International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.128

(11/2005)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Interactive systems for digital television distribution

Set-top gateway specification for transmission systems for interactive cable television services

ITU-T Recommendation J.128

ITU-T Recommendation J.128

Set-top gateway specification for transmission systems for interactive cable television services

Summary

The DOCSIS Set-top Gateway (DSG) specification introduces additional requirements on a DOCSIS Cable Modem Termination System and DOCSIS Cable Modem (Annex B/J.112 and ITU-T Rec. J.122) 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 server) and the customer premises 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.

Source

ITU-T Recommendation J.128 was approved on 29 November 2005 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

DOCSIS Set-top Gateway (DSG).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

		Page
1	Scope	1
1.1	Introduction and Overview	1
1.2	Purpose of the Recommendation	1
2	References	2
2.1	Normative references	2
2.2	Informative references	2
3	Definitions, Abbreviations, and Conventions	4
3.1	Definitions	4
3.2	Abbreviations	6
3.3	Conventions	7
4	Reference Architecture	7
4.1	DSG basic mode	9
4.2	DSG advanced mode	10
4.3	DSG and IP multicast	10
5	DOCSIS set-top gateway	10
5.1	Assumptions and Constraints	10
5.2	Requirements – General	11
5.3	Requirements – DSG tunnel definition	15
5.4	DSG eCM operation	24
5.5	Security considerations	38
5.6	Interoperability	39
5.7	DSG operation	40
Annex A – DOCSIS set-top gateway agent MIB definition		47
Annex B – DOCSIS set-top gateway set-top device MIB definition		63
Annex C – Format and content for DSG eCM event, SYSLOG, and SNMP trap extensions		71
C.1	DSG eCM event extensions description	71
C.2	DSG DOCSIS events extensions	73
Annex D – Delivery of MPEG-2 sections in the broadcast tunnel		75
D.1	MPEG-2 section encapsulation	75
D.2	Layer 4 multiplexing	76
Appendix I – Parsing the MIB in the DSG agent		77
BIBLIOGRAPHY		90

ITU-T Recommendation J.128

Set-top gateway specification for transmission systems for interactive cable television services

1 Scope

1.1 Introduction and Overview

The DOCSIS Set-top Gateway (DSG) Recommendation 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 premises 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 Recommendation in relation to the data-over-cable reference architecture and the other interface specifications in the DOCSIS Cable Modem series.

Traditionally, the physical transport of this Out-Of-Band messaging has been carried over a variety of mechanisms, including [ITU-T J.184]. This Recommendation 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 Recommendation 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 Recommendation is to specify open protocols, with a preference for existing, well-known and well-accepted standards. This interface Recommendation 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.

1.2 Purpose of the Recommendation

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 Recommendation 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 unidirectional and bidirectional transport of Out-Of-Band messaging over Internet Protocol (IP), between the cable system headend and customer locations, over an all-coaxial or hybrid-fibre/coax (HFC) cable network. This is shown in simplified form in Figure 1-1.

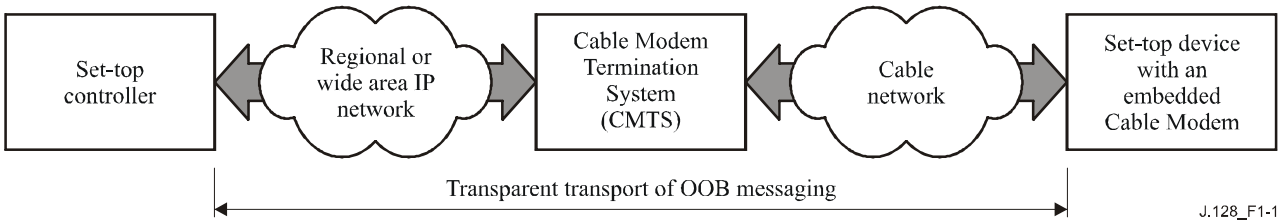


Figure 1-1/J.128 – Transparent out-of-band messaging via DOCSIS

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.

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 signalling.
- 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.

2 References

2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[J.112-B] ITU-T Recommendation J.112 Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification*.

[J.122] ITU-T Recommendation J.122 (2002), *Second-generation transmission systems for interactive cable television services – IP cable modems*.

[DOCSIS-RFI] Refers to both [J.112-B] and [J.122].

2.2 Informative references

[CAS ID] *Conditional Access System Identifier*, CA_system_ID, administered by DVB, www.dvb.org. Table at http://www.dvb.org/index.php?id=174

[ANSI/SCTE 23-3] ANSI/SCTE 23-3 (2003), *DOCSIS 1.1 Part 3: Operations Support System Interface*.

[ANSI/SCTE 79-2] ANSI/SCTE 79-2 (2002), *DOCSIS 2.0 Operations Support System Interface*.

[eDOCSIS] ITU-T Recommendation J.126 (2004), *Embedded Cable Modem device specification*.

[IANA] IANA (2006), *Internet Multicast Addresses*. http://www.iana.org/assignments/multicast-addresses

[IEEE 802.3] IEEE 802.3 (2005), *Local and metropolitan area networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*.

[ITU-T J.94] ITU-T Recommendation J.94 (1998), *Service information for digital broadcasting in cable television systems*.

[ITU-T J.184] ITU-T Recommendation J.184 (2001), *Digital broadband delivery system: Out-of-band transport*.

[GRE 1] IETF RFC 1701 (1994), *Generic Routing Encapsulation (GRE)*. http://www.ietf.org/rfc/rfc1701.txt

[GRE 2] IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE)*. http://www.ietf.org/rfc/rfc2784.txt

[MPEG-SI] ITU-T Recommendation H.222.0 (2000) | ISO/IEC 13818-1: 2000, *Information technology – Generic coding of moving pictures and associated audio information: Systems*.

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

[RFC 1112] IETF RFC 1112 (1989), Host Extensions for IP Multicasting, http://www.ietf.org/rfc/rfc1112.txt

[RFC 2669] IETF RFC 2669 (1999), *DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems*. http://www.ietf.org/rfc/rfc2669.txt

[RFC 3171] IETF RFC 3171 (2001), *IANA Guidelines for IPv4 Multicast Address Assignments*. http://www.ietf.org/rfc/rfc3171.txt

[RFC 3569] IETF RFC 3569 (2003), *An Overview of Source-Specific Multicast (SSM)*. http://www.ietf.org/rfc/rfc3569.txt

[OC-SP-CD-IF] OpenCable TM Common Download Specification – I08, 040831, http://www.opencable.com

[OC-SP-OCAP1.0] OpenCable TM OC-SP-OCAP1.0-I16-050803 for OCAP, http://www.opencable.com

[SCTE-18] SCTE 18 (2002), *Emergency Alert Message for Cable,* http://www.scte.org

3 Definitions, Abbreviations, and Conventions

3.1 Definitions

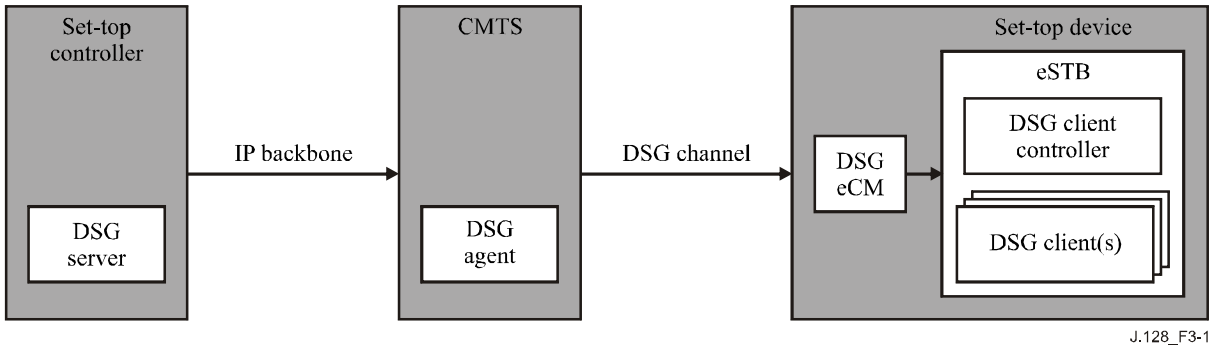


Figure 3-1/J.128 – DSG terminology

This Recommendation defines the following terms:

3.1.1 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 [ITU-T J.94] carried in the Broadcast DSG Tunnel.

3.1.2 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.

3.1.3 DOCSIS Set-Top Gateway (DSG): 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 premises equipment (CPE). The DSG is not intended for the delivery of programming content.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.1.7 DSG basic mode: Operation without the DCD message. Address assignment is static. The DSG Tunnel Address is determined by the DSG Client and learned by the DSG Agent through configuration. This mode provides backwards compatibility with earlier versions of the DSG specification.

3.1.8 DSG channel: Any DOCSIS downstream channel that contains one or more DSG Tunnels.

3.1.9 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.

3.1.10 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.

3.1.11 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.

3.1.12 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 Basic Mode, the DSG Client ID is a 6-byte MAC address. In DSG Advanced Mode, the DSG Client ID may additionally be a 2-byte Application ID, a 2-byte CA_system_ID, or a broadcast ID.

3.1.13 DSG eCM: A DOCSIS Cable Modem that has been embedded into a Set-top Device and includes DSG functionality.

3.1.14 DSG rule: A row entry within the DSG Address Table that assigns a DSG Client ID to a DSG Tunnel Address.

3.1.15 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.

3.1.16 DSG tunnel: A stream of packets sent from the CMTS to the Set-top Terminal. In DSG Basic Mode, a DSG Tunnel is identified solely by its DSG Tunnel Address; all of the DSG Tunnel's packets use the same DSG Tunnel Address and different DSG Tunnels use different DSG Tunnel Addresses. 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: UCID List, Classifier IP addresses, and UDP port numbers.

3.1.17 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.

3.1.18 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.

3.1.19 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.

3.1.20 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 signalling 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.

3.1.21 POD: A detachable device distributed by cable providers that connects to the cable receiver and manages Conditional Access.

3.1.22 QoS parameter set: The set of Service Flow Encodings that describe the Quality of Service attributes of a Service Flow or a Service Class.

3.1.23 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.

3.1.24 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.

3.1.25 set-top device: A cable receiver that contains an embedded Cable Modem for DOCSIS connectivity and an embedded Set-top Box.

3.1.26 two-way: This expression infers that the downstream path and the upstream path are operational.

3.1.27 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 the POD and/or Conditional Access system within the Set-top Device, and has been made known to the MSO for use in configuring the DSG Agent.

3.2 Abbreviations

This Recommendation uses the following abbreviations:

CA	Conditional Access
CM	Cable Modem
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
DCD	Downstream Channel Descriptor
DOCSIS	Data Over Cable Service Interface Specifications
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
HFC	Hybrid Fibre Coax
IP	Internet Protocol
MAC	Media Access Control
MSO	Multiple Service Operator
MTA	Multimedia Terminal Adapter
OOB	Out-Of-Band
SCTE	Society of Cable Telecommunications Engineers
SI	Service Information
SNS	Source Name Sub-Table
TCP	Transmission Control Protocol

UCID Upstream Channel ID

UDP User Datagram Protocol

3.3 Conventions

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

"MUST" This word or the adjective "REQUIRED" means that the item is an absolute requirement of this Recommendation.

"MUST NOT" This phrase means that the item is an absolute prohibition of this Recommendation.

"SHOULD" This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT" This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

"MAY" This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

4 Reference Architecture

The reference architecture for the data-over-cable services and interfaces is shown in Figure 4-1.

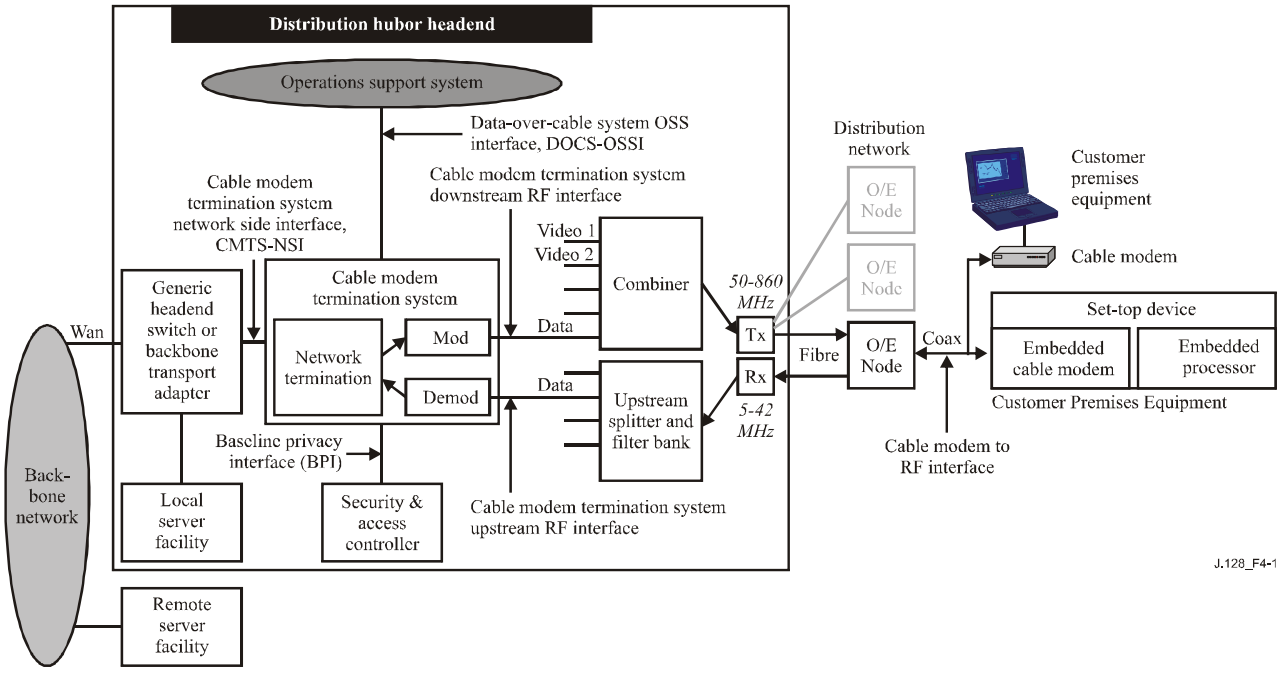


Figure 4-1/J.128 – Data-over-cable reference architecture

The DOCSIS Set-top Gateway architecture is an adaptation of the DOCSIS reference architecture shown in Figure 4-1. Figure 4-2 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.

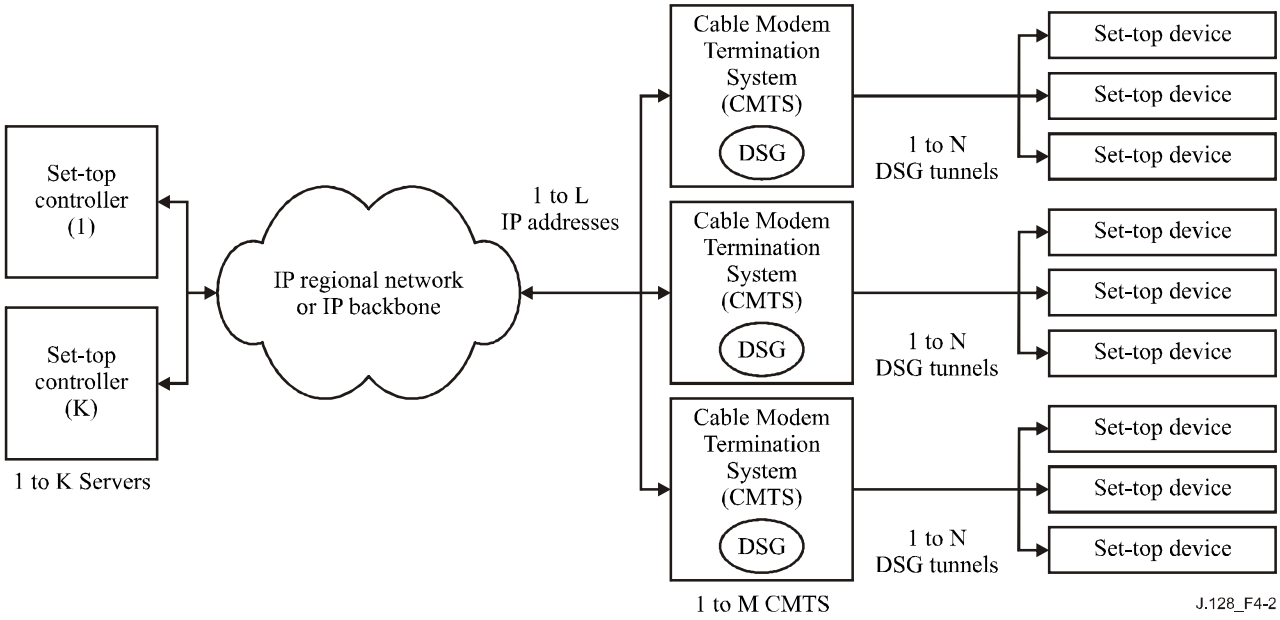


Figure 4-2/J.128 – DOCSIS set-top gateway system physical diagram

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 5.7.9.

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 4-3.

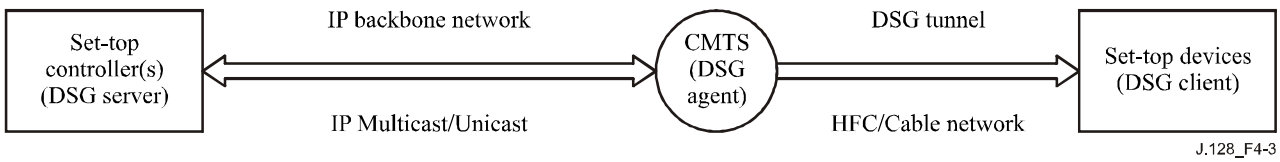


Figure 4-3/J.128 – DOCSIS set-top gateway logical diagram

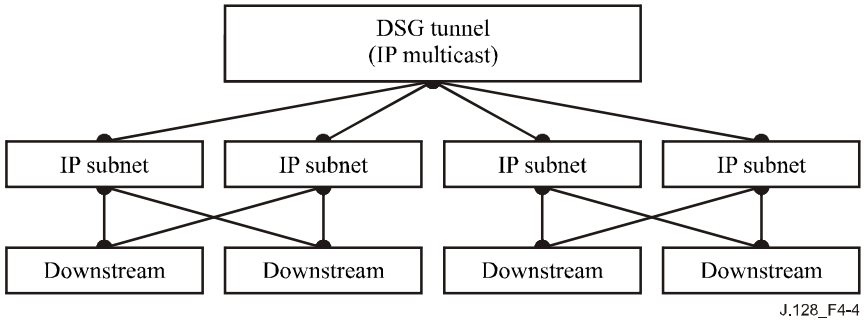


Figure 4-4/J.128 – DSG tunnel within the DSG agent

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 4-4 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

In DSG Basic Mode, the destination MAC address of the DSG Tunnel is set equal to the DSG Client ID which is a multicast (group) MAC Address. There is an early deployment option in the specification which allows operators to use unicast (individual) MAC addresses as well. The DSG Client in the Set-top Device recognizes a DSG Tunnel solely by the uniqueness of the DSG Tunnel Address.

- Multiple IP addresses may use the same DSG Tunnel Address. This allows a many-to-one scenario.
- Each IP address must be resolvable to a single destination MAC address. This is to conform to IP conventions. This disallows a one-to-many scenario.
- The traffic for a single DSG Tunnel may be replicated on one or more DOCSIS downstreams. This group of downstreams may be a subset of the downstreams within one or more IP subnets. No more than one such subset exists for each DSG Tunnel Address.
- The uniqueness of a DSG Tunnel for a particular DSG Client is per IP Subnet.

The following scenario may cause content from the DSG Server to be duplicated on a DOCSIS downstream channel, and should be avoided.

- The same content is sent to multiple IP addresses (unicast or multicast) on the same or different subnets which map to the same DSG Tunnel MAC Address on the same downstream.

A unicast (individual) MAC address was allowed for DSG Basic Mode to prevent a scenario where DOCSIS 1.0 modems that, by default bridge all multicast traffic onto the home network, might become overwhelmed with DSG Tunnel traffic. It should be noted that [RFC 2669] defines MIB

entries for installing address filters in a DOCSIS 1.0 CM that would prevent the forwarding of specific multicast traffic.

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 above conditions for DSG Basic Mode still apply, although there is more flexibility when associating DSG Clients to DSG Tunnels. 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 preferred 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 either another multicast MAC address or a unicast MAC address.

The signalling 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 [ITU-T J.184]. The following clauses detail the requirements and normative behaviour 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 clause 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, and DOCSIS 2.0 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 audiovisual programming (clear, non-scrambled).
  - Digital audiovisual 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 audiovisual programming.

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.

  Informative 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.
- 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.

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 and MUST 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 tunnelling 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 Recommendation.

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.
- 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.

  Informative Note – One application in which rate limiting functionality may be used is an OpenCable™ Advanced Host. The buffer capacity contained in the OpenCable™ Advanced Host is limited and data rates in excess of 2.048 Mbit/s 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 Mbit/s. Note that encapsulation overhead and the size of the packets traversing this interface could reduce the available bandwidth. Refer to [OC-CC-IF] 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 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.

  Informative 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 Recommendation.

- 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.

- The use of an IP Unicast address to transport DSG Tunnel information is intended only to support legacy DSG servers and networks which 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 which 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 tunnelled 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 DSG Agent MUST also be configurable to instead use a unicast (individual) MAC address as the DSG Tunnel Address. It is recommended that the DSG Tunnel Address be a multicast (group) MAC address. The use of a unicast (individual) MAC address is allowed only to support certain legacy DSG Clients. Otherwise, the use of a unicast MAC address is explicitly deprecated.
- A DSG Client operating in DSG Basic Mode will identify and receive a DSG Tunnel based solely on the use of a well-known MAC Address as the DSG Tunnel Address.
- It is recommended that the well-known MAC Address be a multicast (group) Ethernet address. That multicast (group) MAC address may be derived by taking a unicast (individual) MAC address with an OUI [OUI] value set to the OUI value of the Card or Conditional Access system manufacturer, 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].
- Alternatively, the well-known MAC Address may be a unicast (individual) Ethernet address.

  Informative Note – This last provision is to allow for early deployment of DSG, and is not intended for long term use.
- A DSG Client operating in DSG Advanced Mode 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 to use to receive a DSG Tunnel. 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.

5.2.3 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 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.
- 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.
- The DSG eCM MUST support at least 12 simultaneous DSG Classifiers per DSG Tunnel MAC Address, and MUST support at least 32 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 Recommendation 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, the DSG eCM MUST search for the DSG tunnel identifiers based on the DSG operating mode.
    - DSG Basic Mode – In acquiring the appropriate DOCSIS downstream channel, the DSG eCM MUST search for the first DOCSIS channel that contains the well-known Ethernet MAC address(es) reserved by the CA/Card provider.
    - DSG Advanced Mode – In acquiring the appropriate DOCSIS downstream channel, 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 5.4.

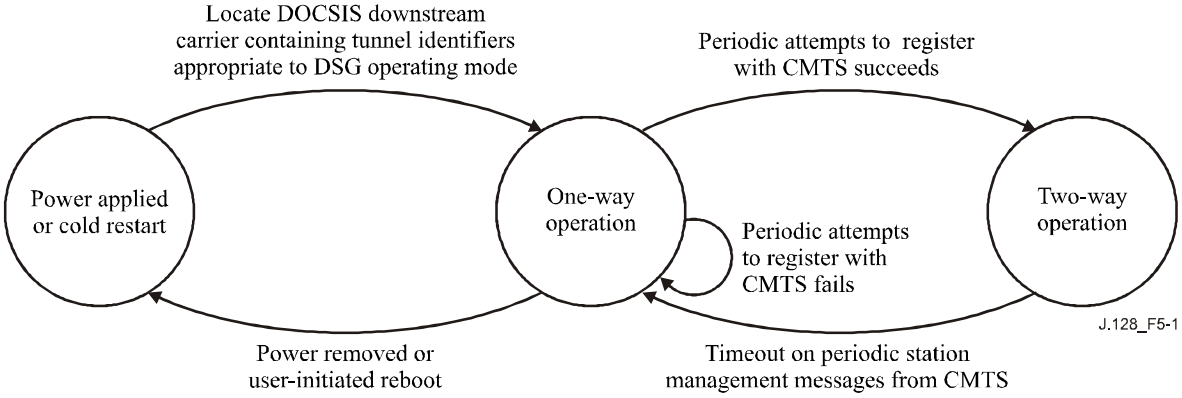


Figure 5-1/J.128 – DSG eCM state transition diagram

5.3 Requirements – DSG tunnel definition

DSG Basic Mode Tunnels use static provisioning based upon an address scheme defined prior to deployment of the Set-top Device. 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 address assigned by the DSG Agent. DSG Advanced Mode also allows the DSG Client to be provided with a downstream filter which will further qualify the DSG Tunnel based upon 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 Basic Mode is able to provide a unique DSG Tunnel per IP subnet for each DSG Client ID. DSG Advanced Mode takes this further by allowing 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 Basic Mode, the content destined for each DSG Client ID is a separate IP flow. 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 demultiplex the stream based upon UDP port number.

The informative text and normative requirements of DSG Basic Mode apply to DSG Advanced Mode, except when those requirements are superseded by requirements of DSG Advanced Mode.

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 and 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 [J.122].

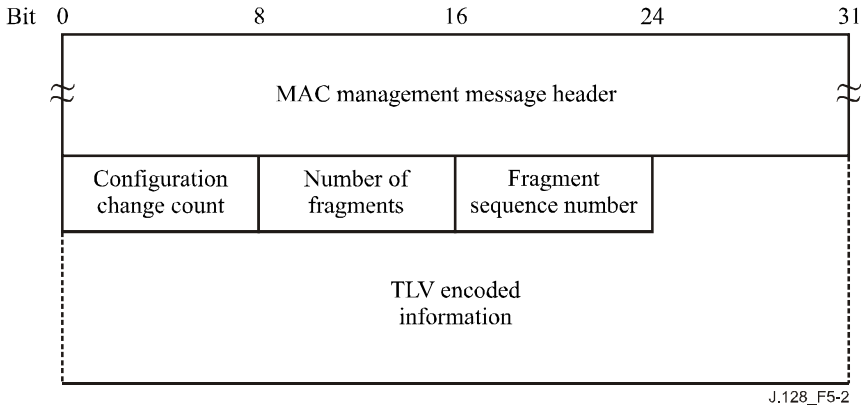


Figure 5-2/J.128 – DCD message fragment structure

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.

Informative Note 1 – 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.

Informative Note 2 – 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 signalling 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 clauses. 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 labelled "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/J.128 – 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		√	O	
50.4	–	DSG Client ID		√	M	
50.4.1	0	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	
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 the clause "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 values of the field specify the matching parameters for the Upstream Channel ID (UCID) for which the DSG Rule applies. If this TLV is omitted, then the DSG Rule applies to all values of UCID, regardless if the UCID is known or unknown by the DSG Client Controller.

Informative Note – If this TLV is included, then an additional DSG Rule would have to be written for a DSG Client Controller residing on a Set-top Device that does not have a UCID available to it because the DSG eCM is operating in one-way mode. This additional DSG Rule would be given a lower DSG Rule Priority, while the DSG Rule with the UCID TLV would be assigned a higher DSG Rule Priority.

UCIDs are 8-bit unsigned integers.

Type	Length	Value
50.3	n	<UCID-1>, <UCID-2>, ... , <UCID-n>

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 AND a match on the UCID List (if present).

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 behaviour 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. If the Length is 0 then the type of data in the tunnel is unspecified. 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.

Informative Note 1 – Client behaviour 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.

Informative Note 2 – 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
50.4.1	2	As defined in Table 5-2

Table 5-2/J.128 – DSG broadcast ID value definitions

Value	Definition
0	Prohibited
1	Contains J.94 [J.94] – Delivery as defined in Annex D
2	Contains EAS [SCTE-18] – Delivery as defined in Annex D
3	Contains OCAP Object Carousel [OC-SP-OCAP1.0]
4	Contains OpenCable Common Download Carousel [OC-SP-CD-IF]
5-55534	Reserved for future use
55535-65535	Reserved for operator specific use

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.

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

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 Subtable (SNS) as defined in [ITU-T J.94]. (Refer to Annex D for information on the delivery of ITU-T Rec. J.94 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.

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 centre frequency of the downstream channel in Hz stored as a 32-bit binary number. The receive frequency MUST be a multiple of 62 500 Hz.

Informative 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. 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.

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. 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.

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. 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.

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. 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.

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 clause "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

5.4.1 DSG modes

The DSG Client Controller, acting on behalf of a Client (or Clients), configures the eCM to operate in either Basic or Advanced Mode depending upon the intrinsic capabilities of the Clients, the Client Controller, the eCM, DCD data, and the local configuration of the STD (not the CM Configuration File). Basic mode makes use of well-known MAC Addresses to define the tunnels. These well-known addresses are provided by the DSG Client Controller and are typically vendor-specific. 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 when operating in one of these modes:

- The DSG eCM MUST NOT operate in any DSG mode unless explicitly instructed to do so by the DSG Client Controller. Upon startup, the DSG Client Controller signals the DSG eCM as to which mode to operate in.
- The DSG eCM MUST be capable of changing DSG mode after startup if instructed to do so by the DSG Client Controller.
- When operating in DSG Advanced mode, the DSG eCM MUST forward the unaltered contents of each DCD fragment that comprises the first DCD message received to the DSG Client Controller.
- When operating in DSG Advanced mode, 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.
- When operating in DSG Advanced mode, 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.
- When operating in DSG Advanced mode, 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 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 Figures 5-3 through 5-10 (and described in 5.4.3), and the second, "DSG Operation", is covered by the state transition diagram in Figure 5-11 (and described in 5.4.4). 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 clauses.

5.4.2.1 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;
- Entering One-way Mode.

5.4.2.2 Messages sent/received by "DSG operation"

Inputs from the DSG Client Controller:

- Start DSG Basic Mode (Filter these MAC Addresses);
- Start DSG Advanced Mode;
- Filter these MAC Addresses and Classifiers (Advanced Mode only);
- Not Valid. Hunt for new DSG Channel.

Outputs to DSG Client Controller:

- DCD Message information.

5.4.3 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 DSG eCM initialization sequence is based on the CM initialization sequence defined in the "Cable Modem Initialization" clause of [DOCSIS-RFI]. The differences from the DOCSIS standard are detailed in the following clauses 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 Basic mode, the DSG eCM MUST use the default timer values as specified in clauses 5.3.1.3.2 through 5.3.1.3.5. When operating in DSG Advanced mode, the DSG eCM MUST use the default timer values as specified in clauses 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 to 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 clauses, 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 process by collecting UCD messages.

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, one containing DSG packets, is acquired.

The DSG Client Controller needs to be made aware of DCC operations so that 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 Client Controller.
- When the CM sends a "DCC-RSP (Arrive)" message, the eCM MUST also send a "2-Way OK, UCID <P1>" (where P1 = Upstream Channel ID) message to the Client Controller.

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

5.4.3.1 DSG eCM initialization overview

Figure 5-3 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 clauses.

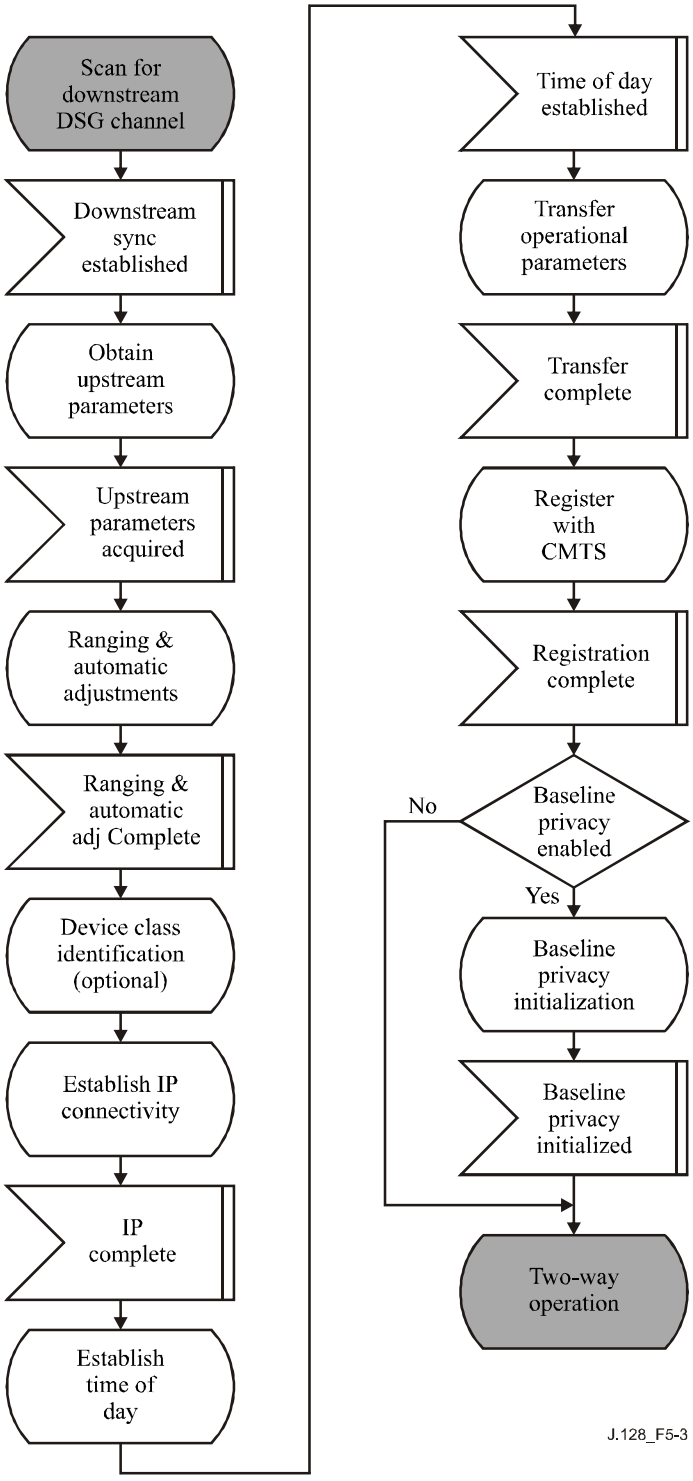


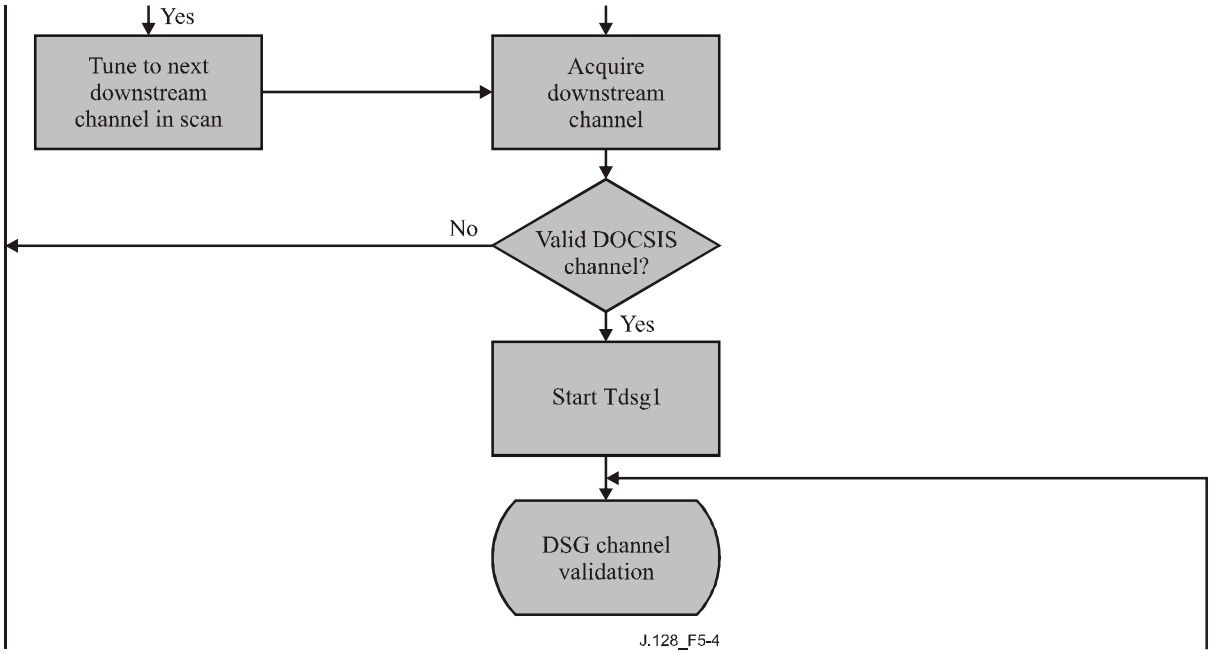
Figure 5-3/J.128 – DSG eCM initialization overview

5.4.3.2 DSG eCM scan for downstream channel

This clause corresponds to the "Scanning and Synchronization to Downstream" clause in [DOCSIS-RFI], although Figure 5-4 does not have a corresponding figure in either Recommendation. 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 Basic or Advanced at startup before scanning for a downstream channel. If the DSG eCM is set to Basic Mode, then it MUST also receive a list of one or more well-known MAC Addresses from the DSG Client Controller before beginning the downstream scan.

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 (TLV1) and the Downstream Channel List (TLV41) as described in [DOCSIS-RFI] still apply.



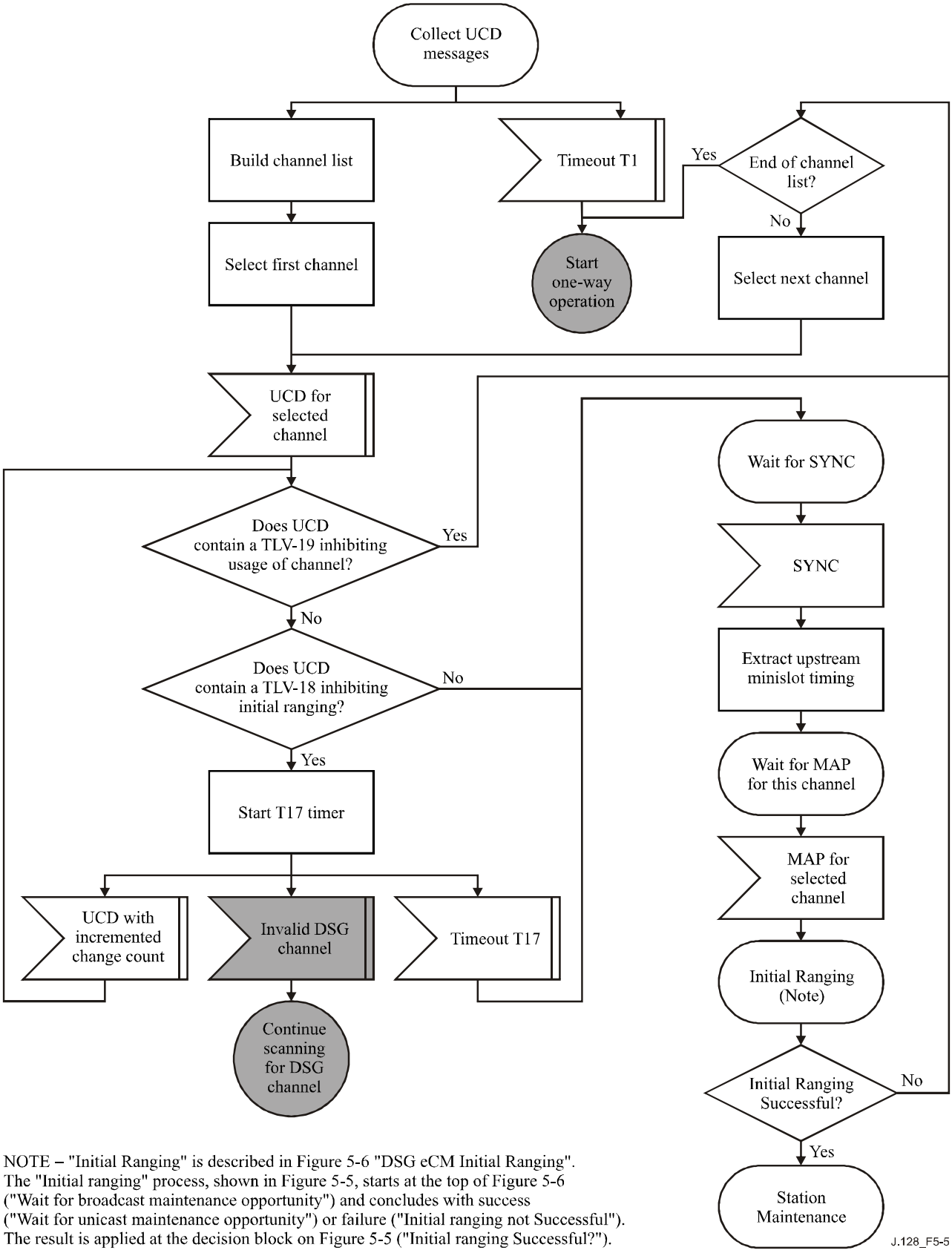
NOTE – Per 11.2.1 of [DOCSIS RFIv2.0].

Figure 5-4/J.128 – DSG eCM scan for downstream DSG channel

5.4.3.3 DSG eCM obtain upstream parameters

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

It should be noted that a DSG modem that does not comply with TLV19 [DOCSIS-RFIv2.0], will move to One-way 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.

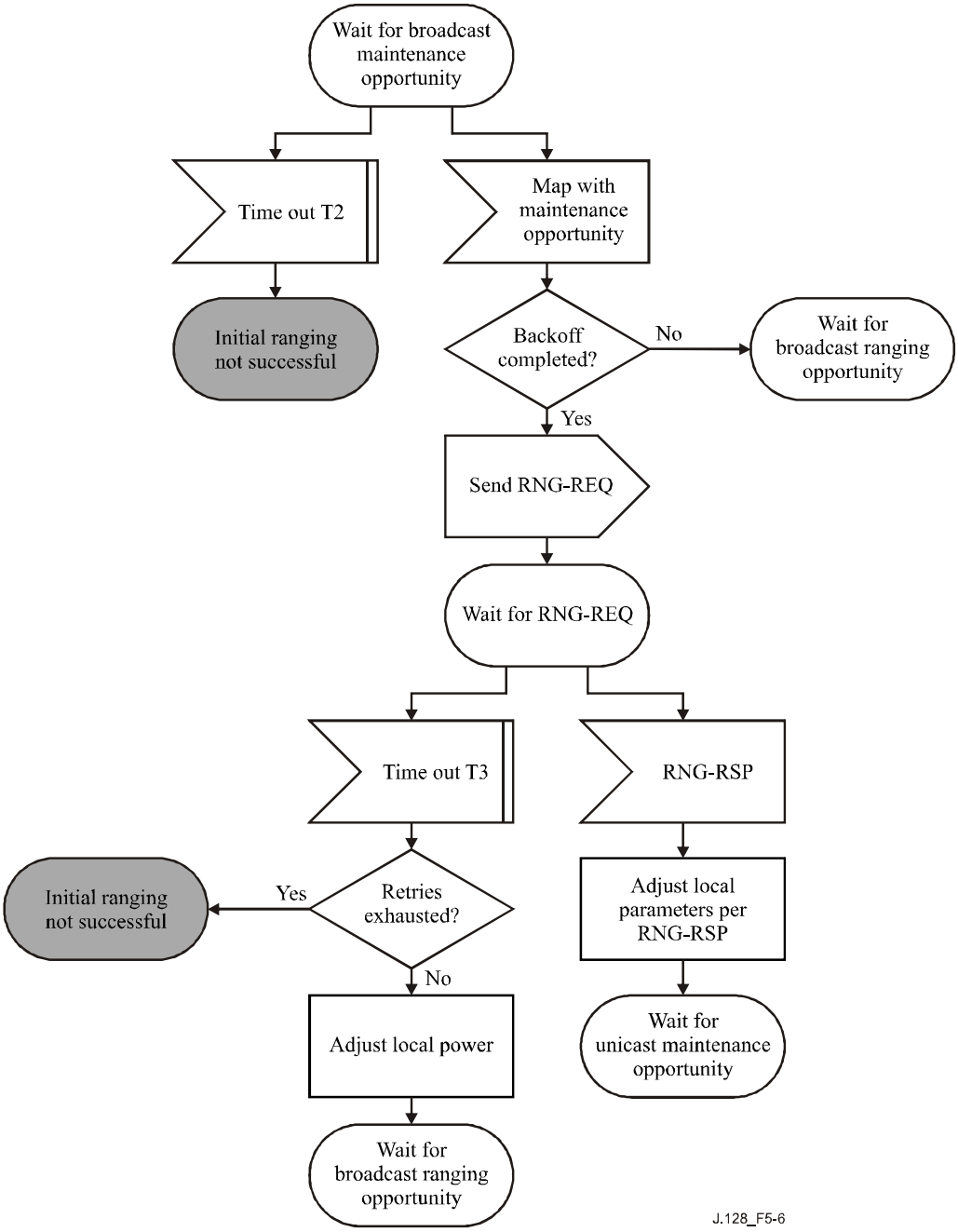


NOTE – "Initial Ranging" is described in Figure 5-6 "DSG eCM Initial Ranging". The "Initial ranging" process, shown in Figure 5-5, starts at the top of Figure 5-6 ("Wait for broadcast maintenance opportunity") and concludes with success ("Wait for unicast maintenance opportunity") or failure ("Initial ranging not Successful"). The result is applied at the decision block on Figure 5-5 ("Initial ranging Successful?").

Figure 5-5/J.128 – DSG eCM obtaining upstream parameters

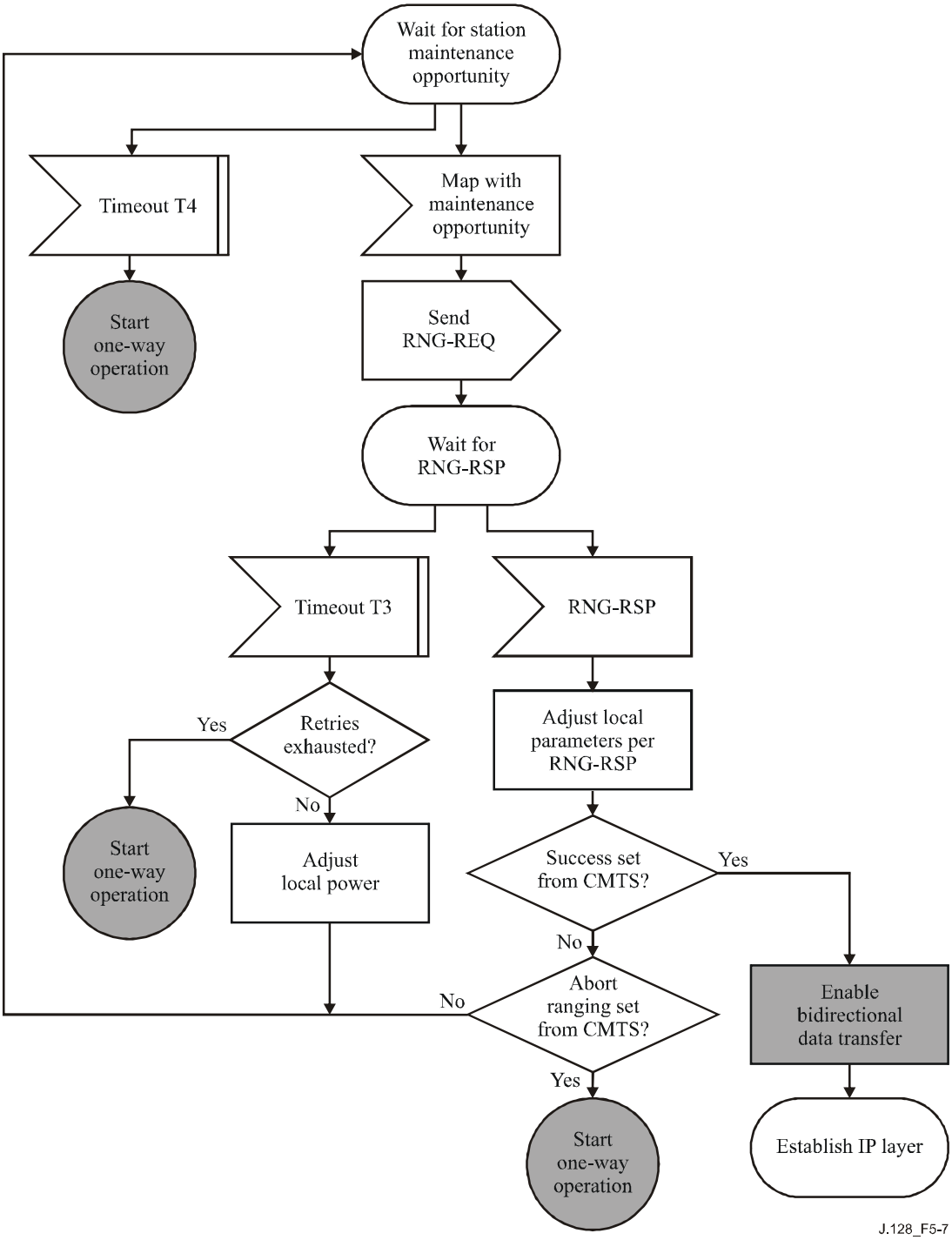
5.4.3.4 DSG eCM ranging and automatic adjustments

This clause corresponds to the "Ranging and Automatic Adjustments" clause 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 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 MUST attempt initial ranging on every suitable upstream channel, before moving to the next available downstream channel.

Figure 5-6/J.128 – DSG eCM initial ranging



NOTE – The path between this point and Figure 5-8 is shown in Figure 5-3, namely from 'Establish IP Connectivity' through 'Establish Time of Day'.

Figure 5-7/J.128 – DSG eCM unicast station maintenance ranging

5.4.3.5 DSG eCM registration

This clause corresponds to the "Registration" clause 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 Operation. There is also a notification to the DSG Client Controller when Two-way Operation has been established.

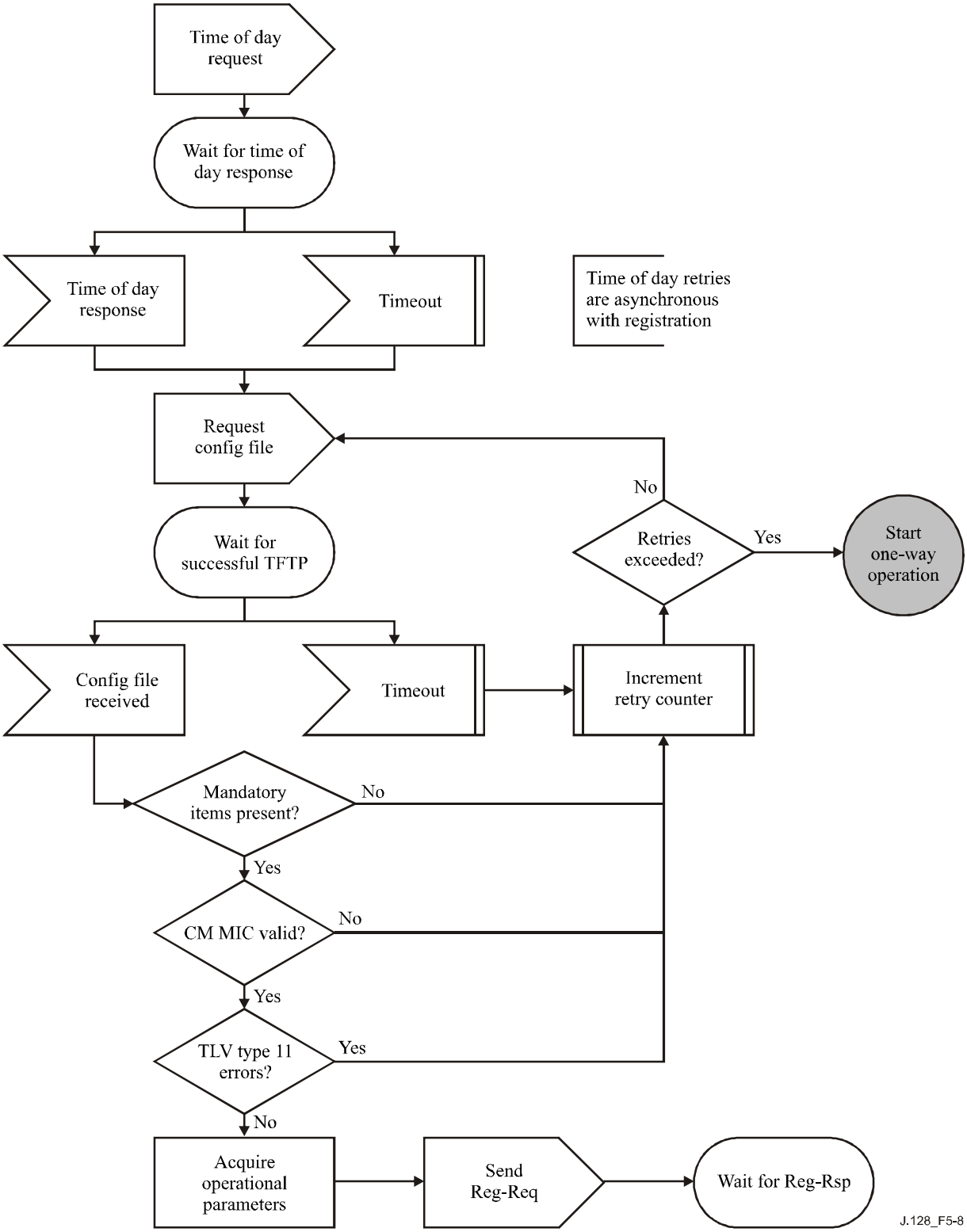


Figure 5-8/J.128 – DSG eCM registration

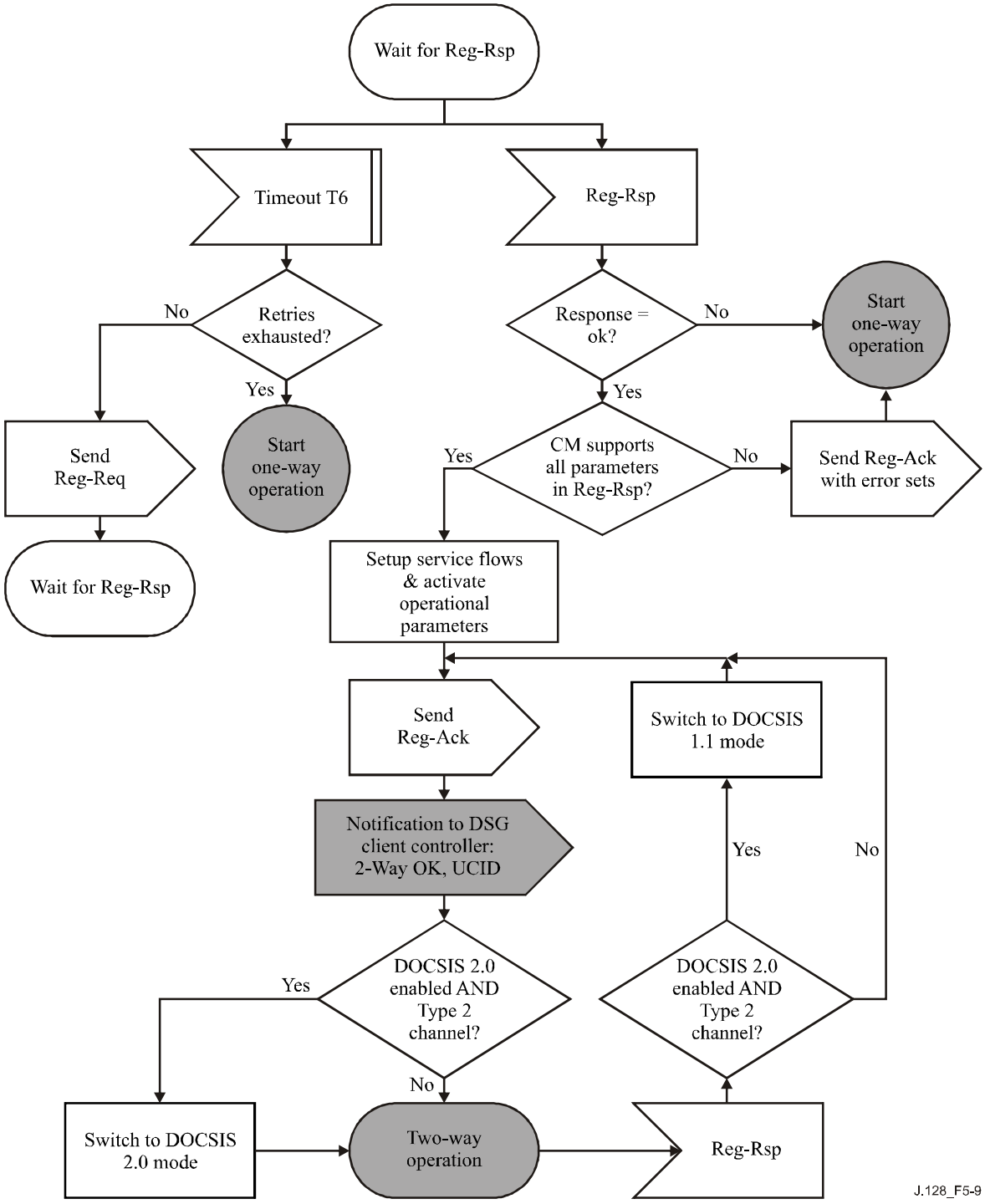


Figure 5-9/J.128 – DSG eCM wait for registration response

5.4.3.6 DSG eCM operation

This clause corresponds in part to the "Periodic Signal Level Adjustment" clause in [DOCSIS-RFI], although it also introduces several completely new concepts. The differences include One-way Operation, Two-way Operation Disabled, and the reception of a Invalid DSG Channel notification.

When the DSG eCM enters one-way operation as a consequence of any of the timeouts or error conditions indicated in the preceding clauses, it MUST remain tuned to and process DSG traffic on the DOCSIS downstream channel. If the eCM enters one-way 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.

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.

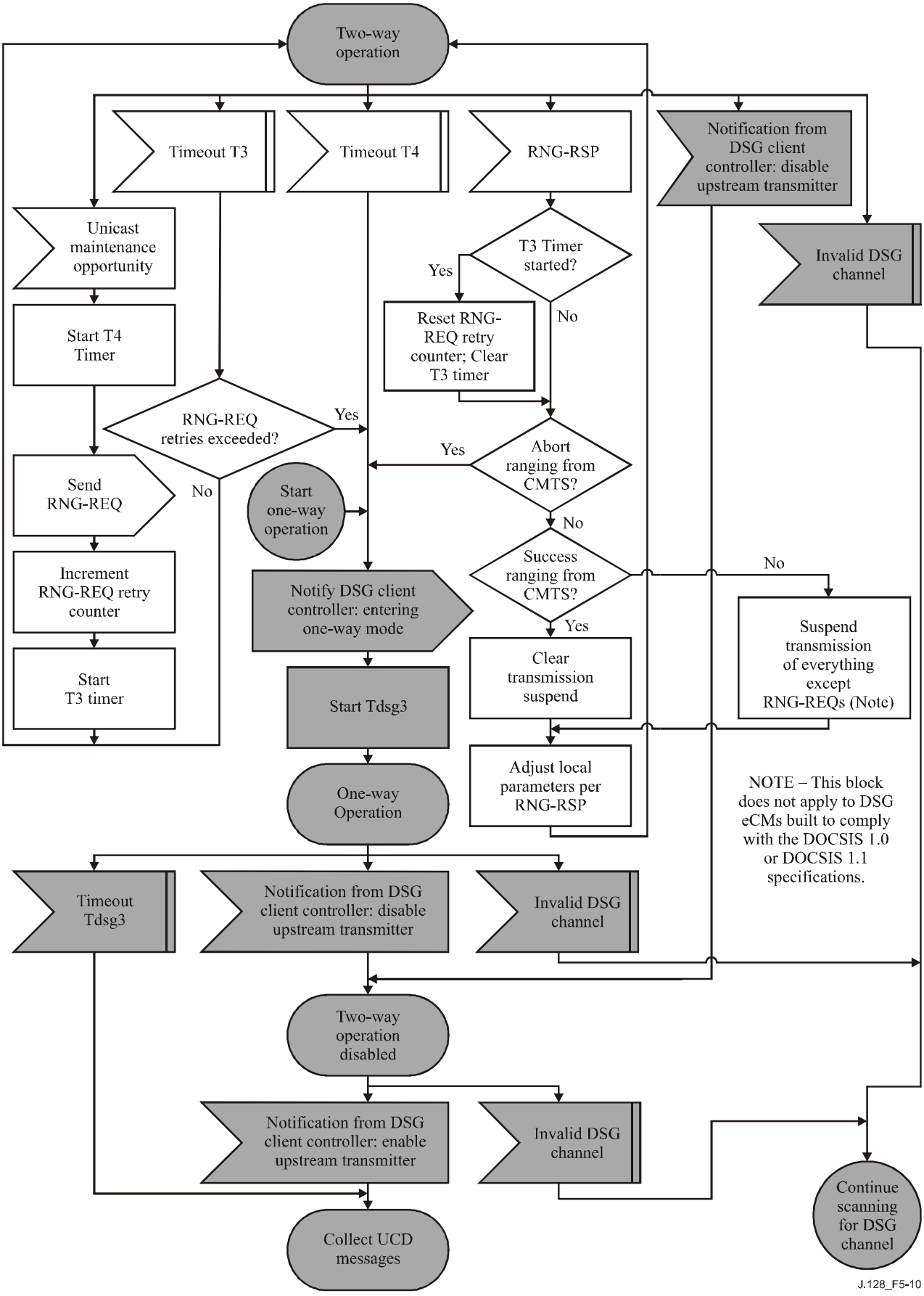


Figure 5-10/J.128 – DSG eCM operation

5.4.4 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.

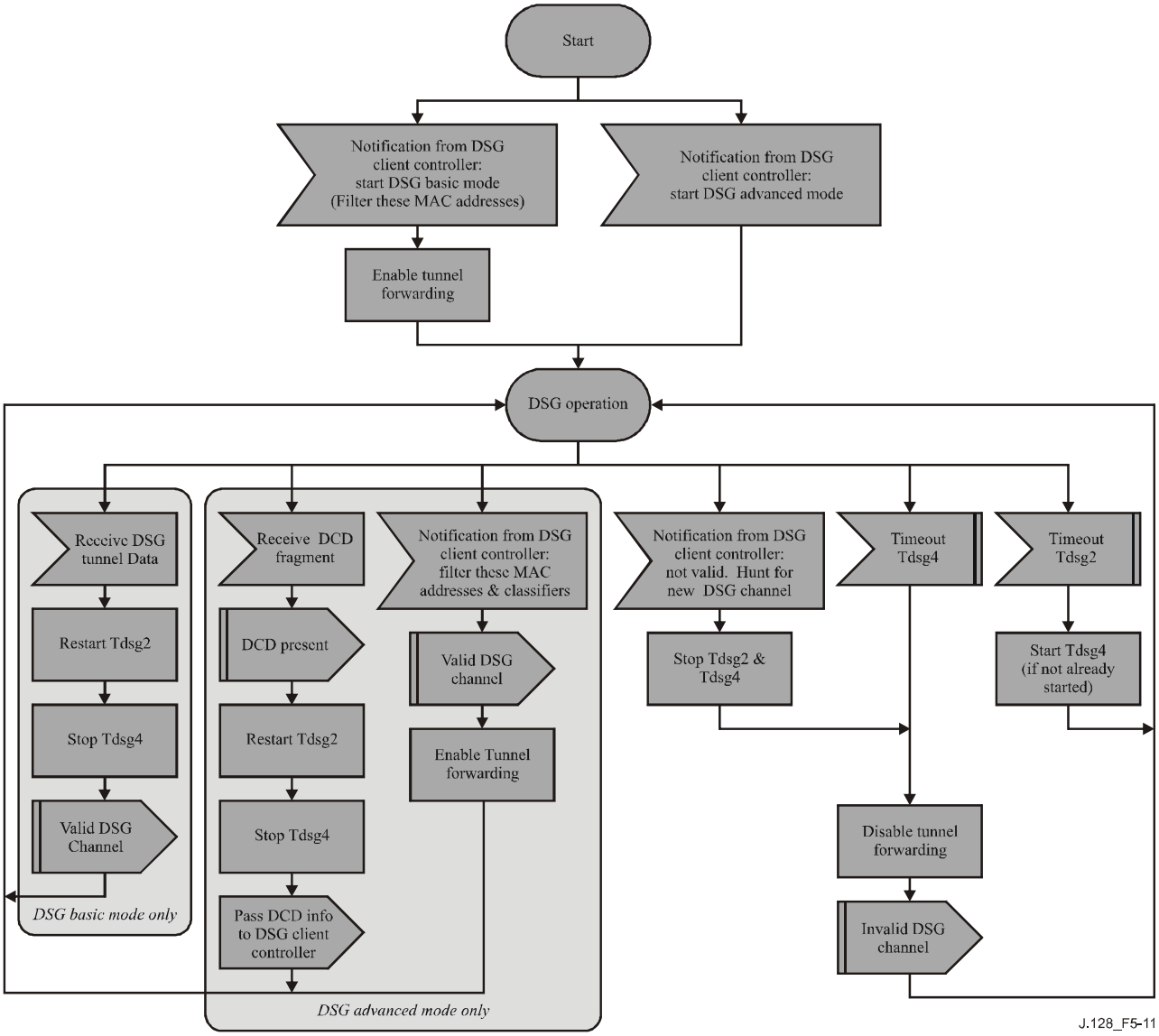


Figure 5-11/J.128 – DSG operation

5.4.4.1 DSG basic mode tunnel acquisition and handling

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

- While scanning, the DSG eCM MUST determine the appropriateness of the current downstream channel by using the list of well-known MAC Addresses that it has acquired from the DSG Client Controller. The DSG eCM MUST consider a downstream channel to be valid if it sees a DSG Tunnel packet which matches any one of these well-known MAC addresses.

- Once an appropriate downstream channel has been located, the DSG eCM MUST begin passing 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 pass DSG Tunnel data to the DSG Client(s) that matches these MAC addresses.
- The DSG eCM MUST dynamically replace the list of well-known MAC Addresses if instructed to do so by the DSG Client Controller without re-initializing.

5.4.4.2 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 pass DSG Tunnel data to the DSG Client(s) until the appropriate filters have been set, based upon information received from the DSG Client Controller.
- Once these filters have been set, the DSG eCM MUST begin passing 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 pass 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.
- After becoming operational in two-way mode, the DSG eCM MUST notify the DSG Client Controller of the UCID the DSG eCM is using.
- 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. For example, UCID-based filters are not removed by the transition from Two-Way to One-Way operation.

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 includes 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.

In DSG Basic Mode, the reserved 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 Basic Mode, the DSG Client receives DSG Tunnels based solely upon the DSG Tunnel Address. This does not provide protection against unauthorized senders.

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 signalling, 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.

Informative Note 1 – This provision is to prevent a security threat in which an external entity sends in a packet or signalling 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.

Informative Note 2 – 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 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, and 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].

Informative Note 1 – 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 signalling protocols for setting up the session. The DSG Tunnel uses the DCD Message, while the standard multicast session over DOCSIS would be using IGMP.

Informative Note 2 – By default, DOCSIS 1.0 cable modems forward multicast traffic onto the home network. This can be avoided by using a unicast (individual) DSG Tunnel Address or by programming the downstream address filters in the CM (through SNMP) to reject the DSG Multicast traffic. Refer to [RFC 2669] for details on the CM filters.

5.6.2 DSG basic mode and DSG advanced mode

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

In 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 STDs operating in 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-HOST-CFR].

5.7 DSG operation

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

5.7.1 DSG basic mode tunnels

The DCD message is ignored by DSG eCMs that are operating in DSG Basic Mode. The DSG eCM would identify and receive the DSG Tunnel, based upon the well-known MAC Address which it received from the DSG Client Controller.

5.7.2 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 5-12, Example #1.

5.7.3 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 usually a multicast (group) MAC address, but may be a unicast MAC address to support legacy Set-top Devices which do not support the DCD message. 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 5-12, Example #1.

5.7.4 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 DSG Servers are going to the same DSG Client.

Both the DSG Basic Mode and the DSG Advanced Mode allow multiple IP flows from the Backbone to merge into one DSG Tunnel. In DSG Advanced Mode, 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 5-12, Example #5.

5.7.5 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. In DSG Basic Mode, one DSG Tunnel would be required for each DSG Client. This would mean duplicating content both on the IP backbone and on the DOCSIS downstream.

This is demonstrated in Figure 5-12, Example #5.

5.7.6 Regionalization

An operator may want to send different content to different Set-top Devices from the same manufacturer on different HFC network segments. This can be accomplished in a variety of ways.

In DSG Basic Mode, this requires placing the different DSG Tunnels on different IP subnets. This is because packets are switched between downstreams within an IP subnet, based upon their destination MAC address. Thus, it is impossible to have different DSG Tunnels with the same DSG

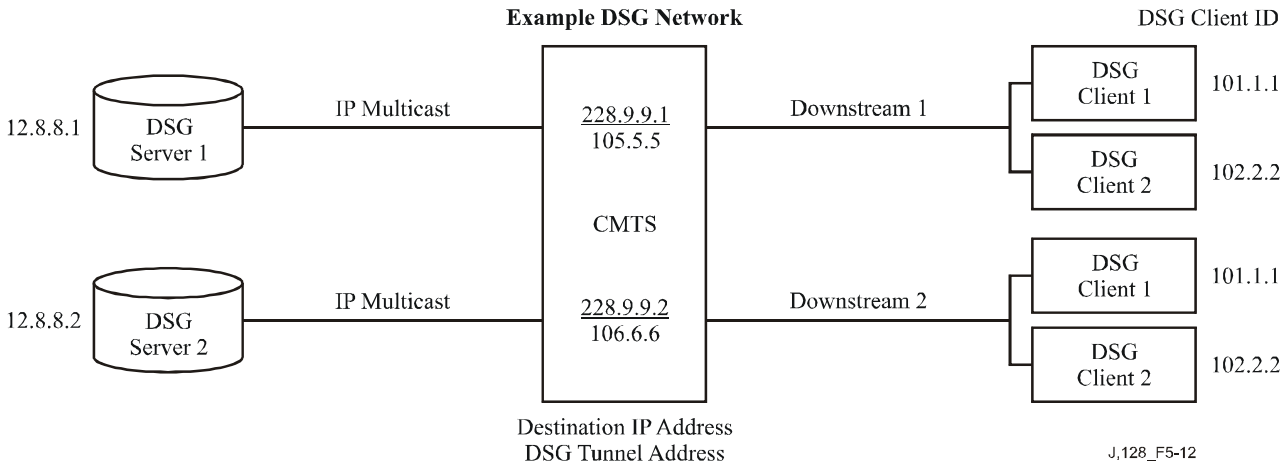
Tunnel Address within an IP subnet with DSG Basic Mode. Since, in practice, IP subnets tend to span an entire CMTS, regionalization in DSG Basic Mode also tends to be done per CMTS.

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 5-12, Example #2.

On a two-way HFC plant, the DSG Client Controller can use the Upstream Channel ID (UCID) for further granularity. One approach is to write a separate DSG Rule for each set of UCIDs that are within a region. Each DSG Rule would be for a separate DSG Tunnel. In this scenario, multiple DSG Rules would have the same DSG Client ID, but a different DSG Tunnel Address and a different UCID List. This is demonstrated in Figure 5-12, Example #3.

A second approach which would use fewer DSG Tunnels is for the DSG Server to place the regionalized content onto different destination UDP ports. Each destination UDP port would then be associated with a different set of UCIDs. In this scenario, multiple DSG Rules would have the same DSG Client ID and the same DSG Tunnel Address, but a different UCID List.

In both approaches, at least one DSG Rule would include the default DSG Tunnel for DSG eCMs which could not register and obtain a UCID. This rule would have a lower Rule Priority than the other DSG Rules.



NOTE – 105.5.5 is short for 0105.0005.0005.

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	101.2.2
DSG Tunnel Address	106.6.6

Example # 3: Regionalization per Upstream (US)

DSG Rule (DS1)	
DSG Rule ID	1
DSG Client ID	101.1.1
DSG UCID List	1, 2, 3
DSG Tunnel Address	105.5.5

DSG Rule (DS1)	
DSG Rule ID	2
DSG Client ID	101.1.1
DSG UCID List	4,5,6
DSG Tunnel Address	106.6.6

Figure 5-12/J.128 – 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 5-12/J.128 – Example DSG configurations

5.7.7 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.

In DSG Basic mode, a different IP stream is required from the DSG Server to the DSG Agent for each DSG Tunnel. 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. A variant of this feature would be to include the UCID List in the DSG Rule to steer content from different UDP ports to different regions.

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 that it forwards the correct content, based upon UDP Port, to the correct destination within the Set-top Device.

5.7.8 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 of whether or not 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.

5.7.9 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 4 operational scenarios, each of which have different solutions. These solutions are described in Table 5-3. Note that tunnelling 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/J.128 – Support strategies for legacy network equipment

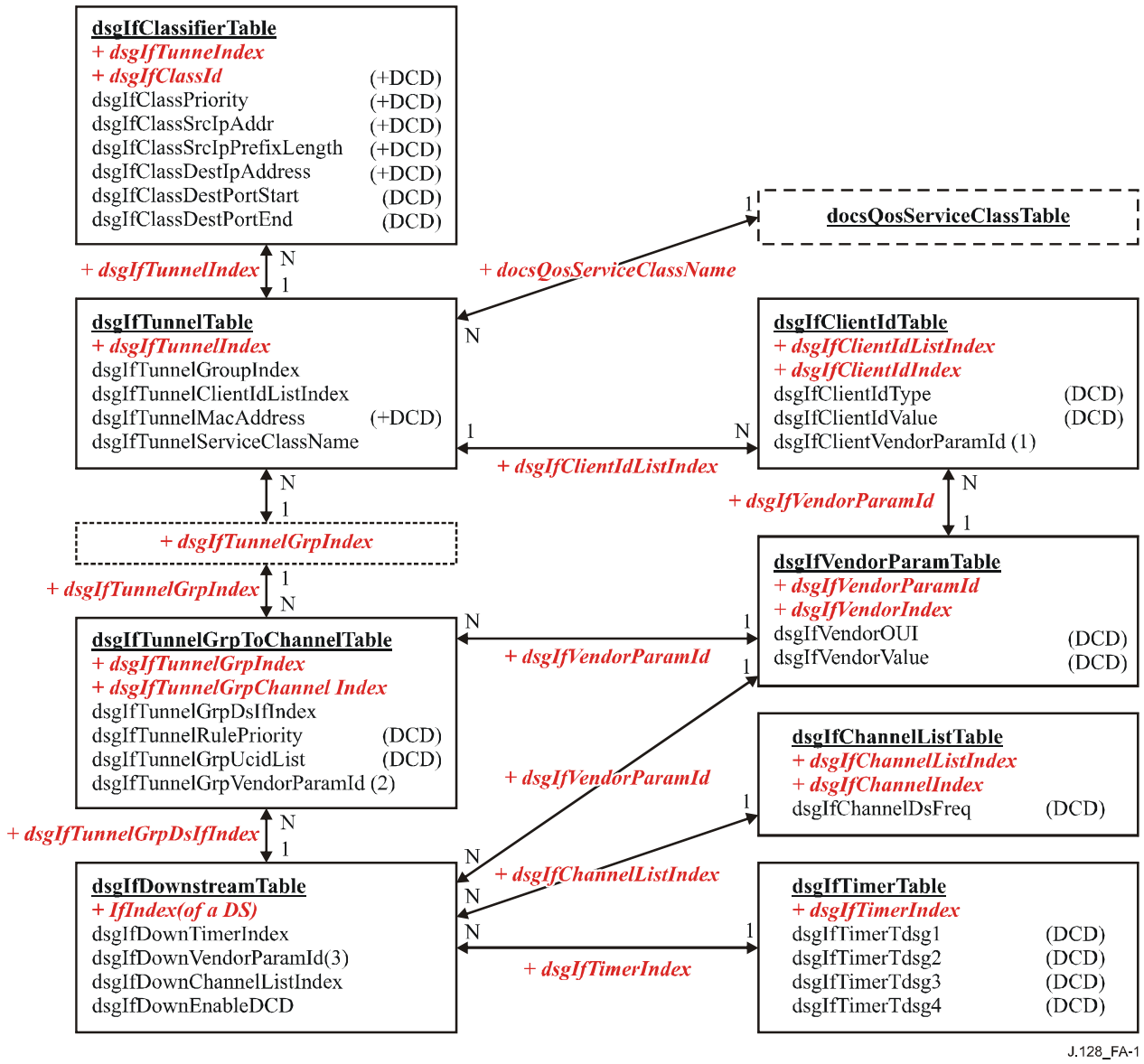
DSG server capability	Network capability	Strategy
Multicast	Multicast	The DSG Server generates an IP Multicast packet. The IP network delivers an IP Multicast packet to the CMTS. The CMTS passes the packet to the DSG Agent. This solution is the preferred solution.
Multicast	Unicast	The DSG Server tunnels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

5.7.10 DCC considerations (Informative)

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, and will eventually begin to hunt for a new downstream, a process that could take a significant period of time. Similarly, if DCC is implemented and used to change upstream channels and the UCID List Rule parameter is being used, then the operator needs to ensure that the US channel the CM is being moved to is a part of that UCID List. If not, then the Set-top Device may begin receiving a different DSG Tunnel or have to search for a new DSG channel altogether. In all cases, if a DSG eCM is subject to DCC operations, then care must be taken to provide the proper provisioning and configuration of the DSG Agent and the DSG eCM.

Annex A

DOCSIS set-top gateway agent MIB definition



NOTE – DCD = Sent to DSG Client via DCD
+ DCD = Applies to DSG Agent & sent to DSG Client via DCD

DSG Rule ={Rule ID, Client IDs,VendorParams(1), Destination MAC Address, Rule Priority, UCID List, VendorParams(2), Classifier IDs}
DCD={Classifier(s), DSG Rule(s),Timers, DSG Channel List,VendorParams(3)}

No actual table, just shown for clarity

Existing table from another MIB

Figure A.1/J.128 – DSG MIB module objects relationships

```
DSG-IF-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32,
    Integer32
        FROM SNMPv2-SMI
    TruthValue,
    MacAddress,
    RowStatus
        FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE
        FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetAddressPrefixLength,
    InetPortNumber
        FROM INET-ADDRESS-MIB
    SnmpAdminString
        FROM SNMP-FRAMEWORK-MIB
    InterfaceIndex,
    ifIndex
        FROM IF-MIB
    clabProjDocsis
        FROM CLAB-DEF-MIB;

dsgIfMIB MODULE-IDENTITY
    LAST-UPDATED   "200411240000Z" -- November 24, 2004
    ORGANIZATION   "Cable Television Laboratories, Inc"
    CONTACT-INFO
            "Postal: Cable Television Laboratories, Inc.
                     858 Coal Creek Circle
                     Louisville, Colorado 80027
                     U.S.A.
            Phone : +1 303-661-9100
            Fax   : +1 303-661-9199
            E-mail: "
    DESCRIPTION
            "This is the MIB Module for the DOCSIS Set-top Gateway
            (DSG). The DSG provides a one-way IP datagram transport
            for Out-Of-Band (OOB) messaging to cable set-top clients.
            The one-way IP datagram transport is called a DSG Tunnel.

            A DSG Tunnel carrying either a broadcast, unicast or
            multicast IP datagram stream originating at the DOCSIS
            Set-top Gateway and carrying Out-Of-Band messages intended
            for set-top clients. It is carried over one or more
            downstream DOCSIS channels.

            Multiple DSG tunnels may exist on a single downstream
            DOCSIS channel."
    REVISION "200408040000Z"
    DESCRIPTION
            "Initial revision, published as part of DOCSIS Set-top
             Gateway Specification."
    ::= { clabProjDocsis 3 }

dsgIfMIBNotifications    OBJECT IDENTIFIER ::= { dsgIfMIB 0 }
dsgIfMIBObjects          OBJECT IDENTIFIER ::= { dsgIfMIB 1 }
dsgIfMIBConformance      OBJECT IDENTIFIER ::= { dsgIfMIB 2 }

dsgIfClassifier          OBJECT IDENTIFIER ::= { dsgIfMIBObjects 1 }
dsgIfTunnel              OBJECT IDENTIFIER ::= { dsgIfMIBObjects 2 }
dsgIfTunnelGrpToChannel  OBJECT IDENTIFIER ::= { dsgIfMIBObjects 3 }
dsgIfDownstreamChannel   OBJECT IDENTIFIER ::= { dsgIfMIBObjects 4 }

dsgIfDCD                 OBJECT IDENTIFIER ::= { dsgIfMIBObjects 5 }

--------------------------------------------------------------------
```

```
--The Classifier Table contains objects for classifying packets.
--The DSG Agent applies the DSG classifier parameters to the inbound
--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 objects in this table with the exception of
--the dsgIfClassDestPortStart and dsgIfClassDestPortEnd objects.
--
--The DSG Agent must also include these encoding in the DCD messages on
--the downstream channels to which the classifiers apply.
--
--The DSG classifier is unique per DSG Agent.
-------------------------------------------------------------------------

dsgIfClassifierTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfClassifierEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Classifier Table contains attributes used to classify
            inbound packets into the tunnel and classifiers for the DSG
            clients, encoding in the DCD messages on the downstream
            channels to which the classifiers apply."
    ::= { dsgIfClassifier 1 }

dsgIfClassifierEntry OBJECT-TYPE
    SYNTAX      DsgIfClassifierEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in the Classifier Table. Rows are created
            by an SNMP SET request setting the value of
            dsgIfClassRowStatus to 'createAndGo'. Each entry is created
            for a tunnel, index by dsgTunnelIndex.

            Rows are deleted by an SNMP SET request setting the value
            of dsgIfClassRowStatus to 'destroy'."
    INDEX { dsgIfTunnelIndex, dsgIfClassId }
    ::= { dsgIfClassifierTable 1 }

DsgIfClassifierEntry ::=  SEQUENCE {
    dsgIfClassId                Unsigned32,
    dsgIfClassPriority          Unsigned32,
    dsgIfClassSrcIpAddrType     InetAddressType,
    dsgIfClassSrcIpAddr         InetAddress,
    dsgIfClassSrcIpPrefixLength InetAddressPrefixLength,
    dsgIfClassDestIpAddressType InetAddressType,
    dsgIfClassDestIpAddress     InetAddress,
    dsgIfClassDestPortStart     InetPortNumber,
    dsgIfClassDestPortEnd       InetPortNumber,
    dsgIfClassRowStatus         RowStatus,
    dsgIfClassIncludeInDCD      TruthValue
    }

dsgIfClassId OBJECT-TYPE
    SYNTAX      Unsigned32 (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index that provides a unique classifier (in a DSG
            Agent). This value corresponds to the Classifier ID TLV
            in the DCD message."
    ::= { dsgIfClassifierEntry 1 }

dsgIfClassPriority OBJECT-TYPE
    SYNTAX      Unsigned32 (0..255)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The priority of this classifier.
            Default value 0 indicates lowest priority."
    DEFVAL { 0 }
```

```
    ::= { dsgIfClassifierEntry 2 }

dsgIfClassSrcIpAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The type of internet address of dsgIfClassSrcIpAddress."
    DEFVAL { ipv4 }
    ::= { dsgIfClassifierEntry 3 }

dsgIfClassSrcIpAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The source IP address to be matched for this classifier.
            A value 0 for this object indicates a match of any IP
            address. A value that contains non-zero bits
            outside the range indicated by dsgIfClassSrcIpPrefixLength
            is invalid and should be rejected."
    DEFVAL { '00000000'h }
    ::= { dsgIfClassifierEntry 4 }

dsgIfClassSrcIpPrefixLength OBJECT-TYPE
    SYNTAX      InetAddressPrefixLength
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The length of the CIDR Prefix carried in
            dsgIfClassSrcIpAddr. In IPv4 addresses, a length of 32 indicates
            a match of a single host address, and a length between
            0 and 32 indicates the use of a CIDR Prefix. A length of
            0 is not allowed. This object is irrelevant and not used
            when dsgIfClassSrcIpAddr value is 0."
    DEFVAL { 32 }
    ::= { dsgIfClassifierEntry 5 }

dsgIfClassDestIpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The type of internet address of dsgIfClassDestIpAddress."
    DEFVAL { ipv4 }
    ::= { dsgIfClassifierEntry 6 }

dsgIfClassDestIpAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The destination IP address to be matched for this
            classifier."
    DEFVAL { '00000000'h }
    ::= { dsgIfClassifierEntry 7 }

dsgIfClassDestPortStart OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "This is the inclusive lower bound of the transport-layer
            source port range that is to be matched."
    DEFVAL { 0 }
    ::= { dsgIfClassifierEntry 8 }

dsgIfClassDestPortEnd OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
            "This is the inclusive higher bound of the transport-layer
            source port range that is to be matched."
    DEFVAL { 65535 }
    ::= { dsgIfClassifierEntry 9 }

dsgIfClassRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of the row.  A value of active(1) indicates
            that this classifier is applied to this tunnel.
            A value of notInService(2) indicates that matching of
            the packets are ignored and this classifier parameters
            will not be included in the DCD message."
    ::= { dsgIfClassifierEntry 10 }

dsgIfClassIncludeInDCD OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Indicates whether or not this DSG Classifier will
            be sent in DCD messages for use as a Layer-3 and
            Layer-4 packet filter by the DSG eCM."
    DEFVAL { false }
    ::= { dsgIfClassifierEntry 11 }

--------------------------------------------------------------------------
-- The DSG Tunnel Table contains group(s) of DSG Tunnel Indexes.
-- Tunnel Entry is mapped to the destination MAC address and each
-- tunnel is associated to the Qos Service Class Name.
--------------------------------------------------------------------------

dsgIfTunnelTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfTunnelEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The DSG Tunnel Table contains group(s) of tunnel(s).
            Each tunnel is associated to the destination MAC address."
    ::= { dsgIfTunnel 1 }

dsgIfTunnelEntry OBJECT-TYPE
   SYNTAX      DsgIfTunnelEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION
           "An entry in the DSG Tunnel Table. Rows are created by
           an SNMP SET request setting the value of
           dsgIfTunnelRowStatus to 'createAndGo'.

           Each entry associated to a tunnel.  A dsgIfTunnelGroupIndex
           represents a group of tunnels that could be associated to
            one or more downstreams. Each dsgIfTunnelIndex represents
            a tunnel.

            Rows are deleted by an SNMP SET request setting the
            value of dsgIfTunnelRowStatus to 'destroy'."
    INDEX { dsgIfTunnelIndex }
    ::= { dsgIfTunnelTable 1 }

DsgIfTunnelEntry ::= SEQUENCE {
    dsgIfTunnelIndex             Unsigned32,
    dsgIfTunnelGroupIndex        Unsigned32,
    dsgIfTunnelClientIdListIndex Unsigned32,
    dsgIfTunnelMacAddress        MacAddress,
    dsgIfTunnelServiceClassName  SnmpAdminString,
    dsgIfTunnelRowStatus         RowStatus
    }
```

```
dsgIfTunnelIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index into the DSG Tunnel table that represents
            a tunnel."
    ::= { dsgIfTunnelEntry 1 }

dsgIfTunnelGroupIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "This index represents a group of tunnels that could be
            associated to one or more downstreams which mapped
            to dsgIfTunnelGrpIndex."
    ::= { dsgIfTunnelEntry 2 }

dsgIfTunnelClientIdListIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "This index represents a group of client id(s)
            which mapped to dsgIfClientIdListIndex."
    ::= { dsgIfTunnelEntry 3 }

dsgIfTunnelMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The DSG tunnel destination MAC address."
    DEFVAL { '000000000000'h }
    ::= { dsgIfTunnelEntry 4 }

dsgIfTunnelServiceClassName OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The Service Class Name that associated to the
            docsQosServiceClassName(in DOCS-QOS-MIB).  Creation of a
            Service Class MUST be configured through the
            docsQosServiceClassTable.  Only partial of the
            docsQosServiceClassTable objects are applicable to the
            DSG service class thus some are ignored.

            If the referenced parameter is not present in the
            corresponding DOCSIS QOS Parameter Set, the default
            value of this object is a zero length string."
    REFERENCE "SP-RFIv1.1-I10-030730, Appendix C.2.2.3.4"
    ::= { dsgIfTunnelEntry 5 }

dsgIfTunnelRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of the row. A value of notInService(2)
            indicates that this tunnel is disabled and no OOB traffic
            will be forwarded to DSG clients and these tunnel parameters
            will not be included in the DCD message."
    ::= { dsgIfTunnelEntry 6}

--------------------------------------------------------------------
--The DSG Tunnel Group to Channel Table contains the association of
--groups of tunnels to one or more downstream channels.  This table
--contains the downstream ifIndex, rule priority, UCID Range and vendor
```

```
--parameter identification(2).
-------------------------------------------------------------------------

dsgIfTunnelGrpToChannelTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfTunnelGrpToChannelEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The DSG Tunnel Group to Channel Table associates a group
            of tunnels to one or more downstream channels."
    ::= { dsgIfTunnelGrpToChannel 1 }

dsgIfTunnelGrpToChannelEntry OBJECT-TYPE
    SYNTAX      DsgIfTunnelGrpToChannelEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in the DSG Tunnel Table. Rows are created by
            an SNMP SET request setting the value of
            dsgIfTunnelGrpRowStatus to 'createAndGo'.

            Rows are deleted by an SNMP SET request setting the
            value of dsgIfTunnelRowStatus to 'destroy'."
    INDEX { dsgIfTunnelGrpIndex, dsgIfTunnelGrpChannelIndex }
    ::= { dsgIfTunnelGrpToChannelTable 1 }

DsgIfTunnelGrpToChannelEntry ::= SEQUENCE {
    dsgIfTunnelGrpIndex         Unsigned32,
    dsgIfTunnelGrpChannelIndex  Unsigned32,
    dsgIfTunnelGrpDsIfIndex     InterfaceIndex,
    dsgIfTunnelGrpRulePriority  Unsigned32,
    dsgIfTunnelGrpUcidList      OCTET STRING,
    dsgIfTunnelGrpVendorParamId Unsigned32,
    dsgIfTunnelGrpRowStatus     RowStatus
    }

dsgIfTunnelGrpIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index into this table."
    ::= { dsgIfTunnelGrpToChannelEntry 1 }

dsgIfTunnelGrpChannelIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index into this table."
    ::= { dsgIfTunnelGrpToChannelEntry 2 }

dsgIfTunnelGrpDsIfIndex OBJECT-TYPE
    SYNTAX      InterfaceIndex
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The downstream ifIndex that will be associated to
            this group of tunnel(s)."
    ::= { dsgIfTunnelGrpToChannelEntry 3 }

dsgIfTunnelGrpRulePriority OBJECT-TYPE
    SYNTAX      Unsigned32 (0..255)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The DSG rule priority determines the order of which
            channel and its associated UCIDs should be applied by
            the DSG client. The default value is 0, which is the lowest
            priority."
    DEFVAL { 0 }
```

```
    ::= { dsgIfTunnelGrpToChannelEntry 4 }

dsgIfTunnelGrpUcidList OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..255))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The list of Upstream Channel ID (UCID) values (octets)
            for which the DSG rule applies. One octet represents one UCID value (0-255) A
            DSG client matches this parameter if its UCID value is included in the list.
            The default value of zero length string indicates that this
            DSG Rule applies to all DSG clients."
    DEFVAL { "" }
    ::= { dsgIfTunnelGrpToChannelEntry 5 }

dsgIfTunnelGrpVendorParamId OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The index of vendor parameter, dsgIfVendorParamId in the
            dsgIfVendorParamTable describing the vendor specific DSG
            parameters. If no associated entry in dsgIfVendorParamTable
            exists, this value is 0."
    DEFVAL { 0 }
    ::= { dsgIfTunnelGrpToChannelEntry 6 }

dsgIfTunnelGrpRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of this row. The value of notInService(2)
            indicates that this tunnel group is disabled and no OOB
            traffic on all the associated tunnel(s) will be forwarded
            to DSG clients and all parameters will not be included in
            the DCD message."
    ::= { dsgIfTunnelGrpToChannelEntry 7 }

--------------------------------------------------------------------------
--The Downstream Table contains the DSG Tunnel Index, the timer
--index, specific vendor parameter identification(3) and the
--index to the downstream channel list.
--------------------------------------------------------------------------

dsgIfDownstreamTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfDownstreamEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The DSG Downstream Table contains the associated timers,
            vendor specific parameters index and the channel list
            index to a specific downstream."
    ::= { dsgIfDownstreamChannel 1 }

dsgIfDownstreamEntry OBJECT-TYPE
    SYNTAX      DsgIfDownstreamEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in the DSG Downstream Table.
            An entry in this table exists for each ifEntry with
            an ifType of docsCableDownstream(128)."
    INDEX { ifIndex }
    ::= { dsgIfDownstreamTable 1 }

DsgIfDownstreamEntry ::= SEQUENCE {
    dsgIfDownTimerIndex       Unsigned32,
    dsgIfDownVendorParamId    Unsigned32,
    dsgIfDownChannelListIndex Unsigned32,
    dsgIfDownEnableDCD        TruthValue
```

```
    }

dsgIfDownTimerIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The index into the timer table, dsgIfTimerTable providing
            the timers used by the DSG client(s).
            The default value 0 indicates there is no associated
            timers that need to be sent in the DCD message."
    DEFVAL { 0 }
    ::= { dsgIfDownstreamEntry 1 }

dsgIfDownVendorParamId OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The index of vendor parameter, dsgIfVendorParamId in the
            dsgIfVendorParamTable describing the vendor specific DSG
            parameters. If no associated entry in dsgIfVendorParamTable
            exists, this value is 0."
    DEFVAL { 0 }
    ::= { dsgIfDownstreamEntry 2 }

dsgIfDownChannelListIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The index of the downstream frequency channel lists,
            dsgIfChannelListIndex in the dsgIfChannelListTable
            providing the list of downstream frequencies that
            contain DSG tunnels."
    DEFVAL { 0 }
    ::= { dsgIfDownstreamEntry 3 }

dsgIfDownEnableDCD OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Used to enable or disable DCD messages to be sent on this
            downstream channel. The value is always true(1) for those
            downstreams that contain one or many DSG Tunnels."
    ::= { dsgIfDownstreamEntry 4 }

--------------------------------------------------------------------------
--The Client Table contains the objects that specify the matching
--parameters for the DSG clients for which the DSG rules applies.
--The DSG clients recognized that ids may be originated from different
--address space.  The same DSG client id may be used by multiple rules.

--------------------------------------------------------------------------

dsgIfClientIdTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfClientIdEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Client Identification Table contains the client
            identification type and value.  It also contains the
            vendor specific parameter identification.  There could
            be multiple client ids associated to a tunnel, grouped
            by the dsgIfClientIdListIndex."
    ::= { dsgIfDCD 1 }

dsgIfClientIdEntry OBJECT-TYPE
    SYNTAX      DsgIfClientIdEntry
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
    DESCRIPTION
            "An entry in the Client Id Table. Rows are created
            by an SNMP SET request setting the value of
            dsgIfClientRowStatus to 'createAndGo'.

            Rows are deleted by an SNMP SET request setting the
            value of dsgIfClientIdRowStatus to 'destroy'."
    INDEX { dsgIfClientIdListIndex, dsgIfClientIdIndex }
    ::= { dsgIfClientIdTable 1 }

DsgIfClientIdEntry ::= SEQUENCE {
    dsgIfClientIdListIndex   Unsigned32,
    dsgIfClientIdIndex       Unsigned32,
    dsgIfClientIdType        INTEGER,
    dsgIfClientIdValue       OCTET STRING,
    dsgIfClientVendorParamId Unsigned32,
    dsgIfClientRowStatus     RowStatus
    }

dsgIfClientIdListIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index to this table."
    ::= { dsgIfClientIdEntry 1 }

dsgIfClientIdIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index to each entry of the Client Id."
    ::= { dsgIfClientIdEntry 2 }

dsgIfClientIdType OBJECT-TYPE
    SYNTAX      INTEGER {
        broadcast(1),
        macAddress(2),
        caSystemId(3),
        applicationId(4)
        }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The Client Identification type.  A DSG client id of type
            broadcast(1) received by all DSG client(s).  A DSG client
            id of type macAddress(2) is received by the DSG client that
            has been assigned with this MAC address where the first 3
            bytes are the Organization Unique Identifier (OUI). A DSG
            client id of type caSystemId(3) is received by the DSG
            client that has been assigned a CA_system_ID.  A DSG client
            id of type applicationId(4) is received by the DSG client
            that has been assigned an application ID."
    DEFVAL { broadcast }
    ::= { dsgIfClientIdEntry 3 }

dsgIfClientIdValue OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(6))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The Client Identification Value. The content depends on
            the value of the dsgIfClientIdType.
            For dsgIfClientIdType of a type broadcast(1), this object will
            have a 16-bit value whether or not it is a length 0 or length 2
            broadcast ID. If the value is 0, then the encoded TLV in the
            DCD would be the original, zero length, broadcast ID.  If the
            value is specified in Table 5-2, then the TLV in the DCD would
            be a length 2 broadcast ID followed by the value.
```

```
          For dsgIfClientIdType of a type macAddress(2), this object
          is a well-known MAC address.
          For dsgIfClientIdType of a type caSystemId(3), this object
          is a CA System ID.
          For dsgIfClientIdType of a type applicationId(4), this object
          is an application ID.
          Client IDs representing types broadcast(1), caSystemId(3) or
          applicationId(4) are encoded in DCD messages as Unsigned
          integers and configured in this object as 6 octet string with
          the 2 LSB for the client ID value, e.g., an applicationId 2048
          (0x0800) is encoded as '000000000800'h."
      REFERENCE
          "DOCSIS Set-top Gateway (DSG) Interface"

      DEFVAL { '000000000000'h }
      ::= { dsgIfClientIdEntry 4 }

  dsgIfClientVendorParamId OBJECT-TYPE
      SYNTAX      Unsigned32
      MAX-ACCESS  read-create
      STATUS      current
      DESCRIPTION
              "The index of the vendor parameter id, dsgIfVendorParamId
              in the dsgIfVendorParamTable describing the vendor specific
              DSG parameters. If no associated entry in
              dsgIfVendorParamTable exists, this value is 0."
      DEFVAL { 0 }
      ::= { dsgIfClientIdEntry 5 }

  dsgIfClientRowStatus OBJECT-TYPE
      SYNTAX      RowStatus
      MAX-ACCESS  read-create
      STATUS      current
      DESCRIPTION
              "The status of the row."
      ::= { dsgIfClientIdEntry 6 }

  ----------------------------------------------------------------------
  --The Vendor Parameter Table contains vendor-specific parameters
  --which allow vendors to send the specific parameters within a
  --DSG rule or within the DSG Configuration block in a DCD message.
  ----------------------------------------------------------------------

  dsgIfVendorParamTable OBJECT-TYPE
      SYNTAX      SEQUENCE OF DsgIfVendorParamEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
              "The DSG Vendor Parameter Table allows vendors to send
              specific parameters to the DSG clients within a DSG
              rule or within the DSG Configuration block in a
              DCD message."
      ::= { dsgIfDCD 2 }

  dsgIfVendorParamEntry OBJECT-TYPE
      SYNTAX      DsgIfVendorParamEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
              "An entry in the DSG Vendor Parameter Table. Rows are
              created by an SNMP SET request setting the value of
              dsgIfVendorRowStatus to 'createAndGo'. Each entry
              represents one or more vendor's specific parameters.
              Rows are deleted by an SNMP SET  request setting the
              value of dsgIfVendorRowStatus to 'destroy'.

              There are limits to the amount of vendor specific
              information that can be carried in a DSG Rule or
              DSG Configuration block. An SNMP SET request which
              would result in these limits being exceeded should be
              rejected."
```

```
    INDEX { dsgIfVendorParamId, dsgIfVendorIndex }
    ::= { dsgIfVendorParamTable 1 }

DsgIfVendorParamEntry ::= SEQUENCE {
    dsgIfVendorParamId    Unsigned32,
    dsgIfVendorIndex      Unsigned32,
    dsgIfVendorOUI        OCTET STRING,
    dsgIfVendorValue      OCTET STRING,
    dsgIfVendorRowStatus  RowStatus
    }

dsgIfVendorParamId OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index of the table."
    ::= { dsgIfVendorParamEntry 1 }

dsgIfVendorIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Vendor Specific Index."
    ::= { dsgIfVendorParamEntry 2 }

dsgIfVendorOUI OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(3))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The Vendor assigned Organization Unique Id (OUI)."
    DEFVAL { '000000'h }
    ::= { dsgIfVendorParamEntry 3 }

dsgIfVendorValue OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..50))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The Vendor Specific Parameter Value."
    DEFVAL { "" }
    ::= { dsgIfVendorParamEntry 4 }

dsgIfVendorRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of the row."
    ::= { dsgIfVendorParamEntry 5 }

--------------------------------------------------------------------------
--The Channel List Table contains lists of one or multiple
--downstream frequencies that are carrying DSG tunnels. The
--appropriate DSG Channel List will be included in the DCD
--message on the associated downstream channel from the
--dsgIfDownstreamTable.
--The DSG Client uses this list to determine which downstream
--frequencies have DSG Tunnels present.
--------------------------------------------------------------------------

dsgIfChannelListTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfChannelListEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The DSG Channel List Table contains list of one or
            multiple downstream frequencies that are carrying DSG
            tunnel(s)."
```

```
    ::= { dsgIfDCD 3 }

dsgIfChannelListEntry OBJECT-TYPE
    SYNTAX      DsgIfChannelListEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in the DSG Channel List Table. Rows are
            created by an SNMP SET request setting the value of
            dsgIfChannelRowStatus to 'createAndGo'.

            Rows are deleted by an SNMP SET  request setting the value
            of dsgIfChannelRowStatus to 'destroy'."
    INDEX { dsgIfChannelListIndex, dsgIfChannelIndex }
    ::= { dsgIfChannelListTable 1 }

DsgIfChannelListEntry ::= SEQUENCE {
    dsgIfChannelListIndex  Unsigned32,
    dsgIfChannelIndex      Unsigned32,
    dsgIfChannelDsFreq     Integer32,
    dsgIfChannelRowStatus  RowStatus
    }

dsgIfChannelListIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index to this table."
    ::= { dsgIfChannelListEntry 1 }

dsgIfChannelIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index for each downstream frequency that
            contains the DSG tunnel(s)."
    ::= { dsgIfChannelListEntry 2 }

dsgIfChannelDsFreq OBJECT-TYPE
    SYNTAX      Integer32 (0..1000000000)
    UNITS       "hertz"
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The DOCSIS downstream centre frequency. The receive
            frequency MUST be a multiple of 62500 Hz."
    DEFVAL { 0 }
    ::= { dsgIfChannelListEntry 3 }

dsgIfChannelRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of the row."
    ::= { dsgIfChannelListEntry 4 }

--------------------------------------------------------------------------
--The Timer Table contains 4 timeout timers that are sent to the DSG
--clients via the DCD message. These timers are sent to the DSG clients
--via the DCD message.
--Each downstream mapped to only one set of timers.
--------------------------------------------------------------------------

dsgIfTimerTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfTimerEntry
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
            "The DSG Timer Table contains timers that are sent to
            the DSG client(s) via the DCD message."
    ::= { dsgIfDCD 4 }

dsgIfTimerEntry OBJECT-TYPE
    SYNTAX      DsgIfTimerEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in the DSG Timer Table. Rows are created
            by an SNMP SET request setting the value of
            dsgIfTimerRowStatus to 'createAndGo'.

            Rows are deleted by an SNMP SET request setting the value
            of dsgIfTimerRowStatus to 'destroy'."
    INDEX { dsgIfTimerIndex }
    ::= { dsgIfTimerTable 1 }

DsgIfTimerEntry ::= SEQUENCE {
    dsgIfTimerIndex     Unsigned32,
    dsgIfTimerTdsg1     Unsigned32,
    dsgIfTimerTdsg2     Unsigned32,
    dsgIfTimerTdsg3     Unsigned32,
    dsgIfTimerTdsg4     Unsigned32,
    dsgIfTimerRowStatus RowStatus
    }

dsgIfTimerIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index to this table."
    ::= { dsgIfTimerEntry 1 }

dsgIfTimerTdsg1 OBJECT-TYPE
    SYNTAX      Unsigned32 (1..65535)
    UNITS       "second"
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Initialization Timeout.  This is the timeout period
            for the DSG packets during initialization of the DSG
            client. The default value is 2 seconds."
    DEFVAL { 2 }
    ::= { dsgIfTimerEntry 2 }

dsgIfTimerTdsg2 OBJECT-TYPE
    SYNTAX      Unsigned32 (1..65535)
    UNITS       "second"
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Operational Timeout.  This is the timeout period for
            the DSG packets during normal operation of the DSG client.
            Default value is 10 minutes."
    DEFVAL { 600 }
    ::= { dsgIfTimerEntry 3 }

dsgIfTimerTdsg3 OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    UNITS       "second"
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Two-way retry timer. This is the retry timer that
            determines when the DSG client attempts to reconnect
            with the DSG Agent and established two-way connectivity.
            Default value is 5 minutes. The value 0 indicates that
            the client will continuously retry two-way operation."
```

```
    DEFVAL { 300 }
    ::= { dsgIfTimerEntry 4 }

dsgIfTimerTdsg4 OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    UNITS       "second"
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "One-way retry timer.  The retry timer that determines
            when the client attempts to rescan for a DOCSIS
            downstream channel that contains DSG packets after a
            dsgIfTimerTdsg1 or dsgIfTimerTdsg2 timeout.
            Default value is 30 minutes. The value 0 indicates that
            the client will immediately begin scanning upon
            dsgIfTimerTdsg1 or dsgIfTimerTdsg2 timeout."
    DEFVAL { 1800 }
    ::= { dsgIfTimerEntry 5 }

dsgIfTimerRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of the row."
    ::= { dsgIfTimerEntry 6 }

--
-- Conformance definitions
--
dsgIfConformance  OBJECT IDENTIFIER ::= { dsgIfMIB 4 }
dsgIfGroups       OBJECT IDENTIFIER ::= { dsgIfConformance 1 }
dsgIfCompliances  OBJECT IDENTIFIER ::= { dsgIfConformance 2 }

dsgIfBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for DOCSIS Set-top Gateway
            systems."

MODULE -- dsgIfMIB

-- conditionally mandatory groups

GROUP dsgIfClassifierGroup
    DESCRIPTION
            "Mandatory in DOCSIS Set-top Gateway systems."

GROUP dsgIfBaseGroup
    DESCRIPTION
            "Mandatory in DOCSIS Set-top Gateway systems."

GROUP dsgIfDCDGroup
    DESCRIPTION
            "Mandatory in DOCSIS Set-top Gateway systems."

    ::= { dsgIfCompliances 1 }

dsgIfClassifierGroup OBJECT-GROUP
    OBJECTS {
            dsgIfClassPriority,
            dsgIfClassSrcIpAddrType,
            dsgIfClassSrcIpAddr,
            dsgIfClassSrcIpPrefixLength,
            dsgIfClassDestIpAddressType,
            dsgIfClassDestIpAddress,
            dsgIfClassDestPortStart,
            dsgIfClassDestPortEnd,
            dsgIfClassRowStatus,
            dsgIfClassIncludeInDCD
            }
```

```
    STATUS      current
    DESCRIPTION
            "A collection of objects providing the classifier
            configuration."
    ::= { dsgIfGroups 1 }

dsgIfBaseGroup OBJECT-GROUP
    OBJECTS {
            dsgIfTunnelGroupIndex,
            dsgIfTunnelClientIdListIndex,
            dsgIfTunnelMacAddress,
            dsgIfTunnelServiceClassName,
            dsgIfTunnelRowStatus,
            dsgIfTunnelGrpDsIfIndex,
            dsgIfTunnelGrpRulePriority,
            dsgIfTunnelGrpUcidList,
            dsgIfTunnelGrpVendorParamId,
            dsgIfTunnelGrpRowStatus,
            dsgIfDownTimerIndex,
            dsgIfDownVendorParamId,
            dsgIfDownChannelListIndex,
            dsgIfDownEnableDCD
            }
    STATUS      current
    DESCRIPTION
            "A collection of objects providing DSG Tunnel and Channel
            configuration."
    ::= { dsgIfGroups 2 }

dsgIfDCDGroup OBJECT-GROUP
    OBJECTS {
            dsgIfClientIdType,
            dsgIfClientIdValue,
            dsgIfClientVendorParamId,
            dsgIfClientRowStatus,
            dsgIfVendorOUI,
            dsgIfVendorValue,
            dsgIfVendorRowStatus,
            dsgIfChannelDsFreq,
            dsgIfChannelRowStatus,
            dsgIfTimerTdsg1,
            dsgIfTimerTdsg2,
            dsgIfTimerTdsg3,
            dsgIfTimerTdsg4,
            dsgIfTimerRowStatus
            }
    STATUS      current
    DESCRIPTION
            "A collection of objects providing Timers configuration."
    ::= { dsgIfGroups 3 }
END
```

Annex B

DOCSIS set-top gateway set-top device MIB definition

```
DSG-IF-STD-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    NOTIFICATION-TYPE,
    Integer32,
    Unsigned32,
    Counter32                FROM SNMPv2-SMI         -- RFC 2578

    OBJECT-GROUP,
    NOTIFICATION-GROUP,
    MODULE-COMPLIANCE        FROM SNMPv2-CONF        -- RFC 2580

    MacAddress               FROM SNMPv2-TC          -- RFC 2579

    InetAddressType,
    InetAddress,
    InetAddressPrefixLength,
    InetPortNumber           FROM INET-ADDRESS-MIB   -- RFC 3291

    IfPhysAddress            FROM IF-MIB             -- RFC 2863

    docsDevEvLevel,
    docsDevEvId,
    docsDevEvText            FROM DOCS-CABLE-DEVICE-MIB   -- RFC 2669

    docsIfCmCmtsAddress,
    docsIfDocsisBaseCapability,
    docsIfCmStatusDocsisOperMode,
    docsIfCmStatusModulationType
                             FROM DOCS-IF-MIB  -- RFI MIB v2.0 draft 05

    clabProjDocsis           FROM CLAB-DEF-MIB;

dsgIfStdMib MODULE-IDENTITY
    LAST-UPDATED "200411240000Z" -- November 24, 2004
    ORGANIZATION "CableLabs DSG Working Group"
    CONTACT-INFO
             "
             Postal: Cable Television Laboratories, Inc.
                     858 Coal Creek Circle
                     Louisville, Colorado 80027
                     U.S.A.
             Phone : +1 303-661-9100
             Fax   : +1 303-661-9199
             E-mail: "
    DESCRIPTION
            "This MIB module provides the management objects of
            the DOCSIS Set-top Gateway (DSG) client controller
            CM component for DSG operations of Set-top devices."
    REVISION    "200411240000Z" -- November 24, 2004
    DESCRIPTION
            "Initial version of this MIB module.
            This revision is published as part of the CableLabs
            DSG specification.

            Copyright 1999-2004 Cable Television Laboratories, Inc.
            All rights reserved."
    ::= { clabProjDocsis 4 }

-------------------------------------------------------------------------
--
-- DSG eCM MIB objects that represent the DSG Configuration parameters
-- Tunnels information and list of available downstream channels
--  carrying the Set-top box content.
```

```
--
-------------------------------------------------------------------------

dsgIfStdNotifications     OBJECT IDENTIFIER ::= { dsgIfStdMib 0 }
dsgIfStdMibObjects        OBJECT IDENTIFIER ::= { dsgIfStdMib 1 }
dsgIfStdConfig            OBJECT IDENTIFIER ::= { dsgIfStdMibObjects 1 }
dsgIfStdTunnelFilter      OBJECT IDENTIFIER ::= { dsgIfStdMibObjects 2 }
dsgIfStdDsgChannelList    OBJECT IDENTIFIER ::= { dsgIfStdMibObjects 3 }

-------------------------------------------------------------------------
-- DSG eCM Scalar objects
-------------------------------------------------------------------------

dsgIfStdDsgMode OBJECT-TYPE
    SYNTAX      INTEGER {
                basic(1),
                advanced(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The DSG Mode of operation of this device."
    ::= { dsgIfStdConfig 1 }

dsgIfStdTdsg1 OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The configured value for the Tdsg1 timer."
    DEFVAL { 2 }
    ::= { dsgIfStdConfig 2 }

dsgIfStdTdsg2 OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The configured value for the Tdsg2 timer."
    DEFVAL { 600 }
    ::= { dsgIfStdConfig 3 }

dsgIfStdTdsg3 OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The configured value for the Tdsg3 timer."
    DEFVAL { 300 }
    ::= { dsgIfStdConfig 4 }

dsgIfStdTdsg4 OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The configured value for the Tdsg4 timer."
    DEFVAL { 1800 }
    ::= { dsgIfStdConfig 5 }

dsgIfStdTdsg1Timeouts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of times Tdsg1 expired in the DSG eCM since
            last reboot."
```

```
    ::= { dsgIfStdConfig 6 }

dsgIfStdTdsg2Timeouts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of times Tdsg2 expired in the DSG eCM since
            last reboot."
    ::= { dsgIfStdConfig 7 }

dsgIfStdTdsg3Timeouts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of times Tdsg3 expired in the DSG eCM since
            last reboot."
    ::= { dsgIfStdConfig 8 }

dsgIfStdTdsg4Timeouts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of times Tdsg4 expired in the DSG eCM since
            last reboot."
    ::= { dsgIfStdConfig 9 }

--------------------------------------------------------------------------
-- Active Tunnel filters, one row per Tunnel classifier
-- (or tunnel for those that don't have classifiers)
--------------------------------------------------------------------------

dsgIfStdTunnelFilterTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfStdTunnelFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "A Table with the DSG tunnels the DSG eCM is filtering
            and forwarding to the DSG Clients."
    ::= { dsgIfStdTunnelFilter 1 }

dsgIfStdTunnelFilterEntry OBJECT-TYPE
    SYNTAX      DsgIfStdTunnelFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The DSG eCM will have one entry for each DSG Tunnel
            Filter. A DSG eCM in Advanced mode will have at least one
            such Filter for each DSG classifier, and at least one such
            Filter for each DSG Tunnel that lacks a DSG classifier
            (i.e., the DSG Tunnel MAC address is the only relevant
            filtering parameter). The DSG eCM in Basic mode will have at
            least one entry for each DSG Tunnel MAC Address. Entries
            are created when the eCM is instructed to begin forwarding
            particular DSG Tunnels by the DSG Client Controller.
            Entries are deleted when the eCM is no longer instructed to
            forward those particular DSG Tunnels by the DSG Client
            Controller."
    INDEX { dsgIfStdTunnelFilterIndex }
    ::= { dsgIfStdTunnelFilterTable 1 }

DsgIfStdTunnelFilterEntry ::=  SEQUENCE {
    dsgIfStdTunnelFilterIndex              Unsigned32,
    dsgIfStdTunnelFilterApplicationId      Integer32,
    dsgIfStdTunnelFilterMacAddress         MacAddress,
    dsgIfStdTunnelFilterIpAddressType      InetAddressType,
    dsgIfStdTunnelFilterSrcIpAddr          InetAddress,
    dsgIfStdTunnelFilterSrcIpMask          InetAddress,
    dsgIfStdTunnelFilterDestIpAddr         InetAddress,
```

```
    dsgIfStdTunnelFilterDestPortStart      InetPortNumber,
    dsgIfStdTunnelFilterDestPortEnd        InetPortNumber,
    dsgIfStdTunnelFilterPkts               Counter32,
    dsgIfStdTunnelFilterOctets             Counter32,
    dsgIfStdTunnelFilterTimeActive         Counter32,
    dsgIfStdTunnelFilterTunnelId           Unsigned32
    }

dsgIfStdTunnelFilterIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The unique index of entries in this table."
    ::= { dsgIfStdTunnelFilterEntry 1 }

dsgIfStdTunnelFilterApplicationId OBJECT-TYPE
    SYNTAX      Integer32 (-1 | 0.. 65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The ID of the application to which this DSG Tunnel is to
            be forwarded. This object returns -1 for: DSG Tunnels that
            do not have an associated Application ID or for DSG Tunnels
            for which the Application ID is unknown. In an OpenCable
            Host, this object returns '0' for a DSG Tunnel whose client
            resides on the Card."
    DEFVAL { -1 }
    ::= { dsgIfStdTunnelFilterEntry 2 }

dsgIfStdTunnelFilterMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The destination MAC Address associated with this
            tunnel entry."
    ::= { dsgIfStdTunnelFilterEntry 3 }

dsgIfStdTunnelFilterIpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for dsgIfStdTunnelFilterSrcIpAddr,
            dsgIfStdTunnelFilterSrcIpMask and
            dsgIfStdTunnelFilterDestIpAddr."
    ::= { dsgIfStdTunnelFilterEntry 4 }

dsgIfStdTunnelFilterSrcIpAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The source IP Address associated to this tunnel for the
            DSG eCM filtering and forwarding process. A value of zero
            indicates that source IP Address filtering does not apply.
            The type of this address is determined by the value of the
            dsgIfStdTunnelFilterIpAddressType object."
    DEFVAL { '00000000'h }
    ::= { dsgIfStdTunnelFilterEntry 5 }

dsgIfStdTunnelFilterSrcIpMask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Source IP Mask to be used along with
            dsgIfStdTunnelFilterSrcIpAddr for filtering
            and forwarding of DSG Tunnel traffic.
            The type of this address is determined by the value of the
```

```
            dsgIfStdTunnelFilterIpAddressType object."
    DEFVAL { 'FFFFFFFF'h }
    ::= { dsgIfStdTunnelFilterEntry 6 }

dsgIfStdTunnelFilterDestIpAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The destination IP Address associated to this tunnel for
            the DSG eCM filtering and forwarding process. A value of
            zero indicates that destination IP Address filtering does
            not apply. The type of this address is determined by the
            value of the dsgIfStdTunnelFilterIpAddressType object."
    DEFVAL { '00000000'h }
    ::= { dsgIfStdTunnelFilterEntry 7 }

dsgIfStdTunnelFilterDestPortStart OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The lower UDP port value to be matched for this tunnel."
    DEFVAL { 0 }
    ::= { dsgIfStdTunnelFilterEntry 8 }

dsgIfStdTunnelFilterDestPortEnd OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The upper UDP port value to be matched for this tunnel."
    DEFVAL { 65535 }
    ::= { dsgIfStdTunnelFilterEntry 9 }

dsgIfStdTunnelFilterPkts OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The total number of Packets being classified and filtered
            for this tunnel entry since creation of the entry."
    ::= { dsgIfStdTunnelFilterEntry 10 }

dsgIfStdTunnelFilterOctets OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "octets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The total number of octets being classified and filtered
            for this tunnel entry since creation of the entry."
    ::= { dsgIfStdTunnelFilterEntry 11 }

dsgIfStdTunnelFilterTimeActive OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "seconds"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The total number of seconds that this tunnel entry has
            been instantiated."
    ::= { dsgIfStdTunnelFilterEntry 12 }

dsgIfStdTunnelFilterTunnelId OBJECT-TYPE
    SYNTAX      Unsigned32 (0 | 1..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "In DSG Advanced Mode, this is the tunnel identifier passed
```

```
            to the DSG eCM by the DSG-Client Controller for this Tunnel
            Filter entry. This value may correspond to the DSG Rule ID
            from the DCD message. In DSG Basic mode this object returns
            zero."
    DEFVAL { 0 }
    ::= { dsgIfStdTunnelFilterEntry 13 }

--------------------------------------------------------------------------
-- DSG Channel List Table, one row per DSG Channel Frequency provided
-- in the DCD message.
--------------------------------------------------------------------------

dsgIfStdDsgChannelListTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DsgIfStdDsgChannelListEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains the list of DSG channels provided to
            the DSG eCM for use in scanning."
    ::= { dsgIfStdDsgChannelList 1 }

dsgIfStdDsgChannelListEntry OBJECT-TYPE
    SYNTAX      DsgIfStdDsgChannelListEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The conceptual row for this table. The DSG eCM
             creates an entry per each downstream channel provided in
             the DCD message. An entry is deleted when removed from the
             DCD message."
    INDEX { dsgIfStdDsgChannelListIndex }
    ::= { dsgIfStdDsgChannelListTable 1 }

DsgIfStdDsgChannelListEntry ::=  SEQUENCE {
    dsgIfStdDsgChannelListIndex      Unsigned32,
    dsgIfStdDsgChannelListFrequency  Unsigned32
    }

dsgIfStdDsgChannelListIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The unique identifier for entries in this table"
    ::= { dsgIfStdDsgChannelListEntry 1 }

dsgIfStdDsgChannelListFrequency OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "Hertz"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The downstream channel center frequency of this entry."
    ::= { dsgIfStdDsgChannelListEntry 2 }

--
-- Notification Definitions
--

dsgIfStdUpstreamEnabledNotify NOTIFICATION-TYPE
    OBJECTS {
            docsDevEvLevel,
            docsDevEvId,
            docsDevEvText,
            ifPhysAddress,
            docsIfCmCmtsAddress,
            docsIfDocsisBaseCapability,
            docsIfCmStatusDocsisOperMode,
            docsIfCmStatusModulationType
           }
    STATUS      current
```

```
    DESCRIPTION
            "Indicates the eCM is being instructed to have the upstream
            transmitter enabled. This notification is sent after CM
            registration.
            Note that the objects docsIfDocsisBaseCapability,
            docsIfCmStatusDocsisOperMode and
            docsIfCmStatusModulationType may not be supported in some
            situations (e.g., for 1.1 CMs in 1.0 mode these objects are
            optional). If that is the case, the above varbind objects
            are indicated as noSuchName or noSuchObject for
            SNMPv1 and SNMPv2 notification PDUs respectively."
    ::= { dsgIfStdNotifications 1 }

dsgIfStdUpstreamDisabledNotify NOTIFICATION-TYPE
    OBJECTS {
            docsDevEvLevel,
            docsDevEvId,
            docsDevEvText,
            ifPhysAddress,
            docsIfCmCmtsAddress,
            docsIfDocsisBaseCapability,
            docsIfCmStatusDocsisOperMode,
            docsIfCmStatusModulationType
           }
    STATUS      current
    DESCRIPTION
            "Indicates the CM is being instructed to have the upstream
            transmitter disabled. This notification is only sent when
            the CM is registered and prior to disable the upstream
            transmitter. Note that the objects
            docsIfDocsisBaseCapability, docsIfCmStatusDocsisOperMode
            and docsIfCmStatusModulationType may not be supported in
            some situations (e.g., for 1.1 CMs in 1.0 mode these objects
            are optional). If that is the case the above varbind
            objects are indicated as noSuchName or noSuchObject for
            SNMPv1 and SNMPv2 notification PDUs respectively."
    ::= { dsgIfStdNotifications 2 }

dsgIfStdTdsg2TimeoutNotify NOTIFICATION-TYPE
    OBJECTS {
            docsDevEvLevel,
            docsDevEvId,
            docsDevEvText,
            ifPhysAddress,
            docsIfCmCmtsAddress,
            docsIfDocsisBaseCapability,
            docsIfCmStatusDocsisOperMode,
            docsIfCmStatusModulationType
           }
    STATUS      current
    DESCRIPTION
            "Notifies that the eCM has a timeout Tdsg2.
            Note that the objects docsIfDocsisBaseCapability,
            docsIfCmStatusDocsisOperMode and
            docsIfCmStatusModulationType may not be supported in some
            situations (e.g., for 1.1 CMs in 1.0 mode these objects are
            optional). If that is the case the above varbind objects
            are indicated as noSuchName or noSuchObject for
            SNMPv1 and SNMPv2 notification PDUs respectively."
    ::= { dsgIfStdNotifications 3 }

--
-- Conformance definitions
--
dsgIfStdConformance  OBJECT IDENTIFIER ::= { dsgIfStdMib 2 }
dsgIfStdCompliances  OBJECT IDENTIFIER ::= { dsgIfStdConformance 1 }
dsgIfStdGroups       OBJECT IDENTIFIER ::= { dsgIfStdConformance 2 }


dsgIfStdBasicCompliance MODULE-COMPLIANCE
    STATUS      current
```

```
    DESCRIPTION
            "The compliance statement for DOCSIS Set-top Gateway eCMs."

MODULE -- dsgIfStdMIB

 -- mandatory groups

MANDATORY-GROUPS {
                 dsgIfStdConfigGroup,
                 dsgIfStdNotifyGroup
                 }
    ::= { dsgIfStdCompliances 1 }


dsgIfStdConfigGroup OBJECT-GROUP
    OBJECTS {
            dsgIfStdDsgMode,
            dsgIfStdTdsg1,
            dsgIfStdTdsg2,
            dsgIfStdTdsg3,
            dsgIfStdTdsg4,
            dsgIfStdTdsg1Timeouts,
            dsgIfStdTdsg2Timeouts,
            dsgIfStdTdsg3Timeouts,
            dsgIfStdTdsg4Timeouts,
            dsgIfStdTunnelFilterApplicationId,
            dsgIfStdTunnelFilterMacAddress,
            dsgIfStdTunnelFilterIpAddressType,
            dsgIfStdTunnelFilterSrcIpAddr,
            dsgIfStdTunnelFilterSrcIpMask,
            dsgIfStdTunnelFilterDestIpAddr,
            dsgIfStdTunnelFilterDestPortStart,
            dsgIfStdTunnelFilterDestPortEnd,
            dsgIfStdTunnelFilterPkts,
            dsgIfStdTunnelFilterOctets,
            dsgIfStdTunnelFilterTimeActive,
            dsgIfStdTunnelFilterTunnelId,
            dsgIfStdDsgChannelListFrequency
            }
    STATUS      current
    DESCRIPTION
            "A collection of configuration elements provided in DCD
            messages and DSG operations."
    ::= { dsgIfStdGroups 1 }

dsgIfStdNotifyGroup NOTIFICATION-GROUP
    NOTIFICATIONS { dsgIfStdUpstreamEnabledNotify,
                    dsgIfStdUpstreamDisabledNotify,
                    dsgIfStdTdsg2TimeoutNotify
                    }
    STATUS      current
    DESCRIPTION
            "The collection of DSG notifications that the eCM reports
             as part of the Set-top device"
    ::= { dsgIfStdGroups 2 }
END
```

Annex C

Format and content for DSG eCM event, SYSLOG, and SNMP trap extensions

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

This annex is an extension of Annex D Format and Content for Event, SYSLOG, and SNMP Trap (normative) of [ANSI/SCTE 79-2]. The eCM MUST conform to the requirements of [ANSI/SCTE 79-2] Section 7.4, Fault management, pertaining to these events, unless otherwise explicitly indicated in this annex.

C.1 DSG eCM event extensions description

"CM event" is used in this clause to reference Annex D [ANSI/SCTE 79-2].

The DSG eCM Events are based on the DSG notifications described in 5.4.2.1 and 5.4.2.2, which can be categorized in 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 (SSDI) for a DSG eCM when the eCM does not support this DOCSIS feature (see C.1.2).

NOTE – Herein, the abbreviation CC is used to refer to the DSG 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 clause C.2.

Table C.1/J.128 – DSG notifications and eCM events relations

Notification direction	Notification	DSG eCM event error code set
DSG CC → eCM	Start DSG Basic Mode (Filter these MAC Addresses)	G01.0
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 → 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
DSG eCM → CC	Entering One-way Mode	G04.1

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 subclauses.

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 two DOCSIS sub-processes, DOWNSTREAM ACQUISITION, and OBTAIN UPSTREAM PARAMETERS.

The DSG extensions for DOWNSTREAM ACQUISITION use Error Code Set G03, while the DSG extensions for OBTAIN UPSTREAM PARAMETERS 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/J.128 – 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 Basic Mode		G01.0	71000100	
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	
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	

Table C.2/J.128 – DSG DOCSIS events extensions

Process	Sub-process	CM priority	Event message	Message notes and details	Error code set	Event ID	Trap name
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	Obtain upstream parameters	Informational	2-Way OK, UCID <P1> NOTE – P1 = UCID, upstream channel ID		G04.0	71000400	
dsgInit	Obtain upstream parameters	Critical	Entering One-way Mode		G04.1	71000401	
SW upgrade general failure							
SW Upgrade	SW upgrade general failure	Notice	DOCSIS SSD not supported		G05.1	71000500	

Annex D

Delivery of MPEG-2 sections in the broadcast tunnel

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., ITU-T Rec. J.94) are sent on the DSG Broadcast Tunnel, then these sections MUST be encapsulated 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 as one section per UDP datagram, where a section MUST NOT exceed a size of 4096 bytes.

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

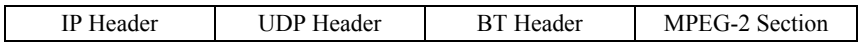


Figure D.1/J.128 – Section encapsulation

Table D.1/J.128 – 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 table, all segments except the last MUST be of equal size and SHOULD be the maximum size possible without exceeding the MTU. Reassembly of segments is the responsibility of the DSG Client. The DSG Server SHOULD minimize segmentation where possible.

Informative 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 the 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 J.94 and EAS Alert Message 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.

Appendix I

Parsing the MIB in the DSG agent

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

This appendix 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 appendix differs from the normative MIB documentation, the MIB documentation predominates.

The figure shows nine tables:

- dsgIfClassifierTable;
- dsgIfTunnelTable;
- dsgIfTunnelGrpToChannelTable;
- dsgIfDownstreamTable;
- dsgIfClientIdTable;
- dsgIfVendorParamTable;
- dsgIfChannelListTable;
- dsgIfTimerTable;
- docsQosServiceClassTable (actually in the DOCS-QOS-MIB).

Numbers in parentheses (51) indicate a TLV type as shown in Table 5-1, "Summary of DCD TLV Parameters". This notation is used throughout the rest of this appendix [DOCSIS RFI] as an aid to tracking text relevant to specific TLVs. The TLV types are documented in Annex C of the [DOCSIS RFI] Recommendation.

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

Table I.1/J.128 – Mapping table 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	dsgIfTunnelGrpUcidList

Table I.1/J.128 – Mapping table TLVs and MIB objects

TLV type	Table 5-1 name	MIB object/(or other method)
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
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 appendix 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 us 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. Start assembling a DCD message using index {IfIndex} and finding one row in the dsgIfDownstreamTable.

It is 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.

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 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.

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 Recommendation. 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), DSG UCID List (dsgIfTunnelGrpUcidList), 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 UCID List (50.3) – Using the value of dsgIfTunnelGrpUcidList 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 is worth noting here that the dsgIfTunnelTable contains an object for dsgIfTunnelServiceClass. This object does not contribute data for the DCD message. It is 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).

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 dsgIfClassSrcIpPrefexLength. 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.

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 in 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 (actually in the DOCS-QOS-MIB);
- dsgIfDownstreamTable;
- dsgIfTunnelGrpToChannelTable;
- dsgIfTunnelTable;
- dsgIfClassifierTable.

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 I.2 show the flow of data, as indicated by the notation "Data flow >>" in the top left.

Figure I.2 was drawn using the table copied directly from Figure I.1. The top row shows four different classifiers. While these four classifiers all have the same structure as 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 I.2, namely:

- docsQosServiceClassTable;
- dsgIfClientTable;
- dsgIfVendorParamTable;
- dsgIfChannelListTable;
- sgIfTimrTable.

Since these tables are largely used to populate individual tables that are shown in Figure I.2, they have been left out of the figure to keep the drawing cleaner. When using this graphical method to design a MIB, do not 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. Do not 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 a 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 5 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 3 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 4 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.

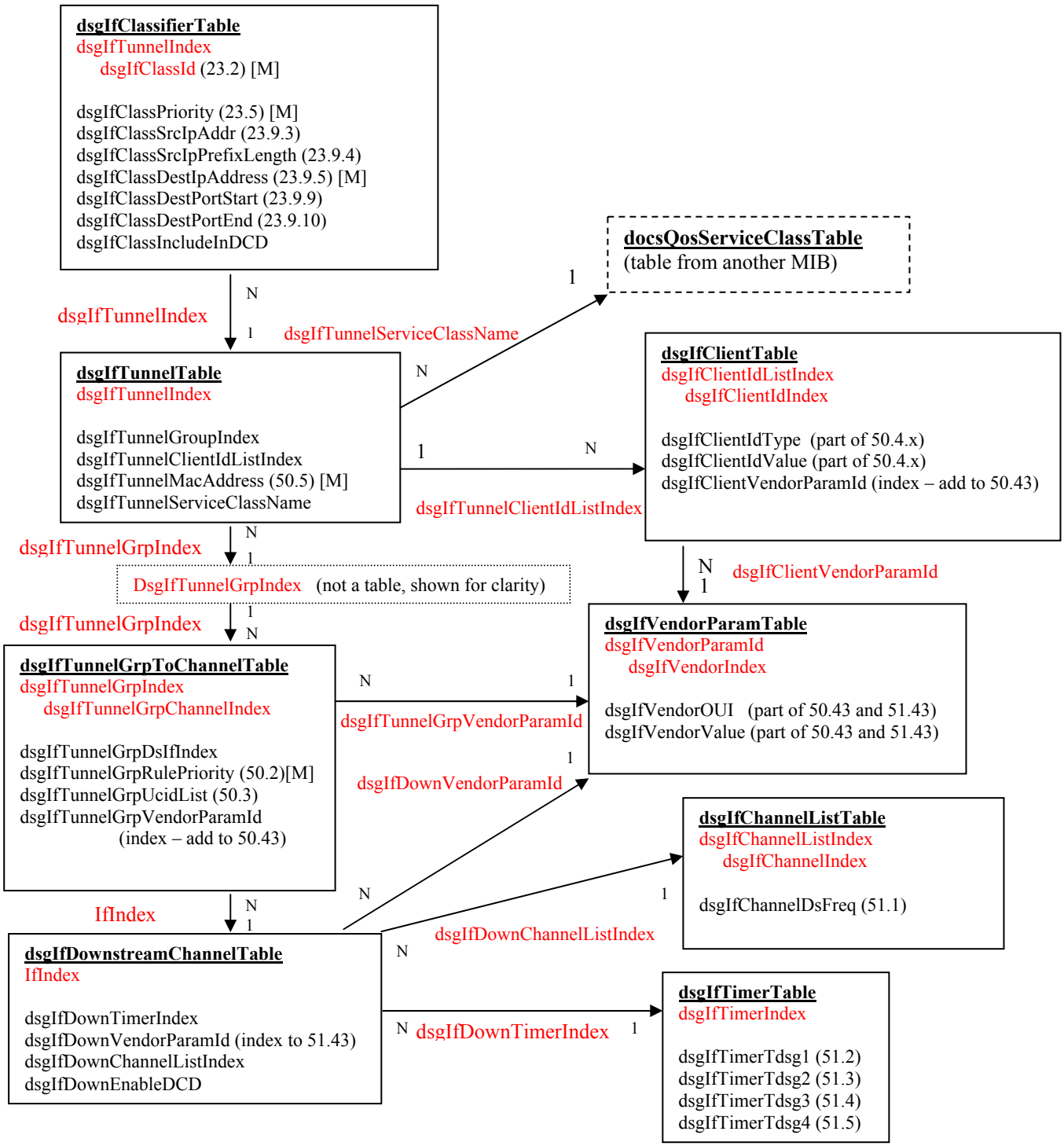
dsgIfTunnelTable – This table will have 3 entries, one for each tunnel, with indexes [1] through [3].

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

Figures I.3, I.4, I.5, and 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/J.128 – MIB structure

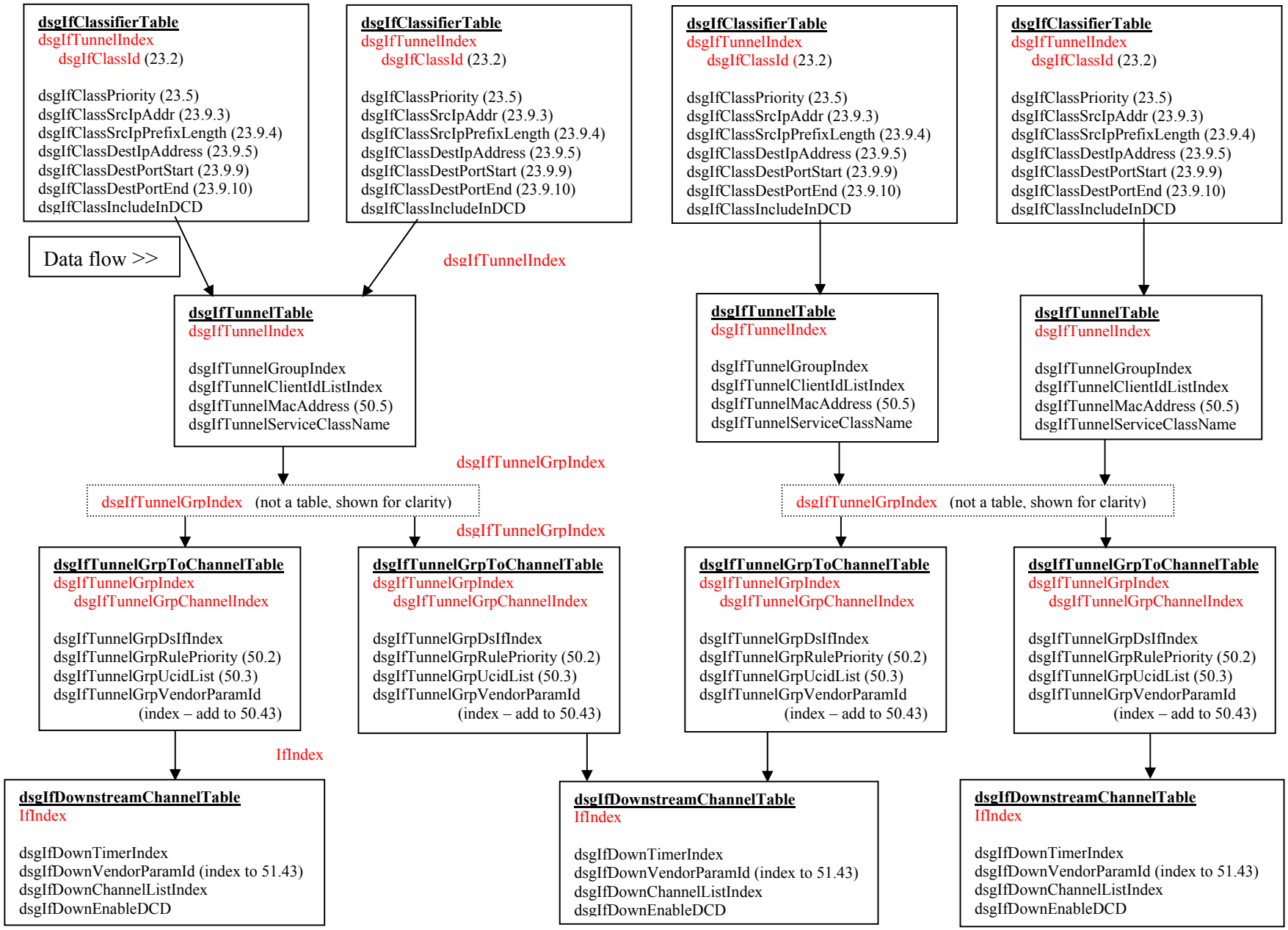


Figure I.2/J.128 – Example of designing

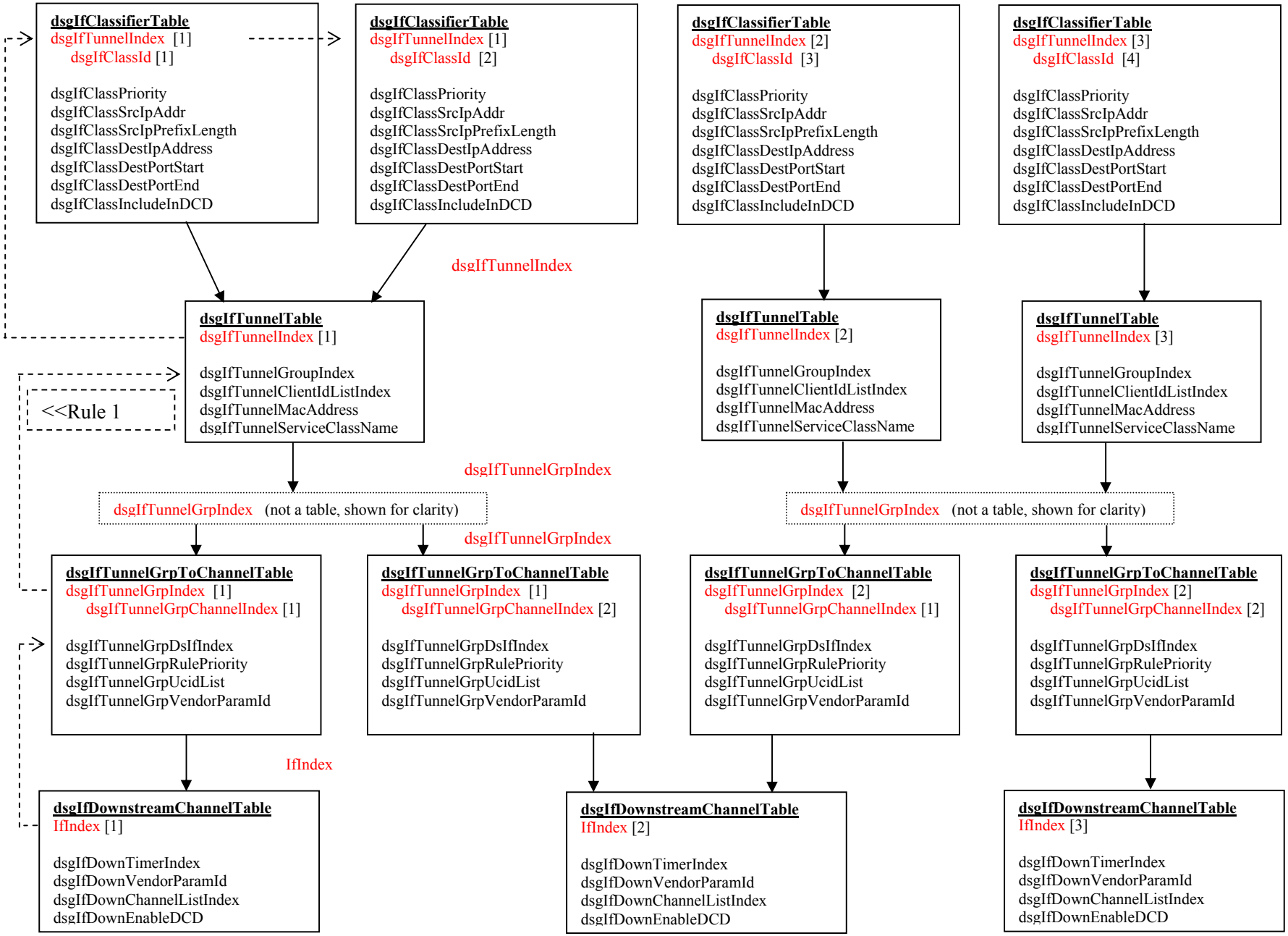


Figure I.3/J.128 – DS1, Rule 1 tunnels

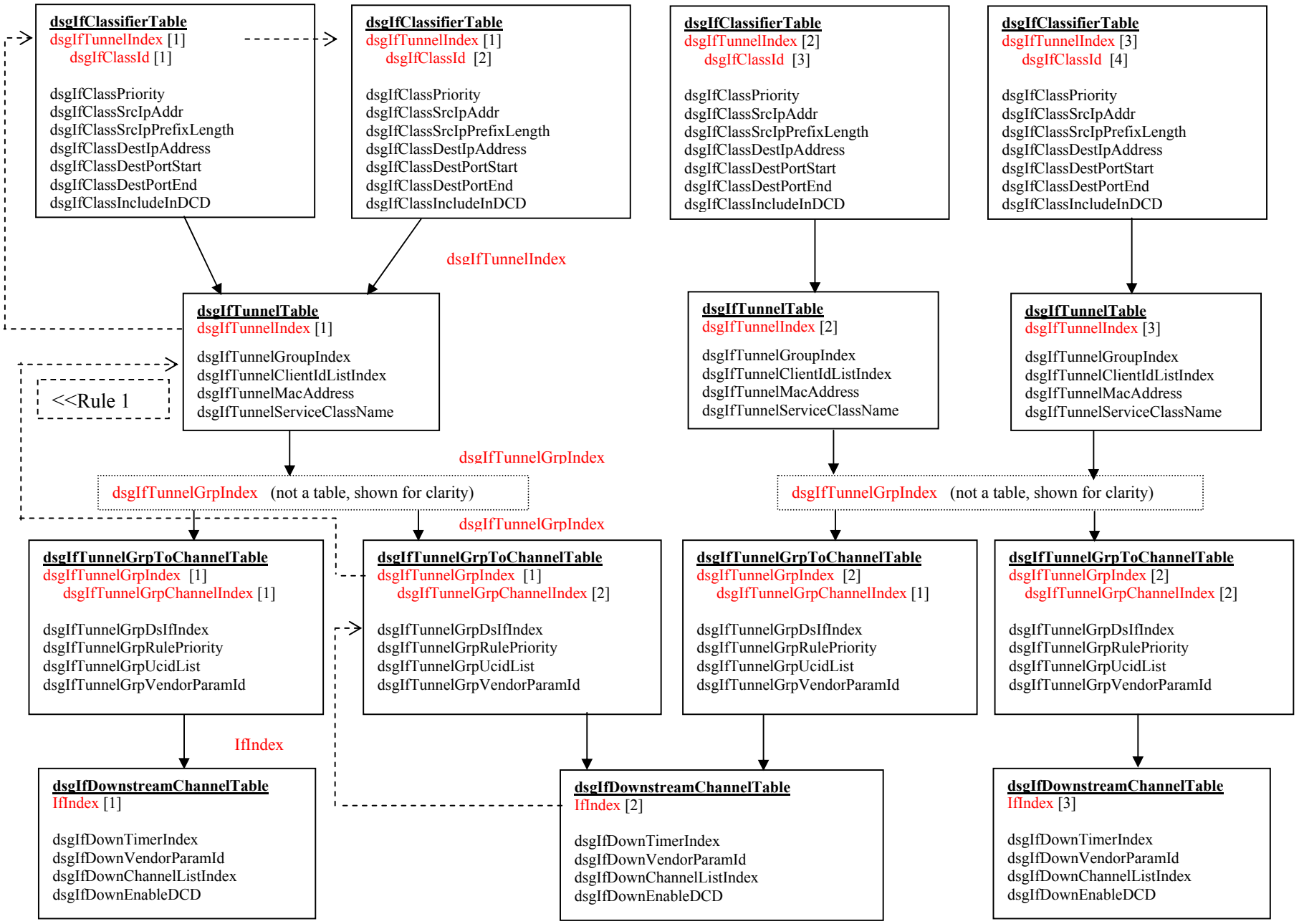


Figure I.4/J.128 – DS2, Rule 1

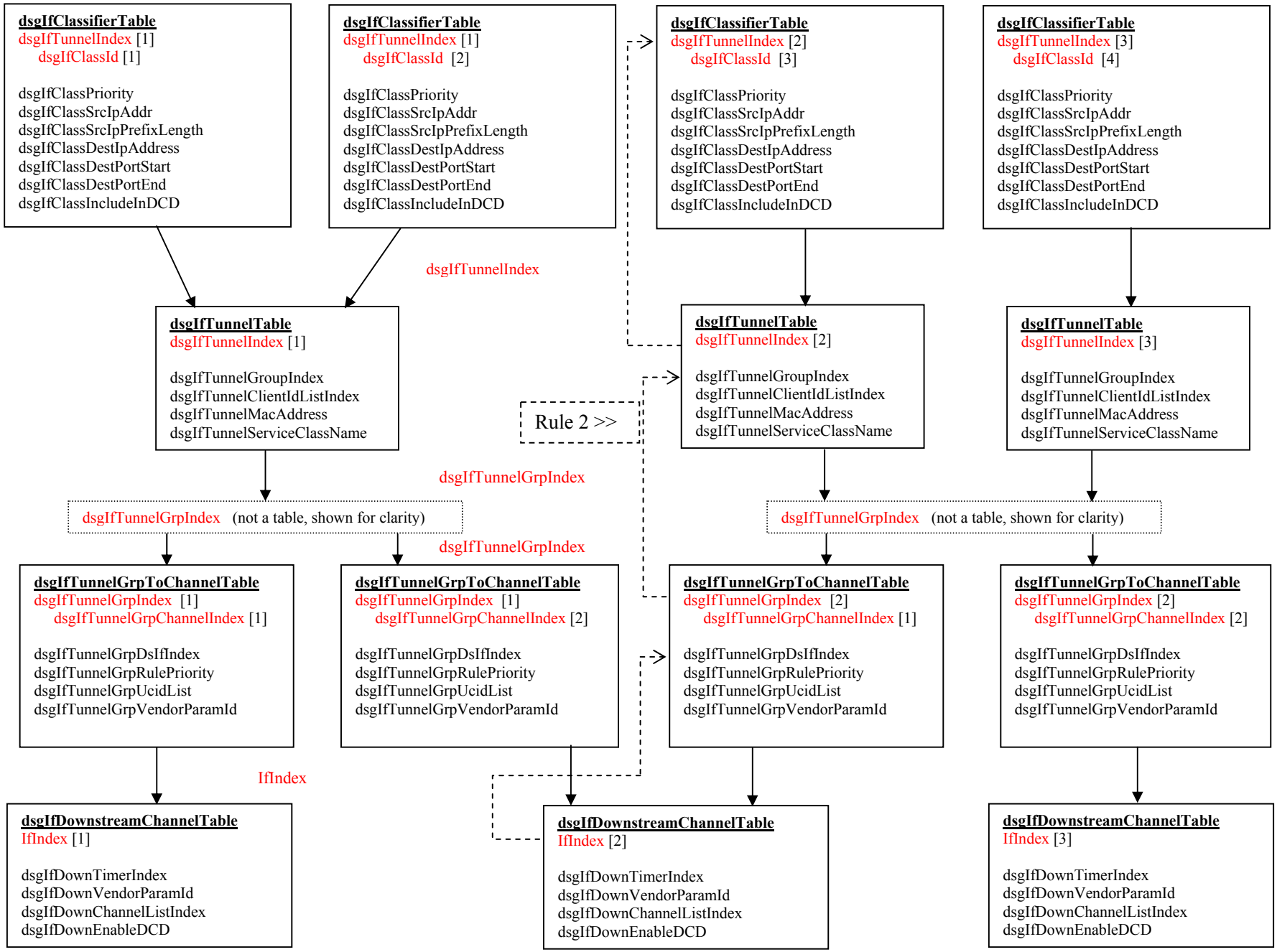


Figure I.5/J.128 – DS2, Rule 2

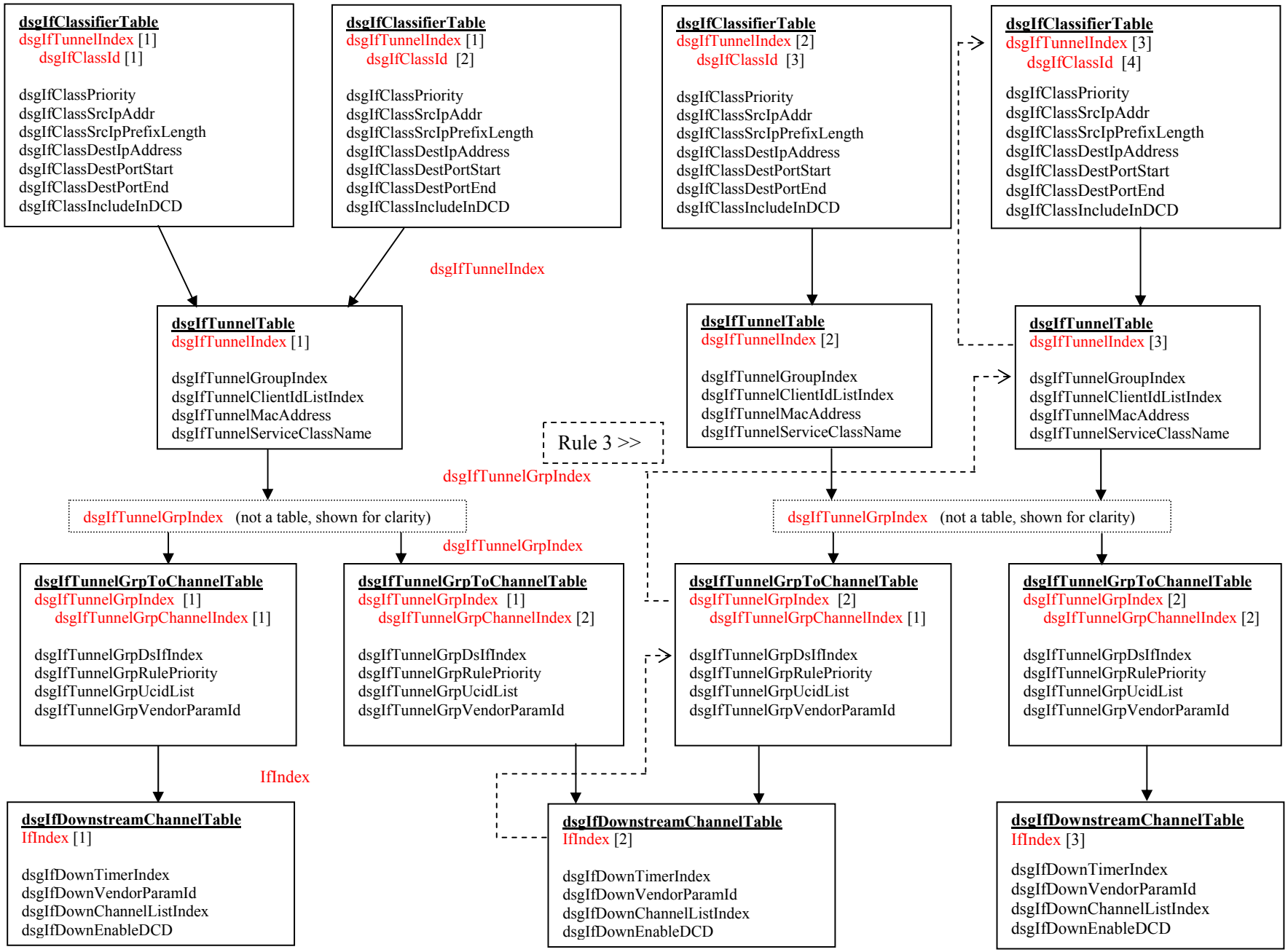


Figure I.6/J.128 – DS2, Rule 3

BIBLIOGRAPHY

[OC-CC-IF] OpenCable™ CableCARD™ Interface Specification, OC-SP-CC-IF-I18-041119, November 19, 2004, http://www.opencable.com/

[OC-HOST-CFR] OpenCable™ Host Device 2.0 Core Functional Requirements, OC-SP-HOST2.0-CFR-I02-041119, http://www.opencable.com/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2006