Point-to-Point Coherent Optics

Coherent Optics Termination Device OSSI Specification

P2PCO-SP-CTD-OSSI-I02-200501

ISSUED

DISCLAIMER

Document Status Sheet

Document Control Number:	P2PCO-SP-CTD-OSSI-I02-200501			
Document Title:	Coherent Optics Termination Device OSSI Specification			
Revision History:	D01 - Released 3/11/2019 D02 - Released 5/9/2019 I01 - Released 6/14/2019 I02 - Released 5/1/2020			
Date:	May 1, 2020			
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 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 Member and Technology Supplier review, cross-vendor interoperability, and is for Certification 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

Table of Contents

List of Figures

List of Tables

1 SCOPE

1.1 Introduction and Purpose

This specification is part of the Point-to-Point Coherent Optics (P2PCO) family of specifications developed by Cable Television Laboratories (CableLabs). These specifications enable the development of interoperable transceivers using coherent optical technology over point-to-point (P2P) links. This specification was developed for the benefit of the cable industry and includes contributions by operators and vendors from North and South America, Europe, Asia, and other regions.

This specification defines the Operations Support System Interface (OSSI) requirements for the Coherent Optics Termination Device (CTD), which includes a transceiver that terminates one end of a P2P coherent optics link. The scope includes requirements for managing the Point-to-Point Coherent Optics Transceiver in the CTD independent of the pluggable form factors in which the transceiver may be deployed (which define the mechanism by which information is shared between the Point-to-Point Coherent Optics Transceiver and the CTD).

1.2 Background

Most operators have a very limited number of fibers available between the Headend (HE)/Hub and the fiber node to use for data and video services; often only 1-2 fiber strands are available to serve groups of fiber nodes. With end users demanding more bandwidth to the home, operators need a strategy for increasing capacity in the optical access network. A solution that re-uses the existing infrastructure much more efficiently is preferred. One such solution is to use coherent optics technology in conjunction with Wavelength Division Multiplexing (WDM) in the optical access network.

Coherent optics technology is common in the submarine, long-haul, and metro networks, but has not yet been applied to access networks due to the relatively high cost of the technology for those applications. However, the cable access network differs from the other types of networks in the following ways: distances from the HE/Hub to the fiber node are much shorter, the network is always a point-to-point architecture, and fixed-wavelength optical passives are utilized. With these differences, the capabilities, performance, and features of transceivers can be relaxed in areas such as optical output power level, transmitter wavelength capability, the amount of fiber chromatic dispersion compensation, and transmitter optical-to-signal-noise ratio (OSNR). This potentially allows lower cost designs and the use of lower cost components in cable access networks. Using coherent optics in the access network opens new possibilities for cable operators as well as for other telecommunication service providers.

Refer to [OPT-P2P-ARCH] for additional details and definitions.

1.3 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.

This document defines many features and parameters, and a valid range for each parameter is usually specified. Equipment (CTD) requirements are always explicitly stated. Equipment complying with all mandatory (MUST and

MUST NOT) requirements is considered compliant with this specification. Support of non-mandatory features and parameter values is optional.

1.4 Device Under Test

Because the "Point-to-Point Coherent Optics Transceiver" – hereafter referred to simply as a transceiver – is not independently addressable, the requirements in this specification are written against the Coherent Optics Termination Device (hereafter referred to as the CTD) which contains the transceiver, even though many of the requirements apply to information from or the configuration of the transceiver.

1.5 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
```

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

1.6 Organization of Document

Section 1 provides an overview of the Coherent Optics Termination Device OSSI specification.

Sections 2 through 4 includes the references, terms, and acronyms used throughout this specification.

Section 5 introduces the FCAPS Network Management Model that forms the organizational foundation of this specification. To maintain consistency with other CableLabs OSSI specifications, the order of the management functions is reordered as follows:

- Configuration Management
- Performance Management
- Accounting Management
- Fault Management
- Security Management

The coherent optics management model via the Coherent Termination Device management agent is described in depth.

Section 6 defines the Configuration Management functions of the transceiver including the management protocols and Information models.

Section 7 defines the Performance Management functions of the transceiver including Information Models.

Section 7.2 defines the Fault Management functions of the transceiver including network management protocols, event reporting requirements, Information Models.

Section 8 defines the Management Protocols include Data Mapping, SNMP and MIB requirements, SNMP protocol and agent requirements, RFCs and CableLabs MIBs, and NETCONF protocol and server requirements. Data model requirements are also included.

1.6.1 Annexes (Normative)

Annex A includes a detailed list of MIB Requirements for the CTD.

Annex B defines the format and content for Event, SYSLOG, and SNMP Notification and NETCONF Notification.

Annex C describes the Data Type Definitions used in both the Information Models and data models.

1.6.2 Appendices (Informative)

Appendix I listed the acknowledgements for authoring this specification.

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.

[CANN]	CableLabs' Assigned Names and Numbers, CL-SP-CANN-I19-190422, April 22, 2019, Cable Television Laboratories, Inc.
[COOPT-CTD-EVENTS-YANG]	P2P Coherent Optics: COOPT-CTD-EVENTS-YANG, http://mibs.cablelabs.com/YANG/CoherentOptics [for future release]
[COOPT-CTD-MIB]	P2P Coherent Optics: COOPT-CTD-MIB, http://mibs.cablelabs.com/MIBs/CoherentOptics [for future release]
[COOPT-CTD-YANG]	P2P Coherent Optics: COOPT-CTD-YANG, http://mibs.cablelabs.com/YANG/CoherentOptics [for future release]
[IEEE-754-2019]	IEEE 754-2019 – IEEE Standard for Floating-Point Arithmetic
[OPT-P2P-PHY]	P2P Coherent Optics Transceiver Physical Layer Specification, P2PCO-SP-PHYv1.0-I03-200501, May 1, 2020, Cable Television Laboratories, Inc.
[RFC 1157]	A Simple Network Management Protocol
[RFC 1901]	Introduction to Community-based SNMPv2 (Informational)
[RFC 2573]	IETF RFC 2573, SNMP Applications, April 1999.
[RFC 2575]	IETF RFC 2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), April 1999.
[RFC 2578]	IETF RFC 2578, Structure of Management Information Version 2 (SMIv2), April 1999.
[RFC 2579]	Textual Conventions for SMIv2
[RFC 2580]	Conformance Statements for SMIv2
[RFC 2856]	IETF RFC 2856
[RFC 2863]	IETF RFC 2863, The Interfaces Group MIB, June 2000.
[RFC 4546]	IETF RFC 4546
[RFC 4639]	IETF RFC 4639, Cable Device Management Information Base for Data-Over-Cable Service Interface Specification (DOCSIS) Compliant Cable Modems and Cable Modem Termination Systems, December 2006.
[RFC 3412]	IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), December 2002.
[RFC 3418]	IETF RFC 3418/STD0062, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), December 2002.
[RFC 5277]	IETF RFC 5277, NETCONF Event Notifications, July 2008.
[RFC 6020]	IETF RFC 6020, YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF), October 2010
[RFC 6021]	IETF RFC 6021
[RFC 6241]	IETF RFC 6241, Network Configuration Protocol (NETCONF), June 2011
[RFC 6242]	IETF RFC 6242, Using the NETCONF Protocol over Secure Shell (SSH), June 2011
[RFC 6243]	IETF RFC 6243, With-defaults Capability for NETCONF, June, 2011
[RFC 6933]	IETF RFC 6933
[RFC 6991]	IETF RFC 6991, Common YANG Data Types, July 2013
[RFC 7950]	IETF RFC 7950, The YANG 1.1 Data Modeling Language, August 2016.
[RFC 8341]	IETF RFC 8341, Network Configuration Access Control Model, March 2018

2.2 Informative References

This specification uses the following informative references.

[CFP MIS]	CFP MSA Management Interface Specification, Version 2.6 r06a, March 24, 2017, http://www.cfp-msa.org/Documents/CFP_MSA_MIS_V2p6r06a.pdf
[ISO 11404]	ISO/IEC 11404, Information Technology -- General Purpose Datatypes (GPD), 2007.
[ITU-T M.3400]	ITU-T Recommendation M.3400 (02/2000): TMN AND Network Maintenance: International Transmission Systems, Telephone Circuits, Telegraphy, Facsimile and Leased Circuits, TMN management functions.
[ITU-T X.692]	ITU-T Recommendation X.692, Information technology - ASN.1 encoding rules: Specification of Encoding Control Notation (ECN) (08/2015)
[OPT-P2P-ARCH]	P2P Coherent Optics Architecture Specification, P2PCO-SP-ARCH-I02-190311, March 11, 2019, Cable Television Laboratories, Inc.
[RFC 3410]	Introduction and Applicability Statements for Internet Standard Management Framework
[RFC 3411]	IETF RFC 3411/STD0062, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, December 2002.
[RFC 3413]	IETF RFC 3413, Simple Network Management Protocol (SNMP) Applications, December 2002.
[RFC 3414]	IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.
[RFC 3415]	IETF RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002.
[RFC 3416]	IETF RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), December 2002.
[RFC 3417]	IETF RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP), December 2002.
[RFC 3419]	IETF RFC 3419, Textual Conventions for Transport Addresses, December 2002.
[RFC 3584]	IETF RFC 3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, August 2003.
[RFC 4001]	IETF RFC 4001, Textual Conventions for Internet Network Addresses, February 2005.
[RFC 4181]	IETF RFC 4181, Guidelines for Authors and Reviewers of MIB Documents, September 2005.
[RFC 4291]	IETF RFC 4291, IP Version 6 Addressing Architecture, February 2006.
[UML Modeling 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
- American National Standards Institute, Inc. 1819 L Street, NW, 6th floor Washington, DC 20036; Phone +1-202-293-8020; Fax +1-202-293-9287; http://www.ansi.org
- IETF, 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/
- CFP MSA, http://www.cfp-msa.org/documents.html
- ITU-T: International Telecommunications Union, Telecommunication Standardization Sector, https://www.itu.int/en/ITU-T/Pages/default.aspx

3 TERMS AND DEFINITIONS

This specification uses the following terms:

Bit	The basic unit of information in computing and digital communications. A bit has one of two values, either 0 or 1, that can be represented electrically and optically as "off " (0) or "on" (1).
Coherent Optics	Coherent Optics encodes information in both in-phase (I) and quadrature (Q) amplitude components of a carrier.
Coherent Optics Termination Device (CTD)	The IP addressable switch, router, or muxponder through which one or more Coherent Optics transceivers are managed. This device hosts the management agent that implements the management requirements described in this specification.
Coherent Optics Transceiver	A transceiver supporting P2P Coherent Optics technology. Refer to Transceiver definition.
Distribution Hub	A location in a cable television network which performs the functions of a headend for customers in its immediate area, and which receives some or all of its television program material from a Master Headend in the same metropolitan or regional area.
Downstream	In cable television, the direction of transmission from the headend to the subscriber.
Ethernet	Computer networking protocol used to send frames between a source and destination address at OSI Layer 2.
Ethernet Switch	A network device for doing Ethernet packet switching.
FCAPS	A set of principles for managing networks and systems, wherein each letter represents one principle. F is for Fault, C is for Configuration, A is for Accounting, P is for Performance, and S is for Security.
Forward Error Correction (FEC)	Forward Error Correction (FEC) is used in optical transmission systems to overcome the effects of noise and other system impairments on the transmitted signal. All FEC schemes add symbols to the transmitted data in such a way that the receiver can recognize and recover from symbol detection errors. The extra symbols – FEC overhead – are added at the transmitter and removed at the receiver.
Gigabit	One billion bits.
Gigahertz (GHz)	One billion cycles per second.
Headend (HE)	A central facility that is used for receiving, processing, and combining broadcast, narrowcast and other signals to be carried on a cable network. Somewhat analogous to a telephone company's central office. Location from which the DOCSIS cable plant fans out to subscribers. See also *distribution hub*.
Internet Protocol (IP)	The computer network protocol (analogous to written and verbal languages) that all machines on the Internet must know so that they can communicate with one another. IP is a layer 3 (network layer) protocol in the OSI model. The vast majority of IP devices today support IP version 4 (IPv4) defined in RFC 791, although support for IP version 6 (IPv6, RFC 2460) is increasing.
IQ Modulation	A method of combining two input channels into one by multiplying the "in-phase" (I) channel by the cosine and the "quadrature" (Q) channel by the sine. This way there is a phase of 90° between them, then added together, the modulator sends the combined signal through the output channel.
Jitter	The fluctuation in the arrival time of a regularly scheduled event such as a clock edge or a packet in a stream of packets. Jitter is defined as fluctuations above 10 Hz.
Kilometer (km)	One thousand meters.
Latency	The time taken for a signal element to pass through a device.
Layer	A subdivision of the Open System Interconnection (OSI) architecture, constituted by subsystems of the same rank.
Management Object	A generic term for either an SNMP MIB object or a YANG object. When this term is used, it applies to both SMIv2 and YANG objects. Functions on the CCAP that monitor for faults and for overall system performance, including traps and alarms.
Management Information Base	A database of device configuration and performance information which is acted upon by SNMP.
Media Access Control (MAC)	Used to refer to the OSI Layer 2 element of the system.
MUX/DEMUX	A device that combines and separates multiple wavelengths/channels from multiple fibers (usually 1 fiber per wave) onto a single fiber with multiple wavelengths.

Muxponder	Combination transponder and multiplexer in a single device. The muxponder refers to an electrical multiplexer that combines up to 10 by10 Gbps interfaces of into a single 100Gbps coherent interface.
Network Configuration Protocol	An IETF network management protocol that provides mechanisms to manipulate the configuration of a device, commonly referred to as NETCONF. NETCONF executes YANG-based XML files containing configuration objects.
Physical Layer (PHY)	Layer 1 in the Open System Interconnection (OSI) architecture; the layer that provides services to transmit bits or groups of bits over a transmission link between open systems and which entails optical, electrical, mechanical and handshaking procedures (PHY).
Quadrature Amplitude Modulation (QAM)	A modulation technique in which an analog signal's amplitude and phase vary to convey information, such as digital data. The name "quadrature" indicates that amplitude and phase can be represented in rectangular coordinates as in-phase (I) and quadrature (Q) components of a signal.
Quadrature Phase Shift Keying (QPSK)	A form of digital modulation in which four phase states separated by 90° support the transmission of two bits per symbol. Also, called 4-QAM.
Simple Network Management Protocol	Allows a host to query modules for network-related statistics and error conditions.
Transceiver	A combination of transmitter and receiver in the same device or component.
Upstream	The direction from the subscriber location toward the head.
YANG	A data modeling language for the NETCONF network configuration protocol.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

ADC	Analog to Digital Converter
APC	Angled Physical Contact
ASE	Amplified Spontaneous Emission
ASIC	Application-Specific Integrated Circuit
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BSS	Business Support System
bps	bits per second
CableLabs	Cable Television Laboratories, Inc.
CCAP	Converged Cable Access Platform
CD	Chromatic Dispersion
CFP	C Form-Factor Pluggable
CFP MSA	C Form-Factor Pluggable Master-Source Agreement
CFP2-DCO	CFP2-Digital Coherent Optics
CLI	Command Line Interface
CMA	Constant Modulus Algorithm
CMOS	Complementary Metal-Oxide Semiconductor
CMTS	Cable Modem Termination System
CTD	Coherent Optics Termination Device
DAC	Digital to Analog Converter
dB	Decibel
dBm	Decibel-milliwatts
DEMUX	Demultiplexer
DFB	Distributed Feedback (laser)
DGD	Differential Group Delay
DP-QPSK	Dual Polarization - Quadrature Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DSP	Digital Signal Processor
DWDM	Dense Wave Division Multiplexing
ECL	External Cavity Laser
EDD	Error Decorrelator De-interleaver
EDFA	Erbium-Doped Fiber Amplifier
EDI	Error Decorrelator Interleaver
EPON	Ethernet Passive Optical Network
FEC	Forward Error Correction
FCAPS	Fault, Configuration, Accounting, Performance and Security
FWM	Four-Wave Mixing
GBaud	Gigabaud
Gbps	Gigabit per second
GE, GbE	Gigabit Ethernet
GHz	Gigahertz
HD	High Definition
IF	Interface
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector
kbit/s	Kilobits per second

kHz	Kilohertz
krad	kiloradians
LO	Local Oscillator
MAC	Media Access Control
MIB	Management Information Base
MLG	Multi-Link Gearbox
MSA	Multi-Source Agreement
MSO	Multiple Systems Operator
MUX	Multiplexer
MZM	Mach-Zehnder Modulator
NETCONF	Network Configuration Protocol
nm	Nanometer
NMS	Network Management System
NOC	Network Operations Center
NRZ	Non-Return Zero
ODC	Optical Distribution Center
ODU	Optical Data Unit
OH	Overhead
OIF	Optical Internetworking Forum
OLT	Optical Line Terminal
OOB	Out-of-Band
OOK	On-Off Keying
OPM	Optical Power Meter
OPU	Optical Payload Unit
OSA	Optical Spectrum Analyzer
OSNR	Optical Signal to Noise Ratio
OSS	Operations Support System
OSSI	Operations Support System Interface
OTN	Optical Transport Network
OTU	Optical Transport Unit
OUI	Organization Unique Identifier
P2P	Point-to-Point
P2PCO	Point-to-Point Coherent Optics
PAM	Pulse Amplitude Modulation
PBC	Polarization Beam Combiner
PBS	Polarization Beam Splitter
PDL	Polarization Dependent Loss
PDM	Polarization Division Multiplexing
PHY	Physical
PIC	Photonic Integration Circuit
PLC	Planar Lightwave Circuit
PM	Polarization Multiplexing
PMD	Polarization Mode Dispersion
PON	Passive Optical Network
ppm	Parts per million
ps	Picosecond
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
QSFP	Quad Small Form-factor Pluggable

RF	Radio Frequency
RIN	Relative Intensity Noise
RPD	Remote PHY Device
Rx	Receiver
SOP	State of Polarization
SMF	Single Mode Fiber
SNMP	Simple Network Management Protocol
SPM	Self-Phase Modulation
Tb	Terabit
TIA	Transimpedance Amplifier
Tx	Transmitter
UML	Unified Modeling Language
VOA	Variable Optical Attenuator
WDM	Wave Division Multiplexing
XPM	Cross-phase Modulation

5 OVERVIEW

The Coherent Optics transceiver is not IP-addressable and therefore cannot be natively managed via higher layer protocols such as SNMP and NETCONF. Therefore, the specification defines a generic, manageable construct termed a Coherent Optics Termination Device (CTD). The CTD is any switch, muxponder, router, or similar device that supports the Coherent Optics Transceiver and conforms to the management recommendations defined in this specification. The managed features of the transceiver are then exposed through the management agent on the CTD.

5.1 FCAPS Network Management Model

The International Telecommunication Union (ITU) Recommendation [ITU-T M.3400] 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 CTD.

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 below.

5.2 CTD Network Topology

The CTD relationship within the network topology of P2P Coherent Optics is described in [OPT-P2P-ARCH].

5.3 Management Architectural Overview

Figure 1 illustrates the Coherent Optics management architecture. The CTD resides within the Network Layer where services are provided to end Subscribers and various metrics are collected about network and service performance, among other things. 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 (i.e., CTDs) within the Network Layer.

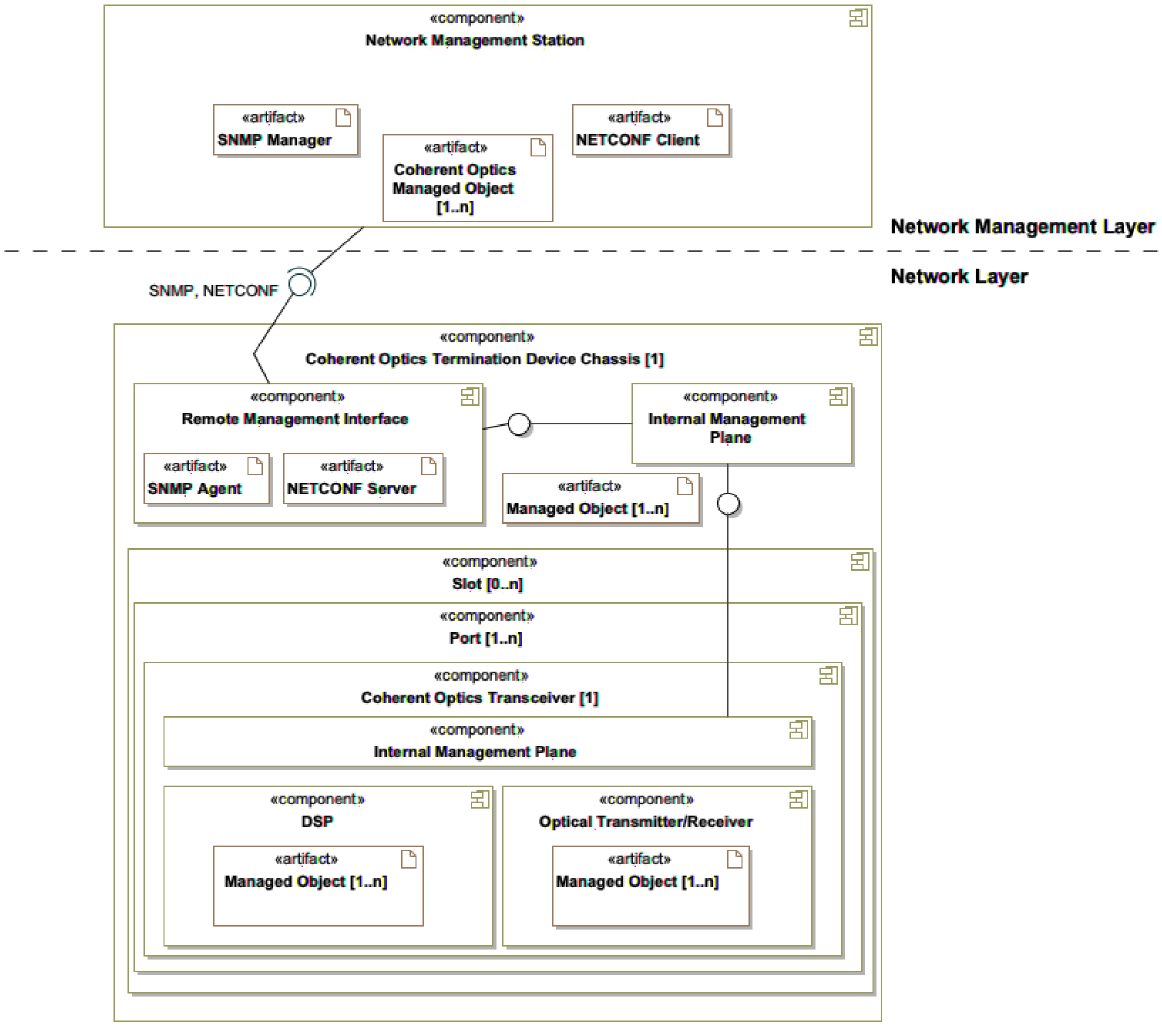

Figure 1 - Coherent Optics Management Architecture Model

Finally, the Business and Service Management Layer (not depicted), which sits north of the Network Management Layer, is where higher-level MSO business processes are implemented via BSS/OSS systems. These BSS/OSS systems utilize the data and information from the Network Management Layer which interrogate data from the Network Layer. Figure 1 shows components and their respective resource artifacts that reside at the Network Layer and Network Management Layer. The Business and Service Management Layer is omitted, as this is not in scope for this specification.

Referring to the architecture in Figure 1 from the bottom up, the CTD resides at the bottom of the Network Layer stack. A CTD has managed resources (referred to as "Managed Objects") that are accessed through two types of management interfaces. A resource may be managed over SNMP via a set of MIBs defining managed objects. A resource may be managed via NETCONF via a set of YANG modules defining managed objects.

A CTD is composed of a set of physical and logical components, where each component may contain a set of managed objects. These include the CTD chassis, zero or more slots (i.e., line cards) containing one or more ports. For each port there is a corresponding Coherent Optics Transceiver. The CTD communicates management and control information over an Internal Management Plane with the Coherent Optics Transceiver, which contains a Digital Signal Processor (DSP) function and Optical Transmitter/Receiver function. The DSP function may be on a line card or a pluggable transceiver. The Optical components consist of a laser (either tunable or fixed wavelength), coherent modulator, and a coherent laser to modulate data onto an optical link and a receiver for the incoming optical signal to be converted into an electrical signal. The CTD contains a Remote Management Interface to support management via SNMP and/or NETCONF and includes an SNMP Agent and NETCONF Server, which are a set of software services that instantiate the corresponding data models. Each management agent configures the transceiver as directed via updates to the CTD data model. The corresponding agent reads the management objects to obtain performance data (i.e., configuration state, status, and statistics data).

Finally, the Network Management Station (NMS) resides in the Network Management Layer and has a representation of all CTD-managed resources. The NMS utilizes the management interfaces shown for managed resources within the CTD. From the NMS point of view, there are no separate resources for physical and logical components with the CTD resource because the CTD abstracts these into a unified view, shown as Coherent Optics Managed Objects in Figure 1.

5.4 Management Use Cases

This section defines a set of use cases for the FCAPS functions. In all the following use cases the <<subsystem>> is the addressable network component (i.e., network node) in which the CTD resides (e.g., switch, muxponder, router, etc.) rather than the transceiver itself.

5.4.1 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. Example Fault Management use cases are shown in Figure 2.

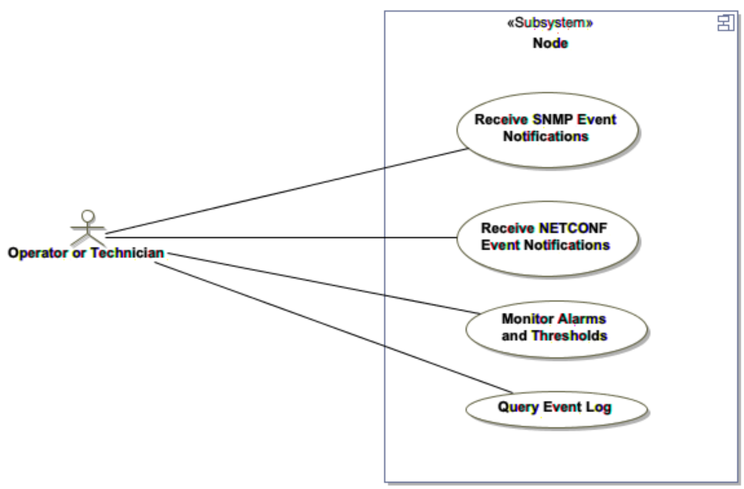

Figure 2 - Fault Management Use Cases

5.4.2 Configuration Management

Configuration Management provides a set of network management functions that typically enables transceiver configuration. Example Configuration Management use cases are shown in Figure 3.

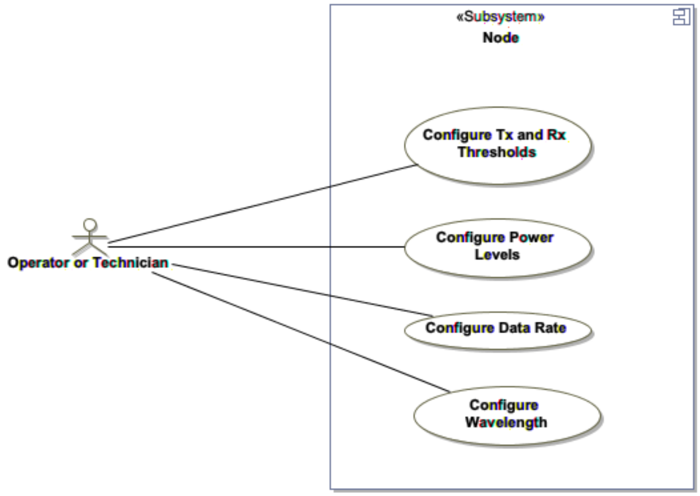

Figure 3 - Configuration Management Use Cases

Configuration Management is primarily concerned with network control via modifying operating parameters on network elements such as the CTD. For Coherent Optics, configuration parameters include the transceiver physical resources.

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 CTD device Configuration Management function may detect that the transmit power has dropped below minimum required level and send the command to increase transmit output.

5.4.3 Performance Management

Performance Management is a proactive and on-demand network management function. [ITU-T M.3400] 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." Example Performance Management use cases are shown in Figure 4.

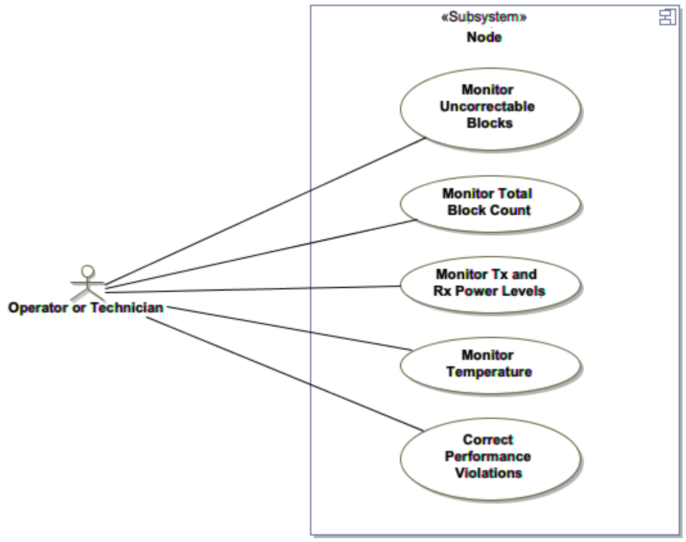

Figure 4 - Performance Management Use Cases

A Performance Management use case might include the NOC performing periodic (15 minutes, for example) collections of transceiver power levels, Pre FEC BER, and Uncorrectable Code Block Counts to identify any potential performance issues that may be occurring on monitored links. 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. Performance Management functions may also include collecting link statistics from the headends and nodes such as traffic loads, frames lost, CRC errors, etc.

5.5 Coherent Optics Management Key Features

Table 1 summarizes the new requirements that support the Coherent Optics transceiver features. The table shows the management features along with the traditional Network Management Functional areas (Fault, Configuration, Accounting, Performance and Security) for the Network Elements (Coherent Optics Transceiver) and the corresponding OSI layer where those features operate.

Table 1 - Management Feature Requirements for Coherent Optics

Features	Management Functional Area	Phy Layer	Description
Proactive monitoring	Configuration	Optics, DSP	Provisioning signal thresholds and performance monitoring intervals
Signal Loss	Fault	Optics	Exceptions to optimal operations Alarm raised when optical signal at Tx or Rx is below vendor-defined minimum output (Tx) or input (Rx) optical power thresholds
Signal Degrade, Loss of Frame	Fault	DSP	Metrics
Laser Power Levels, Temperature	Performance	PHY, MAC, Network	Collection of statistical data sets for link utilization, errors, etc.
Asynchronous Alarms and Events	Fault	Optics, DSP	Minimum/maximum performance thresholds exceeded

5.5.1 Fault Management Features

The goals of fault management are to provide failure detection, diagnosis, and perform or indicate necessary fault correction. Fault identification relies on the ability to monitor and detect problems, such as error-detection events. Fault resolution relies on the ability to diagnose and correct problems. Coherent Optics Transceivers support asynchronous event reporting via the form factor specific interface (e.g., CFP).

CTD Fault Management requirements include:

- Receive and log CTD notifications correlated to transceiver events
- Reporting Loss of Signal
- Generating asynchronous fault notifications

5.5.2 Configuration Management Features

Configuration management is concerned with adding, initializing, maintaining, and updating network elements. In a Coherent Optical environment, network elements include the DSP and Optics.

Configuration management is primarily concerned with modifying operating parameters on network elements such as the CTD. Configuration parameters apply to physical resources (for example, a switched Coherent Optics port) and logical objects (the corresponding ifIndex status for the CTD port).

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 TxPower level. A fault management function may detect and isolate a fault and subsequently issue a configuration change to mitigate or correct that fault.

Configurable objects may also be queried for status of configured objects. Coherent Optics Configuration Management requirements include:

- Transceiver configuration updates
- Transmit wavelengths
- Minimum and Maximum Power Thresholds

5.5.3 Performance Management Features

Performance management functions include reporting status and collecting statistics of parameters such as number of uncorrectable block counts and chromatic dispersion. These monitoring functions are used to determine the health of the coherent optics link. It is anticipated performance information will also enable proactive network management (PNM).

Coherent Optics Performance Management requirements include:

- Transceiver performance data collection
- Link signal quality monitoring for fiber node status and health
- Statistics for dropped frames
- Statistics for link and transceiver errors and traffic volume
- Status objects to report temperature, modulation, and symbol rate unless these are configuration objects.

5.6 Information Models

The Information Model approach is based on object-oriented modeling well known in the industry for capturing requirements and analyzing the data in a protocol-independent representation. This approach defines requirements with use cases to describe the interactions between the operations support systems and the network element. The management information is represented in terms of objects along with their attributes and the interactions between these encapsulated objects (or also referred to as entities in some representations). The diagrams developed to capture these managed objects and their attributes and associations are UML Class Diagrams. The collection of UML Class Diagrams and Use Case Diagrams are referred to as the Coherent Optics Information Models.

The managed objects are then represented in a protocol-specific form referred to as a management data model such as SNMP. SNMP objects and syntax are described using the Structure of Management Information Version 2 (SMIv2) [RFC 2578] and the design of these models is determined by the capabilities of the protocol. The management data models when using NETCONF are described using the YANG data modeling language [RFC 7950] [RFC 6020].

This protocol-agnostic Information Model abstraction enables consistent migration to new management protocols such as NETCONF.

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

6 .CONFIGURATION MANAGEMENT

The Coherent Optics transceiver is primarily pre-configured by the transceiver manufacturer. The configuration is documented in the form-factor documentation supplied by the manufacturer. Remote configuration is available to the MSO via a vendor-defined CLI. In addition to the manufacturer configuration, a subset of objects may be configured using SNMP or NETCONF. The configurable objects are described in the Information Model below.

Installation and initial configuration procedures of a Coherent Optics transceiver are vendor-specific and not included in this specification. This section defines the minimum set of managed objects required to configure a CTD-hosted transceiver. It includes only requirements directly associated with transceiver configuration management at the physical layer. For example, though the CTD most likely supports IPv4 andIPv6, there are no configuration management requirements for such support in this specification.

6.1 Configuration Management Information Model

This section defines the transceiver and CTD requirements for configuration management functions. The Information Model is divided into six groupings.

- Ctd: The Coherent Termination Device container configuration is not within the scope of this specification. It is included to provide context for the transceiver object. This containment hierarchy includes the CTD chassis, slots, line cards and ports associated with the Coherent Optics Transceiver.
- CtdCfg: Defines event reporting configuration for the CTD.
- TransceiverCfg: Defines the DSP and Optical configuration objects.
- DspCfg: Defines the Digital Signal Processor configuration object(s)
- OpticsCfg: Defines Optics component configuration objects.
- IfEnetCfg: Defines Ethernet interface configuration objects.

The objects for configuring a Coherent Optics transceiver, as managed by the CTD, are shown in Figure 5 below.

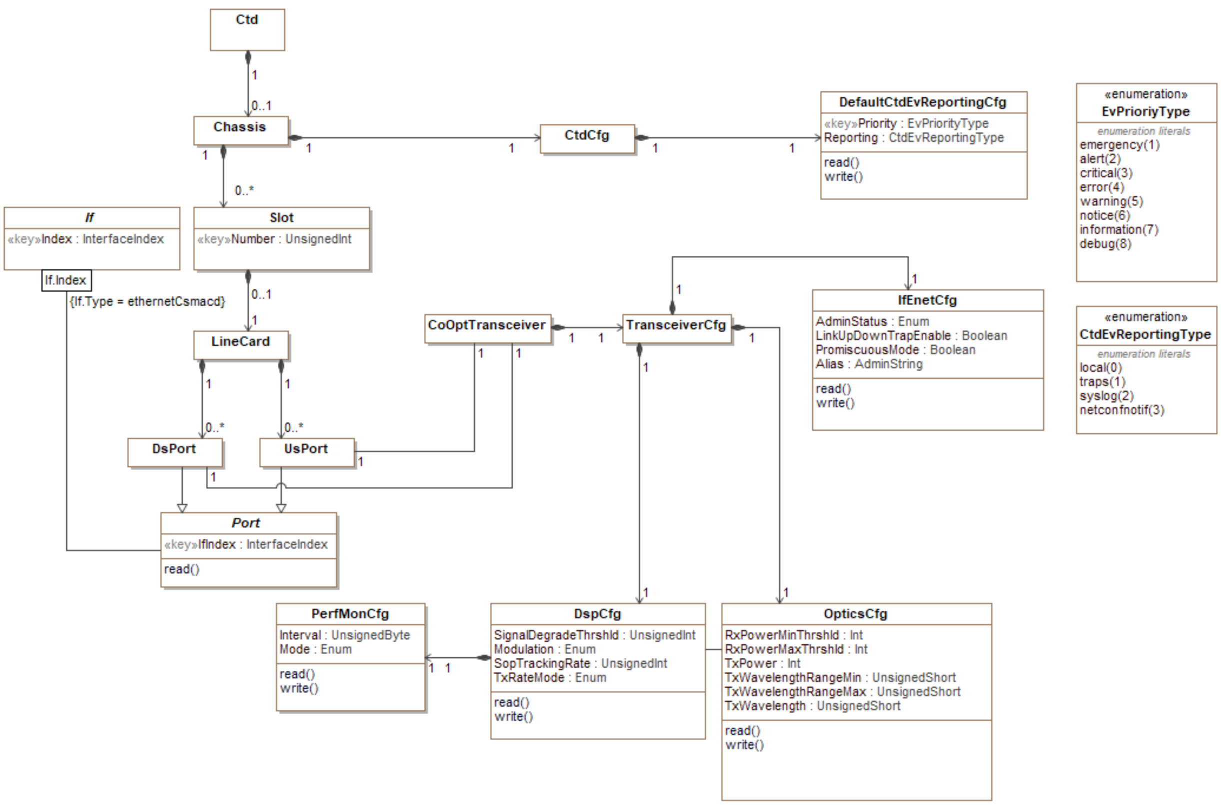

Figure 5 - CTD Configuration Management Information Model

6.1.1 Ctd

The Ctd object provides the context of the transceiver configuration and is the root of the configuration data. The device represented by this object is configured by the MSO utilizing the CTD vendor-specific methods outside the scope of this specification. It's assumed each transceiver upstream interface is associated with a CTD interface index. The Ctd object has no attributes.

Table 2 - Ctd Object Associations

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

6.1.2 Chassis

The Chassis object is a container which allows the user to configure the CTD device-specific elements. The Chassis object has no attributes. The Chassis object has the following associations:

Table 3 - Chassis Object Associations

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

6.1.3 Slot

The Slot object configures a slot within the CTD chassis. Line cards reside in slots. Slots are optional.

Table 4 - Slot Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Number	UnsignedInt	Yes (Key)	0..*		

Table 5 - Slot Object Associations

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

6.1.3.1 Number

This attribute configures the slot number for which a LineCard object will be configured. The Number attribute is a zero- or one-based index that sequentially numbers the physical slots in the chassis. For example, the Slot numbers start at zero and increase to n-1, where n is the number of slots the chassis supports.

6.1.4 CtdCfg

The CtdCfg object is a container that allows the user to configure the CTD device-specific elements. The CtdCfg object has no attributes.

Table 6 - CtdCfg Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
DefaultCtdReportingCfg	Directed composition to DefaultCtdReportingCfg	1	1	

6.1.5 LineCard

The LineCard object is a container which represents cards (with upstream and downstream ports) inserted into Chassis Slots. The LineCard object has no attributes.

Table 7 - LineCard Object Associations

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

6.1.6 If

The If abstract object represents the ifTable and ifXTable defined in [RFC 2863]. Only the index key is listed, due to its association with the Port object.

Table 8 - If Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Index	InterfaceIndex	Yes (Key)			

Table 9 - Slot Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
Port	Association to Port	1	1	

6.1.6.1 Index

This attribute corresponds to the ifIndex of the interface.

6.1.7 Port

The Port object is an abstract class from which all physical port objects on CTD line cards are derived. All physical port objects that derive from Port contain the attributes of a Port. The Port object is a generalization of all physical ports represented as DsPort and UsPort.

Table 10 - Port Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
IfIndex	InterfaceIndex	Yes (Key)			

6.1.7.1 IfIndex

This attribute corresponds to the ifIndex of the port. Port interface types are restricted to Ethernet.

6.1.8 DsPort

The DsPort object is a container that allows the user to configure the downstream port-based objects. There is a one-to-one mapping of DsPort to the Coherent Optics Transceiver object. The DsPort object has no attributes.

Table 11 - DsPort Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
CoOptTransceiver	Association to CoOptTransceiver	1	1	

6.1.9 UsPort

The UsPort object is a container that allows the user to configure the upstream port-based objects. There is a one-to-one mapping of UsPort to the CoOptTransceiver object. The UsPort object has no attributes.

Table 12 - UsPort Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
CoOptTransceiver	Association to CoOptTransceiver	1	1	

6.1.10 CoOptTransceiver

The CoOptTransceiver object is a container that allows the user to configure the Coherent Optics Transceiver-specific elements. The CoOptTransceiver object has no attributes.

Table 13 - CoOptTransceiver Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
TransceiverCfg	Directed composition to TransceiverCfg	1	1	

6.1.11 TransceiverCfg

The TransceiverCfg object serves as the root for the transceiver configuration. This object has no attributes and represents a container.

Table 14 - TransceiverCfg Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
DspCfg	Directed composition to DspCfg	1	1	
OpticsCfg	Directed composition to OpticsCfg	1	1	
IfEnetCfg	Directed composition to IfEnetCfg	1	1	

6.1.12 DspCfg

The DspCfg object provides configuration for DSP functional elements.

Table 15 - DspCfg Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
SignalDegradeThrshld	UnsignedInt	Yes		.01dbQ	.5
Modulation	Enum	Yes	other(1), qam(2), qpsk(3)		
SopTrackingRate	UnsignedInt	Yes		krad/sec	
TxRateMode	Enum	No	other(1), 100Gbps(2), 200Gbps(3)		

Table 16 - DspCfg Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
PerfMonCfg	Directed composition to PerfMonCfg	1	1	
OpticsCfg	Association to OpticsCfg	1	1	

6.1.12.1 SignalDegradeThrshld

This attribute configures the pre-FEC BER criteria and duration over which the BER exceeds the SD threshold before SignalDegrade is raised and an alarm is generated. This threshold is not applicable when operating above the FEC limit.

6.1.12.2 Modulation

This attribute configures the modulation method. The Enum values reflect the supported modulation methods.

6.1.12.3 SopTrackingRate

This attribute configures the State of Polarization Tracking Rate if multiple rates are supported. This attribute reports the current SopTrackingRate.

6.1.12.4 TxRateMode

This attribute configures the transmission rate if transceiver supports both 100 Gbps and 200 Gbps. The attribute reports the current transmission rate.

6.1.13 PerfMonCfg

The PerfMonCfg object configures the performance monitor attributes.

Table 17 - PerfMonCfg Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default
Interval	UnsignedByte	Yes	1..64	Seconds	
Mode	Enum	Yes	internal(1), external(2)		

6.1.13.1 Interval

This attribute defines the performance monitor interval duration. A value of zero results in performance monitor rate reported every 1 second. A value of 30 results in performance monitor date reported every 30 seconds.

6.1.13.2 Mode

This attribute configures the timing source for the performance monitor.

6.1.14 OpticsCfg

The OpticsCfg object enables the configuration of the transceiver optics component. The power thresholds are configured such that, when exceeded, will trigger an alarm to be raised and notification generated. The remaining configuration objects enable configuration of the current power and wavelength.

Table 18 - OpticsCfg Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default
RxPowerMinThrshld	Int	Yes		0.01 dBm	
RxPowerMaxThrshld	Int	Yes		0.01 dBm	
TxPower	Int	Yes		0.01 dBm	
TxWavelengthRangeMin	UnsignedShort	No		nm	
TxWavelengthRangeMax	UnsignedShort	No		nm	
TxWaveLength	UnsignedShort	Yes		nm	

6.1.14.1 RxPowerMinThrshld

This attribute defines the lowest optical power at which the transceiver is guaranteed to meet a post FEC BER < 1E-15. The CTD MAY log Event Id 67090002 if the receive level falls below this threshold.

6.1.14.2 RxPowerMaxThrshld

This attribute defines the highest optical power at which the transceiver is guaranteed to meet a post FEC BER < 1E-15. The CTD MAY log Event Id 67090003 if the transmit level exceeds this threshold.

6.1.14.3 TxPower

This attribute configures the optical power level at which the transceiver will transmit.

6.1.14.4 TxWavelengthRangeMin

This attribute defines the minimum transmit wavelength that the transceiver may utilize. If this attribute is not defined via the management system, it reports the current transmission wavelength.

6.1.14.5 TxWavelengthRangeMax

This attribute defines the maximum transmit wavelength that the transceiver may utilize. If this attribute is not defined via the management system, it reports the current transmission wavelength.

6.1.14.6 TxWavelength

This attribute configures the wavelength used on this link.

6.1.15 IfEnetCfg

This object configures the Ethernet interface attributes specified in the ifTable and ifXTable of [RFC 2863].

Table 19 - IfEnetCfg Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
AdminStatus	Enum	Yes	up(1), down(2), testing(3)		
LinkUpDownTrapEnable	Boolean	Yes			
PromiscuousMode	Boolean	No			
Alias	AdminString	No			

6.1.15.1 AdminStatus

This attribute allows configuration of the state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with AdminStatus in the down(2) state. As a result of either explicit management action or per-configuration information retained by the managed system, AdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state).

6.1.15.2 LinkUpDownTrapEnable

This attribute allows configuration of whether linkup/linkdown traps are generated for this interface.

A value of true indicates that traps are enabled.

A value of false indicates that traps are disabled.

6.1.15.3 PromiscuousMode

This attribute reports a value of false if this interface only accepts packets/frames that are addressed to this interface.

This attribute reports a value of true when the station accepts all packets/frames transmitted on the media.

The value of PromiscuousMode does not affect the reception of broadcast and multicast packets/frames by the interface.

6.1.15.4 Alias

This attribute allows configuration of an Alias for the interface. On the first instantiation of an interface, the value of Alias associated with that interface is the zero-length string. As and when a value is written into an instance of Alias through a network management operation, then the CTD retains the supplied value in the Alias instance associated with the same interface for as long as that interface remains instantiated, including across all re-initializations/reboots of the network management system, including those which result in a change of the interface's Index value.

6.1.16 DefaultCtdEvReportingCfg

This object configures the default event reporting parameters for CTDs to use.

Table 20 - DefaultCtdEvReportingCfg Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default Value
Priority	EvPriorityType	Yes (Key)			
Reporting	CtdEvReportingType	Yes			

6.1.16.1 Priority

This attribute defines the priority level of an event.

6.1.16.2 Reporting

This attribute defines the reporting options for an event.

6.2 Configuration Information Model Data Type Definitions

The following data types have been created to support the CTD Information Models.

Table 21 - Configuration Data Types

Data Type Name	Base Type	Type Constraints	Reference
EvPriorityType	Enum	emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), information(7), debug(8)	[RFC 4639]
CtdEvReportingType	EnumBits	local(0), traps(1), syslog(2), netconfNotif(3)	

6.2.1 EvPriorityType

This data type defines an event priority level. These are ordered from most (emergency) to least (debug) critical. Each event has a particular priority level associated with it (as defined by the vendor).

Reference: [RFC 4639], docsDevEvControlTable, docsDevEvPriority

6.2.2 CtdEvReportingType

This data type defines the action to be taken on occurrence of this event class. Implementations may not necessarily support all options for all event classes but at a minimum allows traps and netconfNotif to be disabled. The enum values are defined as follows:

local – Events will be logged into the CTD local log.

traps – Events will be sent as SNMP notifications.

syslog – Events will be sent to a syslog server.

netconfNotif – Events will be sent as NETCONF notifications.

7 PERFORMANCE MANAGEMENT

This section describes the transceiver and CTD requirements for performance management functions.

This section defines the minimum set of managed objects required to monitor a CTD hosted transceiver. It includes only requirements directly associated with transceiver performance management at the physical layer. For example, though the CTD most likely supports IPv4 andIPv6, there are no performance management requirements for such support in this specification.

7.1 Performance Management Information Model

This section defines the CTD requirements for performance management functions. The Information Model is divided into the following groupings.

- TransceiverStats: Defines the DSP, Optics and Ethernet statistics objects.
- TransceiverStatus: Defines the DSP, Optics and Ethernet status objects.

The objects for performance monitoring of a Coherent Optics Transceiver port, as managed by the CTD, are shown in Figure 6 below. This information is typically contained in the transceiver implementation documentation.

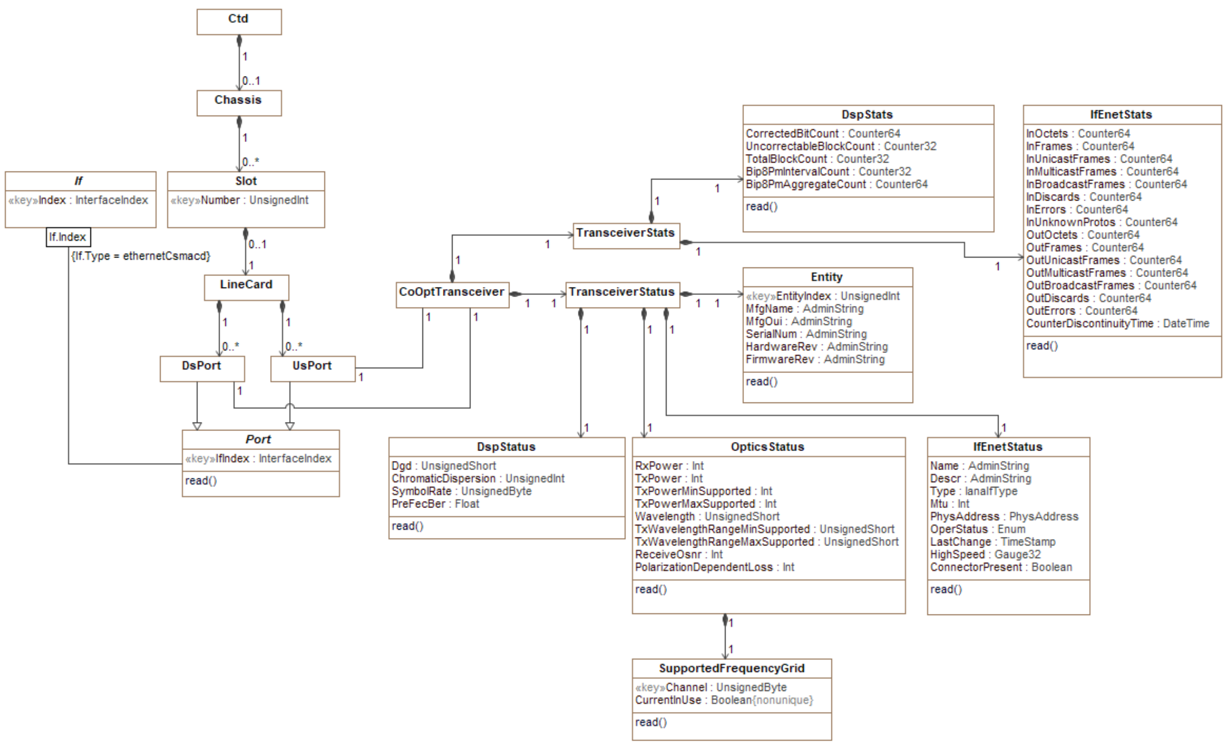

Figure 6 - CTD Performance Management Information Model

7.1.1 Ctd

This object is included in Figure 6 for reference. It is defined in Section 6.1.

7.1.2 Chassis

This object is included in Figure 6 for reference. It is defined in Section 6.1.

7.1.3 Slot

This object is included in Figure 6 for reference. It is defined in Section 6.1.

7.1.4 LineCard

This object is included in Figure 6 for reference. It is defined in Section 6.1.

7.1.5 If

This object is included in Figure 6 for reference. It is defined in Section 6.1.

7.1.6 DsPort

This object is included in Figure 6 for reference. It is defined in Section 6.1.

7.1.7 UsPort

This object is included in Figure 6 for reference. It is defined in Section 6.1.

7.1.8 CoOptTransceiver

This object is included in Figure 6 for reference. It is defined in Section 6.1. Additional object associations are defined below.

Table 22 - CoOptTransceiver Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
TransceiverStats	Directed composition to TransceiverStats	1	1	
TransceiverStatus	Directed composition to TransceiverStatus	1	1	

7.1.9 TransceiverStats

The TransceiverStats object serves as the root for the transceiver statistics model. This object has no attributes and represents a container.

Table 23 - TransceiverStats Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
DspStats	Directed composition to DspStats	1	1	
IfEnetStats	Directed composition to IfEnetStats	1	1	

7.1.10 TransceiverStatus

The TransceiverStatus object serves as the root for the transceiver status model. This object has no attributes and represents a container.

Table 24 - TransceiverStatus Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
DspStatus	Directed composition to DspStatus	1	1	
OpticsStatus	Directed composition to OpticsStatus	1	1	
Entity	Directed composition to Entity	1	1	
IfEnetStatus	Directed composition to IfEnetStatus	1	1	

7.1.11 Entity

The Entity object provides the transceiver manufacturer and related information.

Table 25 - Entity Object Attributes

Attribute Name	Type	Access	Type Constraints	Units	Default
EntityIndex	UnsignedInt	Key	1..2147483647		
MfgName	AdminString	Read-only			
MfgOui	AdminString	Read-only	SIZE(3)		
SerialNum	AdminString	Read-only			
HardwareRev	AdminString	Read-only			
FirmwareRev	AdminString	Read-only			

7.1.11.1 EntityIndex

This key attribute reports an arbitrary value that uniquely identifies the physical entity. Index values for different physical entities are not necessarily contiguous.

7.1.11.2 MfgName

This attribute reports the name of the manufacturer of the transceiver.

7.1.11.3 MfgOui

This attribute reports the IEEE-assigned unique manufacturer identifier for the transceiver.

7.1.11.4 SerialNum

This attribute reports the vendor-specific serial number string for the transceiver.

7.1.11.5 HardwareRev

This attribute reports the vendor-specific hardware revision string for the transceiver.

7.1.11.6 FirmwareRev

This attribute provides the vendor-supplied transceiver firmware version.

7.1.12 DspStatus

The DspStatus object provides key status information for monitoring the coherent optical link health.

Table 26 - DspStatus Object Attributes

Attribute Name	Type	Access	Type Constraints	Units	Default
Dgd	UnsignedShort	Read-only		Picoseconds	
ChromaticDispersion	UnsignedInt	Read-only		Picoseconds/nanometer	
SymbolRate	UnsignedByte	Read-only		Symbols/gBaud	

Attribute Name	Type	Access	Type Constraints	Units	Default
PreFecBer	Float	Read-only		BitErrors/BitsTransmitted	

7.1.12.1 Dgd

This attribute defines the DSP estimated the differential group delay value in ps of the received optical signal between X and Y polarization.

7.1.12.2 ChromaticDispersion

This attribute defines the DSP estimated the chromatic dispersion value in ps/nm of the received optical signal accumulated from propagation.

7.1.12.3 SymbolRate

This attribute defines the number of symbols transmitted per second in units of gBaud.

7.1.12.4 PreFecBer

This attribute reports the current Pre-FEC BER. This is the ratio of receiver detected bit errors over the number of bits transmitted before FEC attempts to correct errors.

7.1.13 DspStats

The DspStats object provides key statistics for performance monitoring of the coherent optical link health.

Table 27 - DspStats Object Attributes

Attribute Name	Type	Access	Type Constraints	Units	Default
CorrectedBitCount	Counter64	Read-only			
UncorrectableBlockCount	Counter32	Read-only			
TotalBlockCount	Counter32	Read-only			
Bip8PmIntervalCount	Counter32	Read-only			
Bip8PmAggregateCount	Counter64	Read-only			

7.1.13.1 CorrectedBitCount

This attribute reports the number of corrected bits by the FEC.

7.1.13.2 UncorrectableBlockCount

This attribute reports the number of FEC blocks that are uncorrectable and flagged as erroneous.

7.1.13.3 TotalBlockCount

This attribute reports the total number of FEC blocks decoded.

7.1.13.4 Bip8PmIntervalCount

This attribute reports the computed bit interleaved parity-8 blocks that have been detected as being in error in the most recent interval.

7.1.13.5 Bip8PmAggregateCount

This attribute reports the sum of all the computed bit interleaved parity-8 blocks that have been detected since the transceiver initialized.

7.1.14 OpticsStatus

The OpticsStatus object provides status information of the transceiver optical component.

Table 28 - OpticsStatus Object Attributes

Attribute Name	Type	Access	Type Constraints	Units	Default
RxPower	Int	Read-only		0.01 dBm	
TxPower	Int	Read-only		0.01 dBm	
TxPowerMinSupported	Int	Read-only		0.01 dBm	
TxPowerMaxSupported	Int	Read-only		0.01 dBm	
Wavelength	UnsignedShort	Read-only		nm	
TxWavelengthRangeMinSupported	UnsignedShort	Read-only		nm	
TxWavelengthRangeMaxSupported	UnsignedShort	Read-only		nm	
ReceiveOsnr	Int	Read-only		dB	
PolarizationDependentLoss	Int	Read-only		dB	

Table 29 - OpticsStatus Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
SupportedFrequencyGrid	Directed composition to OpticsStatus	1	1	

7.1.14.1 RxPower

This attribute reports the measured receive power.

7.1.14.2 TxPower

This attribute reports the measured output power.

7.1.14.3 TxPowerMinSupported

This attribute reports the minimum supported transmit power.

7.1.14.4 TxPowerMaxSupported

This attribute reports the maximum supported transmit power.

7.1.14.5 Wavelength

This attribute reports the current wavelength in use.

7.1.14.6 TxWavelengthRangeMinSupported

This attribute reports the minimum supported transmit wavelength.

7.1.14.7 TxWavelengthRangeMaxSupported

This attribute reports the maximum supported transmit wavelength.

7.1.14.8 ReceiveOsnr

This attribute reports the Optical Signal to Noise Ratio measured at the receiver input.

7.1.14.9 PolarizationDependentLoss

This attribute reports the polarization-dependent loss (PDL), defined as the absolute difference in optical power between the X polarization and the Y polarization seen at the input of a coherent receiver.

7.1.15 SupportedFrequencyGrid

The SupportedFrequencyGrid object reports the supported frequencies by channel number. The frequency in use is noted in the report.

Table 30 - SupportedFrequencyGrid Object Attributes

Attribute Name	Type	Required Attribute	Type Constraints	Units	Default
Channel	Unsignedshort	Key	1..65535		
CurrentInUse	Boolean	Yes			

7.1.15.1 Channel

This attribute reports a supported channel number.

7.1.15.2 CurrentInUse

This attribute reports the channel in use indicated with ‘true’. All other supported channels should report ‘false’.

7.1.16 IfEnetStatus

This object provides details about the Ethernet interfaces on the CTD. The attributes of this object are based on the ifTable/ifXTable specified in [RFC 2863].

Table 31 - IfEnetStatus Object Attributes

Attribute Name	Type	Access	Type Constraints	Units	Default
Name	AdminString	Read-only			
Descr	AdminString	Read-only			
Type	IANAIfType	Read-only			
Mtu	Int	Read-only			
PhysAddress	PhysAddress	Read-only			
OperStatus	Enum	Read-only	up(1), down(2), testing(3), unknown(4), dormant(5), notPresent(6), lowerLayerDown(7)		
LastChange	TimeStamp	Read-only			
HighSpeed	Gauge32	Read-only		Mpbs	
ConnectorPresent	Boolean	Read-only			

7.1.16.1 Name

This attribute reports a textual string representing a name that describes the interface.

7.1.16.2 Descr

This attribute reports a textual string containing information about the Ethernet interface. This string includes the name of the manufacturer, the product name, and the version of the interface hardware/software.

7.1.16.3 Type

This attribute reports the type of interface. Additional values for Type are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention. The types are defined in the IANAifType-MIB. The value reported by this attribute is ethernetCsmacd.

7.1.16.4 Mtu

This attribute reports the size of the largest packet that can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.

7.1.16.5 PhysAddress

This attribute reports the interface's address at its protocol sub-layer. For example, for an 802.x interface, this attribute normally contains a MAC address. The interface's media-specific MIB defines the bit and byte ordering and the format of the value of this attribute. For interfaces that do not have such an address (e.g., a serial line), this attribute reports an octet string of zero length.

7.1.16.6 OperStatus

This attribute reports the current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If AdminStatus is down(2), then OperStatus should be down(2). If AdminStatus is changed to up(1), then OperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components.

7.1.16.7 LastChange

This attribute reports the value of RpdSysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this attribute reports a zero value.

7.1.16.8 HighSpeed

This attribute reports an estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this attribute reports a value of 'n', then the speed of the interface is somewhere in the range of 'n-500,000' to 'n+499,999'. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this attribute reports the nominal bandwidth.

7.1.16.9 ConnectorPresent

This attribute reports the value 'true' if the interface sublayer has a physical connector and the value 'false' otherwise.

7.1.17 IfEnetStats

This object reports statistics for the Ethernet interfaces on the CTD. The attributes of this object are based on the ifTable/ifXTable specified in [RFC 2863].

Discontinuities in the value of these counters can occur at reinitialization of the managed system, and at other times as indicated by the value of CounterDiscontinuityTime.

Table 32 - IfEnetStats Object

Attribute Name	Type	Access	Type Constraints	Units
InOctets	Counter64	Read-Only		octets
InFrames	Counter64	Read-Only		frames

Attribute Name	Type	Access	Type Constraints	Units
InUnicastFrames	Counter64	Read-Only		frames
InMulticastFrames	Counter64	Read-Only		frames
InBroadcastFrames	Counter64	Read-Only		frames
InDiscards	Counter64	Read-Only		frames
InErrors	Counter64	Read-Only		frames
InUnknownProtos	Counter64	Read-Only		frames
OutOctets	Counter64	Read-Only		octets
OutFrames	Counter64	Read-Only		frames
OutUnicastFrames	Counter64	Read-Only		frames
OutMulticastFrames	Counter64	Read-Only		frames
OutBroadcastFrames	Counter64	Read-Only		frames
OutDiscards	Counter64	Read-Only		frames
OutErrors	Counter64	Read-Only		frames
CounterDiscontinuityTime	DateTime	Read-Only		N/A

7.1.17.1 InOctets

This attribute is the count of all octets received by the RPD on this Ethernet interface.

7.1.17.2 InFrames

This attribute is the count of all frames received by the RPD on this Ethernet interface.

7.1.17.3 InUnicastFrames

This attribute is the count of all unicast frames received by the RPD on this Ethernet interface.

7.1.17.4 InMulticastFrames

This attribute is the count of all multicast frames received by the RPD on this Ethernet interface.

7.1.17.5 InBroadcastFrames

This attribute is the count of all broadcast frames received by the RPD on this Ethernet interface.

7.1.17.6 InDiscards

This attribute is the number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

7.1.17.7 InErrors

For packet-oriented interfaces, this attribute reports the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, this attribute reports the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.

7.1.17.8 InUnknownProtos

For packet-oriented interfaces, this attribute reports the number of packets received via the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this attribute will always report 0.

7.1.17.9 OutOctets

This attribute is the count of all octets transmitted by the RPD on this Ethernet interface.

7.1.17.10 OutFrames

This attribute is the count of all frames transmitted by the RPD on this Ethernet interface.

7.1.17.11 OutUnicastFrames

This attribute is the count of all unicast frames transmitted by the RPD on this Ethernet interface.

7.1.17.12 OutMulticastFrames

This attribute is the count of all multicast frames transmitted by the RPD on this Ethernet interface.

7.1.17.13 OutBroadcastFrames

This attribute is the count of all broadcast frames transmitted by the RPD on this Ethernet interface.

7.1.17.14 OutDiscards

This attribute is the number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

7.1.17.15 OutErrors

For packet-oriented interfaces, this attribute reports the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, this attribute reports the number of outbound transmission units that could not be transmitted because of errors.

7.1.17.16 CounterDiscontinuityTime

This attribute reports the date and time at which any one or more of the counters in this group were created or last reset to zero. If the CTD does not acquire time of day, it can report an initial CounterDiscontinuityTime of Jan 1 1970.

7.2 Fault Management

This section defines requirements for remote monitoring/detection, diagnosis, reporting, and correction of problems. The subset of the DOCSIS fault management mechanisms defined in [RFC 4639] are utilized. To maintain consistency in the MSO managed networks, the following recommendations parallel the DOCSIS notification requirements.

7.2.1 Fault Notifications

The CTD MUST generate event notifications to one or more NMSs when the Coherent Optics Transceiver asserts the alarms defined in this specification.

7.2.2 Event Reporting

A Coherent Optics Transceiver raises alarms via the CTD/Transceiver interface to indicate potentially disruptive events (e.g., Loss of Signal) have occurred. Alarms may also be generated to provide warnings that a component's performance is degrading, and service may be impacted. The method the transceiver utilizes to report link or transceiver events to the CTD is transceiver implementation-specific.

When a Coherent Optics Transceiver generates an alarm defined in this specification, the CTD MUST send a notification to the configured notification receiver unless forwarding has been disabled for this notification. The CTD MUST log events to the local log if the notification cannot be generated or sent to the NMS.

A CTD operating in SNMP Coexistence mode MUST support SNMP notification type 'trap' and 'inform' as defined in [RFC 3416] and [RFC 3413].

When the CTD receives an alarm from the Coherent Optics transceiver, the CTD MUST process the alarm utilizing one or more of the following methods.

- Store in the CTD Local Log defined in [RFC 4639] with modifications defined in this specification.
- Send as a message to a Syslog server.
- Report to a Notification Receiver via an SNMP notification.
- Report to a NETCONF client as a NETCONF notification.

Event Notifications are enabled and disabled via configuration settings as defined in Section 6.

The transceiver events are defined in Annex B.

7.2.2.1 Format of Events

The following sections explain in detail how to report these events via the local event logging mechanism.

7.2.2.2 Local Event Logging

A CTD MUST support storing events in a local log in local-volatile storage and local non-volatile storage.

A CTD MUST implement its Local Log as a cyclic buffer with a minimum of ten entries. A CTD MUST persist non-volatile storage events across reboots.

Aside from the procedures defined in this specification, event recording conforms to the requirements defined in [RFC 4639]. Event descriptions are defined in English. A CTD MUST limit Event Message fields to no longer than 255 characters. This is the maximum event descriptor length defined for SnmpAdminString [RFC 3411].

Events are considered identical if the EventId is the same AND the event arguments are the same. For identical events occurring consecutively, the CTD MAY store only a single event. If a CTD stores as a single event when multiple identical events that occur consecutively, the CTD MUST reflect in the event description the most recent event.

The CTD MUST adhere to the rules listed below for creating local volatile and local non-volatile logs following a re-boot.

CTD MUST clear both the local volatile and local non-volatile event logs when an event log is reset via SNMP or NETCONF.

7.2.2.3 Events for CTD

The EventId digit is a 32-bit unsigned integer. EventIds ranging from 0 to (2^{31} - 1) are reserved by P2P Coherent Optics. The CTD MUST report an EventId as a 32-bit unsigned integer and convert the EventId from the error codes defined in Annex B to be consistent with this number format.

The DOCS-CABLE-DEVICE-MIB [RFC 4639] defines 8 priority levels and a corresponding reporting mechanism for each level. The CTD MUST support only the events that are applicable to a Coherent Optics Transceiver.

Emergency event (priority 1)

Reserved for vendor-specific 'fatal' hardware or software errors that prevent normal system operation and cause the reporting system to reboot.

Every vendor may define their own set of emergency events. Examples of such events might be 'no memory buffers available', 'memory test failure', etc.

Alert event (priority 2)

A serious failure, which causes the reporting system to reboot, but it is not caused by hardware or software malfunctioning.

Critical event (priority 3)

A serious failure that requires attention and prevents the Coherent Optics Transceiver from transmitting data but could be recovered without rebooting the system. Examples of such events might be a receive Loss of Signal (LOS).

Error event (priority 4)

A failure occurred that could interrupt the normal data flow but will not cause the Coherent Optics Transceiver to re-initialize. Error events may be reported in real time.

Warning event (priority 5)

A failure occurred that could interrupt the normal data flow. but will not cause the Coherent Optics Transceiver to re-initialize. Examples of such events might be TxPowerLow or TxPowerHigh thresholds exceeded.

Notice event (priority 6)

The event is important but is not a failure and is reported in real time by the CTD.

Informational event (priority 7)

The event is of marginal importance, and is not failure, but could be helpful for tracing the normal operation.

Debug event (priority 8)

Reserved for vendor-specific non-critical events.

During CTD initialization or reinitialization, the CTD MUST persist event reporting configuration in its non-volatile memory. After a CTD factory reset, the CTD MUST support the default event reporting mechanism shown in Table 33.

The reporting mechanism for each priority may be changed using one of the supported management protocols.

Table 33 - CTD Default Event Reporting Mechanism Versus Priority

Event Priority	Local Event Log	Notify
Emergency	Yes	No
Alert	Yes	No
Critical	Yes	No
Error	Yes	No
Warning	No	No
Notice	No	No
Informational	No	No
Debug	No	No

The CTD MUST format notifications that it generates for standard P2P Coherent Optics events as specified in Annex B.

7.2.2.4 Vendor Specific Events

A CTD MUST implement EventIds ranging from 2^{30} to (2^{31} -1) as vendor-specific EventIds using the following format:

- Bit 31 is set to indicate vendor-specific event
- Bits 30-16 contain the lower 15 bits of the vendor's SNMP enterprise number

- Bits 15-0 are used by the vendor to number events

7.2.2.5 Event Priorities and Vendor-Specific Events

This specification defines events that make use of a sub-set of the Event Priority Levels. Vendor-specific events can be defined for any Event Priority Level. Table 34 summarizes those considerations.

A CTD MUST assign P2P Coherent Optics events and vendor-specific events as indicated in Table 34.

Table 34 - Event Priorities Assignment

Event Priority	CTD Event Assignment
Emergency	Vendor-specific
Alert	CTD and Vendor-specific (optional*)
Critical	CTD and Vendor-specific (optional*)
Error	CTD and Vendor-specific (optional*)
Warning	CTD and Vendor-specific (optional*)
Notice	CTD and Vendor-specific (optional*)
Information	CTD and Vendor-specific (optional*)
Debug	Vendor-specific

7.2.3 NETCONF Notifications

NETCONF Notifications [RFC 5277] is a mechanism that provides an asynchronous notification message service built on top of the base NETCONF protocol. The mechanism is based on the concept of clients subscribing to events belonging to named event streams. Clients can associate filter parameters with the subscriptions to receive a defined subset of all events belonging to a stream.

Notification replay is an integral part of the NETCONF Notifications framework. It provides the ability for clients to request sending (or resending) recently generated notifications based on a specific start and an optional stop time. If no stop time is provided, the notification stream will continue until the subscription is terminated.

The CTD MUST implement NETCONF Notifications towards OSS, as specified in [RFC 5277].

The CTD MUST use the YANG module specified in [COOPT-CTD-EVENTS-YANG] for reporting P2P Coherent Optics NETCONF Notifications.

7.3 Fault Management Information Model

This section defines the Information Model for CTD fault management reporting functions. The objects for CTD reporting of Coherent Optics Transceiver events are shown in Figure 7. Note that the Information Model presented in Figure 7 omits the Ctd, Chassis, Slot, LineCard, DsPort, UsPort, Port classes. However, the rooting for class CoOptTransceiver in Figure 7 is identical to the Configuration Management Information Model and Performance Management Model.

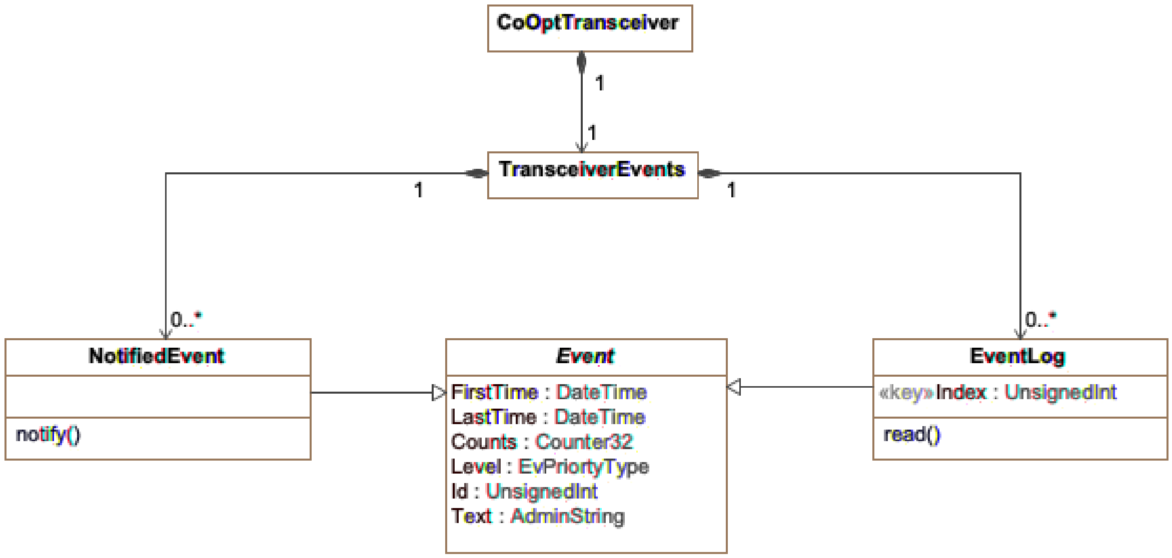

Figure 7 - CTD Fault Management Information Model

7.3.1 CoOptTransceiver

This object is included in Figure 7 for reference. It is defined in Section 6.1. Additional object associations are defined below.

Table 35 - CoOptTransceiver Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
TransceiverEvents	Directed composition to TransceiverEvents	1	1	

7.3.2 TransceiverEvents

The TransceiverEvents object serves as the root for the transceiver event model. This object has no attributes and represents a container.

Table 36 - TransceiverEvents Object Associations

Associated Object Name	Type	Near-end Multiplicity	Far-end Multiplicity	Label
NotifiedEvent	Specialization of Event	1	1	
LocalEvent	Specialization of Event	1	1	

7.3.2.1 Event

The Event object is an abstract class which defines attributes for Coherent Optics Transceiver events and alarms. Events may be of interest in fault isolation and troubleshooting. Events are reported by the CTD.

Table 37 - Event Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
FirstTime	DateTime	Read-only		N/A

Attribute Name	Type	Access	Type Constraints	Units
LastTime	DateTime	Read-only		N/A
Counts	Counter32	Read-only		events
Level	EvPriorityType	Read-only		N/A
Id	UnsignedInt	Read-only	Refer to Annex B Event ID definitions	N/A
Text	AdminString	Read-only	Refer to Annex B Event Message definitions	N/A

7.3.2.1.1 FirstTime

This attribute provides the local CTD time when this event was created.

7.3.2.1.2 LastTime

When an event reports only one event occurrence, this attribute will have the same value as the corresponding instance of FirstTime. When an event reports multiple event occurrence, this attribute will record the local CTD time when the most recent occurrence for this event occurred.

7.3.2.1.3 Counts

This attribute provides the number of consecutive event occurrences reported by this event. This starts at 1 with the creation of this event occurrence and increments by 1 for each subsequent duplicate event occurrence.

7.3.2.1.4 Level

This attribute provides the priority level of this event, as defined by Annex B. These are ordered from most serious (emergency) to least serious (debug).

7.3.2.1.5 Id

This attribute provides the identifier of this event, as defined by Annex B.

7.3.2.1.6 Text

This attribute provides the message text of this event, as defined by Annex B.

7.3.2.2 NotifiedEvent Object

The NotifiedEvent object is a realization of the Event abstract class and contains Coherent Optics Transceiver events logged as configured for notification to the NMS via the CTD (including SNMP and NETCONF Notifications).

NotifiedEvent defines its own number space for the Index key.

7.3.2.3 EventLog Object

The EventLog object is a realization of the Event abstract class and contains events triggered by the Coherent Optics Transceiver and logged in the CTD Local Log.

LocalEvent defines its own number space for the Index key.

Table 38 - EventLog Object Attributes

Attribute Name	Type	Access	Type Constraints	Units
Index	UnsignedInt	Key		N/A

7.3.2.3.1 Index

This key attribute provides relative ordering of the events in the event log. This attribute will always increase except when:

- the log is reset
- the device reboots and does not implement non-volatile storage for this log, or
- it reaches the value 2^31. The next entry for all the above cases is 1.

8 MANAGEMENT PROTOCOL REQUIREMENTS

This specification defines the minimum functionality that a CTD is required to implement to enable remote management of the Coherent Optics Transceiver.

This section defines the minimum set of network management managed objects required to support the management of the transceiver within a CTD.

8.1 Management Protocols

The CDT supports SNMP and, optionally, NETCONF. This specification defines the requirements applicable to both management protocols.

The CTD MUST support the SNMP requirements in this specification.

If the CTD supports NETCONF, the CTD MUST support the NETCONF requirements in this specification.

8.2 Data Type Mapping

The Unified Modeling Language (UML) is used for modeling the Coherent Optics management requirements. The data types defined in Annex C are mapped for use with SNMP MIBs and NETCONF YANG Modules.

This specification defines requirements for the SNMP and NETCONF protocols for network management functions. Basic UML notation is used in this specification and is independent of the data model realization.

8.3 SNMP and MIB Requirements

The CTD MAY augment the required MIBs with objects from other standard or vendor-specific MIBs where appropriate.

The CTD MUST implement the MIB requirements in accordance with this specification regardless of the value of an IETF MIB object's status (e.g., deprecated or optional).

If not required by this specification, deprecated objects are optional. If a CTD implements a deprecated MIB object, the CTD MUST implement the MIB object correctly according to the MIB definition.

If a CTD does not implement a deprecated MIB object, the CTD MUST NOT instantiate the deprecated MIB object. If a CTD does not implement a deprecated MIB object, the CTD MUST respond with the appropriate error/exception condition, such as noSuchObject for SNMPv2c, when an attempt to access the deprecated MIB object is made.

If not required by this specification, additional objects are optional. If a CTD implements any additional MIB objects, the CTD MUST implement the MIB object correctly according to the MIB definition.

If a CTD does not implement one or more additional objects, the CTD MUST NOT instantiate the additional MIB object or objects.

If a CTD does not implement one or more additional objects, the CTD MUST respond with the appropriate error/exception condition, such as noSuchObject for SNMPv2c, when an attempt to access the non-existent additional MIB object is made.

If not required by this specification, obsolete objects are optional. If a CTD implements an obsolete MIB object, the CTD MUST implement the MIB object correctly according to the MIB definition.

If a CTD does not implement an obsolete MIB object, the CTD MUST NOT instantiate the obsolete MIB object.

If a CTD does not implement an obsolete MIB object, the CTD MUST respond with the appropriate error/exception condition, such as noSuchObject for SNMPv2c, when an attempt to access the obsolete MIB object is made.

Objects which are not supported by this specification are not implemented by an agent.

- The CTD MUST NOT instantiate not-supported MIB objects.

- The CTD MUST respond with the appropriate error/exception condition, such as noSuchObject for SNMPv2c, when an attempt to access a not-supported MIB object is made.

The CTD MUST implement the MIB access requirements defined in Annex A as follows:

- MIB objects with Not-Accessible (N-Acc) access type are implemented with not-accessible access and are typically indexes in MIB tables.
- MIB objects with Read-Create (RC) access type are implemented with read-create access.
- MIB objects with Read-Write (RW) access type are implemented with read-write access.
- MIB objects with Read-Only (RO) access type are implemented with read-only access.
- MIB objects with Read-Create (RC) or Read-Only (RO) access types are implemented with either read-create access or read-only access as described in the object.
- MIB objects with Read-Create (RC) or Read-Write (RW) access types are implemented with either read-create access or read-write access as described in the object.
- MIB objects with Read-Write (RW) or Read-Write (RO) access types are implemented with either read-write access or read-only access as described in the object.
- MIB objects with Accessible for SNMP Notification (Acc-FN) access type are implemented as SNMP Notifications or Traps.

If a Coherent Optics Transceiver does not implement an underlying function associated with a deprecated or obsolete data model object, the Coherent Optics Transceiver MUST respond with the form factor-dependent error/exception condition if an attempt to access the deprecated data model object is made.

If a Coherent Optics Transceiver does not implement an underlying function associated with a deprecated or obsolete data model object, the CTD management agent MUST translate the transceiver response into the management protocol-defined response. For example, the agent SNMP forwards the -defined, ‘noSuchObject’ message to the management station.

8.4 SNMP Protocol and Agent Requirements

A CTD MUST support the SNMPv1 and SNMPv2c protocol.

A CTD MUST support SNMPv1 and SNMPv2c Traps as defined in [RFC 3416].

The IETF SNMP-related RFCs listed in Table 39 are supported by the CTD.

Table 39 - IETF SNMP-related RFCs

[RFC 3410]]	Introduction and Applicability Statements for Internet Standard Management Framework
[RFC 3411]	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
[RFC 3412]	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
[RFC 3413]	Simple Network Management Protocol (SNMP) Applications
[RFC 3414]	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
[RFC 3415]	View-based Access Control Model (VACM) for the simple Network Management Protocol (SNMP)
[RFC 3416]	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
[RFC 3417]	Transport Mappings for the Simple Network Management Protocol (SNMP)
[RFC 3418]	Management Information Base for the Simple Network Management Protocol (SNMP)
[RFC 3419]	Textual Conventions for Transport Addresses
[RFC 3584]	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
[RFC 1901]	Introduction to Community-based SNMPv2 (Informational)
[RFC 1157]	A Simple Network Management Protocol

For support of SMIv2, Table 40 lists the IETF SNMP-related RFCs which are supported by the CTD.

Table 40 - SMIv2 IETF SNMP-related RFCs

[RFC 2578]	Structure of Management Information Version 2 (SMIv2)
[RFC 2579]	Textual Conventions for SMIv2
[RFC 2580]	Conformance Statements for SMIv2

8.4.1.1 Requirements for SNMPv3 MIB Modules

The CTD MUST implement the MIBs defined in [RFC 3411] through [RFC 3415] and [RFC 3584].

8.5 CableLabs MIBS

Table 41 - CableLabs P2P Coherent Optics MIBs

Reference	MIB Module	Applicable Device
[COOPT-CTD-MIB]	P2P Coherent Optics: PTPCO-CTD-MIB	CTD

8.6 Specific MIB Object Implementation Requirements

8.6.1 Requirements for SNMPv2 MIB (RFC 3418)

The CTD MUST implement the System Group of [RFC 3418].

8.6.2 Requirements for Interfaces Group MIB (RFC 2863)

The CTD MUST implement the IF-MIB [RFC 2863].

8.6.3 Requirements for P2P Coherent Optics Device MIB (PTPCO-CTD-MIB)

The P2P Coherent Optics CTD MIB provides details about each Coherent Optics Transceiver managed by the CTD.

8.7 NETCONF Protocol and Server Requirements

This specification defines the minimum functionality that the CTD is to implement to enable remote management of the Coherent Optics Transceiver via the NETCONF protocol.

The IETF NETCONF-related RFCs listed in Table 42 are supported by the CTD.

Table 42 - NETCONF RFCs

[RFC 5277]	IETF RFC 5277, NETCONF Event Notifications, July 2008
[RFC 6241]	IETF RFC 6241, Network Configuration Protocol (NETCONF), June 2011
[RFC 6242]	IETF RFC 6242, Using the NETCONF Protocol over Secure Shell (SSH), June 2011
[RFC 6243]	IETF RFC 6243, With-defaults Capability for NETCONF, June, 2011
[RFC 8341]	IETF RFC 8341, Network Configuration Access Control Model, March 2018

For support of YANG, Table 43 lists the IETF YANG-related RFCs which are supported by the CTD.

Table 43 - YANG-related RFCs

[RFC 6020]	IETF RFC 6020, YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF), October 2010
[RFC 6991]	IETF RFC 6991, Common YANG Data Types, July 2013
[RFC 7950]	The YANG 1.1 Data Modeling Language, August 2016

8.7.1 NETCONF Theory of Operation

The CTD supports configuration via the NETCONF protocol. In this case configuration instructions are sent using XML-encoded remote procedure calls (RPCs) in NETCONF protocol messages from a configuration management tool to the CTD. The XML configuration data, representing the CTD configuration, is conformant to the YANG modules specified in this document.

A use case for configuring a CTD via NETCONF is depicted in Figure 8.

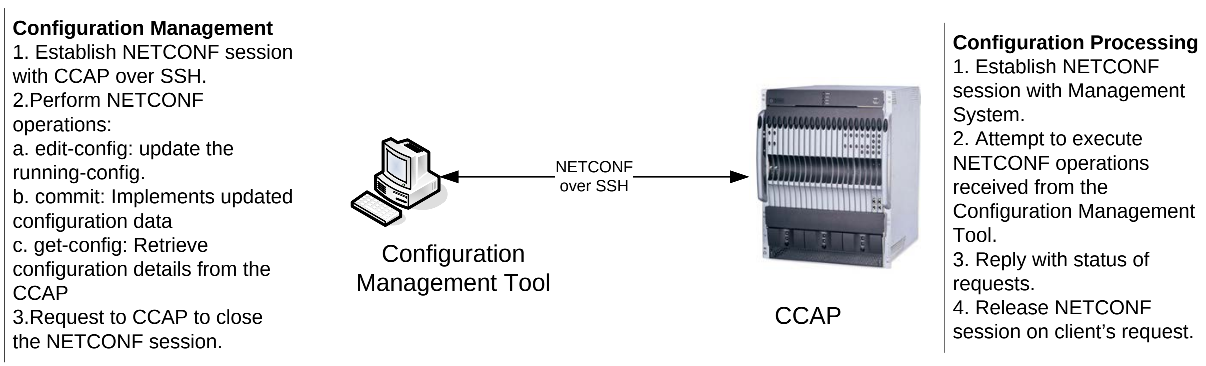

Figure 8 - CTD NETCONF-Based Configuration Use Case

The YANG modules, based on the CTD configuration Information Model, are implemented by the configuration management tool and the CTD; these modules are used to generate valid configuration NETCONF operations and content from the management system and to validate and execute those operations and content on the CTD.

When the configuration management tool begins the configuration process, an SSH session is set up between the configuration management tool and the CTD being configured. The configuration management tool can then deliver full or partial CTD configuration changes using NETCONF operations. The configuration content can be machine-generated or hand created; they are sent in the NETCONF RPC to the CTD.

The CTD receives, parses, and processes the configuration operations received via NETCONF from the configuration management tool. The CTD can be fully or partially reconfigured; invalid configuration instructions can be ignored while valid instructions will still be processed. The CTD can also reject configuration instructions if they cannot be met by the capabilities of the hardware present.

The CTD can also respond to <get-config> operations from the configuration management tool and provide a full or partial XML-based representation of the current device configuration, delivered to the configuration management tool via NETCONF.

The CTD NETCONF configuration process is discussed in the following sections.

8.7.2 NETCONF Overview

NETCONF [RFC 6241] is a configuration management protocol defined by the IETF. NETCONF provides mechanisms to install, manipulate, and delete the configuration of network devices.

NETCONF uses an XML-based data encoding for the configuration data as well as protocol messages. The protocol operations are realized on top of a simple Remote Procedure Call (RPC) layer. A client encodes an RPC in XML and sends it to a server using a secure, connection-oriented session. The server responds with a reply encoded in

XML. The contents of both the request and the response are fully described using YANG ([RFC 6020]) allowing both parties to recognize the syntax constraints imposed on the exchange.

NETCONF is connection-oriented, requiring a persistent connection between peers. This connection is expected to provide reliable, sequenced data delivery. NETCONF connections are long-lived, persisting between protocol operations; the connection is also expected to provide authentication, data integrity, and confidentiality.

NETCONF transport mapping includes SSHv2 [RFC 6242]. The SSH transport protocol mapping is mandatory to implement.

8.7.3 NETCONF Requirements

The CTD MUST implement NETCONF Server, as specified in [RFC 6241].

The CTD NETCONF Server MUST implement the base NETCONF capability identified by the urn:ietf:params:netconf:base:1.0 URN; all remaining capabilities described in the RFC are optional.

The CTD NETCONF Server MUST comply with the mandatory SSHv2 transport mapping specified in [RFC 6242].

The CTD SHOULD support the with-defaults Capability for NETCONF according to the 'report-all' basic mode, as defined in [RFC 6243]. A server that uses the 'report-all' basic mode does not consider any data node to be default data, even schema default data. When a client retrieves data with a <with-defaults> parameter equal to 'report-all', the CTD MUST report all data nodes, including any data nodes considered to be default data by the server.

8.7.3.1 NETCONF Operations

The CTD MUST support the "merge", "replace", and "delete" operations defined in section 7.2 of [RFC 6241]. This specification does not intend to make use of the "create" operation.

8.7.3.2 YANG Module Requirements

The CTD MUST support the ctd.yang module defined in [COOPT-CTD-YANG].

Annex A Detailed MIB Requirements (Normative)

This Annex defines the SNMP MIB modules and MIB objects required for Coherent Optics Termination Devices.

Table 44 - MIB Implementation Support

Requirement Type	Table Notation	Description
Deprecated	D	Deprecated objects are optional. If a vendor chooses to implement the object, the object is required to be implemented correctly according to the MIB definition. If a vendor chooses not to implement the object, an agent will not instantiate such object and must respond with the appropriate error/exception condition (e.g., 'noSuchObject' for SNMPv2c).
Mandatory	M	The object is required to be implemented correctly according to the MIB definition.
Not Applicable	NA	Not applicable to the device.
Not Supported	N-Sup	An agent will not instantiate such object and is required to respond with the appropriate error/exception condition (e.g., 'noSuchObject' for SNMPv2c).
Optional	O	A vendor can choose to implement or not implement the object. If a vendor chooses to implement the object, the object is required to be implemented correctly according to the MIB definition. If a vendor chooses not to implement the object, an agent will not instantiate such object and is required to respond with the appropriate error/exception condition (e.g., 'noSuchObject' for SNMPv2c).
Obsolete	Ob	In SNMP convention, obsolete objects should not be implemented. This specification allows vendors to implement or not implement obsolete objects. If a vendor chooses to implement an obsoleted object, the object is required to be implemented correctly according to the MIB definition. If a vendor chooses not to implement the obsoleted object, the SNMP agent will not instantiate such object and is required to respond with the appropriate error/exception condition (e.g., 'noSuchObject' for SNMPv2c).

Table 45 - SNMP Access Requirements

SNMP Access Type	Table Notation	Description
Not Accessible	N-Acc	The object is not accessible and is usually an index in a table
Read Create	RC	The access of the object is implemented as Read-Create
Read Write	RW	The access of the object is implemented as Read-Write
Read Only	RO	The access of the object is implemented as Read-Only
Read Create or Read Only	RC/RO	The access of the object is implemented as either Read-Create or Read-Only as described in the MIB definition
Read Create or Read Write	RC/RW	The access of the object is implemented as either Read-Create or Read-Write as described in the MIB definition
Read Write / Read Only	RW/RO	The access of the object is implemented as either Read-Write or Read-Only as described in the MIB definition
Accessible for SNMP Notifications	Acc-FN	These objects are used for SNMP Notifications by the Coherent Optics Transceiver SNMP Agent

A.1 CTD MIB Object Details

The CTD instantiates SNMP MIB objects based on its configuration and operational parameters acquired during initialization.

Table 46 provides the MIB object requirements for a CTD. The CTD MUST support the MIB objects as defined in Table 46.

Table 46 - CTD MIB Object Details

P2PCO-CTD-MIB [COOPT-CTD-MIB]		
Object	**Compliance**	**Access**
cooptCtdDspCfgTable	M	N-Acc

P2PCO-CTD-MIB [COOPT-CTD-MIB]		
cooptCtdDspCfgEntry	M	N-Acc
cooptCtdDspCfgSignalDegradeThrshld	O	RW
cooptCtdDspCfgModulation	M	RW
cooptCtdDspCfgSopTrackingRate	M	RW
cooptCtdDspCfgTxRateMode	M	RW
cooptCtdPerfMonCfgTable	M	N-Acc
cooptCtdPerfMonCfgEntry	M	N-Acc
cooptCtdPerfMonIntervalCfg	M	RW
cooptCtdPerfMonModeCfg	M	RW
cooptCtdOpticsCfgTable	M	N-Acc
cooptCtdOpticsCfgEntry	M	N-Acc
cooptCtdOpticsCfgRxPowerMinThrshld	M	RW
cooptCtdOpticsCfgRxPowerMaxThrshld	M	RW
cooptCtdOpticsCfgTxPower	M	RW
cooptCtdOpticsCfgTxWavelengthRangeMin	O	RW
cooptCtdOpticsCfgTxWavelengthRangeMax	O	RW
cooptCtdOpticsCfgTxWavelength	M	RW
cooptCtdOpticsCfgWavelength	M	RW
cooptCtdDspStatusTable	M	N-Acc
cooptCtdDspStatusEntry	M	N-Acc
cooptCtdDspStatusCurrDgd	M	RO
cooptCtdDspStatusCurrChromaticDispersion	M	RO
cooptCtdDspStatusSymbolRate	M	RO
cooptCtdOpticsStatusTable	M	N-Acc
cooptCtdOpticsStatusEntry	M	N-Acc
cooptCtdOpticsStatusRxPower	M	RO
cooptCtdOpticsStatusTxPower	M	RO
cooptCtdOpticsStatusTxPowerMinSupported	M	RO
cooptCtdOpticsStatusTxPowerMaxSupported	M	RO
cooptCtdOpticsStatusWavelength	M	RO
cooptCtdOpticsStatusTxWavelengthRangeMinSupported	M	RO
cooptCtdOpticsStatusTxWavelengthRangeMaxSupported	M	RO
cooptCtdOpticsStatusReceiveOsnr	M	RO
cooptCtdOpticsStatusPolarizationDependentLoss	M	RO
cooptCtdDspStatsTable	M	N-Acc
cooptCtdDspStatsEntry	M	N-Acc
cooptCtdDspStatsCorrectedBitCount	M	RO
cooptCtdDspStatsUncorrectableBlockCount	M	RO
cooptCtdDspStatsTotalBlockCount	M	RO
cooptCtdDspStatsBip8PmIntervalCount	M	RO
cooptCtdDspStatsBip8PmAggregateCount	M	RO
cooptCtdEntityTable	M	N-Acc
cooptCtdEntityEntry	M	N-Acc
cooptCtdEntityIndex	M	N-Acc
cooptCtdEntityMfgName	M	RO
cooptCtdEntityMfgOui	M	RO

P2PCO-CTD-MIB [COOPT-CTD-MIB]		
cooptCtdEntitySerialNum	M	RO
cooptCtdEntityHardwareRev	M	RO
cooptCtdEntityFirmwareRev	M	RO
coOptCtdDefaultEvReportingCfgTable	M	N-Acc
coOptCtdDefaultEvReportingCfgEntry	M	N-Acc
cooptCtdEvReportCfgPriority	M	RW
cooptCtdEvReportCfgReporting	M	RW
cooptCtdIfEnetCfgTable	M	N-Acc
cooptCtdIfEnetCfgEntry	M	N-Acc
cooptCtdIfNetCfgAdminStatus	M	RW
cooptCtdIfNetCfgLinkUpDownTrapEnable,	M	RW
cooptCtdIfNetCfgPromiscuousMode,	M	RW
cooptCtdIfNetCfgAlias	M	RW
cooptCtdIfEnetStatsTable	M	N-Acc
cooptCtdIfEnetStatsEntry	M	N-Acc
cooptCtdIfEnetStatsInOctets	M	RO
cooptCtdIfEnetStatsInFrames	M	RO
cooptCtdIfEnetStatsInUnicastFrames	M	RO
cooptCtdIfEnetStatsInMulticastFrames	M	RO
cooptCtdIfEnetStatsInBroadcastFrames	M	RO
cooptCtdIfEnetStatsInDiscards	M	RO
cooptCtdIfEnetStatsInErrors	M	RO
cooptCtdIfEnetStatsInUnknownProtos	M	RO
cooptCtdIfEnetStatsOutOctets	M	RO
cooptCtdIfEnetStatsOutFrames	M	RO
cooptCtdIfEnetStatsOutUnicastFrames	M	RO
cooptCtdIfEnetStatsOutMulticastFrames	M	RO
cooptCtdIfEnetStatsOutBroadcastFrames	M	RO
cooptCtdIfEnetStatsOutDiscards	M	RO
cooptCtdIfEnetStatsOutErrors	M	RO
cooptCtdIfEnetStatsCounterDiscontinuityTime	M	RO

Annex B Format and Content for Event, SYSLOG, AND SNMP Notification (Normative)

The CTD is required to send management protocol-dependent Notifications to the NMS as defined in Table 47 below for each manage entity in which the Coherent Optics Transceiver resides (e.g., switch port). Notifications will include the following information.

- Event-specific description
- Severity level
- Applicable keywords/values

The CTD is required to use the defined notification format for each defined event prescribed in this specification.

The CTD may append additional vendor-specific text to the end of the event text reported in the Coherent Optics Text object.

The CTD MUST implement the objects in Table 47 - CTD Event Reporting Requirements.

Table 47 - CTD Event Reporting Requirements

Object
CtdEventCtrlEventId
CtdEventCtrlStatus
CtdEventCtrlEventId
CtdEventCtrlStatus

Table 48 in this Annex summarizes the format and content for event, syslog, SNMP notifications and NETCONF notifications required for a P2P Coherent Optics CTD.

Each row specifies a possible event triggered by a Coherent Optics Transceiver and reported by the CTD. These events are to be reported by a CTD via one of the supported event mechanisms specified in Section 7.2.

The "Process" and "Sub-Process" columns indicate in which stage the event happens. The "CTD Priority" column indicates the priority the event is assigned in the CTD. These priorities are the same as is reported in the docsDevEvLevel object in the cable device MIB [RFC 4639] and in the LEVEL field of the syslog.

The "Event Message" column specifies the event text, which is reported in the docsDevEvText object of the CTD device MIB, the text field of the syslog and the NETCONF notification message. The "Message Notes And Detail" column provides additional information about the event text in the "Event Message" column. Some of the text fields include variable information, which are often specified as key-value pairs. The variables are explained in the "Message Notes And Detail" column. For events where the "Event Message" or "Message Notes and Detail" column includes either <P1>, <P2> or <Pn>, there is a colon and single space between the value as defined by <P1>, <P2> or <Pn> and the preceding key text.

The key-value parameters are thus formatted as: [key]: [value]. Key value pairs are delimited by a semi-colon followed by a single space, as the following example indicates:

[key 1]: [value 1]; [key 2]: [value 2]; [key n]: [value n]

The “Event Message” field structure is defined as follows:

<Initial Event Message Text>; [key 1]: [value 1]; [key 2]: [value 2]; [key n]: [value n]; <TAGS>;

Keys which contain values which represent strings can enclose those strings within double-quotations to prevent confusion if those string values contain a delimiter (colon or semicolon). Key strings should capitalize each word (e.g., “Sensor Unit”). If a key’s value is not present, the key is present, but the value is omitted (using a single space). For example:

key 1: ;

It is recommended that <Initial Event Message Text> string does not contain a semicolon since this is used as a delimiter. The <Initial Event Message Text> string follows a normal sentence capitalization scheme where the first word is capitalized as well as any defined terms and acronyms.

For the CTD (without the quotes):"<CTD-ID>;<CTD-ifIndex>"

Where:

```
<CTD-ID>: Unique identifier for the CTD;
Format*: "CTD-ID: xx:xx:xx:xx:xx:xx"
<CTD-ifIndex>: CTD ifIndex associated with Transceiver

Format*: "CTD-ifIndex: nnnnnnnn"
```

(*) without the quotes

The CTD is required to support all mandatory events defined in Table 48.

The CTD may append additional vendor-specific text to the end of the event text reported in the docsDevEvText object, the syslog text field and the NETCONF notification message.

The "Error Code Set" column specifies the error code. The "Event ID" column indicates a unique identification number for the event, which is assigned to the docsDevEvId object in the cable device MIB or YANG message, and the <eventId> field of the syslog. Refer to [CANN] for the rules to generate unique Event IDs from the Error Code Set. The "Notification Name" column specifies the SNMP or NETCONF notification, which notifies this event to a Management notification receiver.

Table 48 - CTD Event Format and Content

Process	Sub-Process	CTD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID	Notification Name
Performance							
Optics	Power	Error	Transmit Power Low; <TAGS>;		C900.00	67090000	CTD: cooptTranscieverEventNotif
Optics	Power	Error	Transmit Power High; <TAGS>;		C900.01	67090001	CTD: cooptTranscieverEventNotif
Optics	Power	Error	Receive Power Out of Range; <TAGS>;		C900.02	67090002	CTD: cooptTranscieverEventNotif
Optics	Power	Error	Transmit Power Out of Range; <TAGS>;		C900.03	67090003	CTD: cooptTranscieverEventNotif
Optics		Error	ITLA TEC Fault; <TAGS>;		C900.04	67090004	CTD: cooptTranscieverEventNotif
Optics		Error	ITLA Age; <TAGS>;		C900.05	67090005	CTD: cooptTranscieverEventNotif
DSP		Critical	Receive Loss of Lock; <TAGS>;		C900.06	67090006	CTD: cooptTranscieverEventNotif
DSP		Error	Loss of Frame (LOF) Detected; <TAGS>;		C900.07	67090007	CTD: cooptTranscieverEventNotif
DSP		Error	Signal Degrade; <TAGS>;		C900.08	67090008	CTD: cooptTranscieverEventNotif
Physical and Environmental							
Environmental	Temperature	Error	Case Temp Low; <TAGS>;		C901.00	67090100	CTD: cooptTranscieverEventNotif
Environmental	Temperature	Error	Case Temp High; <TAGS>;		C901.01	67090101	CTD: cooptTranscieverEventNotif

Annex C Data Type Definitions (Normative)

C.1 Overview

This section includes the data type definitions for the Information Models defined for use in the CTD. UML is used for modeling the management requirements.

The data types defined in this section are mapped for use with SNMP MIBs, IPDR XML schemas, YANG modules and XSD Schemas.

C.1.1 Data Types Mapping

XML is becoming the standard for data definition models. With XML, data transformations can be done with or without a model (DTD or Schema definition). DTDs and XML schemas provide additional data validation layer to the applications exchanging XML data. There are several models to map formal notation constructs like ASN.1 to XML [ITU-T X.692], UML to XML, YANG to XML, or XML by itself can be used for modeling purposes.

Each area of data information interest approaches XML and defines data models and/or data containment structures and data types. Similarly, SNMP took and modified a subset of ASN.1 for defining the Structured Management Information SMIv1 and SMIv2.

Due to the lack of a unified data model and data types for Network Management, a neutral model would be appropriate to allow capturing specific requirements and methodologies from existing protocols and allow forward or reverse engineering of those standards like SNMP to the general object model and vice versa.

C.1.2 Data Types Requirements and Classification

The Information Model has to provide seamless translation for SMIv2 requirements, in particular when creating MIB modules based on the Information Model. This specification needs to provide full support of [RFC 2578], [RFC 2579], and the clarifications and recommendations of [RFC 4181].

The Information Model has to provide seamless translation for YANG modeling requirements, in particular when creating YANG modules based on the Information Model.

Thus, there are two data type groups defined for modeling purposes and mapping to protocol data notation roundtrip.

- General data types

  Required data types to cover all the management syntax and semantic requirement for all OSSI-supported data models. In this category are data types defined in SNMP SMIv2 [RFC 2578], and YANG common data types [RFC 6991].

- Extended data types

  Management protocols specialization based on frequent usage or special semantics. Required data types to cover all the syntax requirement for all OSSI-supported data models. In this category are SNMP TEXTUAL-CONVENTION clauses [RFC 2579] of mandatory or recommended usage by [RFC 2579] and [RFC 4181] when modeling for SNMP MIB modules.

C.1.3 Data Type Mapping Methodology

The specification "XML Schema Part 2: Data types Second Edition" is based on [ISO 11404], which provides language-independent data types (see XML Schema reference). The mapping proposed below uses a subset of the XML schema data types to cover both SNMP forward and reverse engineering, and IPDR types. Any additional protocol being added should be feasible to provide the particular mappings.

SMIv2 has an extensive experience of data types for management purposes; for illustration consider Counter32 and Counter64 SMIv2 types [RFC 2578]. The XML schema data types makes no distinction of derived 'decimal' types and the semantics that are associated to counters, e.g., counters do not necessarily start at 0.

Most of the SNMP information associated to data types are reduced to size and range constraints and specialized enumerations.

C.1.4 General Data Types (SNMP Mapping)

Table 49 represents the mapping between the OSSI Information Model General Types and their equivalent representation for SNMP MIB Modules and IPDR Service Definitions. The permitted values for the data types are indicated in terms of value ranges and string length when applicable. The Information Model Data Type column includes the data types to map to SNMP, using the appropriated type in the corresponding protocol if applicable or available. The SNMP Mapping references to SNMP data types are defined in [RFC 2578] or as described below.

Note that SNMP does not provide float, double or long XML-Schema data types. Also, SNMP might map a type to an SNMP subtyped value. For example, UnsignedByte data type maps to Unsigned32 subtyped to the appropriate range indicated by the Permitted Values (0..255 in this case). Other data types are mapped to SNMP TEXTUAL-CONVENTIONS as indicated by the references.

Table 49 - General Data Types

UML Data Type	XML-Schema data type	Permitted Values	SNMP Mapping
AdminStateType	enumeration	other(1), up(2), down(3), testing(4)	INTEGER
Boolean	Boolean	true = 1 false = 0	TruthValue [RFC 2579]
Byte	byte	-128..127	Integer32
Counter32	unsignedInt		Counter32
Counter64	unsignedLong		Counter64
DateTime	dateTime	SIZE (8 or 11)	DateAndTime
DateTimeMsec	unsignedLong		CounterBasedGauge64 [RFC 2856]
Enum	int	-2147483648..2147483647	INTEGER
EnumBits	hexBinary		BITS
Gauge32	unsignedInt		Gauge32
Float	float	-3.4E+38..+3.4E+38	
HexBinary	hexBinary	A sequence of octets.	OCTET STRING
InetAddress	string	SIZE (0..255)	InetAddress [RFC 4001]
InetAddressIpv4	string	SIZE (4)	InetAddressIPv4 [RFC 4001]
InetAddressIpv6	string	SIZE (16)	InetAddressIPv6 [RFC 4001]
InetAddressType	enumeration	unknown(0), ipv4(1), ipv6(2), ipv4z(3), ipv6z(4), dns(16)	InetAddressType [RFC 4001]
Int	int	-2147483648..2147483647	Integer32
Long	long	-9223372036854775808..-9223372036854775807	N/A
MacAddress	hexBinary	SIZE (6)	MacAddress
Opaque	hexBinary		Opaque
OperStatusType	enumeration	other(0), up(1), down(2), testing(3), dormant(4), notPresent(5), lowerLayerDown(6)	INTEGER
Short	short	-32768..32767	Integer32
String	string		SnmpAdminString [RFC 3411]
UnsignedByte	unsignedByte	0..255	Unsigned32
UnsignedInt	unsignedInt	0..4294967295	Unsigned32

UML Data Type	XML-Schema data type	Permitted Values	SNMP Mapping
UnsignedLong	unsignedLong	0..18446744073709551615	CounterBasedGauge64 [RFC 2856]
UnsignedShort	unsignedShort	0..65535	Unsigned32
Uuid	hexBinary		OCTET STRING
UUIDorZero	hexBinary		OCTET STRING (SIZE (0|16)) [RFC 6933]

C.1.5 Primitive Data Types (YANG Mapping)

Table 50 represents the mapping between the CCAP Core primitive data types and their equivalent representation in YANG. The permitted values for the data types are indicated in terms of value ranges and string length when applicable. The UML Primitive Data Type column includes the data types to map to YANG, using the appropriate type in YANG. The YANG Built-In Data Type Mapping references YANG data types defined in [RFC 6021] or as described below.

Table 50 - Primitive Data Types

UML Primitive Data Type	YANG Data Type Mapping	Permitted Values
Boolean	Boolean	true, false
Byte	int8	-128..127
Enum	enumeration	-2147483648..2147483647
EnumBits	bits	
HexBinary	ccap-octet-data-type	([0-9a-fA-F]{2})*
Int	int32	-2147483648..2147483647
Long	int64	-9223372036854775808..9223372036854775807
Short	int16	-32768..32767
String	string	
UnsignedByte	uint8	0..255
UnsignedInt	uint32	0..4294967295
UnsignedLong	uint64	0..18446744073709551615
UnsignedShort	uint16	0..65535

C.1.6 Extended Data Types (SNMP Mapping)

There are two sources of Extended Data Types: Protocol specific data types, and OSSI data types.

SNMP derived types are defined in SNMP MIB Modules. The most important are in [RFC 2579], which is part of SNMP STD 58, and are considered in many aspects part of the SNMP protocol. Other MIB modules TEXTUAL-CONVENTION definitions have been adopted and recommended (e.g., [RFC 4181]) for re-usability and semantics considerations in order to unify management concepts; some relevant RFCs that include commonly used textual conventions are [RFC 4001], [RFC 2863], [RFC 3411], and [RFC 3419] among others (see [RFC 4181]).

Table 51 includes the most relevant data types taken from SNMP to provide a direct mapping of the OSSI Information Model to SNMP MIB modules. For example, TagList comes from [RFC 3413] SnmpTaglist and preserves its semantics; AdminString comes from [RFC 3411] SnmpAdminString.

In general, when an OSSI Information Model needs to reference an existing SNMP textual convention for the purpose of round-trip design from UML to SNMP, these textual conventions can be added to this list. Other sources of textual conventions not listed here are from MIB modules specific to DOCSIS, either as RFCs or in this specification. Some of those sources are [RFC 4546] and Annex A.

OSSI data types are also defined in this specification in Annex A.

Table 51 - Extended Data Types

OM Data Type	XML-Schema data type	Permitted Values	SNMP Mapping
AdminString	string	SIZE (0..255)	SnmpAdminString
DocsEqualizerData	hexBinary		DocsEqualizerData [RFC 4546]
DocsisQosVersion	int		DocsisQosVersion [RFC 4546]
DocsisUpstreamType	int		DocsisUpstreamType [RFC 4546]
Duration	unsignedInt	0..2147483647	TimeInterval
InetAddressPrefixLength	unsignedInt	0..2040	InetAddressPrefixLength [RFC 4001]
InetPortNumber	unsignedInt	0..65535	Unsigned32
PhysicalIndexOrZero	unsignedInt	0..2147483647	Integer32
RowStatus	int		RowStatus
StorageType	int		StorageType
TagList	string	SIZE (0..255)	SnmpTaglist
TenthdB	int		TenthdB [RFC 4546]
TenthdBmV	int		TenthdBmV [RFC 4546]
TimeStamp	unsignedInt		TimeStamp

C.1.7 Derived Data Types (YANG Mapping)

Table 52 represents the mapping between the CCAP Core derived data types and their equivalent representation in YANG. The permitted values for the data types are indicated in terms of value ranges and string length when applicable. The UML Derived Data Type column includes the data types to map to YANG, using the appropriate type in YANG. The YANG Derived Data Type Mapping references YANG data types defined in [RFC 6021] or as described below.

Table 52 - Derived Data Types

UML Derived Data Type	YANG Derived Data Type Mapping	Permitted Values
AdminStateType	admin-state-type	other(1), up(2), down(3), testing(4)
Counter32	counter32	
Counter64	counter64	
Gauge32	gauge32	
Float	decimal64	-3.4E+38..+3.4E+38
InetAddress	ip-address	IPv4 or IPv6 Address
InetAddressIpv4	ipv4-address	IPv4 Address
InetAddressIpv6	ipv6-address	IPv6 Address
InetAddressPrefixLength	address-prefix-len-type	0..2040
InetIpv4Prefix	ipv4-prefix	IPv4 Address "/" IPv4 Prefix Length
InetIpv6Prefix	ipv6-prefix	IPv6 Address "/" IPv6 Prefix Length
InetPortNumber	port-number	0..65535
MacAddress	mac-address	e.g., 01:23:45:67:89:ab
TagList	snmp-tag-list-type	String(SIZE(0..255))
TenthHz	uint8	0..9
TimeStamp	timestamp	
Uri	uri	

C.2 Common Terms Shortened

The following table lists common terms which have been shortened to allow shorter SNMP MIB names. These shortened names are desired to be used consistently throughout the object models, SNMP MIBs and IPDR schemas.

Table 53 - Shortened Common Terms

Original Word	Shortened Word
Address	Addr
Aggregate	Agg
Algorithm	Alg
Allocation	Alloc
Application	App
Attribute	Attr
Authorization	Auth
Channel	Ch
Command	Cmd
Config*	Cfg
Control	Ctrl
Default	Def
Destination	Dest
Direction	Dir
Downstream	Ds
Encryption	Encrypt
Equalization	Eq
Group	Grp
Length	Len
Maximum	Max
Minimum	Min
Multicast	Mcast
Provision*	Prov
Receive	Rx
Registration	Reg
Replication	Repl
Request	Req
Resequence	Reseq
Resequencing	Reseq
Response	Rsp
Segment	Sgmt
Sequence	Seq
Service	Svc
ServiceFlow	Sf
Session(s)	Sess
Source	Src
Threshold	Thrshld
Total	Tot
Transmit	Tx

Original Word	Shortened Word
Upstream	Us
* indicates a wildcard	

C.2.1 Exceptions

Data types and managed objects do not consistently use the shortened names.

Appendix I Acknowledgements (Informative)

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

Contributor	Company Affiliation
Mike Pan	Acacia
Chris Gosnell, Eric Maniloff	Ciena
Brian Hedstrom	OAM Technology Consulting
Steve Burroughs, Matthew Schmitt, Ken Barringer, Christie Poland	CableLabs

Appendix II Revision History

Engineering Changes incorporated into P2PCO-SP-CTD-OSSI-I02-200501:

ECN Identifier	Accepted Date	Title of EC	Author
CTD-OSSI-N-19.0011-1	3/11/20	Initial Coherent Optics MIB module COOPT-CTD-MIB	Jewitt
CTD-OSSI-N-19.0012-1	3/11/20	Initial Coherent Optics YANG module	Thompson
CTD-OSSI-N-19.0013-1	3/11/20	Issues identified in the spec when defining the COOPT-CTD-MIB	Hedstrom

* * *