Optical Operations and Maintenance
PON Ops Solutions for the Cable Industry

Optical Operations and Maintenance Solutions for PON

OOM-TR-PON-Ops-V02-260122

RELEASED

Notice

This OOM technical report is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by CableLabs® in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third-party documents, including open source licenses, if any.

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provide any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, infringement, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	OOM-TR-PON-Ops-V02-260122			
Document Title:	Optical Operations and Maintenance Solutions for PON			
Revision History:	V01 – Released 06/02/2025 V02 – Released 01/22/2026			
Date:	January 22, 2026			
Status:	~~Work in Progress~~	~~Draft~~	**Released**	~~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.
Draft	A document that is considered largely complete but is undergoing review by working groups, members, and vendors. Drafts are susceptible to substantial change during the review process.
Released	A public or gated document that has undergone review. Released technical reports are **not** subject to the Engineering Change process.
Closed	A static document that has been closed to further changes through CableLabs.

Trademarks

Contents

Figures

Tables

1 SCOPE

1.1 Introduction

There is momentum to provide fiber to the premises (FTTP) solutions in the cable industry. Though optical technologies have been a part of the cable network for over 40 years, FTTP is increasingly being considered for the access network. For FTTP, the premises can be a subscriber's home, a commercial location, a campus environment, a multi-dwelling unit (MDU), etc. Over the past couple of decades, operators have embraced Passive Optical Network (PON) technology for their access network implementations. The 1-to-N topology of PON lends itself nicely to current and future designs of the cable network.

1.2 Scope

PON is not the only optical solution for operators (e.g., point-to-point), but given economies of scale, network topology, and optionality, PON is a clear choice for operators. As such, this technical report covers PON technology—specifically, IEEE PON, ITU-T PON, and 25GS-PON (multi-source agreement) technologies.

1.3 Purpose of Report

This report serves to align the cable industry on telemetry to support optical operations use cases, maintenance use cases, and operator needs for assuring service over optical access technologies. It focuses specifically on PON technology but remains agnostic as to the version or related standards chosen, such as ITU-T or IEEE. This report lays a foundation for aligning telemetry, and work will continue after the publication of this version.

The goals of the work include the following.

- Reduce time and costs of troubleshooting and problem resolution while increasing network capacity and uptime.
- Create and document traceability from the architecture and its elements that must be managed through to the telemetry.
- Identify the most important use cases for cable operators that must be supported in PON access.
- Align key performance metrics with existing cable operator approaches.
- Enable alignment with existing tools and practices used for DOCSIS access networks.

The scope of this report includes

- proactive, reactive, and predictive maintenance, other forms of maintenance, and fault management;
- the physical layer and above; and
- telemetry alignment, solution development, and more.

It will provide traceability from the architecture scope through faults and failures that must be managed, through use cases that describe how operators will maintain these systems, and through the information needed to assure service over these systems, to the telemetry that are specified to enable efficient operations. Therefore, this report will contain and/or reference other documents that describe each of these elements and will describe how the parts connect, providing the needed traceability.

Future work will include development of models and tools that enable efficient operations.

2 REFERENCES

2.1 Informative References

This technical report uses the following informative references.

[Cable OpenOMCI]	Cable OpenOMCI Specification, CPMP-SP-Cable-OpenOMCI-I03-251211, December 11, 2025, Cable Television Laboratories, Inc.
[DOCSIS Prov]	DOCSIS Provisioning of ITU-T PON, CPMP-TR-DOCSIS-Prov-V02-250519, May 19, 2025, Cable Television Laboratories, Inc.
[DPoE]	DPoE Architecture Specification, DPoE-SP-ARCHv2.0-I08-230322, March 22, 2023, Cable Television Laboratories, Inc.
[eRouter]	IPv4 and IPv6 eRouter Specification, CM-SP-eRouter-I22-240503, May 5, 2024, Cable Television Laboratories, Inc.
[G.984.3]	ITU-T Recommendation G.984.3 (01/2014) Amendment 1 (03/2020), Gigabit Capable Passive Optical Network (G-PON), Transmission Convergence Layer Specification
[G.984.4]	ITU-T Recommendation G.984.4 (02/2008) Amendment 3 (07/2010), Gigabit Capable Passive Optical Network (G-PON), ONT Management and Control Interface Specification
[G.988]	ITU-T Recommendation G.988 (2022) Amendment 2 (05/2024), ONU Management and Control Interface (OMCI) Specification
[G.9804.1]	ITU-T Recommendation G.9804 (11/2019) Amendment 2 (01/2024), Higher Speed Passive Optical Network Requirements
[G.9807.1]	ITU-T Recommendation G.9807.1 (02/2023), 10-Gigabit Capable Symmetric Passive Optical Network (XGS-PON)
[IEEE 802.1ad]	IEEE Std 802.1ad-2005, IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges, May 2006
[IEEE 802.3]	IEEE Std 802.3-2018, IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks, Specific Requirements—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, August 2018
[RFC 2597]	IETF RFC 2597, Assured Forwarding PHB Group, J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, June 1999
[RFC 2698]	IETF RFC 2698, A Two Rate Three Color Marker, J. Heinanen, R. Guerin, September 1999
[RFC 2819]	IETF RFC 2819, Remote Network Monitoring Management Information Base, S. Waldbusser, May 2000
[RFC 2863]	IETF RFC 2863, The Interfaces Group MIB, K. McCloghrie, F. Kastenholz, June 2000
[RFC 4115]	IETF RFC 4115, A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic, O. Aboul-Magd, S. Rabie, July 2005
[SCTE 292]	ANSI SCTE 292 2024R1, Broadband Component QR Code Technical Requirements, 2024
[TR-069]	Broadband Forum Technical Report 069, CPE WAN Management Protocol, May 2004
[TR-104]	Broadband Forum Technical Report 104, VoiceService:2.0 Service Object Definition [USP], January 2020
[TR-143]	Broadband Forum Technical Report 143, CPE WAN Management Protocol, September 2024
[TR-181]	Broadband Forum Technical Report 181, Device Data Model for CWMP Endpoints and USP Agents, September 2024, https://device-data-model.broadband-forum.org/index.html
[Wichman 2024]	"You Might Have a Screw Loose: Remote Detection of Thermal Imperfections," M. Wichman, V. Mutalik, J. Cook, SCTE TechExpo 2024, September 23–26, 2024, Atlanta, GA

2.2 Reference Acquisition

- BBF: Broadband Forum, 39221 Paseo Padre Pkwy, Suite J, Fremont, CA 94538; www.broadband-forum.org
- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone: +1 303-661-9100; Fax: +1 303-661-9199; www.cablelabs.com
- IEEE: Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, NY 10016-5997; Phone: +1 212-419-7900; Fax: +1 212-752-4929; www.ieee.org
- IETF: Internet Engineering Task Force Secretariat, c/o Association Management Solutions, LLC (AMS), Fremont, CA 94538; Phone: +1 510-492-4080, Fax: +1 510-492-4001; http://www.ietf.org
- ITU-T Recommendations: International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, 1211 Geneva 20, Switzerland; Phone: +41 22 730 5852; Fax: +41 22 730 5853; www.itu.int
- SCTE: Society of Cable Telecommunications Engineers, 140 Philips Road, Exton, PA 19341; Phone: +1 610-363-6888; www.scte.org

3 TERMS AND DEFINITIONS

3.1 Terms and Definitions

This technical report uses the following terms.

application	Software that comprises one or more automated functions for a purpose or use case
application programming interface	A way for computer programs to communicate information via a set of protocols
batch	A set of components, subsystems, or systems that are produced at the same general time at the same location from the same manufacturer following the same design and materials
component/part	The smallest division item in a network or system that is used in combination with other like items to create subsystems and systems, including a field replaceable unit
dashboard	A way to display information (telemetry, statistics, etc.) for human comprehension
failure	Lack of success; cease function
fault	Weakness, sub-optimal performance, impairment
field replaceable unit	A component or subsystem that can be replaced by the operator in the field as a whole without replacing the larger subsystem or system, usually in the context of repair, upgrade, fault mitigation, etc., in a network or system; spares are maintained.
interface	A point where two or more systems, computers, users, and other entities communicate
Kafka	A binary protocol using TCP for delivery
key performance indicator	A quantifiable measure of performance or effectiveness relating to a specific objective
network	Interconnected computer systems that communicate data
network element	A defined system participating in the network, providing a function or functions in the network
open telemetry	A collection of application interfaces and development kits and tools to aid in the support of telemetry that is open source and vendor neutral
Optical Operations and Maintenance	Network operations functions relating to optical networking
log	A time-stamped-event-based historical data element about the status of the machine or network element
query	A request for machine or network data, with expectation of a response, and that the data are from the current state of the network, in contrast to a test. A query may be for data that already exist or are being collected by the machine or network device, or may require an action to start the data collection that is a separate action.
serial number	A unique identifier for a system, subsystem, or field replaceable unit that contains information about its manufacturer and date and order of production; it also may contain additional information.
serial part	The portion of the serial number that is incremented to assure uniqueness of the serial number for like items from the same manufacturer and location
subscription	A process in which machine or network data may be requested and delivered indefinitely or for a period of time. The data may not be delivered until subscribed to, but can be obtained once subscribed to, and is delivered as advertised, be that on a periodic basis or by event, for example.
subsystem	A part of a system that is a system itself but that provides some lower function as part of the larger system functions
system	A functionally combined group of subsystems and/or components connected to provide defined functions
telemetry	Useful data from network devices. In general, telemetry can refer to useful data obtainable from any machine; in our context, that would most commonly be a network device but could also include test equipment, records in a database, and more.
test	A procedure consisting of performing an action under a given set of conditions with the expectation of collecting data. Note that this definition of test lies within the context of telemetry data collection.
use case	A method or system description to execute a function; a method to identify, clarify, and specify requirements

4 ABBREVIATIONS

This technical report uses the following abbreviations.

AAA	authentication, authorization, and accounting
ACS	auto configuration server
AI	artificial intelligence
AP	access point
API	application programming interface
ATA	analog terminal adapter
AVC	attribute value change
BER	bit error rate
BNG	broadband network gateway
BOM	bill of material
BSS	business support system
CAC	conditional access control
CCF	common collection framework
CIN	converged interconnect network
CIR	committed information rate
CLI	command line interface
CPE	customer premise equipment
CPU	central processing unit
CRC	cyclic redundancy check
CRM	customer relationship management
CWMP	CPE WAN Management Protocol
dB	decibel
dBm	decibel-milliwatts
DHCP	Dynamic Host Configuration Protocol
eBPF	extended Berkeley packet filter
eDVA	embedded digital voice adapter
EIR	excess information rate
EMS	element management system
eMTA	embedded multimedia terminal adapter
EPON	Ethernet PON
FEC	forward error correction
FTTP	fiber to the premise
GEM	GPON encapsulation method
GER	GEM error rate
GIS	geographical information system
gNMI	remote procedure call (RPC) network management interface
GPON	gigabit passive optical network
gRPC	cross-platform high-performance remote procedure call (RPC) framework
GUI	graphic user interface
HEC	header error control
HFC	hybrid fiber coax
HSD	high speed data
HSI	high speed internet
HTTP	Hypertext Transfer Protocol
HW	hardware
ICMP	Internet Control Message Protocol
ID	identification
IEEE	Institute of Electrical and Electronics Engineering
IP	Internet Protocol

IPDR	Internet Protocol detail record
iPerf	Internet performance test (tool)
IPFIX	Internet Protocol flow information export
ITU-T	International Telecommunications Union – Telecommunications Sector
KPI	key performance indicator
L1, L2, L3	layer 1, layer 2, layer 3
LAG	link aggregation
LLID	logical link identifier
LLM	large language model
MAC	media or medium access control layer
MDU	multi-dwelling unit
ME	management entity
MIC	manufacturing installed certificate
ML	machine learning
MQTT	message queueing telemetry transport
MSA	multi-source agreement
NAP	network access point
Netconf	Network Configuration Protocol
NID	network interface device
NMS	network management system
NOC	network operations center
OAM	operations, administration, and management
ODF	optical distribution frame
ODN	optical distribution network
OLT	optical line terminal
OMCI	ONU management and control interface
OOM	optical operations and maintenance
ONT	optical network terminal
ONU	optical network unit
OSI	open systems interconnect
OSP	outside plant (network)
OSS	operation support system
OTDR	optical time domain reflectometer
PHM	prognostics and health management
PHY	Physical Layer
PIC	photonic integrated circuit
PID	port identification
PIR	peak information rate
PLOAM	physical layer operation administration and maintenance
PNM	proactive network maintenance
PON	passive optical network
PPPoE	point-to-point protocol over Ethernet
ProOps	proactive operations platform
RG	residential gateway
R-OLT	remote OLT
RPD	remote PHY device
RX, Rx	receive
SD	software defined
SF	signal failure
SFP	small form-factor pluggable
SMB	small and midsize business
SNMP	Simple Network Management Protocol
SW	software

TCA	time critical application
TGPON	transceiver for GPON
TX, Tx	transmit
USP	user services platform
VCI	virtual channel identifier
VLAN	virtual local area network
WAN	wide area network
WLAN	wireless local area network
Wi-Fi	wireless fidelity
YANG	Yet Another Next Generation (protocol)

5 ARCHITECTURE

The baseline architecture for this effort is the PON topology within a cable access network, depicted in Figure 1, Figure 2, and Figure 3. This technical report includes components and functionality that are specific to that access network and its layer 1 and layer 2 functions and components, including any functionality at other layers and outside the boundaries that still support the PON layer 1 and layer 2 functions. The functionality of the required network is the motivation for this report—it will not define specific components or dictate where those components are located.

The baseline architecture supports all the objectives and work detailed in this report. This architecture includes the entirety of the access network and everything operators need to manage faults and failures and monitor functions of the network segment. Figure 1 shows the high-level architecture. The scope of this report, highlighted in yellow/gold, extends through the access network and functions that support layers 1 and 2.

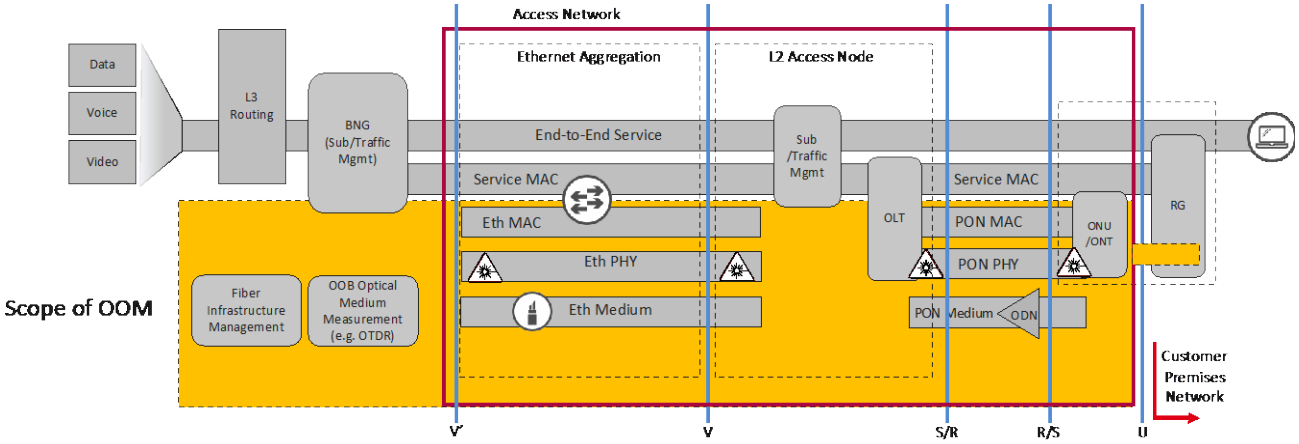


Figure 1 - PON Access Architecture with Scope of Report Highlighted

Assumptions

- An access node may contain more than one optical line terminal (OLT) (port).
- The residential gateway (RG) may be co-resident with the optical network unit (ONU) (or the optical network terminal, ONT; herein, the term "ONU" will also reference this device). An ONU with a co-resident RG is an integrated or embedded ONU.
- In an MDU, a single ONU might serve several RGs over different media.
- BNG (broadband network gateway) is noted as a generic function for subscriber/traffic management and may be resident in the access node or in the "cloud" and may be distributed, but it does not have to be a true BNG.
- Ethernet (e.g., IP over Ethernet) encapsulation resides only in the access network (e.g., no PPPoE).
- Routing may be co-resident in the access node.

This architecture applies to both distributed and centralized solutions; the functions and components are generalized to ensure equal application regardless of the solution chosen. The main difference between centralized and distributed network solutions is that failure modes may differ, which leads to the lowest common denominator driving the relevant operations use cases. Figure 2 depicts the access architecture with PON components in a distributed and a centralized fashion.

A centralized PON topology is a more traditional implementation for delivering broadband network access to operator subscribers. The most apparent distinction for this topology is that the OLT is located in the hub or headend or outside cabinet. Given this implementation, and because this is a point-to-multipoint topology, the backhaul or transport fiber run from the hub or headend to the first split point may be longer, thereby reducing the total reach of the PON.

A distributed PON is a newer implementation of PON topology. Because this implementation pushes the OLT farther out into the optical distribution network (ODN), the OLT is referred to as a remote OLT (R-OLT). Disaggregation of the access network is becoming a popular way to design the access network and provides many advantages. Though this report does not discuss the advantages or disadvantages of such an implementation, it and associated documents do call out any specific differences and how to support those differences.

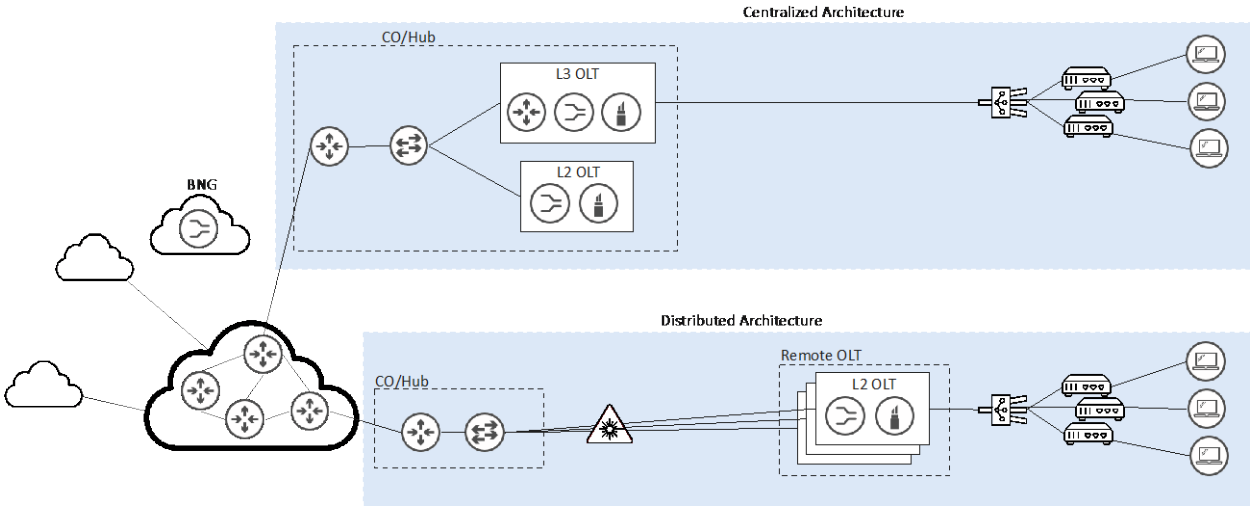


Figure 2 - Comparison of Centralized and Distributed PON Architectures

To meet the goals of Optical Operations and Maintenance (OOM), a generalized data collection and presentation architecture is also identified. Figure 3 shows the elements of the tools stack.

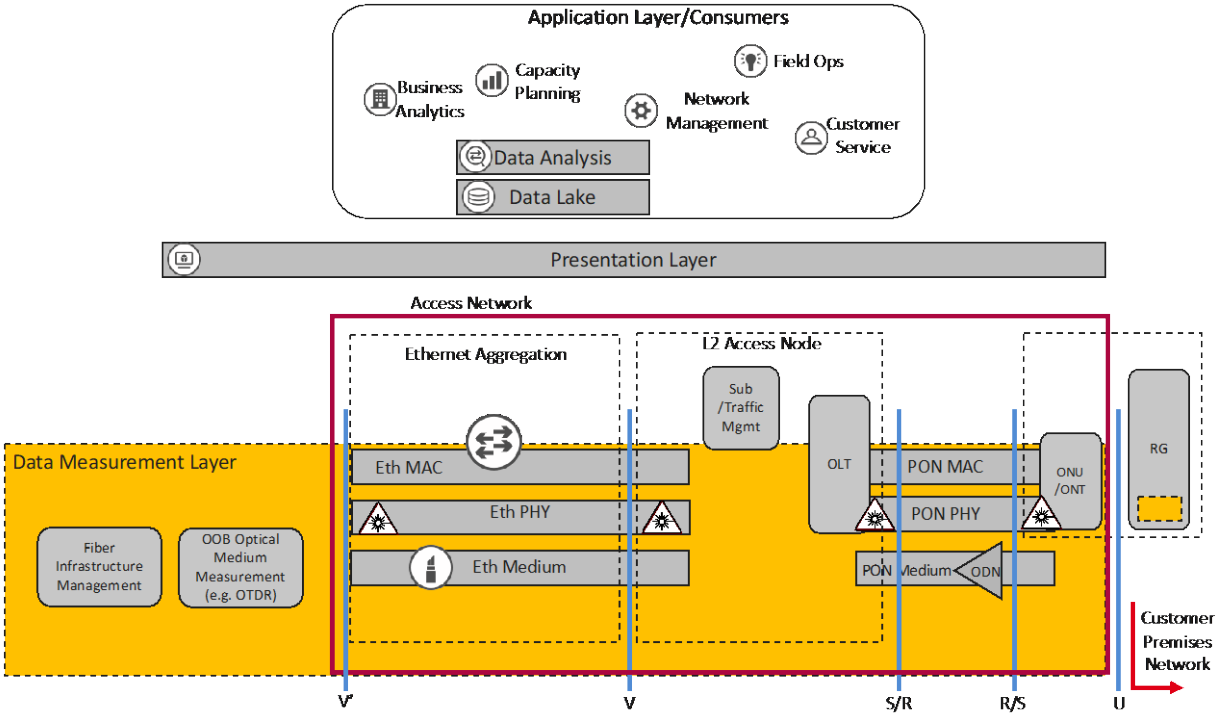


Figure 3 - PON Architecture with Scope of Report Highlighted and Tools Stack for Reference

The sections that follow will describe portions of the architecture and the included components.

5.1 PON MAC/PHY and Fiber

Figure 4 depicts the photonic access network. The systems included in the PON portion of the architecture are shown in the green frame and include the entire fiber system between the OLT and ONU, including the optoelectronics. The scope of this report is highlighted in yellow/gold. Note the boundaries of the access network (red frame) overlap but do not contain the scope, as the functionality of the access network extends beyond the access network itself.

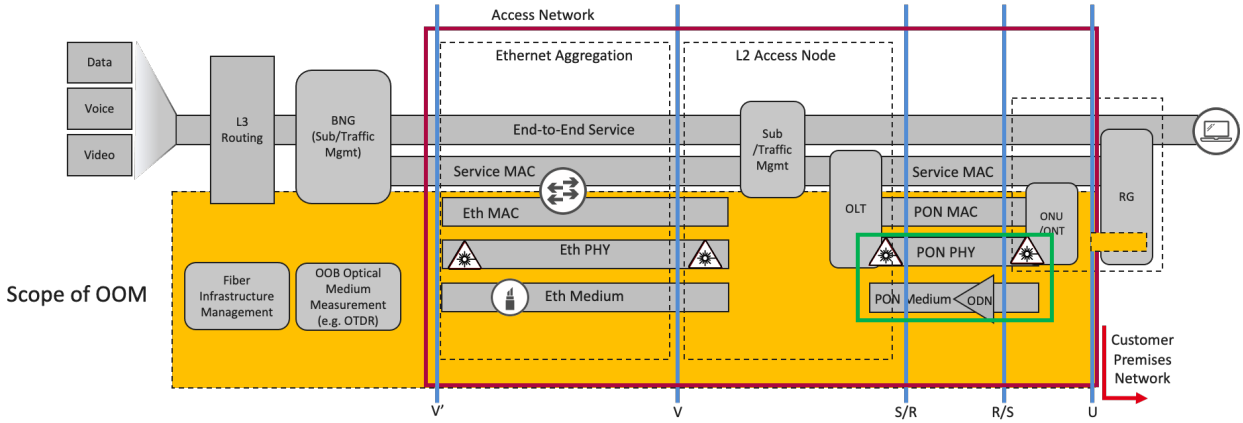


Figure 4 - Photonic Access Network with Scope of Report Highlighted and PON MAC/PHY and Fiber Use Case Category in Green

The fiber system for the optical distribution network (ODN), including the optical components on the ends and any splices, connectors, or other devices in between, must be maintained against faults and failures. When faults or failures occur, the system needs to reveal the condition, allow identification of the fault or failure, and support localization.

The function of this system is to carry data over the PON between the OLT and ONU. Data are carried to provide a number of services, so upper layer functions must be supported. For this reason, layer 2 and layer 3 (L2/L3) functions must also be included in this system.

The subsystems included in the PON portion of the architecture are as follows.

- PON MAC—the PON-specific protocols that manage the PON and access to the PON
- PON PHY—the transmitter and receiver for the PON
- PON medium—the physical medium for the PON (ODN)

The PON system consists of the ONU, the OLT, and the network elements between. All components and functions need to be maintained by the operator, so use cases are defined to support operation of the elements.

The ONU sits at the customer premise and consists of components of interest to OOM, listed below. The ONU may comprise these components, but some of these components may not be included in all ONU, or they may be a part of the ONU but not separable for repair.

- Chassis
- Fan (when it exists)
- PIC (photonic integrated circuit) or transceiver
- MAC bridge
- Ethernet switch
- Software
- End-point device

The PON link system consists of the following components; there may be different flavors of these components that must be described for some use cases.

- Fiber
- Splice or connector
- Splice case
- Conduit
- Pole attachment

At the other end of the PON system is the OLT, comprising several components on the PON facing side, listed below.

- Chassis
- Central processing unit (CPU)
- Memory
- Fan (when it exists)
- Board or back plane
- PIC or transceiver
- Transmission convergence
- MAC bridge
- GEM (GPON encapsulation method) ports, sub-interfaces
- Allocation ID, LLID (logical link identifier)
- Software
- EMS (element management system)
- Controller
- Power supply

Each component needs to be monitored for state and function in some way, directly or indirectly (inferred by function of another component or system).

5.1.1 Fault and Failure

All faults and failures in the fiber and transponder optical interfaces and all failure modes should be covered by telemetry, i.e., no faults or failures should go undetected, be insufficiently localized, or lack protection if designed and available. These include all fiber, connector, splice, and optoelectronics issues affecting the optical signal significantly enough to impact the telemetry or service in some way. When the telemetry is impacted before service, this is an opportunity for proactivity, and all proactive opportunities should be identified and reported in useful ways.

A high-level list of failure modes and effects for a general PON architecture is given in Table 1.

Table 1 - Failure Modes and Effects on a General PON Network

Failure Mode	Cause	Class	Impact	Action(s)	Indicator
OLT					
HW	Var	Hardware—multiple/shock/degradation	Service failure	Replace	OLT heartbeat
SW	Var	Software—multiple/shock/degradation	Service failure	Restart	SW heartbeat
CPU	Utilization	Hardware—multiple/shock/degradation	Latency, jitter, failure	Reengineer	CPU utilization
Case	Open	Hardware—multiple/shock/degradation	Damage, service degradation		Case state
Power	Var	Hardware—shock/degradation	Service failure	Fix power	Power state/OLT heartbeat
Alarm	Software failure, logic failure	Software—shock/degradation	Alarm failure	Restart	Alarm state
PIC					
Tx loss	Degradation, aging, damage, alignment	Hardware—shock/degradation	Inadequate signal strength reaching the ONU, leading to degraded performance or service interruptions	Rehabilitate or replace	Tx level, Rx level
Rx loss	Degradation, aging, damage, alignment	Hardware—shock/degradation	Inadequate signal strength reaching the ONU, leading to degraded performance or service interruptions	Rehabilitate or replace	Tx level, Rx level
Tx timing problems					
Not silent when not in transmit					
HW	Aging, damage	Hardware—multiple	Service failure	Replace	PIC state
SW	Var	Software—multiple	Service failure	Restart	PIC state
Aging	Degradation, aging, damage, alignment	Hardware—degradation	Attenuation-data service degradation or failure	Replace	Tx level, Rx level
Fiber					
Break	Physical damage to the fiber optic cables due to accidents, digging, construction activities, or severe weather conditions	Hardware—shock	Loss of signal or data transmission between the OLT and ONUs	Rehabilitate or replace	Tx level, Rx level
Bend (micro, excessive)	Damage, access	Hardware—shock	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Pull	Damage, access	Hardware—shock	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Stress/strain	Damage, access	Hardware—shock	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Temperature var	Damage, access	Hardware—shock/degradation	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Aging/weathering	Damage, access	Hardware—degradation	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Rodent/bird	Damage, access	Hardware—shock	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Other attenuation	Damage, access	Hardware—multiple	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level

Failure Mode	Cause	Class	Impact	Action(s)	Indicator
Splitter					
Fail	Degradation, aging, damage, alignment	Hardware—multiple	Attenuation-data service degradation or failure	Replace	Tx level, Rx level
Reflection	Damage, access	Hardware—shock	Attenuation-data service degradation or failure	Replace	Tx level, Rx level
Incorrect split	Human	Hardware—shock	Attenuation-data service degradation or failure	Replace	Tx level, Rx level
Splice/Connector					
Loss	Degradation in optical signal strength due to fiber attenuation, connector losses, or poor quality of fiber splicing	Hardware—multiple	Inadequate signal strength reaching the ONU, leading to degraded performance or service interruptions	Rehabilitate	Tx level, Rx level
Reflection	Alignment, damage, access	Hardware—shock	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Quality	Degradation, aging, damage, alignment	Hardware—shock	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Loose	Degradation, aging, damage, alignment	Hardware—shock/degradation	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Dirty/contaminated	Degradation, aging, damage, alignment	Hardware—shock/degradation	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
Water/moisture	Degradation, aging, damage, alignment	Hardware—shock/degradation	Attenuation-data service degradation or failure	Rehabilitate	Tx level, Rx level
ONU					
HW	Var	Hardware—multiple	Service failure	Replace	ONU heartbeat
SW	Var	Software—multiple	Service degradation or failure	Restart	SW heartbeat
UNI port errors					
Tx loss	Degradation, aging, damage, alignment	Hardware—shock/degradation	Attenuation-data service degradation or failure	Replace	Tx level, Rx level
Rx loss	Degradation, aging, damage, alignment	Hardware—shock/degradation	Attenuation-data service degradation or failure	Replace	Tx level, Rx level
Aging	Degradation, aging, damage, alignment	Hardware—degradation	Attenuation-data service degradation or failure	Replace	Tx level, Rx level
Power	Var	Hardware—multiple	Service failure	Fix power	Power state/ONU heartbeat
Alarm	Software failure, logic failure	Software—multiple	Alarm failure	Restart	Alarm state
Alarm Agent					
SW	Software failure, logic failure	Software—multiple	Silent alarms	Restart	Alarm heartbeat
System					
Configuration	Human error, software failure, logic failure	Operations—multiple	Service degradation or failure	Correct configuration	
Wavelength mismatch	Human error, software failure, logic failure	Hardware/operations—multiple	Attenuation-data service degradation or failure	Correct configuration	

Failure Mode	Cause	Class	Impact	Action(s)	Indicator
Interference	Design	Hardware—shock/degradation	Attenuation-data service degradation or failure	Correct design	
Cross talk	Design	Hardware—shock/degradation	Attenuation-data service degradation or failure	Correct design	
Environmental extremes	Design	Hardware—shock/degradation	Service degradation or failure	Correct design	
High utilization/oversubscribe	Human error, software failure, logic failure	Operations—multiple	Latency, jitter, loss	Correct design	

5.2 Aggregation Network

This part of the architecture connects the access node to the next level toward the core network (e.g., metro).

- Eth MAC—Ethernet MAC as used in the Ethernet aggregation function
- Eth PHY—the transmitter and receiver for the Ethernet aggregation function
- Eth medium—the physical medium (the "wire") for the Ethernet aggregation function

There may be zero or more instances of the Ethernet aggregation function in the access network, including the switching function. Other connecting technologies such as fixed wireless backhaul are excluded unless a use case dictates otherwise.

The aggregation/backhaul or Ethernet section of the access network includes the OLT portion that faces the switch over the aggregation network, the fiber connecting to the switch, and the switch that terminates the access network.

The OLT portion of the aggregation network consists of the following parts.

- Board or back plane
- PIC or transceiver
- Ethernet interface
- Link aggregation (LAG)

The aggregation link system consists of the following components; there may be different specific details about these components that must be described for some use cases.

- Fiber
- Splice
- Splice case
- Conduit

The aggregation link system may terminate at a network switch, router, or similar device with appropriate functions.

In some instances, there may be OTN functions or a hub. At the very least, the following components are at the termination device.

- Chassis
- Board or back plane
- PIC or transceiver
- L2/L3 functions

5.3 Other Components

The overall architecture will consist of more components beyond the PON and aggregation portions, such as those listed below. For example, there may be subsystems that become relevant to the use cases or are sources of important information.

- Subscriber Management
- Traffic Management
- Fiber Management
- Tools for troubleshooting and provisioning
- Fiber Infrastructure Management

- Tools to track physical plant components and connections
- Out of Band Optical Medium Measurement System
- Performs measurements on the physical medium and collects relevant metrics (e.g., OTDR measurements, power meter, or spectrum analyzer)
- Connected to the Ethernet medium and the PON medium

5.4 Interfaces

For OOM, each layer in the model represents a set of metrics. Each interface in the model represents a point at which those metrics may be measured.

5.4.1 Reference Point V'

This reference point is the boundary between aggregation and the core network. It provides traffic aggregation, class of service distinction, and user isolation and traceability.

- Ethernet MAC
- Ethernet PHY—port, transceiver
- Ethernet medium—PHY connector
- Ethernet switch (opt.)—hardware, software, inventory

5.4.2 Reference Point V

This reference point is the interface between the access node and the aggregation network.

- Ethernet MAC
- Ethernet PHY—port, transceiver
- Ethernet medium—PHY connector
- Ethernet switch (opt.)—hardware, software, inventory

5.4.3 Reference Point S/R

- PON MAC
- PON PHY—port, transceiver
- PON medium—PHY connector
- Device (ONU/OLT)—hardware, software, inventory
- OTDR (optical time domain reflectometer) measurement
- Power loss measurement

5.4.4 Reference Point R/S

- PON MAC
- PON PHY—port, transceiver
- PON medium—PHY connector
- Device (ONU/OLT)—hardware, software, inventory
- OTDR measurement
- Power loss measurement

5.4.5 Reference Point U

This reference point is the subscriber-facing interface at the access node (ONU user port). At this reference point, the interface is exposed if it is not an integrated gateway; otherwise, it is internal. It is the same interface as Ethernet V or V' with the addition that it may be electrical or optical.

5.5 Fault, Performance, and Network Operations Telemetry

Faults, failures, and service assurance are supported with a tools stack that extends beyond the network. It includes element management systems, network management systems, data lakes, data protocols, tools, methods, and processes to support network operations and service assurance. A simplified view of this architecture is provided in Table 2, Table 3, and Table 4.

In the following three figures, the leftmost column is the row label and the other columns are use case sets, identified in the top row. The scope of the use case is set by the network layer (Ethernet WAN, PON, and Ethernet LAN) in the bottom row. The device function is named in the row above that (BNG function [can be virtual], OLT, ONU, and RG for residential gateway), then the telemetry and business application.

Table 2 - Current Telemetry Stack with Existing Telemetry Sources

Use Cases	Configuration	Fault	Service	Monitoring	Assurance
Business applications	NMS	EMS	Data Lake/DB	Data broker	Applications
Telemetry protocol	CWMP	SNMP	IPDR (DPoE)	IPFIX	
Device functions	BNG	OLT	ONU	RG	
Networks	Ethernet WAN	PON	Ethernet LAN		

Table 3 - Future Telemetry Stack with Expected Telemetry Sources

Use Cases	Configuration	Fault	Service	Monitoring	Assurance
Business applications	NMS	EMS	Data Lake/DB	Data broker	Applications
Telemetry protocol	IPFIX	gNMI	Kafka	eBPF -> Open Telemetry	Netconf/YANG -> USP
Device functions	BNG	OLT	ONU	RG	
Networks	Ethernet WAN	PON	Ethernet LAN		

Cable operators and vendors differ on their preferred telemetry approach—gNMI and gRPC, Kafka, or Netconf/YANG. eBPF is another option. IPFIX exists today, but some vendors expect it will continue to serve telemetry effectively.

Cable operators have expressed the need to align on telemetry to reduce the burden of data management. Narrowing the options for telemetry protocols may help this effort, but eliminating specific network and element management systems (NMS and EMS) or pushing the alignment functions to lower levels will likely be necessary to enable data broker and data services functions like those created for DOCSIS networks and those currently being built. What remains for NMS and EMS can be virtualized (vNMS and vEMS). Table 4 shows such a telemetry stack, with vNMS, vEMS, and layers for data broker and data services functions.

Table 4 - Telemetry Stack as Envisioned by Cable Operators, Including Common Data Broker and Data Services Functions and Eliminating a Separate NMS and EMS

This view unifies the network operations tools and business functions for streamlined operations.

Use Cases	Configuration	Fault	Service	Monitoring	Assurance
Business applications	vNMS	vEMS	Data Lake/DB Data services (API) Data broker (CCF)	Applications	
Telemetry protocol	IPFIX	gNMI	Kafka	eBPF -> Open Telemetry	Netconf/YANG -> USP
Device functions	BNG	OLT	ONU	RG	CM -> CMTS
Networks	Ethernet WAN	PON	Ethernet LAN		

Telemetry in any form is collected to satiate a need for information. These needs cover a number of network operator processes including fault and failure management, service assurance, planning and engineering, network management, service management, operations management, vendor management, and reporting. These needs are described as use cases.

Telemetry in a request form can be a query or a test. A query can be delivered in an immediate response, after any needed compilation for the request, unless requiring a first initial step to start collecting. Collection of the data does not change the network conditions. A test is initiated by the request, and the response is provided after the test completes, which may take more time than compiling a query. Telemetry obtained in a subscription form is delivered in the advertised form and cadence.

Telemetry provides information, but for the information to be understood, a model to convert the information is often required. This conversion takes place after the transformation of compressed telemetry into useful units of measurement, as conversion helps with interpretation. Some conversions are as simple as a plot for human readability or a table. The main use of this information, however, is in decision making, which usually requires conversion to a statistic, i.e., a measure of performance. Multiple measures of performance can be combined and used in a different model to provide a measure of effectiveness. That overall concept, as well as the various models and outputs, may be applied to nearly any use case that telemetry can help address.

As a result, to keep the nomenclature clear for this report, the first telemetry discussed is from the network components and systems (including EMS and NMS), delivered into a data repository or data broker such as a common collection framework (CCF). This CCF manages the collection and delivery of telemetry from various sources. Applications that serve use cases can interface with the CCF for telemetry, making requests for data from the network. The data in the CCF are held for a time, but the CCF is not intended to be a data lake for holding data over long periods of time. Instead, any archive for the data would appear as an application interfacing the CCF. For example, ProOps was created to be a general application framework that serves many use cases including its main use case of proactive network maintenance (PNM). ProOps can serve as an agentic architecture with data lake capabilities for other applications and also host applications, helping to manage the polling cadence and logic that leads to cadence changes, requesting new telemetry, or even interfacing with external data sources to serve use cases. Note that there is some application-level functionality within EMS and NMS, so those functions are shown in Table 4 as virtualized: vEMS and vNMS.

Within the applications layer is the transition from telemetry to the information needed to support use cases. This transition involves data models, statistics, and various forms of logic that transform data into actionable information (ProOps). As the raw encoded data are collected, translation may be necessary to turn it into useful information, or at least to organize it into a data object. Additional logic may be needed to calculate statistics, rules for archiving, purging, or otherwise managing the data in raw or decoded form. There will also be more complicated models and logic that supports use cases in unified ways, including the information that directly feeds KPIs (key performance indicators), enables prioritization of work, and supports decision making for maintenance and proactive operations.

There are various models for acquiring data in support of use cases. In this technical report, we categorize the acquisition methods into the following method categories.

- Alarm/Trigger—An alarm requires control of the alarm logic and an ability to confirm an alarm and the information from which the alarm is based, via polling.
- Poll—Frequent polling is required. If polling a log or other meta information, control of the triggering is required.
- Heartbeat/Stream—A heartbeat or stream of telemetry is delivered on a controlled or reported cadence, and in the case of triggered telemetry, the ability to control the triggering logic is also required. Polling is also needed for the same reasons it is required for alarms.
- Analyze/Meter—Network data can be acquired by attaching a device for data collection or maintenance, such as an OTDR or field meter.

Each of these methods

- can be based on tests or queries,
- provides different fault coverage, and
- can require subscription or authentication.

The use case categories that follow, by their nature, suggest which method is favored or needed most, though all four could be useful in use cases in all categories.

- NOC/NMS—alarm, poll, heartbeat
- Birth certificate—poll, analyze
- Repair—poll, analyze (reactive: alarm, heartbeat)
- Service delivery (KPIs)—poll, alarm, heartbeat

Several telemetry protocols are mentioned in Table 2, Table 3, and Table 4. Note that the number of protocols listed increases; this trend is counter to the goals of the OOM working group and will need to be addressed. When a new protocol emerges as a better option, it will need to replace at least one existing protocol. To punctuate the issue, see the number of protocols identified for various parts of the XGS-PON architecture in Table 5.

Table 5 - Common Configuration and Management Protocols for XGS-PON Deployments

	Configuration Management	Status Monitoring (Req/Resp)	Performance Monitoring (Bulk)	Fault Management (Async Events)
Management of the OLT	OLT CLI, EMS GUI, Netconf	OLT CLI, EMS GUI, OLT Netconf, OLT/EMS APIs	IPFIX, IPDR, Message bus topic	Netconf Event, Message bus topic, EMS GUI
Management of the ONU	OLT CLI, EMS GUI, OLT Netconf, OLT/EMS APIs Above all feed into OMCI ME Set operations	OLT CLI, EMS GUI, OLT Netconf, OLT/EMS APIs Above all feed into OMCI ME Get Req/Resp operations	OMCI Layer stats from ME Get Req/Resp or ME Periodic Reporting feed into bulk reports from OLT	OMCI Layer Alarms, TCAs, and AVC's feed into Async Events from OLT
Management of the eRouter/eDVA	CWMP, USP (using [TR-181] and [TR-104] data models), eDVA Config File	CWMP, USP (using [TR-181] and [TR-104] data models)	HTTP or MQTT to bulk data collector	CWMP Inform, USP Notify

6 USE CASES BY CATEGORY

In the context of OOM, a use case consists of a description of how operators meet a particular goal relevant to the operation of optical networks. It can be used to establish requirements.

This report describes the system from the use case perspective. The use case actors will hold numerous roles with the network operator—technicians, engineers, and tools or other systems used to accomplish the use case goal.

The scenario/procedures are not necessary for all use cases; some can be aligned to the telemetry necessary to support the use case without them. When the procedures are needed, they will be written as generally as possible to enable broad applicability.

Most of the use cases in this report will explain a successful scenario. Many use cases will describe failure or fault scenarios; the outcome will be successful and in that context the use case will describe a successful scenario for fault management and/or failure repair or recovery. Alternative paths, possibly failure scenarios, may be defined, such as a use case in which a fault is not alarmed but leads to a failure that may not be discoverable if telemetry are not suitable. A lack of sufficient information to support the success path for a use case is an important reason for describing the failure path, as motivation for an improved telemetry source.

For all use cases, the actors are assumed to be defined as needed. In most cases, they are represented by the following categories.

- Engineers
- Technicians
- Field technicians
- Data lakes, databases, and servers
- Tools

This report defines four use case categories:

1. Network operations center (NOC) and network management system (NMS)—monitoring state, function, performance, and capacity of network components, subsystems, and their functions
2. Birth certificates—snapshots of the provisioned state of network sections and customer connections
3. Repair—truck rolls, i.e., all repair and maintenance activities, including proactive, preventive, and reactive
4. Service delivery (KPIs)—all other functions that assure service to customers and management targets. This category will include provisioning, management KPIs, decision support, planning and engineering use cases, and more.

Other use case categories may be defined in revisions to this report or other documents aligned with the goals of the OOM working group.

6.1 NOC and NMS: Monitoring State, Function, Performance and Capacity of Network Components, Subsystems, and Their Functions

NOC and NMS functions for PON systems involve end-point monitoring and performance data about the connections as well as data on upper layer state, performance, and capacity. Generally, when using an OSI layer organization, the high-level categories of what to monitor are as follows.

6.1.1 L1: Layer 1 Use Cases

1. ONU state monitoring, including a dying gasp alert
2. OLT state monitoring
3. Switch state monitoring
4. PIC or transponder state monitoring (pluggable and optical sub-assembly form factors for examples)

5. Link state monitoring—degradation and variability
6. Protocol health—though protocol specific, it involves information about encoding failures, packet failures, etc.

6.1.2 BNG Use Cases

All connections on a PON network aggregate at a central broadband network gateway (BNG) element (Figure 5). Therefore, monitoring the BNG router's performance is crucial. To monitor BNG traffic, the operator may use the BNG's built-in capabilities to track individual residential gateways (RGs).

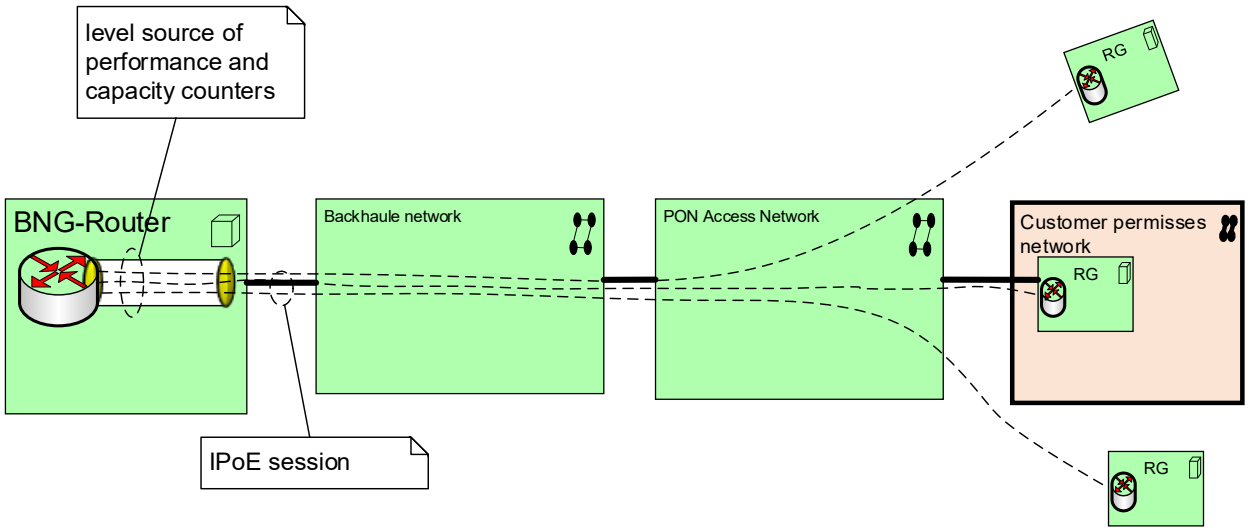


Figure 5 - FTTP-XGSPON Connection Model from RG to BNG

6.1.2.1 Traffic Monitoring on the BNG

The BNG router plays a crucial role in managing subscriber access and traffic. Its key functions are listed below.

Subscriber Access Management

- Authentication and authorization—The BNG uses DHCP-based authentication to authenticate subscribers, verifies subscriber credentials, and authorizes access to specific services based on their subscriptions.
- IP address assignment—The BNG, often acting as a DHCP server or proxy, assigns IP addresses to subscriber devices connected to the network.
- Session management—The BNG establishes and manages individual subscriber sessions, tracking their online status and resource usage.

Traffic Aggregation and Routing

- Aggregation—The BNG aggregates traffic from multiple subscribers connected to the network through the OLT.
- Routing—The BNG routes this aggregated traffic towards the service provider's core network and the Internet. It acts as the gateway between the access network and the provider's metro or core network.

Service Delivery and Policy Enforcement

- Quality of service (QoS)—The BNG can enforce QoS policies to prioritize certain types of traffic (e.g., VoIP, video streaming) and ensure a consistent user experience.
- Service differentiation—The BNG enables service providers to offer different service tiers and packages by applying specific policies and configurations to individual subscribers or groups of subscribers.

Network Security

- Security—The BNG can implement security measures, such as traffic filtering and access control lists, to protect the network and subscribers from potential threats.

6.1.2.2 In the Internet Protocol Over Ethernet (IPoE) Model

The BNG needs to be able to identify subscribers based on information provided by the OLT (e.g., circuit ID, MAC address) to apply the correct policies and configurations.

The BNG router is a critical component in an FTTP network, responsible for managing subscriber access, aggregating traffic, routing it to the provider's network, and enforcing service policies. It acts as the central point for controlling and managing broadband services delivered over the access network. Within the BNG, performance and capacity counters can be reported.

6.1.2.3 BNG Counters

The BNG counters can be divided on interface and subscriber management.

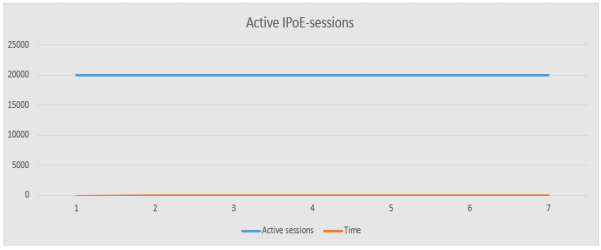
Interface utilization measures the bandwidth utilization on the interfaces to the OLT backhaul network, which will help identify potential bottlenecks.

- Packets in/out—measures the number of packets entering and leaving the BNG
- Bytes in/out—tracks the volume of data being processed by the BNG
- Packet loss—monitors the number of packets dropped by the BNG because of congestion or errors
- Retransmissions—tracks the number of packets that need to be retransmitted, indicating potential
- DHCP requests/responses—tracks the number of DHCP requests and responses processed by the BNG
- Active sessions—counts the number of currently active subscriber sessions, providing an overview of the BNG's load
- Authentication success/failures—tracks the number of successful and failed authentication attempts, which can help identify authentication issues or security threats

These counters can also be reported by using streaming telemetry counters in the BNG routers.

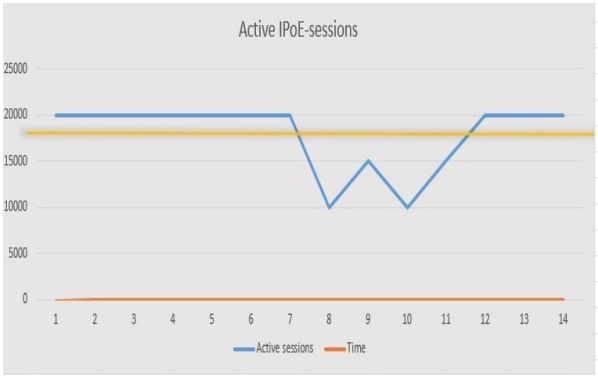
In the example above, each ONU is tracked, along with its associated RG, MAC address, and session status. The core concept involves periodically collecting this information from the BNG and storing it in a data lake for service assurance purposes and more. These data facilitate the creation of a baseline graph. When a disruption occurs in any element between the RG and the BNG, sessions will terminate, causing a decrease in the number of established sessions. Based on a pre-defined threshold for terminated sessions, an event is triggered and sent to the fault management system, which generates a ticket for an engineer to address the network impairment. The scenarios below illustrate a network block outage use case and the steps applicable to this incident management process.

Scenario 1: Normal Operation (Birth Certificate)



In this scenario, both the on-network and off-network elements in the end-to-end chain are fully operational, with no reported issues. At this point, there are a total of 20,000 active connected users. This state is the "birth certificate" for the situation at time zero.

Scenario 2: Network Outage Detection



In this scenario, at time 7, an outage is detected somewhere within the network, in either the ON-NET or OFF-NET segments. The BNG router identifies this outage and reports a drop in the number of active sessions—up to 10,000 sessions have become inactive, i.e., 10,000 customers are experiencing network issues as a result of the outage.

6.1.3 L2/3: Layer 2 and Layer 3 Use Cases

1. PON/ONU capacity and utilization—rate and service flow (CIR, EIR, PIR)
2. Ethernet backhaul capacity and utilization
3. MAC bridge capacity and utilization
4. Session flow capacity and utilization
5. ONU software state
6. OLT software state
7. Switch software state
8. Ethernet state
9. Routing and switching tables

Troubleshooting in PON systems usually occurs through state and performance monitoring, then external tools are used to conduct fault and failure management steps: identify, localize, and mitigate or remove.

Use cases, however, require a more detailed alignment of monitoring to the telemetry that supports NOC and NMS functions.

6.1.4 NOC and NMS General Monitoring Use Cases

Monitoring a PON network requires several basic use cases to be met, all around monitoring for function and capacity. That includes the assurance that a function is performing as intended and that there is sufficient capacity for assured service without action necessary to relieve a capacity limitation. Based on the OSI model and sub-functions of the layers, the following breakdown can be applied.

First, a component must be defined. A component is not limited to a physical element but may be a field replaceable unit. However, any field replaceable unit may comprise software and functions that may be distinguishable and therefore identifiable as separate components, and vice versa. Therefore, it is important to identify all components, subsystems, and functions (which are a specific class of component). Subsystems may also comprise components and be managed as components themselves along with the components they comprise.

Each identifiable component must be monitored for each feature, if the feature exists.

1. Addressability—Can it be communicated with? For example, via OMCI layer connectivity for communications.

2. Identity—Does it have a discoverable, unique identification? That is, a serial number (MAC address optional) or ONU ID (ephemeral, session based). Active field replaceable units need to be remotely discoverable or identifiable by the serial number and OEM model number. Regardless of whether the serial number or MAC is used, the device must have at least an ephemeral MAC, and this identity must bind to a customer account.
3. Functional state (hardware, software) + dying gasp—What is the functional state of the hardware, hardware components, software, and software functions? Can it send a dying gasp message when warranted? See above.
4. Network participation permission—Has it authenticated with the network? This is a gap needing further development, but operators must be able to determine whether a network element should be attached at a given location before the attachment is made.
5. Management function—Can it communicate and be managed?
6. Connectivity—Is it connected to the service network? Light, FEC (forward error correction), and Ethernet statistics provide this via a combination of information, as well as the operational state of the element.
7. Services—What services does it support? That is, the service flow parameters.
8. Traffic bearers—Which defined interfaces exist and can carry traffic? Includes physical and virtual interfaces.
9. Domain—What is its function in the network, and what is the scope of what it can communicate with or have control or domain over?
10. Functions—What network functions does it support? This can include services, but it will always include OSI layer functions that enable services.
11. Physical location—Such as GIS, slot and port, etc. Topology is proprietary and architecture specific.

Each function of a component must be monitored for functional state and performance; those with limited capacity must also be monitored for capacity.

Some functions are provided by a subsystem of the network, which requires additional monitoring considerations of function, capacity, and performance of multiple entities including physical, software, and virtual components. In these cases, the intended function of the subsystem dictates the breakdown of the components, functions, capacities, and performance that must be monitored.

The PON connection can be considered as a subsystem of the overall PON system with the PIC or transponder as the end points. The architecture in Figure 4 shows this system as PON medium (ODN), PON PHY, and PON MAC touching the Service MAC. Note that these end points function as a system, in part, with their own local functions as well, and it is convenient to discuss them as a system with respect to the functionality.

PON end-point monitoring (transponder, PIC, transceiver, pluggable, and optical sub-assembly form factors) includes the following.

1. Addressability—unique address of the end point and confirmation of response
2. Identity—unique identity (MAC or serial number (SN))
3. Functional state (hardware, software) + dying gasp—list of and state of the hardware, hardware components, software, and software functions and status for dying gasp messages, including ability to send them.
4. Network participation permission—authentication state
5. Management function—management state and capabilities
6. Services—list of services supported and state of the support
7. Connectivity—connectivity details for service
8. Transmit-receive headroom—amount of transmit power, receive power, and electrical power consumption
    a. Power consumption
    b. Transmit levels

   c. Receive levels
   d. Link budget

9. Frames—details of all frames
   a. Size/fragment
   b. Lost/dropped
   c. Latency/jitter
   d. Drops

10. Error correction—status and function and statistics of error corrections
   a. FEC, HEC, CRC
   b. Error limits – capabilities of the system and where functionality is stressed, etc.

11. Encryption capabilities and state—encryption capabilities, state, and function

12. Service path, adaptation (GEM PID, LLID)—Services require the function of several communication functions, so their states need to be known, and any limits of these counts need to be reported.

13. Bandwidth—amount of link capacity consumed and allocated, limit on full capacity, and any divisions of the capacity and those limits (count of divisions and capacity of each division, e.g., flow)
   a. Allocation
   b. Capability
   c. Usage
   d. Per user/flow

14. Operations, administration, and management (OAM) reporting—management status and reporting
   a. Status
   b. Capabilities

15. Ranging/registration—logical and physical connectivity status
   a. State
   b. Logs

16. Collision management—collision event logging, reporting, notification, etc.

17. Data link control—data link status and health, logical link control status and performance
   a. Status
   b. Performance

18. MAC control—MAC layer capacity, status, performance
   a. Status
   b. Performance
   c. MAC bridge capacity

19. Physical data translation—symbol encoding, transmission, reception and decoding, status and performance
   a. Status
   b. Performance

20. Physical monitoring—physical connection layer status and performance, mostly hardware status and performance
   a. Status
   b. Performance

21. Association/domain—which customers, end points, virtual ports, etc., are associated and the full scope of entities this component associates with, has control over, etc.

From this way of organizing components and functions, the ONU and OLT monitoring requirements are simplified to mostly state knowledge, i.e., the component basic monitoring parts listed above.

The use cases that the NOC and NMS function supports include triggering maintenance to avoid downtime, fixing the network in cases of failure, identifying capacity issues to be addressed by planning and engineering, and assuring service standards are met, among others.

Likewise, on the aggregation network, very similar monitoring is required. The link system is very much the same, and the end points are monitored as described above. The lists above are general and apply to that system as well, with extensions for topology. For ring systems, details about the protection are added and will be defined as needed. For point-to-point, the point-to-multipoint solution applies.

NOTE: Alarms should be reported within 15 seconds of being triggered. Less ephemeral state changes that are informative but not service impacting may be reported within 1 minute, 5 minutes, or 10 minutes as appropriate.

Octet counts for usage are reportable every 15 seconds from switches, BNGs, and ONTs. ONU telemetry and alarms are reportable every 10 seconds.

6.1.5 Use Case: Component, Subsystem, and System Analysis

Telemetry provides either a unique serial number (SN) or a unique identifier that can be used to look up the SN (such as a unique MAC address with a lookup table provided by the manufacturer, vendor, or supplier). If the SN is known, all other information can be discovered though lookup tables.

A particular network element may utilize parts or components from different batches with unchanged SNs. However, some batches of components have reliability issues that need to be identified, tracked, and managed out of the network, and to do this, operators need to know which component batches and source manufacturers (and at times models or part numbers) are used in each SN network element, subsystem, or field replaceable unit. Without the knowledge of these differences in components at the network element level, the burden of discovery is higher on the operator analyst who must use statistics to identify whether there is evidence of different hazard functions among the population, then work manually with manufacturers to determine if there is a warranty, batch problem, or other cause to mitigate. The analysis is simplified and uncertainty is reduced when knowledge of different batches or suppliers is applied to components of network elements. Therefore, the operator needs to know whether a given SN of a network element comprises components from the various potential batches of components that may have been used.

Vendors often maintain bills of materials (BoMs) for the network element that indicate which batch each component came from and the manufacturer of the component batch by SN. The vendor should provide the details by SN so that the operator analyst can determine the batch differences when analyzing the data to identify cause and finding hazard functions for components and network elements. Providing this information ahead of time allows pre-batching of network elements by SN groups according to batch differences of concern.

To further simplify the analyst's work, and to facilitate automation, certain information needs to be contained in or associated with each SN: manufacturer, date, and serial part within that date range. With the information about the components comprised by the network element, the operator analyst can trace back to the information needed.

Ideally, an SN would be sufficient for the analyst to do this needed work, but packing all these details into a simple SN with its limited field would be a challenge. Instead, having manufacturer, date, and serial part would be sufficient to look up other details such as the location of manufacture (as provided) and the component details (as described above via lookup).

Further, it would simplify the analyst's work if all SNs were in the same format. Such is not required as long as the valid information is encoded, but it would reduce the need to decode the SN into its parts. The analyst would still need to look up information to determine the additional detail, so the advantage of a common SN format is small, but it is nevertheless recommended that manufacturers follow [SCTE 292] from the node toward the core. (For simplicity, it may be applied to the ONU as well.) Each network component type and manufacturer would then need to guarantee unique SNs and provide the lookup tables that enable the analyst to obtain the data needed.

Additionally, the SNs must be discoverable remotely, via telemetry. If there is risk of SN overlap, there needs to be a method to avoid it.

Based on the rules for network equipment SNs dictated by current standards, changes cannot be made to existing network element SNs.

The process to employ a common SN can be mapped out as follows.

- SN ↔ manufacturer, date, serial part ↔ manufacturer location
- SN ↔ manufacturer, date, serial part ↔ component BOM details (component, manufacturer, batch, date, serial component if available)

6.1.6 Use Case: Transponder Health Monitoring and Fiber Link Monitoring for Degradation

The PON and ODN systems must be monitored for health, in part to assure that any degradation is addressed in a timely manner. In the future, the OOM working group will develop proactive and prognostic capabilities for PON systems based on currently available telemetry, with the intent to prove the need for telemetry and tools to support more advanced and embedded proactive maintenance and prognostics.

6.1.6.1 Description

Transponder (PIC) health monitoring is important for avoiding outages from large scales down to single customer service failures. Transponders can degrade over time, so it is important to determine if a degradation in the signal is due to transponder degradation or a fiber condition. The use case is to monitor the system for degradation then determine the cause. In the case of transponder degradation, additional data can reveal the (probabilistic) timing for replacement before failure; this is known as prognostics and health management (PHM).

6.1.6.1.1 Fault and Failure

Identifying and removing transponders with degrading performance before they fail is the primary target. Fiber degradation is secondary, but it is covered by this use case in part. Abrupt failures may also be identified.

6.1.6.2 Scenarios

1. Collect power consumption, Tx, and Rx data from each PIC. Weekly or daily collection may be sufficient for monitoring PIC degradation. Variability in the system would need more frequent collection. Temperature data may also be needed.
2. Identify the PIC on each system end point.
3. Calculate statistics as needed (eliminate cyclic effects).
4. Report statistics to the decision system.

6.1.6.3 Information and Telemetry

The following information elements are required to support this use case.

- Tx and Rx light levels
- Power levels (electrical)
- Temperature
- PIC identification
- PIC association to chassis and network element type

6.1.6.3.1 Source, Scope, Requirements, Methods, Telemetry, Endpoints

Capable PICs report data to capable chassis and management systems. See the data reporting architecture.

NOTE: Unification of this use case across PICs requires that the PICs in the systems use the same units and report the data in the same manner and format.

Unification of S/N calculation methodologies is also important. It must be done across different laser technologies or lots, and some calibration or agreement of laser bias current must be defined.

6.1.7 Use Case: Node Module Monitoring

Text in this section has been reproduced with permission from [Wichman 2024] and has been formatted to adhere to CableLabs publication style.

Today's field hardware is becoming more advanced and can be impacted by environmental factors. Traditional node housings now contain a variety of advanced modules that have capabilities of delivering symmetrical gigabit speed to customers. To deliver reliable bandwidth, all components and modules in the node must be installed correctly.

Incorrectly installed components can cause modules to overheat, causing reduced life of the module, reset, reboot or even complete sudden failure. With advanced analysis of telemetry, we can detect loose or improperly installed modules well ahead of customer impacting events. This new detection method will improve the customer experience, reduce outages, and extend the service life of field installed modules.

Advanced consistent telemetry of all temperature sensors in a node tells a complete story that one sensor alone cannot reveal. Today's node modules are capable of reporting individual temperature readings and, in some cases, multiple temperatures from components, like small form-factor pluggables (SFPs) and chips. Individually, we can tell if a module or component is overheating, but this leaves out the impact of external temperature the node housing is experiencing due to weather or the node location. When individual temperature readings are combined into a complete picture, we show in [Wichman 2024] how to remotely determine if the node is overheating because of external forces or if individual modules and components are the cause of an overheated reading.

6.1.7.1 Faults Resolved and Their Impact

Text in this section has been reproduced with permission from [Wichman 2024] and has been formatted to adhere to CableLabs publication style. It has also been extended slightly for use in the context of PON.

It is important for operators to monitor and maintain individual module temperatures. Adverse impacts can degrade or interrupt service that may not be easily identified. Each module can only be identified as a cause of the impact if they are monitored as part of a wholistic node environment logic.

Impacts of Overheat and Loose Modules

- SFP resets
- SFP frame errors
- Reduced signal quality
- Remote Phy (physical layer) device (RPD) and other node type reboots
- RPD or node offline, failure to bootup
- Shortened life span of components
- Sudden complete failure of the module

Without thermal information and logic, field teams have a hard time understanding the cause of a problem or why the repair fixes the service call. With the right information, not only can techs quickly resolve the issue, but also fix the problem before these conditions occur.

6.1.7.2 Scenario, Process

1. Collect temperature data from each device and the chassis or enclosure. Weekly or daily collection may be sufficient for monitoring, but it should also be triggered by any maintenance or installation activity in the area. Variability in the system would need more frequent collection. Note the ability to report temperature data for each component in the system is required.
2. Identify the components on each system end point (node, OLT, ONU, switch, etc.).
3. Calculate statistics as needed (eliminate cyclic effects).
4. Report statistics to the decision system.

6.1.7.3 Information Required

- External temperature of the node or chassis
- PIC temperature
- Card (e.g., amplifier, processor) temperature
- PIC or card identification

6.1.7.4 Laser Drift

Telemetry on the transmitted and received frequencies is collected to obtain additional information about laser behavior for maintenance purposes.

When the received frequency is near the edge of the acceptable range, a test meter will indicate that the received levels are good but that the signal may not be easy for the detector to receive and demodulate. In these cases, the cause of the issues is not determinable, so the technician will often just swap the affected pluggable optical transceiver or SFP without identifying the problem and why it occurred. Even if the receive levels are good, the signal may fail in some applications because the center frequency is off target—once the light goes through the filter, the receiver does not get the right light level.

One way to determine causes of poor performance, properly troubleshoot, and even proactively identify potential issues is to check laser drift. Adding drift detection to maintenance processes allows the technician to address the right laser and swap the right one out without troubleshooting. It also eliminates dirty fiber connectors or bends as the cause.

Drift caused by temperature, which is usually part of the cause, does not improve over time, so it is important to identify the affected transceiver or SFP and remove it from the network.

This use case applies to any on-off keying (OOK) optical communication.

To identify drift, the operator needs to take regular measurements of the received frequency of each transceiver or SFP and compare them to the range of the receiver. The following information must be gathered.

- A center frequency measurement at the receiver side should be obtainable at least once a minute.
- Though it may be sufficient to monitor the center frequency of the received signal (to compare also to the specified), it will be better to collect the power level over frequencies over the band to analyze the spread.

6.2 Birth Certificates: Snapshot State

Using birth certificates to define and confirm capabilities must be done at various network segments and at different phases of deployment. Confirmation can be achieved in multiple ways, including: what is the design, is the design sufficient, is the design met, is the deployment as designed, is the configuration as designed, and is the service what it is designed to be? Some specific use cases and uses include the following.

- Physical outside plant certification—install system quality; include fiber distance and ODN details: attenuation at each network access point (NAP) port and physical correlation between OLT port, ODN port, and NAP chain.
- Network certification, end-to-end certification—install ONU and customer service quality: OLT to BNG, BNG to core, service platforms, and service resources.
- PON port move management—When transitioning customers to new ports, collect new birth certificate details and update records.
- PON line assignment
- Provisioning and repair qualification

Table 6 organizes some of the birth certificate information that needs to be collected.

Table 6 - Organization of High-Level Birth Certificate Information

Certificates	OLT	PON	Drop	Install
Presence	OLT-ID	OLT port ID, location	PON-ID, Address	ONU-ID
Quality	Checklist	OTDR report	OTDR report	RX, tests
Initial values	Transmit power level	Return loss, distance	Return loss, distance	RX, TX, bias, test results

The main idea of a birth certificate is to quantify multiple relevant data elements that describe network and service conditions during various delivery scenarios (first installation, trouble call, change of address, etc.) for business operations and decisions.

Several decisions are involved.

- Allow the administrative process of the service order and/or work order to flow and control end-status, i.e., when the provisioning does not work, capture the firmware version and optical parameters.
- Move forward with the installation and delivery of the customer's services or stop and check potential faulty parameters (depending on the outcome and messages of the involved platforms).
- Trigger technical support processes.
- Involve the needed resources/groups (Engineering, Tech Support, IT, Operations, etc.).
- Replace equipment.
- Wait for the resolution or re-schedule the installation.

6.2.1 Use Case: New FTTP Coverage, Physical Outside Plant Certification

General Certification Process

- OTDR tests on fiber optic cables before installation—Confirm that the fiber optic reels are in optimal operating conditions before sending them to the contractor.
- OTDR tests on fiber optic cables after installation—Ensure that the fiber optic cables have not suffered any damage during the installation process performed by the contractor.
- Fiber optic splices—Validate the correct execution of fiber optic splicing according to the operator's optical testing protocol.
- OTDR bidirectional backscatter tests—Perform optical tests on the feeder and sub-feeder, ensuring that the passive components of the network comply with the permissible losses according to the operator's optical testing protocol and standards.
- HUB-ODN correspondence tests—Validate that each of the strands assigned to the ODNs matches according to the fusion schematic plan sent by the design team (ODF vs. ODN).
- Optical power measurement in ODNs—Perform optical power measurements on each port of the ODNs to validate that they adhere to the network's optical design.
- ODN-NAPs correspondence tests—Validate that each ODN port matches the nomenclature of the NAPs' cascades according to the plan sent by the design team. Finally, the color flag type identifiers (or alternate identifiers) are placed on each cable that feeds the NAPs' cascades.
- Optical power measurement in the NAPs—Perform optical power measurement on all NAPs to validate that they are in accordance with the losses issued in the optical design.

Records of these results are captured for future use including troubleshooting.

6.2.1.1 Attenuation Measurement on Each NAP Port: Examples

Field measurements on each NAP port must be captured and should be within ±1 dB of the theoretical value estimated for the OSP design.

Table 7 - OSP Technical Memory Example

OLT	OLT Port	Tx OLT Power (dBm)	OSP Long. (mts)	NAP/DP	OSP Theoretical Attenuation (dB)	NAP Theoretical Rx (dBm)	NAP Measurement Rx (dBm)[1]	OSP Attenuation (dB)
OLTXX	1-1-1			NAP01			Must be ±1 dBm theoretical	Must be ±1 dB theoretical
OLTXX	1-1-2			NAP02			Must be ±1 dBm theoretical	Must be ±1 dB theoretical

OLT	OLT Port	Tx OLT Power (dBm)	OSP Long. (mts)	NAP/DP	OSP Theoretical Attenuation (dB)	NAP Theoretical Rx (dBm)	NAP Measurement Rx (dBm)[1]	OSP Attenuation (dB)
OLTXX	1-1-3			NAP03			Must be ±1 dBm theoretical	Must be ±1 dB theoretical
OLTXX	1-1-4			NAP04			Must be ±1 dBm theoretical	Must be ±1 dB theoretical
OLTXX	1-1-5			NAP05			Must be ±1 dBm theoretical	Must be ±1 dB theoretical
OLTXX	1-N			NAPxx			Must be ±1 dBm theoretical	Must be ±1 dB theoretical
[1] Rx power measurement (dBm) between NAP port and OLT (operator specific choice for measurement target).								

Table 8 - Physical Correlation Between OLT Port, ODN Port, and NAP Chain and Optical Fiber Assignment Between OLT, ODN, and NAP

HUB	OLT	TGPON	NN	Area FTTP	ODF	ODF Pos.	Troncal Cable (TC)	Buffer	Fiber	NAPs	NAP Port
Site Name	OLTXX	1	1	Name coverage area	1	1	TC01	01	01	NAPXX	01
Site Name	OLTXX	1	2	Name coverage area	1	2	TC01	01	02	NAPXX	02
Site Name	OLTXX	1	3	Name coverage area	1	3	TC01	01	03	NAPXX	03
Site Name	OLTXX	1	4	Name coverage area	1	4	TC01	01	04	NAPXX	04
Site Name	OLTXX	2	1	Name coverage area	1	5	TC01	02	01	NAPXX	01
Site Name	OLTXX	2	2	Name coverage area	1	6	TC01	02	02	NAPXX	02
Site Name	OLTXX	2	3	Name coverage area	1	7	TC01	02	03	NAPXX	03
Site Name	OLTXX	2	4	Name coverage area	1	8	TC01	02	04	NAPXX	04
Site Name	OLTXX	N	N	Name coverage area	N	N	TC N	N	N	NAP N	N

6.2.1.2 KPIs for Acceptance from Construction

To manage construction of FTTP networks, operators track KPIs such those shown in Table 9.

Table 9 - KPIs for Managing Acceptance from Construction

Name	Dimension	Source
BNG count	Count of birth certified BNGs (per week + total)	BNG telemetry
CIN active port count	Count of birth certified CIN ports (per week + total)	CIN telemetry
OLT count	Count of birth certified OLTs (per week + total)	OLT telemetry
PON count	Count of birth certified PONs (per week + total)	OLT telemetry
Homes Fiber Connected	Count of birth certified Fiber drops (per week + total)	Construction

6.2.2 Use Case: Network Certification End-to-End Testing

A process (or certification) needs to be in place to ensure that all elements involved in the provisioning of services for the end customer are working correctly across all levels of the network. This certification aims to test, directly in the hub, services in a percentage of PON ports of every OLT ready to go into service.

A set of the main actions that are involved in the initial installation of the customer's services and in the subsequent life of the product are recreated during this process. All elements are involved, including business and operation support system (BSS/OSS) commands and business rules. Some of these services are described below.

6.2.2.1 Basic Access Configuration

High Speed Internet (HSI) or High Speed Data (HSD) Service

- All product tiers available in the city/region to be certified
- Provisioning
- Tier change
- Deprovisioning
- Speed test
  - With local equipment connected to the ONU
  - Synthetic testing with the ACS [TR-143]

Telephony

- Services offered
- Provisioning
- Change in numbers
- Collections
- Deprovisioning

Video

- VLAN configuration (with specific virtual channel identifier [VCI] parameters linked to set-top boxes)
- Provisioning
- Package change
- Collections
- Deprovisioning
- The abovementioned actions, for both broadcast and over-the-top offerings

Small and Midsize Business (SMB)

- Services offered in the city/region to be certified (some examples follow)
  - Quality of service (QoS) tiers
  - Semi-dedicated links
  - L2 services
  - Digital voice offerings (with analog terminal adapter [ATA] configured and attached to an Ethernet port)
  - Additional customer premise equipment (CPE) configuration and testing (SD-WAN box, Wi-Fi access points, firewall/router, etc.)

By performing network certification, the following paths/platforms/elements are tested.

OLT–BNG

- OLT-to-BNG links (physical connections, optical budget, etc.)
- Redundancy connectivity between OLT and BNG (if applicable)

- WLAN configurations
- SMB/Enterprise configurations (additional uplinks to disaggregate traffic, QoS, etc.)

BNG–Core

- Physical links
- Logical validation
  - BNG uplinks to the core
  - BNG links to caching platforms/services
  - Internet connection
  - Capacity

Service Platforms

- Capacity validation in caching platforms
- IP pools in DHCP platforms
- OLT/ONU connectivity to provisioning platforms
  - Network services orchestrator (OSS)
  - BSS
- OLT/ONU connectivity to management platforms
  - AAA (authentication, authorization, and accounting)
  - ACS (autoconfiguration server)
  - EMS (element management system)
- NOC (alarms and events monitoring) confirmation

6.2.2.2 Service Resources

Management Resources

- OLT/ONU management IP assignment
- OLT VLAN management assignment

Voice Service Resources

- OLT voice VLAN assignment
- ONU voice service IP pool assignment
- ONU telephone line assignment

Data Service Resources

- OLT data services VLAN assignment
  - L3 services
  - L2 services
- ONU data service IP pool assignment
  - Dynamic IP pools

- Static IP pools

Video Service Resources

- OLT video VLAN assignment
- ONU video service IP pool assignment

6.2.2.3 Example Documentation for OLT Certification

6.2.2.3.1 Rack and OLT Information

Element	Description
Date	
Site name	
Site ID	
OLT Name	
OLT Model	
OLT Type	
OLT ID	
Uplink Router to OLT Distance	
Wavelength (DWDM)	
Link Loss	
Uplink Optics Model/Type	
Uplink Optic Speed	
Uplink Interface	
Rack location (pole location if aerial, cabinet, lat, long)	
Rack position	

6.2.2.3.2 Inventory

Slot	Card Type	Part Number	Serial Number
1			
2			
N			

6.2.2.3.3 Base Configuration and Management

Description	Result
Management IP address NE	x.x.x.x
Version	
SNMP community	
UPLINKs redundancy	
Cards commissioning	
Port activation	
Profiles validation	
Alarms validation	

6.2.2.3.4 PON Port Measurements (Examples)

Power measurements must be done at each port to ensure the integrity of all PON modules. The example below is from an operator who deployed GPON.

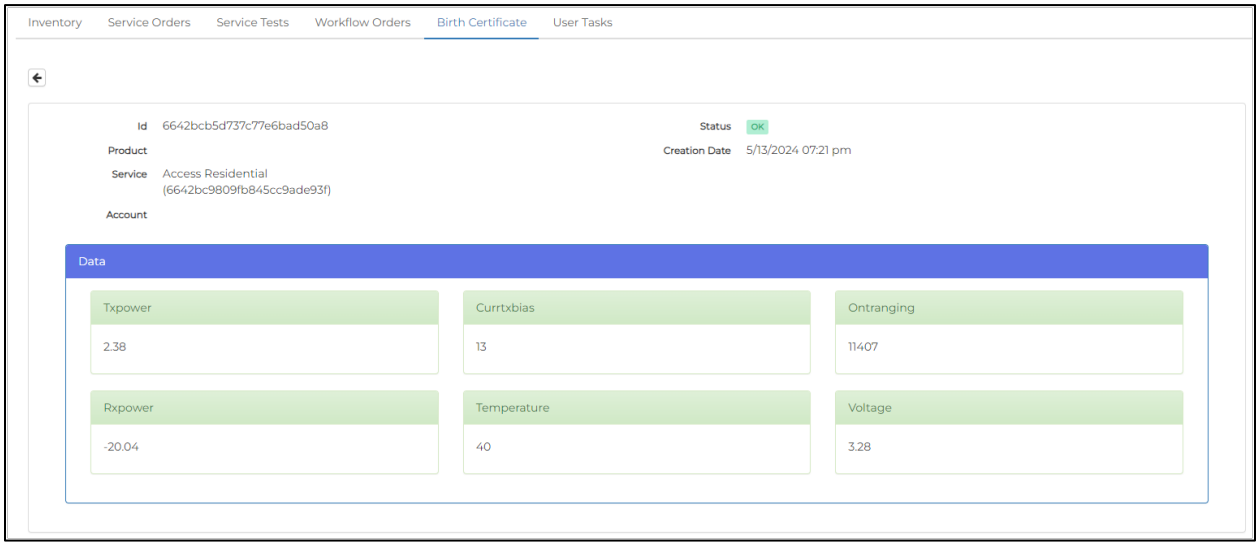
Port	Transceiver	Expected	Result
Port 1-1-1		+1.5 to +5 dBm	
Port 1-1-2		+1.5 to +5 dBm	
Port 1-1-3		+1.5 to +5 dBm	
Port 1-1-4		+1.5 to +5 dBm	
Port N		+1.5 to +5 dBm	

6.2.2.3.5 Service Tests

Service tests must be performed on each card according to the offered HSI speeds and voice/video services.

Slot	HSI	Voice	Video
1			
2			
N			

6.2.2.3.6 Network Services Orchestrator Screenshots and Reports



6.2.2.4 OLT Provisioning KPI

The count of OLT provisioned is tracked in addition to the birth certificate details.

OLTs provisioned and compliant refers to the count of provisioned OLTs and the number that pass a compliancy check. The source of the data is the OLT telemetry and OSS.

6.2.3 Use Case: Network Inventory

The network inventory platform is a multi-module, multi-technology solution for the inventory of logical and physical network elements and the support of the network management process and sales management. It includes the following.

- Physical and logical network inventory
- Network design and planning

- Service inventory
- Physical resources
- GIS data viewer
    - Web application
    - Web viewer for commercial and technical coverage areas
    - Verifies whether a given service can be provided at specified locations or between specified locations (coverage areas)

6.2.3.1 Port Registration

For FTTP, NAP port mapping during the customer life cycle is a must to support capacity and failure management. CRM integration with the network inventory platform registers services sold to customers and reserves network resources used for the services, creating a database for troubleshooting and commercial strategies.

The CRM–Field Services Platform supplies the technical parameters required to activate a given service in a service activation process.

6.2.4 Use Case: Customer Installation Process and Certification

During the general process of installation, there are two specific moments in which (birth) certificates are processed:

- when the PON gateway has been installed and provisioned and
- when Wi-Fi services have been configured.

There is a third correlated event, i.e., when the ONU has been provisioned and quality of signal measurements are performed.

The main difference between passing all tests and the emission of a certificate is that during the latter, technical data from the process are recorded and the installer is unable to finish the order (close the order) if a determined criteria of values/thresholds has not been met. For the purpose of this report, the house check is the relevant process.

6.2.4.1 House Check

This process involves checking the signal strength levels received in devices like ONUs and eMTAs within the subscriber's home. The goal is to ensure that the installation meets the required technical parameters to guarantee service quality before completion.

1. Values are obtained locally (via measurement equipment) and remotely (from monitoring/management platforms, where applicable).
2. If the “pass” criteria are met, the installer is able to finish/close that phase of the service order, with everything kept in the customer’s record.
3. If such criteria are not met, the system will not allow the rest of the service order to complete.
4. A process of verification is then launched. It can go from local revision all the way to requesting assistance from technical personnel from OSP and/or hubs/sites.
5. Once everything is in order, the process goes through the testing and certification phase again, aiming to finally complete the order.

6.2.4.2 ONU Provisioning KPIs

As for OLTs, operators track the ONUs provisioned in addition to the birth certificate for the services.

ONUs provisioned and compliant is the count of provisioned ONUs plus those passing the compliancy check. The data are sourced from OLT telemetry and OSS.

At installation, *ONUs installed* refers to the count of birth-certified ONUs (per week + total). The source of the data is OLT telemetry and field operations information.

6.2.4.3 Calibrate Tx and Rx Levels

At deployment of an ONU, and potentially at network certification, some operators may choose to collect Tx and Rx levels at the customer premise and/or the node to compare against technician measurements using calibrated devices. By collecting the telemetry from the network and comparing it to the readings of the test device, the technician can estimate any offset between the calibrated instrument and the reported telemetry. With multiple measurements, any measurement variability can be gaged as well. Process steps at the ONU may include the following.

1. Collect downstream Rx light levels using a calibrated field meter; multiple collections may be warranted.
2. Connect ONU to port.
3. Collect one or more ONU telemetry light level samples over time.
4. Store the telemetry samples with the field meter data into a birth certificate record and for later analysis.

This process can be done at the OLT location to collect upstream light levels as well. This process may also be done at the ONU for upstream and/or OLT location for downstream levels if desired.

After installation of an ONU, a birth certificate should be generated. This includes verification of the six parameters regarding optical levels. For this, the below values are measured or calculated as indicated.

- ONU up Tx measured
- OLT up Rx measured
- OLT down Tx measured
- ONU down Rx measured
- Downstream link loss = OLT down TX – ONU down RX (calculated)
- Upstream link loss = ONU up TX – OLT up RX (calculated)

Because the birth certificate must be generated during installation and possibly a couple of times, the telemetry must be available on demand. This means the data must be collected on the instance and delivered to the user/application within 10 to 15 seconds after the request. This requirement must translate into the method of telemetry collection (MIB, stream, subscription, IPFIX, YANG, etc.). If possible within this timeframe, multiple measurements (samples) should be performed to ensure the results are stable.

This is an excellent time to calibrate distance estimates that the PON system may provide as well. The known fiber distance at deployment can be compared to the output from the PON-provided information to compare and calibrate in a way similar to the above procedure.

6.2.5 Notes

- Business expectations regarding "readiness state" or assessment of operations readiness are considered.
- The idea of having a snapshot available for later analysis could lose relevance as we approach a network digital twin, where network status is available in a time frame much closer to "real time" for massive operation crews.
- The frequency and traceability of different snapshots seem to be manageable/control levers.

6.2.6 Birth and Move

PON services present a common network resource to customers sharing a single port on the PON ONU. Additionally, multiple services may be provided over a single ONU at the customer's premises. For example, a customer may subscribe to both a video service and high-speed data service for Internet access, with each provided by different service flows or VLANs across the service. A commercial customer may likewise subscribe to multiple data services, which may include metro Ethernet services or a dedicated Internet access service that includes service-level guarantees with credits awarded if the service fails to meet contracted service-level agreements. Even when all traffic is best-effort and there are no contracted service-level agreements, customer satisfaction depends on meeting service-level expectations. It is important to measure the performance of the service on day one, when it is activated, to provide a point of comparison for service performance at a later date.

For this measurement to be valid, four sets of data points must be collected:

- Layer 1 certification testing,
- provisioned service speeds or data rates,
- throughput measured at service initiation (i.e., a "service birth certificate"), and
- periodic measurements, taken at fixed intervals or on-demand when the customer reports an issue.

Before any service can be provisioned, the outside plant must be extended from the OLT to the customer premise ONU. This ODN includes the fiber path between the physical port on the OLT, passive elements such as splitters on to the network interface device (NID) at the customer premise, any inside wiring, and finally the ONU. The expected loss as designed, the loss estimated by a planning tool, and the actual measured loss values are recorded for future reference, along with the physical coordinates of the network elements.

This testing and certification must be completed before the customer premise can be considered "on-net." These certification records must be stored and associated with physical plant records that can be corelated with specific services at time of provisioning.

Some commercial services such as metro Ethernet or dedicated Internet access services require "better than best-effort" service delivery with differentiated QoS, including enhanced queuing mechanisms, prioritized or weighted scheduling disciplines, or drop profiles. To meet service-level agreements and customer expectations, the ability to enforce a bandwidth cap per PON port for capacity/provisioned capacity oversubscription management becomes important. It requires additional information regarding the priority characteristics of these better than best-effort services to be maintained.

Though conditional access control (CAC) can be applied to services provisioned with a committed or guaranteed minimum information rate, the port must be known first. PON systems typically do not track PON ports at time of provisioning because the port is dynamically assigned. Because the port is not known at time of provisioning, network CAC cannot be applied until ONUs are discovered on the network. Furthermore, not all "higher priority" services have a committed information rate (CIR) defined because CIR cannot be oversubscribed, and it may be desired to allow an oversubscription ratio for some classes of service.

The provisioned service data rate typically represents the maximum rate that the service will provide to the customer; optionally, it may also include a minimum committed or guaranteed rate and a service priority. Because the service is multiplexed with other services using the same resources on the OLT, it is necessary to keep track of all of the other services mapped to the same PON OLT port to ensure that the maximum committed rate is not exceeded and business rules defining oversubscription rates on maximum rates are not exceeded (which may depend on the nature of the service or the priority assigned). Note that this check occurs at time of service provisioning, or even when the service is ordered, which is prior to service activation. That is, before the service can be activated and measured and the birth certificate results recorded, the service must be validated against all the other services already provisioned on the same port to protect service-level requirements.

This does present a difficulty, particularly when utilizing a dynamic provisioning system such as DOCSIS Provisioning of EPON, in which the customer's ONU is not known in advance but rather is discovered at time of activation when the ONU is first connected to the network. Furthermore, it is necessary to run through this provisioning check for any minimum committed rate and for the maximum provisioned rate for each service on an ONU if that ONU is moved to a different PON port on the OLT.

Similarly, each time a service is added to a PON port, particularly if it is provisioned as a higher priority service, this provisioning check must be run again to ensure that all services utilizing the same PON port remain within the defined business rules defined for each service.

Once the initial provisioning check is completed, the next stage of service activation occurs. At this stage, the OLT and ONU are in active, bidirectional communication with each other using the channel defined by the service provisioning model (service-flow, VLAN, etc.). At this point, a service activation test can be performed. This is an "out-of-service" test such as Y.1564, MEF 48, TWAMP/STAMP, or iPerf designed to generate and pass traffic at the provisioned data rates and report on parameters such as

- throughput,
- maximum transmit size,
- maximum burst size,
- frame loss, and
- latency between OLT and ONU over a defined service activation test period.

Quite often these measurements are not strictly isolated to the network between the OLT and ONU because measurement usually involves a measurement server. There may be ways to account for the difference to isolate closely to the network segment desired.

After this initial soak period has passed and the service is delivered to the customer, periodic or on-demand in-service testing occurs, using either the same OAM tools or low-impact fault monitoring tools such as Bidirectional Forwarding Detection, ICMP echo, or another keep-alive mechanism.

A best practice would be to store the results from this testing in a way that each provisioning activity that results in additional or deletion of a service on the PON is recorded along with the results of a service activation test for the modified service, as well as the results of a set of in-service tests for the other services (not scheduled concurrently with each other or the new service activation test).

6.2.7 Information and Telemetry

To certify installation, much information needs to be captured in order to confirm acceptance from construction, provisioning, and installation. Telemetry must support the specific processes and details associated with the architecture and products sold by the operator. Table 10 below outlines the types of information to be collected.

Table 10 - Information That Must Be Captured for Various Deployment Activities

Name	Dimension	Source
Acceptance from Construction		
BNG count	count of birth-certified BNGs (per week + total)	BNG telemetry
CIN active port count	count of birth-certified CIN ports (per week + total)	CIN telemetry
OLT count	count of birth-certified OLTs (per week + total)	OLT telemetry
PON count	count of birth-certified PONs (per week + total)	OLT telemetry
Fiber-connectable units	count of potentially connectable units	HP reporting
Fiber-connected units	count of birth-certified fiber drops (per week + total)	Construction
Provisioning		
OLTs provisioned and compliant	count of provisioned OLTs + compliancy check	OLT telemetry + OSS
ONUs provisioned and compliant	count of provisioned ONUs + compliancy check	OLT telemetry + OSS
Installation		
ONUs installed	count of birth certified ONUs (per week + total)	OLT telemetry + field ops

To avoid complexity, this document recommends thresholds based on the ITU specification. For the different types of optics (columns in the table), these work out as in Table 11.

Table 11 - Tx and Rx Thresholds Based on ITU Specifications, as an Example for Use

	N1	N2	E1	E2
OLT US RX	-26 < OLT US RX < -5	-28 < OLT US RX < -7	-30 < OLT US RX < -9	-32 < OLT US RX < -11
ONU DN RX	-28 < ONU DN RX < -9	-28 < ONU DN RX < -9	-28 < ONU DN RX < -9	-28 < ONU DN RX < -9
OLT DN TX	2 < OLT DN TX < 5	4 < OLT DN TX < 7	6 < OLT DN TX < 9	8 < OLT DN TX < 11
ONU US TX	4 < ONU US TX < 9	4 < ONU US TX < 9	4 < ONU US TX < 9	4 < ONU US TX < 9

For assessment of the variability of levels during the week (statistical range of the samples), it is recommended to use a 3 dB margin as the threshold.

Depending on the application, an operation may choose to use different thresholds. The hierarchy can be defined as follows:

1. Specified by the standard—Within this range, good operation must be possible.
2. Alarm—Trigger for corrective action.
3. Operational—Within this range, no actions required.
4. Birth certificate—New installations are only accepted within this range.

It is highly recommended that any deviation from the standard is clearly stated when in use.

In addition, operators will want to compare the measurements to the design of the network to validate measured levels against what is possible given the network design. For example, for a known splitter configuration, one can estimate expected values for receive levels and use that to validate the network design, then compare the expected values from the design limitations to the measurements to validate the measurements as well. Fiber distance is also a factor in the design and expected loss impacting the receive levels, so it needs to be factored in as well. These checks are particularly important during the birth certification processes most operators use and then the results are useful for monitoring for unwarranted change in receive levels.

6.2.8 Uses of Birth Certificates in Other Use Case Contexts

6.2.8.1 Troubleshooting

This uses the same ad hoc sampling as birth certification, with the difference that the samples can be taken multiple times and, if required for a prolonged period, forming a 'trace'. Also, samples from within the same PON are collected to determine the location of a fault and its impact.

6.2.8.2 Alarm Monitoring

Alarms are collected, correlated, and sorted to generate incident tickets. Depending on the system, this can be an automated process, including triggering the troubleshooting procedure for 'anomaly detection'. This can be integrated into the monitoring of other types of alarms. Alarms may need to be created outside of the telemetry systems, using streaming or notifications, if the available mechanisms from the telemetry system do not support alarm configuration as the operator needs.

6.2.8.3 Trending

This is intended to provide early warnings of ONUs getting out of spec. The same average and variability values should be stored over multiple weeks. For example, the weekly average and variability for every ONU is stored for 52 weeks. These data can be analyzed to derive degradation curves, allowing maintenance to take preventive measures. This can be integrated into analysis of other metrics such as laser bias, module temperature, etc.

6.3 Repair: Truck Rolls and Dispatch

When technicians are dispatched to find and fix outside plant faults, active and passive elements are treated.

Typically, to localize passive faults, the technician must infer or find either reflection or spurious noise failure modes and localize to the customer premises, outside plant (PON or aggregation, etc.) location, cabinet, hub or headend, etc. When troubleshooting the passive network (including PON and backhaul/Ethernet), technicians typically use an OTDR, a light meter, or a PON power meter to localize faults and failures.

6.3.1 Use Case: Fiber System Fault Identification and Localization

Transmission quality must be measured to identify a fault, and an OTDR or similar function must be used to localize it. This use case assumes that a fiber monitoring function is in place or that the operator relies on customer calls to trigger the use case.

6.3.1.1 Scenarios

When the fiber system experiences an impairment or fault in the system, the fault must be identified and localized.

1. The process is triggered by either customer complaints or monitoring that indicates a change in system performance, perhaps including a fiber cut *reportable within 15 seconds*. Monitoring of power levels (Tx and Rx) is sufficient but must be conducted in near real time (*at least once per second*).
2. An OTDR is initialized from the OLT. A first estimate is gathered to determine distance to fault.
3. Records (including GIS) are consulted for an estimated location on a map.
4. A technician is sent to the location to search for any visible damage. Records of recent maintenance activity are also consulted.
5. If the location is not immediately found, the technician goes to the far end of the system. The technician then uses OTDR in the reverse direction and determines a second estimate of location and distance to fault.
6. Records (GIS) are consulted for an estimated location on a map.
7. The technician uses the two data points to find an overlapping area of where the problem must be and then travels the length of the cable until finding a probable cause.
8. The technician inspects the probable cause to find noticeable damage or signs of fault. The search continues until the problem is found.
9. Once found, the technician affects repair by splicing a new connection, cleaning a jumper, replacing a bad splice or connector, etc.
10. Once corrected, the technician checks the quality of the connection by reestablishing communication in the system and checking Tx and Rx levels. Those levels are then compared to the birth certificate, specifications, or standards. If not to required levels, the technician repeats the process using OTDR to find faults to remove. If a fault exists at the same location, the technician repeats repair until sufficient. Once the repair is complete and confirmed, the technician returns and closes the ticket.

6.3.2 Fault Management and Maintenance

6.3.2.1 Fault Management

A fault in this respect relates to an optical level that is higher or lower (or absent) than required for normal operation of the service. The thresholds for faults may be less stringent than for other processes because they are driven by the question of whether the services work or not. For detection of faults, an alarm agent is needed. This agent must trigger an alarm message when a threshold is breached—ideally, without delay. Network devices (OLT, ONU) provide this function, but the telemetry protocol must be set up to trigger alarms on the correct thresholds and allow these messages to propagate quickly.

One method could be that the optical levels are collected very frequently and compared with thresholds on a central server. Another method would be to program the OLT to trigger an alarm based on pre-programmed thresholds.

Various methods have pros and cons regarding telemetry traffic, storage, availability of metrics, and flexibility. When faults are being fixed, the same requirement as for installation for on-demand telemetry occurs.

In addition, it may be required to create a 'trace' with multiple measurements in sequence. The duration of a trace varies depending on the type of fault. Ideally, it would be programmed between 10 minutes and one full week (for intermittent failures). In practice, a small number of options would be sufficient. For example, 10 minutes with 15-second intervals, one hour with one-minute intervals, and one day with 15-minute intervals up to one week with hourly intervals. The granularity depends on the expected load on the network and systems.

6.3.2.2 Maintenance

Maintenance in this respect focuses on preventing degradation from becoming a fault. Translated to processes:

- ONUs out of spec management. This is reporting ONUs with optical levels outside the thresholds for good operation but may or may not have triggered a corrective action.
- Fault prevention with predictions based on degradation curves.

Both processes require the collection and storage of telemetry over long periods, up to several years. To limit the data volume, the frequency of collection can be reduced, and statistics can be stored instead of the full history of raw data.

A practical implementation can be to collect samples throughout the week and only store the lowest (min), the highest (max), and the average value for each ONU. Alternately, statistical quantiles can be calculated and updated as needed, without storing the full data history.

6.3.3 Information and Telemetry

The information required for this use case includes the following.

- Tx and Rx levels at each end point
- Light meter or PON power meter capabilities at OLT, splice points, and ONU
- OTDR capabilities at OLT, splice points, and ONU—The OTDR capability must be accurate to within one percent of the total distance.
- GIS information to align fiber distance to geographic location
- Basic records for comparisons including birth certificate information

Further, the information used to trigger action are shown in Table 12, formed into KPIs for management uses.

Table 12 - Information That Can Trigger Troubleshooting Actions

Name	Dimension	Source
CIN laser bias	Count of CIN laser bias < threshold	CIN telemetry
CIN TX level	Count of CIN laser TX < threshold	CIN telemetry
CIN RX level	Count of CIN RX level < threshold	CIN telemetry
OLT up laser bias	Count of (uplink) laser bias < threshold	OLT telemetry
OLT up TX level	Count of (uplink) TX level < threshold	OLT telemetry
OLT dn RX level	Count of (uplink) RX level < threshold	OLT telemetry
PON laser bias	Count of OLT PON laser bias < threshold	OLT telemetry
PON TX level	Count of OLT PON TX level < threshold	OLT telemetry
ONU laser bias	ONU of count with laser bias < threshold	ONU telemetry
ONU TX level	ONU of count with TX level < threshold	ONU telemetry
ONU up RX level	ONU of count with OLT RX < threshold	OLT telemetry
ONU dn RX level	ONU of count with RX < threshold	ONU telemetry
Preventive Action	Count of preventive actions (no failure)	Network operations

Name	Dimension	Source
ONU distance	Distance between OLT and ONU	ONU telemetry
OLT PON optic info	OLT optic information (vendor/part number)	OLT telemetry
ONU PON optic info	ONU optic information (vendor/part number)	ONU telemetry
Transmit frequency	Center frequency transmitted, range of frequency or tolerance	OLT/ONU/CIN
Receive frequency	Center frequency received, range of frequency or tolerance	OLT/ONU/CIN

6.3.3.1 Input Requirements

In short, the telemetry should enable the following.

- Ad hoc samples of four level values plus two estimated link losses. The data should be near real-time (< 15 seconds).
- A trace of multiple ad hoc samples. Covering samples for a prolonged period (e.g., 24 hours) for individual ONUs.
- Alarms for threshold breaches. In essence, this is comparing actual values to the alarm thresholds (preferably programmable) and triggering an alarm quickly in case of breach.
- Trend analysis based on low-cadence (e.g., every 6 hours) collection of values over long periods (e.g., one year) for every ONU. The data can be aggregated to min-max-average on a weekly basis.

6.3.3.2 Implementation Suggestions

The following three types of telemetry are recognized.

- Fast. The applications in which (multiple) samples are needed with short delivery times are related to individual ONUs or all ONUs in one PON. Triggers for these samples will be at installation events (on demand), troubleshooting (on demand), or alarms (automatically). This means low volume of data, ad hoc generated, and fast delivery.
- Alert. Alarms should be always generated for every ONU with fast delivery. This means high volume and continuous comparison with thresholds. This suggests a simple mechanism with low network and CPU load. Maybe even using only alarm functions from OLTs or ONUs. This has the potential to combine this functionality with solutions for other alarms (e.g., dying gasp).
- Clever. Trend analysis requires data from all ONUs over a long period but allows slow collection and aggregation before storing. This can be a separate process of polling OLTs or using the data from an existing management system.

6.4 Service Delivery (KPIs)

Service delivery is assured to protect the overall customer experience. This assurance includes tracking service availability (up time, performance, BER, etc.) and proactive customer and service management. Operations must also determine when there is a rate negotiation problem. This action requires telemetry to support assured service and avoid an unnecessary truck roll and more.

Internet usage is tracked to assure service, project capacity issues, inform planning and engineering work, and potentially support billing. Tracking and assuring service can also help identify and localize L2/L3 problems.

6.4.1 Use Case: KPI and Management

Managing network operations has been mentioned earlier in this report but fault, performance, and capacity management are also critical to service assurance. Table 13 lists information that must be tracked.

Table 13 - Information That Must Be Tracked to Assure Service Delivery

Name	Dimension	Source
Fault Management		
Service calls	Count service calls	Customer care
Truck rolls (TRs)	Count service truck rolls (repair)	Field operations
Early life failure of truck roll	Subset of TR within 28 days after previous TR	Field operations
Early life failure of Install	Subset of TR within 28 days after ONU installed	Field operations
Network corrective actions	Count corrective actions (failure)	Network operations
Performance Management		
Network availability	Calculated from TRs and network corrective actions + duration	Network + field operations
BNG traffic	UP and DN; busiest hour, busiest sample, and wk average	BNG telemetry
CIN traffic	UP and DN; busiest hour, busiest sample, and wk average	CIN telemetry
OLT traffic	UP and DN; busiest hour, busiest sample, and wk average	OLT telemetry
PON traffic	UP and DN; busiest hour, busiest sample, and wk average	OLT telemetry
ONU traffic	UP and DN; busiest hour, busiest sample, and wk average	ONU telemetry
BNG error rate	UP and DN; errored packets/total packets; max + wk average	BNG telemetry
CIN error rate	UP and DN; errored packets/total packets; max + wk average	CIN telemetry
OLT error rate	UP and DN; errored packets/total packets; max + wk average	OLT telemetry
PON error rate	UP and DN; errored packets/total packets; max + wk average	OLT telemetry
ONU error rate	UP and DN; errored packets/total packets; max + wk average	ONU telemetry
BNG packet loss rate	UP and DN; dropped packets/total packets; max + wk average	BNG telemetry
CIN packet loss rate	UP and DN; dropped packets/total packets; max + wk average	CIN telemetry
OLT packet loss rate	UP and DN; dropped packets/total packets; max + wk average	OLT telemetry
PON packet loss rate	UP and DN; dropped packets/total packets; max + wk average	OLT telemetry
ONU packet loss rate	UP and DN; dropped packets/total packets; max + wk average	ONU telemetry
ONU network latency	Latency test according to standardized probe	Probes
ONU network speed	Speed test according to standardized probe	Probes
Capacity Management		
BNG capacity	UP and DN; capacity	BNG telemetry
CIN capacity	UP and DN; capacity	CIN telemetry
OLT capacity	UP and DN; capacity	OLT telemetry
PON capacity	UP and DN; capacity	OLT telemetry
ONU capacity	UP and DN; capacity	ONU telemetry
BNG utilization	UP and DN; BNGtraff/capacity at busiest hour, sample, and wk	BNG telemetry
CIN utilization	UP and DN; CINtraff/capacity at busiest hour, sample, and wk	CIN telemetry
OLT utilization	UP and DN; OLTtraff/capacity at busiest hour, sample, and wk	OLT telemetry
PON utilization	UP and DN; PONtraff/capacity at busiest hour, sample, and wk	OLT telemetry
ONU utilization	UP and DN; ONUtraff/capacity at busiest hour, sample, and wk	ONU telemetry
BNG speed room	UP and DN; BNGspeedroom at busiest hour, sample, and wk	BNG telemetry
CIN speed room	UP and DN; CINspeedroom at busiest hour, sample, and wk	CIN telemetry
OLT speed room	UP and DN; OLTspeedroom at busiest hour, sample, and wk	OLT telemetry
PON speed room	UP and DN; PONspeedroom at busiest hour, sample, and wk	OLT telemetry
ONU speed room	UP and DN; ONUspeedroom at busiest hour, sample, and wk	ONU telemetry

6.4.2 Port Capacity and Performance

At each layer and interface, PON has defined a unit of capacity, and operators need to monitor the capacity utilization of each resource. The amount of capacity that the system is capable of delivering, the amount of capacity that the system is provisioned to deliver, and the amount of capacity consumed (utilized) are all useful data elements for KPIs. The proportion of capacity consumed can be estimated by ratios of the capacity consumed to the capacity available to form a useful KPI for resource utilization.

In addition, at each layer where units of data can be lost or discarded, it is important to track the failure rate of the data delivery.

For example, take GEM frames. The total number of GEM frames would need to be reported, for intervals of time, as well as the number of uncorrectable GEM frames that are discarded. These statistics can be sampled over intervals of time for KPI tracking. A GEM error rate (GER) can be defined as the ratio of errored packets to total packets over the sample interval, and that statistic is then compared to benchmarks for KPI management. The KPI should be monitored in both directions.

7 ALIGNMENT TO CABLE OPEN OMCI

The ONU management and control interface (OMCI) focuses on ONU data elements. The [Cable OpenOMCI] specification details the necessary data elements for cable operators utilizing PON as an access network technology. The primary use case concern for the ONU focuses on monitoring for state and capacity, categorized here as NOC and NMS. This section aligns [Cable OpenOMCI] with the NOC and NMS use cases outlined in this report.

7.1 NOC and NMS: Monitoring State, Function, Performance, and Capacity of Network Components, Subsystems, and Their Functions

NOC and NMS functions for PON systems involve end-point monitoring and performance data about the connections as well as data on upper layer state, performance, and capacity. Elements representing ONU functionality that are covered in OMCI are described below.

7.1.1 L1: Layer 1 Use Cases

1. ONU state monitoring, including a dying gasp alert: bit and/or alarm
    - Though the ONU-G (9.1.1) Alarm number 7 "Dying gasp" has not been explicitly mandated in [Cable OpenOMCI], it is assumed that the ONU supports a more reliable method to indicate a loss of power.
    - The ONU supports a reliable method to indicate loss of power. This method is defined in [G.9807.1] and [G.9804.1] as the "Ind Field" bit 0, known as the dying gasp bit. This bit is sent in every packet.
2. PIC or transponder state monitoring (e.g., pluggable and optical sub-assembly form factors)
    - Optical power levels: from ANI-G (9.2.1)
        - Optical signal level: as reported by ONU
        - Lower optical threshold: 254..0 (default 0xFF selects the ONU's internal policy)
        - Upper optical threshold: 254..0 (default 0xFF selects the ONU's internal policy)
        - Transmit optical level: as reported by ONU
        - Lower transmit power threshold (default 0x81 selects the ONU's internal policy)
        - Upper transmit power threshold (default 0x81 selects the ONU's internal policy)
    - Bias voltage/current

Table 14 - ANI-G (9.2.1): Alarms

Req No.	Alarm	Description
0	Low received optical power	Received downstream optical power below threshold
1	High received optical power	Received downstream optical power above threshold
2	SF	Bit error-based signal fail. Industry practice normally expects the BER to improve by at least an order of magnitude before clearing the alarm.
3	SD	Bit error-based signal degrade. Industry practice normally expects the BER to improve by at least an order of magnitude before clearing the alarm.
4	Low transmit optical power	Transmit optical power below lower threshold
5	High transmit optical power	Transmit optical power above upper threshold
6	Laser bias current	Laser bias current above threshold determined by vendor; laser end of life pending
7..207	Reserved	
208..223	Vendor-specific alarms	

3. Link state monitoring: degradation and variability
   - Optical power levels (see above)
   - Bias voltage/current (see above)
4. Protocol health—Though it is protocol specific, it involves information about encoding failures, packet failures, etc.

Table 15 - XG-PON Downstream Management Performance Monitoring History Data (9.2.16): Threshold Crossing Alert

Number	Threshold Crossing Alert	Threshold Value Attribute No.
1	PLOAM MIC error count	1
2	OMCI MIC error count	2

Table 16 - Enhanced FEC Performance Monitoring History Data (9.2.22): Threshold Crossing Alert

Number	Threshold Crossing Alert	Threshold Value Attribute No.
0	Corrected bits/bytes	1
1	Corrected code words	2
2	Uncorrectable code words	3
4	FEC seconds	4

7.1.1.1 Forward Error Correction Performance Monitoring History Data (9.2.9)

Text in this section has been reproduced from [G.988] and has been formatted to adhere to CableLabs publication style.

This ME collects PM data associated with PON downstream forward error correction (FEC) counters. Instances of this ME are created and deleted by the OLT.

For a complete discussion of generic PM architecture, refer to clause I.4.

Relationships

An instance of this ME is associated with an instance of the ANI-G ME or an instance of the time and wavelength division multiplexing (TWDM) channel ME.

Attributes

Managed Entity ID: This attribute uniquely identifies each instance of this ME. Through an identical ID, this ME is implicitly linked to an instance of the ANI-G or a TWDM channel. (R, set-by-create) (mandatory) (2 bytes)

Interval End Time: This attribute identifies the most recently finished 15 min interval. (R) (mandatory) (1 byte)

Threshold Data 1/2 ID: This attribute points to an instance of the threshold data 1 ME that contains PM threshold values. Since no threshold value attribute number exceeds 7, a threshold data 2 ME is optional. (R, W, set-by-create) (mandatory) (2 bytes)

Corrected Bits/Bytes: This attribute counts the number of bits/bytes that were corrected by the FEC function. For PON systems that use LDPC (e.g., HSP PON), this counter represents the count of corrected bits. For other PON technologies (e.g., GPON/XGS/NGPON2), this counter counts the number of corrected bytes. (R) (mandatory) (4 bytes)

Corrected Code Words: This attribute counts the code words that were corrected by the FEC function. (R) (mandatory) (4 bytes)

Uncorrectable Code Words: This attribute counts errored code words that could not be corrected by the FEC function. (R) (mandatory) (4 bytes)

Total Code Words: This attribute counts the total received code words. (R) (mandatory) (4 bytes)

FEC Seconds: This attribute counts seconds during which at least one uncorrectable FEC codeword was received. (R) (mandatory) (2 bytes)

7.1.1.2 Enhanced FEC Performance Monitoring History Data (9.2.22)

Text in this section has been reproduced from [G.988] and has been formatted to adhere to CableLabs publication style.

This ME collects PM data associated with PON downstream FEC counters for XGS-PON and subsequent ITU-T PON systems. Instances of this ME are created and deleted by the OLT.

For a complete discussion of generic PM architecture, refer to clause I.4.

Attributes

Managed Entity ID: This attribute uniquely identifies each instance of this ME. Through an identical ID, this ME is implicitly linked to an instance of the ANI-G or a TWDM channel. (R, set-by-create) (mandatory) (2 bytes)

Interval End Time: This attribute identifies the most recently finished 15 min interval. (R) (mandatory) (1 byte)

Threshold Data 64 bit ID: This attribute points to an instance of the threshold data 64 bit ME that contains PM threshold values. (R, W, set-by-create) (mandatory) (2 bytes)

Corrected Bits/Bytes: This attribute counts the number of bits/bytes that were corrected by the FEC function. For PON systems that use LDPC (e.g., HSP PON), this counter represents the count of corrected bits. For other PON technologies (e.g., XGS/NGPON2), this counter counts the number of corrected bytes. (R) (mandatory) (8 bytes)

Corrected Code Words: This attribute counts the code words that were corrected by the FEC function. (R) (mandatory) (8 bytes)

Uncorrectable Code Words: This attribute counts errored code words that could not be corrected by the FEC function. (R) (mandatory) (8 bytes)

Total Code Words: This attribute counts the total received code words. (R) (mandatory) (8 bytes)

FEC Errored Seconds: This attribute counts seconds during which at least one uncorrectable FEC codeword was received. (R) (mandatory) (2 bytes)

7.1.2 L2/L3: Layer 2 and Layer 3 Use Cases

1. PON/ONU capacity—Rate and service flow (CIR, EIR, PIR) are generally proprietary. [Cable OpenOMCI] does not cover this function.
2. ONU software state

7.1.2.1 Software Image (9.1.4)

Text in this section has been reproduced from [G.988] and has been formatted to adhere to CableLabs publication style.

This ME models an executable software image stored in the ONU (documented here as its fundamental usage). It may also be used to represent an opaque vendor-specific file (vendor-specific usage).

Fundamental Usage

The ONU automatically creates two instances of this ME upon the creation of each ME that contains independently manageable software, either the ONU itself or an individual circuit pack. It populates ME attributes according to data within the ONU or the circuit pack.

Some pluggable equipment may not contain software. Others may contain software that is intrinsically bound to the ONU's own software image. No software image ME need exist for such equipment, though it may be convenient for the ONU to create them to support software version audit from the OLT. In this case, the dependent MEs would support only the get action.

A slot may contain various equipment over its lifetime, and if software image MEs exist, the ONU must automatically create and delete them as the equipped configuration changes. The identity of the software image is tied to the cardholder.

When an ONU controller packs are duplicated, each can be expected to contain two software image MEs, managed through reference to the individual controller packs themselves. When this occurs, the ONU should not have a global pair of software images MEs (instance 0), since an action (download, activate, commit) directed to instance 0 would be ambiguous.

Attributes

Managed Entity ID: This attribute uniquely identifies each instance of this ME. The first byte indicates the physical location of the equipment hosting the software image, either the ONU (0) or a cardholder (1..254). The second byte distinguishes between the two software image ME instances (0..1). (R) (mandatory) (2 bytes)

Version: This string attribute identifies the version of the software. (R) (mandatory) (14 bytes)

Is Committed: This attribute indicates whether the associated software image is committed (1) or uncommitted (0). By definition, the committed software image is loaded and executed upon reboot of the ONU or circuit pack. During normal operation, one software image is always committed, while the other is uncommitted. Under no circumstances are both software images allowed to be committed at the same time. On the other hand, both software images could be uncommitted at the same time if both were invalid. Upon ME instantiation, instance 0 is initialized to committed, while instance 1 is initialized to uncommitted (i.e., the ONU ships from the factory with image 0 committed). (R) (mandatory) (1 byte)

Is Active: This attribute indicates whether the associated software image is active (1) or inactive (0). By definition, the active software image is one that is currently loaded and executing in the ONU or circuit pack. Under normal operation, one software image is always active while the other is inactive. Under no circumstances are both software images allowed to be active at the same time. On the other hand, both software images could be inactive at the same time if both were invalid. (R) (mandatory) (1 byte)

Is Valid: This attribute indicates whether the associated software image is valid (1) or invalid (0). By definition, a software image is valid if it has been verified to be an executable code image. The verification mechanism is not subject to standardization; however, it should include at least a data integrity check [e.g., a cyclic redundancy check (CRC)] of the entire code image. Upon ME instantiation or software download completion, the ONU validates the associated code image and sets this attribute according to the result. (R) (mandatory) (1 byte)

Product Code: This attribute provides a way for a vendor to indicate product code information on a file. It is a character string, padded with trailing nulls if it is shorter than 25 bytes. (R) (optional) (25 bytes)

Image Hash: This attribute is an MD5 hash of the software image. It is computed at completion of the end download action. (R) (optional) (16 bytes)

Actions

Get: Software upgrade is described in clause I.3. All of the following actions are mandatory for ONUs with remotely manageable software.

Start Download: Initiate a software download sequence. This action is valid only for a software image instance that is neither active nor committed.

Download Section: Download a section of a software image. This action is valid only for a software image instance that is currently being downloaded (image 1 in state S2, image 0 in state S2').

End Download: Signal the completion of a download image sequence, providing both CRC and version information for final verification. This action is valid only for a software image instance that is currently being downloaded (image 1 in state S2, image 0 in state S2').

Activate Image: Load/execute a software image. When this action is applied to a software image that is currently inactive, execution of the current code image is suspended, the associated software image is loaded from non-volatile memory, and execution of this new code image is initiated (i.e., the associated entity reboots on the previously inactive image). When this action is applied to a software image that is already active, a soft restart is performed. The software image is not reloaded from non-volatile memory; the current volatile code image is simply restarted. This action is only valid for a valid software image.

Commit Image: Set the is committed attribute value to 1 for the target software image ME and set the is committed attribute value to 0 for the other software image. This causes the committed software image to be loaded and executed by the boot code upon subsequent start-ups. This action is only applicable when the target software image is valid.

Notifications

Attribute Value Change

Number	Attribute Value Change	Description
1	Version	
2	Is committed	
3	Is active	If an autonomous change to this attribute is associated with an ONU reboot, the ONU should send the AVC (one for each primary software image instance) after the reboot.
4	Is valid	
5	Product code	
6	Image hash	
7..16	Reserved	
NOTE: Older implementations of the OMCI may not support these notifications, which have been introduced in this version of this Recommendation.		

7.1.2.2 Ethernet Frame Extended PM 64 Bit (9.3.34)

Text in this section has been reproduced from [G.988] and has been formatted to adhere to CableLabs publication style.

This ME collects some of the PM data at a point where an Ethernet flow can be observed. It is based on the Etherstats group of [RFC 2819] and [RFC 2863]. Instances of this ME are created and deleted by the OLT. References to received frames are to be interpreted as the number of frames entering the monitoring point in the direction specified by the control block.

For a complete discussion of generic PM architecture, refer to clause I.4.

Relationships

An instance of this ME may be associated with an instance of an ME at any Ethernet interface within the ONU. The specific ME is identified in the control block attribute.

Attributes

Managed Entity ID: This attribute uniquely identifies each instance of this ME. To facilitate discovery, it is encouraged to identify instances sequentially starting with 1. (R, set-by-create) (mandatory) (2 bytes)

Interval End Time: This attribute identifies the most recently finished 15 min interval. If continuous accumulation is enabled in the control block, this attribute is not used and has the fixed value 0. (R) (mandatory) (1 byte)

Control Block: This attribute contains fields defined as follows.

Threshold Data 64 bit ID: (2 bytes). This attribute points to an instance of the threshold data 64-bit ME that contains PM threshold values. When PM is collected on a continuously running basis, rather than in 15 min intervals, counter thresholds should not be established. There is no mechanism to clear a TCA, and any counter parameter may eventually be expected to cross any given threshold value.

Parent ME Class: (2 bytes). This field contains the enumerated value of the ME class of the PM ME's parent. Together with the parent ME instance field, this permits a given PM ME to be associated with any OMCI ME. The supported ME classes are as follows.

- 46 MAC bridge configuration data
- 47 MAC bridge port configuration data

- 11 Physical path termination point Ethernet UNI
- 98 Physical path termination point xDSL UNI part 1
- 266 GEM IW termination point
- 281 Multicast GEM IW termination point
- 329 Virtual Ethernet interface point
- 162 Physical path termination point MoCA UNI

Parent ME Instance: (2 bytes). This field identifies the specific parent ME instance to which the PM ME is attached.

Accumulation Disable: (2 bytes). This bit field allows PM accumulation to be disabled; refer to Table 9.3.32-1. The default value 0 enables PM collection. If bit 15 is set to 1, no PM is collected by this ME instance. If bit 15 = 0 and any of bits 14..1 are set to 1, PM collection is inhibited for the attributes indicated by the 1 bits. Inhibiting PM collection does not change the value of a PM attribute, but if PM is accumulated in 15 min intervals, the value is lost at the next 15 min interval boundary.

Bit 16 is an action bit that always reads back as 0. When written to 1, it resets all PM attributes in the ME, and clears any TCAs that may be outstanding.

TCA Disable: (2 bytes). Also clarified in Table 9.3.32-1, this field permits TCAs to be inhibited, either individually or for the complete ME instance. As with the accumulation disable field, the default value 0 enables TCAs, and setting the global disable bit overrides the settings of the individual thresholds. Unlike the accumulation disable field, the bits are mapped to the thresholds defined in the associated threshold data 1 and 2 ME instances. When the global or attribute-specific value changes from 0 to 1, outstanding TCAs are cleared, either for the ME instance globally or for the individual disabled threshold. These bits affect only notifications, not the underlying parameter accumulation or storage.

If the threshold data 64 bit ID attribute does not contain a valid pointer, this field is not meaningful.

Thresholds should be used with caution if PM attributes are accumulated continuously.

Control Fields: (2 bytes). This field is a bit map whose values govern the behaviour of the PM ME. Bits are assigned as follows:

Bit 1 (LSB)	The value 1 specifies continuous accumulation, regardless of 15 min intervals. There is no concept of current and historic accumulators; get and get current data (if supported) both return current values. The value 0 specifies 15 min accumulators exactly like those of classical PM.
Bit 2	This bit indicates directionality for the collection of data. The value 0 indicates that data are to be collected for upstream traffic. The value 1 indicates that data are to be collected for downstream traffic.
Bits 3..14	Reserved, should be set to 0 by the OLT and ignored by the ONU.
Bit 15	When this bit is 1, the P bits of the TCI field are used to filter the PM data collected. The value 0 indicates that PM is collected without regard to P bits.
Bit 16	When this bit is 1, the VID bits of the TCI field are used to filter the PM data collected. The value 0 indicates that PM is collected without regard to VID.

TCI: (2 bytes). This field contains the value optionally used as a filter for the PM data collected, under the control of bits 15..16 of the control fields. This value is matched to the outer tag of a frame. Untagged frames are not counted when this field is used.

Reserved: (2 bytes). Not used; should be set to 0 by the OLT and ignored by the ONU.

(R, W, set-by-create) (mandatory) (16 bytes)

Drop Events: The total number of events in which frames were dropped due to lack of resources. This is not necessarily the number of frames dropped; it is the number of times this event was detected. (R) (mandatory) (8 bytes)

Octets: The total number of octets received, including those in bad frames, excluding framing bits, but including FCS. (R) (mandatory) (8 bytes)

Frames: The total number of frames received, including bad frames, broadcast frames and multicast frames. (R) (mandatory) (8 bytes)

Broadcast Frames: The total number of received good frames directed to the broadcast address. This does not include multicast frames. (R) (mandatory) (8 bytes)

Multicast Frames: The total number of received good frames directed to a multicast address. This does not include broadcast frames. (R) (mandatory) (8 bytes)

CRC Errored Frames: The total number of frames received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error). (R) (mandatory) (8 bytes)

Undersize Frames: The total number of frames received that were less than 64 octets long, but were otherwise well formed (excluding framing bits, but including FCS octets). (R) (mandatory) (8 bytes)

Oversize Frames: The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. (R) (mandatory) (8 bytes)

Frames 64 Octets: The total number of received frames (including bad frames) that were 64 octets long, excluding framing bits, but including FCS. (R) (mandatory) (8 bytes)

Frames 65 to 127 Octets: The total number of received frames (including bad frames) that were 65..127 octets long, excluding framing bits but including FCS. (R) (mandatory) (8 bytes)

Frames 128 to 255 Octets: The total number of frames (including bad frames) received that were 128..255 octets long, excluding framing bits but including FCS. (R) (mandatory) (8 bytes)

Frames 256 to 511 Octets: The total number of frames (including bad frames) received that were 256..511 octets long, excluding framing bits but including FCS. (R) (mandatory) (8 bytes)

Frames 512 to 1023 Octets: The total number of frames (including bad frames) received that were 512..1023 octets long, excluding framing bits but including FCS. (R) (mandatory) (8 bytes)

Frames 1024 to 1518 Octets: The total number of frames (including bad frames) received that were 1024..1518 octets long, excluding framing bits but including FCS. (R) (mandatory) (8 bytes)

Notifications

Threshold Crossing Alert

Number	Threshold Crossing Alert	Threshold Value Attribute No.
1	Drop events	1
2	CRC errored frames	2
3	Undersize frames	3
4	Oversize frames	4
NOTE—This number associates the TCA with the specified threshold value attribute of the "threshold data 64 bit" managed entity (see clause 9.12.17).		

7.1.3 NOC and NMS General Monitoring Use Cases

Each identifiable component must be monitored for each feature, if the feature exists.

1. Addressability—Can it be communicated with? OMCI layer connectivity implies addressability, but the addressability occurs outside of OMCI.
2. Identity—Does it have a discoverable, unique identification? That is, a serial number (MAC address optional) or ONU ID (ephemeral, session based). Active field replaceable units need to be remotely discoverable or identifiable by the serial number and OEM model number. Regardless of whether the serial number or MAC

is used, the device must have at least an ephemeral MAC, and this identity must bind to a customer account.

OMCI requires identity, closely coupled with addressability, but it occurs outside of OMCI. See [Cable OpenOMCI], "Functional Set 1: Base," for identity of ONU circuit packs and ONU details such as manufacturing data.

3. Functional state (hardware, software) + dying gasp—What is the functional state of the hardware, hardware components, software, and software functions? These are covered in OMCI in a number of ways as outlined above. See [Cable OpenOMCI], "Functional Set 1: Base."
4. Network participation permission—Has it authenticated with the network? This is a gap needing further development, but operators must be able to determine whether a network element should be attached at a given location before the attachment is made.
5. Management function—Can it communicate and be managed? OMCI layer connectivity is implied from the test function.
6. Connectivity—Is it connected to the service network? Light, FEC, and Ethernet statistics provide this via a combination of information. Loss of management function without loss of connectivity implies a specific failure mode.
7. Services—What services does it support? Service flow parameters can provide service state.
8. Traffic bearers—Which defined interfaces exist and can carry traffic? Traffic descriptors are pushed to the ONU by the OLT. Performance measurements indicate these details as far as the ONU can provide.
9. Domain—What is its function in the network, and what is the scope of what it can communicate with or have control or domain over? This is implied by its role, which is discoverable outside of OMCI.
10. Functions—What network functions does it support? This can include services, but it will always include OSI layer functions that enable services.

    See [Cable OpenOMCI], "Functional Set 1: Base," for much of this category of information.

    MAC bridge configuration data

    - MAC bridge port bridge table data
    - MAC bridge port configuration data
    - MAC bridge port designation data
    - MAC bridge port filter preassign table
    - MAC bridge port filter table data
    - MAC bridge service profile

    IP host config data

    - Ethernet frame extended PM
    - Ethernet frame extended PM 64-Bit
    - Ethernet frame performance monitoring history data downstream
    - Ethernet frame performance monitoring history data upstream
11. Physical location—Such as GIS, slot and port, etc. Topology is proprietary and architecture specific. IPFIX options will be investigated.

PON end-point monitoring (transceiver in pluggable and optical sub-assembly form factors) includes the following.

1. Addressability—unique address of the end point and confirmation of response
   OMCI layer connectivity implies addressability, but the addressability occurs outside of OMCI.

2. Identity—unique identity (MAC usually)
3. Functional state (hardware, software) + dying gasp—list of and state of the hardware, hardware components, software, and software functions and status for dying gasp messages
4. Network participation permission—authentication state
5. Management function—management state and capabilities
6. Services—list of services supported and state of the support
7. Connectivity—connectivity details for service
8. Transmit-receive headroom—amount of transmit power, receive power, and electrical power consumption.
    a. Power consumption
    b. Transmit levels
    c. Receive levels
    d. Link budget
9. Frames—details of all frames
    a. Size/fragment
    b. Lost/dropped
    c. Latency/jitter
    d. Drops
10. Error correction—status and function and statistics of error corrections
    a. FEC, HEC, CRC
    b. Error limits
11. Encryption capabilities and state—encryption capabilities, state, and function
12. Service path, adaptation (GEM PID, LLID)—Services require the function of several communication functions, so their states need to be known, and any limits of these counts need to be reported.
13. Bandwidth—amount of link capacity consumed and allocated, limit on full capacity, and any divisions of the capacity and those limits (count of divisions, and capacity of each division, e.g., flow)
    a. Allocation
    b. Capability
    c. Usage
    d. Per user/flow
14. OAM reporting/LLM—management status and reporting
    a. Status
    b. Capabilities
15. Ranging/registration—logical and physical connectivity status
    a. State
    b. Logs
16. Collision management—collision event logging
17. Data link control—data link status and health, logical link control status and performance
    a. Status
    b. Performance
18. MAC control—MAC layer capacity, status, performance
    a. Status
    b. Performance
    c. MAC bridge capacity
19. Physical data translation—symbol encoding, transmission, reception and decoding, status and performance
    a. Status
    b. Performance

20. Physical monitoring—physical connection layer status and performance, mostly hardware status and performance
    a. Status
    b. Performance
21. Association/domain—which customers, end points, virtual ports, etc., are associated and the full scope of entities this component associates with, has control over, etc.

NOTE: Alarms should be reported within 15 seconds of being triggered. Less ephemeral state changes that are informative but not service impacting may be reported within 1 minute, 5 minutes, or 10 minutes as appropriate.

ONU telemetry and alarms are reportable every 10 seconds.

7.1.3.1 Traffic Descriptor (9.2.12)

Text in this section has been reproduced from [G.988] and has been formatted to adhere to CableLabs publication style.

The traffic descriptor is a profile that allows for traffic management. A priority controlled ONU can point from a MAC bridge port configuration data ME to a traffic descriptor in order to implement traffic management (marking, policing). A rate controlled ONU can point to a traffic descriptor from either a MAC bridge port configuration data ME or a GEM port network CTP to implement traffic management (marking, shaping).

Packets are determined to be green, yellow or red as a function of the ingress packet rate and the settings in this ME. The colour indicates drop precedence (eligibility), subsequently used by the priority queue ME to drop packets conditionally during congestion conditions. Packet colour is also used by the optional mode 1 DBA status reporting function described in [G.984.3]. Red packets are dropped immediately. Yellow packets are marked as drop eligible, and green packets are marked as not drop eligible, according to the egress colour marking attribute.

The algorithm used to determine the colour marking is specified by the meter type attribute. If [RFC 4115] is used, then:

- CIR4115 = CIR
- EIR4115 = PIR – CIR (EIR: excess information rate)
- CBS4115 = CBS
- EBS4115 = PBS – CBS

Relationships

This ME is associated with a GEM port network CTP or a MAC bridge port configuration data ME.

Attributes

Managed Entity ID: This attribute uniquely identifies each instance of this ME. (R, set-by-create) (mandatory) (2 bytes)

CIR: This attribute specifies the committed information rate, in bytes per second. The default is 0. (R, W, set-by-create) (optional) (4 bytes)

PIR: This attribute specifies the peak information rate, in bytes per second. The default value 0 accepts the ONU's factory policy. (R, W, set-by-create) (optional) (4 bytes)

CBS: This attribute specifies the committed burst size, in bytes. The default is 0. (R, W, set-by-create) (optional) (4 bytes)

PBS: This attribute specifies the peak burst size, in bytes. The default value 0 accepts the ONU's factory policy. (R, W, set-by-create) (optional) (4 bytes)

Colour Mode: This attribute specifies whether the colour marking algorithm considers pre-existing marking on ingress packets (colour-aware) or ignores it (colour-blind). In colour-aware mode, packets can only be demoted (from green to yellow or red, or from yellow to red). The default value is 0.

- 0 Colour-blind
- 1 Colour-aware

(R, W, set-by-create) (optional) (1 byte)

Ingress Colour Marking: This attribute is meaningful in colour-aware mode. It identifies how pre-existing drop precedence is marked on ingress packets. For DEI and PCP marking, a drop eligible indicator is equivalent to yellow; otherwise, the colour is green. For DSCP AF marking, the lowest drop precedence is equivalent to green; otherwise, the colour is yellow. The default value is 0.

- 0 No marking (ignore ingress marking)
- 2 DEI [IEEE 802.1ad]
- 3 PCP 8P0D [IEEE 802.1ad]
- 4 PCP 7P1D [IEEE 802.1ad]
- 5 PCP 6P2D [IEEE 802.1ad]
- 6 PCP 5P3D [IEEE 802.1ad]
- 7 DSCP AF class [RFC 2597]

(R, W, set-by-create) (optional) (1 byte)

Egress Colour Marking: This attribute specifies how drop precedence is to be marked by the ONU on egress packets. If set to internal marking only, the externally visible packet contents are not modified, but the packet is identified in a vendor-specific local way that indicates its colour to the priority queue ME. It is possible for the egress marking to differ from the ingress marking; for example, ingress PCP marking could be translated to DEI egress marking. The default value is 0.

- 0 No marking
- 1 Internal marking only
- 2 DEI [IEEE 802.1ad]
- 3 PCP 8P0D [IEEE 802.1ad]
- 4 PCP 7P1D [IEEE 802.1ad]
- 5 PCP 6P2D [IEEE 802.1ad]
- 6 PCP 5P3D [IEEE 802.1ad]
- 7 DSCP AF class [RFC 2597]

(R, W, set-by-create) (optional) (1 byte)

Meter Type: This attribute specifies the algorithm used to determine the colour of the packet. The default value is 0.

- 0 Not specified
- 1 [RFC 4115]
- 2 [RFC 2698]

(R, set-by-create) (optional) (1 byte)

7.1.4 Use Case: Transponder Health Monitoring and Fiber Link Monitoring for Degradation

7.1.4.1 Information and Telemetry

The following information elements are required to support this use case. Each of these is identified in [Cable OpenOMCI].

- Tx and Rx light levels
- Power levels (electrical)
- Temperature
- PIC identification
- PIC association to chassis and network element type

8 CONCLUSIONS AND WORK TO BE DONE

Alignment of use cases to telemetry simplifies the work of network operations. This technical report is a beginning to that end, with much more work to be done. Further, the goal of this working group to define proactive network operations for optical networks is just beginning with the foundational alignment represented in this report.

Several use cases in the PON system and more subsystems are yet to be defined in this technical report, including

- fault categorization,
- fault severity assessment, and
- performance monitoring, link quality monitoring – BER, etc.

These are left for future work.

In addition, the alignment of the use case telemetry requirements is largely incomplete. [Cable OpenOMCI] provides the cable industry view on required OMCI management entities beyond OMCI's default version, but that covers ONUs without providing the view of the link, OLT, or optical links back to the switch. Future updates to this report may include identifying and better connecting the use cases in this report to existing standards, or they may turn attention to defining the requirements for the cable industry that extend these other standards.

Finally, the alignment of use cases to [Cable OpenOMCI] is not yet complete in that it is largely untested and undemonstrated. This work will be considered in the future.

Appendix I Compiled Measurements

This document mentions several measurements. Many of them are linked to telemetry (data from the network) but not all. A complied list of the telemetry-related data elements that support the use cases described in this document is shown in Table 17.

Table 17 shows a reduced set of the data elements needed to support the use cases in this document with potential sources of supporting telemetry from standards documents. The connections between these two sources are described as tasks, though work continues to better define the tasks to link directly to the standards-based telemetry, and to verify the existence of these telemetry in the field.

Table 17 - Telemetry Elements That Must Be Supported for the Use Cases in This Report, by Category

Subcategory	Data Element Purpose and Description
Monitoring	
OLT	Addressability—Can it be communicated with, e.g., through OMCI layer connectivity?
	Identity—Does it have a discoverable, unique identification, i.e., a serial number (MAC address optional) or ONU ID (ephemeral, session based)? Active field replaceable units need to be remotely discoverable or identifiable by the serial number and OEM model number. Regardless of whether the serial number or MAC is used, the device must have even an ephemeral MAC, and this identity must bind to a customer account.
	Functional state (hardware, software) + dying gasp—What is the functional state of the hardware, hardware components, software, and software functions? See above.
	Network participation permission—Has it authenticated with the network? This is a gap needing further development, but operators must be able to determine whether a network element should be attached at a given location before the attachment is made.
	Management function—Can it communicate and be managed?
	Connectivity—Is it connected to the service network? Light, FEC (forward error correction), and Ethernet statistics provide this via a combination of information.
	Services—What services does it support? This refers to the service flow parameters.
	Traffic bearers—Which defined interfaces exist, and can they carry traffic? This includes physical and virtual interfaces.
	Domain—What is its function in the network, and what is the scope of what it can communicate with or have control or domain over?
	Functions—What network functions does it support? This can include services, but it will always include OSI layer functions that enable services.
	Physical location—This refers to information such as GIS or slot and port. Topology is proprietary and architecture specific. IPFIX options will be investigated.
ONU	Addressability—Can it be communicated with, e.g., through OMCI layer connectivity?
	Identity—Does it have a discoverable, unique identification, i.e., a serial number (MAC address optional) or ONU ID (ephemeral, session based)? Active field replaceable units need to be remotely discoverable or identifiable by the serial number and OEM model number. Regardless of whether the serial number or MAC is used, the device must have even an ephemeral MAC, and this identity must bind to a customer account.
	Functional state (hardware, software) + dying gasp—What is the functional state of the hardware, hardware components, software, and software functions? See above.
	Network participation permission—Has it authenticated with the network? This is a gap needing further development, but operators must be able to determine whether a network element should be attached at a given location before the attachment is made.
	Management function—Can it communicate and be managed?
	Connectivity—Is it connected to the service network? Light, FEC (forward error correction), and Ethernet statistics provide this via a combination of information.
	Services—What services does it support? This refers to the service flow parameters.
	Traffic bearers—Which defined interfaces exist, and can they carry traffic? This includes physical and virtual interfaces.

Subcategory	Data Element Purpose and Description
	Domain—What is its function in the network, and what is the scope of what it can communicate with or have control or domain over?
	Functions—What network functions does it support? This can include services, but it will always include OSI layer functions that enable services.
	Physical location—This refers to information such as GIS or slot and port. Topology is proprietary and architecture specific. IPFIX options will be investigated.
System	Addressability—unique address of the end point and confirmation of response
	Identity—unique identity (MAC usually)
	Functional state (hardware, software) + dying gasp—list of and state of the hardware, hardware components, software, and software functions and status for dying gasp messages
	Network participation permission—authentication state
	Management function—management state and capabilities
	Services—list of services supported and state of the support
	Connectivity—connectivity details for service
	Transmit-receive headroom—amount of transmit power, receive power, and electrical power consumption Power consumption Transmit levels Receive levels Link budget
	Frames—details of all frames Size/fragment Lost/dropped Latency/jitter Drops
	Error correction—status and function and statistics of error corrections FEC, HEC, CRC Error limits
	Encryption capabilities and state—encryption capabilities, state, and function
	Service path, adaptation (GEM PID, LLID)—Services require the function of several communication functions, so their states need to be known, and any limits of these counts need to be reported.
	Bandwidth—amount of link capacity consumed and allocated, limit on full capacity, and any divisions of the capacity and those limits (count of divisions and capacity of each division, e.g., flow) Allocation Capability Usage Per user/flow
	Operations, administration, and management (OAM) reporting/LLM—management status and reporting Status Capabilities
	Ranging/registration—logical and physical connectivity status State Logs
	Collision management—collision event logging
	Data link control—data link status and health, logical link control status and performance Status Performance
	MAC control—MAC layer capacity, status, performance Status Performance MAC bridge capacity

Subcategory	Data Element Purpose and Description
	Physical data translation—symbol encoding, transmission, reception and decoding, status and performance Status Performance
	Physical monitoring—physical connection layer status and performance, mostly hardware status and performance Status Performance
	Association/domain—which customers, end points, virtual ports, etc., are associated and the full scope of entities this component associates with, has control over, etc.
Component, Subsystem, System Analysis - PIC/SFP	Identity—serial number
	Power consumption
	Tx power
	Rx power
	Chassis SN
	End point/connection
	SFP temperature
	Resets
	Frame errors
	State
	Card temp
	Chassis temp
Birth Certificate	
System	Fiber distance (OLT to ONU)
	Tx avg
	Rx avg
	OLT ID
	OLT Port ID
	ONU ID
	PON-ID Address (Drop)
	OTDR test results (various)
	OTDR back scatter results (various)
	ODN optical power measurements
	ODN-NAP correspondence
	NAP optical power measurements
	BNG count
	CIN active port count
	OLT count
	PON count
	Homes fiber connected count
	Verified product tiers
	Verified provisioned
	Verified tier changes
	Verified collections
	Verified deprovision
	Speed test results

Subcategory	Data Element Purpose and Description
	VLAN configuration
	Services offered
	Verified QoS
	Verified L2
	Verified links
	CPE
	OLT to BNG link
	OLT to BNG redundant link
	WLAN config
	Enterprise config
	BNG to Core link
	BNG to caching services
	BNG to Internet
	Capacity link
	IP pools, DHCP platforms
	OLT to ONU connectivity
	OSS connectivity
	BSS connectivity
	AAA connectivity
	ACS connectivity
	EMS connectivity
	NOC alarm confirmation
	OLT to ONU management IP
	OLT to ONU VLANs
	OLT L2
	OLT L3
	OLT IP pools
	Gateway installed
	Wi-Fi working
	House check records
	Service throughput
	Service maximum transmit size
	Service maximum burst size
	Service maximum frame loss
	Service latency (OLT to ONU)
Truck Roll	
dispatch repair/install	OTDR
	GIS
CIN	Tx
	Rx
	Laser bias
OLT	Tx
	Rx
	Laser bias
ONU	Tx
	Rx

Subcategory	Data Element Purpose and Description
	Laser bias
System	ONU distance
	OLT PON optic info
	ONU PON optic info
	Transmit frequency
	Receive frequency
Service Delivery	
KPI support	
Fault Management	Service calls
	Truck rolls (TRs)
	Early life failure of truck roll
	Early life failure of install
	Network corrective actions
Performance Management	Network availability
	BNG traffic
	CIN traffic
	OLT traffic
	PON traffic
	ONU traffic
	BNG error rate
	CIN error rate
	OLT error rate
	PON error rate
	ONU error rate
	BNG packet loss rate
	CIN packet loss rate
	OLT packet loss rate
	PON packet loss rate
	ONU packet loss rate
	ONU network latency
	ONU network speed
Capacity Management	BNG capacity
	CIN capacity
	OLT capacity
	PON capacity
	ONU capacity
	BNG utilization
	CIN utilization
	OLT utilization
	PON utilization
	ONU utilization
	BNG capacity head room
	CIN capacity head room
	OLT capacity head room
	PON capacity head room
	ONU capacity head room

Appendix II Acknowledgements

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

Contributor	Company Affiliation
Glen Kramer	Broadcom
John Bevilacqua, Kevin A. Noll, Jon Schnoor, Jason Rupe	CableLabs
Marta Seda	Calix
Mustanser Siddique	Charter
Mark Laubach	Ciena
Matt Wichman	Comcast
Igor Tavrovsky	Cox
John Bender	GCI
Israel Madiedo, Pablo Alberto Castillo Brizuela, Jesus Gastelum Tirado	Izzy
Robert-Jan van Minnen	Liberty Global
Stephen Kraiman	Vecima
Abdul Asserti	Vodafone Ziggo

Jason Rupe, CableLabs

* * *