boot up, initialize DOCSIS and attempt to provision. More than one DSG Capable Device completes registration and advertises as a candidate SEB Server, while one or more other devices become SEB Client devices.

1. "n" DSG capable devices configured for two-way DSG mode where eCM bridging capabilities are enabled, where configured is defined as follows:
   a. DSG mode = two-way advanced
   b. ifAdminStatus for Home Network interface is set to UP

c. Maximum Number of CPEs assigned to the eCM > 2 (one for the SEBS eSAFE and one for an attached device.)

d. eCM's Network Access Control Object = 1.

e. DSG SEB Control Object = TRUE.

2. DSG capable devices acquire DSG Tunnel(s).
3. DSG capable devices attempt to provision DOCSIS and establish Home Network (not necessarily in this order),
4. One or more of the "n" DSG capable devices completes DOCSIS registration
   a. provisions DHCP IP address for the eCM and eSTB as per [eDOCSIS]
   b. provisions link-local IP address for the eSTB as per [RFC 3927] for use on the Home Network.
      i. Link-local IP address used for DSG SEB communications
5. DSG capable devices that complete DOCSIS registration measure their DOCSIS channel performance and verify that the channel characteristics meet the minimum requirements for becoming an SEBS.
6. DSG capable devices that complete DOCSIS registration calculate the Figure of Merit value, reflecting the quality of their DOCSIS channels.
7. DSG capable devices that complete DOCSIS registration issue UPnP:Discovery:Advertisement:Notify-Alive as per [UPNP-DA].
8. DSG capable devices that fail to complete registration assume role of SEBC and gather SEBS service advertisements.
9. After waiting for advertisements, the SEBC queries each candidate SEBS for its device description and service description.
10. SEBS responds providing the Root Description of the SEBS.
11. SEBC posts GetServiceState service action request to each SEBS to retrieve the candidate server's Figure of Merit and number of connected devices.
12. SEBC examines the returned service state information and selects a candidate server:
    a. If any SEBS reports non-zero number of connected devices, select that SEBS.
    b. If all SEBS report zero (0) connected devices, SEBC selects SEBS with highest reported Figure of Merit.
    c. If all SEBS with zero (0) connected devices report identical Figure of Merit values, select SEBS with lowest MAC address.
13. SEBC proceeds with tunnel establishment using selected SEBS.

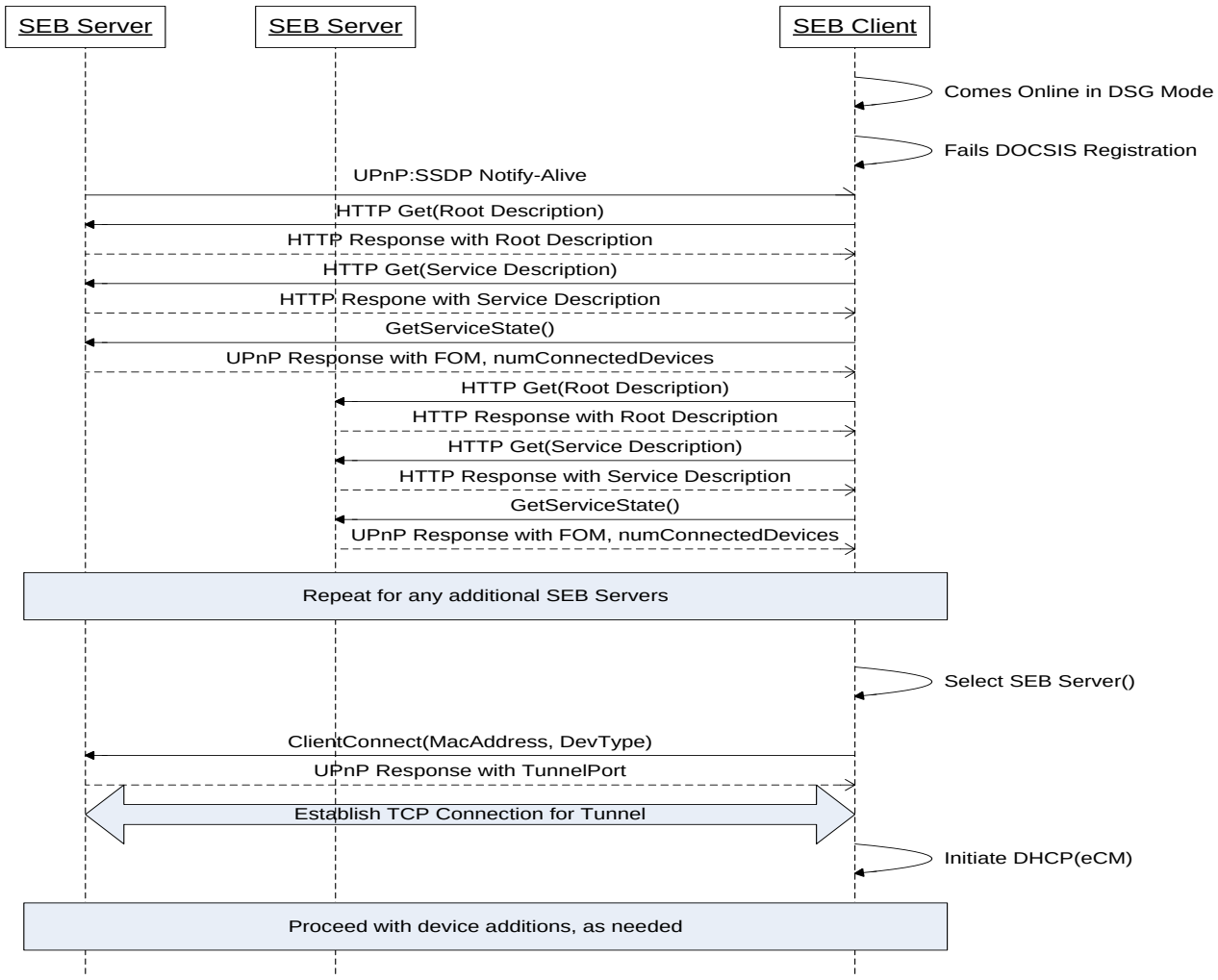


Figure F–4 - SEBS and SEBC configuration with Multiple SEBS Candidates

F.4 Procedure to Select SEB Server and Establish SEB Tunnel

F.4.1 Client View

F.4.1.1 SEB Client Eligibility

For a device containing an eCM, the following requirements determine when to enable SEB Tunnel acquisition mode.

- When the eCM enters the One-way Operation state, the SEBC MUST enable SEB Tunnel acquisition mode.
- When the eCM enters the Two-way Operation state, the SEBC MUST disable SEB Tunnel acquisition mode.

F.4.1.2 Establishing the SEB Tunnel

A DSG capable device that is not able to establish a DOCSIS upstream channel and initiates SEBC functionality will use the procedures in this section to search for a SEBS, establish the SEB Tunnel, and thereby establish interactive layer 2 connectivity with the HFC plant. The DSG capable device that is not operating as a SEBC MUST

NOT attempt to establish a SEB Tunnel. The DSG capable device that terminates SEBC functionality MUST immediately close the TCP connection associated with any previously established SEB Tunnel.

The SEBC gathers service advertisements and selects a SEBS by examining each service advertisement Figure of Merit and the number of connected devices. When no server currently has connected devices, the SEBC MUST select the server with the highest server Figure of Merit value. When two or more servers advertise the same (highest) Figure of Merit, the SEBC MUST select the server with the lowest MAC address.

When the SEBC finds a SEBS that already has one or more connected devices, the SEBC MUST select that server, regardless of the server's advertised Figure of Merit.

Upon selecting a SEB Server advertisement, the SEBC MUST open a TCP connection using the port number obtained using the UPnP ClientConnect action. Then the SEBC MUST use this TCP connection to establish a TLS connection. The SEB Client device will use a single TCP connection for all connected devices, and MUST NOT open more than one TCP connection at a time for the SEB Tunnel. If either the TCP connection or the TLS connection cannot be established, the SEB Client MUST discard its cached server information and restart the SEB Server advertisement collection process.

The client's server selection process is illustrated in Figure F–5 and Figure F–6.

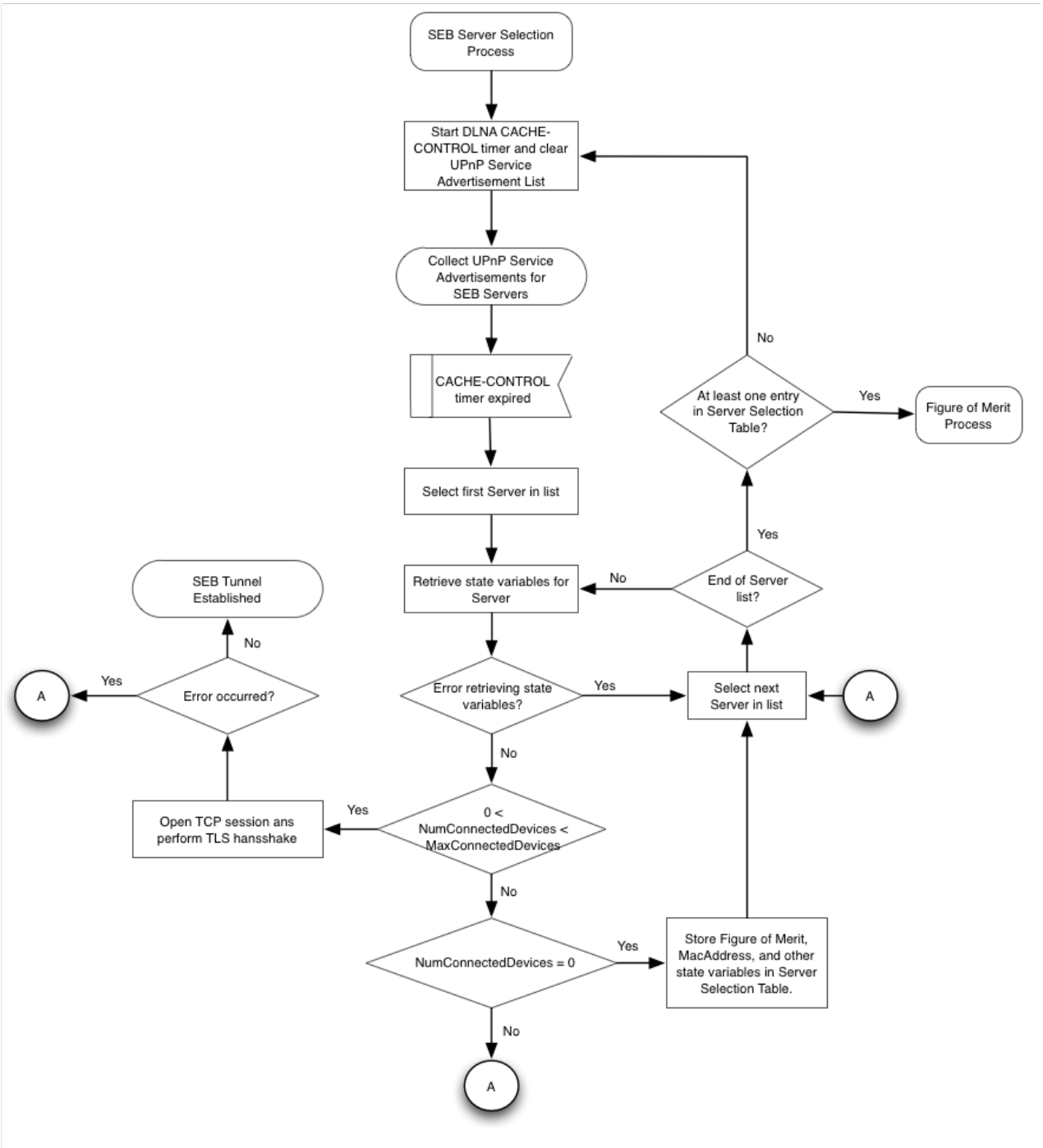


Figure F–5 - SEB Server Selection Process

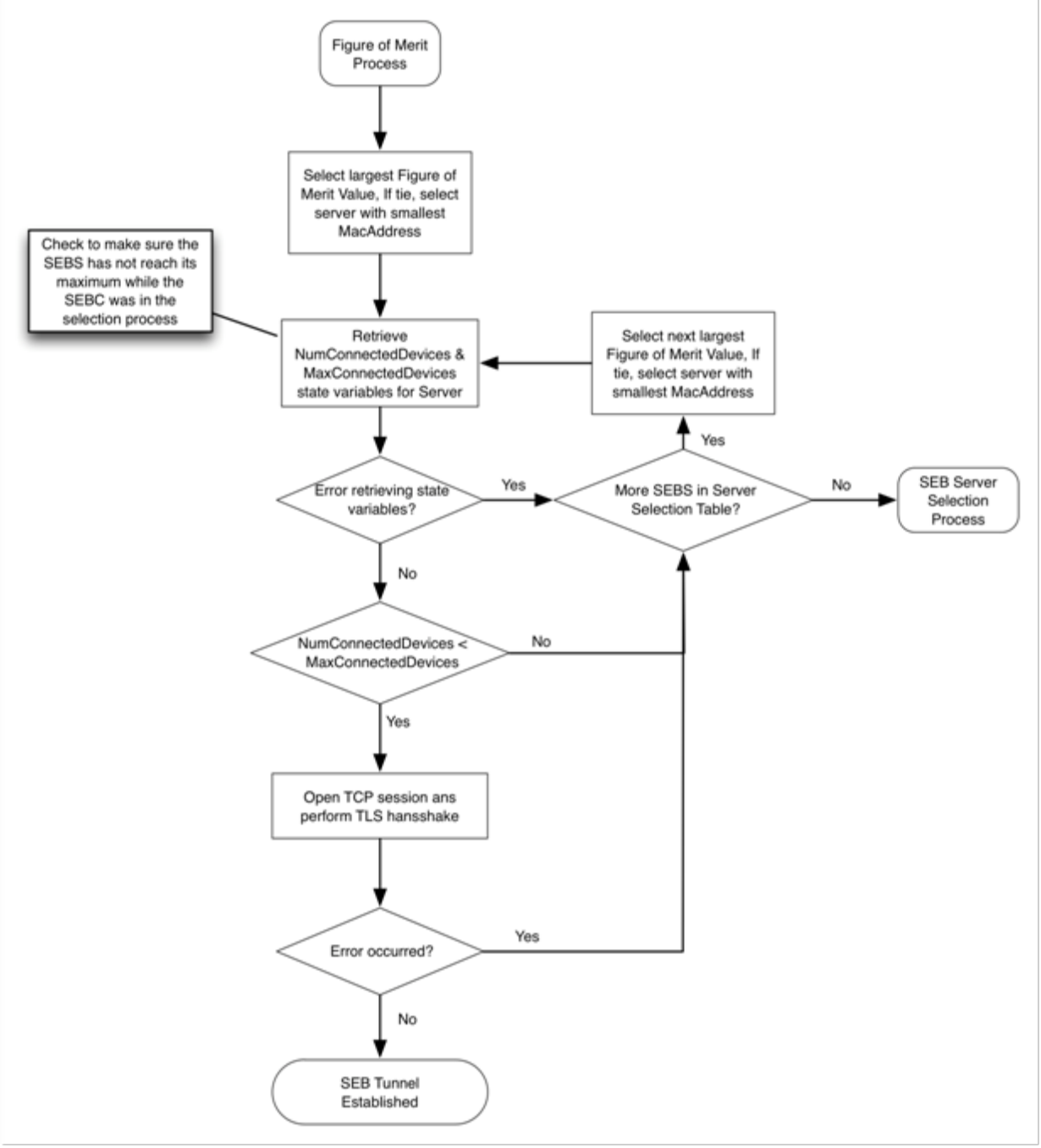


Figure F–6 - SEB Server Selection Figure of Merit Process

F.4.1.3 SEB eCM Management

Generally, an eCM in the One-way Operation state is not manageable from the headend. However, in a device with an established SEB Tunnel, the SEB eCM is manageable through the SEB Tunnel.

When the SEB Tunnel is established, the eCM MUST attempt SEB Tunnel SEB eCM IP Acquisition by using the following procedure:

- The eCM MUST perform the Establish IP Connectivity process. For the DOCSIS 2.0+IPv6 eCM or DOCSIS 3.0 eCM, the IP mode is selected using standard methods (e.g., MDD TLV 5.1 or the IpProvMode attribute).
- If an error occurs, the eCM MUST restart the Connectivity process.
- The eCM MUST perform the Establish Time of Day process.
- The eCM MUST perform the Transfer Operational Parameters process.
- If an error occurs, the eCM MUST release its IP address and restart the Transfer Operational Parameters procedure.

The details of the steps above are described in [DOCSIS-RFIv2.0] or [DOCSIS-MULPI] depending on the capabilities of the eCM.

The eCM continues periodically attempting to re-establish the upstream as dictated by the Tdsg3 timer. When the Tdsg3 timer expires, the eCM MUST release its IP address. If the attempt to re-establish the upstream fails, the eCM MUST perform the SEB Tunnel SEB eCM IP Acquisition procedure again.

The eCM Host interface to the SEB Tunnel is considered an RF interface for the [DOCSIS-RFIv2.0] and [DOCSIS-MULPI] requirements about management traffic. In particular, the eCM is permitted to send and receive DHCP, DHCPv6, TFTP, and IPv6 Router Advertisements using the SEB Tunnel. The interface to the SEB Tunnel is not considered a CMCI port.

Likewise, the [DOCSIS-OSSIv3.0] section, "OSSI for PHY, MAC, and Network Layers" or [SCTE 79-2] section, "OSSI for Radio Frequency Interface", applies to SEB eCM communication using the SEB Tunnel.

In some cases, the eCM will alternate between Two-Way Operation and management through the SEB Tunnel. If the standard eCM MAC address is used for management through the SEB Tunnel, then the CMTS might conclude that MAC address spoofing is occurring. To avoid the appearance of spoofing, a different MAC address will be used for management through the SEB Tunnel.

The SEB eCM will create an alternate MAC address for use on the SEB Tunnel by inverting the Universally/Locally Administered address bit of its standard MAC address. In the hexadecimal representation of the MAC address, the Universally/Locally Administered bit is represented as 02-00-00-00-00-00. For example, the address 00-01-A6-D0-0B-1E would be transformed into 02-01-A6-D0-0B-1E.

The following requirements describe the use of this transformed MAC address:

- The eCM MUST construct the SEB Management Address by inverting the Universally/Locally Administered bit of its standard MAC address.
- The SEB eCM MUST use the SEB Management Address as the source MAC address of all ethernet frames inserted into the SEB Tunnel.
- The SEB eCM MUST discard any unicast ethernet frame received from the SEB Tunnel with a destination address other than the SEB Management Address.
- The SEB eCM MUST use the SEB Management Address to identify itself in any packet sent over the SEB Tunnel. This includes DHCPv4 and DHCPv6 packets that embed a MAC address.
- The SEB eCM MUST use the SEB Management Address to construct Link-local and Solicited-node IPv6 addresses to use on the SEB Tunnel.

F.4.2 Server View

F.4.2.1 SEB Server Eligibility and Advertisement

Upon booting a device will examine the eCM operational status as illustrated in Figure F–7 to determine if it is eligible to send SEB Server advertisements.

The device will continue to monitor the eCM operational status as illustrated in Figure F–7. The device MUST re-evaluate its eligibility upon any change to a FOM parameter in Table F–19 or to any weighting factor. Other administrative controls such as SNMP MIBs can also cause a device to disable its SEB Server component.

An eligible device MUST enable its SEB Server component.

An ineligible device MUST disable its SEB Server component. When the SEB Server component is disabled:

- The device MUST NOT send SEB Server advertisements.
- The device MUST close any established SEB Tunnels by sending a TCP FIN packet.

The term "SEB Server" is used in all other sections of this document to describe an eligible device with an enabled SEB Server component.

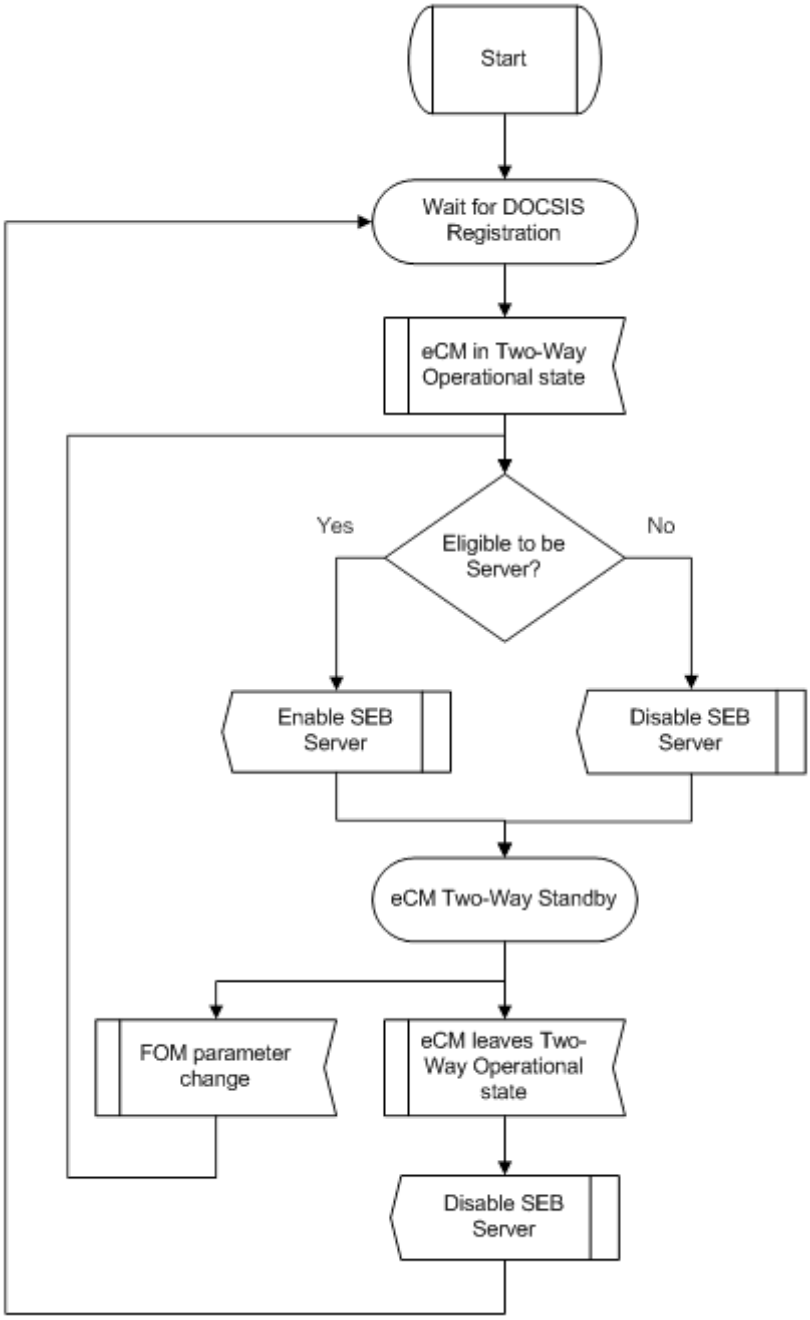


Figure F–7 - SEB Server Enable/Disable State

F.4.2.2 Establishing the SEB Tunnel

Upon receiving a UPnP ClientConnect service action, the SEBS will determine if it can support an additional connected device as illustrated in Figure F–8. If the SEBS can support an additional connected device, it will create a TCP listener port and instantiate an instance of the state machine illustrated in Figure F–9. If the SEBS cannot support an additional connected device, then the SEBS will return a UPnP error.

The maximum number of connected devices supported by the SEBS is constrained by the eCM's Maximum Number of CPEs configuration file parameter as well as implementation limits. When the connected device limit is reached, the SEB Server MUST continue to transmit SEB Server advertisements.

If a TLS session is not successfully established within the SEB Tunnel Timeout, the SEBS MUST close this TCP listener port and free all associated resources to avoid resource depletion. The default SEB Tunnel Timeout value MUST be 120 seconds. If a SEBC attempts to establish a TCP connection to a SEBS to a closed listener port, then the SEBS MUST refuse the TCP connection by sending a TCP RST packet.

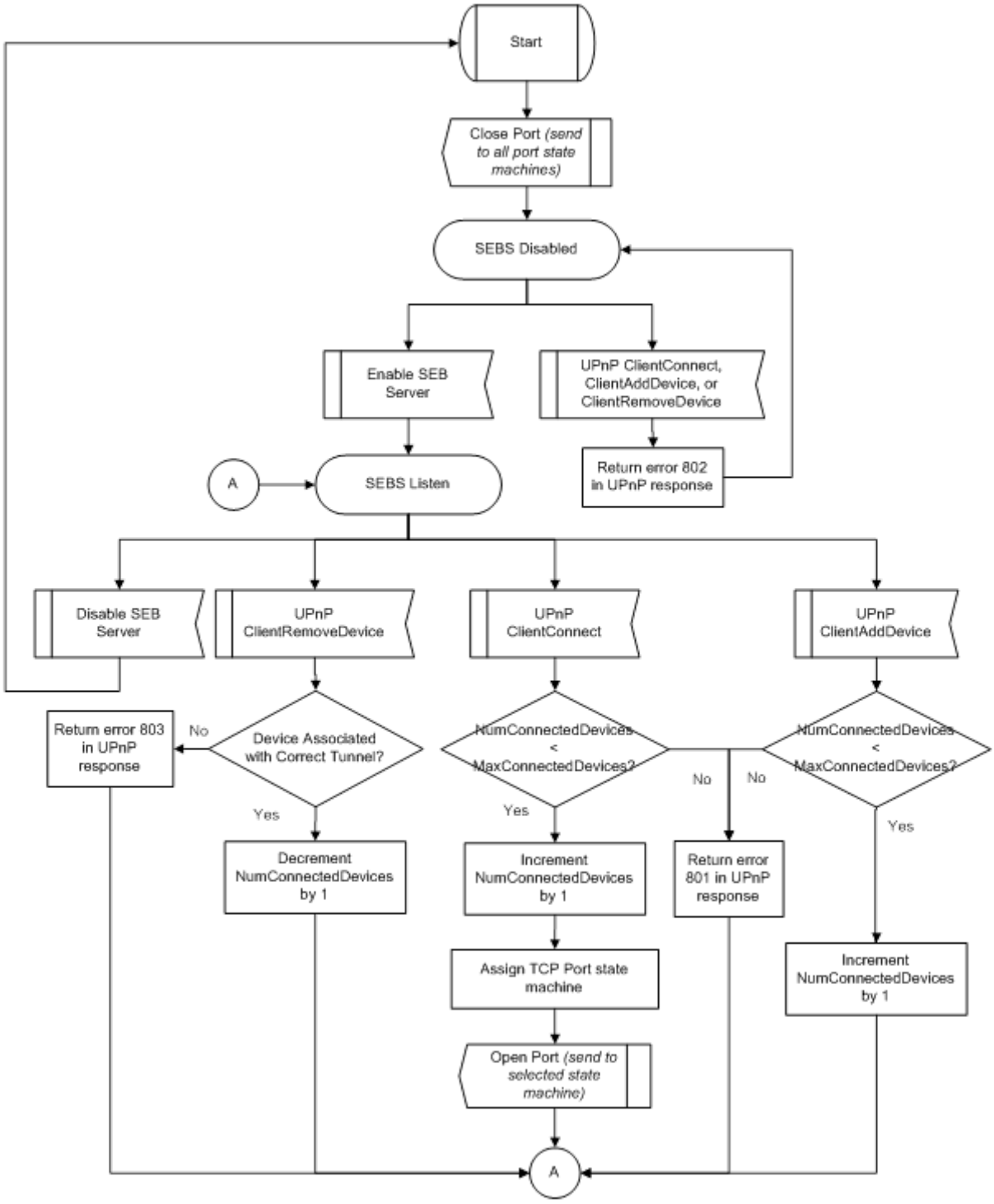


Figure F–8 - SEB Server Response to UPnP ClientConnect, ClientAddDevice, and ClientRemoveDevice service actions.

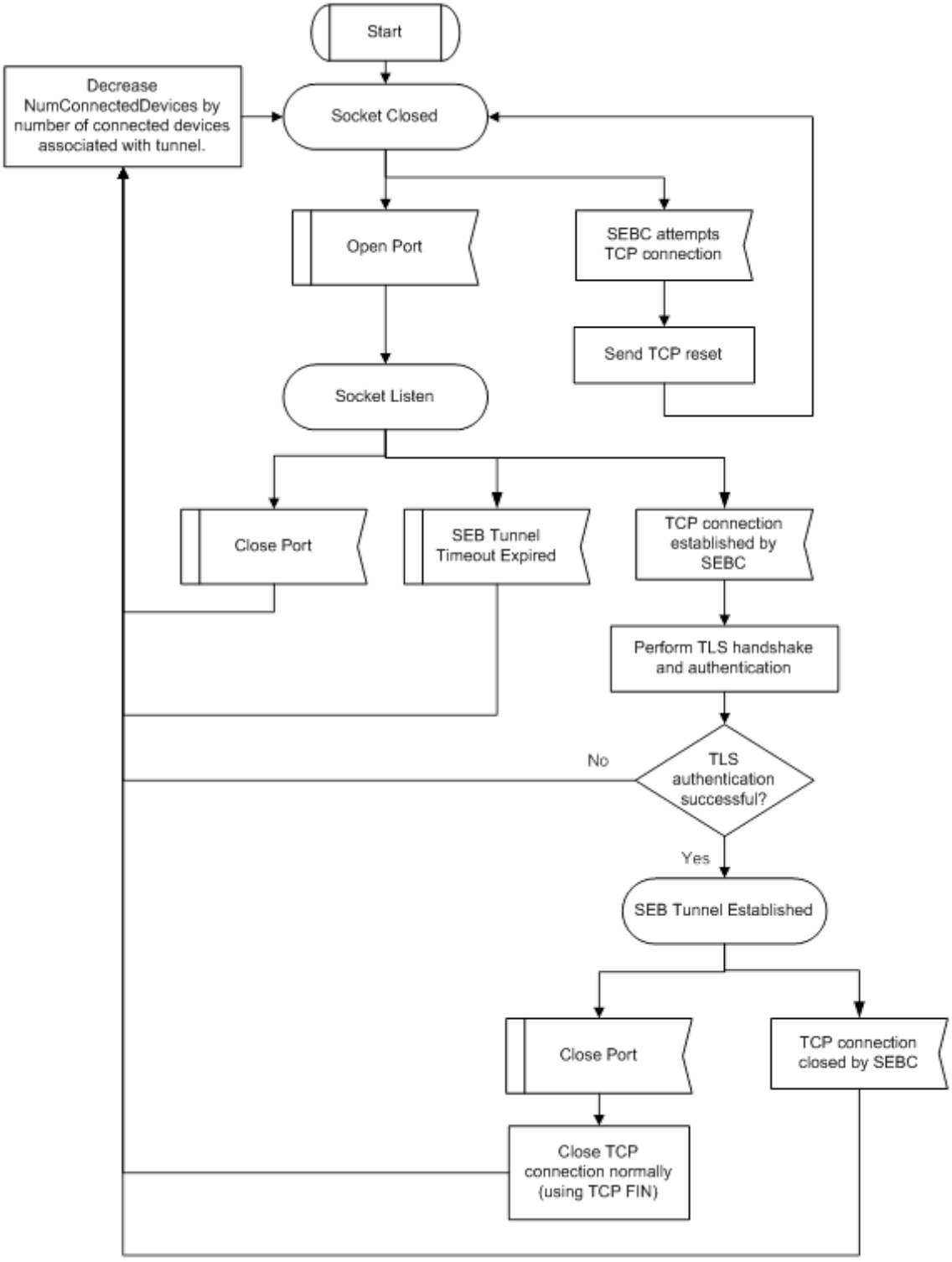


Figure F–9 - SEB Tunnel TCP Socket Handling

F.5 Determining Server Figure of Merit

When 2 or more DSG SEB capable devices are advertising SEBS, the following process is used by each candidate SEBS to determine a "Figure of Merit" that represents its fitness to act as the SEBS on the home network.

F.5.1 Definitions

This section defines several physical measurements and constants used in the "Figure of Merit" calculation:

Table F–19 - SEBS Figure of Merit Calculation - Definitions

Parameter	Description	Default	Comments
USTXPWR	Upstream Transmit Power (dBmV)		Measured
USPWRHR	Upstream Transmit Power Headroom (dB)	6	Configurable: dsgIfStdDsgSebFomUsPwrHr
MFMXPWR	Maximum Power for Modulation Format (dBmV)	See Table F–21	Configurable: dsgIfStdDsgSebFomMfQpsk dsgIfStdDsgSebFomMfQam16 dsgIfStdDsgSebFomMfQam64
DSRXPWR	Downstream Receive Power (dBmV)		Measured
DESDSPWR	Desired Receive Power (dBmV)	0	Configurable: dsgIfStdDsgSebFomDsDesPwr
DSPMAX	Downstream Receive Maximum Power (dBmV)	+5	Configurable: dsgIfStdDsgSebFomDspMax
DSPMIN	Downstream Receive Minimum Power (dBmV)	-6	Configurable: dsgIfStdDsgSebFomDspMin
NMTERNG	Non-Main Tap Power Range (dB)	80	Configurable: dsgIfStdDsgSebFomNmteRng
NMTER	Non-Main Tap Energy Ratio [ ]		Calculated
NMTEMAX	Maximum Permissible NMT Power (dB)	-5	Configurable: dsgIfStdDsgSebFomNmteMax
MTC	Main Tap Compression		Calculated
MTCMIN	Main Tap Compression Minimum	-2	Configurable: dsgIfStdDsgSebFomMtcMin

The device MUST calculate NMTER and MTC as specified in [DOCSIS-PNMP].

Table F–20 - Maximum Upstream Transmit Power by Modulation Format

Parameter	QPSK	QAM16	QAM64
MFMXPWR	58 dBmV	55 dBmV	54 dBmV

F.5.2 SEB Server Minimum Requirements

Candidate SEB servers first must ensure that DOCSIS connection meets certain minimum requirements. If the candidate server's DOCSIS connection does not meet these minimum criteria, then the device MUST NOT advertise the SEB service. The minimum criteria are summarized in Table F–21.

Table F–21 - Server DOCSIS Connection Parameters, Minimum Requirements

DOCSIS Parameter	Minimum Requirement
Upstream Transmit Power	USTXPWR < (MFMXPWR - USPWRHR)
Downstream Receive Power	DSPMIN ≤ DSRXPWR ≤ DSPMAX
Main Tap Compression	MTC > MTCMIN

F.5.3 SEB Server FOM

The SEB Server "Figure of Merit" consists of three terms contributed by upstream transmit power level measurement, downstream receive power level measurement, and downstream equalizer performance. The FOM value is given by

$$FOM = FOM_{USPWR} + FOM_{DSPWR} + FOM_{EQ}$$

Where FOMUSPWR is the contribution from upstream transmit power level, FOMDSPWR is the contribution from downstream receive power level, and FOMEQ is the contribution from equalizer performance.

F.5.4 SEB Server FOM – Upstream Transmit Power

A device that is transmitting near its maximum upstream power level for the active modulation format should not attempt to assume the role of SEBS. To be a SEBS candidate, a device's upstream transmit power level MUST be less than the maximum upstream transmit power level for the active upstream transmit modulation format, less an operator-configurable headroom. When a device does not meet the minimum requirement that USTXPWR < (MFMXPWR - USPWRHR), then the device MUST NOT advertise itself as an SEBS.

The upstream transmit power level contribution to the "Figure of Merit" calculation is given by:

$$FOM_{USPWR} = \left\lceil 1 - \left(\frac{USTXPWR}{MFMXPWR}\right)\right\rceil \text{ x } W_{USPWR}$$

where W_{USPWR} is an operator configurable weighting factor (defined by the dsgIfStdDsgSebFomWeightUpstreamPower object) with values from 0 to 100 for the upstream transmit power term. When W_{USPWR} is set to zero (0), the device MUST NOT include upstream transmit power level in the FOM calculation. When W_{USPWR} is set to zero (0), the device MUST NOT perform the upstream transmit power level minimum requirement test.

F.5.5 SEB Server FOM – Downstream Receive Power

A device that is receiving its downstream channel at an extremely low or high power level should not attempt to assume the role of SEBS. To be a SEBS candidate, a device's downstream receive power level MUST be greater than or equal to the configured minimum downstream receive power level, DSPMIN, and less than or equal to the configured maximum downstream receive power level, DSPMAX. When a device does not meet the minimum requirement that DSPMIN ≤ DSRXPWR ≤ DSPMAX, then the device MUST NOT advertise itself as an SEBS.

The downstream receive power level contribution to the "Figure of Merit" calculation is given by:

$$FOM_{DSPWR} = \left\lceil 1 - \alpha bs\ \left(\frac{DSTXPWR - DESDSPWR}{DSPMAX - DSPMIN}\right)\right\rceil \text{ x } W_{DSPWR}$$

where W_{DSPWR} is an operator configurable weighting factor (defined by the dsgIfStdDsgSebFomWeightDownstreamPower object) with range 0 to 100, for the downstream receive power term. When W_{DSPWR} is set to zero (0), the device MUST NOT include downstream receive power level in the FOM calculation. When W_{DSPWR} is set to zero (0), the device MUST NOT perform the downstream transmit power level minimum requirement test.

F.5.6 SEB Server FOM – Equalizer

When a device's upstream equalizer is struggling to cope with impairments in the access network and home network, the device should not attempt to assume the role of SEBS.

Two measures of equalizer performance are used to help determine the quality of the device's connection:

1. As described in [DOCSIS-PNMP], the adaptive equalizer main tap compression (MTC) at the CM is a good indicator of the available margin for the equalization compensation process. The equalizer main tap compression, MTC, is tested to determine when the device should disqualify itself from consideration. For MTC, being an application of attenuation, larger negative values indicate that the equalizer is working harder to overcome plant impairments.

2. As described in [DOCSIS-PNMP], the adaptive equalizer's non-main tap to total energy ratio is a useful distortion metric for the distortion level in the upstream path. The equalizer non-main tap compression ratio, NMTER, provides an overall evaluation of equalizer performance over the entire range, with low values particularly indicating that the device is not suffering impairments through microreflections. In addition, any individual non-main tap energy level being above a maximum value indicates significant impairment.

To be an SEBS candidate, the device's main tap compression, MTC, must be greater than an operator configurable minimum value, MTCMIN. When a device does not meet the minimum requirement that MTC > MTCMIN, then the device MUST NOT advertise itself as an SEBS. In addition, no individual non-main tap energy level should be above an operator configurable maximum value, NMTEMAX. When any NMTE > NMTEMAX, then the device MUST NOT advertise itself as an SEBS.

The equalizer contribution to the "Figure of Merit" calculation is given by:

$$FOM_{EQ} = \left\lceil \frac{(0 - NMTER)}{NMTERNG} \right\rceil \text{ x } W_{EQ}$$

Where W_{EQ} is an operator configurable weighting factor (defined by the dsgIfStdDsgSebFomWeightEqualizer object) with range 0 to 100, for the equalizer term. When W_{EQ} is set to zero (0), the device MUST NOT include equalizer performance in the FOM calculation. When W_{EQ} is set to zero (0), the device MUST NOT perform the minimum main tap compression requirement test.

F.5.7 Calculating FOM

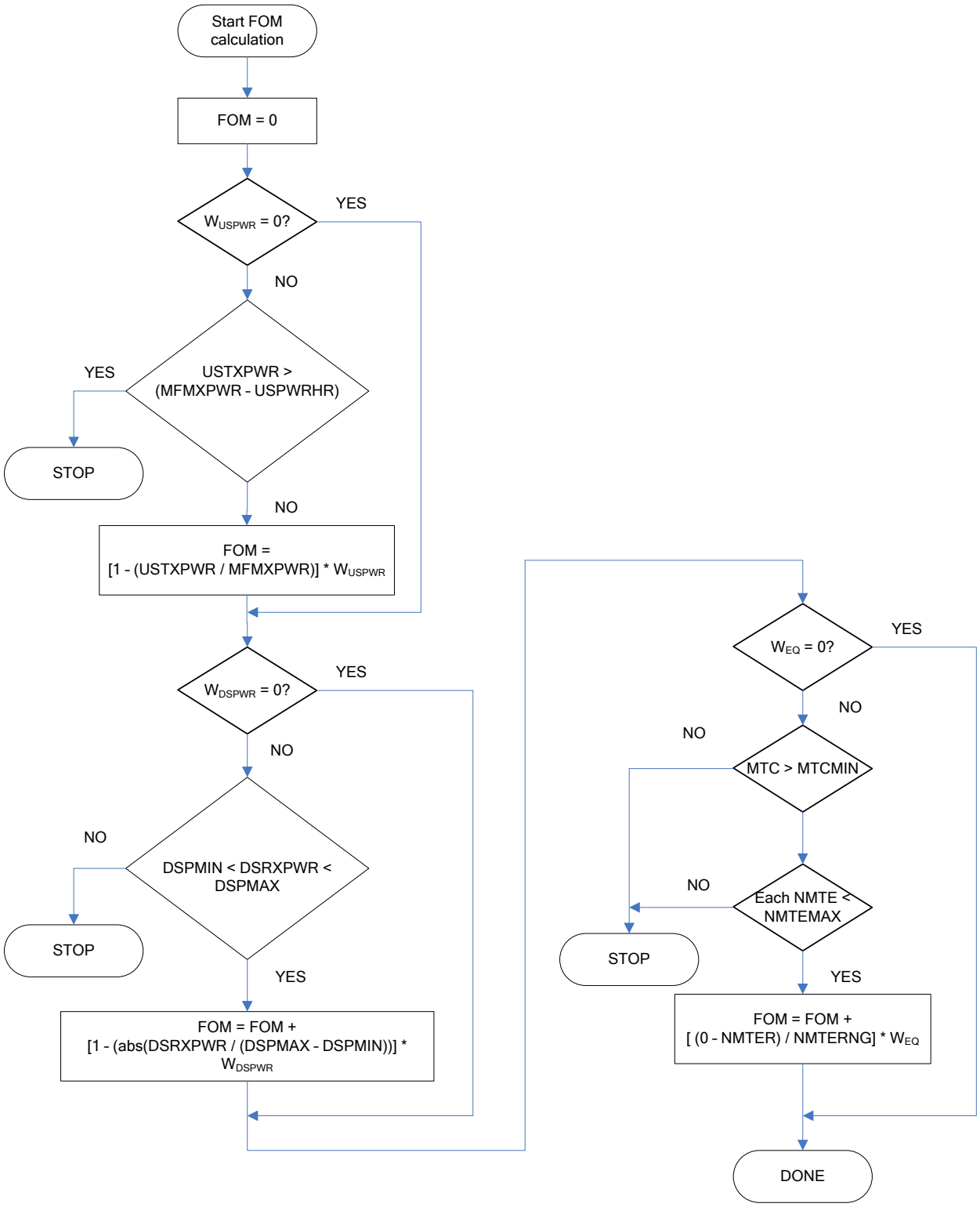


Figure F–10 - Figure of Merit Calculation

Appendix I Parsing the MIB in the DSG Agent (Informative)

The DOCSIS Set-top Gateway MIB (DSG-IF-MIB) is illustrated in the Figure I-1 below. The figure illustrates the relationships between the several tables in the MIB.

This section details the manner in which the MIB data can be parsed in the Agent to form the DCD message on each downstream. The format and data contained within the MIB are specified within the MIB documentation. If this informative section differs from the normative MIB documentation, the MIB documentation predominates.

The figure shows nine tables:

dsgIfClassifierTable
dsgIfTunnelTable
dsgIfTunnelGrpToChannelTable
dsgIfDownstreamTable
dsgIfClientIdTable
dsgIfVendorParamTable
dsgIfChannelListTable
dsgIfTimerTable
docsQosServiceClassTable (see [DOCSIS-OSSIv3.0]).

Numbers in parentheses (51) indicate a TLV type as shown in Table 5–1. This notation is used throughout the rest of this section as an aid to tracking text relevant to specific TLVs. The TLV types are documented in Annex C of [DOCSIS RFI/MULPI].

Here is the mapping between the TLVs shown in Table 5–1 and the MIB objects.

Table I–1 - Mapping TLVs and MIB Objects

TLV Type	Table 5-1 Name	MIB Object /(or other method)
23	Downstream Packet Classification Encoding	
23.2	Classifier Identifier	dsgIfClassId
23.5	Classifier Priority	dsgIfClassPriority
23.9	IP Packet Classification Encodings	
23.9.3	Source IP Address	dsgIfClassSrcIpAddr
23.9.4	Source IP Mask	computed from dsgIfClassSrcIpPrefixLength
23.9.5	Destination IP Address	dsgIfClassDestIpAddress
23.9.9	Dest TCP/UDP Port Start	dsgIfClassDestPortStart
23.9.10	Dest TCP/UDP Port End	dsgIfClassDestPortEnd
50	DSG Rule	
50.1	DSG Rule Identifier	(computed during parsing)
50.2	DSG Rule Priority	dsgIfTunnelGrpRulePriority
50.3	DSG UCID List *(Deprecated)*	dsgIfTunnelGrpUcidList *(Deprecated)*
50.4	DSG Client ID	
50.4.1	DSG Broadcast	dsgIfClientIdType
50.4.2	DSG Well-Known Mac Addr	dsgIfClientIdType / Value
50.4.3	CA System ID	dsgIfClientIdType / Value
50.4.4	Application ID	dsgIfClientIdType / Value
50.5	DSG Tunnel Address	dsgIfTunnelMacAddress
50.6	DSG Classifier Identifier	dsgIfClassId
50.43	DSG Rule Vendor Specific Params	dsgIfVendorOUI / Value

TLV Type	Table 5-1 Name	MIB Object /(or other method)
51	DSG Configuration	
51.1	DSG Channel List	dsgIfChannelDsFreq
51.2	DSG Initialization Timeout (Tdsg1)	dsgIfTimerTdsg1
51.3	DSG Operational Timeout (Tdsg2)	dsgIfTimerTdsg2
51.4	DSG Two-way Retry Timer (Tdsg3)	dsgIfTimerTdsg3
51.5	DSG One-way Retry Timer (Tdsg4)	dsgIfTimerTdsg4
51.43	DSG Config Specific Parameters	dsgIfVendorOUI / Value

The DCD message that is unique for an individual downstream is constructed using one row from the dsgIfDownstreamTable chosen with index {IfIndex}. The remainder of this section describes how one individual DCD message is parsed from the MIB. This process can be repeated for each DCD message.

The following procedure outlines how to assemble a DCD message from the MIB. The procedure moves through the MIB from the starting point (let's call it the 'root') to a single 'leaf' on the tree. At each juncture, TLVs are added to the DCD message. Along that journey from the root to the leaf, the procedure calls for iteration to select 'branches' not taken. Bear in mind then, that the procedure below must be used iteratively (in places) to construct all of the Rules and Classifiers that must go into the final DCD message. Where iteration is called for, the notation (*iteration*) is used.

The goal is to assemble a DCD message populated with TLVs listed in Table 5–1. Start assembling a DCD message using index {IfIndex} and finding one row in the dsgIfDownstreamTable.

It's worth noting here that the dsgIfDownstreamTable contains an entry for dsgIfDownEnableDCD. This value is used via SNMP to control the Agent as specified in the DSG specification. It does not have a direct counterpart entry in the DCD message. Because a DCD containing a tunnel cannot be disabled, this object is used only to enable/disable DCD messages on channels that are not carrying DSG Tunnels. Such channels might then carry DSG Configuration TLVs, and in particular, the DSG Channel List.

I.1 DSG Configuration TLVs (51)

The dsgIfDownstreamTable contains the information necessary to construct the DSG Configuration TLV. Add a DSG Configuration TLV (51) to the DCD message if any of the following TLVs are added to the DCD message.

- DSG Channel List (51.1)
    - The dsgIfDownstreamTable has the index {dsgIfDownChannelListIndex}, which (when it exists) points to the proper rows of downstream channels in the dsgIfChannelListTable. Use the second index {dsgIfChannelIndex} to walk through those rows. Add each channel frequency to the DCD via an instance of TLV 51.1.
    - When zero, the dsgIfDownChannelListIndex indicates that no TLV 51.1 should be added to the DCD.
- DSG Timeouts
    - The dsgIfDownstreamTable has the index {dsgIfDownTimerIndex}, which (when non-zero) points to the proper set of timer values in the dsgIfTimerTable. Add all four timer values to the DCD (even if some take default values):
        - DSG Initialization Timeout (Tdsg1) (51.2)
        - DSG Operational Timeout (Tdsg2) (51.3)
        - DSG Two-way Retry Timer (Tdsg3) (51.4)
        - DSG One-Way Retry Timer (Tdsg4) (51.5)
- When zero, the dsgIfDownTimerIndex indicates that no DSG Timeout TLVs (51.2, 51.3, 51.4, 51.5) should be added to the DCD.

- DSG Config Specific Parameters (51.43) - The dsgIfDownstreamTable has the index {dsgIfDownVendorParamId}, which points to the proper rows of Vendor-Specific Parameter (VSP) values in the dsgIfVendorParamTable. Use the second index {dsgIfVendorIndex} to walk through the Vendor-Specific Parameters in those rows. The dsgIfVendorValue object is a string of octets inserted immediately following the TLV 43.8 (Vendor ID). The VSP TLV structure is: 43, L, 8, 3, dsgIfVendorOUI, dsgIfVendorValue. The length byte "L" equals the length of dsgIfVendorValue plus 5 bytes. Add a TLV 51.43 to the DCD for each corresponding row.

I.2 DSG Rule (50)

The DCD can contain zero or more DSG Rules, each Rule corresponding to a DSG Tunnel.

Tunnel Group membership:

- The first step in populating the DCD message with DSG Rules is to determine which Tunnel Groups the downstream channel belongs to. The concept of Tunnel Groups is introduced only in the MIB in order to simplify the configuration. Tunnel Groups are not visible in the DCD message, nor are they explicitly linked to other concepts in this specification. A downstream channel may belong to zero or more Tunnel Groups. The dsgIfTunnelGrpToChannelTable encodes the Tunnel Group membership for each downstream channel.
- For each row in dsgIfTunnelGrpToChannelTable where the entry for dsgIfTunnelGrpDsIfIndex matches the downstream index {IfIndex}, the corresponding dsgIfTunnelGrpIndex indicates a Tunnel Group to which this downstream channel belongs. Additionally, each row contains the DSG Rule Priority (dsgIfTunnelGrpRulePriority), and potentially some instances of the DSG Rule Vendor-Specific Parameters (via dsgIfTunnelGrpVendorParamId) that apply to ALL DSG Rules for this Tunnel Group.

Once the Tunnel Group membership is known, the DSG Agent can begin building DSG Rules. Iterating through each Tunnel Group to which the downstream channel belongs (*iteration*), the DSG Agent will add a TLV 50 for each associated DSG Tunnel (i.e., each row in the dsgIfTunnelTable with the appropriate dsgIfTunnelGroupIndex).

To start a DSG Rule, add a DSG Rule TLV (50) to the DCD message. The following paragraphs within this DSG Rule subsection only cover the parsing and assembly of a single DSG Rule within the DCD message. For each DSG Rule created in the DCD, these procedures must be repeated (*iteration*) for each DSG Tunnel in the Tunnel Group, and for each Tunnel Group to which the downstream channel belongs.

- DSG Rule Identifier (50.1) - The Rule Identifiers are unique per DCD message. The Agent assigns the DSG Rule Identifier.
- DSG Rule Priority (50.2) - Using the value of DSG Rule Priority from the dsgIfTunnelGrpToChannelTable, add it to the DSG Rule.
- DSG Client ID (50.4) - The row in the dsgIfTunnelTable contains dsgIfTunnelClientIdListIndex which is used to index into dsgIfClientIdTable to fetch DSG Client IDs for the DSG Rule. Using index {dsgIfClientIdIndex}, add every valid DSG Client ID in the row of dsgClientIdTable to the DSG Rule. These Client IDs may be any or all of the following and should all be added to the DSG Rule.
    - DSG Broadcast (50.4.1)
    - DSG Well-Known MAC Address (50.4.2)
    - CA System ID (50.4.3)
    - Application ID (50.4.4)

      Additionally, the Client ID list may contain index {dsgIfClientVendorParamId} which indexes to a (set of) row(s) in the dsgIfVendorParamTable that will be used to populate the DSG Rule Vendor-Specific Parameters TLV (50.43) below.
- DSG Tunnel Address (50.5) - The row in dsgIfTunnelTable contains dsgIfTunnelMacAddress. Add it to the DSG Rule.

- DSG Classifier Identifier (50.6) - For all rows in the dsgIfClassifierTable that are indexed by this dsgIfTunnelIndex, and that also have dsgIfClassIncludeInDCD set to true, the corresponding index {dsgIfClassId} is added to the DSG Rule via TLV 50.6.
- DSG Rule Vendor-Specific Parameters (50.43) - The DSG Rule could have zero or more lists of vendor-specific parameters (each with one or more VSPs) associated with it. The lists are indicated via a Vendor Param ID index. There are multiple sources for this ID. The first source could be the value of index {dsgIfTunnelGrpVendorParamId} from the dsgIfTunnelGrpToChannelTable. The second source, as mentioned above, could be the value of index {dsgIfClientVendorParamId} in any row in the dsgIfClientTable that is associated with this DSG Rule. This set of Vendor Param IDs is then used as a set if indexes into the dsgIfVendorParamTable. Use the second index {dsgIfVendorIndex} to walk through the individual Vendor-Specific Parameters for each of the Vendor Param IDs in the dsgIfVendorParamTable. The dsgIfVendorValue object is a string of octets inserted immediately following the TLV 43.8 (Vendor ID). The VSP TLV structure is: 43, L, 8, 3, dsgIfVendorOUI, dsgIfVendorValue. The length byte "L" equals the length of dsgIfVendorValue plus 5 bytes. Each row becomes an individual instance of TLV 50.43 that is added to the DCD.

It's worth noting here that the dsgIfTunnelTable contains an object for dsgIfTunnelServiceClass. This object does not contribute data for the DCD message. It's used to provide Quality of Service for the DSG Tunnel via a Named Service Class (and the associated QoS Parameter Set defined in the docsQosServiceClassTable).

I.3 DownStream Packet Classification Encoding (23)

The DCD can contain one or more DSG Classifiers. Once the DSG Rules have been built for the DCD, it is a simple matter of walking through those DSG Rules and, for every instance of the DSG Classifier Identifier (TLV 50.6), add a classifier to the DCD message starting with the Classification Encoding (TLV 23). Each classifier will contain the following sub TLVs:

- Classifier Identifier (23.2) - Add the index {dsgIfClassID} directly to the DSG Rule as the Classifier ID.
- Classifier Rule Priority (23.5) - The row in dsgIfClassifierTable contains dsgIfClassPriority. Add it to the DSG Rule.
- IP Packet Classification Encodings (23.9) - Classifiers may contain one or more of the following TLVs:
    - Source IP Address (23.9.3) - The row in dsgIfClassifierTable contains dsgIfClassSrcIpAddr. Add it to the DSG Rule.
    - Source IP Mask (23.9.4) - The row in dsgIfClassifierTable contains dsgIfClassSrcIpPrefixLength. Add it to the DSG Rule.
    - Destination IP Address (23.9.5) - The row in dsgIfClassifierTable contains dsgIfClassDestIpAddress. Add it to the DSG Rule.
    - Destination TCP/UDP Port Start (23.9.9) - The row in dsgIfClassifierTable contains dsgIfClassDestPortStart. Add it to the DSG Rule.
    - Destination TCP/UDP Port End (23.9.10) - The row in dsgIfClassifierTable contains dsgIfClassDestPortEnd. Add it to the DSG Rule.

Iteration

This completes one 'path' through the MIB as mentioned above. Seek out the notations marked (*iteration*) to complete the assembly of the DCD message from the MIB.

I.4 Order of data entry into the MIB

No one correct method exists for entering data into the Agent MIB. In some cases, an Agent toolset may be provided to build the MIB in a prescribed manner. If no such guidance is provided, consider the following.

Since the MIB has many indexes and an ordered data structure, it may be quicker to enter data in an orderly sequence. The arrows on Figure I–1 show the use of the indexes from table to table. Consider working backwards

against the flow of the arrows as data is entered. The following list of tables illustrates one possible method of entering data in an orderly sequence.

- dsgIfVendorParamTable
- dsgIfChannelListTable
- dsgIfTimerTable
- dsgIfClientIdTable
- docsQosServiceClassTable (see [DOCSIS-OSSIv3.0])
- dsgIfDownstreamTable
- dsgIfTunnelGrpToChannelTable
- dsgIfTunnelTable
- dsgIfClassifierTable

I.5 Building the MIB from a model of communication paths - (example)

Figure I–2 illustrates how to design the MIB given a drawing of data flowing down tunnels. This figure shows only one hypothetical example of a MIB design; it does not represent a generalized data structure like Figure I–1 does. Figure I–2 illustrates the scratch notes that might be drawn up early in the design of the MIB. IP packets filter through the classifiers at the top of Figure I–2 and move down through various tunnels that enter downstream channels at the bottom of the figure.

NOTE: The solid arrows in Figure 1–2 show the flow of data, as indicated by the notation "Data flow >>" in the top left.

Figure 1–2 was drawn using table copied directly from Figure I–1. The top row shows four different classifiers. While these four classifiers all have the same structure from Figure I–1, they can all contain different TLVs for classifying IP packets, as needed for the data flows they control.

Note that various MIB tables have been omitted from Figure 1–2, namely:

docsQosServiceClassTable
dsgIfClientTable
dsgIfVendorParamTable
dsgIfChannelListTable
dsgIfTimerTable

Since these tables are largely used to populate individual tables that are shown in Figure 1–2, they've been left out of the figure to keep the drawing cleaner. When using this graphical method to design a MIB, don't forget to include information from these missing tables.

In this example, we want to design three tunnels as indicated by the three entries in the dsgIfTunnelTable in the second row. The data flow will be as follows:

- IP packets matching the first two classifiers both flow into the first tunnel (on the top left). That tunnel is mapped into two different downstream channels one and two via the dsgIfTunnelGrpToChannelTable.
- IP packets matching the third classifier enter the second tunnel and into the second and third downstream channels.
- IP packets matching the fourth classifier enter the third tunnel and into the second and third downstream channels.
- Summary - Downstream one will contain tunnel 1; downstream two will contain tunnels 1 through 3; and downstream two will contain tunnels 2 and 3.

To build the MIB, populate the boxes in Figure I–2 and collapse the boxes (horizontally) into individual tables of the MIB. Don't forget to build the other tables that were omitted from Figure I–2 (listed above). Use the

recommendations in the section above entitled "Order of data entry into the MIB "to put the data into the MIB." It should make things simpler.

How then to build the MIB objects and tables for this particular example? There may be multiple ways to do this, including the following method. Figure I–3 serves dual purpose. It will show how DCD Rules are found in the graphical representation of a design. The figure also shows values that might be assigned to the indexes to organize the objects within the MIB. The index values referred to in the discussion immediately below can be seen in Figure I–3 contained in brackets, i.e., [index]. The values chosen for the indexes can be assigned in the manner shown, as one of many possibilities.

First, the following five tables in the MIB, omitted from Figure I–2, can be populated with object data to suit the application:

docsQosServiceClassTable
dsgIfClientTable
dsgIfVendorParamTable
dsgIfChannelListTable
dsgIfTimerTable

dsgIfDownStreamChannelTable - This table will have three entries, one for each of the downstreams shown in the bottom of Figure I–2. The indexes can be 1, 2, and 3.

dsgIfTunnelGrpToChannelTable - This table will have four entries:

- The first two objects comprise the first entry, each with a first index of [1] and sub-indexes of [1] and [2] for the first two downstreams. Each downstream will have the index {dsgIfTunnelGrpDsIfIndex} set equal to the IfIndex of the corresponding downstream in dsgIfDownStreamChannelTable.
- The third and fourth objects comprise the second entry, each with a first index of [2] and sub-indexes of [1] and [2] for the last two downstreams. Each downstream will have the index {dsgIfTunnelGrpDsIfIndex} set equal to the IfIndex of the corresponding downstream in dsgIfDownStreamChannelTable.

dsgIfTunnelTable - This table will have 3 entries, one for each tunnel, with indexes [1] through [3].

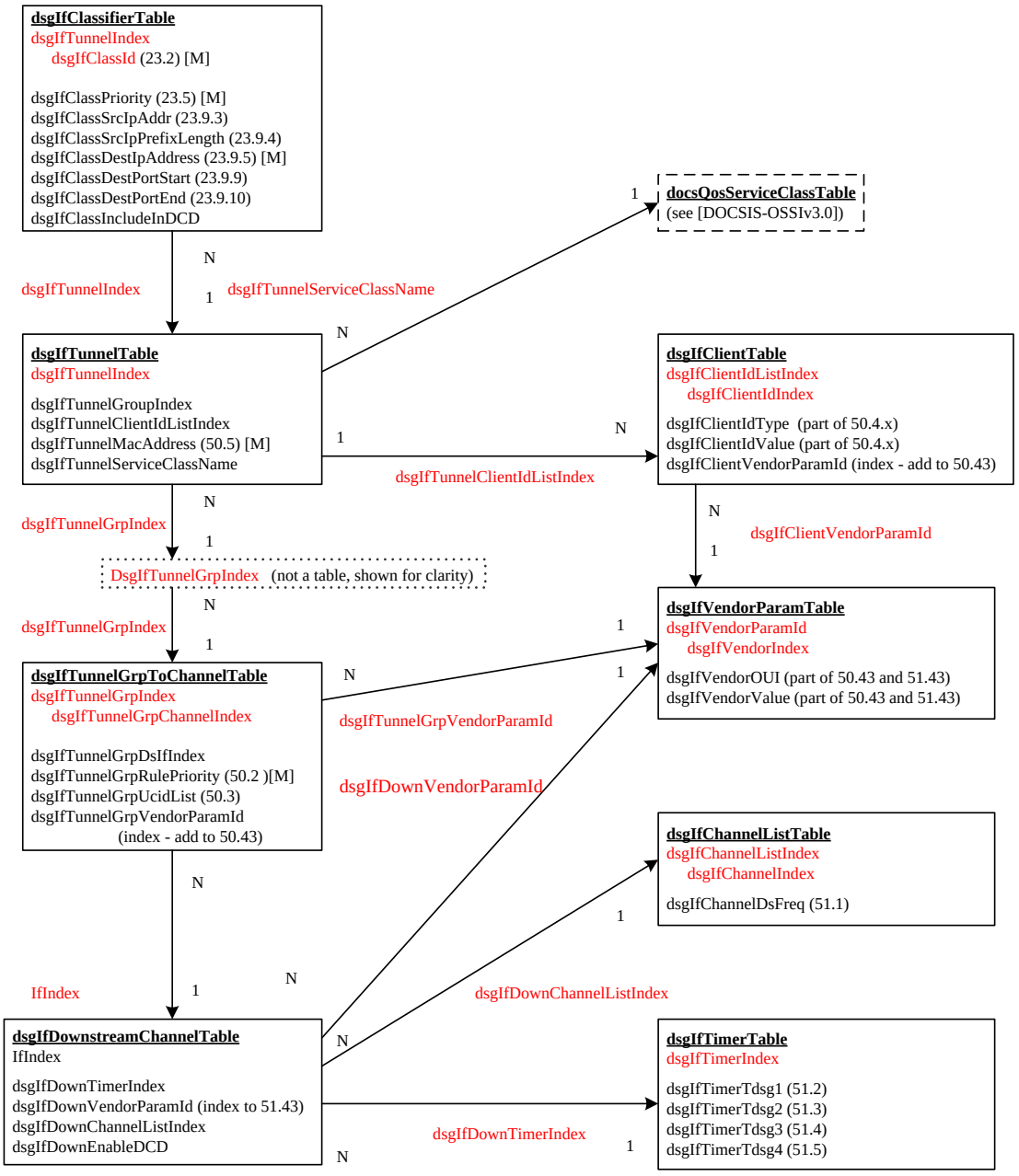
dsgIfClassifierTable - In this example, this table will have 3 entries:

- The first two objects comprise the first entry with a primary index [1] and sub-indexes of [1] and [2] for the two classifiers of tunnel one.
- The second and third entries, with primary indexes [2] and [3], each contain single classifiers and one sub-index. The sub-indexes are the Classifier IDs.

DCD Rules from this example:

Figure I–3, Figure I–4, Figure I–5, and Figure I–6 illustrate the formation of DCD Rules in our example MIB.

- Downstream one, Rule 1 -Figure I–3 shows Rule 1, the only Rule for downstream 1. The dotted line on the left of the figure shows the Rule formation as denoted by "<< Rule 1". Formally speaking, the dotted line that goes up to the dsgIfClassifierTable is not part of the Rule, but shows the association of the classifiers to the Rule.
- Downstream two, Rule 1 - Figure I–4 shows Rule 1 for downstream 2. It gets data from the first tunnel.
- Downstream two, Rule 2 - Figure I–5 shows Rule 2 for downstream 2. It gets data from the second tunnel.
- Downstream two, Rule 3 - Figure I–6 shows Rule 3 for downstream 2. It gets data from the third tunnel.
- Downstream three Rules - There are no figures illustrating the two rules for downstream 3. These two rules are very similar in construct to Rules 2 and 3 of downstream two and are left as an exercise for the reader. Downstream three should get data from the second and third tunnels.



[M] - Means 'Mandatory,' as defined in Table 5–1.

Figure I–1 - MIB Structure

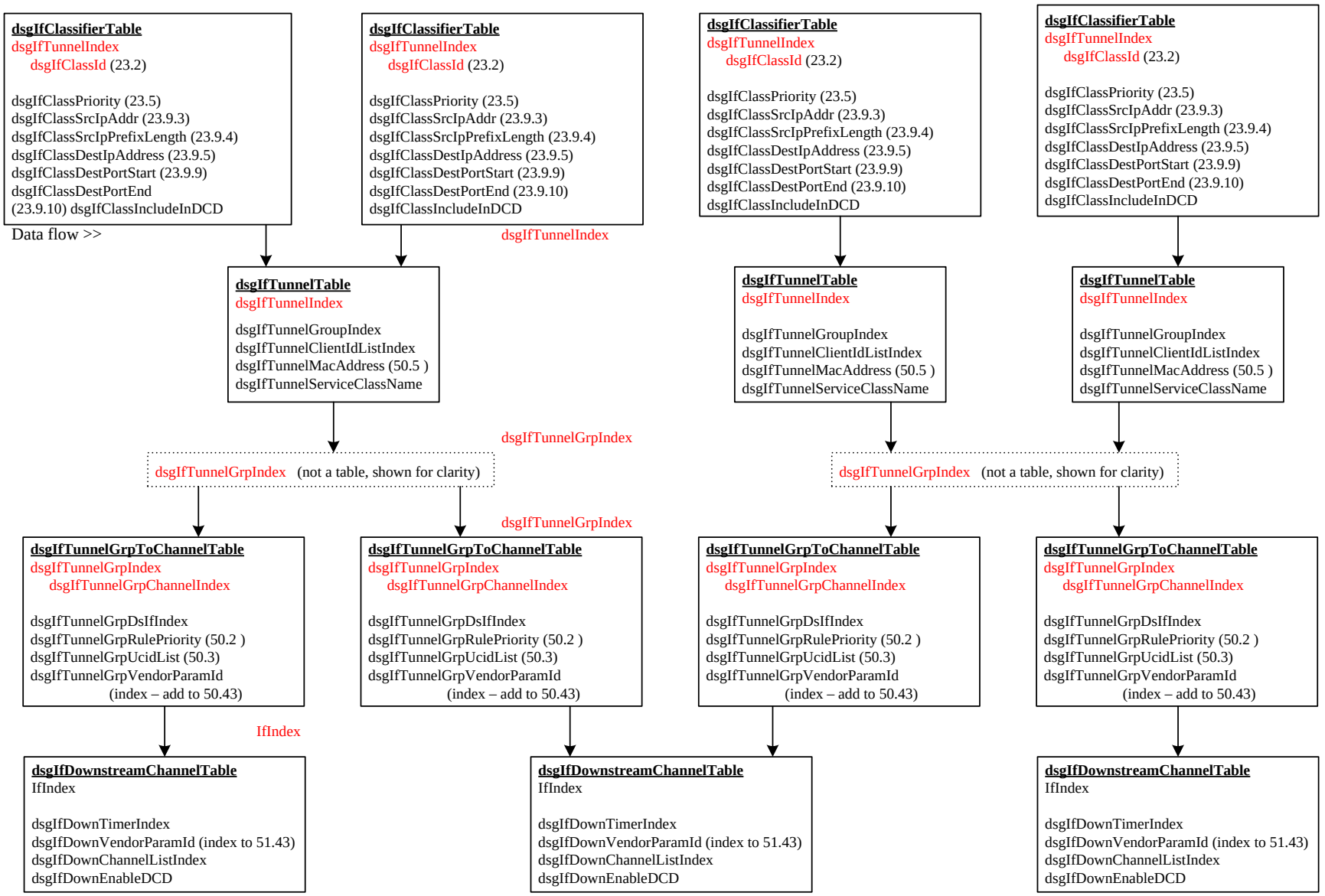


Figure I–2 - Example of Designing 3 Tunnels

Figure I–3 - DS 1, Rule 1

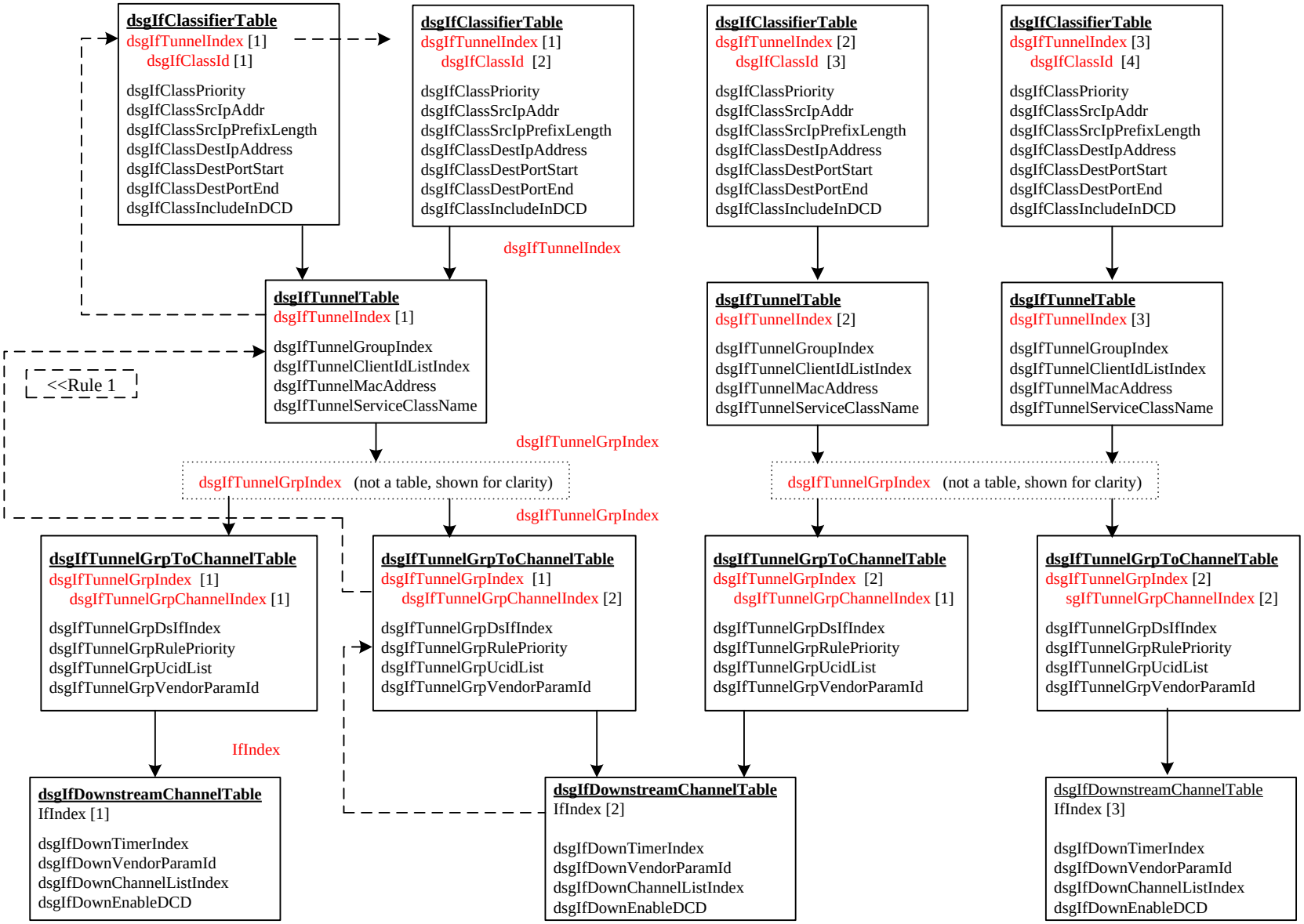


Figure I–4 - DS 2, Rule 2

Figure I–5 - DS 2, Rule 2

Figure I–6 - DS 2, Rule 3