Data Over Cable Service Interface Specifications
Mobile Applications

Mobile Xhaul Operations Support System Interface

CM-SP-LLX-OSS-I01-220506

ISSUED

Document Status Sheet

Document Control Number:	CM-SP-LLX-OSS-I01-220506			
Document Title:	Mobile Xhaul Operations Support System Interface			
Revision History:	D01 – Released 01/31/22 D02 – Released 04/20/22		I01 – Released 05/06/22	
Date:	May 6, 2022			
Status:	~~Work in Progress~~	~~Draft~~	**Issued**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	**Public**

Key to Document Status Codes

Work in Progress	An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document in specification format that is considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A generally public document that has undergone rigorous Member and Technology Supplier review, cross-vendor interoperability, and is suitable for certification/qualification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Contents

Figures

Tables

1 SCOPE

1.1 Introduction and Purpose

This specification is part of the DOCSIS® family of specifications developed by Cable Television Laboratories (CableLabs). In particular, this specification is part of the Low Latency Mobile Xhaul over DOCSIS® Technology [LLX] set of specifications that describe techniques for supporting Quality of Service and reducing upstream latency of mobile telecommunications traffic while traversing the DOCSIS data-over-cable network.

This document defines the requirements necessary for the Configuration, Fault Management, and Performance Management of the Cable Modem Termination System (CMTS) or Converged Cable Access Platform (CCAP) system and of the cable modem. The intent of this specification is to define a common, cross-vendor set of functionalities for the configuration and management of CMTSs, CCAPs, and cable modems for the delivery of services over mobile telecommunications equipment.

CableLabs Low Latency Mobile Xhaul over DOCSIS Technology specification leverages and extends CableLabs DOCSIS MULPI [MULPIv3.1] and PHY [PHYv3.1] specifications. This specification similarly leverages and extends CableLabs DOCSIS CCAP OSSI [CCAP-OSSIv3.1] and DOCSIS Cable Modem OSSI [CM-OSSIv3.1] specifications. Requirements in this specification apply to DOCSIS 3.1 and later -compliant CMTS and cable modems.

This specification is intended to complement management features defined for Radio Access Networks by the O-RAN Alliance, to support management of DOCSIS networks traversed by mobile telecommunications traffic.

1.2 Requirements

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

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

1.3 Conventions

In this specification the following convention applies any time a bit field is displayed in a figure. The bit field should be interpreted by reading the figure from left to right, then from top to bottom, with the MSB being the first bit so read and the LSB being the last bit so read.

```
MIB syntax, XML Schema and YANG module syntax are represented by this code sample font.
```

NOTE: Notices and/or Warnings are identified by this style font and label.

1.4 Organization of Document

Section 1 provides an overview of the Low Latency Mobile Xhaul Operations Support Systems Interface (OSSI) specification.

Section 2 includes a list of normative and informative references used in this specification.

Section 3 defines terms used in this specification.

Section 4 defines the abbreviations and acronyms used in this specification.

Section 5 provides an introduction to the FCAPS Network Management Model, which forms the organizational structure of this specification. In order to provide a more logical flow, one that mirrors processes in place at MSOs, the order of functions has been shifted, and is organized as CPF:

- Configuration Management
- Performance Management
- Fault Management

No new Security Management requirements specific to Low Latency Mobile Xhaul have been identified. If a need is identified for new Security Management requirements they will be added in a future version of this specification.

No new Accounting Management requirements specific to Low Latency Mobile Xhaul have been identified. If a need is identified for new Accounting Management requirements they will be added in a future version of this specification.

Section 6 defines the Configuration Management Information Model for the CCAP specific to management support for Low Latency Mobile Xhaul.

Section 7 defines the Performance Management Information Model for the CCAP specific to management support for Low Latency Mobile Xhaul.

Section 8 defines the Fault Management events for the CCAP that are specific to mobile xhaul.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

[3GPP17MgtOrch] 3GPP Release 17 SA5 – Management and Orchestration APIs, December 2020 https://forge.3gpp.org/rep/sa5/MnS/blob/ccc8249ee855af75d6182fad1dcb67a0c6d13daa/yang-models/_3gpp-5gc-nrm-configurable5qiset.yang.

[3GPPTS38.321] 3GPP TS 38.321 v16.6.0, Medium Access Control (MAC) protocol specification (Release 16), September 2021 https://www.3gpp.org/.

[CCAP-OSSIv3.1] DOCSIS 3.1 CCAP Operations Support System Interface Specification, CM-SP-CCAP-OSSIv3.1-I23-220216, February 16, 2022, Cable Television Laboratories, Inc.

[CTI-Common] O-RAN Cooperative Transport Interface Transport Management Plane YANG Models, Module o-ran-cti-common, March 2021, O-RAN Alliance https://www.o-ran.org.

[CTI-ODU] O-RAN Cooperative Transport Interface Transport Management Plane YANG Models, Module o-ran-cti-odu, March 2021, O-RAN Alliance https://www.o-ran.org.

[CTI-TnDocsis] O-RAN Cooperative Transport Interface Transport Management Plane YANG Models, Module o-ran-cti-tn-docsis, March 2021, O-RAN Alliance https://www.o-ran.org.

[CTI-TnGeneric] O-RAN Cooperative Transport Interface Transport Management Plane YANG Models, Module o-ran-cti-tn-generic, March 2021, O-RAN Alliance https://www.o-ran.org.

[IANA-Proto] Internet Assigned Numbers Authority, Protocol Registries https://www.iana.org/protocols.

[dmm-fpc-cpdp] IETF draft-ietf-dmm-fpc-cpdp-04, Protocol for Forwarding Policy Configuration (FPC) in DMM, September 29, 2016.

[LLX] Low Latency Mobile Xhaul over DOCSIS Technology Specification, CM-SP-LLX-I02-200623, June 23, 2020, Cable Television Laboratories, Inc.

[MULPIv3.1] MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.1-I23-220328, March 28, 2022, Cable Television Laboratories, Inc.

[PHYv3.1] DOCSIS 3.1 Physical Layer Specification, CM-SP-PHYv3.1-I19-211110, November 10, 2021, Cable Television Laboratories, Inc.

[RFC 2474] IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.

[RFC 3168] IETF RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP, September 2001.

2.2 Informative References

This specification uses the following informative references.

[CCF] Combined Common Collection Framework Architecture Technical Report, CL-TR-XCCF-PNM-V01-180814, August 14, 2018, Cable Television Laboratories, Inc.

[CM-OSSIv3.1] DOCSIS 3.1 Cable Modem Operations Support System Interface Specification, CM-SP-CM-OSSIv3.1-I22-220216, February 16, 2022, Cable Television Laboratories, Inc.

[RFC 2578] IETF RFC 2578, Structure of Management Information Version 2 (SMIv2), April 1999.

[RFC 2863] IETF RFC 2863, The Interfaces Group MIB, June 2000.

[RFC 6020] IETF RFC 6020, YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF), October 2010.

[UML Guidelines] UML Modeling Guidelines, CM-GL-OSS-UML-V01-180627, June 27, 2018, Cable Television Laboratories, Inc.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, http://www.ietf.org
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org/
  Note: Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time.
  The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.
  Internet-Drafts may also be accessed at http://tools.ietf.org/html/.
- O-RAN Alliance e.V., Buschkauler Weg 27, 53347 Alfter/Germany, http://www.o-ran.org.

3 TERMS AND DEFINITIONS

3.1 Terms and Definitions

This specification uses the following terms.

backhaul	In a cellular network, the portion of the network that runs between the 4G LTE base station to the mobile core network
crosshaul	Generic term that includes fronthaul, midhaul, and backhaul
fronthaul	In a cellular network, the network link between the remote radio heads at the cell sites and the centralized baseband controller
xhaul	backhaul, midhaul, or fronthaul

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations.

AE	access entity
BSS	business support systems
BWR	bandwidth report
CCAP	Converged Cable Access Platform
CCF	common collection framework
ECN	explicit congestion notification
ECT	explicit congestion notification-capable transport
FCAPS	fault, configuration, accounting, performance and security
MSO	multiple system operator
MXh	mobile xhaul
NOC	network operations center
OSS	operations support system
QoS	quality of service
UML	Unified Modeling Language

5 OVERVIEW

5.1 FCAPS Network Management Model

The International Telecommunication Union (ITU) Recommendation defines a set of management categories, referred to as the FCAPS model, represented by the individual management categories of Fault, Configuration, Accounting, Performance and Security. Telecommunications operators, including MSOs, commonly use this model to manage large networks of devices. This specification uses these management categories to organize the requirements for the configuration and management of the CCAP platform.

Fault management seeks to identify, isolate, correct and record system faults. Configuration management modifies system configuration variables and collects configuration information. Accounting management collects usage statistics for subscribers, sets usage quotas and bills users according to their use of the system. Performance management focuses on the collection of performance metrics, analysis of these metrics and the setting of thresholds and rate limits. Security management encompasses identification and authorization of users and equipment, provides audit logs and alerting functions, as well as providing vulnerability assessment.

Each of these management categories is discussed in further detail in the following sections.

A DOCSIS 3.1-compliant CCAP implementing Low Latency Mobile Xhaul requirements complies with management requirements specified in [CCAP-OSSIv3.1] in addition to CCAP requirements defined in this specification, unless explicitly excepted in this specification.

A DOCSIS 3.1-compliant cable modem implementing Low Latency Mobile Xhaul requirements complies with management requirements specified in [CM-OSSIv3.1] in addition to CM requirements defined in this specification, unless explicitly excepted in this specification.

5.1.1 Fault Management

Fault management is a proactive and on-demand network management function that allows non-standard/abnormal operation on the network to be detected, diagnosed, and corrected. A typical use case involves network elements detecting service-impacting abnormalities; when detected, an autonomous event (often referred to as an alarm notification) is sent to the network operations center (NOC) to alert the MSO of a possible fault condition in the network affecting a customer's service. Once the MSO receives the event notification, further troubleshooting and diagnostics can be performed by the MSO to correct the fault condition and restore the service to proper operation.

5.1.2 Configuration Management

Configuration Management provides a set of network management functions that enables system configuration building and instantiating, installation and system turn up, network and device provisioning, auto-discovery, backup and restore, software download, status, and control (e.g., checking or changing the service state of an interface).

Configuration Management is primarily concerned with network control via modifying operating parameters on network elements such as the CCAP. Configuration parameters could include both physical resources (for example, an Ethernet interface) and logical objects (for example, QoS parameters for a given service flow).

While the network is in operation, Configuration Management is responsible for monitoring the configuration state and making changes in response to commands by a management system or some other network management function.

For example, a performance management function may detect that response time is degrading due to a high number of uncorrected frames and may issue a Configuration Management change to modify the modulation type from 16-QAM to QPSK. A Fault Management function may detect and isolate a fault and may issue a configuration change to mitigate or correct that fault.

5.1.3 Accounting Management

Accounting Management is a network management function that allows MSOs to measure the use of network services by subscribers for the purposes of cost estimation and subscriber billing. The Mobile Xhaul OSSI specification does not introduce new Accounting Management requirements for the DOCSIS CCAP or CM.

5.1.4 Performance Management

Performance Management is a proactive and on-demand network management function. The ITU Recommendation defines its role as gathering and analyzing "statistical data for the purpose of monitoring and correcting the behavior and effectiveness of the network, network equipment, or other equipment and to aid in planning, provisioning, maintenance and the measurement of quality." A Performance Management use case might include the NOC performing periodic (15 min, for example) collections of QoS measurements from network elements to perform monitoring and identification of any potential performance issues that may be occurring with the service being monitored. With the historical data that has been collected, trending analysis can be performed to identify issues that may be related to certain times of day or other corollary events. The MSO can run reports on the data to identify suspect problems in service quality, or the NOC application can be provisioned, so that when certain performance thresholds are violated, the MSO is automatically notified that a potential service quality problem may be pending. Significant intelligence can be integrated into the NOC application to automate the ability to detect the possible degradation of a customer's service quality and take actions to correct the condition. Service level agreement compliance is not possible without strong performance management.

Performance Management functions include collecting statistics of parameters such as number of frames lost at the MAC layer and number of codeword errors at the PHY layer. These monitoring functions are used to determine the health of the network and whether the offered Quality of Service (QoS) to the subscriber is met. The quality of signal at the PHY layer is an indication of plant conditions.

Additional Performance Management functions include Proactive Network Maintenance to enable measurement and reporting of network conditions such that undesired impacts such as plant equipment and cable faults, interference from other systems and ingress can be detected and measured. With this information, cable network operations personnel can make modifications necessary to improve conditions and monitor network trends to detect when network improvements are needed.

5.1.5 Security Management

Security Management provides for the management of network and operator security, as well as providing an umbrella of security for the telecommunications management network functions. Security Management functions include authentication, access control, data confidentiality, data integrity, event detection, and reporting. A Security Management use case might include providing authentication and data confidentiality when transferring a configuration file that contains the entire configuration data set for the device to a network element. The Mobile Xhaul OSSI specification does not introduce new Security Management requirements for the CCAP or CM.

5.2 Management Architectural Overview

Figure 1 illustrates the CCAP management architecture including management interfaces and logical components. Refer to the following sections for descriptions of the architectural components.

This specification defines the Oss-Ccap and Oss-Ae interfaces indicated in Figure 1 for management of Bandwidth Reporting (BWR) service defined in [LLX].

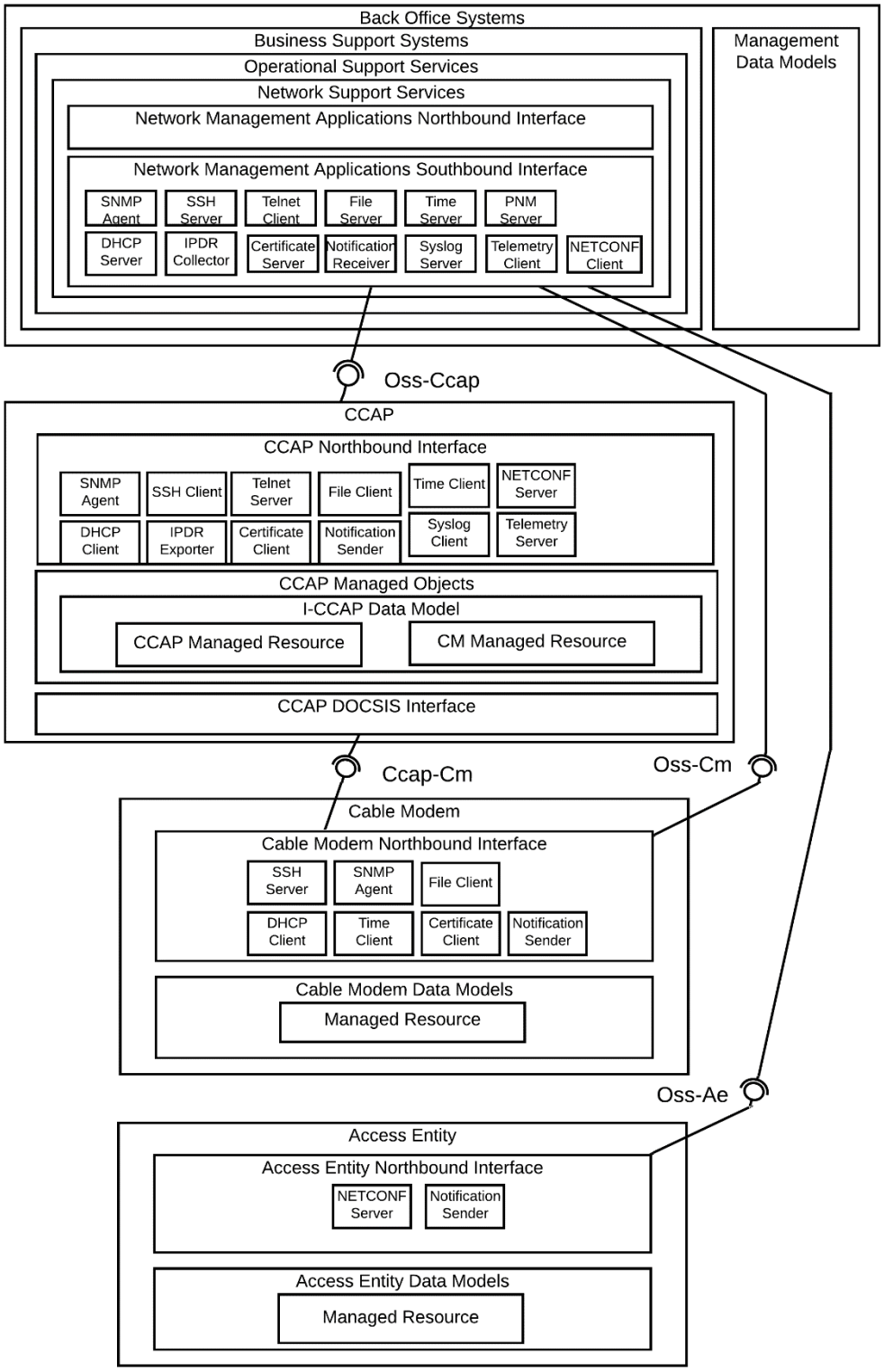

Figure 1 - CMTS, CCAP, and Access Entity Management Architecture

5.2.1 Back Office Systems

MSO back office systems support the delivery of their subscriber services. This is generally represented as a layered model:

- Business Support Services

  Business Support Services (BSSs) include business and commercial level systems for customer management, revenue management, billing, etc.

- Operational Support Services

  Operational Support Services (OSSs) include service-level systems for service delivery and orchestration and service monitoring.

- Network Support Services

  Network support services, including Network Management Systems (NMSs) and Element Management Systems (EMSs), include network facing systems for network management, monitoring, administration and control. This is often referred to as the Network Management Layer. Network Support Services provide an abstraction layer to the Operational Support Services via a Network Management Applications Northbound Interface.

- Management Data Models

  In a model-driven architecture, each layer in the Back Office contains an abstracted view of the underlaying layer below it. Management data models provide implementation-specific programmable models which can be used by all applications in each layer. This specification uses UML to model protocol-agnostic Information Models as described in Section 5.4.

5.2.2 Network Management Applications

Various management servers, including Network Management Stations, reside in the Network Management Layer within the MSO back office to provision, monitor, and administer the Network Elements or network functions within the Network Layer.

The following set of network management applications are supported in the architecture:

- SNMP Manager – performs SNMP queries against a CCAP's SNMP Agent.
- SSH Client – provides secure access to the CCAP.
- Telnet Client – provides Telnet capabilities into the CCAP.
- File Server – provides a file transfer mechanism for the CCAP.
- Time Server – provides a CCAP with current Time of Day (ToD).
- DHCP Server – has the responsibility of assigning a CCAP its IPv4 and/or IPv6 addresses as well as other DHCP parameters.
- IPDR Collector – primary and secondary – collect bulk data statistics, such as usage metrics, via the IPDR/SP protocol.
- Certificate Server – provides information and status for security certificates.
- Notification Receiver – receives autonomous SNMP and optional NETCONF notifications and Syslog messages from a CCAP.
- Syslog Server – provides the ability to receive SYSLOG messages from the CCAP.
- NETCONF Client – performs provisioning for CCAPs supporting NETCONF Servers.
- PNM Server – provides an interface to triggering PNM tests in the CCAP and collecting PNM measurements.
- Telemetry Client – provides a Streaming Telemetry subscription interface.

The Business and Service Management Layer, which sits north of the Network Management Layer, is where higher-level MSO business processes are implemented via BSS/OSS systems (Business Support Services and Operational Support Services). These BSS/OSS systems utilize the data and information from the Network Management Layer (via the Network Management Applications Northbound Interface) that interrogate data from the Network Layer. Figure 1 illustrates components and their respective resource artifacts that reside at the Network Layer and Network

Management Layer, which include the CCAP and Cable Modem and their respective Network Management Applications.

5.2.3 CCAP

The CMTS is an access-side networking element or set of elements that includes one or more MAC Domains and one or more Network System Interfaces. This device is located at the cable television system headend or distribution hub and provides data connectivity between a DOCSIS Radio Frequency Interface and a wide-area network.

The CCAP is an access-side networking element or set of elements that combines the functionality of a CMTS with that of an Edge QAM, providing high-density services to cable subscribers.

The CMTS/CCAP and Cable Modems reside within the Network Layer where services are provided to end Subscribers and various metrics are collected about network and service performance, among other things.

5.2.3.1 CCAP Northbound Interface

The CCAP Northbound Interface provides a standardized set of management and operations protocols to enable back office management of DOCSIS components. In addition, this interface provides an abstracted model view of the DOCSIS system components to the back office management applications.

The following set of network management protocols are supported by the architecture:

- SNMP Agent
- SSH Server
- Telnet Server
- File Client
- Time Client
- DHCP Client
- IPDR Exporter
- Certificate Client
- Notification Sender
- Syslog Client
- NETCONF Server
- Telemetry Subscription
- Telemetry Publication

These represent client or server applications that enable communication with the backoffice network management applications.

5.2.3.2 CCAP Managed Objects

This represents the set of data models, containing groupings of managed objects, which enables the back office to manage, administer, monitor and provision the CCAP component. In this specification, this information is specified in a protocol-neutral UML modeling language and then translated into the required protocol-specific data models based on each type of network management interface and its requirements for data encoding and associated messaging protocols. There are two basic types of managed objects: CCAP managed resources, which enable the back office to manage aspects of the CCAP component, and CM managed resources, which enable the back office to manage aspects of Cable Modems via the DOCSIS protocol.

5.2.3.3 CCAP Southbound Interface

The CCAP Southbound Interface represents the interface between the CCAP and CM. This interface communicates with the southbound CMs in the Network Layer to manage MAC and PHY level characteristics.

5.2.4 Cable Modem

The Cable Modem is a modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system. The Cable Modem also contains a set of Information Models and associated protocol specific data models as specified in [CM-OSSIv3.1].

5.2.5 Access Entity

The Access Entity is the network element in a DOCSIS crosshaul system where the scheduler for the mobile data communications network resides [LLX]. Management traffic between the AE and the backoffice systems traverses the CCAP or CMTS and cable modem in the DOCSIS backhaul and DOCSIS midhaul topologies [LLX]. The Access Entity contains a set of Information Models and specific data models as specified in [LLX] and this specification.

5.3 Mobile Xhaul OSSI Key Features

The DOCSIS Mobile Xhaul OSSI specifications introduce management features that build upon those defined in DOCSIS 3.1 OSSI specifications.

5.3.1 Configuration Management Features

The configuration of the DOCSIS protocols for CM/CCAP interactions for configuring features in support of PHY, MULPI/QoS, and Security (BPI) uses the CM configuration file and CMTS policies via MAC messages exchange. Configuration of features and functions of the CCAP is performed via vendor-proprietary mechanism or via NETCONF, if supported.

The Mobile Xhaul OSSI specification defines and models CCAP and AE configuration parameters required to initialize mobile xhaul-specific functions defined in [LLX].

5.3.2 Performance Management Features

The Mobile Xhaul OSSI performance management requirements include status objects to report state and status of Bandwidth Reporting (BWR). DOCSIS OSSI performance management features specified in [CCAP-OSSIv3.1] and [CM-OSSIv3.1] manage the operation and status monitoring of other DOCSIS capabilities supporting Low Latency Mobile Xhaul operation including Quality of Service (QoS) and traffic statistics.

5.3.3 Fault Management Features

Fault management is a proactive and on-demand network management function that enables rapid detection and reporting of abnormal operation(s) on the network. to be diagnosed and corrected. A typical use case involves network elements detecting service-impacting abnormalities; when detected, an autonomous event (often referred to as an alarm notification) is sent to the network operations center (NOC) to alert the MSO of a possible fault condition in the network affecting a customer's service. Once the MSO receives the event notification, further troubleshooting and diagnostics can be performed by the MSO to correct the fault condition and restore the service to proper operation.

5.4 Information Models

Information Models, based on object-oriented modeling, are commonly utilized in the industry for capturing requirements and analyzing the data in a protocol independent representation. This specification uses the Unified Modeling Language (UML) to graphically represent the various elements comprising the Information Model. This approach defines requirements with use cases to describe the interactions between the operations support systems and the network elements. Use Case diagrams identify the interactions that a user or, actor, interacts with the CCAP or the AE. Sequence diagrams model the sequence of exchanged messages (e.g., SNMP, NETCONF) and actions for a specific operation and are often used to identify specific scenarios for the defined Use Cases. The management information is represented in terms of classes and attributes and the interactions between these encapsulated objects (or also referred to as entities in some representations). Class diagrams provide this conceptual, static model of the structure of the system (i.e., CCAP OSS Interface and AE OSS interface). Component diagrams model the components of a system and the interactions between the components.

The managed objects, operations, and notifications are then represented in a protocol specific form referred to as a management data model. Xhaul requires YANG data models [RFC 6020] managed with NETCONF and/or RESTCONF.

Refer to [UML Guidelines] for information modeling concepts used throughout this specification.

5.5 Mobile Xhaul Management Use Cases

The following Use Cases represent example FCAPS operations for managing mobile xhaul features in the CCAP and cable modem.

5.5.1 Configuration Management Use Cases

Refer to [CCAP-OSSIv3.1] section 5.1.2 Configuration Management for a description of Configuration Management Use Cases for the CCAP. The same Configuration Management Use Cases apply for configuration of BWR in the AE.

5.5.2 Performance Management Use Cases

The following represents general CCAP Performance Management Use Cases.

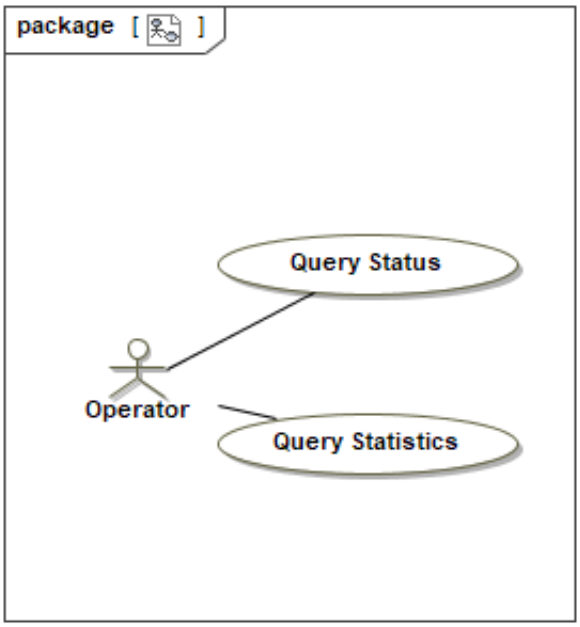

Figure 2 - General Performance Management Use Cases

5.5.3 Fault Management Use Cases

Refer to [CCAP-OSSIv3.1] section 5.1.1 Fault Management for a description of Fault Management Use Cases for the CCAP.

6 MOBILE XHAUL CONFIGURATION MANAGEMENT

Mobile xhaul functionality requires configuration of DOCSIS-defined features in CCAPs in the DOCSIS network. [CCAP-OSSIv3.1] and [CM-OSSIv3.1] define standard DOCSIS configuration features and capabilities for DOCSIS 3.1 CCAP and DOCSIS 3.1 cable modems, respectively. This specification references [CCAP-OSSIv3.1] for existing defined configuration management functionality, information models, and data models leveraged for Mobile Xhaul functionality, and defines information models and management requirements that are new and unique to mobile xhaul.

CCAP configuration protocol and transport requirements specified in [CCAP-OSSIv3.1] apply for CCAP configuration of mobile xhaul-specific features.

No new configuration parameters or protocols had to be defined for DOCSIS 3.1 cable modems to support mobile xhaul operation in a DOCSIS network.

6.1 Data Type Definitions

Refer to [CCAP-OSSIv3.1] Annex F, *CCAP Data Type Definitions* for the definition of data types used for CCAP Configuration Information Model.

6.2 Mobile Xhaul Configuration Management

CableLabs Low Latency Mobile Xhaul over DOCSIS® Technology specification [LLX] describes three topologies when using DOCSIS networks as the crosshaul transport network for mobile networks:

DOCSIS backhaul

DOCSIS midhaul

DOCSIS fronthaul

In the backhaul and midhaul topologies the DOCSIS CMTS or CCAP and cable modem provide data services to the AE and pass management messages between the Mobile Core and the back office systems to the AE.

In the fronthaul topology the CMTS or CCAP and cable modem do not provide data services to the AE and configuration of Bandwidth Reporting (BWR) service occurs between the AE and the CCAP or CMTS through the CCAP or CMTS northbound interface. Reference: [LLX] DOCSIS Xhaul Architecture section.

The Mobile Xhaul OSSI specification addresses the DOCSIS backhaul and DOCSIS midhaul topologies. The DOCSIS fronthaul topology is out of scope for this specification.

6.2.1 CCAP Mobile Xhaul Configuration Information Model

This section defines the Information Models for DOCSIS CCAP Mobile Xhaul.

6.2.1.1 CCAP Mobile Xhaul Configuration Data Type Definitions

This section defines any required data type definitions used in the CCAP Mobile Xhaul Configuration Information Model.

6.2.1.1.1 CCAP Mobile Xhaul Configuration Complex Data Type Definitions

This section defines classes used in the CCAP Mobile Xhaul Information Model as complex data types.

6.2.1.1.1.1 FilterType

This class provides the management interface for configuring the filter to be applied to a flow for a BWR session.

Table 1 - FilterType Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Ethernet	Directed Composition to Ethernet	1	0..*	
UdpIp	Directed Composition to UpdIp	1	0..*	

6.2.1.1.1.2 Ethernet

This class defines parameters for Ethernet Filter Type to be applied to a flow for a BWR session.

Table 2 - Ethernet Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
SrcMac	MacAddress	Read-write		
DestMac	MacAddress	Read-write		
Ethertype	UnsignedShort	Read-write		
Pcp	UnsignedByte	Read-write	0..7	
VlanId	UnsignedShort	Read-write	1..4094	

6.2.1.1.1.2.1 SrcMac

This attribute configures the source MAC address filter for the BWR session flow.

6.2.1.1.1.2.2 DestMac

This attribute configures the destination MAC address filter for the BWR session flow.

6.2.1.1.1.2.3 Ethertype

This attribute configures the Ethertype filter for the BWR session flow.

Reference: [MULPIv3.1] Ethertype/DSAP/MacType section

6.2.1.1.1.2.4 Pcp

This attribute configures the IEEE 802.1P user priority filter for the BWR session flow.

Reference: [MULPIv3.1] IEEE 802.1P User_Priority section

6.2.1.1.1.2.5 VlanId

This attribute configures the Virtual LAN identifier filter for the BWR session flow.

6.2.1.1.1.3 UdpIp

This class defines the parameters for UDP/IP Filter Type to be applied to a flow for a BWR session.

Table 3 - UdpIp Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
SrcAddress	IpAddress	Read-write		
SourcePrefix	IpPrefix	Read-write		
DestAddress	IpAddress	Read-write		
DestPrefix	IpPrefix	Read-write		
Dscp	UnsignedByte	Read-write	0..63	

Attribute Name	Type	Access	Type Constraints	Units
SrcPortStart	UnsignedInt	Read-write		
SrcPortEnd	UnsignedInt	Read-write		
DestPortStart	UnsignedInt	Read-write		
DestPortEnd	UnsignedInt	Read-write		
Ipv4Protocol	UnsignedShort	Read-write	0..257	
Ipv6TcLow	HexBinary	Read-write		
Ipv6TcHigh	HexBinary	Read-write		
Ipv6TcMask	HexBinary	Read-write		
Ipv6Flow	UnsignedInt	Read-write	0..1048575	
Ipv6NextHeader	UnsignedByte	Read-write		
Ipv4Ecn	Enum	Read-write	nonEct(0), ect1(1), ect0(2), congestionEncountered(3)	

6.2.1.1.1.3.1 SrcAddress

This attribute configures the matching value for the source IP address filter for the BWR session flow.

6.2.1.1.1.3.2 SourcePrefix

This attribute configures the matching value for the source IP address prefix filter for the BWR session flow.

6.2.1.1.1.3.3 DestAddress

This attribute configures the matching value for the destination IP address filter for the BWR session flow.

6.2.1.1.1.3.4 DestPrefix

This attribute configures the matching value for the destination IP address prefix filter for the BWR session flow.

6.2.1.1.1.3.5 Dscp

This attribute configures the matching value for the Differentiated Services Code Point filter for the BWR session flow.

6.2.1.1.1.3.6 SrcPortStart

This attribute configures the matching value for the starting port number of the source port number range filter for the BWR session flow.

6.2.1.1.1.3.7 SrcPortEnd

This attribute configures the matching value for the ending port number of the source port number range filter for the BWR session flow.

6.2.1.1.1.3.8 DestPortStart

This attribute configures the matching value for the starting port number of the destination port number range filter for the BWR session flow.

6.2.1.1.1.3.9 DestPortEnd

This attribute configures the matching value for the ending port number of the destination port number range filter for the BWR session flow.

6.2.1.1.1.3.10 Ipv4Protocol

This attribute configures the matching value for the IP Protocol field filter for the BWR session flow. If this parameter is omitted, then comparison of the IP header Protocol field for this entry is irrelevant.

There are two special IP Protocol field values: value "256" matches traffic with any IP Protocol value and value "257" matches both TCP and UDP traffic. The CCAP is required to invalidate for comparisons an IP Protocol field value greater than 257, i.e., no traffic can match this entry.

References: [MULPIv3.1] IP Protocol TLV Type description, [IANA-Proto]

6.2.1.1.1.3.11 Ipv6TcLow

This attribute configures the matching value for the IPv6 Traffic Class byte filter corresponding to the value “tc-low” for TLV Type [22/23/60].12.1 [MULPIv3.1] for the BWR session flow.

Reference: [MULPIv3.1] IPv6 Traffic Class Range and Mask TLV Type description

6.2.1.1.1.3.12 Ipv6TcHigh

This attribute configures the matching value for the IPv6 Traffic Class byte filter corresponding to the value “tc-high” for TLV Type [22/23/60].12.1 [MULPIv3.1] for the BWR session flow.

Reference: [MULPIv3.1] IPv6 Traffic Class Range and Mask TLV Type description

6.2.1.1.1.3.13 Ipv6TcMask

This attribute configures the matching value for the IPv6 Traffic Class byte filter corresponding to the value “tc-mask” for TLV Type [22/23/60].12.1 [MULPIv3.1] for the BWR session flow.

Reference: [MULPIv3.1] IPv6 Traffic Class Range and Mask TLV Type description

6.2.1.1.1.3.14 Ipv6Flow

This attribute configures the matching value for the IPv6 Flow Label filter for the BWR session flow.

Reference: [MULPIv3.1] IPv6 Flow Label TLV Type description

6.2.1.1.1.3.15 Ipv6NextHeader

This attribute configures the matching value for the IPv6 Next Header filter for the BWR session flow.

Reference: [MULPIv3.1] IPv6 Next Header Type TLV Type description

6.2.1.1.1.3.16 Ipv4Ecn

This attribute configures the matching value for the IPv4 or IPv6 Explicit Congestion Notification (ECN) filter for the BWR session flow. The two-bit value corresponds to the two ECN bits in the Differentiated Services (DS) field of the IPv4 and IPv6 packet header. Values defined for this attribute are listed below:

nonEct(0): The packet is not using ECN-capable transport (ECT)
ect1(1): ECT 1 codepoint: The endpoints are ECN-capable
ect0(2): ECT 0 codepoint: The endpoints are ECN-capable
congestionEncountered(3): Congestion exists between end nodes

References: [RFC 2474], [RFC 3168]

6.2.1.1.1.4 PatternType

This class defines parameters for configuring the BWR pattern.

Reference: [LLX]

Table 4 - PatternType Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
PatternId	UnsignedInt	Read-write		
PatternDuration	UnsignedByte	Read-write		125 microseconds
PatternEvents	UnsignedByte	Read-write		
PatternEventMultiplier	UnsignedByte	Read-write		
PatternEventBytes	UnsignedShort	Read-write		

6.2.1.1.1.4.1 PatternId

This attribute configures a unique identifier for a BWR pattern.

6.2.1.1.1.4.2 PatternDuration

This attribute configures the length of a single mobile slot time, in units of 125 µs.

6.2.1.1.1.4.3 PatternEvents

This attribute configures the number of events per BWR pattern.

6.2.1.1.1.4.4 PatternEventMultiplier

This attribute configures the number of sequential events that have the same byte count. PatternEventMultiplier and PatternEventBytes are repeated as a pair to describe an event.

6.2.1.1.1.4.5 PatternEventBytes

This attribute configures the number of bytes per event. A byte count is allowed to be 0 bytes. Value 0xFFFF indicates a residual average, where:

Residual average = [BWR byte count - sum(explicit bytes described)]/sum(events without explicit bytes described)

6.2.1.1.1.5 BwrFlowsType

This class defines parameters for configuring BWR session flows.

Table 5 - BwrFlowsType Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
FlowId	UnsignedByte	Read-write		
MaxPortionT34Latency	UnsignedShort	Read-write		5 microseconds
AssociatedScn	String	Read-write	1..15	
Filter	FilterType	Read-write		

6.2.1.1.1.5.1 FlowId

This attribute configures the unique identifier for the BWR session flow instance.

6.2.1.1.1.5.2 MaxPortionT34Latency

This attribute configures the portion of the maximum T34 latency allocated to CMTS-CM network in units of 5 microseconds.

6.2.1.1.1.5.3 AssociatedScn

This attribute configures the Service Class Name associated with the BWR flow. DOCSIS specifies that the maximum size is 16 ASCII characters including a terminating zero.

6.2.1.1.1.5.4 Filter

This attribute configures the filter for the BWR session flow.

6.2.1.1.1.6 CcapBwrConnectivityType

This class defines parameters for configuring the connectivity between the BWR server and the BWR client.

Reference: [LLX]

Table 6 - CcapBwrConnectivityType Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Ethernet	Directed Composition to Ethernet	1	0..*	
UdpIp	Directed Composition to UdpIp	1	0..*	

6.2.1.1.1.6.1 Ethernet

This class defines parameters for an Ethernet connection between the BWR client and the BWR server.

Table 7 - Ethernet Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
ClientMacAddr	MacAddress	Read-write		

6.2.1.1.1.6.1.1 ClientMacAddr

This attribute configures the MAC Address of the BWR client.

6.2.1.1.1.6.2 UdpIp

This class defines parameters for an UDP/IP connection between the BWR client and the BWR server.

Table 8 - UdpIp Object Attribute

Attribute Name	Type	Access	Type Constraints	Units
ClientHostName	Host	Read-write		

6.2.1.1.1.6.2.1 ClientHostName

This attribute configures the IP address or Domain Name of the BWR client.

6.2.1.2 CCAP Mobile Xhaul Configuration Class Diagram

Figure 3 - CCAP Mobile Xhaul BWR Configuration Information Model defines objects for the configuration of the CCAP for mobile xhaul operation.

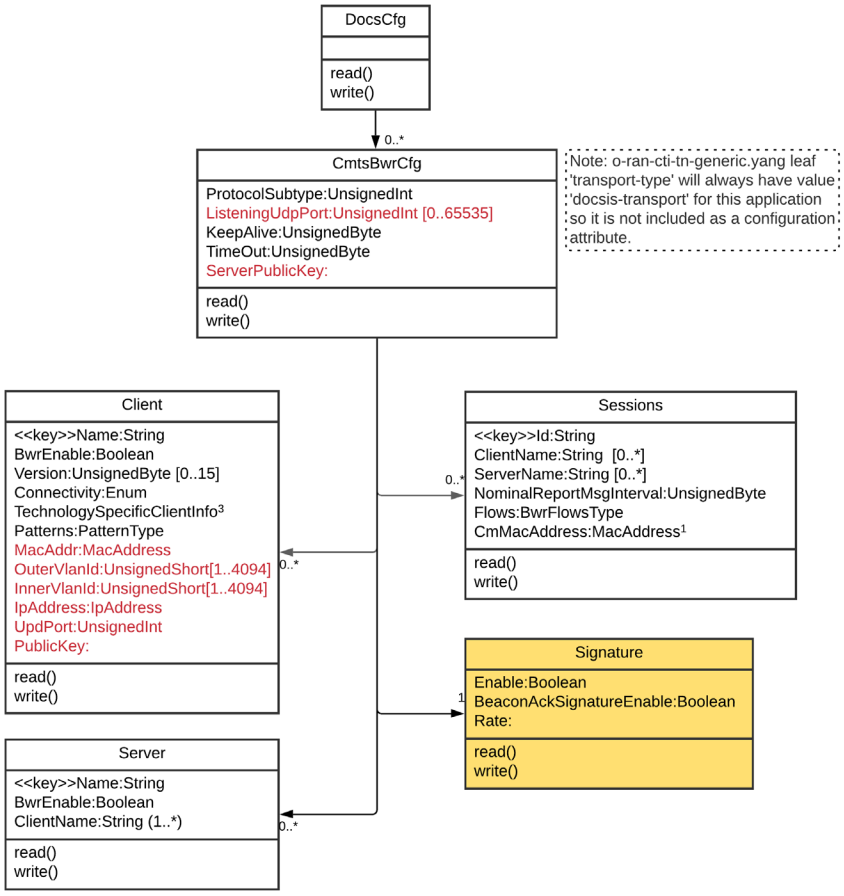

Figure 3 - CCAP Mobile Xhaul BWR Configuration Information Model

6.2.1.2.1 DocsCfg

The DocsCfg object is the root for DOCSIS configuration data.

Reference: [CCAP-OSSIv3.1] DocsCfg section

Table 9 - DocsCfg Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
CmtsBwrCfg	Directed composition to CmtsBwrCfg	1	0..*	

6.2.1.2.2 CmtsBwrCfg

The CmtsBwrCfg provides the management interface for Mobile Xhaul CCAP Bandwidth Reporting configuration.

Table 10 - CmtsBwrCfg Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
ProtocolSubtype	UnsignedInt	No			
ListeningUdpPort	UnsignedInt	Yes	0..65535		

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
KeepAlive	UnsignedByte	Yes		Tenth second	
TimeOut	UnsignedByte	Yes		Tenth second	
ServerPublicKey	<TBD>				

Table 11 - CmtsBwrCfg Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Client	Directed composition to Client	1	0..*	
Server	Directed composition to Server	1	0..*	
Sessions	Directed composition to Sessions	1	0..*	
Beacon	Directed composition to Beacon	1	0..1	
Signature	Directed composition to Signature	1	0..1	

6.2.1.2.2.1 ProtocolSubtype

This attribute is the 16-bit sub-type to be used with the standardized Ethertype value 0x9433. This attribute can be deleted once a common sub-type is specified.

Reference: [CTI-Common]

6.2.1.2.2.2 ListeningUdpPort

This attribute is the UDP destination port to use for all CTI messages.

Reference: [CTI-Common]

6.2.1.2.2.3 KeepAlive

This attribute is the maximum time interval between consecutive BWR Keep-Alive messages between the BWR client and the BWR server.

Reference: [CTI-TnGeneric]

6.2.1.2.2.4 TimeOut

This attribute is the timeout value that a BWR-Beacon-Ack message needs to be received by the BWR client (AE) or the BWR server (CMTS) before that respective system suspends BWR operations and returns to its BWR configuration state.

Reference: [CTI-TnGeneric]

6.2.1.2.2.5 ServerPublicKey

This attribute is the public encryption key used to validate the BWR-Beacon-Ack signature.

<TBD: data type and format>

Reference: [LLX]

6.2.1.2.3 Client

This object provides the management interface for configuring the BWR server on the CMTS with the list of BWR clients.

Table 12 - Client Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Name	String	Yes (Key)			
BwrEnable	Boolean	Yes			
Version	UnsignedByte	No	0..15		
Connectivity	ConnectivityType	No			
Patterns	PatternType	No			
MacAddr	MacAddress				
OuterVlanId	UnsignedShort		1..4094		
InnerVlanId	UnsignedShort		1..4094		
UdpPort	UnsignedInt				
PublicKey	<TBD>				

6.2.1.2.3.1 Name

This key attribute is a name for the BWR client.

Reference: [CTI-TnGeneric]

6.2.1.2.3.2 BwrEnable

This attribute configures the BWR client for Bandwidth Reporting (BWR). A value ‘true’ for this attribute enables BWR for the client. A value ‘false’ for this attribute disables BWR for the client.

Reference: [CTI-TnGeneric]

6.2.1.2.3.3 Version

This attribute configures the list of BWR Transport Control plane versions that can be used with the client.

Reference: [CTI-TnGeneric]

6.2.1.2.3.4 Connectivity

This attribute configures the BWR Client’s connectivity to the BWR Server.

Reference: [CTI-TnGeneric]

6.2.1.2.3.5 Patterns

This attribute configures the BWR pattern type for the BWR Client.

Reference: [CTI-TnGeneric]

6.2.1.2.3.6 MacAddr

This attribute configures the Ethernet MAC Address of the BWR client. This is the MAC Address the CMTS will send BWR messages to.

Reference: [CTI-TnGeneric]

6.2.1.2.3.7 OuterVlanId

This attribute configures the outer Virtual LAN ID for the BWR client.

Reference: [LLX]

6.2.1.2.3.8 InnerVlanId

This attribute configures the inner Virtual LAN ID for the BWR client.

Reference: [LLX]

6.2.1.2.3.9 UdpPort

This attribute configures the UDP port number of the BWR client.

Reference: [CTI-TnGeneric]

6.2.1.2.3.10 PublicKey

This attribute configures the public encryption key for validating the BWR signature on the BWR client.

Reference: [LLX]

6.2.1.2.4 Server

This object provides the management interface for configuring the BWR server on the CMTS.

Table 13 - Server Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Name	String	Yes (Key)			
BwrEnable	Boolean	Yes			
ClientName	String	Yes			

6.2.1.2.4.1 Name

This key attribute configures a unique name for the BWR server instance.

Reference: [CTI-TnGeneric]

6.2.1.2.4.2 BwrEnable

This attribute configures the BWR server for Bandwidth Reporting (BWR). A value ‘true’ for this attribute enables BWR for the server. A value ‘false’ for this attribute disables BWR for the server.

Reference: [CTI-TnGeneric]

6.2.1.2.4.3 ClientName

This attribute is a list of Client Names for BWR clients associated with this BWR server instance.

Reference: [CTI-TnGeneric]

6.2.1.2.5 Sessions

This object provides the management interface for configuring the BWR server on the CMTS with the list of BWR sessions.

Table 14 - Sessions Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Id	String	Yes (Key)			
ClientName	String	No			
ServerName	String	No			
NominalReportMsgInterval	UnsignedByte	Yes		0.25 milliseconds	

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Flows	BwrFlowsType	Yes			
CmMacAddr	MacAddress	Yes			

6.2.1.2.5.1 Id

This key attribute configures a unique identifier for the BWR session.

Reference: [CTI-TnGeneric]

6.2.1.2.5.2 ClientName

This optional attribute configures a name for the BWR client terminating the session.

Reference: [CTI-TnGeneric]

6.2.1.2.5.3 ServerName

This optional attribute configures a name for the BWR server terminating the session.

Reference: [CTI-TnGeneric]

6.2.1.2.5.4 NominalReportMsgInterval

This attribute configures the nominal BWR reporting message time interval in units of 0.25 milliseconds.

Reference: [CTI-TnGeneric]

6.2.1.2.5.5 Flows

This attribute configures the flows for the BWR session.

Reference: [CTI-TnGeneric]

6.2.1.2.5.6 CmMacAddr

This attribute configures the MAC address of the cable modem connected to the radio unit.

Reference: [CTI-TnDocsis]

6.2.1.2.6 Signature

This object provides the management interface for configuring the BWR server on the CMTS with the BWR-Beacon-Ack signature.

Table 15 - Signature Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Enable	Boolean	Yes			
BeaconAckEnable	Boolean	Yes			
Rate	UnsignedShort	Yes		Signatures per microsecond	

6.2.1.2.6.1 Enable

This attribute configures the use of the BWR signature on the CMTS. Value 'true' indicates BWR signature is enabled. Value 'false' indicates BWR signature is not enabled.

Reference: [LLX]

6.2.1.2.6.2 BeaconAckEnable

This attribute configures the use of the BWR-Beacon-Ack signature on the CMTS. Value 'true' indicates BWR-Beacon-Ack signature is enabled. Value 'false' indicates BWR-Beacon-Ack signature is not enabled.

Reference: [LLX]

6.2.1.2.6.3 Rate

This attribute configures the rate at which the CMTS sends a BWR signature or BWR-Beacon-Ack signature.

Reference: [LLX]

6.2.2 CM Mobile Xhaul Configuration Information Model

No BWR-specific configuration parameters are defined for the cable modem.

6.2.3 Access Entity Configuration Information Model

This section defines the configuration information models for Access Entity mobile xhaul use cases defined in [LLX].

6.2.3.1 Access Entity Configuration Data Type Definitions

This section defines any required data type definitions used in the Access Entity Configuration Information Model.

6.2.3.1.1 Access Entity Configuration Complex Data Type Definitions

This section defines classes used in the Access Entity Information Model as complex data types.

6.2.3.1.1.1 FilterType

Refer to the definition of FilterType complex data type in Section 6.2.1.1.1.1, FilterType.

6.2.3.1.1.2 PatternType

Refer to the definition of PatternType complex data type in Section 6.2.1.1.1.4, PatternType.

6.2.3.1.1.3 AeBwrConnectivityType

This class defines parameters for configuring the connectivity between the BWR server and the BWR client.

Reference: [LLX]

Table 16 - AeBwrConnectivityType Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Ethernet	Directed Composition to Ethernet	1	0..*	
UdpIp	Directed Composition to UdpIp	1	0..*	

6.2.3.1.1.3.1 Ethernet

This class defines parameters for an Ethernet connection between the Access Entity BWR client and the BWR server.

Table 17 - Ethernet Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
VlanTag	UnsignedInteger	Read-write	1..4094	

6.2.3.1.1.3.1.1 VlanTag

This attribute configures the virtual LAN tag of the Access Entity BWR client for an Ethernet connection.

Reference: [CTI-ODU]

6.2.3.1.1.3.2 UdpIp

This class defines parameters for an UDP/IP connection between the Access Entity BWR client and the BWR server.

Table 18 - UdpIp Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
VlanTag	UnsignedInteger	Read-write	1..4094	

6.2.3.1.1.3.2.1 VlanTag

This attribute configures the virtual LAN tag of the Access Entity BWR client for a UDP/IP connection.

Reference: [CTI-ODU]

6.2.3.1.1.4 AeServerConnectivityType

This class defines parameters for configuring the connectivity for the BWR server in the CMTS.

Table 19 - AeServerConnectivityType Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Ethernet	Directed Composition to Ethernet	1	0..*	
UdpIp	Directed Composition to UdpIp	1	0..*	

6.2.3.1.1.4.1 Ethernet

This class defines parameters for an Ethernet connection between the Access Entity BWR client and the BWR server.

Table 20 - Ethernet Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
BwrServerMacAddr	MacAddress	Read-write		

6.2.3.1.1.4.1.1 BwrServerMacAddr

This attribute configures the MAC Address for the BWR server in the CMTS to be used as a destination address for BWR messages for an Ethernet connection.

Reference: [CTI-ODU]

6.2.3.1.1.4.2 UdpIp

This class defines parameters for an UDP/IP connection between the Access Entity BWR client and the BWR server.

Table 21 - UdpIp Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
BwrServerHost	Host	Read-write		

6.2.3.1.1.4.2.1 BwrServerHost

This attribute configures the IP address or domain name for the BWR server in the CMTS to be used as a destination address for a UDP/IP connection.

Reference: [CTI-ODU]

6.2.3.2 Access Entity Configuration Class Diagram

Figure 4 - Access Entity Configuration Information Model defines objects for configuration of the Access Entity.

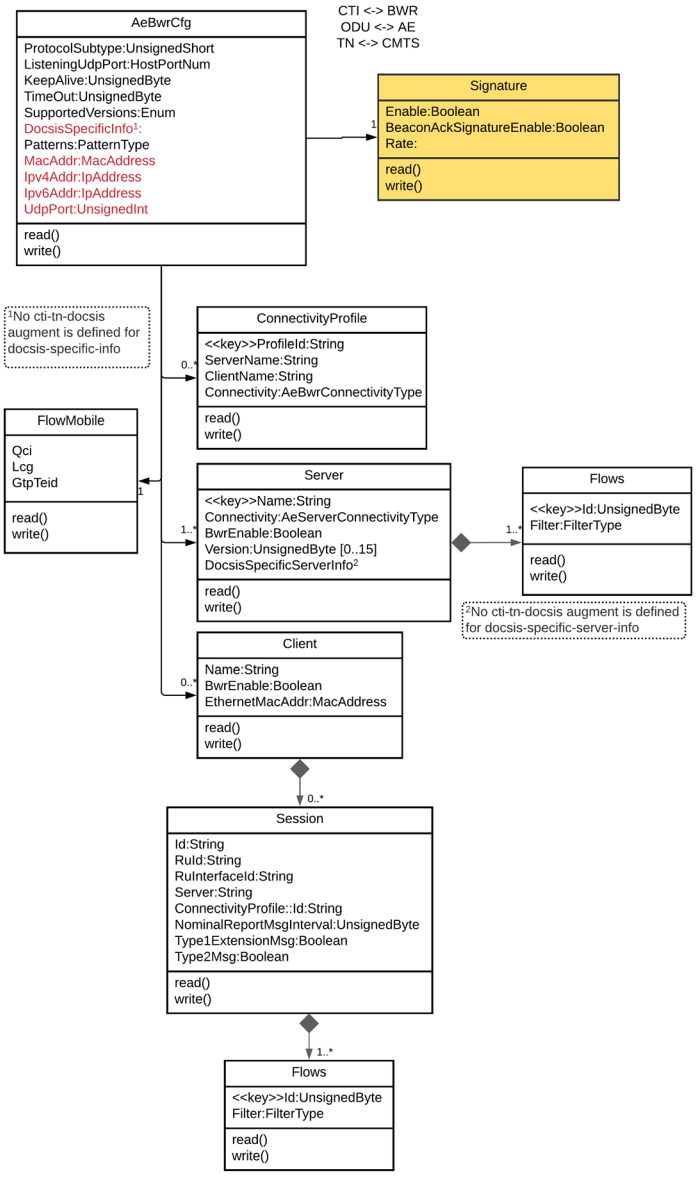

Figure 4 - Access Entity Configuration Information Model

6.2.3.2.1 AeBwrCfg

The AeBwrCfg provides the management interface for Access Entity BWR configuration.

Table 22 - AeBwrCfg Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
ConnectivityProfile	Directed association to ConnectivityProfile	1	0..*	
Server	Directed association to Server	1	1..*	
Client	Directed association to Client	1	0..*	
Beacon	Directed association to Beacon	1	1	
Signature	Directed association to Signature	1	1	
FlowMobile	Directed composition to FlowMobile	1	1	

Table 23 - AeBwrCfg Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
ProtocolSubtype	UnsignedShort	Yes			
ListeningUpdPort	HostPortNum	Yes			
KeepAlive	UnsignedByte	Yes		0.1 second	
TimeOut	UnsignedByte	Yes		0.1 second	
SupportedVersions	Enum	Yes			
Patterns	PatternType	Yes			
MacAddr	MacAddress	Yes			
Ipv4Addr	IpAddress	No			
Ipv6Addr	IpAddress	No			
UdpPort	UnsignedInt	Yes			

6.2.3.2.1.1 ProtocolSubtype

This attribute configures the 16-bit sub-type to be used with the standardized Ethertype value 0x9433 standardized for O-RAN.

Reference: [CTI-ODU]

6.2.3.2.1.2 ListeningUdpPort

This attribute configures the number of the UDP port on the Access Entity on which the Access Entity will receive BWR messages.

Reference: [CTI-ODU]

6.2.3.2.1.3 KeepAlive

This attribute configures the maximum time interval between consecutive BWR-Keep-Alive messages between the BWR client and the BWR server.

Reference: [CTI-ODU]

6.2.3.2.1.4 TimeOut

This attribute configures the timeout value that a BWR-Beacon-Ack message needs to be received by the BWR client or the BWR server before that respective system suspends BWR operations and returns to its BWR configuration state.

Reference: [CTI-ODU]

6.2.3.2.1.5 SupportedVersions

This attribute configures the BWR version(s) supported by the Access Entity.

Reference: [CTI-ODU]

6.2.3.2.1.6 Patterns

This attribute configures the BWR pattern type for the Access Entity.

Reference: [CTI-ODU]

6.2.3.2.1.7 MacAddress

This attribute is the Access Entity Ethernet MAC address. This serves as a globally unique identifier for the Access Entity.

Reference: [CTI-ODU]

6.2.3.2.1.8 Ipv4Address

This attribute configures the Access Entity's IPv4 address.

Reference: [LLX]

6.2.3.2.1.9 Ipv6Address

This attribute configures the Access Entity's IPv6 address.

Reference: [LLX]

6.2.3.2.1.10 UdpPort

This attribute configures the Access Entity with the UDP port number to be used for the BWR connection.

Reference: [LLX]

6.2.3.2.2 ConnectivityProfile

This object provides the management interface for configuring the transport parameters for BWR connectivity between the BWR client and the BWR server.

Table 24 - ConnectivityProfile Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
ProfileId	String	Yes (Key)			
ServerName	String	Yes			
ClientName	String	Yes			
Connectivity	AeBwrConnectivityType	Yes			

6.2.3.2.2.1 ProfileId

This attribute uniquely identifies an instance of the Access Entity Connectivity Profile. Each Connectivity Profile contains parameters for the exchange of BWR messages with the BWR server corresponding to the BWR Session ID.

Reference: [CTI-ODU]

6.2.3.2.2.2 ServerName

This attribute configures the BWR server for this Connectivity Profile.

Reference: [CTI-ODU]

6.2.3.2.2.3 ClientName

This attribute configures the BWR client for this Connectivity Profile.

Reference: [CTI-ODU]

6.2.3.2.2.4 Connectivity

This attribute configures the type of connectivity for this Connectivity Profile.

Reference: [CTI-ODU]

6.2.3.2.3 Server

This object provides the management interface for configuring the BWR server on the Access Entity.

Table 25 - Server Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Flows	Directed composition to Flows	1	0..*	

Table 26 - Server Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Name	String	Yes (Key)			
Connectivity	AeServerConnectivityType	Yes			
BwrEnable	Boolean	Yes			false
Version	UnsignedByte	Yes	0..15		

6.2.3.2.3.1 Name

This key attribute configures the name of the BWR server and uniquely identifies this BWR Server instance for the Access Entity.

Reference: [CTI-ODU]

6.2.3.2.3.2 Connectivity

This attribute configures the connectivity type used by the BWR server in the CMTS.

Reference: [CTI-ODU]

6.2.3.2.3.3 BwrEnable

This attribute configures whether the BWR server in the CMTS is enabled. Value 'true' enables the BWR server. Value ‘false’ disables the BWR server. The default value of this attribute is 'false'.

Reference: [CTI-ODU]

6.2.3.2.3.4 Version

This attribute configures the list of versions of BWR TC-Plane that are supported by the BWR server.

Reference: [CTI-ODU]

6.2.3.2.4 Flows

This object provides the management interface for configuring BWR flows on the BWR server on the Access Entity.

Table 27 - Flows Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Id	UnsignedByte	Yes (Key)			
Filter	FilterType	Yes			

6.2.3.2.4.1 Id

This key attribute uniquely identifies the instance of the Flow Filter for BWR flows.

Reference: [CTI-ODU]

6.2.3.2.4.2 Filter

This attribute configures the type of Flow Filter for the BWR flows.

Reference: [CTI-ODU]

6.2.3.2.5 Client

This object provides the management interface for configuring the BWR server on the Access Entity with information about the BWR Client.

Table 28 - Client Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Session	Directed composition to Session	1	0..*	

Table 29 - Client Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Name	String	Yes (Key)			
BwrEnable	Boolean	Yes			
EthernetMacAddr	MacAddress	No			

6.2.3.2.5.1 Name

This key attribute configures the Client Name that uniquely identifies the instance of BWR Client parameters.

Reference: [CTI-ODU]

6.2.3.2.5.2 BwrEnable

This attribute configures whether the BWR client is enabled for BWR operation. Value ‘true’ enables the BWR client for BWR operation. Value ‘false’ disables the BWR client for BWR operation.

Reference: [CTI-ODU]

6.2.3.2.5.3 EthernetMacAddr

This optional attribute configures the BWR client MAC address.

Reference: [CTI-ODU]

6.2.3.2.6 Session

This object provides the management interface for configuring BWR sessions on the Access Entity.

Table 30 - Session Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Flows	Directed composition to Flows	1	0..*	

Table 31 - Session Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Id	String	Yes			
RuId	String	Yes			
RuInterfaceId	String	Yes			
Server	String	Yes			
ConnectivityProfile::Id	String	Yes			
NominalReportMsgInterval	UnsignedByte	Yes		0.25 milliseconds	
Type1ExtMsg	Boolean	Yes			
Type2Msg	Boolean	Yes			

6.2.3.2.6.1 Id

This attribute configures the Session identifier used as the unique identifier for the Session instance.

Reference: [CTI-ODU]

6.2.3.2.6.2 RuId

This attribute configures the unique identifier for the Radio Unit based on Vendor, equipment, and/or serial number.

Reference: [CTI-ODU]

6.2.3.2.6.3 RuInterfaceId

This attribute configures the identifier for the Radio Unit interface based on O-RU-ID and MAC address of interface.

Reference: [CTI-ODU]

6.2.3.2.6.4 Server

This attribute configures the BWR server to which BWR report messages are to be sent for this BWR Session ID.

Reference: [CTI-ODU]

6.2.3.2.6.5 ConnectivityProfile::Id

This attribute is an instance of the identifier attribute Id for the ConnectivityProfile object.

Reference: [CTI-ODU]

6.2.3.2.6.6 NominalReportMsgInterval

This attribute configures the nominal BWR reporting message interval in 0.25 milliseconds.

Reference: [CTI-ODU]

6.2.3.2.6.7 Type1ExtMsg

This attribute configures the Access Entity use of the Type 1 Extension Message in the BWR report message per BWR session. Value 'true' configures the Access Entity to use the Type 1 Extension Message in the BWR report

message. Value 'false' configures the Access Entity to not use the Type 1 Extension Message in the BWR report message.

Reference: [LLX]

6.2.3.2.6.8 Type2Msg

This attribute configures the Access Entity use of the Type 2 Message per BWR session. Value 'true' configures the Access Entity to use the Type 2 Message. Value 'false' configures the Access Entity to not use the Type 2 Message.

Reference: [LLX]

6.2.3.2.7 Flows

This object provides the management interface for configuring the list of BWR message flows in use for a particular BWR Session Id.

Table 32 - Flows Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Id	UnsignedByte	Yes (Key)			
Filter	FilterType	Yes			

6.2.3.2.7.1 Id

This attribute configures the Flow identifier used as the unique identifier for the Flow instance.

6.2.3.2.7.2 Filter

This attribute configures the type of Flow filter to apply to the BWR session flow.

Reference: [CTI-ODU]

6.2.3.2.8 Signature

This optional object provides the management interface for configuring the BWR Signature on the Access Entity.

Reference: [LLX]

Table 33 - Signature Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Enable	Boolean	No			
BeaconAckSignatureEnable	Boolean	No			
Rate	<TBD>	No		Messages per Second	

6.2.3.2.8.1 Enable

This attribute configures operation of the BWR signature function. If the value of Enable is 'true', the Access Entity enables BWR Digital Signature operation. If the value of Enable is 'false', the Access Entity disables BWR Digital Signature operation.

6.2.3.2.8.2 BeaconAckSignatureEnable

This attribute configures operation of the BWR Beacon-Ack signature. If the value of BeaconAckSignatureEnable is 'true', the Access Entity enables use of the BWR Beacon-Ack Signature. If the value of BeaconAckSignatureEnable is 'false', the Access Entity disables use of the BWR Beacon-Ack Signature.

6.2.3.2.8.3 Rate

This attribute configures the how often the Access Entity is to transmit a BWR Signature or a BWR Beacon-Ack Signature.

6.2.3.2.9 FlowMobile

This object provides the management interface for configuring Long-term Evolution (LTE) quality of service (QoS) on the Access Entity.

Reference: [LLX]

Table 34 - FlowMobile Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Qci	UnsignedShort	No	1..9		
5Qi	UnsignedInt	No	1..255		
Lcg	UnsignedByte	No	0..7		
GtpTeid	UnsignedInt	No			

6.2.3.2.9.1 Qci

This attribute configures the Quality of Service Class Indicator (QCI) for the LTE QoS on the Access Entity.

Reference: [dmm-fpc-cpdp]

6.2.3.2.9.2 5Qi

This attribute configures the Quality of Service Class Indicator for the 5G QoS on the Access Entity.

Reference: [3GPP17MgtOrch]

6.2.3.2.9.3 Lcg

This attribute configures the Logical Channel Group for the LTE QoS on the Access Entity.

Reference: [3GPPTS38.321]

6.2.3.2.9.4 GtpTeid

This attribute configures the GPRS Tunneling Protocol (GTP) Tunnel Endpoint Identifier (TEID) for the LTE QoS on the Access Entity.

Reference: [dmm-fpc-cpdp]

7 MOBILE XHAUL PERFORMANCE MANAGEMENT

DOCSIS Low Latency Mobile Xhaul performance management for CCAP and cable modems provides status and statistics for BWR-related configuration, topology, and operation.

7.1 Data Type Definitions

Refer to [CCAP-OSSIv3.1] Annex F *CCAP Data Type Definitions* for the definition of data types used for the CCAP Performance Information Model.

Refer to [CM-OSSIv3.1] Annex D *Type Definitions* for the definition of data types used for CM information models.

7.2 CCAP Mobile Xhaul Performance Management Information Model

The CCAP Mobile Xhaul Performance Management Information Model has been divided into the following categories:

- State Data: These objects are used to gather state information from the CCAP.
- Statistical Data: These objects are used to gather statistical information from the CCAP.

A CCAP that supports DOCSIS backhaul or DOCSIS midhaul topologies MUST support the Mobile Xhaul Performance Management information model.

7.2.1 CCAP Mobile Xhaul Performance Data Type Definitions

No new data types are defined for the CCAP Mobile Xhaul Performance Management Information Model.

7.2.2 CCAP Mobile Xhaul Status Class Diagram

Figure 5 - CCAP Mobile Xhaul BWR Status Information Model defines objects for CCAP Mobile Xhaul status reporting.

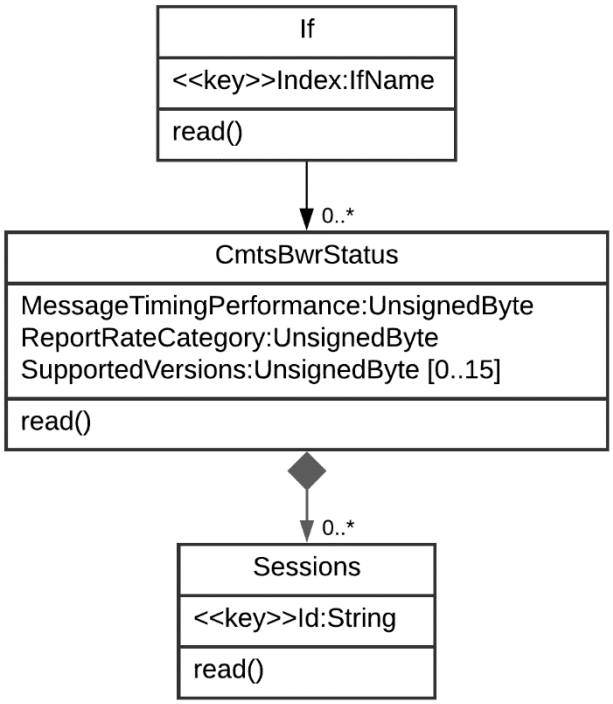

Figure 5 - CCAP Mobile Xhaul BWR Status Information Model

7.2.2.1 CcapBwrStatus

This object provides a management interface for reporting the status of the BWR client in the CCAP.

Table 35 - CcapBwrStatus Object Associations

Associated Object Name	Type		Near-end Multiplicity	Far-end Multiplicity	Label
Sessions	Directed composition to Sessions		1	0..*	

Table 36 - CcapBwrStatus Object Attributes

Attribute Name	Type	Required Attribute	Access	Type Constraints	Units
MessageTimingPerformance	UnsignedByte	Yes	Read-only		20 microseconds
ReportRateCategory	Enum	Yes	Read-only	5(1), 2(2), 1(3), 0.5(4), 0.25(5)	milliseconds
SupportedVersions	UnsignedByte	Yes	Read-only	0..15	

7.2.2.1.1 MessageTimingPerformance

This attribute reports he minimal spacing needed between the arrival time of the BWR message and the start boundary at Ra of the mobile slot N being reported in the message.

Reference: [CTI-TnGeneric]

7.2.2.1.2 ReportRateCategory

This attribute reports the supported message interval in milliseconds. Allowed values are 5 ms, 2ms, 1 ms, 0.5 ms, and 0.25 ms.

Reference: [CTI-TnGeneric]

7.2.2.1.3 SupportedVersions

This attribute reports the list of versions of BWR TC-Plane that are supported by the BWR client.

Reference: [CTI-TnGeneric]

7.2.2.2 Sessions

This optional object reports the list of BWR sessions active in the CCAP.

Table 37 - Sessions Object Attributes

Attribute Name	Type	Required Attribute	Access	Type Constraints	Units
Id	String	Yes (Key)	Read-only		

7.2.2.2.1 Id

This key attribute is the unique identifier within the MAC Domain for the BWR Session.

Reference: [CTI-TnGeneric]

7.3 CM Mobile Xhaul Performance Management Information Model

No BWR-specific statistics or counters are defined for the cable modem.

7.4 Access Entity Performance Management Information Model

This section defines the Performance Management Information Model for the Access Entity.

7.4.1 Access Entity Performance Data Type Definitions

No new data types are defined for the Access Entity Performance Management Information Model.

7.4.2 Access Entity Status Class Diagram

Figure 6 - Access Entity Status Information Model defines objects for Access Entity status reporting.

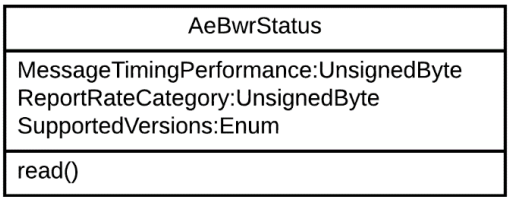

Figure 6 - Access Entity Status Information Model

7.4.2.1 AeBwrStatus

This object provides a management interface for reporting the status of the BWR client in the Access Entity.

Table 38 - AeBwrStatus Object Attributes

Attribute Name	Type	Required Attribute	Access	Type Constraints	Units
MessageTimingPerformance	UnsignedByte	Yes	Read-only		20 microseconds
ReportRateCategory	Enum	Yes	Read-only	5(1), 2(2), 1(3), 0.5(4), 0.25(5)	milliseconds
SupportedVersions	UnsignedByte	Yes	Read-only	0..15	

7.4.2.1.1 MessageTimingPerformance

This attribute reports the minimal spacing needed between the arrival time of the BWR message and the start boundary at Ra of the mobile slot N being reported in the message.

Reference: [CTI-ODU]

7.4.2.1.2 ReportRateCategory

This attribute reports the supported message interval in milliseconds. Allowed values are 5 ms, 2ms, 1 ms, 0.5 ms, and 0.25 ms.

Reference: [CTI-ODU]

7.4.2.1.3 SupportedVersions

This attribute reports the list of versions of BWR TC-Plane that are supported by the BWR client.

Reference: [CTI-ODU]

8 MOBILE XHAUL FAULT MANAGEMENT

8.1 CCAP Mobile Xhaul Fault Management

Event notification for DOCSIS Mobile Xhaul operation for the CCAP follows the CCAP Event Notification Information Model and Fault Management and Reporting requirements defined in [CCAP-OSSIv3.1]. Mobile Xhaul- and BWR-specific events for the CCAP listed in Table 39 - Event Format and Content below are extensions of *Format and Content for Event, SYSLOG, and SNMP Notification* in [CCAP-OSSIv3.1] Annex D.

Table 39 - Event Format and Content

Process	Sub-Process	CMTS/ CCAP Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID	Notification Name
Mobile Xhaul							
AE	Init	Debug	AE authenticated<TAGS>;		Y.200.0	89020000	CMTS: docsIf3CmtsEventNotif
BWR	Connection	Error	BWR transport system did not become operational: BWR Beacon not received<TAGS>;		Y.200.1	89020001	CMTS: docsIf3CmtsEventNotif
BWR	Connection	Error	BWR transport system did not become operational: BWR Report not received<TAGS>;		Y.200.2	89020002	CMTS: docsIf3CmtsEventNotif
BWR	Connection	Debug	BWR transport system is operational<TAGS>;		Y.200.3	89020003	CMTS: docsIf3CmtsEventNotif
BWR	Connection	Error	BWR transport system suspended: BWR Report not received<TAGS>;		Y.200.4	89020004	CMTS: docsIf3CmtsEventNotif
BWR	Connection	Error	BWR transport system suspended: BWR Keep Alive not received<TAGS>;		Y.200.5	89020005	CMTS: docsIf3CmtsEventNotif
BWR	Connection	Error	BWR_KA timer exhausted<TAGS>;		Y.200.6	89020006	CMTS: docsIf3CmtsEventNotif
BWR	Connection	Error	BWR_TO timer exhausted<TAGS>;		Y.200.7	89020007	CMTS: docsIf3CmtsEventNotif
BWR	Connection	Warning	BWR Keep Alive not received<TAGS>;		Y.200.8	89020008	CMTS: docsIf3CmtsEventNotif

8.2 Access Entity Fault Management

Access Entity fault management is out of scope for this specification.

Appendix I Acknowledgements

We wish to thank the following participants contributing directly to this document.

Contributor	Company Affiliation
Ram Ranganathan	Commscope
Steve Burroughs	CableLabs
Kevin Luehrs	CableLabs

* * *