TECHNICAL REPORT

TR-489

ONU Authentication and Selection of eOMCI or vOMCI

Issue: 1
Issue Date: June 2023

Notice

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER’S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

Issue History

Issue Number	Issue Date	Issue Editor	Changes
1	21 June 2023	Robert Peschi, Nokia	Original

Comments or questions about this Broadband Forum Technical Report should be directed to help@broadband-forum.org.

Editor	Robert Peschi	Nokia
PON Management Project Stream Leader	Joey Boyd	Adtran
Fiber Access Network Work Area Director(s)	Marta Seda	Calix

Table of Contents

List of Figures

Executive Summary

As modern networks increasingly rely on Cloud and virtualization, in particular concerning ONU authentication and management, it is important to specify the process by which the Management System and the OLT will agree on which one is exclusively responsible to authenticate and manage an ONU. This specification is critical for interoperability in a multivendor network.

To this matter, this Technical Report specifies the functional split of responsibility between Management Plane and OLT for different deployment scenarios. It provides the network interactions to resolve each of them, and it formalizes the list of requirements set on each involved network entity to support them. These requirements are key to define the supportive YANG data nodes defined in other TRs, such as for instance TR-385.

This Technical Report is intended to be a reference to all applications dealing with ONU authentication and ONU management, embedded in the OLT, performed by the Management System or performed by a disaggregated OLT Software component.

1 Purpose and Scope

1.1 Purpose

The diversity of situations for authenticating a given Optical Network Unit (ONU) and deciding whether it should be managed by the Optical Line Termination (OLT) using an embedded OMCI function (eOMCI) or by the Management System using a virtualized OMCI function (vOMCI) requires a consistent network operation reference specification for these matters. This is the purpose of this Technical Report.

This Technical Report focuses on ONU authentication methods that are based on ONU serial number, registration ID and/or LOID.

1.2 Scope

This Technical Report provides a comprehensive definition of the functional architecture, scenarios, interfaces and requirements to be followed by the Optical Line termination (OLT) and the Management Plane in order to authenticate an Optical Network Unit (ONU) when it is connected to the network and decide whether it should be managed by the Optical Line Termination (OLT) using an embedded OMCI function (eOMCI) or by the Management System using a virtualized OMCI function (vOMCI).

This Technical Report is based on existing standard ways to authenticate ONUs as described in ITU-T G.984.3 [4], Clause VI.1, ITU-T G.989.3 [6], Clause 15.2.1 and ITU-T G.988 Clause 9.1.1.

This Technical Report assumes that BBF YANG models are used for the management of devices.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [13].

MUST This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the term “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.

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

MAY This word, or the term “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below. A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document		Title	Source	Year
[1]	TR-383	*Common YANG Modules for Access Networks*	BBF	2022
[2]	TR-385	*ITU-T PON YANG Modules*	BBF	2020
[3]	TR-451	*vOMCI Interface Specification*	BBF	2022
[4]	G.984.3	*G-PON: Transmission convergence layer specification*	ITU-T	2014
[5]	G.987	*XG-PON systems: Definitions, abbreviations and acronyms*	ITU-T	2012
[6]	G.987.3	*XG-PON: Transmission convergence (TC) layer specification*	ITU-T	2014

[7]	G.988	*ONU management and control interface (OMCI) specification*	ITU-T	2012
[8]	G.989	*NG-PON2: Definitions, abbreviations and acronyms*	ITU-T	2015
[9]	G.989.2	*NG-PON2: Physical Media Dependent (PMD) layer specification*	ITU-T	2014
[10]	G.989.3	*NG-PON2: Transmission convergence layer specification*	ITU-T	2015
[11]	G.989.3 Amendment 1	*NG-PON2: Transmission convergence layer specification*	ITU-T	2016
[12]	G.9807.1	*10-Gigabit-capable symmetric passive optical network (XGS-PON)*	ITU-T	2016
[13]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[14]	RFC 7950	*The YANG 1.1 Data Modeling Language*	IETF	2016
[15]	RFC 6991	*Common YANG Data Types*	IETF	2013
[16]	RFC 7317	*A YANG Data Model for System Management*	IETF	2014
[17]	RFC 7223	*A YANG Data Model for Interface Management*	IETF	2014
[18]	RFC 8528	*YANG Schema Mount*	IETF	2019

2.3 Definitions

The following terminology is used throughout this Technical Report.

Activation A set of distributed procedures executed by the optical line termination (OLT) and the optical network units (ONUs) that allows an inactive ONU to join or resume operations on the passive optical network (PON) as for instance defined in ITU-T 984.3, Clause 3.2.1 and ITU.T 989 Clause 3.2.3.1.

Channel Group A set of channel pairs carried over a common fiber, as defined in ITU-T G.989 [8].

Channel Pair A set of one downstream wavelength channel and one upstream wavelength channel that provides connectivity between an OLT and one or more ONUs, as defined in ITU-T G.989.

Channel Partition Any of the operator-specified non-overlapping subsets of TWDM or PtP WDM channels in an NG-PON2 system, as defined in ITU-T G.989.

Channel Termination Refer to ITU-T G.989. In the G-PON, XG-PON, or XGS-PON context, the term channel termination refers to a logical function associated with an OLT port that terminates an XGS-PON.

Device Management The lowest layer of the Management Plane. It is responsible for the Device Aggregation function and the Device management function of each OLT and ONU devices. The device aggregation function contains the YANG Device Data Stores of each device.

Disaggregate OLT (D-OLT) A logical host for all the functions to be virtualized. It can be located in local servers close to pOLT or centrally in the cloud. It can be also split among multiple locations (local and central).

Logical ONU ID (LOID) An optional ONU credential defined in OMCI for the purpose of ONU authentication.

Management Plane All functions located in the cloud related to the management of the xPON access network in the broad sense.

Metadata Data that relates to a device (for instance an ONU) but that is not part of the device YANG configuration data store itself. Metadata can for instance be used in an ONU device aggregation function to help it handling the ONU, e.g., to authenticate it or determine its management mode.

Model A data model.

Module Refer to [14].

eOMCI (function) The network side termination of OMCI (function) when embedded in the OLT.

ONU management and control interface (OMCI) An operation and management channel between the OLT and an ONU that is message-based and employs an extendable management information base as specified in ITU-T G.988 [7]

Optical Distribution Network (ODN) A point-to-multipoint optical fiber infrastructure, as defined in ITU-T G.989.

Optical Line Termination (OLT) A network element in an ODN-based optical access network that terminates the root of at least one ODN and provides an OAN SNI, as defined in ITU-T G.989.

Optical Network Unit (ONU) A network element in an ODN-based optical access network that terminates a leaf of the ODN and provides an OAN UNI as defined in ITU-T G.989.

Physical OLT (pOLT) A pOLT supports the functions related to access lines, L2 user plane functions and specifically all the related functions that are not virtualized. This term is especially useful when some OLT functions are realized by a D-OLT. When there is no D-OLT involved, pOLT and OLT are synonyms.

Submodule Refer to [14].

vOMCI (function) The network side termination of OMCI (function) when virtualized in the Management Plane as specified in TR-451.

xPON xPON is a generic term used to denote any ITU-T PON variant such as G-PON, XG-PON, XGS-PON, NG-PON2.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

D-OLT	Disaggregated OLT
LOID	Logical ONU ID
OLT	Optical Line Termination
OMCI	ONU management and control interface
ONU	Optical Network Unit
ODN	Optical Distribution Network
pOLT	Physical OLT

PON	Passive Optical Network
PLOAM	Physical Layer Operations, Administration and Maintenance
TR	Technical Report
WA	Work Area
WT	Working Text

3 Technical Report Impact

3.1 Energy Efficiency

This Technical Report describes the requirements that need to be fulfilled to support various network deployments, such as defined in TR-451 vOMCI but it does not specify itself such deployments.

While different deployments solutions may have intrinsic impacts on energy efficiency, this Technical Report has no impact on them and it is not in the scope of this Technical Report to discuss them.

3.2 Security

This Technical Report describes the requirements that need to be fulfilled to support various network deployments, such as defined in TR-451 vOMCI but it does not specify itself such deployments.

This Technical Report provides the necessary security to authenticate an ONU over a PON infrastructure. This Technical Report builds on existing ITU standards on ONU authentication.

3.3 Privacy

This Technical Report has no impact to privacy.

4 Introduction

4.1 Basic Concepts

When an ONU is connected to a channel termination, before it can get connectivity services, the following phases need to take place in strict sequence:

1) Authenticating the ONU.
2) Binding the ONU to a management entity.
3) Managing the ONU device (to start with, configuring the ONU with its intended configuration).

ONU Authentication, ONU binding and ONU management are very distinct concepts clarified in the next sections.

This Technical Report exclusively deals with *ONU authentication* and *ONU binding to a managing entity*. Section 5 will analyze which Network Entities can realize these functions.

ONU management itself is outside the scope of this Technical Report.

4.1.1 What is ONU Authentication ?

ONU authentication is the process by which the xPON access network:

- Verifies whether the ONU is *authorized* to exchange GEM frames with the OLT once it is in O5 state (Ref. for instance to ITU-T G.984.3 Clause 10.2.1 or ITU-T G.989.3 Clause 12.1.4.1) .
- Relates the ONU to a *vANI* inside the OLT for proper traffic handling inside the OLT such as xPON transport and frame forwarding, (ref TR-385 [2]).
- Relates the ONU to an *ONU* Device identifier so that a proper Management Function can be engaged for the ONU. This ONU Device identifier can be of different nature as long as it gives a way to retrieve the ONU Device configuration. For instance, in the Management Plane, an ONU device can be identified by its key “name” in the Device Aggregation Function, (ref. TR-383 [1], “bbf-device-aggregation.yang”). In the OLT, in TR-385 Combined NE mode, an ONU device is identified by its ANI interface.

ONU authentication occurs at ONU activation time, by having the xPON access network compare the credential(s) offered by the ONU with the ones of pre-configured expected ONUs. An ONU is successfully authenticated when a match is found.

ONU authentication credentials exclusively considered in this Technical Report are the **serial number**, r**egistration ID** and **LOID** as per ITU-T G.984.3 [4], Clause VI.1, ITU-T G.989.3 [6], Clause 15.2.1 and ITU-T G.988 [7] Clause 9.1.1. It is an operator’s decision in function of specific deployment strategies which of the serial number, registration ID or LOID credential(s) need to be considered for each ONU. Depending on use-cases, the applicable credential(s) for a given ONU could even change over time, e.g., to ease its truck-roll replacement in case of failure.

> **Note:** It should be noted that the eOMCI/vOMCI ONU management decision can only be done after the ONU is authenticated. When performing Logical ONU ID (LOID) based authentication, the LOID is fetched from the ONU via OMCI (by the OLT via eOMCI or by the Management Plane via vOMCI if the OLT is not able to do it) before the ONU is authenticated, hence before knowing whether the ONU will ultimately be expected to be managed by eOMCI or vOMCI.
>
> In the context of TR-489, during the ONU authentication phase, it is indifferent to fetch the LOID via eOMCI or vOMCI; it can be done independently of the later decision to use eOMCI or vOMCI to

manage the ONU once it is authenticated. In other words, the initial fetching of LOID during ONU authentication is not considered to be part of ONU Management.

4.1.2 What is ONU Binding to a Management Function ?

TR-489 assumes that the xPON access network uses BBF YANG models for all its managed devices.

ONU Binding to a Management Function is the process of engaging an appropriate ONU Management Function to manage this ONU using its specific YANG configuration.

Thus, a YANG/OMCI converting function (“OMCI function” in short) will be present “somewhere” between the ONU Management function and the ONU device, as in Figure 4-1.

4.1.3 What is ONU Device Management ?

Once the ONU has been authenticated and bound to a Management Function, ONU Device Management is the process responsible to:

- push configuration data to this ONU,
- read state information from this ONU,
- send actions to this ONU
- receive autonomous notifications/alarms from this ONU

Figure 4-1 illustrates in all generality the functional architecture for ONU Authentication, Binding and Management. In the figure, the colored arrows are an *abstraction* of flows and transactions respectively involved in authentication, binding, management using YANG data and management over OMCI. These flows/interactions will be illustrated in each scenario of section 5 and will be further detailed in section 6.2.

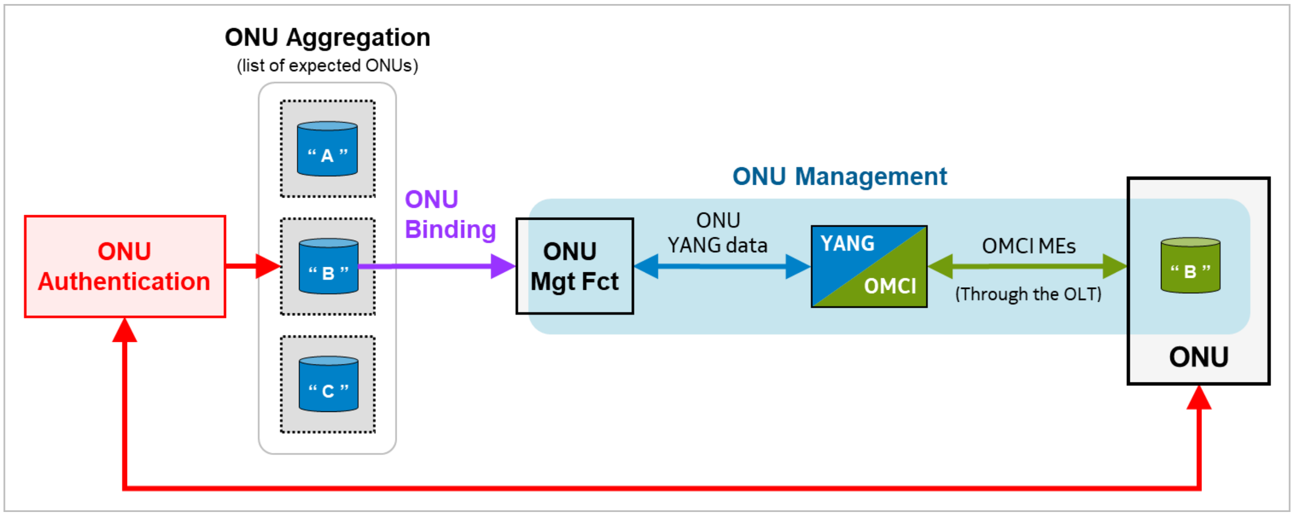


Figure 4-1 - Functional Architecture for ONU Authentication, Binding and Management

4.2 Type of credentials: some practicalities.

As a matter of practical considerations, depending on the credentials used and the ONU-ID allocation method, one should be aware that there can be interference between ONU authentication and ONU-ID allocation that need to be taken care of. This section provides an insight.

TR-385 allows two ways to allocate an ONU-ID to an ONU that connects to an xPON.

One possibility is to have the OLT Management system configure the vANI in the OLT with the ONU-ID to be used when the corresponding ONU shows-up (ref: feature ‘configurable-v-ani-onu-id’ defined in submodule bbf-xponvani-v-ani-body).

An alternative is to have the OLT autonomously allocate an ONU-ID from a local pool of free ONU-IDs (ref: feature ‘pon-pools’ defined in submodule bbf-xpon-channel-group-body). In principle, the OLT can allocate the ONU-ID as soon as the vANI is created or just when the ONU shows-up. Either way, the allocated ONU-ID will be visible as vANI YANG state data as soon as the OLT makes the allocation.

Serial number used for ONU authentication

When an ONU is connected to the xPON fiber, whatever xPON type, it always provides its serial number through PLOAM before it gets allocated an ONU-ID (ref ITU-T G.9807.1 C.11.3, US PLOAM “0x01 Serial_Number_ONU”). Hence if the serial number is sufficient to authenticate the ONU, the OLT will always be able to allocate the right and definite ONU-ID at once to the ONU, even when it is pre-associated with the vANI.

Registration ID used for ONU authentication

In case the ONU needs to be authenticated by means of registration ID, the OLT needs first to allocate an arbitrary ONU-ID to the ONU in order to query it for its registration ID via PLOAM (ref ITU-T G.9807.1 C.11.3, DS PLOAM “0x09 Request_Registration”). Only then can authentication take place identifying a vANI in the OLT. If the vANI has a pre-associated ONU-ID to be allocated, the OLT will have to reallocate this ONU-ID to the ONU. To do so, the OLT should temporarily learn the ONU serial number before deactivating the ONU via PLOAM (ref ITU-T G.9807.1 C.11.3, DS PLOAM “0x05 Deactivate_ONU-ID”). When the ONU shows-up again the OLT immediately recognizes the corresponding vANI through the learned serial number and then directly allocates to the ONU the ONU-ID pre-associated with the vANI. Note that the details about the temporary learning and usage of the ONU serial number are left to OLT vendor implementation and are outside the scope of this Technical Report.

LOID used for ONU authentication

A comparable problem arises with LOID as with Registration ID. Hence the OLT will have to follow a similar procedure after the ONU is authenticated.

5 Possible Scenarios to Authenticate and/or Manage an ONU

The xPON access network consists in OLT and ONU devices and their Management Plane as illustrated in the Figure 5-1.

In general, the Device Management part of the Management Plane is functionally organized as follows; note that this description is purely functional and does not constrain nor suggest a particular implementation of the Management Plane:

- **The Device Aggregation Function**: it contains a list of all devices handled by the Management plane. This typically takes the form of a YANG schema-mounted list (Ref to TR-383 [1], bbf-device-aggregation.yang and RFC 8528 [18]), which contains for each device the mounted YANG configuration of the device itself and some metadata about the device. When the device is an ONU, the metadata contains among other things the expected credentials associated to this ONU.
- **The OLT Management Function**: this is the function responsible of the create, read, update, and delete (CRUD) management of a specific OLT device. It uses the corresponding OLT YANG configuration stored in the Device Aggregation Function.
- **The ONU Management Function**: this is the function responsible of the create, read, update, and delete (CRUD) management of a specific ONU device as described in section 1.1. It uses the corresponding ONU YANG configuration stored in the Device Aggregation Function.

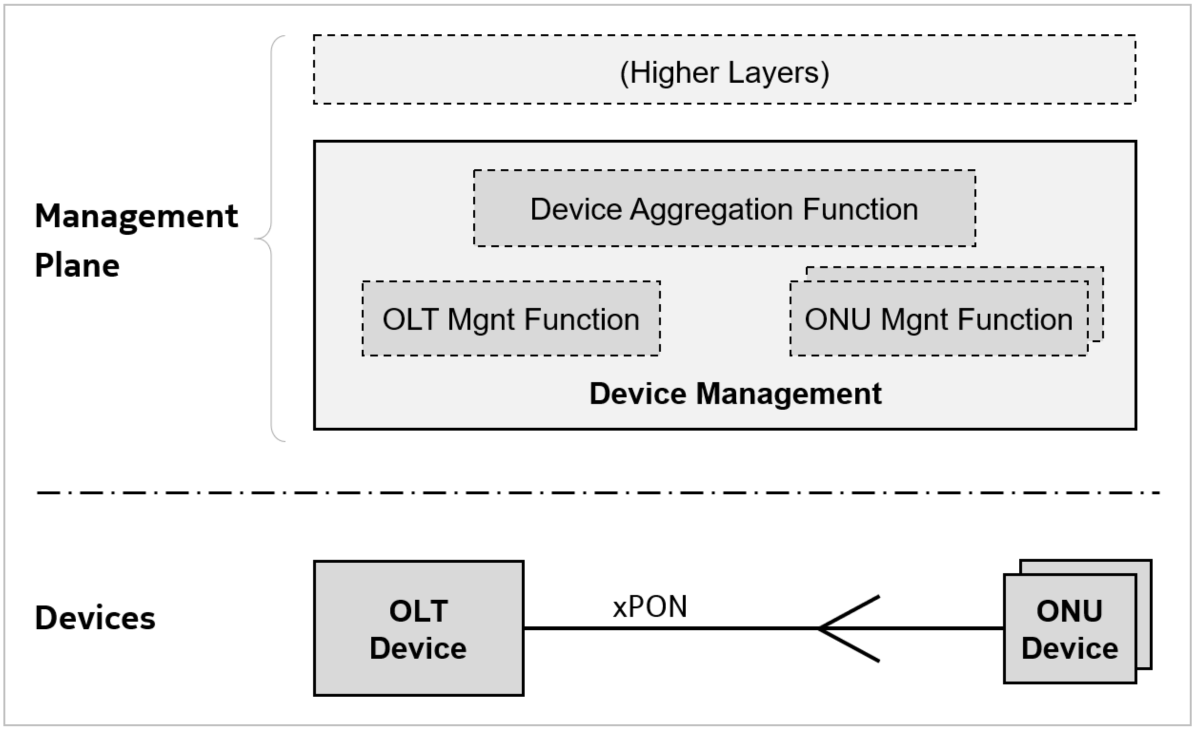


Figure 5-1 - Network Entities involved in ONU Authentication and Management

Conceptually, ONU authentication, binding and device management functions are ultimately a responsibility of the Device Management Plane, which has - as seen above - the knowledge of the credentials of the expected ONUs and the configuration data for each of them.

However, several deployments scenarios are possible where the Management Plane gradually delegates more and more of its authority to the OLT. This Technical Report exclusively considers the four scenarios detailed below.

It should be carefully noted that in all scenarios, any authority delegated to the OLT, remains ultimately *controlled by the Management Plane* using the OLT YANG model.

5.1 Scenario 1

In a first scenario the Management Plane keeps direct authority for the authentication and management of ONUs

In this deployment, the *TR-385 Separated NE mode* is used for the ONU device. ONU authentication relies on the ONU device aggregation function of the Management Plane, that typically holds a list of schema-mounted expected ONUs, keyed by a device “name” string, (Ref. TR-383, bbf-device-aggregation.yang and RFC 8528). The expected credentials for each ONU are stored in the ONU metadata appended to the ONU mount-points.

The Management Plane realizes its ONU management responsibility according to TR-451 [3], where the YANG / OMCI conversion is done in a vOMCI virtualized entity.

The colored arrows are an *abstraction* of flows and transactions respectively involved in authentication, binding, management using YANG data and management over OMCI. Their realization is further detailed in Figure 6-2.

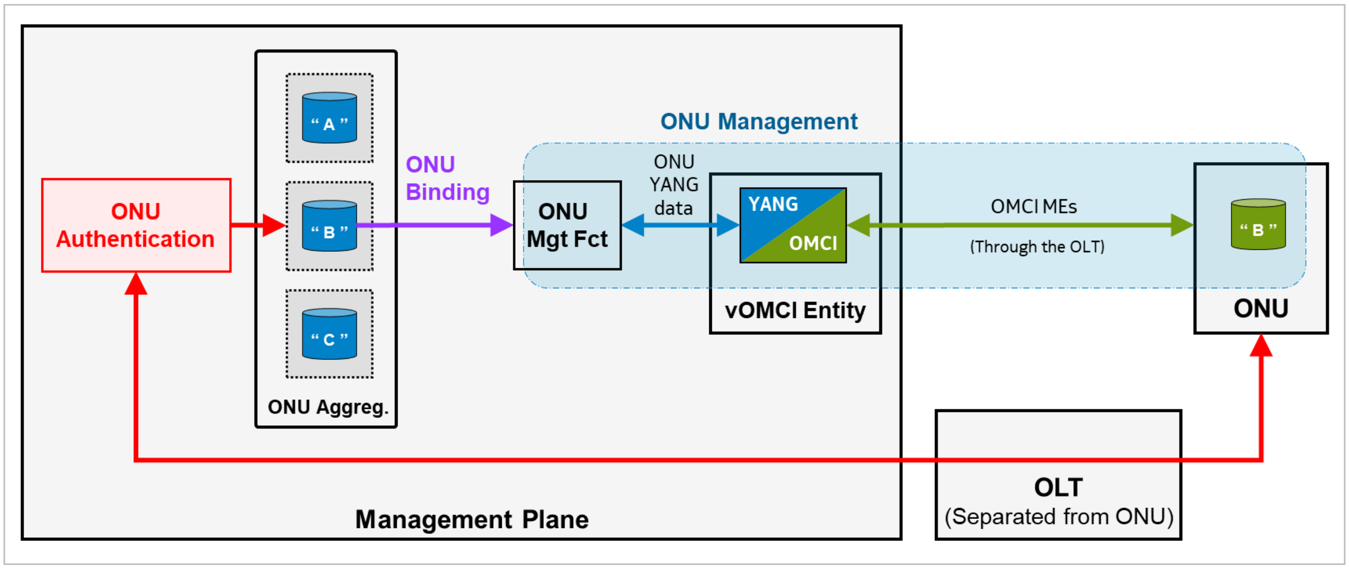


Figure 5-2 - Mapping Functions on Network Entities for Scenario 1

5.2 Scenario 2

In a second scenario the Management Plane keeps direct authority for ONU management but delegates its ONU authentication authority to the OLT.

In this deployment, the TR-385 Separated NE mode is also used for the ONU device. In this case, the OLT performs ONU authentication based on credentials stored at vANIs (ref TR-385).

Like Scenario 1. the Management Plane realizes its ONU management responsibility according to TR-451, where the YANG / OMCI conversion is done in a vOMCI virtualized entity.

The colored arrows are an *abstraction* of flows and transactions respectively involved in authentication, binding, management using YANG data and management over OMCI. Their realization is further detailed in Figure 6-3

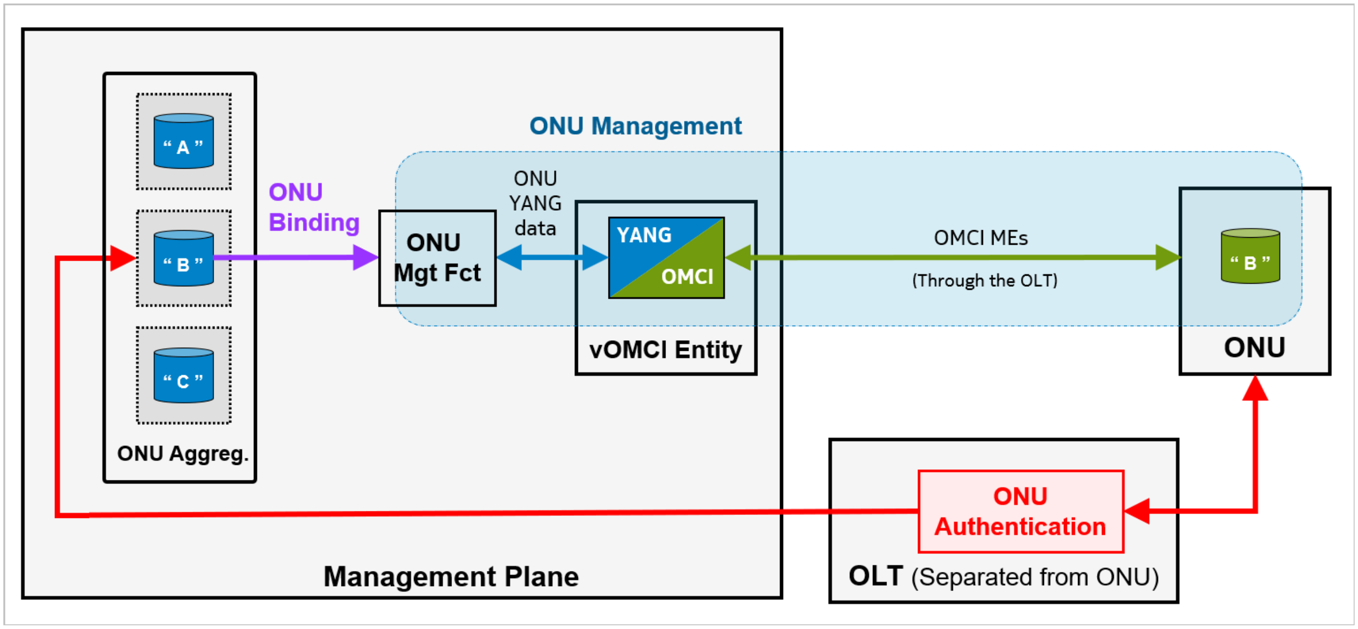


Figure 5-3 - Mapping Functions on Network Entities for Scenario 2

5.3 Scenario 3

In a third scenario the Management Plane keeps the authority to authenticate the ONU but delegates its ONU management authority to the OLT.

This deployment relies on the *TR-385 Separated NE mode* in the Management System and the *TR-385 Combined mode* in the OLT.

In this scenario, the Management plane maintains a list of the ONUs to be authenticated.

Also, the OLT device contains a local ONU Aggregation Function with a list of ONU devices embedded in its own YANG configuration. In TR-385 Combined NE Mode, the configuration of the ONUs is embedded in the OLT configuration in the form of ANI interfaces (interleaved with the genuine OLT interfaces) and their directly related data nodes. To manage these ONUs the OLT will make use of an embedded OMCI function (eOMCI).

For the purpose of managing the OLT, the Management Plane keeps a local copy of the OLT YANG configuration (itself containing the configuration data of ONUs as said above).

In the figure below, the colored arrows are an *abstraction* of flows and transactions respectively involved in authentication, binding, management over YANG and management over OMCI. Their realization is further detailed in Figure 6-4.

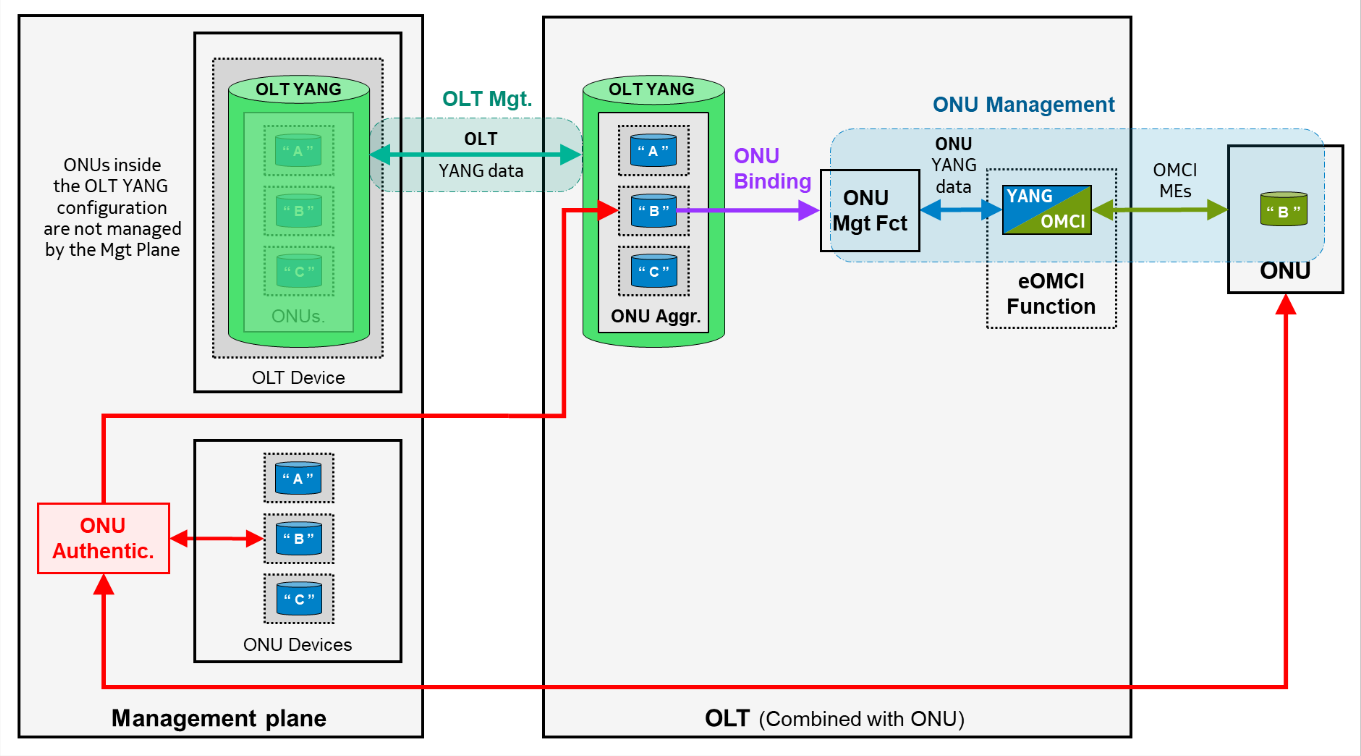


Figure 5-4 - Mapping Functions on Network Entities for Scenario 3

5.4 Scenario 4

Finally, in a fourth scenario the Management Plane delegates to the OLT its authority for both authentication and management of ONUs.

This deployment relies on the *TR-385 Combined NE mode* both in the Management Plane and the OLT. In this scenario, the OLT performs ONU authentication based on credentials stored at the vANIs [TR-385].

Also, in this scenario the OLT contains a local ONU Aggregation Function with a list of ONU devices embedded in the OLT own YANG configuration. In TR-385 Combined NE Mode, the configuration of the ONUs is embedded in the OLT configuration in the form of ANI interfaces (interleaved with the genuine OLT interfaces) and their directly related data nodes.

To manage these ONUs the OLT will make use of an embedded OMCI function (eOMCI).

The colored arrows are an *abstraction* of flows and transactions respectively involved in authentication, binding, management over YANG and management over OMCI. Their realization is further detailed in Figure 6-5.

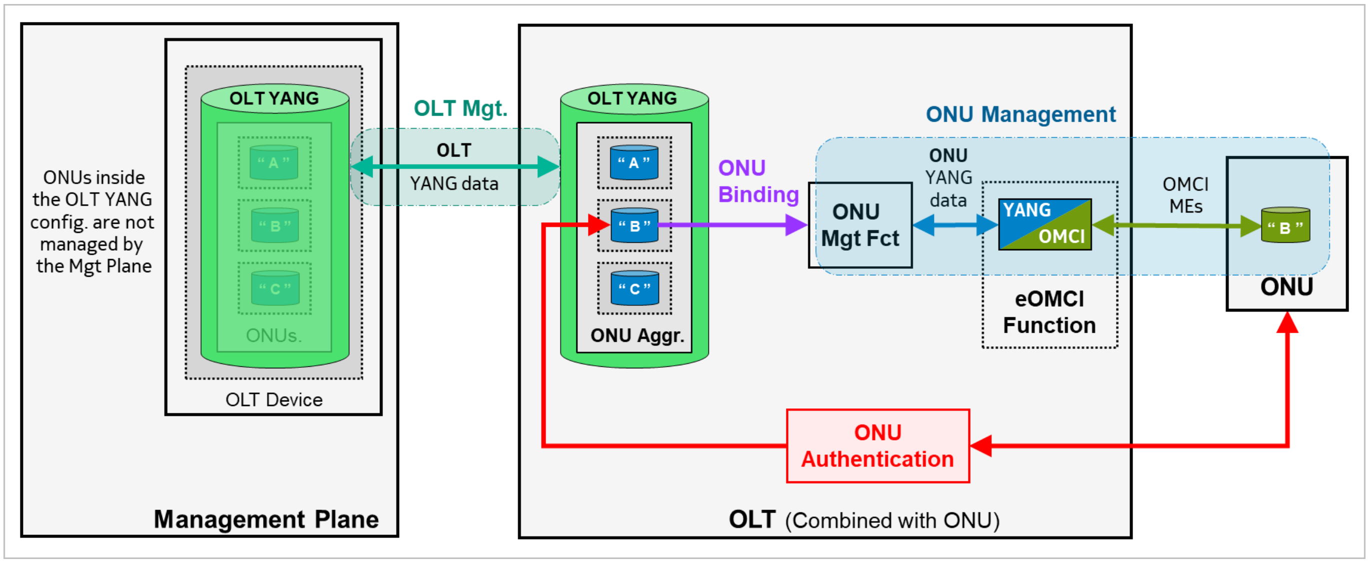
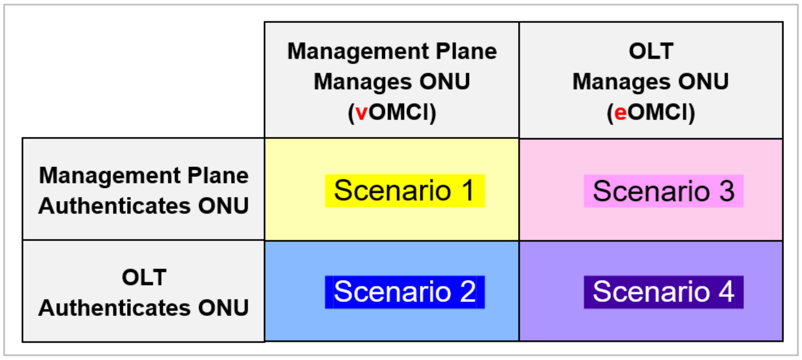


Figure 5-5 - Mapping Functions on Network Entities for Scenario 4

5.5 Summary of all 4 Scenarios

The four deployments scenarios considered by this Technical Report are summarized in the figure below making apparent that ONU Authentication and ONU Management are orthogonal functions when it comes to map them to the Management Plane or the OLT.



	Management Plane Manages ONU (vOMCI)	**OLT Manages ONU (eOMCI)**
Management Plane Authenticates ONU	Scenario 1	Scenario 3
OLT Authenticates ONU	Scenario 2	Scenario 4

Figure 5-6 - The four possible Scenarios for ONU Authentication and Management

Migration scenarios from non-SDN to SDN architecture require that xPON access networks in general - and OLTs in particular - allow any mix of ONUs on the same xPON channel termination such that for instance:

- some of them are authenticated and managed by the Management Plane
- some of them are authenticated by the OLT and managed by the Management Plane
- some of them are authenticated by the Management Plane and managed by the OLT
- and the others are authenticated and managed by the OLT.

6 Determining which Scenario Applies to a Specific ONU

6.1 Principle

The previous section listed the four scenarios in which an ONU could be handled, some of them involving a responsibility split between the OLT and the Device Management Plane, more specifically its ONU Aggregation Function. Thus, when an ONU is connected to the network, the OLT and Device Management Plane must consistently determine on their respective side in which scenario this ONU must be handled.

The behavior of the OLT and the ONU Aggregation Function will ultimately be driven by the configuration of their own YANG models consistently reflecting for each ONU one or the other scenario.

Since OLT and Management Plane are independent entities, they also need to dynamically synchronize and handshake between each other. This synchronization will be realized by means of a notification from the OLT to the Device Management Plane and an action from the Device Management Plane to the OLT.

When an ONU is connected to the network, it is the OLT (based on its configuration) that will first determine if it is expected and/or able to authenticate it by itself or not. The general principle is as follows:

- If the OLT is expected and able to authenticate the ONU, it will do so. Then the OLT will further determine whether it is expected and able to manage it itself using eOMCI. If it is not the case, the OLT will rely on the Management Plane to apply vOMCI to the ONU.
- If the OLT is not expected or able to authenticate the ONU by itself, it will rely on the ONU Aggregation Function of the Device Management Plane for the authentication of the unknown ONU. The OLT will then receive the confirmation that (hopefully) the identified ONU is legitimate and whether it should be managed by the OLT with its local eOMCI or instead that it will be managed by vOMCI.
- If both the OLT and the ONU Aggregation Function of the Device Management Plane are unable to authenticate the ONU, and thus are unable to manage it, then the ONU will not go into service. At that stage the event should be escalated higher up in the Management Plane.

The OLT will run this decision process for each ONU to determine which of the four scenarios applies to the ONU. This is illustrated in the next figure.

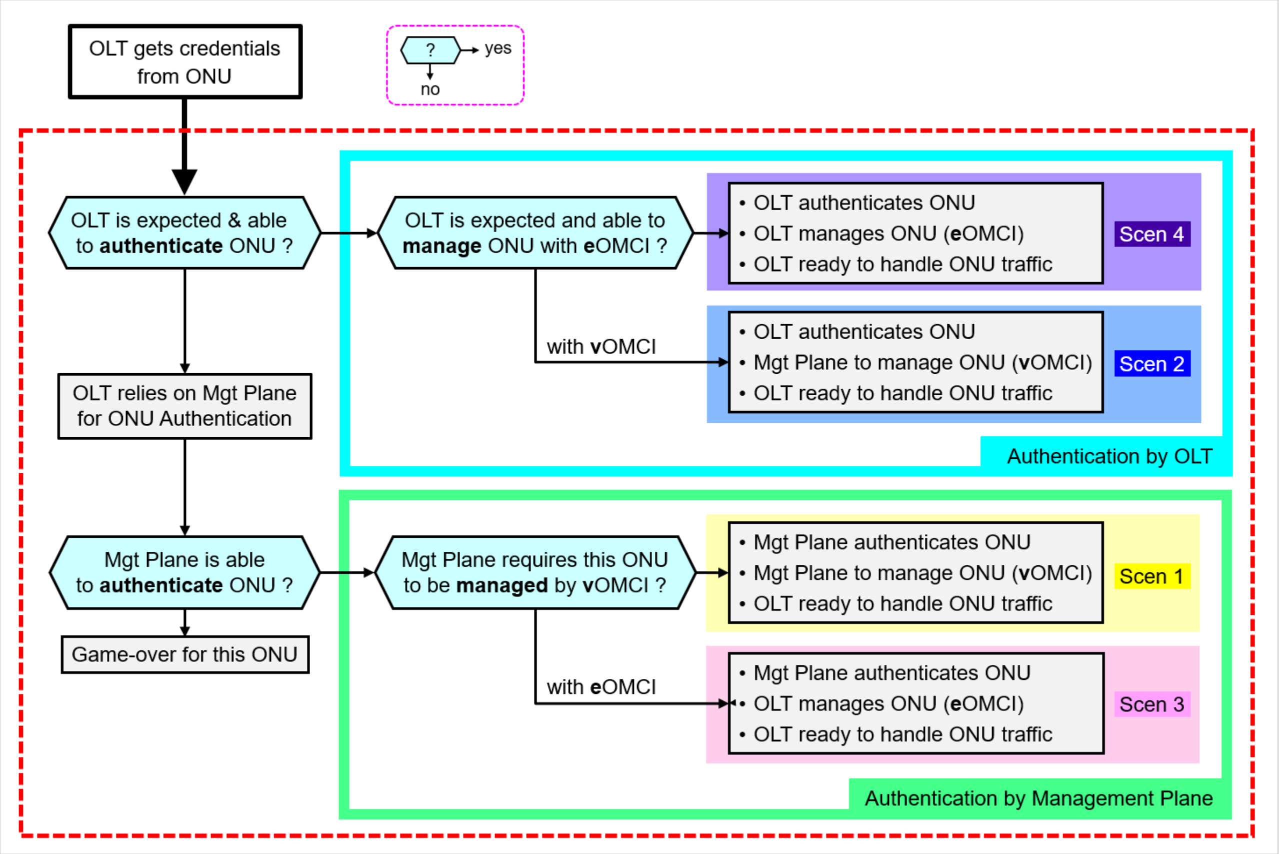

OLT gets credentials from ONU
?
yes
no
OLT is expected & able to **authenticate** ONU ?
OLT is expected and able to **manage** ONU with **e**OMCI ?
• OLT authenticates ONU
• OLT manages ONU (**e**OMCI)
• OLT ready to handle ONU traffic
Scen 4
with **v**OMCI
• OLT authenticates ONU
• Mgt Plane to manage ONU (**v**OMCI)
• OLT ready to handle ONU traffic
Scen 2
Authentication by OLT
OLT relies on Mgt Plane for ONU Authentication
Mgt Plane is able to **authenticate** ONU ?
Mgt Plane requires this ONU to be **managed** by **v**OMCI ?
• Mgt Plane authenticates ONU
• Mgt Plane to manage ONU (**v**OMCI)
• OLT ready to handle ONU traffic
Scen 1
Game-over for this ONU
with **e**OMCI
• Mgt Plane authenticates ONU
• OLT manages ONU (**e**OMCI)
• OLT ready to handle ONU traffic
Scen 3
Authentication by Management Plane

Figure 6-1 - Principle how OLT determines which scenario applies to an ONU

6.2 A closer look at interactions between OLT and Management Plane

This section analyses, in more details, how the elementary action mentioned in section 6.1 is realized in the OLT and in the Management Plane to authenticate an ONU and determine whether eOMCI or vOMCI must be applied.

6.2.1 Realizing Elementary Actions

How can an OLT forward traffic from and to an ONU ?

In all cases and situations, an OLT can provide service to an ONU *only* on the condition that it is configured with a vANI corresponding to the ONU. At the very least, the vANI is the lowest layer interface for any traffic forwarding to and from this ONU.

Hence, whichever way done and wherever done, ONU authentication will always result for the OLT to know *the* vANI corresponding to *the* ONU.

How can an OLT authenticate an ONU ?

When it is planned that the OLT must authenticate a given ONU, credentials expected to be provided by this ONU are configured on its corresponding vANI. Hence, local ONU authentication in the OLT results in the OLT parsing its vANI list by the credentials fetched from the ONU: serial number, registration ID and/or LOID, [TR-385].

How can an OLT determine whether an authenticated ONU is planned to be managed via eOMCI or vOMCI ?

When on ONU is authenticated the vANI is also the place for the OLT to determine or verify whether eOMCI or vOMCI should be applied to the ONU. When the ONU is to be managed by the OLT, the OLT will instantiate an ONU management function, bind it with the locally available ONU YANG configuration and engage its local OMCI stack, [TR-385]. When the ONU is to be managed by the Management Plane, the OLT will just run the procedures specified in TR-451 to let Management plane set-up a management chain though a vOMCI instance to the ONU, [TR-451].

How can the Management Plane authenticate an ONU ?

When it is planned that the Management Plane must authenticate a given ONU, credentials expected to be provided by this ONU are configured in the metadata of this ONU in the ONU aggregation list of the Management Plane. Hence, ONU authentication in the Management Plane results in parsing the ONU device list of its Aggregation Function by the credentials fetched from the ONU: serial number, registration ID and/or LOID [TR-451/TR-383].

How can the Management Plane determine whether an authenticated ONU is planned to be managed via eOMCI or vOMCI ?

When on ONU is authenticated, the ONU metadata in the ONU Aggregation Function in the Management Plane is also the place to determine whether eOMCI or vOMCI should be applied to the ONU (or to verify the consistency of what the OLT has determined for the ONU). When the ONU is to be managed by vOMCI the Management Plane will run the procedures specified in TR-451 to set-up a management chain though a vOMCI instance to the ONU, [TR-451].

The next sections describe how the OLT and Management Plane interwork in each of the four scenarios.

> **Note:** In the next sections, only the notifications and actions that are strictly necessary for the purpose of ONU authentication and eOMCI/vOMCI decision are indicated.

6.2.2 Scenario 1: Mgt Plane authenticates ONU and manages it via vOMCI

In Scenario 1 as the OLT is not able to authenticate the ONU (for instance no matching vANI found, no capability to parse vANI, or parsing vANI globally disabled,..) it will notify the Management Plane with a notification about the unknown ONU, just providing the credentials it could gather from the ONU, hoping that the Management Plane will be able to authenticate the ONU and report the result. Ultimately the Management Plane will issue an action to the OLT telling the success (or failure) of the authentication and in case of success:

- The vANI YANG leaf reference corresponding to the ONU and the ONU name (key in the Management Plane ONU aggregation function).
- That the ONU management mode for this ONU is vOMCI

Upon reception of this action, the OLT will check that the indicated vANI is not configured with an ONU management mode indicating “eOMCI”; in a consistent network configuration, this may not happen: the vANI ONU management mode would be configured as “vOMCI” or possibly just not configured. At that stage, the OLT starts transport and forwarding functions for the ONU, such as generating bandwidth maps for ONU upstream traffic. It is up to the Management plane to manage the ONU through vOMCI and make it ready to forward traffic.

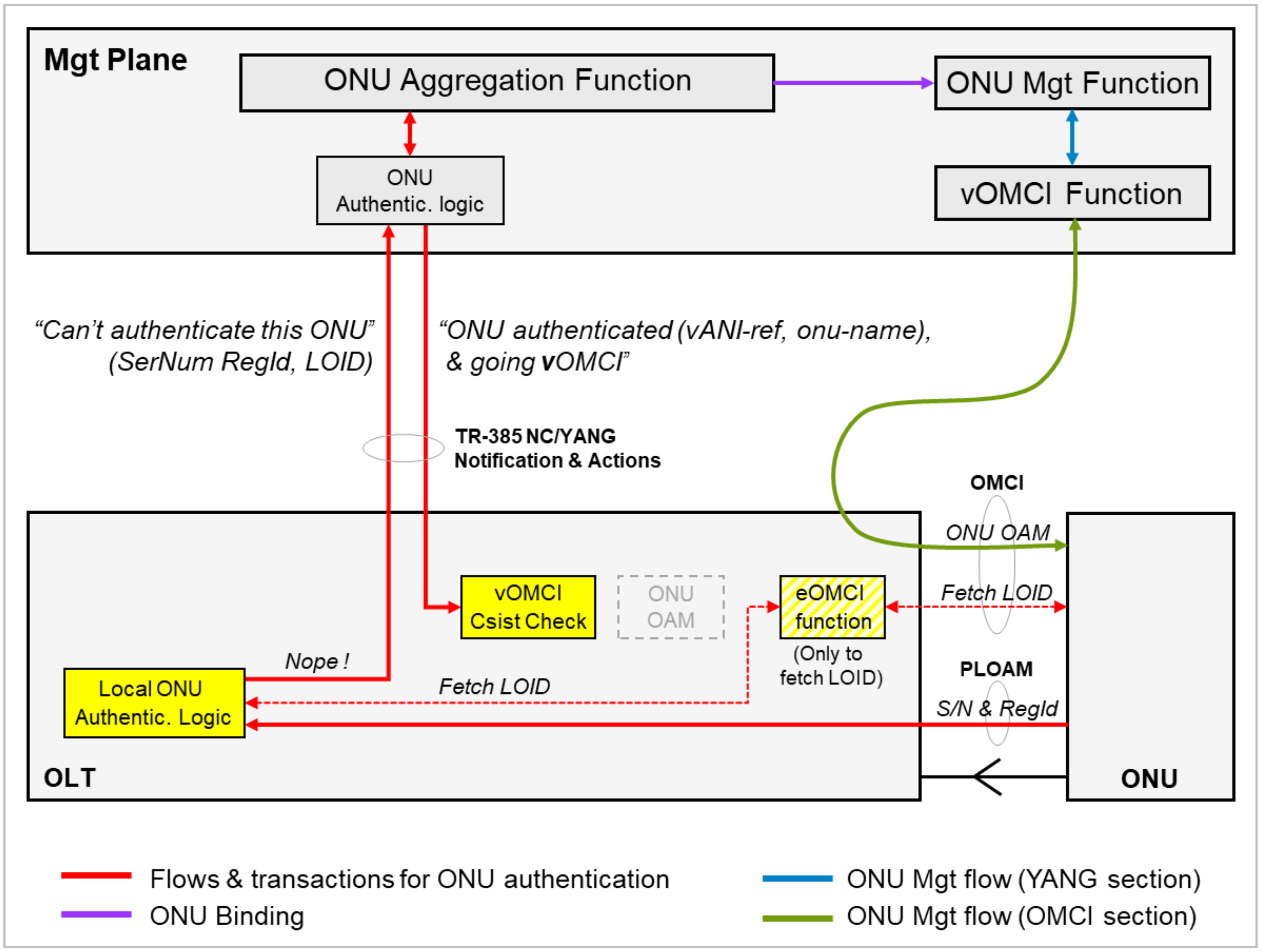

Mgt Plane
ONU Aggregation Function
ONU Mgt Function
ONU Authentic. logic
vOMCI Function
“Can’t authenticate this ONU” (SerNum RegId, LOID)
“ONU authenticated (vANI-ref, onu-name), & going vOMCI”
TR-385 NC/YANG Notification & Actions
OMCI
ONU OAM
Fetch LOID
vOMCI Csist Check
ONU OAM
eOMCI function
(Only to fetch LOID)
Nope !
Fetch LOID
Local ONU Authentic. Logic
PLOAM
S/N & RegId
OLT
ONU
Flows & transactions for ONU authentication
ONU Binding
ONU Mgt flow (YANG section)
ONU Mgt flow (OMCI section)

Figure 6-2 - Interactions for Scenario 1

6.2.3 Scenario 2: OLT authenticates the ONU, Mgt Plane manages it via vOMCI

After the OLT has authenticated the ONU by finding a matching vANI, the OLT determines that the planned management mode for the ONU is vOMCI - as typically configured in the vANI or by considering that it is not able to provide eOMCI for this ONU anyway. It will send a notification indicating so and containing the vANI corresponding to the ONU. This notification will allow the Management Plane to know the “onu-name”, key in its ONU Aggregation function.

At that stage, the OLT starts initializing the local transport and forwarding functions for the ONU, such as generating bandwidth maps for ONU upstream traffic.

On its side, upon reception of the notification, the Management Plane will check that the indicated ONU is indeed consistently configured in the ONU aggregation function with an ONU management mode indicating “vOMCI”; in a correct network configuration, for scenario 2, this must be the case. The Management Plane then starts managing the ONU through vOMCI and makes it ready to forward traffic.

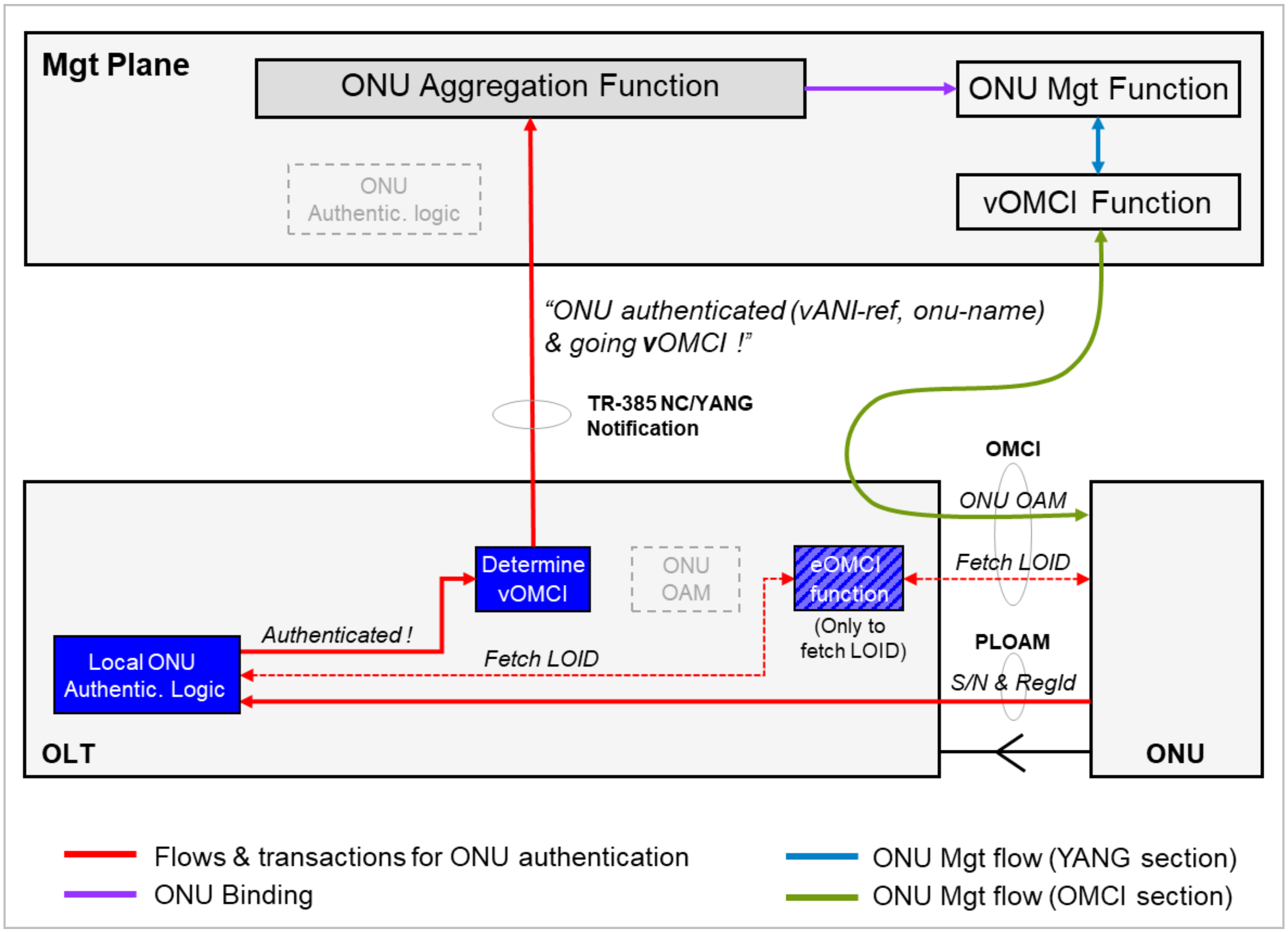


Figure 6-3 - Interactions for Scenario 2

6.2.4 Scenario 3: Mgt Plane authenticates ONU, OLT manages it via eOMCI

In Scenario 3 as the OLT is not able to authenticate the ONU (for instance no matching vANI found, no capability to parse vANI, or parsing the vANI is globally disabled,..) it will notify the Management Plane with a notification about the unknown ONU, just providing the credentials it could gather from the ONU and expecting that the Management Plane will be able to authenticate the ONU and report the result. Ultimately the Management Plane will issue an action to the OLT telling the success (or failure) of the authentication and in case of success:

- The vANI YANG leaf reference corresponding to the ONU and the ONU name (key in the Management Plane ONU aggregation function).
- That the ONU management mode for this ONU is eOMCI

Upon reception of this action, the OLT will check that the indicated vANI is not configured with an ONU management mode indicating “vOMCI”; in a consistent network configuration, this may not happen, the vANI ONU management mode would be configured as “eOMCI” or possibly just not configured. At that stage, the OLT starts

- initializing the local transport and forwarding functions for the ONU, such as generating bandwidth maps for ONU upstream traffic.
- managing the ONU through eOMCI and make it ready to forward traffic. The ONU configuration is retrieved through the ANI associated with the vANI (as per TR-385 in Combined NE Mode); note that if an “onu-name” is configured on the vANI, it must match the one provided by the Management Plane.

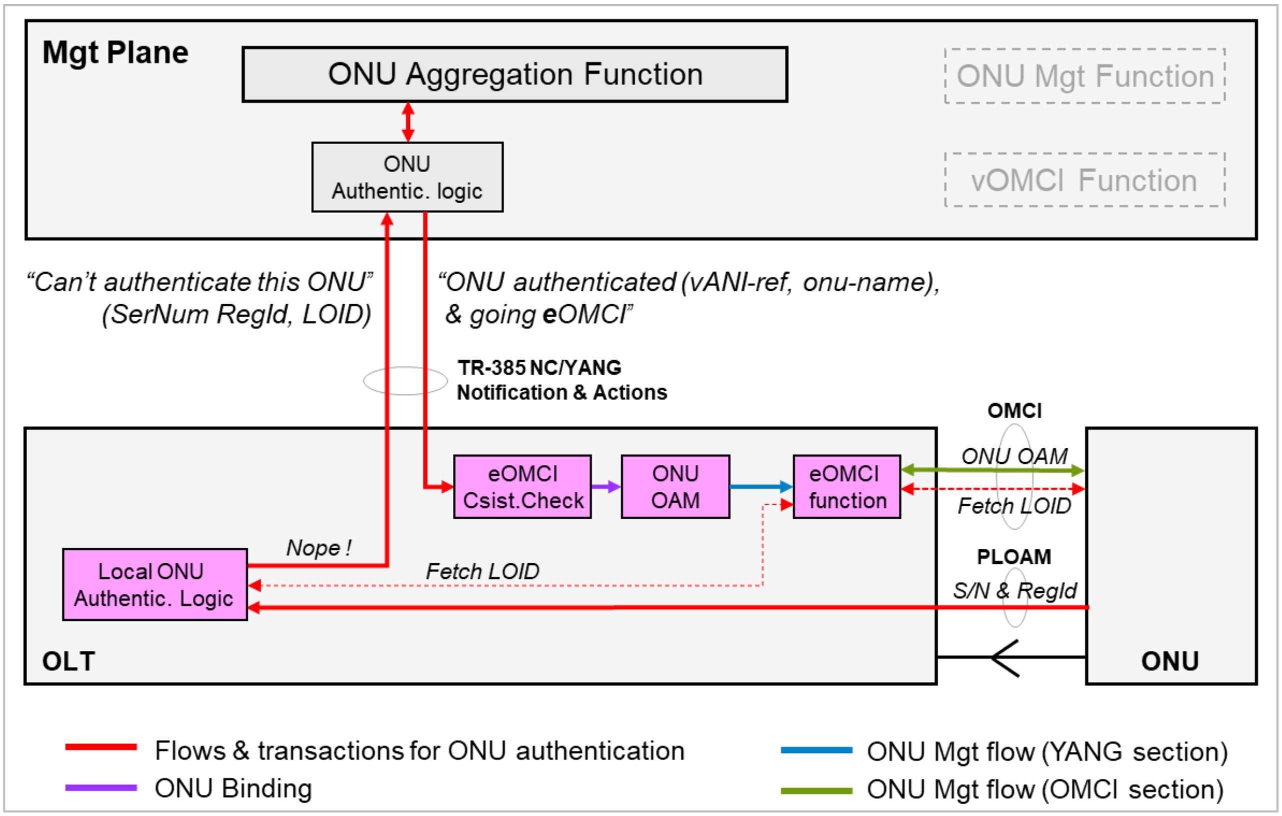

Mgt Plane
ONU Aggregation Function
ONU Mgt Function
ONU Authentic. logic
vOMCI Function
“Can’t authenticate this ONU” (SerNum RegId, LOID)
“ONU authenticated (vANI-ref, onu-name), & going eOMCI”
TR-385 NC/YANG Notification & Actions
OMCI
ONU OAM
Fetch LOID
PLOAM
S/N & RegId
eOMCI Csist.Check
ONU OAM
eOMCI function
Nope !
Fetch LOID
Local ONU Authentic. Logic
OLT
ONU
Flows & transactions for ONU authentication
ONU Binding
ONU Mgt flow (YANG section)
ONU Mgt flow (OMCI section)

Figure 6-4 - Interactions for Scenario 3

6.2.5 Scenario 4: OLT authenticates ONU and manages it via eOMCI

After the OLT has authenticated the ONU by finding a matching vANI, the OLT determines that the planned management mode for the ONU is eOMCI - as typically configured in the vANI or if not configured, by considering that it is able to provide eOMCI for this ONU anyway.

At that stage, the OLT starts

- initializing the local transport and forwarding functions for the ONU, such as generating bandwidth maps for ONU upstream traffic.
- managing the ONU through eOMCI and make it ready to forward traffic. The ONU configuration is retrieved through the ANI associated with the vANI (as per TR-385 in Combined NE Mode).

Note that in scenario 4 there is no strict need for the OLT to send a notification to the Management Plane telling about the authenticated ONU and the fact that it will be managed by eOMCI since in Scenario 4 the OLT can proceed without any guidance from the Management Plane. Such a notification can be issued, though, for general information of the Management Plane.

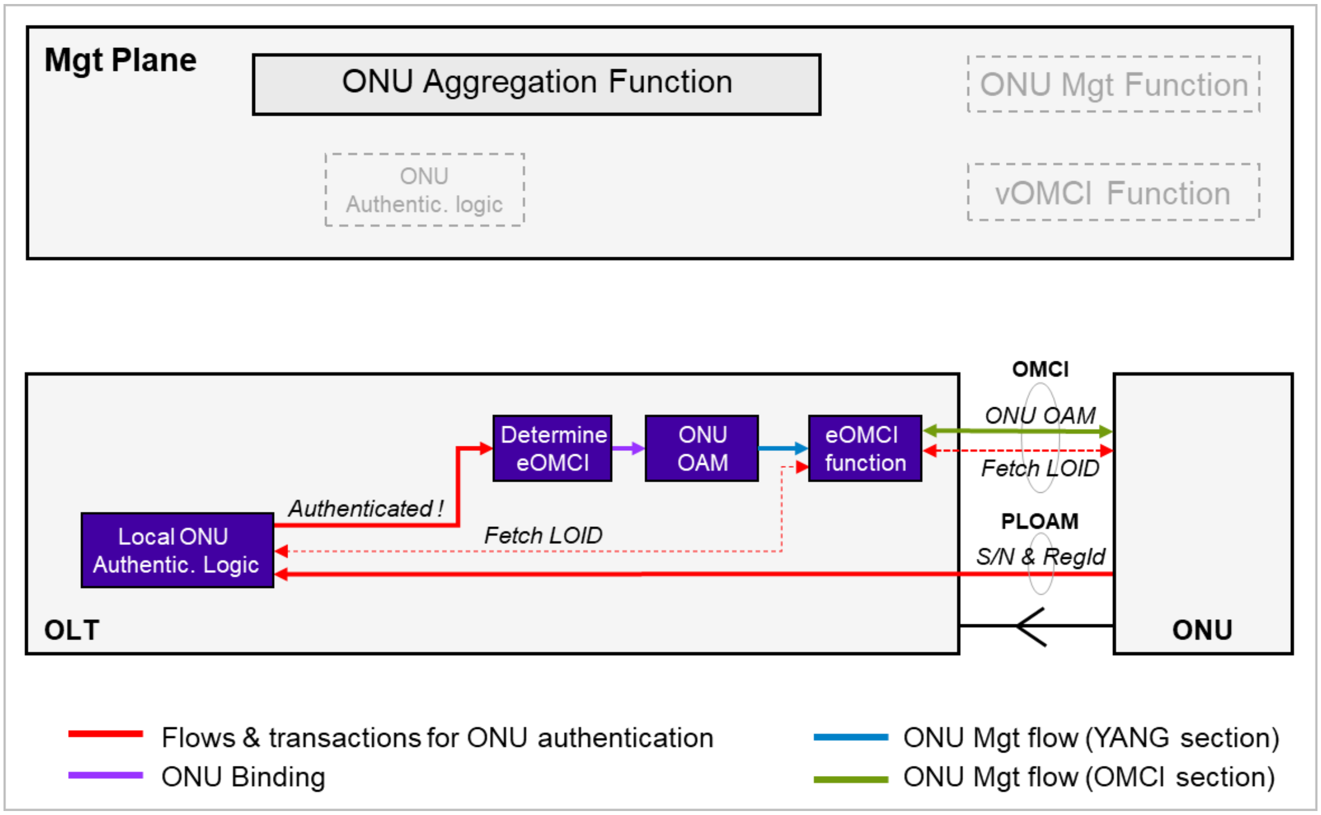


Figure 6-5 - Interactions for Scenario 4

6.2.6 *OLT* Detailed Decision Tree

The following decision tree integrates the details of all scenarios seen in sections 6.2.2 to 6.2.5 seen from the perspective of the *OLT*. It is actually a zoomed-in version of Figure 6-1.

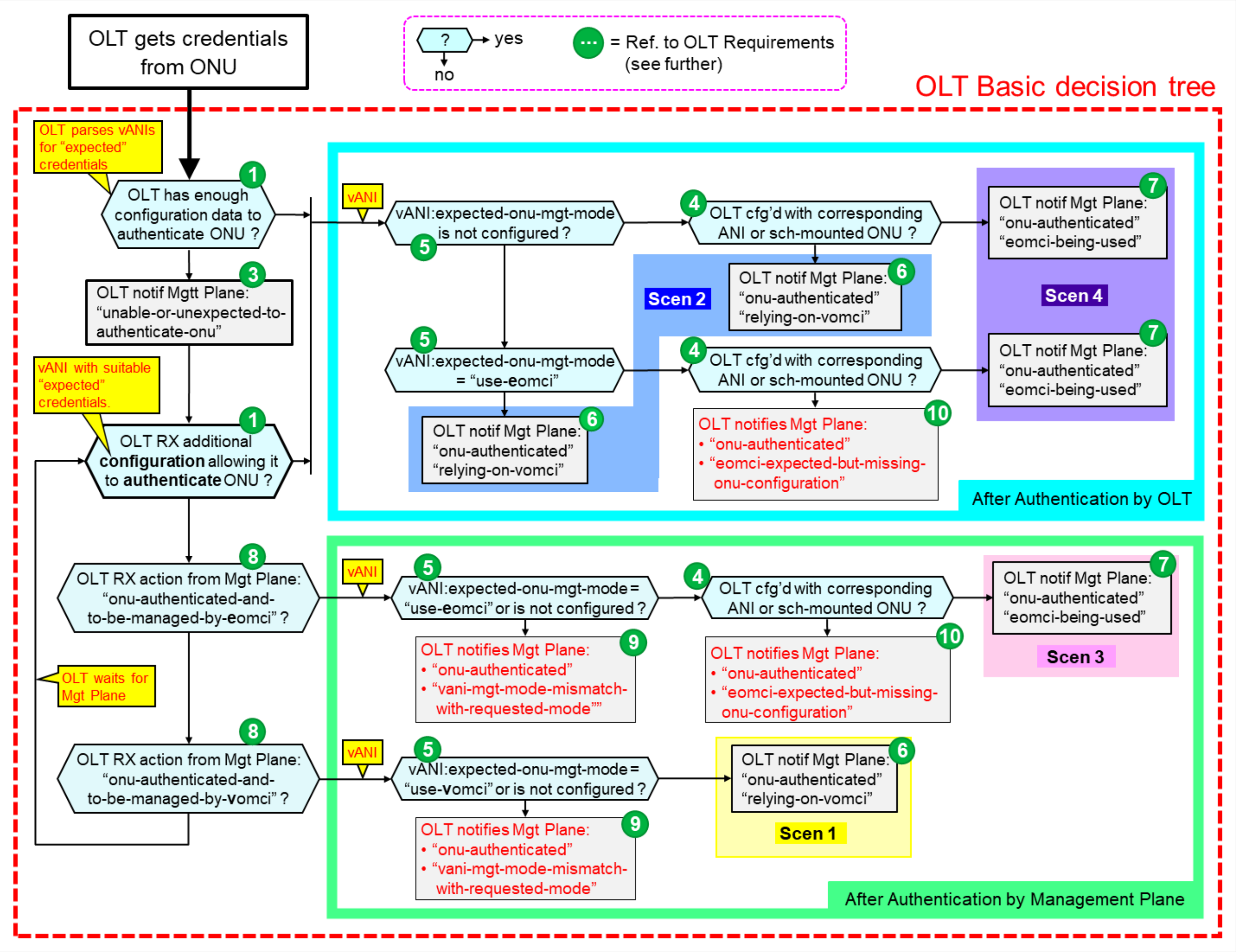

OLT gets credentials from ONU
? yes no
… = Ref. to OLT Requirements (see further)
OLT Basic decision tree
OLT parses vANIs for "expected" credentials
1 OLT has enough configuration data to authenticate ONU ?
3 OLT notif Mgtt Plane: "unable-or-unexpected-to-authenticate-onu"
vANI with suitable "expected" credentials.
1 OLT RX additional configuration allowing it to authenticate ONU ?
8 OLT RX action from Mgt Plane: "onu-authenticated-and-to-be-managed-by-eomci" ?
OLT waits for Mgt Plane
8 OLT RX action from Mgt Plane: "onu-authenticated-and-to-be-managed-by-vomci" ?
vANI
5 vANI:expected-onu-mgt-mode is not configured ?
4 OLT cfg'd with corresponding ANI or sch-mounted ONU ?
7 OLT notif Mgt Plane: "onu-authenticated" "eomci-being-used"
Scen 2
6 OLT notif Mgt Plane: "onu-authenticated" "relying-on-vomci"
Scen 4
5 vANI:expected-onu-mgt-mode = "use-eomci"
4 OLT cfg'd with corresponding ANI or sch-mounted ONU ?
7 OLT notif Mgt Plane: "onu-authenticated" "eomci-being-used"
6 OLT notif Mgt Plane: "onu-authenticated" "relying-on-vomci"
10 OLT notifies Mgt Plane: • "onu-authenticated" • "eomci-expected-but-missing-onu-configuration"
After Authentication by OLT
vANI
5 vANI:expected-onu-mgt-mode = "use-eomci" or is not configured ?
4 OLT cfg'd with corresponding ANI or sch-mounted ONU ?
7 OLT notif Mgt Plane: "onu-authenticated" "eomci-being-used"
Scen 3
9 OLT notifies Mgt Plane: • "onu-authenticated" • "vani-mgt-mode-mismatch-with-requested-mode""
10 OLT notifies Mgt Plane: • "onu-authenticated" • "eomci-expected-but-missing-onu-configuration"
vANI
5 vANI:expected-onu-mgt-mode = "use-vomci" or is not configured ?
6 OLT notif Mgt Plane: "onu-authenticated" "relying-on-vomci"
Scen 1
9 OLT notifies Mgt Plane: • "onu-authenticated" • "vani-mgt-mode-mismatch-with-requested-mode"
After Authentication by Management Plane

Figure 6-6 - OLT Detailed Basic Decision Tree

This decision tree can be refined by adding the capability for the OLT to unconditionally skip ONU authentication for any ONUs of a given channel-partition. Doing so could be useful to save OLT processing power in some deployment. This refinement comes as an addition to Figure 6-6 as illustrated below:

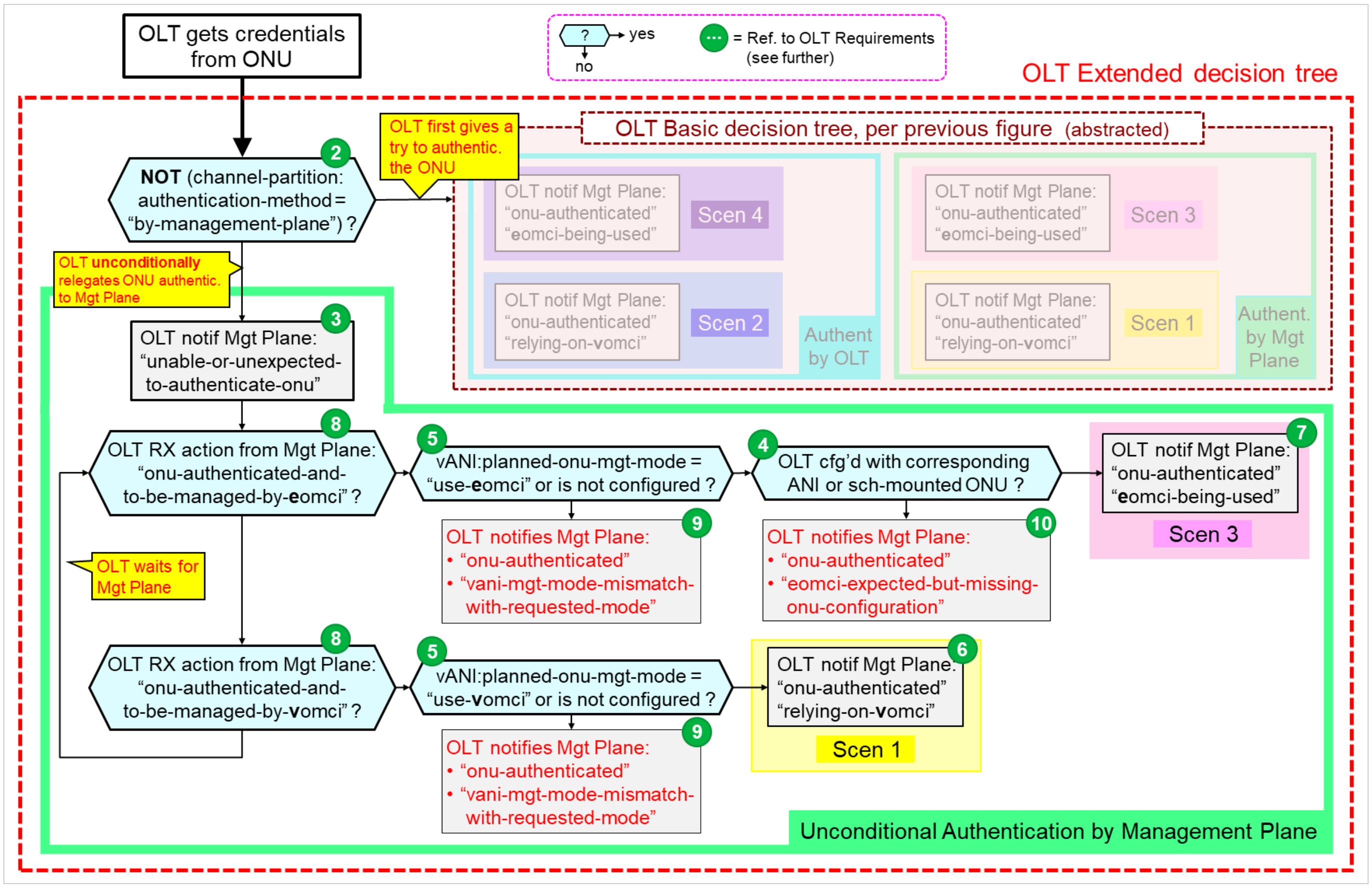

OLT gets credentials from ONU
? yes no
= Ref. to OLT Requirements (see further)
OLT Extended decision tree
OLT Basic decision tree, per previous figure (abstracted)
OLT first gives a try to authentic. the ONU
2
NOT (channel-partition: authentication-method = “by-management-plane”) ?
OLT unconditionally relegates ONU authentic. to Mgt Plane
3
OLT notif Mgt Plane: “unable-or-unexpected-to-authenticate-onu”
OLT notif Mgt Plane: “onu-authenticated” “eomci-being-used” Scen 4
OLT notif Mgt Plane: “onu-authenticated” “relying-on-vomci” Scen 2
Authent by OLT
OLT notif Mgt Plane: “onu-authenticated” “eomci-being-used” Scen 3
OLT notif Mgt Plane: “onu-authenticated” “relying-on-vomci” Scen 1
Authent. by Mgt Plane
8
OLT RX action from Mgt Plane: “onu-authenticated-and-to-be-managed-by-eomci” ?
5
vANI:planned-onu-mgt-mode = “use-eomci” or is not configured ?
4
OLT cfg’d with corresponding ANI or sch-mounted ONU ?
7
OLT notif Mgt Plane: “onu-authenticated” “eomci-being-used”
Scen 3
9
OLT notifies Mgt Plane: • “onu-authenticated” • “vani-mgt-mode-mismatch-with-requested-mode”
10
OLT notifies Mgt Plane: • “onu-authenticated” • “eomci-expected-but-missing-onu-configuration”
OLT waits for Mgt Plane
8
OLT RX action from Mgt Plane: “onu-authenticated-and-to-be-managed-by-vomci” ?
5
vANI:planned-onu-mgt-mode = “use-vomci” or is not configured ?
6
OLT notif Mgt Plane: “onu-authenticated” “relying-on-vomci”
Scen 1
9
OLT notifies Mgt Plane: • “onu-authenticated” • “vani-mgt-mode-mismatch-with-requested-mode”
Unconditional Authentication by Management Plane

Figure 6-7 - OLT Detailed Refined Decision Tree

6.2.7 *Management Plane* Detailed Decision Tree

The following decision tree integrates the details of all scenarios seen in previous sections 6.2.2 to 6.2.5 as seen from the perspective of the *Management Plane*. It closely interworks with the OLT decision tree of section 6.2.6 by means of notification and action.

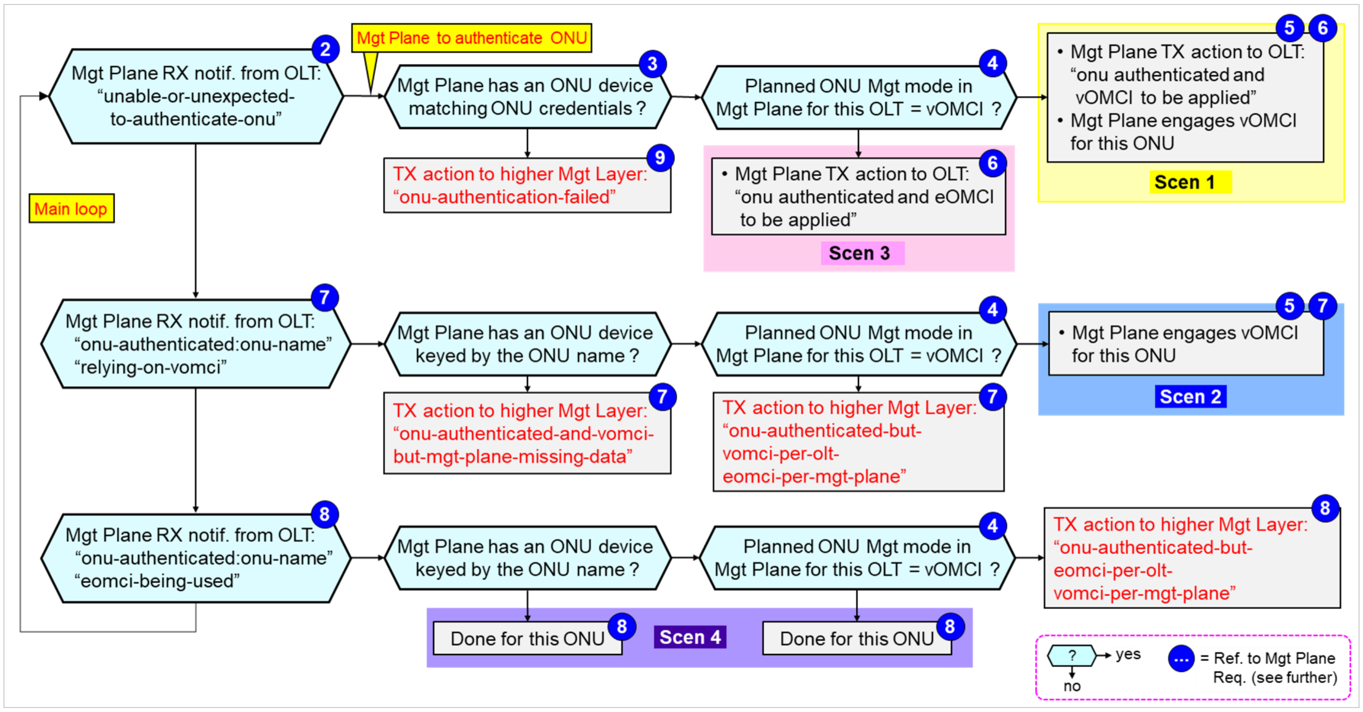

Mgt Plane to authenticate ONU
Mgt Plane RX notif. from OLT: "unable-or-unexpected-to-authenticate-onu"
2
Mgt Plane has an ONU device matching ONU credentials ?
3
Planned ONU Mgt mode in Mgt Plane for this OLT = vOMCI ?
4
• Mgt Plane TX action to OLT: "onu authenticated and vOMCI to be applied"
• Mgt Plane engages vOMCI for this ONU
5
6
Scen 1
Main loop
TX action to higher Mgt Layer: "onu-authentication-failed"
9
• Mgt Plane TX action to OLT: "onu authenticated and eOMCI to be applied"
6
Scen 3
Mgt Plane RX notif. from OLT: "onu-authenticated:onu-name" "relying-on-vomci"
7
Mgt Plane has an ONU device keyed by the ONU name ?
Planned ONU Mgt mode in Mgt Plane for this OLT = vOMCI ?
4
• Mgt Plane engages vOMCI for this ONU
5
7
Scen 2
TX action to higher Mgt Layer: "onu-authenticated-and-vomci-but-mgt-plane-missing-data"
7
TX action to higher Mgt Layer: "onu-authenticated-but-vomci-per-olt-eomci-per-mgt-plane"
7
Mgt Plane RX notif. from OLT: "onu-authenticated:onu-name" "eomci-being-used"
8
Mgt Plane has an ONU device keyed by the ONU name ?
Planned ONU Mgt mode in Mgt Plane for this OLT = vOMCI ?
4
TX action to higher Mgt Layer: "onu-authenticated-but-eomci-per-olt-vomci-per-mgt-plane"
8
Done for this ONU
8
Scen 4
Done for this ONU
8
? yes
no
... = Ref. to Mgt Plane Req. (see further)

Figure 6-8 - Management Plane Detailed Decision Tree

7 When D-OLT performs ONU authentication on behalf of OLT

The general goal of OLT disaggregation is to realize some function(s) of the OLT by means of a Disaggregated OLT (D-OLT) software component, remoted from the Physical OLT (pOLT).

When it comes to ONU authentication, a remote D-OLT component performs ONU authentication on behalf of the pOLT acting a kind of remote co-processor for the pOLT. This is depicted in Figure 7-1 below.

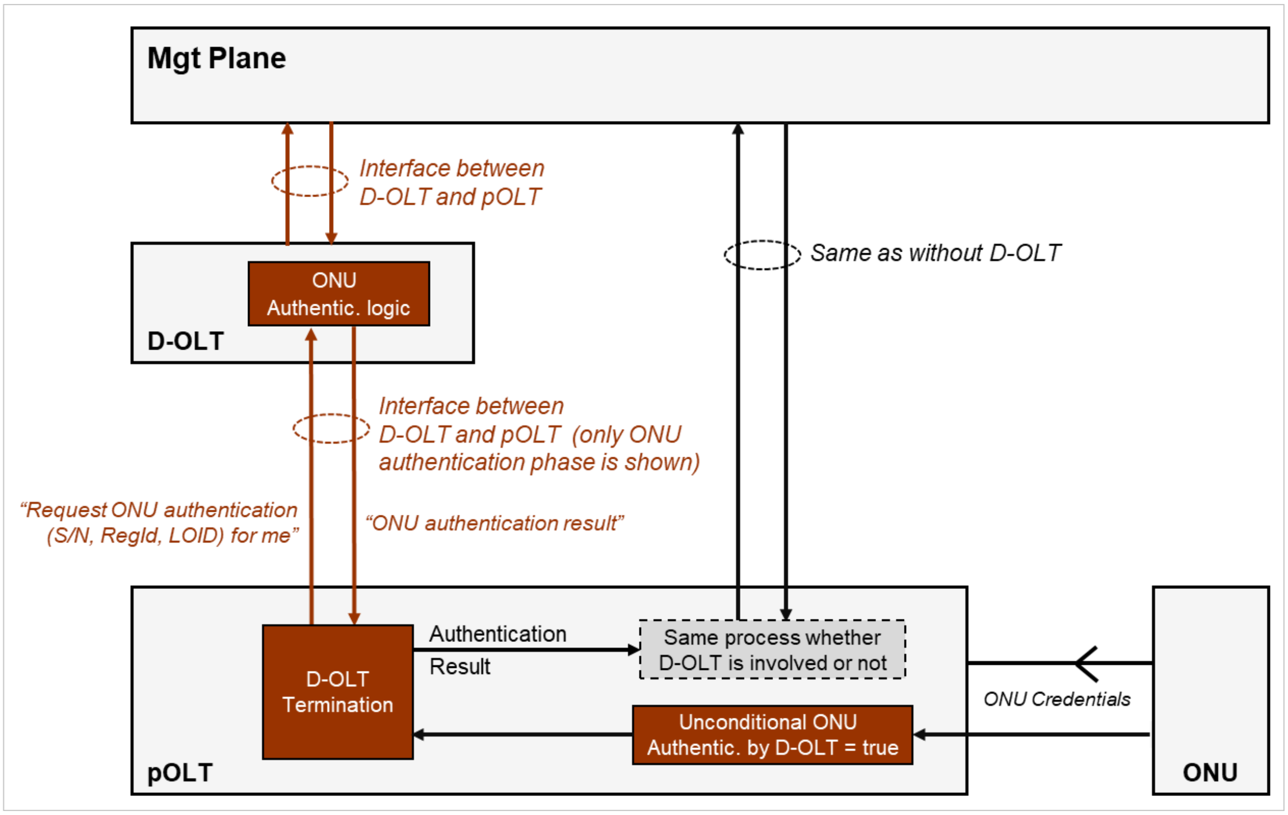

Mgt Plane
Interface between D-OLT and pOLT
Same as without D-OLT
ONU Authentic. logic
D-OLT
Interface between D-OLT and pOLT (only ONU authentication phase is shown)
"Request ONU authentication (S/N, RegId, LOID) for me"
"ONU authentication result"
D-OLT Termination
Authentication Result
Same process whether D-OLT is involved or not
Unconditional ONU Authentic. by D-OLT = true
ONU Credentials
pOLT
ONU

Figure 7-1 - ONU authentication realized by D-OLT Software Component

When D-OLT ONU authentication function is enabled on the pOLT, for each ONU that shows-up the pOLT asks D-OLT to do the authentication on its behalf. When the D-OLT reports the ONU authentication result, positive or negative, the pOLT proceeds as if it had performed itself the ONU authentication function.

A typical use of D-OLT ONU authentication in the case of Scenario 2 and 4, where successful ONU authentication is done by the D-OLT rather than by the pOLT itself.

7.1 Interface between D-OLT and Management plane

TR-489 only addresses the aspects of this interface that relate to ONU authentication. Other aspects of the interface are beyond the scope of this Technical Report.

For the purpose of TR-489, the following interactions are expected to take place between the Management Plane and the D-OLT:

1. Management Plane configures the identification of the pOLT for which the D-OLT will perform ONU authentication, unconditionally for all ONUs showing up in the pOLT.
2. Management Plane configures the list of all ONUs to be authenticated in the form of a list of vANIs (as known by the pOLT) per regular TR-385 YANG; in particular each vANI in the D-OLT is configured with all credentials required to authenticate the corresponding ONU.
3. Optionally, the D-OLT can notify the Management Plane that it could or could not authenticate an ONU. Note that this interaction is not strictly necessary because this information will be included in the notification anyway sent by the pOLT to the Management Plane, independently whether a D-OLT is involved or not (ref. R-OLT_3, R-OLT_6 and R-OLT_7). Note also that when supported, this D-OLT notification is only entitled to report the ONU authentication status to the management Plane. This is in contrast with R-OLT_6 and R-OLT_7 that besides successful ONU authentication also report whether the pOLT has determined that vOMCI or vOMCI is to be applied to the ONU.

7.2 Interface between D-OLT and pOLT

TR-489 only addresses the aspects of this interface that relate to ONU authentication. Other aspects of the interface are beyond the scope of this TR.

For the purpose of TR-489, the following interactions are expected to take place between D-OLT an pOLT as part of TR-385 Management interface:

1. D-OLT configures the pOLT to make it aware that ONU authentication is exclusively to be done by the D-OLT.
2. When an ONU shows-up, the pOLT requests D-OLT to authenticate it via a notification, including in the notification the credentials provided by the ONU.
3. D-OLT indicates back to the pOLT via an action the result of the authentication, positive or negative and, if positive, the vANI reference corresponding to the ONU.

It can be noted that interactions 2. and 3. above between D-OLT and pOLT can be mapped to the same interactions as respectively between Management plane and OLT, as described in Section 6.

7.3 Decision tree in OLT when D-OLT is in charge of ONU authentication

Figure 7-2 shows the additional branches - highlighted in pink - to the OLT decision tree when D-OLT is in charge of ONU authentication.

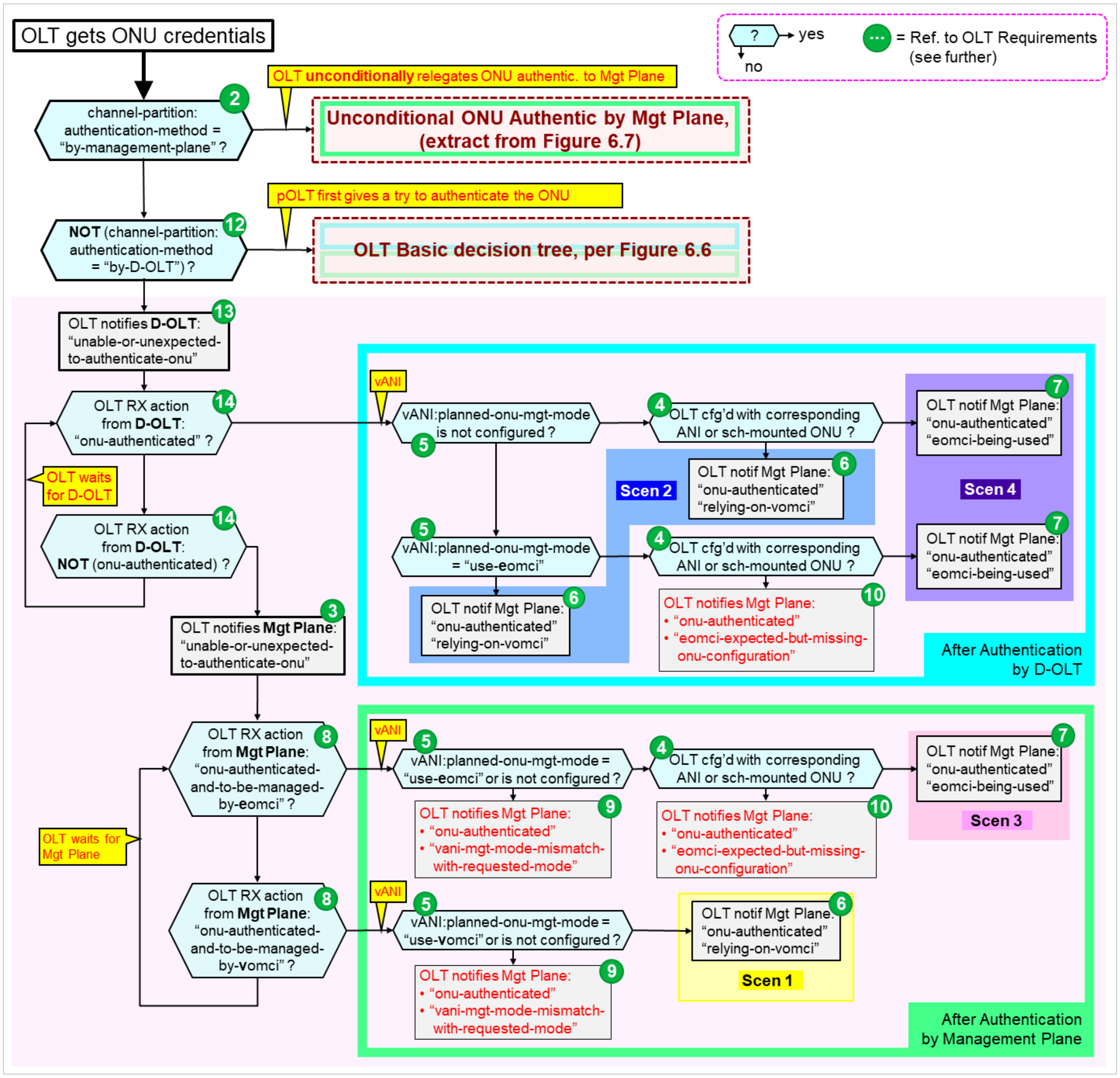

OLT gets ONU credentials
? yes
no
... = Ref. to OLT Requirements (see further)
OLT unconditionally relegates ONU authentic. to Mgt Plane
2
channel-partition: authentication-method = "by-management-plane"?
Unconditional ONU Authentic by Mgt Plane, (extract from Figure 6.7)
pOLT first gives a try to authenticate the ONU
12
NOT (channel-partition: authentication-method = "by-D-OLT")?
OLT Basic decision tree, per Figure 6.6
13
OLT notifies D-OLT: "unable-or-unexpected-to-authenticate-onu"
14
OLT RX action from D-OLT: "onu-authenticated"?
OLT waits for D-OLT
14
OLT RX action from D-OLT: NOT (onu-authenticated)?
3
OLT notifies Mgt Plane: "unable-or-unexpected-to-authenticate-onu"
vANI
5
vANI:planned-onu-mgt-mode is not configured?
4
OLT cfg'd with corresponding ANI or sch-mounted ONU ?
7
OLT notif Mgt Plane: "onu-authenticated" "eomci-being-used"
Scen 4
6
OLT notif Mgt Plane: "onu-authenticated" "relying-on-vomci"
Scen 2
5
vANI:planned-onu-mgt-mode = "use-eomci"
4
OLT cfg'd with corresponding ANI or sch-mounted ONU ?
7
OLT notif Mgt Plane: "onu-authenticated" "eomci-being-used"
6
OLT notif Mgt Plane: "onu-authenticated" "relying-on-vomci"
10
OLT notifies Mgt Plane:
• "onu-authenticated"
• "eomci-expected-but-missing-onu-configuration"
After Authentication by D-OLT
8
OLT RX action from Mgt Plane: "onu-authenticated-and-to-be-managed-by-eomci"?
OLT waits for Mgt Plane
vANI
5
vANI:planned-onu-mgt-mode = "use-eomci" or is not configured?
4
OLT cfg'd with corresponding ANI or sch-mounted ONU ?
7
OLT notif Mgt Plane: "onu-authenticated" "eomci-being-used"
Scen 3
9
OLT notifies Mgt Plane:
• "onu-authenticated"
• "vani-mgt-mode-mismatch-with-requested-mode"
10
OLT notifies Mgt Plane:
• "onu-authenticated"
• "eomci-expected-but-missing-onu-configuration"
8
OLT RX action from Mgt Plane: "onu-authenticated-and-to-be-managed-by-vomci"?
vANI
5
vANI:planned-onu-mgt-mode = "use-vomci" or is not configured?
6
OLT notif Mgt Plane: "onu-authenticated" "relying-on-vomci"
Scen 1
9
OLT notifies Mgt Plane:
• "onu-authenticated"
• "vani-mgt-mode-mismatch-with-requested-mode"
After Authentication by Management Plane

Figure 7-2 - OLT decision tree with D-OLT performing ONU Authentication

8 Requirements

This chapter captures the requirements for all scenarios for ONU Authentication and the decision whether an ONU should be managed by eOMCI or vOMCI, set on the OLT, the D-OLT and the Management Plane in order to organize their specific behavior and mutual interactions. Requirements will be expressed assuming the following network architecture:

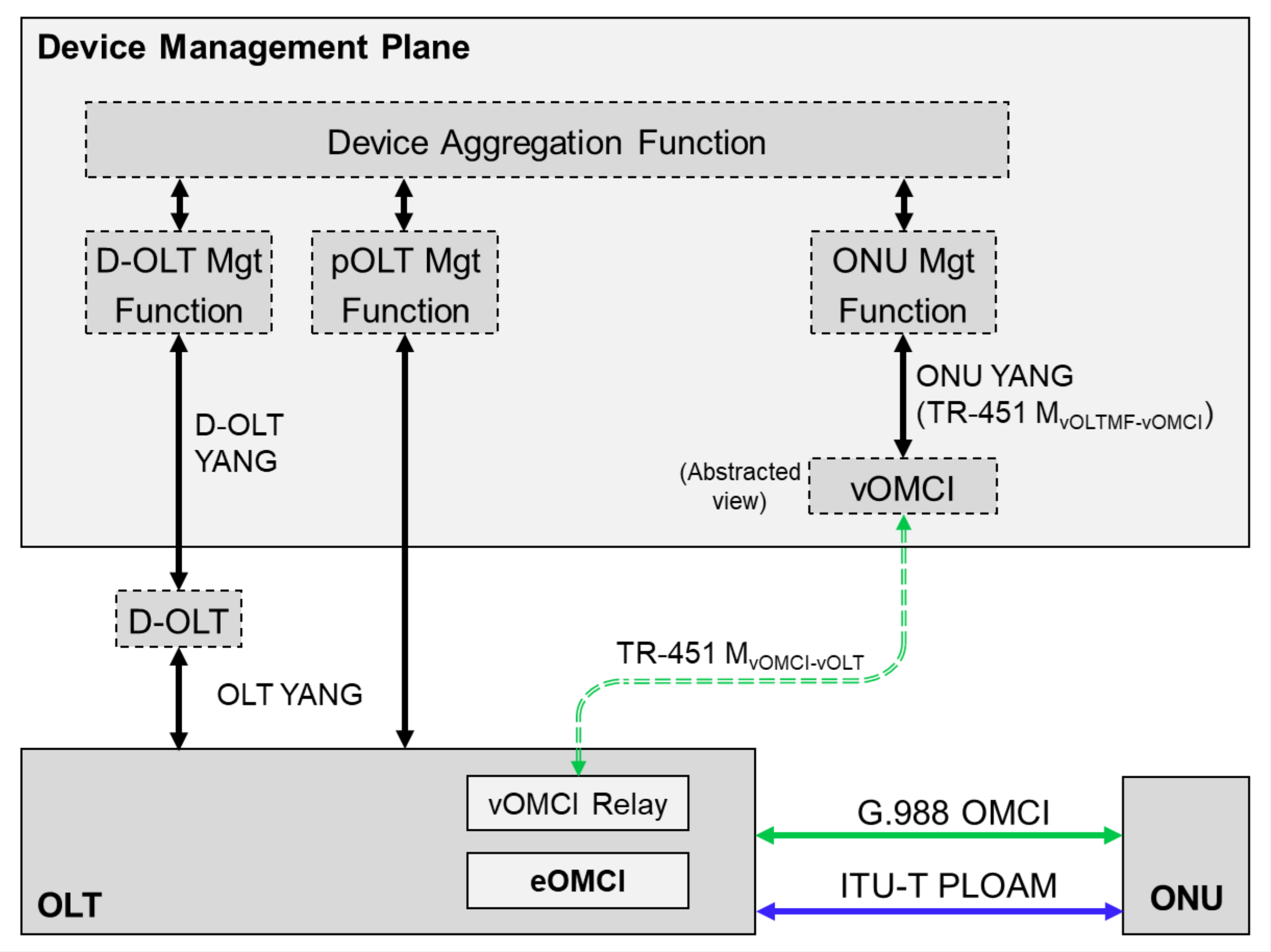


Figure 8-1 - Network Architecture for Requirements

8.1 General Requirements

R-GEN_1 – For what concerns ONU Authentication and the decision to have ONU management done by the OLT (using eOMCI) or by the Management Plane (using vOMCI), the YANG models of the ONU Aggregation Function in the Device Management Plane and of the OLT Device must be able to support all four scenarios depicted in Figure 5-2, Figure 5-3, Figure 5-4 and Figure 5-5, concurrently on the same channel termination, on a per ONU basis.

R-GEN_2 – The YANG models of the ONU Aggregation Function in the Device Management Plane and of the OLT Device must be able to support ONU authentication with any combination of the following credentials, selected on a per ONU basis:

- Serial Number
- Registration ID
- LOID

8.2 Requirements for the OLT

The following OLT requirements are identified. Note that for the ease of reference each such requirement “R-OLT_i” is reported in Figure 6-6 and Figure 6-7 as a white number “ i ” on a green circular background:

R-OLT_1 – The OLT MUST have the capability to be configured by the Management Plane with information allowing the OLT to authenticate an ONU that starts its activation cycle with the OLT (ref for instance to ITU-T G.984.3, Clause 3.2.1 and ITU.T G.989 Clause 3.2.3.1.).

R-OLT_2 – The OLT MUST have the capability to be configured by the Management Plane so that all ONUs that show-up on a given channel-partition are exclusively authenticated by the Management Plane.

R-OLT_3 – The OLT MUST notify the Management Plane of an ONU that shows-up and that it is not able or not expected to authenticate.

R-OLT_4 – The OLT MUST have the capability to be configured by the Management Plane with information allowing the OLT to manage an ONU via a local eOMCI function.

R-OLT_5 – The OLT MUST have the capability to be configured by the Management Plane so that a given authenticated ONU, known by its vANI, is expected to be managed by an eOMCI local function or a vOMCI function. This “onu-management-mode” configuration is done at vANI level.

R-OLT_6 – The OLT MUST notify the Management Plane of an authenticated ONU that shows-up and that it expects to be managed with vOMCI.

R-OLT_7 – The OLT MUST notify the Management Plane of an authenticated ONU that has shown-up and that it will manage with eOMCI.

R-OLT_8 – The OLT MUST have the capability to accept an action from the Management Plane indicating that an ONU is confirmed authenticated (or not) and - if authenticated - the vANI reference corresponding to the ONU and whether the Management Plane expects the ONU to be managed by a vOMCI entity or by an eOMCI function in the OLT.

R-OLT_9 – The OLT MUST notify the Management Plane that for a given ONU, its vANI “onu-management-mode” conflicts with the “onu-management-mode” provided by the Management Plane per R-OLT_8.

R-OLT_10 – The OLT MUST notify the Management Plane that it is expected to manage the ONU via eOMCI but lacks the configuration to do so (missing ANI or missing schema-mounted ONU device).

R-OLT_11 – The OLT SHOULD have the capability to query the LOID of a yet unknown ONU with an eOMCI function. This capability should be present even when the OLT is not expected to manage any ONUs itself.

R-OLT_12 – In case a D-OLT software component is to be used for ONU authentication, the physical OLT MUST have the capability to be configured by the D-OLT software component (or possibly by the Management Plane) so that the physical OLT unconditionally requests the D-OLT to authenticate all ONUs showing-up on a given channel partition, instead of attempting the authentication itself.

R-OLT_13 – In case a D-OLT software component is to be used for ONU authentication, the physical OLT MUST notify the D-OLT that an ONU needs to be authenticated, including the credentials provided by the ONU.

R-OLT_14 – In case a D-OLT software component is to be used for ONU authentication, the physical OLT MUST have the capability to accept an action from the D-OLT reporting that an ONU is confirmed authenticated (or not) and, if authenticated, the vANI reference corresponding to the ONU. Upon reception of such a action, the physical OLT MUST similarly proceed as if the ONU authentication had been locally performed (or attempted).

8.3 Requirements for the Management Plane

The following requirements on the Management Plane are identified. Note that for the ease of reference each such “R-MP_i” requirement is reported in Figure 6-8 as a white number “ i ” on a dark blue circular background:

R-MP_1 – The Management Plane MUST be able to configure the OLT so that the OLT is able to fulfill the requirements listed in section 8.2.

R-MP_2 – When receiving a notification from the OLT indicating that it is not able or expected to authenticate an ONU (R-OLT_3) the Management Plane MUST engage its ONU Aggregation function to attempt ONU authentication. This MAY involve the Management Plane to further engage a vOMCI function when additional credential information is required from the ONU via OMCI.

R-MP_3 – For each ONU that the Management Plane intends to authenticate itself, it must be possible to configure the ONU Aggregation function of the Management Plane with suitable ONU credential information.

R-MP_4 – For each ONU that the ONU Aggregation function of the Management Plane is aware of, the ONU Aggregation function of the Management Plane MUST be configured whether it is expected to manage the ONU with a vOMCI function or conversely whether the ONU must be managed by the OLT eOMCI function. This information must be configured per ONU and per OLT expected to host the ONU (the "per OLT" is to support ONU nomadism).

R-MP_5 – For each ONU that the Management Plane intends to manage itself via vOMCI, the ONU Aggregation function of the Management Plane MUST be configured with suitable information to allow ONU management with a vOMCI function.

R-MP_6 – The Management Plane MUST signal the OLT via an action the result, positive or negative, of an ONU authentication it has attempted. In particular, upon successful authentication, the Management Plane MUST indicate to the OLT the vANI, as known by the OLT, and the ONU name (key in the ONU Aggregation function in the Management Plane) corresponding to the ONU. It SHOULD also indicate whether the ONU must be managed by the eOMCI function in the OLT or instead will be managed by a vOMCI entity (cf R-OLT_8). In the latter case the Management Plane MUST directly engage the proper vOMCI entity to manage the ONU.

R-MP_7 – When receiving a notification from the OLT indicating successful ONU authentication and the expectation that the ONU is to be managed via vOMCI (R-OLT_6), the Management Plane MUST verify whether it is indeed expected to do so in which case it MUST engage its ONU Aggregation function to identify a vOMCI function suitable for managing the ONU. If it is not the case because the Management Plane expects the ONU to be managed by the OLT via eOMCI, or has simply no awareness of the ONU, the Management Plane MUST escalate higher up, respectively, the inconsistency with the OLT or that it misses the ONU configuration.

R-MP_8 – When receiving a notification from the OLT indicating that an ONU is successfully authenticated and that the ONU is currently managed via eOMCI (R-OLT_7), the Management Plane MUST verify that this is not conflicting with its own expectations: this is the case when the ONU Aggregation function is not aware of the ONU or when it is aware of the ONU and is not expected to manage it with vOMCI. If the ONU

Aggregation is aware of the ONU but expects the ONU to be managed by vOMCI the Device Management Plane MUST escalate higher up in the Management Plane the inconsistency with the OLT.

R-MP_9 – The Device Management Plane MUST escalate higher up in the Management Plane that an ONU has shown-up but neither the OLT nor the Device Management Plane are able to authenticate it.

R-MP_10 – In case a D-OLT software component is to be used for ONU authentication, the Management Plane MUST have the capability to configure the D-OLT with the identification of physical OLT (pOLT) for which the D-OLT will perform ONU authentication.

R-MP_11 – In case a D-OLT software component is to be used for ONU authentication, the Management Plane MUST have the capability to configure the D-OLT with the list of all ONUs to be authenticated in the form of a list of vANIs (as known by the pOLT) per regular TR-385 YANG; in particular each vANI in the D-OLT must be configured with all credentials required to authenticate the corresponding ONU.

R-MP_12 – In case a D-OLT software component is to be used for ONU authentication, the Management Plane MUST have the capability to receive a notification from the D-OLT indicating that an ONU is confirmed authenticated or not.

R-MP_13 – The Management Plane SHOULD have the capability to query the LOID of a yet unknown ONU with an vOMCI function. This capability should be present even when the Management Plane is not expected to manage any ONUs itself.

8.4 Requirements for the D-OLT

R-DOLT_1 – In case a D-OLT software component is to be used for ONU authentication, the D-OLT MUST have the capability to be configured by the Management plane with the identification of the physical OLT (pOLT) for which the D-OLT will perform ONU authentication.

R-DOLT_2 – In case a D-OLT software component is to be used for ONU authentication, the D-OLT MUST have the capability to be configured by the Management plane with the list of all ONUs to be authenticated in the form of a list of vANIs (as known by the pOLT) per regular TR-385 YANG; in particular each vANI in the D-OLT must be configured with all credentials required to authenticate the corresponding ONU.

R-DOLT_3 – In case a D-OLT software component is to be used for ONU authentication, the D-OLT MUST be able to configure the physical OLT so that all ONUs that appear on a given channel partition are unconditionally authenticated by the D-OLT rather than by the physical OLT itself.

R-DOLT_4 – In case a D-OLT software component is to be used for ONU authentication, the D-OLT MUST be able to receive a notification from the physical OLT requesting to authenticate an ONU, including the credentials provided by the ONU.

R-DOLT_5 – In case a D-OLT software component is to be used for ONU authentication, the D-OLT MUST report to the physical OLT via an action the result, positive or negative, of an ONU authentication it has attempted. In particular, upon successful authentication, the D-OLT MUST indicate to the OLT the vANI and the ONU name corresponding to the ONU - as known on the pOLT.

R-DOLT_6 – In case a D-OLT software component is to be used for ONU authentication, the D-OLT MAY send a notification to the Management Plane that it could or could not authenticate an ONU.

End of Broadband Forum Technical Report TR-489