DOCSIS 3.0 Cable Modem IP Verification

Major Project Report

By

SHAH ARPAN BHINESHKUMAR

09mec019

Department Of Electronics and Communication Engineering

Institute Of Technology

Nirma University Of Science And Technology

Ahmedabad-382481

May-2011

DOCSIS 3.0 Cable Modem IP Verification

Major Project Report

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Electronics and Communication

(VLSI Design)

By

SHAH ARPAN BHINESHKUMAR

09mec019

Guided By

Prof. Usha Mehta

Department Of Electronics And Communication Engineering

Institute Of Technology

Nirma University Of Science And Technology

Ahmedabad-382481

May-2011

Declaration

This is to certify that

i) The thesis comprises my original work towards the degree of Master of Technology in Electronics and communication (VLSI Design) at Nirma University and has not been submitted elsewhere for a degree.

ii) Due acknowledgement has been made in the text to all other material used.

Shah Arpan Bhineshkumar

CERTIFICATE

This is to certify that the M.Tech Major Project Report entitled *DOCSIS 3.0 Cable Modem IP Verification* submitted by **SHAH ARPAN BHINESHKUMAR** (09mec019) towards the partial fulfillment of the requirements for the **Sem. IV** of Master of Technology (Electronics and Communication) in the field of **VLSI Design** of Institute of Technology, Nirma University, Ahmedabad, is the record of the work carried out under our supervision and guidance. The work submitted has in our opinion reached a level required for being accepted for examination. The result embodied in this project work to the best of our knowledge has not been submitted to any other University or Institute for the award of any degree.

Date: Place: Ahmedabad

Mrs. Annu Gupta Senior Design engineer, HVD-HED IP Verification, STMicroelectronics, Gr.Noida.	Prof. Usha Mehta Associate Professor, Institute of Technology, Nirma University, Ahmedabad.	Dr. N. M. Devashrayee PG Coordinator, Institute of Technology, Nirma University, Ahmedabad.
Prof. A. S. Ranade HOD, Electrical Department, Institute of Technology, Nirma University, Ahmedabad.		Dr. K. Kotecha Director, Institute of Technology, Nirma University, Ahmedabad.

ABSTRACT

Thesis discusses about functionality check of DOCSIS 3 standard Cable Modem IP. Packets transfer from CMTS model (Distribution Hub) to Cable Modem is called Downstream path transmission. Packets transfer from Cable Modem to CMTS model is called Upstream path transmission. This thesis discusses development of Test configuration to check Upstream path modules, Downstream path modules functionality. Have covered features in the test cases are Data suppression, Concatenation of the frame, Fragmentation of the frame, Data Encryption, High Priority and Low Priority for specific traffic, Ether type version IPv4 and IPv6 used in one test case etc. All above features are covered to check functionality of IP modules. Grey box functional verification approach is used to verify RTL of Cable Modem IP. Register programming for the above mentioned features are linked with RTL by software using Type-1 ST communication bus (32 bit Data width). Packets are transferred from DDR memory to RTL by software using Type-3 ST communication bus (128 bit Data width). Thesis discusses about error debugging work (1) Software check:- File generated by the software must be according to the test configuration. (2) RTL check:- Checking response of each IP module on waveform. Main purpose is to check functionality of each IP module (3) CMTS reference model check:- For successful verification file generated by the software and file generated by the CMTS reference model must be matched. Thesis discusses development of check script for Upstream path which compares file generated by the Upstream software and file generated by the CMTS reference model. Upstream test cases are passed for which No of packets, Destination Address, Source Address, Ether type version, Service Flow, Packet size, Each byte of the packet match correctly in both the file. Check script for Downstream path compares file generated by the CMTS reference model and file generated by the Downstream software when packets are received at DDR memory. Downstream test cases are passed if No of packets, Downstream Service ID, Each byte of the packet, Destination Address and Source Address are matched in both the files.

ACKNOWLEDGEMENT

I express my gratitude and appreciation for all those with whom I worked and interacted at Institute of Technology, Nirma University, Ahmedabad, and thank all of them for their help and co-operation.

First and foremost I would like to express my heartily gratitude **Prof. Usha Mehta**, Institute of Technology, Nirma University, for giving me the valuable guidance to carried out the project work.

I am deeply indebted to my thesis supervisor **Mrs. Annu Gupta** at the ST Microelectronics for their constant guidance and motivation. They have devoted significant amount of their valuable time to plan and discuss the thesis work. Without their experience and insights, it would have been very difficult to do quality work.

I am also thankful to **Dr. N. M. Devashrayee** (PG Coordinator), of Department of Electronics and Communication Engineering, Institute of Technology, Nirma University, Ahmedabad, for providing me all the necessary guidance throughout the term which provides lots of help in course of my Project work.

Arpan B. Shah
M.Tech Student(VLSI Design),
Institute of Technology,
Nirma University of Science and Technology.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Cable Modem Description

A Cable Modem is a device that enables to hook up PC to a local cable line and receive data at about 1.5 Mbps. This data rate far exceeds that of the prevalent 28.8 and 56 Kbps telephone modems and the up to 128 Kbps of Integrated Services Digital Network (ISDN) and is about the data rate available to subscribers of Digital Subscriber Line (DSL) telephone service. A Cable Modem can be added to or integrated with a set-top box that provides your TV set with channels for Internet access. In most cases, Cable Modems are furnished as part of the cable access service and are not purchased directly and installed by the subscriber.

A Cable Modem has two connections: one to the cable wall outlet and the other to a PC or to a set-top box for a TV set. Although a Cable Modem does modulation between analog and digital signals, it is a much more complex device than a telephone modem. It can be an external device or it can be integrated within a computer or set-top box. Typically, the Cable Modem attaches to a standard 10BASE-T Ethernet card in the computer.

All of the Cable Modems attached to a cable TV company coaxial cable line communicate with a Cable Modem Termination System (CMTS) at the local cable

TV company office. All Cable Modems can receive from and send signals only to the CMTS, but not to other Cable Modems on the line. Some services have the upstream signals returned by telephone rather than cable, in which case the Cable Modem is known as a Telco-return Cable Modem.

The actual bandwidth for Internet service over a cable TV line is up to 27 Mbps on the download path to the subscriber with about 2.5 Mbps of bandwidth for interactive responses in the other direction. However, since the local provider may not be connected to the Internet on a line faster than a T-carrier system at 1.5 Mpbs, a more likely data rate will be close to 1.5 Mpbs

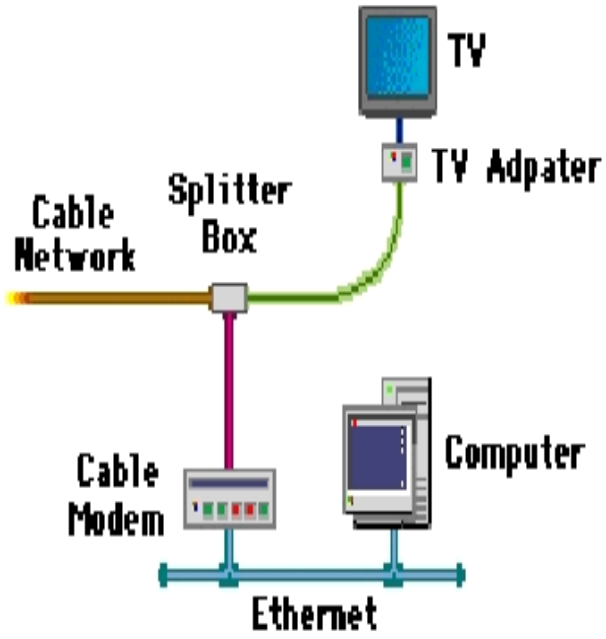

Fig. 1.1: Cable Modem Interface

1.2 DOCSIS Network and System Architecture

The elements that participate in the provisioning of DOCSIS services are shown in Figure 1-2. The CM connects to the operator's HFC network and to a home network, bridging packets between them. Many CPE devices can connect to the CM's LAN interfaces, can be embedded with the CM in a single device, or they can be separate standalone devices (as shown in Figure 1-2). CPE devices may use IPv4, IPv6 or both forms of IP addressing. Examples of typical CPE devices are home routers, set-top devices, personal computers, etc.

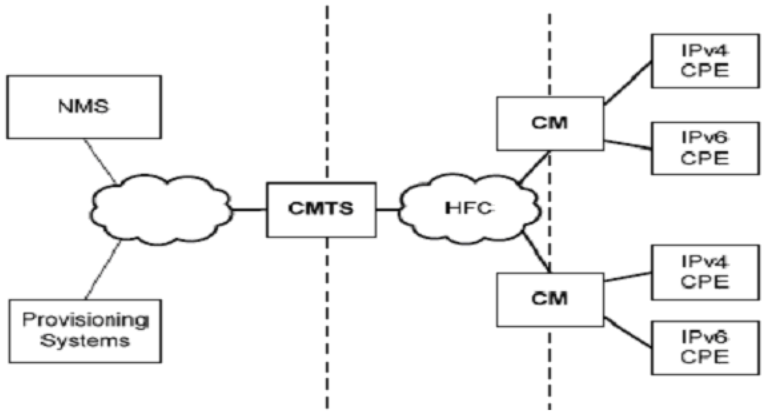

Fig. 1.2: DOCSIS Network

The CMTS connects the operator's back office and core network with the HFC network. Its main function is to forward packets between these two domains, and between upstream and downstream channels on the HFC network.

Various applications are used to provide back office configuration and other support to the devices on the DOCSIS network. These applications use IPv4 and/or IPv6 as appropriate to the particular operator's deployment. The following applications include:

1.2.1 Provisioning Systems

- The DHCP servers provide the CM with initial configuration information, including the device IP addresses, when the CM boots.
- The Configuration File server is used to download configuration files to CMs when they boot. Configuration files are in binary format and permit the configuration of the CM's parameters.
- The Software Download server is used to download software upgrades to the CM.
- The Time Protocol server provides Time Protocol clients, typically CMs, with the current time of day.
- Certificate Revocation server provides certificate status

1.2.2 Network Management System (NMS)

- The SNMP Manager allows the operator to configure and monitor SNMP Agents, typically the CM and the CMTS.
- The syslog server collects messages pertaining to the operation of devices.
- The IPDR Collector server allows the operator to collect bulk statistics in an efficient manner.

1.3 Cable Modem IP Description

Cable Modem IP is divided into three sections.

1. Bridge
2. MAC (Media Access Control)

3. Phy

One interface of IP with the Software by using ST communication bus and other interface of the IP is with the Reference model of the CMTS.

For verifying Bridge section of Cable Modem IP excel sheet is programmed. Excel sheet contains registers. Register programming in excel sheet is done according to the test configuration. Text file is generated from the excel sheet. Register programming information in this text file is linked with the System C coding of software. Software generate packets according to the test configuration. All Packets are stored in the DDR memory. Packets are transfered from DDR memory to Cable Modem IP by type 3 ST communication bus. Type 3 ST communication bus has data width of 128 bit. First section of the Cable Modem IP is Bridge. Register programming for the Bridge part is also stored in DDR memory. ST bus type 1 with data width of the 32 bit is used for the register programming transfer to the RTL.

After packets pass through Bridge modules they are stored in the DDR memory. MAC section of the Cable Modem IP receives packets from DDR memory. packets are received from the DDR memory to the MAC section of the IP. Following features are covered by the modules of MAC section and Phy section of Cable Modem IP.

MAC section send request frame to CMTS model for bandwidth allocation process for further data transmission to the RF path. The CMTS model provides grant correspondence of that request. CMTS model allocates bandwidth for the upstream data transmission and also provide timing and sync information. MAC section starts sending data for further transmission according to the information provided by the CMTS model.

1.4 Functional Verification

Functional Verification is the process used to demonstrate the functional correctness of a design. Also it is called logic verification or simulation.

There are basically three functional verification approach

1. Black box verification:- To verify a black box, one need to understand the function and be able to predict the outputs based on the inputs. Controllability and visibility of the IP is not available.

2. White box verification:- White box verification means that the internal facilities are visible and utilized by the testbench stimulus. It has complete controllability and visibility of inner module. Mostly used for unit or module level verification.

3. Grey box verification:- Grey box verification means that a limited number of facilities are utilized in a mostly black-box environment. Prediction of correct results on the interface is almost impossible without viewing an internal signal for Cable Modem IP. Some stage of controllability and visibility are there in the IP.

IP is considered as Grey box here. Grey box function verification approach is used for check. Here changing in the Register programming of RTL is done for functionality check. Register programming in the Software links with the RTL. Main thing is done during verification is changing in the Register programming of the the test cases and observe the response for them on waveform. Checking of software and checking of the RTL both are done in this case. During software check need to ensure that file generated by the software must be according to the test configuration. Software links Register programming with RTL of Cable Modem using Type 1 ST bus. Main purpose of verification is to check functionality by observing response of each module on the waveform. Response of each module must be according to the test configuration. Here we are checking functionality of each module of Bridge, MAC and Phy section. IF any design issue is found during functionality check informed to RTL provider about that bug and the location of the bug in the design. For given test case if functionality of the RTL is correct and no issue with the software than checker for the upstream path compares file generated by the software and file generated by the CMTS model finally give pass status for the test case. Check script in perl compares both the file. Perl script first parse the final genrerated by the software. Script stores Service flow,

No of packet, Destination Addresses, Source Addresses etc in the array and variables. Script parse another file generated by CMTS model it stores information of No of packet, Destination Addresses, source addresses in the array and variables. Finally decision of test case is passed or failed taken by the script after comparison of above things in both files.

Chapter 2

DOCSIS Versions and Description

2.1 Previous Versions

Prior generations of DOCSIS were commonly referred to as DOCSIS 1.0, 1.1 and 2.0. DOCSIS 3.0 is backward-compatible with equipment built to the previous specifications. DOCSIS 3.0-compliant CMs interoperate seamlessly with DOCSIS 2.0, DOCSIS 1.1, and DOCSIS 1.0 CMTSs. DOCSIS 3.0-compliant CMTSs seamlessly support DOCSIS 2.0, DOCSIS 1.1, and DOCSIS 1.0 CMs.

A CM operates in this mode when: 1) Multiple Transmit Channel (MTC) Mode is disabled; 2) the Enable 2.0 Mode configuration setting in the REG-RSP is set to 1(Enable) explicitly or by default; and 3) it operates on an upstream channel using the burst descriptors associated with IUC 9, 10, and 11 as opposed to IUC 5 and 6. A CM is enabled for DOCSIS 2.0 Mode when the Enable 2.0 Mode configuration setting in the REG-RSP is set to 1 (Enable). A CM may be enabled for DOCSIS 2.0 Mode but may not be operating in DOCSIS 2.0 Mode. When a CM has MTC Mode enabled, the CM is not considered to be in DOCSIS 2.0 Mode even if some of the upstream channels it is using are operating with post-1.1 DOCSIS physical layer mechanisms. Therefore, "DOCSIS 2.0 Mode" does not have relevance for a CM operating in MTC Mode.

2.2 DOCSIS 3.0 Key Features

DOCSIS 3.0 introduces a number of features that build upon what was present in previous versions of DOCSIS. This specification includes the following key new features for the MAC and Upper Layer Protocols Interface

Downstream Channel Bonding with Multiple Receive Channels: DOCSIS 3.0 introduces the concept of a CM that receives simultaneously on multiple receive channels. Downstream Channel Bonding refers to the ability (at the MAC layer) to schedule packets for a single service flow across those multiple channels. Downstream Channel Bonding offers significant increases in the peak downstream data rate that can be provided to a single CM.

Upstream Channel Bonding with Multiple Transmit Channels: DOCSIS 3.0 introduces the concept of a CM that transmits simultaneously on multiple transmit channels. Upstream Channel Bonding refers to the ability to schedule the traffic for a single upstream service flow across those multiple channels. Upstream Channel Bonding offers significant increases in the peak upstream data rate that can be provided to a single CM. DOCSIS 3.0 also introduces other enhancements in the upstream request-grant process that improve the efficiency of the upstream link.

IPv6: DOCSIS 3.0 introduces built-in support for the Internet Protocol version 6. DOCSIS 3.0 CMs can be provisioned with an IPv4 management address, an IPv6 management address, or both. Further, DOCSIS 3.0 CMs can provide transparent IPv6 connectivity to devices behind the cable modem (CPEs), with full support for Quality of Service and filtering.

Source-Specific Multicast: DOCSIS 3.0 supports delivery of Source-Specific IP Multicast streams to CPEs. Rather than extend the IP multicast protocol awareness of cable modems to support enhanced multicast control protocols, DOCSIS 3.0 takes a different approach. All awareness of IP multicast is moved to the CMTS, and a new DOCSIS-specific layer 2 multicast control protocol between the CM and CMTS is defined which works in harmony with downstream channel bonding and allows

efficient and extensible support for future multicast applications.

Multicast QoS: DOCSIS 3.0 defines a standard mechanism for configuring the Quality of Service for IP multicast sessions. It introduces the concept of a "Group Service Flow" for multicast traffic that references a Service Class Name that defines the QoS parameters for the service flow.

DOCSIS 3.0 defines a mechanism to increase the peak rate of upstream and downstream forwarding between the CMTS and a CM by utilizing multiple independent physical layer channels. This feature is termed channel bonding. Due to the inherent differences in the MAC layer definition for upstream transmission relative to downstream, the bonding mechanisms are themselves quite different in the two directions. This specification defines the requirements for CMs and CMTSs to support both upstream and downstream channel bonding.

DOCSIS 3.0 introduces a number of enhancements to the operation of upstream request and grant scheduling, including the ability to request in terms of bytes instead of mini-slots and to have multiple outstanding requests per upstream service flow. The set of upstream enhancements introduced with DOCSIS 3.0 is collectively called the "Multiple Transmit Channel Mode" of operation on the CM.

Additionally, DOCSIS 3.0 introduces enhancements to the way that IP multicast is handled. DOCSIS 1.1 and 2.0 required that cable modems actively participate in tracking layer-3 IP multicast group membership. DOCSIS 3.0, in contrast, provides a CMTS controlled layer-2 multicast forwarding mechanism. DOCSIS 3.0 also introduces the ability for cable operators to configure Quality of Service guarantees for multicast traffic. These features can be used to reliably deliver source-specific as well as any-source multicast sessions to clients behind the cable modem.

DOCSIS 3.0 introduces full support for IPv6, including the provisioning and management of a cable modem with an IPv6 address, and the ability to manage and transport IPv6 traffic.

This specification also includes MAC layer protocol definitions for support of additional DOCSIS 3.0 features defined in the other DOCSIS 3.0 specifications

Chapter 3

Traffic through Data Over Cable System and Theory of Operation

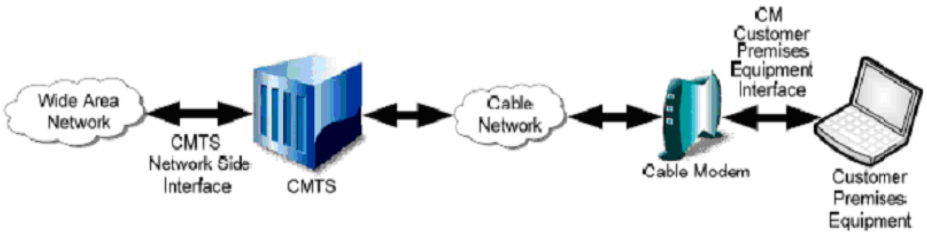

Fig. 3.1: Traffic through Data Over Cable System

3.1 CMTS (Cable Modem Termination System)

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

A CMTS is considered to be a DOCSIS network element that forwards packets between one or more Network Side Interface (NSI) ports . there are two types of CMTS:

1. **A**n "Integrated" CMTS that directly implements the NSI and RFI ports in a single network element;

2. **A** "Modular" CMTS that implements the NSI and Upstream RF Interfaces in a "Modular CMTS Core" network element and Downstream RF interfaces on an Edge QAM (EQAM) element. This section gives an overview of the CMTS model.

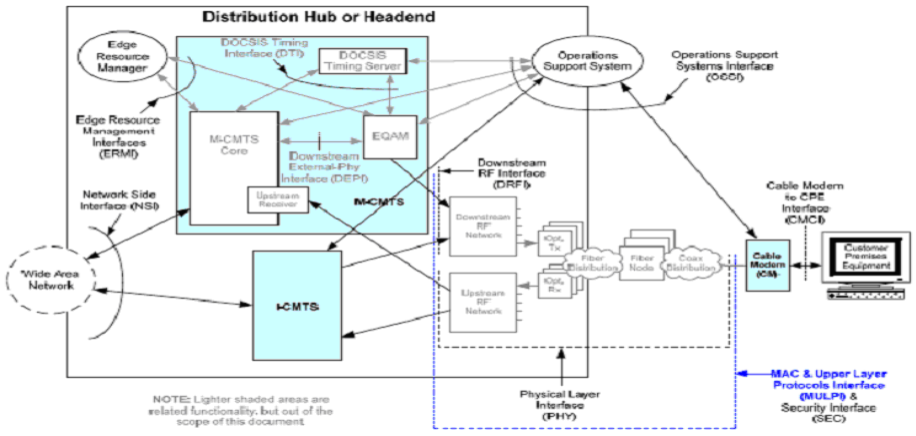

Fig. 3.2: Data-over-Cable Reference Architecture

3.1.1 Types of CMTS

3.1.1.1 Integrated CMTS

An Integrated CMTS implements a single OSSI entity (SNMP agent, IPDR exporter) for Cable Operator configuration and management of the Downstream RF Interfaces (DRFIs) and Upstream RF Interfaces (URFIs) of the CMTS.

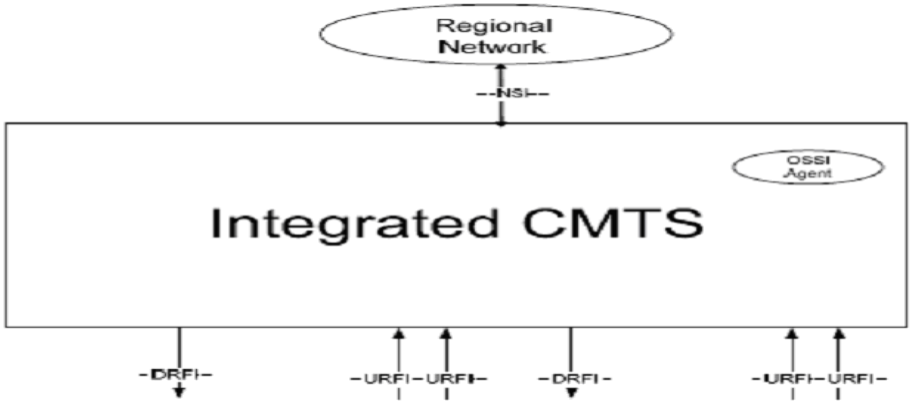

Fig. 3.3: Integrated CMTS model

3.1.1.2 Modular CMTS

Figure 3.4 depicts a Modular CMTS (M-CMTS) network diagram. The M-CMTS Core implements the Network Side Interfaces and the Upstream RF Interfaces of a CMTS. The M-CMTS Core tunnels the contents of Downstream

DOCSIS channels across a Converged Interconnect Network (CIN) to one or more Edge QAMs (EQAMs) using the DOCSIS-standardized Downstream External Physical Interface [DEPI]. The M-CMTS Core and all EQAMs are synchronized by a DOCSIS Timing Server using a standardized DOCSIS Timing Interface [DOCSIS DTI].

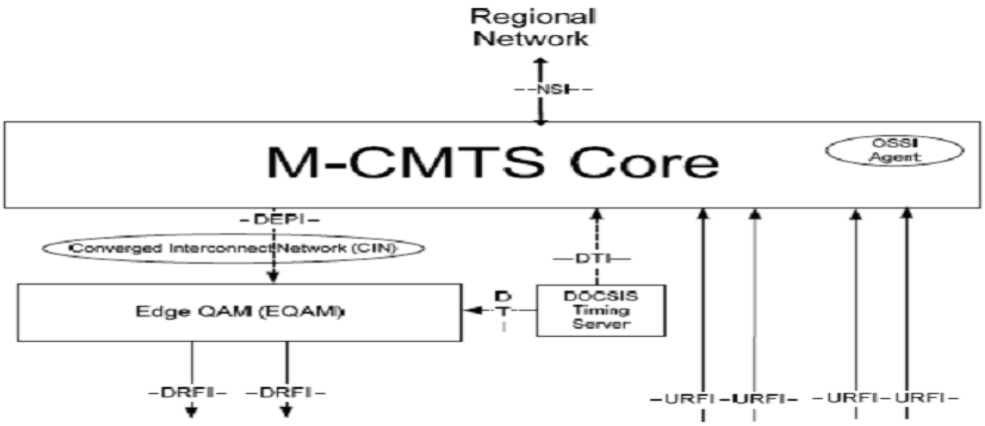

Fig. 3.4: Modular CMTS model

3.1.2 CMTS Internal Forwarding Model

Figure 3.5 depicts the logical operational model of internal packet forwarding within a CMTS

The CMTS internal forwarding model consists of two types of sub-components:

- CMTS Forwarders which forward packets with layer 2 bridging or layer 3 routing;
- MAC Domains which manage and forward data to and from Cable Modems reached by a set of Downstream and Upstream channels.

A CMTS Forwarder is responsible for forwarding packets between a Network Side Interface and the MAC Domains. In DOCSIS 3.0 the MAC Domain is not considered to forward data packets from its Upstream to its own Downstream channels; all Upstream data packets are considered to be delivered to a CMTS Forwarder. DOCSIS 3.0 leaves most details of CMTS Forwarder operation to CMTS vendor-specific implementation. DOCSIS versions 1.0, 1.1, and 2.0 required that the CMTS permit

IPv4 communication across the NSI port to CPE host(s) attached to CMs, along with IPv4 management of the CMTS and CMs themselves.

DOCSIS 3.0 adds the requirement to manage CMs with IPv6, as well as to provide IPv6 connectivity across an NSI port to CPE IPv6 hosts. DOCSIS does not specify whether the CMTS implements layer 2 or layer 3 forwarding of the IPv4 and IPv6 protocols, or prevent one protocol from being bridged and the other protocol from being routed. In addition, the DOCSIS Layer 2 Virtual Private Networking specification [DOCSIS L2VPN] standardizes transparent layer 2 forwarding between NSI ports and CM CPE interfaces, and requires the implementation of an "L2VPN" CMTS Forwarder that is distinct from the "non-L2VPN" CMTS Forwarders for IPv4/IPv6 bridging or routing.

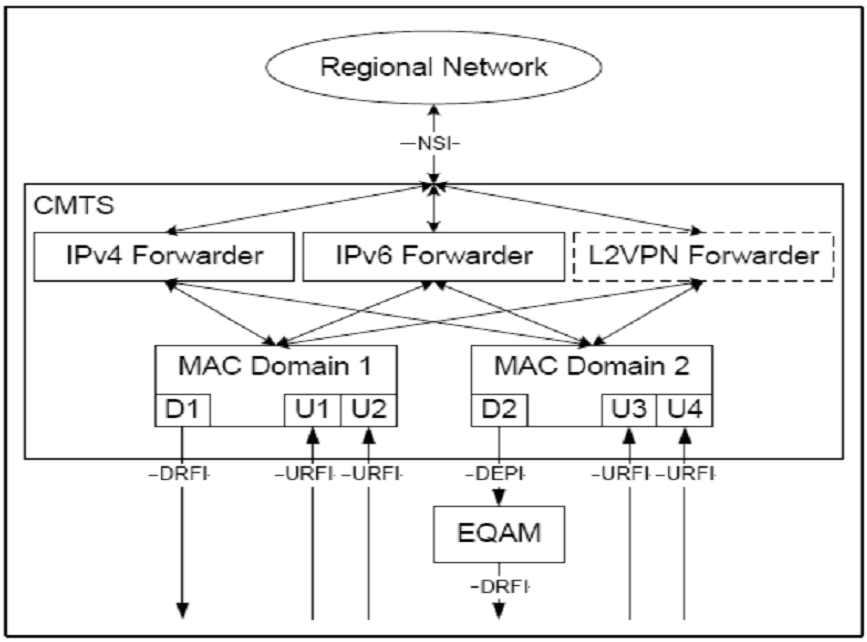

Fig. 3.5: CMTS Internal Forwarding Model

3.1.3 CMTS MAC Domain

A DOCSIS MAC Domain is a logical sub-component of a CMTS that is responsible for implementing all DOCSIS functions on a set of Downstream channels and Upstream channels. A CMTS MAC Domain contains at least one Downstream channel and at least one Upstream channel.

A MAC Domain is responsible for sending and receiving all MAC Management Messages (MMMs) to and from a set of CMs that are registered on that MAC Domain. A CM is registered to only a single MAC Domain at any given time.

A MAC Domain provides layer 2 data transmission services between the CMTS Forwarders and the set of CMs registered to that MAC Domain. The MAC Domain classifies Downstream packets into Downstream "service flows" based on layer 2, 3, and 4 information in the packets. The MAC Domain schedules the packets for each Downstream service flow to be transmitted on its set of Downstream channels.

In the Upstream direction, the MAC Domain indicates to a CMTS Forwarder component when a Layer 2 packet has been received from a particular CM. Each CMTS Forwarder component is responsible for forwarding and replicating (if necessary) Layer 2 packets between the MAC Domains and the NSI port(s) of a CMTS. All Upstream DOCSIS Layer 2 packets are delivered to a CMTS Forwarder subcomponent; the MAC Domain does not directly forward Layer 2 packets from Upstream to Downstream channels. Since the CMTS Forwarder is responsible for building the Layer 2 Ethernet header of Downstream Data PDU packets, the IPv4 ARP and IPv6 ND protocols are considered to be implemented within the CMTS Forwarder.

3.1.3.1 Downstream Data Forwarding in a MAC Domain

A MAC Domain provides Downstream DOCSIS data forwarding service using the set of Downstream channels associated with the MAC Domain. Each Downstream channel in a MAC Domain is assigned an 8-bit Downstream Channel ID (DCID). A Downstream channel itself is defined as either:

- A "Downstream (RF) Channel", representing a single-channel Downstream RF signal on a Downstream RF Port of an Integrated CMTS.

- A "Downstream M-CMTS Channel", representing a single-channel Downstream RF signal at a remote Edge QAM that is reached via a DEPI tunnel from an M-CMTS Core.

At an M-CMTS Core, the term "Downstream M-CMTS Channel" refers to the origination of a DEPI session. At an EQAM, the term "Downstream M-CMTS Channel" refers to the termination of a DEPI session

3.1.3.2 Upstream Data Forwarding in a MAC Domain

An "Upstream channel" can be used to refer to either:

- A "Physical Upstream Channel"

- A "Logical Upstream Channel" of a Physical Upstream Channel.

A "Physical Upstream Channel" is defined as the DOCSIS RF signal at a single center frequency in an Upstream carrier path.

Multiple "Logical Upstream Channels" can share the center frequency of a Physical Upstream Channel, but operate in different subsets of the time domain. Transmit opportunities for each Logical Upstream Channel are independently scheduled by the CMTS.

A MAC Domain provides Upstream DOCSIS data forwarding service using the set of logical Upstream channels associated with the MAC Domain. Each logical Upstream channel in a MAC Domain is assigned an 8-bit Upstream Channel ID (UCID).

All logical Upstream channels operating at the same frequency on an Upstream RF Interface port are contained in the same MAC Domain.

3.2 CM Model

A CM is a DOCSIS network element that forwards (bridges) layer-2 traffic between a Radio Frequency Interface (RFI) and one or more Customer Premises Equipment ports.

Data coming from Wide Area Network and moving to the Cable Modem Termination System, Cable Modem toward Customer Premises Equipment that is called Downstream path.

Data coming from Customer Premises Equipment and moving to Cable Modem, Cable Modem Termination System toward Wide Area Network. that is called Upstream path.

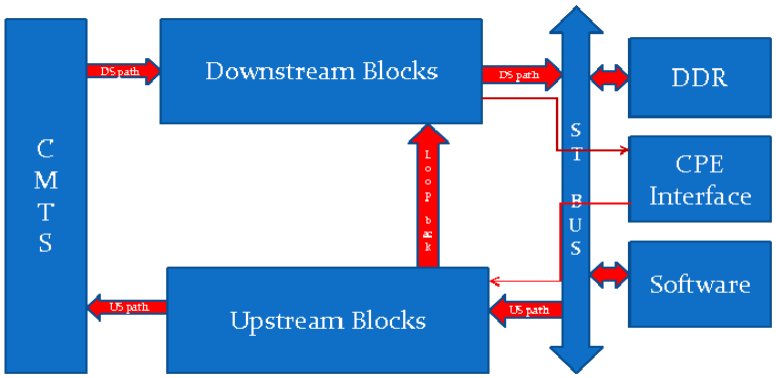

Fig. 3.6: Block Diagram

Data moving either from Wide Area Network to the Customer Premises Equipment or Customer Premises Equipment to the Wide Area Network it passes from various Cable Modem blocks. Interface of IP with the Software by using ST communication bus and other interface of the IP is with the Reference model of the CMTS.

For verifying Bridge section of Cable Modem IP excel sheet is programmed. Excel sheet contains registers. Register programming in excel sheet is done according to the test configuration. Text file is generated from the excel sheet. Register programming information in this text file is linked with the System C coding of software. Software generate packets according to the test configuration. All Packets are stored in the DDR memory. Packets are transfered from DDR memory to Cable Modem IP by type 3 ST communication bus. Type 3 ST communication bus has data width of 128 bit. First section of the Cable Modem IP is Bridge. Register programming for the Bridge part is also stored in DDR memory. ST bus type 1 with data width of the 32 bit is used for the register programming transfer to the RTL.

Following process done by the modules of Bridge section Cable Modem IP. Those information to the Bridge modules are provided by the software according to the test configuration.

1. Data suppression according to the rules which are given by the software
2. Priority give for particular service flow by providing high priority or low priority. Software serves first high priority queue.
3. Provide Limitation for the packet size
4. Provide 48 bit MAC Broadcast Destination Address and Source Address
5. Provide 48 bit MAC Multicast Destination Address and Source Address
6. Provide 48 bit MAC Unicast Destination Address and Source Address
7. Single filtering done depends on filtering condition given.
8. Multiple filtering done depends on filtering condition given.
9. Drop those packets for some condition like 48 bit MAC destination address and 48 bit MAC source address is same for the one packet.

After packets pass through Bridge modules they are stored in the DDR memory. MAC section of the Cable Modem IP receives packets from DDR memory. packets are received from the DDR memory to the MAC section of the IP. Following features are covered by the modules of MAC section and Phy section of Cable Modem IP.

1. Multiple transmission mode on or off. For DOCSIS 3.0 version of Cable Modem IP it always ON. For pre-DOCSIS version of Cable Modem IP it always OFF.

2. Selection of transmission type ATDMA, TDMA, SCDMA.

3. Fragmentation of the frame occurs in the MAC section.

4. Concatenation of the frame occurs in the MAC section.

5. Which IUC used for transmission depends on the types of transmission and version of the DOCSIS.

6. Segmentation ON or OFF. If we want to transmit data in segmented form than segmentation ON information provided here.

7. Selection of Channel type used.

8. Selection of Request frame depends. For DOCSIS 3.0 protocol queue depth based request is used when multiple transmit channel mode is enable.

MAC section send request frame to CMTS model for bandwidth allocation process for further data transmission to the RF path. The CMTS model provides grant correspondence of that request. CMTS model allocates bandwidth for the upstream data transmission and also provide timing and sync information. MAC section starts sending data for further transmission according to the information provided by the CMTS model.

3.3 DOCSIS MAC Operation

3.3.1 Quality of service (QoS)

This section provides an overview of the QoS protocol mechanisms and their part in providing end-to-end QoS. Some of the Quality of Service related features described in this specification include:

- Packet Classification and Flow Identification
- Service Flow QoS Scheduling with a set of QoS Parameters
- Traffic Priority
- Token Bucket Rate Shaping/Limiting
- Reserved (Guaranteed) Data Rate
- Latency and Jitter Guarantees
- Both Static and Dynamic QoS Establishment
- Two-Phase Activation Model for Dynamic QoS

This version of DOCSIS introduces a new feature to control prioritized data forwarding through the CM. This version of DOCSIS also defines a mechanism to configure QoS for Downstream multicast traffic. The various DOCSIS protocol mechanisms described in this document can be used to support Quality of Service (QoS) for both Upstream and Downstream traffic through the CM and the CMTS.

The principal mechanism for providing QoS is to classify packets traversing the DOCSIS RF interface into a Service Flow and then to schedule those Service Flows according to a set of QoS parameters. A Service Flow is a unidirectional flow of packets that is provided a particular Quality of Service. The requirements for Quality of Service include:

- A configuration and registration function for pre-configuring per-CM QoS Service Flows and traffic parameters.
- A signaling function for dynamically establishing QoS-enabled Service Flows and traffic parameters.
- CMTS MAC scheduling of Downstream and Upstream Service Flows based on QoS parameters for the Service Flow.
- CM and CMTS traffic-shaping, traffic-policing, and traffic-prioritization based on QoS parameters for the Service Flow.
- Classification of packets arriving from the upper layer service interface to a specific active Service Flow.
- Grouping of Service Flow properties into named Service Classes, so upper layer entities and external applications (at both the CM and CMTS) can request Service Flows with desired QoS parameters in a globally consistent way.
- Assignment of Service Flows to particular Upstream or Downstream channels that reach the CM based on elements of the QoS parameter set for the Service Flow.

The primary purpose of the Quality of Service features defined here is to define transmission ordering and scheduling on the Radio Frequency Interface. However, these features often need to work in conjunction with mechanisms beyond the RF interface in order to provide end-to-end QoS or to police the behavior of Cable Modems.

Specifically, the following behaviors are required in DOCSIS 3.0:

- In the Upstream and Downstream direction the CMTS can be configured to overwrite the Diff Service Field setting.
- The queuing of Downstream PDU packets may be prioritized at the CMCI output of the CM by the Traffic Priority.

Additional behaviors are permitted, for example:

- The queuing of packets at the CMTS in the Upstream and Downstream directions may be based on the Diff Serv Field.
- Downstream packets can be reclassified by the CM to provide enhanced service onto the subscriber-side network.

Service Flows exist in both the Upstream and Downstream direction, and may exist without actually being activated to carry traffic. Service Flows have a 32-bit Service Flow Identifier (SFID) assigned by the CMTS. All Service Flows have an SFID; active and admitted Upstream Service Flows are also assigned a 14-bit Service Identifier (SID) or one or more SID Clusters (which comprise a SID Cluster Group). At least two Service Flows must be defined in each Configuration file: one for Upstream and one for Downstream service. The first Upstream Service Flow describes the Primary Upstream Service Flow, and is the default Service Flow used for otherwise unclassified traffic, including both MAC Management Messages and Data PDUs. Similarly, the first Downstream Service Flow describes the Primary Downstream Service Flow, which is the default Service Flow in the Downstream direction. Additional Service Flows can be defined in the Configuration file to provide additional QoS services.

Incoming packets are matched to a Classifier that determines to which QoS Service Flow the packet is forwarded. The Classifier can examine the LLC header of the packet, the IP/TCP/UDP header of the packet or some combination of the two. If the packet matches one of the Classifiers, it is forwarded to the Service Flow indicated by the SFID attribute of the Classifier. If the packet is not matched to a Classifier, it is forwarded on the Primary Service Flow.

3.3.2 Individual and Group Service Flows

Downstream Service Flows may be distinguished by whether they provide service to an individual CM or a group of CMs:

- Individual Service Flows are defined as Service Flows created by the Registration process of a single CM or a Dynamic Service Addition process to a single CM.

- Group Service Flows are created by the CMTS and may or may not be communicated to the CM.

A CMTS classifies packets offered for forwarding by an individual CM to an Individual Service Flow. Individual Service Flows (and their classifiers) apply to only packets forwarded by the CMTS to hosts (embedded or non-embedded) reachable through a single CM. Individual Service Flow traffic is usually addressed to a unicast Destination MAC Address learned by the CMTS as reachable through that CM. However, that with Layer 2 Virtual Private Network service [DOCSIS L2VPN], traffic with a non-unicast Destination MAC Address will also be forwarded through a single CM by requiring such traffic to be encrypted in the BPI Primary SAID of the CM.

Group Service Flows are intended primarily for traffic with a non-unicast Destination MAC Address, such as ARP broadcasts and Downstream IP multicasts. A CMTS could send a Downstream packet with a unicast Destination MAC Address on a Group Service Flow. One example is when the CMTS does not know to which CM the single Destination MAC Address is attached.

3.3.2.1 Channel Bonding

1. **Downstream Channel Bonding:**

   In order to provide peak Downstream data rates in excess of 100Mbps to customers, while maintaining interoperability with legacy CMs, DOCSIS 3.0 introduces a mechanism by which the CMTS dynamically distributes Downstream packets over a set of Downstream channels for delivery to a single CM. Each Downstream channel in the set is a 6 MHz or 8 MHz (depending on region) MPEG Transport channel, consistent with those used in previous versions of DOCSIS. Each packet is tagged with a sequence number so that proper data

sequencing is not lost if there are differences in latency between the channels in the set.

The CM, in turn, has multiple receivers and is tuned to receive all of the channels in the set. The CM re-sequences the Downstream data stream to restore the original packet sequence before forwarding the packets to its CPE port(s). The term "Downstream channel bonding" means the distribution of packets from the same service flow over different Downstream channels. A "Downstream Bonding Group" (DBG) refers to the group of Downstream

Channels over which the CMTS distributes the packets of a Downstream service flow. The term "Downstream Bonding Group" is intended to refer to a set of two or more Downstream channels, although during transition periods only a single channel may be defined or operational in a Downstream Bonding Group. Downstream to provide the DSID value and the packet's sequence number specific to that DSID. The use of a DSID to identify a particular packet stream sequence allows DOCSIS 3.0 CMs to filter Downstream packets based on the DSID value and resequence only those packets intended to be forwarded through the CM.

The particular set of Downstream channels on which a CM receives, distributed sequenced packets with a DSID label is called the Resequencing Channel Set of the DSID at that CM.

The stream of packets identified by a DSID is independent of a CMTS service flow. For example, the CMTS may utilize a single sequence number space (and one DSID) for one or more Service Flows forwarded to the same CM. Alternatively, the CMTS may classify different IP multicast sessions to the same Group Service Flow, in which case packets transmitted from the same group service flow could be transmitted with different DSIDs.

The set of Downstream channels assigned to an individual CM is called its Receive Channel Set, and is explicitly configured by the CMTS. The CMTS

assigns a CM's bonded service flows to Downstream Bonding Groups that have channels in the CM's Receive Channel Set.

The CMTS assigns a Receive Channel Set to a CM by sending the CM a Receive Channel Configuration. The Receive Channel Set is the complete list of Downstream Channels that were defined in the Receive Channel Configuration.

The CMTS controls the Receive Channel Set for each CM, and in doing so, can optimally support deployments where the aggregate data capacity needed (in terms of numbers of Downstream channels) exceeds the number of channels that a single CM can receive. In this situation, the CMs can be dynamically balanced across the available Downstream channels by manipulation of their respective Receive Channel Sets. For example, a particular fiber node could be configured to carry six Downstream channels, yet each individual CM might only have the capability to receive four Downstream channels simultaneously. By dynamically balancing the load (via Receive Channel Set assignments),

the CMTS can provide the aggregate data capacity of all 6 Downstream channels. To support future CM hardware designs and limitations, DOCSIS 3.0 provides a flexible means for a CM to advertise its receiver characteristics (Receive Channel Profiles) and any limitations on Receive Channel Set assignment.

2. **Upstream Channel Bonding:**

   Cable operators would like to be able to provide higher Upstream bandwidth per user in order to compete with FTTx offerings and provide services to small businesses.

   The Cable Operators have stated an objective of 100Mbps Upstream throughput from a single user or group of users. Given the current impracticality of using very high orders of modulation (e.g., 1024-QAM) and wider channels in the Upstream, the only way to achieve the desired throughput using cable is to allow a user to transmit on multiple Upstream channels simultaneously. This

concept of a CM transmitting on multiple Upstream channels simultaneously is new to DOCSIS and is referred to as Upstream Channel Bonding in that the smaller bandwidth Upstream channels can be bonded together to create a larger bandwidth pipe

The actual bonding process is controlled by the CMTS as part of the scheduling process via grants. The CM makes a request for bandwidth for a given service flow on one of the service flow's associated Upstream channels. The CMTS then chooses whether to grant the request on one or more of the channels associated with that service flow. The CMTS is responsible for allocating the bandwidth across the individual Upstream channels. This centralized control allows the system the best statistical multiplexing possible and allows the CMTS to do real-time load balancing of the Upstream channels within a bonding group. When the CM receives grants over multiple channels, it divides its transmission according to the transmit time for each grant and the size of each grant. The CM places an incrementing sequence number in the traffic transmitted in each grant. The grants may be staggered in time across any or all of the channels and may require the CM to transmit on all bonded Upstream channels simultaneously. The CMTS then uses the sequence number in the traffic to reconstruct the original data stream

3.3.3 Traffic Segmentation Overview

The Upstream channels within the bonding group may have very different physical-layer characteristics. One channel may be 1280 ksps with QPSK data regions and TDMA framing while another may be 5.12 Msps with 64 QAM data regions and S-CDMA framing. The CMTS decides how to segment the bandwidth based on the bandwidth requested by the CM and the other traffic on the Upstream channels. Figure shows an example of four Upstream TDMA channels with varying mini-slot sizes. Each row in the figure represents bandwidth across a single Upstream channel.

The vertical lines demarcate the mini-slot boundaries. The letters and shadings in the figure represent the service flow to which the block of bandwidth has been allocated by the CMTS. Blocks E and D represent small grants to different flows supporting voice service. In this example, the CMTS chooses to grant A's request by using bandwidth on only Channels 1 and 2. Similarly the CMTS chooses to grant B's request by using only Channels 3 and 4. The CMTS chooses to grant C's request spread across all four Upstream channels.

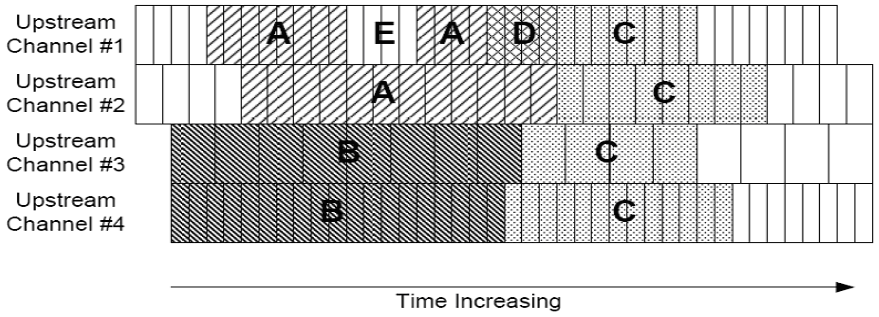

Fig. 3.7: Traffc segment overview

Each contiguous group of mini-slots assigned to the same service flow on the same channel in the figure becomes a segment. Thus the grant to service flow B consists of 2 segments and the grant to service flow C consists of 4 segments. Since the grant to service flow A on Channel 1 consists of two portions separated by the grant to service flow E, the overall grant to service flow A consists of 3 segments: two on Channel 1 and one on Channel 2. Each of these segments is treated like a legacy grant from the standpoint of physical layer overhead. Each segment will need a preamble at the beginning and, if TDMA transmission is used, guard time at the end. The physical

layer properties of each segment are specified by the channel's physical parameters and the segment's burst parameters. The set of channels over which the CMTS may segment bandwidth for a given service flow is called the service flow's Upstream Bonding Group. The Upstream Bonding Group is used by the CMTS to know on which channels it may allocate grants to a service flow.

3.4 Multicast Operation

DOCSIS 3.0 enhances support for IP Multicast with the addition of new features such as Source Specific Multicast, Quality of Service support for multicast traffic, IPv6 multicast, and bonded multicast. These enhanced IP Multicast features enable cable operators to offer various IP Multicast-based multimedia services, such as Internet Protocol Television (IPTV), over the DOCSIS network. The following new features are added in DOCSIS 3.0 while maintaining backwards compatibility with the DOCSIS 2.0 multicast mode of operation:

- Forwarding of Source Specific Multicast (SSM) traffic for CPE devices
- Support for bonded multicast traffic
- Provisioning of Quality of Service (QoS) for multicast traffic
- Support for IPv6 multicast traffic including Neighbor Discovery (ND), Router Solicitation (RS), etc.
- Explicit tracking of CPEs joined to a multicast group at the CMTS to aid load balancing, usage tracking, billing, etc.

DOCSIS 3.0 simplifies the operation of a Cable Modem(CM) by removing the IGMP snooping requirement of DOCSIS 1.1 and 2.0 (in some cases), instead of extending the use of IGMP snooping to support the above mentioned new features. The CM transparently forwards IGMP/MLD messages received from clients to the CMTS.

A new CMTS-initiated layer-2 control mechanism is defined that configures the forwarding of Downstream multicast packets to specific interfaces on the CM. The CMTS labels all multicast packets with a DSID From the CMTS perspective, a DSID identifies a set of CMs intended to receive the same multicast packets.

The CMTS communicates to a CM a DSID and associated group forwarding attributes, such as the set of CM interfaces to which these DSID-labeled multicast packets need to be forwarded. The same mechanism of DSID based filtering and forwarding is used for pre-registration as well as post-registration well-known IPv6 multicast traffic, such as Neighbor Discovery (ND) and Router Solicitation (RS). The CMTS can optionally encrypt multicast packets belonging to a particular multicast session using a Security Association (SA) communicated to a CM

3.5 Network and Higher Layer Protocols

At the Network Layer DOCSIS requires the use of Internet Protocol version 4 and version 6 for transporting management and data traffic across the HFC link between the CMTS and the CM.

As described above the CMTS could perform MAC Layer bridging or Network Layer routing of data traffic, while the CM only performs MAC layer bridging of data traffic. However both CMTS and CM are Network Layer and Transport Layer aware. Specifically, the CM and CMTS support classifying user traffic, based on Network Layer and Transport Layer criteria, for purposes of providing Quality of Service and packet filtering.

Additionally, DOCSIS requires use of the following Higher Layer Protocols for operation and management of the CM and CMTS:

- SNMP (Simple Network Management Protocol)
- TFTP (Trivial File Transfer Protocol), which is used by the modem for downloading operational software and configuration information.

- DHCP (Dynamic Host Configuration Protocol) IPv4 and IPv6, frameworks for passing configuration information to hosts on a TCP/IP network

3.6 CM and CPE Provisioning and Management

3.6.1 Initialization, Provisioning and Management of CMs

During initialization, the CM goes through a number of steps before becoming fully operational on the DOCSIS network, but at a high level comprises four fundamental stages:

- Topology resolution and physical layer initialization,
- Authentication and encryption initialization,
- IP initialization
- Registration (MAC layer initialization).

In the first stage, topology resolution and physical layer initialization, the CM acquires a single Downstream channel (either via a stored last-known-good channel, or by scanning the Downstream channel map) and receives broadcast information from the CMTS that provides it with enough information to identify what set of Downstream channels are available to it, as well as what Upstream channels might be available. The CM then attempts to initialize the Upstream physical layer by "ranging" on a selected Upstream channel. Via a series of attempts and alternative channel selections, the CM succeeds in contacting the CMTS and completing the ranging process. At this point, the CMTS has located the CM in the plant topology (i.e., is aware of what Downstream channels and Upstream channels physically reach the CM) and has established two way communication via a single Downstream/Upstream channel pair. While this section has referred to the first stage in terms of physical layer initialization, a provisional MAC layer initialization has been performed, with the full initialization of the MAC layer being deferred to the final stage.

The second stage, authentication and encryption initialization, involves the CM sending its X.509 digital certificate (including the CM's RSA public key) to the CMTS for validation. If the CM has sent a valid certificate, the CMTS will respond with a message that triggers the exchange of AES (or DES) encryption keys that are used to encrypt the Upstream and Downstream data transmissions from this point forward. This "Early Authentication and Encryption" can be disabled. If so, the CM will attempt authentication and encryption initialization after the registration stage.

In the third stage, IP initialization, the CM acquires an IP address in the Cable Operator address space, as well as the current time-of-day, and a binary configuration file. DOCSIS 3.0 defines use of IP version 4 and IP version 6 and four provisioning modes: IPv4 Only, IPv6 Only, Alternate, and Dual-stack. For IPv4 Only provisioning, the CM uses DHCPv4 to acquire an IPv4 address and operational related parameters. To facilitate compatibility with existing provisioning systems, this process is identical to the DOCSIS 2.0 CM provisioning process. For IPv6 Only provisioning, the CM uses DHCPv6 to acquire an IPv6 address and operational parameters. The CM uses the IPv6 address to obtain the current time-of-day and a configuration file. For Alternate Provisioning Mode (APM) the CM combines the first two provisioning modes, IPv6 Only and IPv4 Only, in sequential order, attempting IPv6 provisioning first and, if this fails, attempting IPv4 provisioning next. In the first three provisioning modes, IPv6 Only, IPv4 Only, and APM, the CM operates with only one IP address type (v4 or v6) at any given time, and thus these modes are called single-stack modes. For Dual-stack Provisioning Mode (DPM), the CM acquires both IPv6 and IPv4 addresses and parameters through DHCPv6 and DHCPv4 almost simultaneously, prioritizing the use of the IPv6 address for time-of-day and configuration file acquisition. In this mode, the CM makes both the IPv4 and the IPv6 addresses available for management.

The fourth stage, registration, involves a three-way handshake between the CM and the CMTS in which the CM passes certain contents of the configuration file to the CMTS, the CMTS validates the contents, reserves or activates MAC layer resources based on the service provisioning information that it received, and communicates

MAC layer identifiers back to the CM. Once the CM acknowledges receipt of the CMTS's response, the MAC layer initialization is complete. After the CM completes initialization, it is a manageable network element in the operator's IP network.

The CM supports SNMP (as mentioned above), and responds to queries directed to the IP (v4 or v6) address that it acquired during initialization. DOCSIS 3.0 also supports a dual-stack operational mode in which the CM is manageable via both IPv4 and IPv6 addresses simultaneously. This mode is initialized (i.e., the CM acquires a second IP address) after the CM is operational. This feature is also intended to help provide a streamlined migration from IPv4 to IPv6 in DOCSIS networks.

3.6.2 Initialization, Provisioning and Management of CPEs

DOCSIS assumes the use of DHCP for provisioning of CPE devices. To that end the CMTS supports a DHCP relay agent which allows the operator to associate a CPE IP Address request with the subscriber Cable Modem MAC Address. This feature is also used as the basis of a mechanism that prevents spoofing of IP Addresses. DOCSIS 3.0 gives operator the option to provision CPE devices with an IPv4 or an IPv6 or both types of IP Addresses simultaneously.

3.7 Relationship to the Physical HFC Plant Topology

Here explains how DOCSIS relates the HFC Plant Topology to CM Service Groups, MAC Domains, and Bonding Groups.

3.7.1 RF Topology Configuration

CMTSs and CMs are interconnected by an RF combining and splitting network. A CMTS Downstream channel is said to "reach" a CM when its Downstream RF signal can be received by the CM. A CMTS Upstream channel is said to "reach" a CM if

the CMTS can receive the Upstream transmission by that CM. In most CMTS field deployments, the RF interconnection network is a Hybrid Fiber/Coax (HFC) network. An HFC network features a star wiring topology in which long distance fibers from a single head-end or hub location are distributed to fiber nodes throughout a geographic region. A fiber node usually terminates one or more Downstream forward carrier paths from the head-end and originates one or more Upstream reverse carrier path(s) to the head end.

The fiber node connects the Upstream and Downstream signals from the fiber onto several coaxial cable segments (typically 2 to 4 segments). Multiple Cable Modems connect their important topological feature of HFC networks is that all CMs connected to the same coax segment of a fiber node reach the same set of Downstream and Upstream channels on the CMTS(s) at the head-end.

The CMTS is configured with the physical topology of the plant. An operator configures the list of fiber nodes in the plant and configures which fiber nodes are reached by each Downstream and Upstream channel. A CMTS supports non-volatile configuration of a printable text name for each fiber node.

The operator also configures the set of MAC Domains in the CMTS, and assigns each Downstream and Upstream channel to a MAC Domain. The CMTS automatically determines the MD-CM-SGs from the topology configuration of the operator.

Figure 3.8 depicts an example RF splitting/combining network to three fiber nodes. In this example, all channels are assumed to be configured to the same MAC Domain. Although the Downstream connectivity is not typical, it has been chosen to demonstrate the flexibility of the topology configuration introduced with DOCSIS 3.0.

The CMTS implements six Downstream channels organized as two Downstream RF channels per Downstream RF Port. The D1/D2 RF port is split three ways to reach to all three fiber nodes: nodes "FN-A", "FNB", and "FN-C". The D3/D4 port reaches only the fiber node named "FN-A" The D5/D6 port reaches only fiber node named "FN-B"

The Upstream from FN-A is connected to a single Upstream RF port to which are attached receivers for separate Upstream channels U1 and U2. For FN-B and FN-C, however, the signals from their Upstream fiber are electrically combined and then split and connected to two CMTS RF ports. As a result, both fiber nodes "FN-B" and "FN-C" share the same set of Upstream channels U3/U4/U5/U6.

The CMTS implements a "Node Configuration Table" management object with which an operator configures a textual name and number for each fiber node. The CMTS implements a "Topology Configuration Table" with which the operator configures which fiber nodes are reached by which Downstream and Upstream channels. The following tables represent the logical information of a Node Configuration Table and the Topology Configuration Table to describe the topology depicted in Figure above

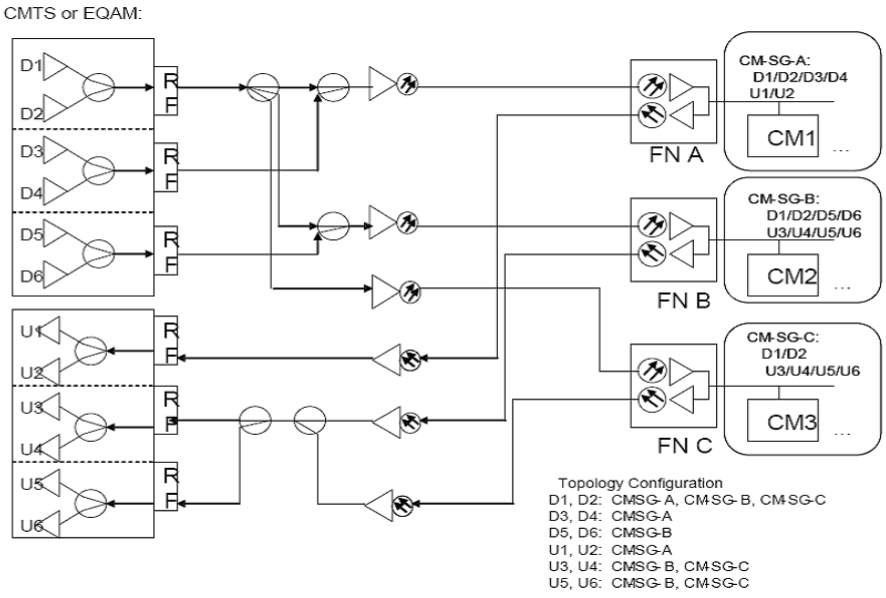

Fig. 3.8: CM Topology Configuration

Node No	Node name
1	FN-A
2	FN-B
3	FN-C

Tab. I: Node Configuration table

Node	Channel
1	D1
1	D2
1	D3
1	D4
1	U1
1	U2
2	D1
2	D2
2	D5
2	D6
2	U3
2	U4
2	U5
2	U6
3	D1
3	D2
3	U3
3	U4
3	U5
3	U6

Tab. II: Topology Configuration Table

Chapter 4

Verification Environment

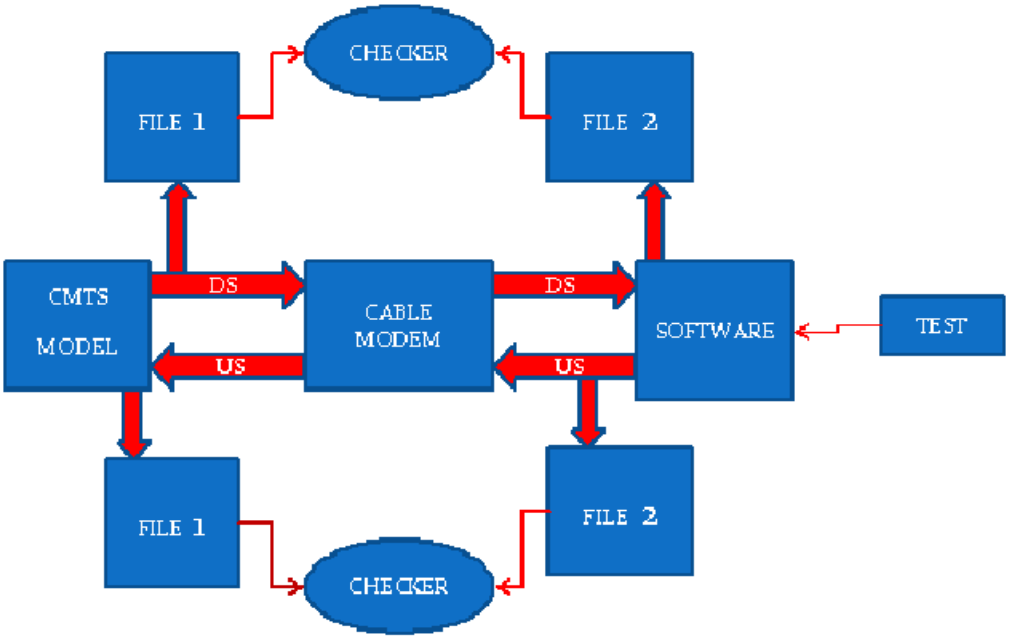

Fig. 4.1: Verifiation Environment

4.1 Verification Environment for Downstream Path

Packet moves from Wide Area Network to the customer premises equipment through CMTS, Cable Modem in Downstream path transmission. CMTS model generates one file according to the data coming from the Wide Area Network. That data contains routing information, TCP Header, IP Header, Downstream Service ID. Test configurations are made such that they verifies Downstream IP blocks. In test configuration Cable Modem registers are programmed. Register programming is linked with the RTL of Cable Modem. Software links register programming by using type 1 ST communication bus. When packet is received in DDR memory by using type 3 ST communication bus. Downstream software generates another file. Downstream check Script compares file generated by the CMTS model with file generated by the software when packet received in DDR memory. If following things are matched in both the files test case is pass otherwise it is fail:

- No of packets
- Downstream Service ID
- Packet size
- Each bytes of the packets

4.2 Verification Environment for Upstream Path

Packet moves from customer premises equipment to the Wide Area Network through Cable Modem, CMTS in Upstream path. If multiple transmit channel mode is enable than packet transfers using more than one channel. One service flow traffic divides in different channels depends on the segmentation on or off features. Software generates one dump file according to the test configuration. Actual packets are stored in DDR memory. CM sends request to software for receiving data from DDR memory. Software starts sending data from DDR memory by providing grant for request. Packets

are transfer from DDR memory to Cable Modem IP by using the ST bus type 3 communication. According to functionality covered in the test configuration packets change. Finally packets received by CMTS model. CMTS model generates another file according to the data provided to it. CMTS model Decrypt, unconcatenate, unfragment and unsuppress the data if test cases cover ,Encryption, concatenation, fragmentation, suppression features. Upstream Check script compares files generated by software and files generated by the CMTS model. Check script compares the following things in both files:

- No of packets
- Destination Address
- Source Address
- Ether Type
- Service Flow
- Packet size
- Each bytes of the packets

If RF bit is set for packet checker for Upstream path compares file generated by the software and file generated by the Cable Modem Termination System. Test cases are passed for which No of packets, Destination Address, Source Address, Ether Type, Service Flow, Packet size, each byte of the packet matches correctly. Register programming is linked with the RTL of Cable Modem by using type 1 ST communication bus.

4.3 Verification Environment for Loopback Path

In this case both Upstream modules and Downstream modules use for the packet transmission. In Ioopback test cases Upstream software generates one file according

to the test configuration. For Loopback test cases RF bit is not set in the routing field so packet does not go to RF path for further transmission by the CMTS model to the Wide Area Network or Network Side Interface. Packets are return to cpe interface through Downstream path. In this case MAC interface and CMTS model are not coming in the path because packets are return back from Bridge section of the IP. Finally Downstream software generates one file when packets are received at DDR memory. Script compares final generated by the Upstream software and file generated by the Downstream software when packet received at DDR memory.If no of send packets and no of received packets are matches than test case is pass otherwise it is fail.

Chapter 5

Test Cases Development and Error Debugging for Bridge Section of IP

5.1 Test Cases Development

5.1.1 Upstream ATDMA Test Cases and TDMA Test Cases

Test cases are made such that it verifies Upstream path IP blocks. Features of the Cable Modem are controlled by the register programming of the Cable Modem IP block modules. Some of the features included in test cases are as follow:

1. Data suppression:-

   Payload data is suppressed by the Cable Modem modules according to the mask bit is set for the particular phs rule. Payload data is unsuppressed by the CMTS model according to the phs rule.

2. Concatenation:-

   Concatenation means after completion of the first frame next frame starts soon after. CMTS modem unconcatenates the frame. The Concatenation Frame is for Pre-3.0 DOCSIS support and MUST NOT be used by CMs operating in Multiple Transmit Channel Mode.

3. Fragmentation:-

   The Fragmentation MAC Header provides the basic mechanism to split a larger MAC PDU into smaller pieces that are transmitted individually and then re-assembled at the CMTS. As such, Fragmentation is only applicable in the Upstream.

4. Encryption:-

   Encrypted data is transferred by Cable Modem if encryption on for the test cases. Encryption key is provided to CM by the CMTS model. CMTS model does decryption.

5. Priority:-

   High Priority given to the particular source traffic and low priority given for particular source traffic is controlled by the programming of the registers.

6. Maximum limitation for the packet size:-

   Packet drop if packet length is more than the packet max length allowed.

7. Control direction of flow for the packet:-

   Packet send either to send out side world or to Loopback path (CPE interface) controlled by programming of the register in Cable Modem.

8. Routing of the packet:-

   Route packets in particular queues. whether to send packet for the RF interface or to the other CPE devices control by the routing information in the packet.

9. Dropping of the packet:-

   Drop of packets for particular condition in different Cable Modem modules.

10. Filtering condition:-

Different filtering condition given in the ip filter. Final routing for the RF path or for the Loopback path is decided after the filtering done for the particular destination address.

11. Protocol:-

    Dual stack mode is supported in the DOCSIS 3.0 IP. Both IPv6 and IPv4 protocol is supported in the DOCSIS 3.0 IP.

5.1.2 Loopback Test cases

In Loopback testcases(cpe to cpe) packet transmitted by the one or more sources but packet does not go to RF path for further transmission to the Wide Area Network but it transfers to Downstream path through Loopback path. This kind of test cases developed to verify flow of traffic from one or more customer premises equipments to the other customer premises equipment. Purpose of this test cases development to verify Loopback path. Loopback path of the Cable Modem is working according to the register programming or not. some of the features are covered in these test cases are as following:

1. Filtering condition:-

   Checking of Multiple filtering condition and signal filtering condition for the Downstream filter as well as Upstream filter.

2. One source to the other sources:-

   Packet transfers from one CPE device to other CPE interface.only one Source Address and multiple Destination Addresses are used in this test cases.

3. Source from many CPEs to one CPE:-

   Packet transfers from many CPE interface to one cpe interface. Multiple Source Addresses are used and only one Destination Address is used.

4. Routing:-

   RF bit is not set for the packets in routing field. If other routing set in the configuration so packet is transfered only in the Loopback path.

5.2 Error Debugging for Bridge section

Error debugging by checking the file generated by the software is according to the test configuration or not. checking output of each Cable Modem module on waveform to check the response of it which must according to test configuration. Checking of register programming which links properly or not with the RTL of Cable Modem.

5.2.1 Software Check

Here checking of file generated by the software is according to functionality covered in the test configuration or not. Checking of the system C coding which links the text files of the test cases. Register programming is done in the test configuration linked with RTL by the software. Type-1 ST communication bus is used for that. Type-1 ST communication bus has 32 bit data width. After reading the register programming from the test configuration software itself generates file. If test case covers data suppression feature than file generated by the software contains information about suppressed data. Packets generated by the software stored in DDR memory. When request from the CM for data transmission received by the software it provides grant and starts Packet transmission from the DDR memory. Packets are transmitted from the DDR memory to Cable Modem IP by using ST bus Type 3 communication bus. Data width for the Type 3 ST communication bus is 128 bit. File generated by the software has 48 bit MAC Destination Address, 48 bit MAC Source Address, Ether type version, Source port Address, Destination port Address, Frame type must be according to the functionality covered in the test configuration. File generated by the software is linked with the RTL so if any wrong functionality taken by the software

than that functionality also effects the RTL behavior.

5.2.2 RTL Check

checking response of Bridge IP modules on waveform. For Bridge section debugging have checked response of each IP blocks according to the functionality covered in test configuration or not. Checking response of the Bridge IP blocks when covered below functionality in the Test Cases.

1. Data suppression according to the rules are given by the software
2. Priority given for particular service flow by providing high priority or low priority.
3. Limitation for the packet size
4. 48 bit MAC Broadcast Destination Address and Source Address
5. 48 bit MAC Multicast Destination Address and Source Address
6. 48 bit MAC Unicast Destination Address and Source Address
7. Single filtring condition
8. Multiple filtering condition
9. 48 bit MAC destination address and 48 bit MAC source address is same for the one packet. For these kind of test cases packets must be dropped by design.
10. Ether type version IPv4 or IPv6 or both for same test.

Chapter 6

MAC Frame Check

6.1 MAC Frame Format Check

A MAC frame is the basic unit of transfer between MAC sublayers at the CMTS and the cable modem. The same basic structure is used in both the Upstream and Downstream directions. MAC frames are variable in length. The term "frame" is used in this context to indicate a unit of information that is passed between MAC sublayer peers. This is not to be confused with the term "framing" that indicates some fixed timing relationship. There are three distinct regions to consider, as shown in Figure 6-1. Preceding the MAC frame is either PMD sublayer overhead (Upstream) or an MPEG transmission convergence header (Downstream). The first part of the MAC frame is the MAC Header. The MAC Header uniquely identifies the contents of the MAC frame. Checking of the identification for the frame is occurred properly or not. If frame is not identified properly or another frame taken instead of featured frame than it must RTL or software issue.

6.1.1 Bandwidth Allocation Check for PMD Overhead

In the Upstream direction, the PHY layer indicates the start of the MAC frame to the MAC sublayer. From the MAC sublayer's perspective, it only needs to know

the total amount of overhead so it can account for it in the Bandwidth Allocation process. The FEC overhead is spread throughout the MAC frame and is assumed to be transparent to the MAC data stream. The MAC sublayer does need to be able to account for the overhead when doing Bandwidth Allocation. Here checking of the allocated bandthwidth is for whole pdu with PHY overhead or not. If bandwidth is not allocated properly than test cases hang in middle. For these kind of bugs test cases run with the waves and check the request grant process between CMTS model and cable modem IP.

6.1.2 Checking of Order for MAC Frame Transport

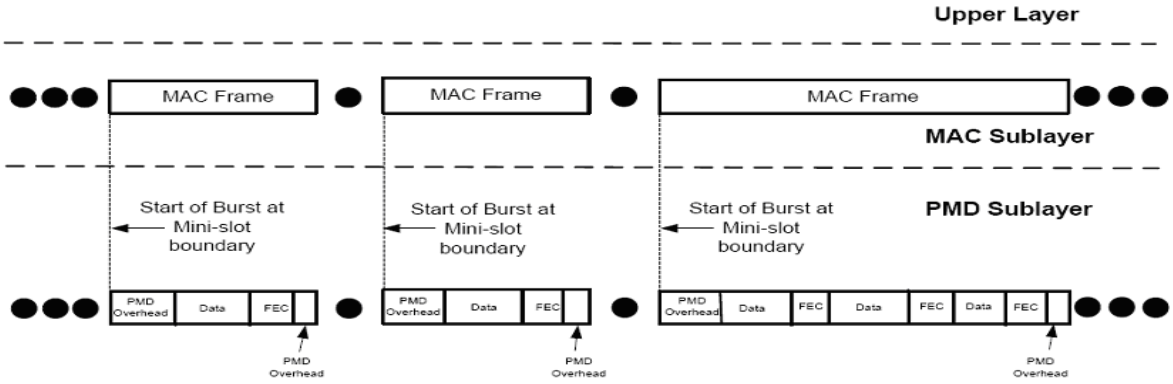

Fig. 6.1: MAC Frame Transport

CMTS PHY ensures that, for a given channel, the CMTS MAC receives Upstream MAC frames in the same order the CM mapped the MAC frames onto mini-slots. That is to say that if MAC frame X begins in mini-slot n and MAC frame Y begins in mini-slot n+m, then the CMTS MAC will receive X before it receives Y. This is true even when, as is possible with S-CDMA, mini-slots n and n+m are actually simultaneously transmitted within the PHY layer. To Check above things observe the frame sequence in file generated by the CMTS model when frame received. Compare

frame sequence in file generated by CMTS model with the mapped allocation sequence provided to CM.

6.2 MAC Header Format and HCS Check

The CM or CMTS must use the MAC Header format as shown in Figure .

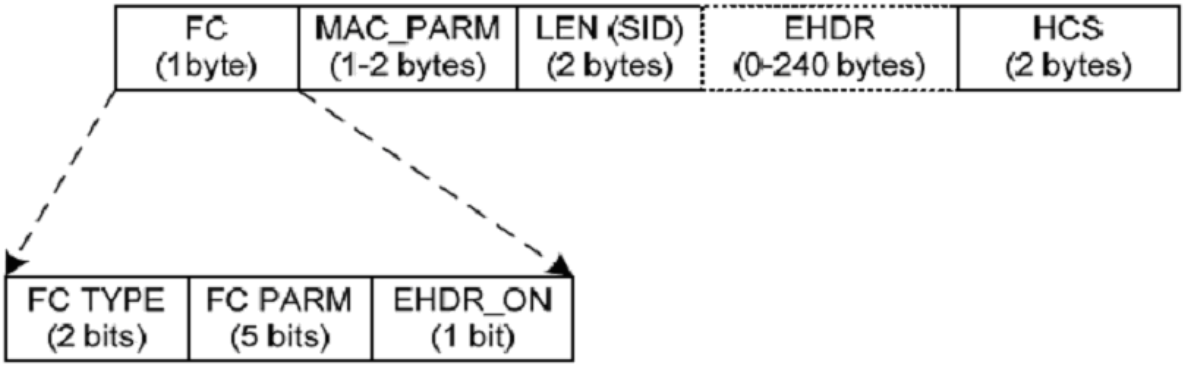

Fig. 6.2: MAC Frame Format

The CM must comply with all MAC Headers. The CMTS must comply with all MAC Headers. The Frame Control (FC) field is the first byte and uniquely identifies the rest of the contents within the MAC Header. The FC field is followed by 3 bytes of MAC control; an optional Extended Header field (EHDR); plus a Header Check Sequence (HCS) to ensure the integrity of the MAC Header. Incorrect frame error shown by the CMTS model when integrity of the MAC header is not done properly.

6.3 Packet Based MAC Frame Check

The CM or CMTS MAC sublayer must support both, a variable-length Ethernet type Packet Data PDU MAC Frame and a variable-length Ethernet type Isolation Packet

Data PDU MAC Frame. The Isolation Packet Data PDU MAC Frame is used to prevent certain Downstream packets from being received and forwarded by Pre-3.0 DOCSIS cable modems.

PDU and the Isolation Packet PDU can be used to send packets of any type (unicast, multicast and broadcast). With the exception of packets which have been subject to Payload Header suppression, the Packet PDU must be passed across the network in its entirety, including its original CRC. In the case where payload header Suppression has been applied to the Packet PDU, all bytes except those suppressed must be passed across the network by the CM and CMTS, and the CRC covers only those bytes actually transmitted.

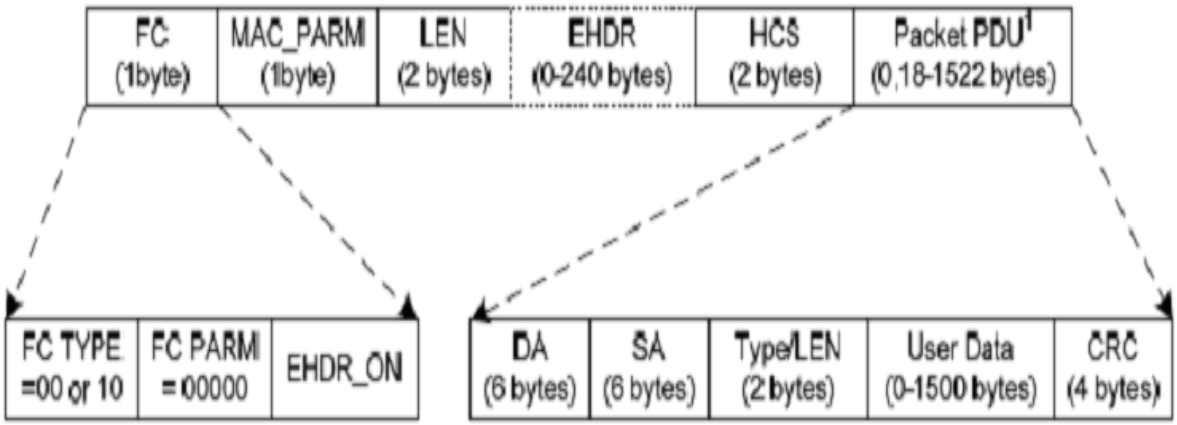

Fig. 6.3: Packet PDU or Isolation Packet PDU MAC Frame Format

Under certain circumstances it may be necessary to transmit a packet PDU MAC frame without an actual PDU. This is done so that the extended header can be used to carry certain information about the state of the service flow, e.g., a 5-byte Downstream Service Extended Header containing the current Sequence Number for a particular DSID (also known as a "null packet"), or a Service Flow Extended Header

containing the number of active grants for a UGSAD service flow. This could also happen as a result of PHS in the Upstream direction. Such a frame will have the length field in the MAC header set to the length of the extended header and will have no packet data, and therefore no CRC. Checking of value of the above parameter in header as well as in extended header by using waveform.

6.4 Checking for Discard Process in CM or in CMTS for ATM Cell MAC Frames

The FC_TYPE 0x01 is reserved for future definition of ATM Cell MAC Frames. This FC_TYPE field in the MAC Header indicates that an ATM PDU is present. This PDU must be silently discarded by CMs and CMTSs compliant with this version (3.0) of the specification. Compliant version 3.0 CM and CMTS implementations must use the length field to skip over the ATM PDU.

6.5 MAC-Specific Headers Check

There are several MAC headers which are used for very specific functions. These functions include support for Downstream timing and Upstream ranging/power adjustment, requesting bandwidth, fragmentation and concatenating multiple MAC frames.FC_PARM usage within the MAC Specific Header. Checking of MAC Specific Header if test configuration covers corresponding features. MAC-Specific header field is dependent on the features cover in the test cases. For Timing, MAC management Message, concatenation, Fragmentation, PHS suppression these all fields are different.

6.5.1 Timing Header Check

A specific MAC Header is identified to help support the timing and adjustments required. In the Downstream, this MAC Header must be used by the CMTS to

transport the Global Timing Reference to which all cable modems synchronize. In the Upstream, this MAC Header must be used by the CM as part of the Ranging message needed for a cable modems timing and power adjustments. The Timing MAC Header is followed by a Packet Data PDU. The CM must comply with Figure 6.4 for Timing Headers. The CMTS must comply with Figure 6.4 for Timing Headers.

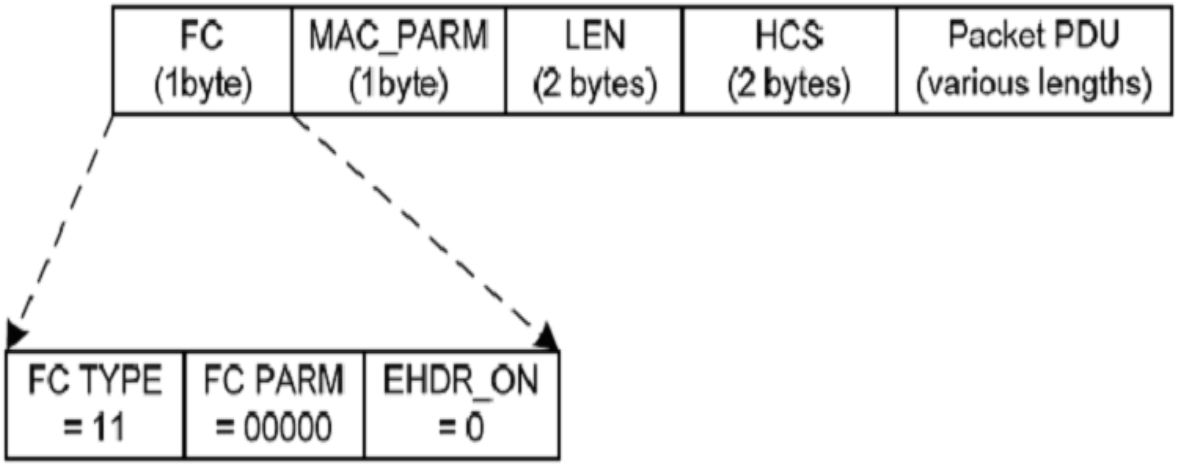

Fig. 6.4: Timing Header

6.5.2 MAC Management Header Check

A specific MAC Header is identified to help support the MAC management messages required. This MAC Header must be used by CMs and CMTSs to transport all MAC management messages . The CM must comply with Figure 6.5 for MAC Management Headers. The CMTS must comply with Figure 6.5 for MAC Management Headers.

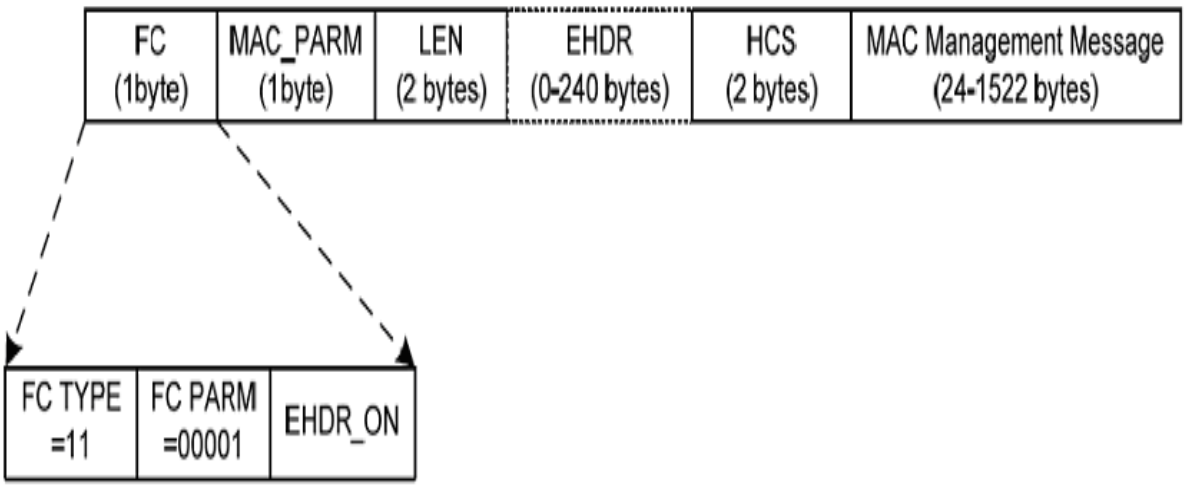

Fig. 6.5: MAC Management Header

6.5.3 Request Frame Check

The Request Frame is the basic mechanism that a cable modem uses to request bandwidth. As such, it is only applicable in the Upstream. The CM must NOT include any Data PDUs following the Request Frame. The CM must comply with Figure 6.6 for Request Frames

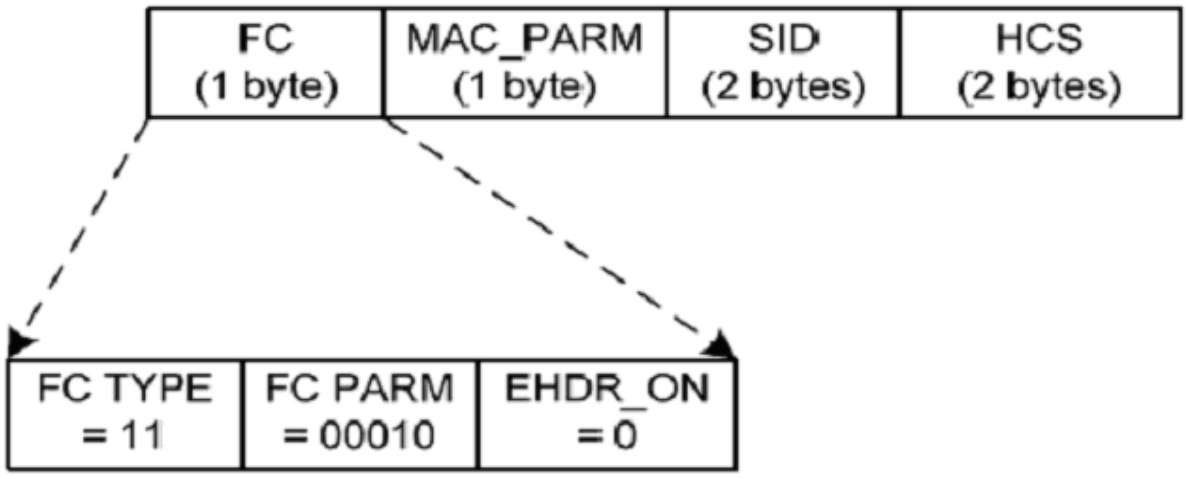

Fig. 6.6: Request Frame Header

Because the Request Frame does not have a Data PDU following it, the LEN field is not needed. The CM must replace the LEN field with a SID. The SID uniquely identifies a particular Service Flow within a given CM. The CM must specify the bandwidth request, REQ, in mini-slots. The CM must indicate the current total amount of bandwidth requested for this service queue including appropriate allowance for the PHY overhead in the MAC_PARM field.

6.5.4 Fragmentation Header Check

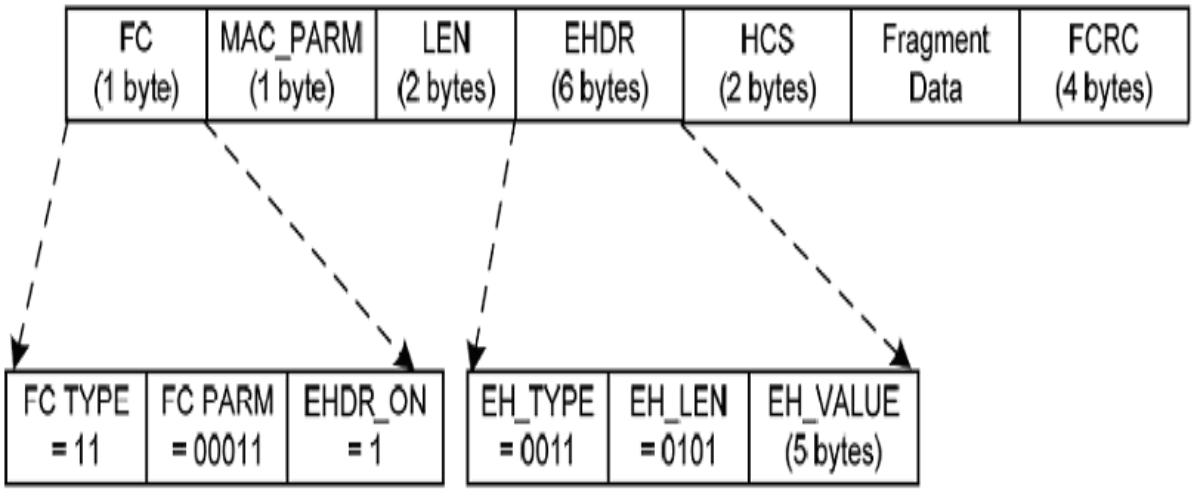

Fig. 6.7: Fragmentation MAC Header Format

The Fragmentation MAC Header provides the basic mechanism to split a larger MAC PDU into smaller pieces that are transmitted individually and then re-assembled at the CMTS. As such, Fragmentation is only applicable in the Upstream. The CM must comply with Figure 6.7 for Fragmentation MAC Headers. A compliant CM must support fragmentation. A compliant CMTS must support fragmentation. To decrease the burden on the CMTS and to reduce unnecessary overhead, fragmentation headers must NOT be used by a CM on unfragmented frames.

6.5.5 Concatenation Header Check

The MAC_PARM field in the Concatenation MAC header provides a count of MAC frames as opposed to EHDR length or REQ amount as used in other MAC headers. If the field is non-zero, then it indicates the total count of MAC Frames (CNT) in this concatenation burst. The Concatenation Frame is for Pre-3.0 DOCSIS support and must NOT be used by CMs operating in Multiple Transmit Channel Mode

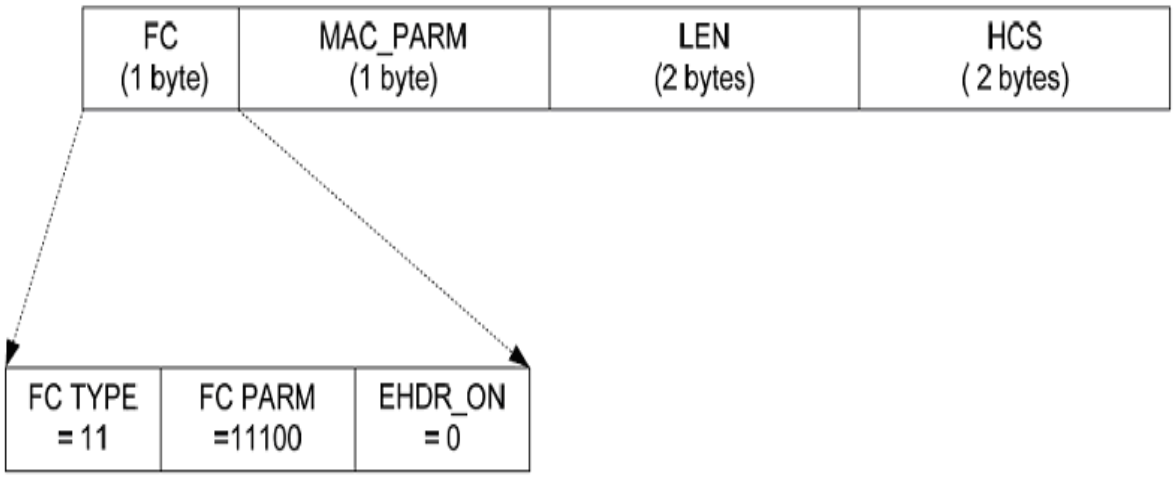

Fig. 6.8: Concatenation MAC Header Format

6.6 Extended MAC Header Check

Every MAC Header, except the Timing, Concatenation MAC Header, Request Frame, and Queue-depth Based Request Frame, has the capability of defining an Extended Header field (EHDR). Check when frames using one of the above header format Extended Header must not be present in the design. The CM or CMTS must indicate the presence of an EHDR field by the EHDR_ON flag in the FC field being set. Whenever this bit is set, then the CM or CMTS must use the MAC_PARM field as

the EHDR length (ELEN). The minimum defined EHDR is 1 byte. The maximum EHDR length is 240 bytes.

A compliant CMTS and CM must support extended headers.The CM must comply with Figure 6.10 for MAC Headers with an Extended Header. The CMTS must comply with Figure 6.10 for MAC Headers with an Extended Header.

The CM must NOT use Extended Headers in Request Frames or Queue-depth Based Request Frames. The CM and CMTS must NOT use Extended Headers in Timing MAC Headers.

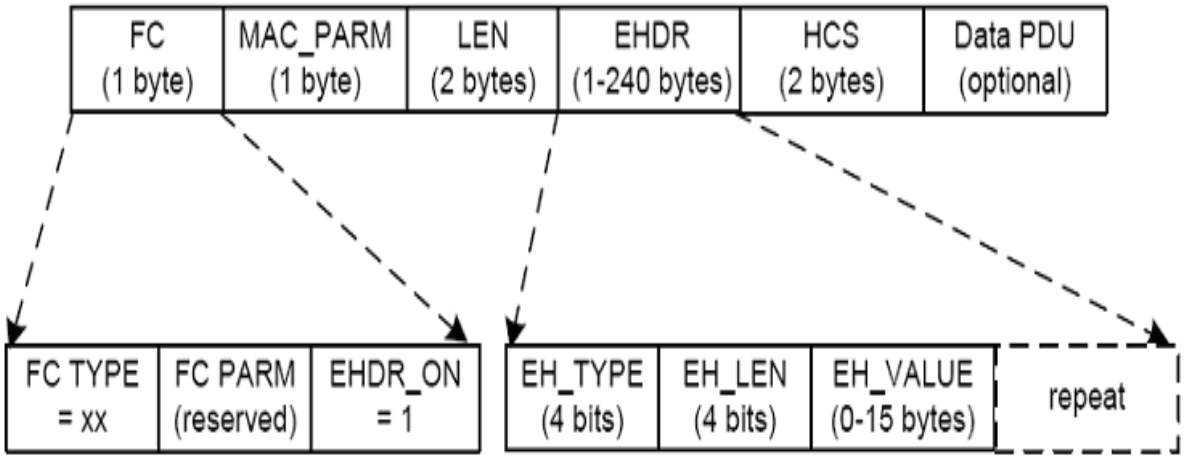

Fig. 6.9: Extended MAC Header Format

Chapter 7

MAC Protocol Operation Check

7.1 Timing and Synchronization Check

One of the major challenges in designing a MAC protocol for a cable network is compensating for the delays involved. These delays can be an order of magnitude larger than the transmission burst time in the upstream. To compensate for these delays, check for the cable modem transmissions precisely to arrive at the CMTS at the start of the assigned mini-slot. To accomplish this, two pieces of information are needed by each cable modem:

- a global timing reference check sent downstream from the CMTS to all cable modems.
- a timing offset check, calculated by the CMTS during a ranging process, for each cable modem.

7.1.1 Global Timing Reference Check

For TDMA channels, the CMTS must create a global timing reference by transmitting the Time Synchronization (SYNC) MAC management message downstream at a nominal frequency. The message contains a timestamp that exactly identifies

when the CMTS transmitted the message. Cable modems must then compare the actual time the message was received with the timestamp and adjust their local clock references accordingly. Comparison is checked in the MAC section of the IP.

For S-CDMA channels, Checking for the CMTS creates a global timing reference by transmitting the Time Synchronization (SYNC) and Upstream Channel Descriptor (UCD) MAC messages downstream at a nominal frequency.

7.1.2 Synchronization Check for CM

When the Symbol Clock Locking Indicator indicates "Locked", the cable modem achieves MAC synchronization once it has received at least two SYNC messages, received one UCD message, has locked to the downstream symbol clock, and has verified that its clock tolerances are within specified limits.

When the Symbol Clock Locking Indicator is not present and the CM selects a TDMA upstream channel, the cable modem achieves MAC synchronization once it has received at least two SYNC messages and has verified that its clock tolerances are within specified limits

7.1.3 Ranging Check

Ranging is the process of acquiring the correct timing offset such that the cable modems transmissions are aligned to the correct mini-slot boundary. In ranging check timing offset provided by CMTS such that CM upstream transmission properly aligned with mini-slot boundary. The timing delays through the PHY layer of the CM and CMTS must be relatively constant with the exception of the timing offsets, related to modulation rate changes to accommodate a Pre-3.0 DOCSIS upstream receiver implementation. For TDMA check for the any variation in the PHY delays must be accounted by the CMTS in the guard time of the upstream PMD overhead. Ranging check done for following category

7.1.3.1 Broadcast Initial Ranging

The cable modem must transmit either a Bonded Initial Ranging Request message (B-INIT-RNG-REQ), an Initial Ranging Request message (INIT-RNG-REQ), or a Ranging Request message (RNG-REQ) in a Broadcast Initial Maintenance region. A CM must transmit B-INIT-RNG-REQ if the CM detected an MDD on its candidate Primary Downstream Channel and is ranging for the first time after power-up or reinitialization on the first upstream channel A CM must transmit an INIT-RNG-REQ if the upstream is a Type 3 or a Type 4 channel rest of the cases CM must uses RNG-REQ.

7.1.3.2 Unicast Initial Ranging

The cable modem must now wait for an individual Station Maintenance or Unicast Initial Maintenance region assigned to its temporary SID (or previous primary SID if ranging as a result of a UCC, DCC, or UCD change, or Ranging SID if one has been assigned). The CM must now transmit a Ranging Request (RNG-REQ) message at this time using the temporary SID (or primary/Ranging SID, as appropriate) along with any power level and timing offset corrections. The CMTS must return another Ranging Response message to the cable modem with any additional fine tuning required. The ranging request/response steps must be repeated by the CM and CMTS, until the response contains a Ranging Successful notification or the CMTS aborts ranging. Once successfully ranged, the cable modem must join normal data traffic in the upstream.

7.2 Upstream Data Transmission

7.2.1 Upstream Bandwidth Allocation Check

The CMTS allocates bandwidth for one or more upstream channels. Bandwidth allocated to one CM may be allocated across multiple channels upon which the CM

can transmit. An upstream channel is modeled as a stream of mini-slots. The CMTS must generate the time reference for identifying these slots. The CMTS must also control access to these slots by the cable modems. For example, the CMTS may grant some number of contiguous slots to a CM for it to transmit a data PDU. CM must time its transmission so that the CMTS receives the CM's transmission in the time reference specified. Check for the CMTS receive data in time reference specified. For bandwidth allocation checking the elements of the protocol used in requesting, granting, mapping. Some types of request mentioned below

7.2.1.1 Requesting with Multiple Transmit Channel Mode Disabled

Request send by the CM to CMTS. Multiple Transmit Channel Mode is disabled, when a DOCSIS 3.0 CM is operating on a Pre-3.0 DOCSIS CMTS, or a Pre-3.0 DOCSIS CM that does not support Multiple Transmit Channel Mode is operating on a DOCSIS 3.0 CMTS.

Requests refer to the mechanism that a CM uses to indicate to the CMTS that it needs upstream bandwidth allocation. Here check the flow of request occurs between CM and AMTS for different condition. In this case Multiple Transmission Channel Mode is disabled so Queue depth based request is not used. A Request transmitted by a CM MAY come as a stand-alone Request Frame transmitter as a piggyback request in the EHDR of another Frame transmission Request Frames transmitted by a CM must be sent during one of the following intervals:

- Request IE
- Request/Data IE
- Short Data Grant IE
- Long Data Grant IE
- Adv PHY Short Data Grant IE

- Adv PHY Long Data Grant IE
- Adv PHY Unsolicited Grant IE

A piggyback request transmitted by a CM must be sent in one of the following Extended Headers:

- Request EH element
- Upstream Privacy EH element
- Upstream Privacy EH element with Fragmentation

A request transmitted by a CM must include:

- The Service ID making the request
- The number of mini-slots requested

The CM must request the number of mini-slots needed to transmit an entire frame, or a fragment containing the entire remaining portion of a frame that a previous grant has caused to be fragmented. The frame may be a single MAC frame or a MAC frame that has been formed by the concatenation of multiple MAC frames. The request from the CM must be large enough to accommodate the entire necessary physical layer overhead for transmitting the MAC frame or fragment. Check CM must not make a request that would violate the limits on data grant sizes in the UCD message or any limits established by QoS parameters associated with the Service Flow. Check CM must not request more mini-slots than are necessary to transmit the MAC frame. Check if the CM is using Short and Long Data IUCs to transmit data and the frame can fit into a Short Data Grant, the CM must use the Short Data Grant IUC attributes to calculate the amount of bandwidth to request and make a request less than or equal to the Short Data maximum Burst size. Check if the CM is using Advanced PHY Short and Long Data IUCs to transmit data and the

frame can fit into an Advanced PHY Short Data Grant, the CM use the Advanced PHY Short Data Grant IUC attributes to calculate the amount of bandwidth to request and make a request less than or equal to the Advanced PHY Short Data maximum Burst size. Check CM must have only one request outstanding at a time per Service ID. If the CMTS does not immediately respond with a Data Grant, the CM is able to unambiguously determine that its request is still pending because the CMTS must continue to issue a Data Grant Pending in every MAP that has an ACK Time indicating the request has already been processed until the request is granted or discarded.

7.2.1.2 Requesting with Multiple Transmit Channel Mode Enabled

In case of Multiple Transmit Channel Mode is enable the CM must request for the Mutiple channel for data transmission. CMTS provides grant for mutiple channel. Checking when the CM is operating in Multiple Transmit Channel Mode, it does not use the Request Frame (bandwidth request in minislots), but rather it uses the Queue-Depth Based Request Frame (bandwidth request in bytes).

1. Request process check for Segment Header OFF Service Flows:

   Segment Header Off operation is only defined for service flows that have a scheduling type of UGS or UGS-AD. UGS and UGS-AD service flows are required to have an R/T Policy which prohibits the use of contention request opportunities, request/data opportunities, and piggyback requests. Check if queue depth based request frame is created by the software is properly or not. As such, the only defined request mechanism for Segment Header Off service flows is the Queue-depth Based Request Frame transmission used to restart grants during a period of rtPS for a UGS-AD service flow. The CM must be capable of sending a Queue-depth Based Request Frame for a UGS-AD service flow with Segment Headers OFF during a unicast Request IE interval. Check register programming for the CM is properly for the queue depth based request

to generate. When sending a Queue-depth Based Request Frame for a UGS-AD service flow, the CM must set the number of bytes requested to a non-zero value. Since the CMTS is required to provide fixed-size grants based on the UGS Grant Size parameter, the actual number of bytes requested is irrelevant. Piggyback request is used for the subsequent transmission on the packet with only one request send by the CM for the multiple service flow. Piggyback requesting for CMs in Multiple Transmit Channel mode is only defined for Segment Header ON operation. Check register programming for the piggy back request is not done for segment header off condition.

2. Request process check for Segment Header ON Service Flows:

   For a service flow configured for Segment Header ON operation, the CM can send a Request as a stand-alone Queue-depth Based Request Frame transmission. The CM must be capable of sending a Queue-depth based Request Frame to request bandwidth for a Segment. Check for this case piggyback request register is enabled for the subsequent transmission. Generally queue depth based request is send for each service flow but by using the piggy back request ON subsequent transmission for any no of service flow is possible with only one request frame. Header ON service flow during both of the following intervals:

   - Request IE;
   - Request/Data IE;

   A Queue-depth Based Request Frame transmitted by a CM must include:

   - The Service ID making the request;
   - The number of bytes requested with respect to the request byte multiplier for that service flow.

   Piggyback requests for a Segment Header ON service flow transmitted by a CM must only be sent in the Segment Header Request field of the Segment Header.

A piggyback request transmitted in the Segment Header Request field by a CM must include:

- SID Cluster ID associated with the request
- The number of bytes requested with respect to the request byte multiplier for that service flow.

7.3 Upstream Channel Association Check within MAC Domain

7.3.1 MAP and UCD Messages

UCD and MAP messages for a given upstream channel may be sent on any downstream channel in the MAC Domain, regardless of whether or not the channel is a Primary-Capable Downstream Channel. UCD and MAP messages for a given upstream channel may be sent on more than one downstream channel. Check CMTS transmit MAP and UCD messages for each upstream channel in a CMs Transmit Channel Set on at least one downstream channel in that CMs Receive Channel Set. Also check for CMTS is ensuring the UCDs and MAPs for a given upstream channel are identical on all downstream channels on which they are transmitted. Since each CM is only required to receive MAP messages for a particular upstream channel on a single downstream channel, the CMTS must transmit all of the MAPs for a given upstream channel on each of the downstream channels on which those MAPs are carried. The CMTS must transmit all UCDs for a particular upstream channel on each of the downstream channels on which the MAPs for that upstream channel are transmitted. On each Primary-Capable Downstream Channel, the CMTS must transmit UCDs and MAPs for each upstream channel listed in the Upstream Ambiguity Resolution Channel List TLV contained in the MDD on that downstream channel.

7.3.2 Multiple MAC Domain

The CMTS might operate in a configuration in which downstream channels are shared across multiple MAC domains. If a downstream channel is shared between multiple MAC domains, the CMTS must ensure that the downstream channel is primary-capable in only one of the MAC domains. On a given downstream channel, the CMTS must ensure that MAPs and UCDs are transmitted for only a single MAC domain. If a downstream channel is primary capable and shared across multiple MAC domains, the CMTS must include the MAP and UCD Transport Indicator TLV in the MDD message. If the MAP and UCD Transport Indicator TLV is present in the MDD message, the CM must restrict the set of channels on which it receives MAPs and UCDs to those indicated by the MAP and UCD Transport Indicator TLV. If the MAP and UCD Transport Indicator TLV is not present in the MDD message, the CM can receive MAPs and UCDs from any of the Downstream Channels in its Receive Channel Set per the Primary Downstream Channels.

Chapter 8

Final Check for the Test Cases

8.1 CMTS reference Model Check

After packet completely transfers from the bridge, MAC, PHY section of the cable modem IP packets are received by the CMTS model. C language is used for the CMTS model development. CMTS model generates one file when packets are received by the CMTS model. Following things are checked in CMTS model:

1. Request received:- CM sends request to the CMTS model for bandwidth allocation process. CMTS model responds to the request by giving the grant, timing reference, MAP for Upstream data transmission. CMTS Parse the request frame compare it with the C language reference model of CMTS. Error message generated if reading of the request frame is not occurred properly. Check C model reference architect when error occurring during parsing and reading the frame.

2. Unconcatenation:- CMTS model receives concatenated frames. CMTS model parse and read concatenated frame from the information available to it. It splits concatenated frame in to two part (1) concatenated header (2) concatenated data. Concatenation reference model parse and read concatenated header and used it to unconcatenate the data. Finally file generated by the CMTS model shows unconcatenated data which is same as file generated by the software.

Checking for the above mentioned flow done properly or not in reference model in case of any error occurred during unconcatenation process of the frame.

3. Unfragmentation:- CMTS model receives fragmented frames. CMTS model parse and read fragmented frame from the information available to it. It splits fragmented frame in to two part (1) fragmented header (2) fragmented data. Fragmentation reference model parse and read fragmented header and used it to unfragmented the data. Finally file generated by the CMTS model shows unfragmented data which is same as file generated by the software. Checking for the above mentioned flow done properly or not in reference model if any error occurred during unfragmentation of the frame.

4. Unsuppression:- CMTS model receives suppressed frames. CMTS model parse and read suppressed frame from the information available to it. It splits suppressed frame in to two part (1) suppressed header (2) suppressed data. Suppression reference model parse and read suppressed header and used it to unsuppressed the data. Finally file generated by the CMTS model shows unsuppressed data which is same as file generated by the software. Checking for the above mentioned flow done properly or not in reference model if any error occurred during unsuppression of the frame.

8.2 Final Perl Check Script for Test Cases

8.2.1 Checking for Upstream Path

Checker compares file generated by software and file generated by Cable Modem Termination System. In Upstream tests software generates one file according to the test configuration set in excel sheet then packet transfers to Cable Modem Termination System. MAC frame is the communication medium between the Cable Modem and the Cable Modem Termination System. Cable Modem Termination System finally

make one dump file from the MAC frame received. Perl script first read file generated by the software. Script stores packet information in the variable and in the array. Software than read file generated by the CMTS model. Script stores packet related information in the variable and in the array. Checker finally compares both files generated by software and file generated by Cable Modem Termination System. Checker make decision either to pass or fail the test after comparing following things from both the files:

- Destination Address
- Source Address.
- Ether Type or len .
- No of packets in both files.
- Packet size
- Service flow
- Each byte of the packet.
- Source index from where the packet is coming.
- No of packet for each source index. Each byte for that source index.

Checker give list of pass packets and fail packets. Pass packets are those whose Destination Address, Source Address, Ether Type/len, Service flow, Size of the packet, Each byte of the packet are same in both the files file generated by the Cable Modem Termination System and file generated by the software. If above things are match in both the file then test case is pass otherwise test case is fail.

8.2.2 Checking for Downstream Path

Checker compares file generated by Cable Modem Termination System and file generated by software. In Downstream tests Cable Modem Termination System generates one file from the packet which are coming from outside world and file generated by the software when packet is received at DDR memory.

Checker finally compares both files generated by software and file generated by Cable Modem Termination System. Checker make decision either to pass or fail the test after comparing following things from both the files:

- No of packets in both files.
- Packet size
- DSID
- Each byte of the packet.

Checker give list of pass packets and fail packets. Pass packets are those whose DSID, size of that packet, Each byte in that packet are same in both files file generated by software and file generated by the Cable Modem Termination System.if above things are matched than test case is pass otherwise test is fail.

8.2.3 Checking for Loopback Path

In Loopback path comparison of the two files are done. One of them is file generated by the Upstream software and other one is file generated by the software when packets are received at DDR memory.No of packet send by the Upstream software per queue must match with the no of packet when they are received at DDR memory.IF no of packets send and received packets are matched than test cases is pass otherwise it is fail.

Chapter 9

Conclusion

Have developed test cases to verify Upstream path (Data transfer from the Cable Modem to CMTS model), Downstream path (Data transfer from CM to CMTS model) and Loopback path (Data transfer from CPE to CPE). Have covered and observed features are Data suppression for specific traffic, Concatenation of the frame in the MAC section of the IP, Fragmentation of the frame in the MAC section of the IP, Data Encryption in the MAC section of the IP, High Priority and Low Priority for specific traffic, Control direction of flow for the packets, Types of transmission (Broadcast, Multicast, Unicast) by checking header of the frame which transmits from CM to CMTS, Routing information for packets, Ether type version IPv4 (0x800) and IPv6 (0x86DD) both in one test case, Packets drop in modules according to the test configuration, Route packets in particular queues etc. Have Observed CMTS model Deconcatenate, Defragment, Unsuppress the data if test cases cover Concatenation, Fragmentation, Suppression functionality. No of frames received by the CMTS model must be exact the no of packet transmitted by CM for which RF bit is set.

Have done error debugging work for bridge and MAC section of the IP. (1) Software check:- Have checked file generated by the software according to the test configuration. (2) RTL check:- Have checked response of bridge and MAC section IP modules on waveform. For bridge section checked response of IP blocks according to the functionality covered in test configuration. For MAC section of the IP request-

grant functionality is checked. (3) CMTS reference model check:- Have checked file generated by CMTS model according to the test configuration. For successful verification file generated by the software and file generated by the CMTS reference model must be same.

Have developed Perl check script for the Upstream path. If RF bit is set for packet checker for Upstream path compares file generated by the software and file generated by the CMTS model finally give PASS or FAIL status. Those test cases are passed for which No of packets, Destination Address, Source Address, Ether Type, Service Flow, Packet size, Each byte of the packet matched correctly. In mix test cases in which RF bit is set and packet also transfers to Loopback path checker for Upstream path compares file generated by software and file generated by the CMTS model and checker for Downstream path compares file generated by the Upstream software and file generated by Downstream software when packet is received at DDR memory. Observed Mix test case is passed if it is passed in both the script.

References

[1] CM-SP-MULPIv3.0-112-100115, 15 April, 2010.

[2] [DOCSIS NSI] CMTS Network Side Interface, SP-CMTS-NSI-I01-960702, Cable Television Laboratories. July 2, 1996.

[3] [DOCSIS BPI] Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, CM-SP-BPI+-C01-081104, Cable Television Laboratories. November 4, 2008.

[4] [DOCSIS PHY] DOCSIS 3.0, Physical Layer Specification, CM-SP-PHYv3.0-I08-090121, Cable Television Laboratories, January 21, 2009.

[5] [DOCSIS CMCIv3.0] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, CM-SP-CMCIv3.0-I01-080320, Cable Television Laboratories, March 20, 2008.

[6] www.cablelabs.com/cable modem.

[7] [IEEE 802.1D] IEEE 802.1D-2004, IEEE standard for local and metropolitan area networks–Media access control (MAC) Bridges (Incorporates IEEE 802.1t-2001 and IEEE 802.1w).

[8] [ISO/IEC 8802-3] ISO/IEC 8802-3:2000, Information technology, Telecommunications and information exchange between systems, Local and metropolitan area networks, Specific requirements.