

O-RAN.WG4.MP.0-v07.01

**O-RAN Alliance Working Group 4**

**Management Plane Specification**

1st – 2024.09.25

For this re-published version, the prior versions of the IPR Policy will apply, except that the previous requirement for Adopters (as defined in the earlier IPR Policy) to agree to an O-RAN Adopter License Agreement to access and use Final Specifications shall no longer apply or be required for these Final Specifications after 1st July 2022.

The copying or incorporation into any other work of part or all of the material available in this specification in any form without the prior written permission of O-RAN ALLIANCE e.V. is prohibited, save that you may print or download extracts of the material on this site for your personal use, or copy the material on this site for the purpose of sending to individual third parties for their information provided that you acknowledge O-RAN ALLIANCE as the source of the material and that you inform the third party that these conditions apply to them and that they must comply with them.

목차

[Revision History 4](#_Toc178927306)

[History 4](#_Toc178927307)

[Keywords: 4](#_Toc178927308)

[Foreword 4](#_Toc178927309)

[Modal verbs terminology 5](#_Toc178927310)

[Executive summary 5](#_Toc178927311)

[1. Scope 5](#_Toc178927312)

[2. References 6](#_Toc178927313)

[2.1 Normative References 6](#_Toc178927314)

[3 Definitions of Terms and Abbreviations 8](#_Toc178927315)

[3.1 Terms 8](#_Toc178927316)

[3.3 Abbreviations 10](#_Toc178927317)

[4. General 12](#_Toc178927318)

[4.1 Conventions 12](#_Toc178927319)

[4.2 Topics for Future Specification Versions 12](#_Toc178927320)

[4.3 Revision and Compatibility Handling 12](#_Toc178927321)

[4.4 Namespace Compatibility Handling 13](#_Toc178927322)

[5 High Level Description 14](#_Toc178927323)

[5.1 Top level functional description, terminology, including hybrid, hierarchical 14](#_Toc178927324)

[5.1.1 Architecture for O-RAN WG4 Fronthaul functional split 14](#_Toc178927325)

[5.1.2 M-Plane architecture model 15](#_Toc178927326)

[5.1.3 Transport Network 16](#_Toc178927327)

[5.1.4 M-Plane functional description 17](#_Toc178927328)

[5.2 Interfaces 18](#_Toc178927329)

[5.3 YANG Module Introduction 18](#_Toc178927330)

[5.4 Security 19](#_Toc178927331)

[6 “Start-up” installation 20](#_Toc178927332)

[6.1 General 20](#_Toc178927333)

[6.2 Management Plane Transport aspects 23](#_Toc178927334)

[6.2.1 Transport Establishment 23](#_Toc178927335)

[6.2.2 O-RU identification in DHCP 24](#_Toc178927336)

[6.2.3 Management Plane VLAN Discovery Aspects 25](#_Toc178927337)

[6.2.4 O-RU Management Plane IP Address Assignment 26](#_Toc178927338)

[6.2.5 O-RU Controller Discovery 27](#_Toc178927339)

[6.2.6 Multi-Vendor Plug-and-Play 29](#_Toc178927340)

[6.2.7 Event-Collector Discovery 30](#_Toc178927341)

[6.3 NETCONF Call Home to O-RU Controller(s) 32](#_Toc178927342)

[6.4 NETCONF Connection Establishment 32](#_Toc178927343)

[6.4.1 NETCONF Security 33](#_Toc178927344)

[6.4.2 NETCONF Authentication 33](#_Toc178927345)

[6.4.3 User Account Provisioning 34](#_Toc178927346)

[6.5 NETCONF Access Control 35](#_Toc178927347)

[6.6 NETCONF capability discovery 36](#_Toc178927348)

[6.7 Monitoring NETCONF connectivity 37](#_Toc178927349)

[6.8 Closing a NETCONF Session 39](#_Toc178927350)

[6.9 PNF Registration 39](#_Toc178927351)

[6.9.1 Introduction 39](#_Toc178927352)

[6.9.2 PNF Registration Procedure 40](#_Toc178927353)

[6.10 Encoding of PNF Registration Notification 40](#_Toc178927354)

[7 O-RU to O-DU Interface Management 40](#_Toc178927355)

[7.1 O-RU Interfaces 40](#_Toc178927356)

[7.2 Transceiver 41](#_Toc178927357)

[7.3 C/U Plane VLAN Configuration 42](#_Toc178927358)

[7.4 O-RU C/U Plane IP Address Assignment 42](#_Toc178927359)

[7.5 Definition of processing elements 43](#_Toc178927360)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Revision** | **CR#** | **Description** |
| 2021.10.19 | 07.00.01 | CIS-032 | Alignment on British English |
| 2021.10.19 | 07.00.01 | CIS-033 | Clarifying Annex A as Normative |
| 2021.10.19 | 07.00.01 | CIS-034 | ETSI PAS Renumbering |

# History

|  |  |  |
| --- | --- | --- |
| **Date** | **Revision** | **Description** |
| 2019.03.11 | 01.00 |  |
| 2019.07.03 | 02.00 |  |
| 2020.04.17 | 03.00 |  |
| 2020.08.10 | 04.00 |  |
| 2020.12.10 | 05.00 |  |
| 2021.03.22 | 06.00 |  |
| 2021.07.26 | 07.00 |  |
| 2021.10.28 | 07.01 |  |

# Keywords:

Open-Fronthaul, lower-layer-split

# Foreword

This Technical Specification (TS) has been produced by O-RAN Alliance.

# Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the O-RAN Drafting Rules (Verbal forms for the expression of provisions).  
본 문서에서 "해야한다", "하지 않아야 한다", "해야 한다", "하지 말아야 한다", "할 수 있다", "할 필요가 없다", "할 것이다", "하지 않을 것이다", "할 수 있다", "할 수 없다"는 O-RAN 초안 작성 규칙의 조항 3.2(조항 표현을 위한 구두 형태)에 설명된 대로 해석되어야 합니다.

"must" and "must not" are NOT allowed in O-RAN deliverables except when used in direct citation.  
"must" 및 "must not"은 직접 인용에 사용되는 경우를 제외하고 O-RAN 성과물에서 허용되지 않습니다.

# Executive summary

This Technical Specification defines the Management Plane for the O-RAN Open Fronthaul based on the selected lower-layer split point as defined within the Open Fronthaul Control Plane, User Plane and Synchronization Plane specification. This Technical Specification is used in combination with a set of associated YANG models to enable operation of an O-RAN alliance defined O-RU.  
이 기술 사양은 Open Fronthaul Control Plane, User Plane 및 Synchronization Plane 사양에 정의된 선택된 하위 계층 분할 지점을 기반으로 O-RAN Open Fronthaul의 관리 평면을 정의합니다. 이 기술 사양은 연관된 YANG 모델 세트와 함께 사용되어 O-RAN 얼라이언스 정의 O-RU의 작동을 가능하게 합니다.

# 1. Scope

This Technical Specification has been produced by the O-RAN.org.

The contents of the present document are subject to continuing work within O-RAN WG4 and may change following formal O-RAN approval. Should the O-RAN.org modify the contents of the present document, it will be re-released by O-RAN Alliance with an identifying change of release date and an increase in version number as follows:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Release x.y.z | | |
|  | where: | | |
|  |  | x | the first digit is incremented for all changes of substance, i.e., technical enhancements, corrections, updates, etc. (the initial approved document will have x=01). |
|  |  | y | the second digit is incremented when editorial only changes have been incorporated in the document. |
|  |  | z | the third digit included only in working versions of the document indicating incremental changes during the editing process. |

The present document specifies the management plane protocols used over the fronthaul interface linking the O-RU (O-RAN Radio Unit) with other management plane entities, that may include the O-DU (O-RAN Distributed Unit), the O-RAN defined **Service Management and Orchestration (SMO)** functionality as well as other generic Network Management Systems (NMS).  
본 문서에서는 O-RU(O-RAN 무선 장치)와 다른 관리 평면 엔티티를 연결하는 프런트홀 인터페이스에서 사용되는 관리 평면 프로토콜을 지정합니다. 여기에는 O-DU(O-RAN 분산 장치), O-RAN에서 정의한 서비스 관리 및 오케스트레이션(SMO) 기능은 물론 기타 일반 네트워크 관리 시스템(NMS)이 포함될 수 있습니다.

# 2. References

## 2.1 Normative References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

* References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
* For a specific reference, subsequent revisions do not apply.
* For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in Release 15.

[1] 3GPP TR 21.905: “Vocabulary for 3GPP Specifications”  
[2] ORAN-WG4.CUS.0-v07 “Control, User and Synchronization Plane Specification”, O-RAN Alliance, Working Group 4  
[3] RFC 6241, “Network Configuration Protocol (NETCONF)”, IETF, June 2011  
[4] RFC 7950, “The YANG 1.1 Data Modeling Language”, IETF, August 2016  
[5] RFC 6242, “Using the NETCONF Protocol over Secure Shell (SSH)”, IETF, June 2011  
[6] RFC 4252, “The Secure Shell (SSH) Authentication Protocol”, IETF, January 2006  
[7] RFC 4253, “The Secure Shell (SSH) Transport Layer Protocol”, IETF, January 2006  
[8] RFC 2132, “DHCP Options and BOOTP Vendor Extensions”, IETF, March 1997  
[9] RFC 3925, “Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)”, IETF, October 2004  
[10] RFC 2131, “Dynamic Host Configuration Protocol”, IETF, March 1997  
[11] RFC 4862, “IPv6 Stateless Address Autoconfiguration”, IETF, September 2007  
[12] RFC 3315, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, IETF, July 2003  
[13] RFC 3736, “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6”, IETF, April 2004  
[14] RFC 8572, “Secure Zero Touch Provisioning (SZTP)”, IETF, April 2019  
[15] RFC 8071, “NETCONF Call Home and RESTCONF Call Home”, IETF, February 2017  
[16] SFF-8472v11, “Diagnostic Monitoring Interface for Optical Transceivers”, SFF Committee, September 2010  
[17] IEEE 802.1ag, “IEEE Standard for Local and Metropolitan Area Networks Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management”, IEEE, 2007  
[18] RFC 862, “Echo Protocol”, IETF, May 1983  
[19] MEF.38, “Service OAM Fault management YANG Modules”, Metro Ethernet Forum, April 2012  
[20] RFC 7895, “YANG Model Library”, IETF, June 2016  
[21] RFC 5277, “NETCONF Event Notifications”, IETF, July 2008  
[22] G.8275.1, “Precision time protocol telecom profile for phase/time synchronization with full timing support from the network”, ITU, June 2016  
[23] G.810, “Definitions and terminology for synchronization networks”, ITU, August 1996  
[24] 1588v2-2008, “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”, IEEE, 2008  
[25] Y.1731, “Operation, administration and maintenance (OAM) functions and mechanisms for Ethernet based networks”, ITU, August 2015  
[26] AISG 2.0, “Control interface for antenna line devices”, Antenna Interface Standards Group, June 2006  
[27] 3GPP 37.462, “Iuant interface: Signalling transport”, 3GPP  
[28] 3GPP 37.466, “Iuant interface: Application part”, 3GPP  
[29] VOID  
[30] ITU X.733, “Information Technology – Open Systems Interconnection - System Management: Alarm Reporting Function”, 1992  
[31] RFC 6187, “X.509v3 Certificates for Secure Shell Authentication”, IETF, March 2011  
[32] 3GPP TS 36.213, “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures”, 3GPP, V13.6.0 (2017-06)  
[33] RFC 4361, Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4), IETF, February 2006  
[34] SFF-8636v2.9.3, “Specification for Management Interface for Cabled Environment”, SFF Committee, April 2019  
[35] RFC 6470, “Network Configuration Protocol (NETCONF) Base Notifications”, IETF, February 2012  
[36] VES Event Listener 7.2 https://docs.onap.org/projects/onap-vnfrqtsrequirements/en/latest/Chapter8/ves\_7\_2/ves\_event\_listener\_7\_2.html  
[37] RFC 8639, “Subscription to YANG Notifications”, IETF, September 2019  
[38] RFC 7951, “JSON Encoding of Data Modeled with YANG”, IETF, August 2016  
[39] RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2", IETF, August 2008  
[40] RFC 6125, “Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS) “, IETF, March 2011  
[41] RFC 7589, “Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication”, IETF, June 2015[41] RFC 7540, “Hypertext Transfer Protocol Version 2 (HTTP/2)”, IETF, May 2015  
[42] RFC 8446, “The Transport Layer Security (TLS) Protocol Version 1.3”, IETF, August 2018  
[43] RFC 7030, “Enrollment over Secure Transport”, IETF, October 2013  
[44] RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol".  
[45] Transport Layer Security (TLS) Parameters. https://www.iana.org/assignments/tls-parameters/tlsparameters.xhtml, Internet Assigned Numbers Authority, (IANA), January 27, 2021.  
[46] 3GPP TS 33.210, “Network Domain Security (NDS); IP network layer security”, Release 16, 3GPP, July 2020.  
[47] RFC 5289, "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)”, IETF, August 2008.  
[48] RFC 5288, “AES Galois Counter Mode (GCM) Cipher Suites for TLS”, August 2008.  
[49] RFC 7540, “Hypertext Transfer Protocol Version 2 (HTTP/2”, May 2015  
[50] IEEE Std 1588-2019 “Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”, November 2019.  
[51] 3GPP 33.310, “Network Domain Security (NDS); Authentication Framework (AF)”  
[52] 3GPP 32.509, “Data formats for multi-vendor plug and play eNode B connection to the network”  
[53] RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol", September 2005  
[54] RFC 4217: "Securing FTP with TLS”, IETF, October 2005  
[55] RFC 8996: “Deprecating TLS 1.0 and TLS 1.1”, IETF, March 2021  
[56] “O-RAN Security Protocols Specifications”, version 1.0, section 2.2.2 “TLS Protocol profiles specifications”, O-RAN-SFG.O-RAN-Security-Protocols-Specifications-v01.00.01, O-RAN Alliance  
[57] 3GPP TS28.552 “5G performance measurements”, Release 16, 3GPP, July 2020

# 3 Definitions of Terms and Abbreviations

## 3.1 Terms

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Antenna Line**: connection between O-RU and antenna

**C-Plane**: **Control Plane**: refers specifically to real-time control between O-DU and O-RU, and should not be confused with the UE’s control plane

**DL**: **DownLink**: data flow towards the radiating antenna (generally on the LLS interface)

**eAxC**: **extended Antenna-Carrier**: a data flow for a single antenna (or spatial stream) for a single carrier in a single sector.

**Event-Collector**: A REST server to which an O-RU supporting NON-PERSISTENT-NETCONF feature can send a JSON notification

**FHM mode**: Mode of Shared cell which is realized by FHM and several O-RUs in star topology.

**LLS**: Lower Layer Split: logical interface between O-DU and O-RU when using a lower layer (intra-PHY based) functional split.

**LLS-U**: Lower Layer Split User-plane: logical interface between O-DU and O-RU when using a lower layer functional split.

**LLS-C**: Lower Layer Split Control-plane: logical interface between O-DU and O-RU when using a lower layer functional split.

**LLS-S**: Lower Layer Split Synchronization-plane: logical interface between O-DU and O-RU when using a lower layer functional split.

**High-PHY**: those portions of the PHY processing on the O-DU side of the fronthaul interface, including FEC encode/decode, scrambling, and modulation/demodulation.

**Low-PHY**: those portions of the PHY processing on the O-RU side of the fronthaul interface, including FFT/iFFT, digital beamforming, and PRACH extraction and filtering.

**M-Plane**: Management Plane: refers to non-real-time management operations between the O-DU and the O-RU

**North-node**: the O-DU or a connected O-RU closer to the O-DU for the O-RU, e.g., the cascade O-RU#1 connected to O RU#2 is north-node for O-RU#2, when O-DU, O-RU#1 and O-RU#2 are in cascade chain topology. The O-DU in star topology connected to an FHM is north-node for the FHM.

**NMS**: A Network Management System dedicated to O-RU operations

**Port**: End of a transport link – in most cases this is an optical port

**Port Number**: A number which identifies a port (see Port). In case of SFP/SFP+ port, port number value is 0 to N-1 where N is number of ports in the device. Numbers 0 to N-1 are assigned to ports in order following order of labels on the device (labels for ports are not necessarily numbers starting from zero)

**O-DU**: O-RAN Distributed Unit: a logical node hosting PDCP/RLC/MAC/High-PHY layers based on a lower layer functional split.

**O-RU**: O-RAN Radio Unit: a logical node hosting Low-PHY layer and RF processing based on a lower layer functional split. This is similar to 3GPP’s “TRP” or “RRH” but more specific in including the Low-PHY layer (FFT/iFFT, PRACH extraction).

**O-RU Controller**: A network function that is permitted to control the configuration of an O-RU. Examples of O-RU controllers include, an O-DU, a classical NMS, an O-RAN Service Management and Orchestration function, or other network automation platforms.

**S-Plane**: Synchronization Plane: refers to traffic between the O-RU or O-DU to a synchronization controller which is generally an IEEE-1588 Grand Master (however, Grand Master functionality may be embedded in the O-DU).

**Shared cell**: The operation for the same cell by several O-RUs.

**Shared cell network**: the network for several cascade O-RUs in a chain topology or the network for one FHM and several O RUs in a star topology.

**South-node**: a connected O-RU far from O-DU for the O-RU, e.g., the cascade O-RU#2 connected to O-RU#1 is south-node for O-RU#1, when O-DU, O-RU#1 and O-RU#2 are in cascade chain topology. The O-RU in star topology connected to an FHM is south-node for the FHM.

**Spatial stream**: the data flow on the DL associated with precoded data (may be same as layers or different if there is expansion in the precoding), and on UL associated with the number of outputs from the digital beamforming (sometimes called “beams”).

**SSM**: Synchronization Status Message: part of ITU G.781 and G.8264 standards.

**TRX**: Refers to the specific processing chain in an O-RU associated with D/A or A/D converters. Due to digital beamforming the number of TRXs may exceed the number of spatial streams, and due to analogue beamforming, the number of TRXs may be lower than the number of antenna elements.

**U-Plane**: User Plane: refers to IQ sample data transferred between O-DU and O-RU

**UL**: Up-Link: data flow away from the radiating antenna (generally on the LLS interface)

**Virtual Connection**: a connection between O-RU and O-RU controller. This connection is established by means of autodetection procedure and is supervised by supervision procedure.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

|  |  |  |
| --- | --- | --- |
|  | ALD | Antenna Line Device |
|  | AVP | Average Power |
|  | BCN | BTS Clock Number |
|  | CA | Certificate Authority |
|  | CA/RA | Certificate Authority/Registration Authority |
|  | CMP | Certificate Management Protocol |
|  | CRC | Cyclic Redundancy Check |
|  | CUS | Control/User/Synchronization |
|  | DHCP | Dynamic Host Configuration Protocol |
|  | DMTC | DRS Measurement Timing Configuration |
|  | DRS | Discovery Reference Signal |
|  | DSCP | Differentiated Services Code Point |
|  | FHM | Fronthaul Multiplexer |
|  | FTPES | File Transfer Protocol Explicit-mode Secure |
|  | HDLC | High-Level Data Link Control |
|  | lls-M | Lower Layer Split Management plane |
|  | LAA | Licensed Assisted Access |
|  | LBM | Loop-Back Message |
|  | LBR | Loop Back Reply |
|  | LBT | Listen Before Talk |
|  | ME | Maintenance Entity |
|  | MEP | Maintenance association End Point |
|  | NAT | Network Address Translation |
|  | NDM | Non-Delay Managed |
|  | NETCONF | Network Configuration Protocol |
|  | O-DU | O-RAN Distributed Unit (see definitions section) |
|  | O-RU | O-RAN Radio Unit |
|  | OMA | Optical Modulation Amplitude |
|  | PDV | Packet Delay Variation |
|  | PNF | Physical Network Function |
|  | QoS | Quality of Service |
|  | RET | Remote Electrical Tilt |
|  | RPC | Remote Procedure Call |
|  | SFP | Small Form-factor Pluggable |
|  | sFTP | Secure File Transfer Protocol or SSH File Transfer Protocol |
|  | SLAAC | Stateless Address Auto Configuration |
|  | SMO | Service Management and Orchestration |
|  | SRS | Sounding Reference Signal |
|  | SSH | Secure Shell |
|  | TLS | Transport Layer Security |
|  | T-TSC | Telecom Time Subordinate Clock. This is what ITU-T standards refer to as a Telecom Time Slave Clock |
|  | VLAN | Virtual LAN |
|  | YANG | Yet Another Next Generation |
|  |  |  |
|  |  |  |
|  | **eAxC\_ID** | Extended Antenna Carrier ID. 5G와 LTE 네트워크에서 사용되는 O-RAN 및 eCPRI 표준에서 정의된 식별자. RU와 DU간의 통신에서, 여러 안테나 및 캐리어를 구분하는데 사용. |
|  | FQDN | Fully Qualified Domain Name 완전한 도메인 이름을 의미  <호스트 이름>.<서브도메인>.<도메인>.<최상의 도메인>  [www.example.com](http://www.example.com) www: 호스트 이름, example: 도메인 이름, .com: 최상위 도메인 |
|  | IANA | Internet Assigned Numbers Authority 인터넷의 주요 자원(IP주소, 도메인 이름, 프로토콜 번호 등)을 관리하고 할당하는 국제기구. |
|  | ONAP | Open Network Automation Platform 네트워크 및 클라우드 인프라를 자동화하고 관리하기 위한 오픈 소스 플랫폼. |
|  |  |  |
|  | Probe message | 네트워크와 통신 시스템에서 상태 확인이나 연결 상태 테스트를 위해 사용되는 메시지. 예) ICMP(Internet Control Message Protocol), Wi-Fi Probe Request/Response |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 4. General

## 4.1 Conventions

This management plane specification includes cross references to a set of associated YANG models. Text may reference particular YANG leafs, notifications and remote procedure calls (RPCs). In order to assist in readability, all cross references to YANG defined elements will keep the identical case format as defined in the corresponding YANG model, with the font-weight set to bold. This convention applies only to text and not to YANG elements embedded into figures.  
이 관리 플레인 사양에는 연관된 YANG 모델 집합에 대한 교차 참조가 포함됩니다. 텍스트는 특정 YANG 리프, 알림 및 원격 프로시저 호출(RPC)을 참조할 수 있습니다. 가독성을 돕기 위해 YANG 정의 요소에 대한 모든 교차 참조는 해당 YANG 모델에 정의된 것과 동일한 케이스 형식을 유지하고 글꼴 두께를 굵게 설정합니다. 이 규칙은 텍스트에만 적용되며 그림에 포함된 YANG 요소에는 적용되지 않습니다.

If there is any conflict between the YANG models and the accompanying text description in this specification, the definition of the YANG models shall take precedence.

## 4.2 Topics for Future Specification Versions

다음 주제는 사양의 향후 버전에서 고려되어야 합니다.

1. 다양한 유형의 빔포밍을 위한 빔 ID 필드 해석
2. 중복성 및 장애 조치 시나리오
3. IP 정의 흐름에 대한 공유 셀 지원
4. O-RAN Alliance O1 사양과 더 잘 일치하도록 개선

## 4.3 Revision and Compatibility Handling

The revision statement in the YANG models will be used to describe future revisions to the models that are backwards compatible, where backwards compatibility changes follow the rules defined in section 11 of RFC 7950 [4]. Backwards incompatible changes will be addressed by incrementing the number used as part of the model name and namespace, effectively creating a new YANG model. The format of the namespace used in all O-RAN YANG models is “urn:o-ran:”“:”, where the initial used in a newly defined YANG model is “1.0”. Where this document makes reference to models, irrespective of their backward compatibility, a generic of “x.y” is used to enable reference to all versions of the namespace for a particular .  
YANG 모델의 개정 설명은 이전 버전과 호환되는 모델에 대한 향후 개정을 설명하는 데 사용되며, 이전 버전과의 호환성 변경은 RFC 7950 [4]의 섹션 11에 정의된 규칙을 따릅니다. 이전 버전과 호환되지 않는 변경 사항은 모델 이름과 네임스페이스의 일부로 사용되는 숫자를 증가시켜 처리하여 효과적으로 새로운 YANG 모델을 만듭니다. 모든 O-RAN YANG 모델에서 사용되는 네임스페이스의 형식은 "urn:o-ran:"<모델 이름>":"<모델 번호>이며, 여기서 새로 정의된 YANG 모델에서 사용되는 초기 <모델 번호>는 "1.0"입니다. 이 문서에서 이전 버전과의 호환성과 관계없이 모델을 참조하는 경우, 특정 <모델 이름>에 대한 모든 버전의 네임스페이스를 참조할 수 있도록 "x.y"의 일반 <모델 번호>를 사용합니다.

The revision statement in all YANG models includes a reference statement used to cross-reference to the first version of this document where the corresponding description was introduced. For example, the reference in all revision statements for the initial O-RAN models include cross-reference to “ORAN-WG4.MP.0-v01.00”.  
모든 YANG 모델의 개정 설명서에는 해당 설명이 도입된 이 문서의 첫 번째 버전을 교차 참조하는 데 사용되는 참조 설명서가 포함되어 있습니다. 예를 들어, 초기 O-RAN 모델에 대한 모든 개정 설명서의 참조에는 "ORAN-WG4.MP.0-v01.00"에 대한 교차 참조가 포함되어 있습니다.

The revision statement of the YANG models also includes a description which is used to track the versioning of the YANG model. All revision statement descriptions will begin with “version ”“.”“.”, where , and are used to reflect the version of the YANG model, where

<a> corresponds to the first digit of the O-RAN WG4 management plane specification version where the corresponding description was first introduced, corresponding to in clause 1  
<b> is incremented when errors in the YANG model have been corrected  
<c> is incremented only in working versions of the YANG model indicating incremental changes during the editing process

NOTE : O-RU Controllers that receive YANG library information from the O-RU with a module revision that is a higher version than the module revision currently used by the O-RU Controller can assume that models with the same namespace have been updated to ensure backwards compatibility. The O-RU Controller can continue to use its current module version and any unknown schema nodes received from the O-RU, i.e., those introduced in later revisions, should be ignored by the O-RU Controller.

## 4.4 Namespace Compatibility Handling

If backwards incompatible changes have been made, the used in the YANG model namespace shall be incremented. Following such changes, an O-RU may include multiple backwards incompatible namespaces in its YANG library, for example “urn:o-ran:”“:1.0” and “urn:o-ran:”“:2.0”.  
이전 버전과 호환되지 않는 변경 사항이 있는 경우 YANG 모델 네임스페이스에서 사용되는 <모델 번호>가 증가합니다. 이러한 변경 사항에 따라 O-RU는 YANG 라이브러리에 여러 이전 버전과 호환되지 않는 네임스페이스를 포함할 수 있습니다. 예를 들어 "urn:o-ran:"<모델 이름> ":1.0" 및 "urn:o-ran:"<모델 이름> ":2.0"입니다.

The O-RAN Adopter License Agreement in Chapter ZZZ defines terms regarding the modification of O-RAN defined specifications. When such modifications are necessary, the preferred approach for realizing such is for the third-party licensee to publish their own augmentations to the O-RAN defined YANG models and procedures. An O-RU that supports such thirdparty modifications shall include such model augmentations in its YANG library. Consequently, an O-RU Controller should be prepared to ignore any unknown models, e.g., developed according to such a procedure.

# 5 High Level Description

## 5.1 Top level functional description, terminology, including hybrid, hierarchical

### 5.1.1 Architecture for O-RAN WG4 Fronthaul functional split

This O-RAN FH specification addresses the lower layer functional split as depicted in Figure 5.1.1.1. Refer to the O-RAN CUS plane specification [2] for more details on the split architecture. The Lower-Layer Split M-plane (LLS-M) facilitates the initialization, configuration and management of the O-RU to support the stated functional split.  
이 O-RAN FH 사양은 그림 5.1.1.1에 나와 있는 것과 같이 하위 계층 기능 분할을 다룹니다. 분할 아키텍처에 대한 자세한 내용은 O-RAN CUS 평면 사양[2]을 참조하십시오. 하위 계층 분할 M 평면(LLS-M)은 명시된 기능 분할을 지원하기 위해 O-RU의 초기화, 구성 및 관리를 용이하게 합니다.

텍스트, 스크린샷, 도표, 폰트이(가) 표시된 사진

자동 생성된 설명

### 5.1.2 M-Plane architecture model

A NETCONF/YANG based M-Plane is used for supporting the management features including “start up” installation, software management, configuration management, performance management, fault management and file management towards the O-RU. The M-Plane supports two architectural models:

1. **Hierarchical model**. As shown on the left side Figure 5.1.2.1, the O-RU is managed entirely by one or more O-DU(s) using a NETCONF based M-Plane interface. When the O-RU is managed by multiple O-DUs, it is typically for enabling O-DU and/or transport connectivity redundancy capabilities. Refer to clause 6 for more details.  
   왼쪽 그림 5.1.2.1에 표시된 대로 O-RU는 NETCONF 기반 M-Plane 인터페이스를 사용하는 하나 이상의 O-DU에 의해 완전히 관리됩니다. O-RU가 여러 O-DU에 의해 관리되는 경우 일반적으로 O-DU 및/또는 전송 연결 중복 기능을 활성화하기 위한 것입니다. 자세한 내용은 조항 6을 참조하십시오.
2. **Hybrid model**. As shown on the right side of Figure 5.1.2.1, the hybrid architecture enables one or more direct logical interface(s) between management system(s) and O-RU in addition to a logical interface between O-DU and the O-RU. It should be noted that the NETCONF clients connecting to the O-RU may be of different classes (e.g., O-DU and SMO). For example, functions like O-RU software management, performance management, configuration management and fault management can be managed directly by the management system(s).  
   그림 5.1.2.1의 오른쪽에 표시된 것처럼 하이브리드 아키텍처는 O-DU와 O-RU 간의 논리적 인터페이스 외에도 관리 시스템과 O-RU 간에 하나 이상의 직접적인 논리적 인터페이스를 가능하게 합니다. O-RU에 연결하는 NETCONF 클라이언트는 서로 다른 클래스(예: O-DU 및 SMO)일 수 있습니다. 예를 들어, O-RU 소프트웨어 관리, 성능 관리, 구성 관리 및 오류 관리와 같은 기능은 관리 시스템에서 직접 관리할 수 있습니다.

In the hybrid model, the O-RU has end to end IP layer connectivity with the SMO. From a physical network point of view, this connectivity could be via the O-DU, where the O-DU is acting as an IP/Ethernet packet forwarder, forwards the packets between O-RU and the SMO. Direct logical communication between an O-RU and SMO can be enabled via O-RUs being assigned routable IPs or local private IPs resolved by a NAT function in the network (or implemented at the O-DU). Refer to clause 6 for details how O-RU acquires the IP address of O-DU and SMO for the M-plane communication.  
하이브리드 모델에서 O-RU는 SMO와 엔드투엔드 IP 계층 연결을 갖습니다. 물리적 네트워크 관점에서 이 연결은 O-DU를 통해 이루어질 수 있으며, 여기서 O-DU는 IP/Ethernet 패킷 포워더 역할을 하며 O-RU와 SMO 간에 패킷을 전달합니다. O-RU와 SMO 간의 직접적인 논리적 통신은 O-RU에 네트워크의 NAT 기능(또는 O-DU에서 구현)으로 해결되는 라우팅 가능 IP 또는 로컬 개인 IP가 할당되어 활성화될 수 있습니다. O-RU가 M-플레인 통신을 위해 O-DU와 SMO의 IP 주소를 획득하는 방법에 대한 자세한 내용은 절 6을 참조하십시오.

As described in clause 6, there is no explicit signalling to indicate that an O-RU is operating in a hierarchical or hybrid configuration. All NETCONF servers supporting this M-Plane specification shall support multiple NETCONF sessions, and hence all compliant O-RUs shall be able to support both hierarchical and hybrid deployment.  
6절에 설명된 대로, O-RU가 계층적 또는 하이브리드 구성에서 작동하고 있음을 나타내는 명시적 신호는 없습니다. 이 M-Plane 사양을 지원하는 모든 NETCONF 서버는 여러 NETCONF 세션을 지원해야 하며, 따라서 모든 호환 O-RU는 계층적 및 하이브리드 배포를 모두 지원할 수 있어야 합니다.

텍스트, 스크린샷, 도표, 폰트이(가) 표시된 사진

자동 생성된 설명

NETCONF/YANG is used as the network element management protocol [3] and data modelling language [4]. Use of such a standardized framework and common modelling language simplifies integration between O-DU and O-RU as well as operator network integration (in terms of running service) in case of elements sharing a common set of capabilities. The framework supports integration of products with differing capabilities enabled by well-defined published data models. NETCONF also natively supports a hybrid architecture which enables multiple clients to subscribe and receive information originating at the NETCONF server in the O-RU.

### 5.1.3 Transport Network

Based on the transport topology, various modes of network connectivity are possible between O-RU and O-DU and SMO.

The basic requirement for M-Plane is to have end to end IP connectivity between the O-RU and the elements managing it (ODU, SMO, or so called “O-RU Controllers”). The connectivity between the O-DU and SMO and its management plane are not in scope of this specification. The O-RU shall support either IPv4 or IPv6 and optionally support dual stack (IPv4 and IPv6).  
M-Plane의 기본 요구 사항은 O-RU와 이를 관리하는 요소(O DU, SMO 또는 소위 "O-RU 컨트롤러") 간에 엔드투엔드 IP 연결이 있어야 한다는 것입니다. O-DU와 SMO 및 해당 관리 플레인 간의 연결은 이 사양의 범위에 포함되지 않습니다. O-RU는 IPv4 또는 IPv6를 지원해야 하며 선택적으로 듀얼 스택(IPv4 및 IPv6)을 지원해야 합니다.

NOTE: In previous versions of this specification, only IPv4 was mandatory. In order to ensure backwards compatibility with equipment supporting earlier versions of this specification, an operator and vendor can agree to use a common IP version in the O-RU, O-DU and any other O-RU controllers.

### 5.1.4 M-Plane functional description

The M-Plane provides the following major functionalities to the O-RU. These features are implemented using the NETCONF provided functions.

**“Start-up” installation**

During start-up, the O-RU acquires its network layer parameters either via static (pre-configured in the O-RU) or dynamically via DHCP or DHCPv6. During this process the O-RU may acquire the IP address of the O-RU controller(s), in which case the O-RU establishes the NETCONF connectivity using the “call home” feature. When the O-RU is operating in an environment which include the O-RAN defined SMO, the O-RU may acquire the IP address of the event-collector(s), in which case the O-RU performs a pnfRegistration which triggers the SMO to establish NETCONF connectivity using the information recovered from the pnfRegistration procedure. The capability exchange is performed between the client and server as part of the initial NETCONF Hello exchanges. Details of these steps are provided in clause 6.

NOTE : The use of “start up” terminology in this specification is distinct from the “start-up” capability used in a NETCONF environment to indicate that a device supports separate running and startup configuration datastores. This specification makes specific reference to configuration which is required to be stored in “reset persistent memory”. The O-RU shall use this stored configuration as its “startup” configuration.

**SW management**

The M-Plane is responsible for software download, installation, validation and activation of new SW when requested by O-RU Controller. The software download is triggered by NETCONF RPC procedures, and the actual software package download is performed using sFTP with SSH or FTPES [54] with TLS.

**Configuration management**

Configuration management covers various scenarios like Retrieve Resource State, Modify Resource State, Modify Parameters and Retrieve Parameters. NETCONF get-config and edit-config RPCs shall be used for configuration parameter retrieval and updates at the O-RU

**Performance management**

Performance management describes the measurements and counters used to collect data related to O-RU operations. The purpose of Performance Management is optimizing the operation of the O-RU.

The measurement results are reported by two options:

1. **YANG Notification**: This option uses the stats definition of YANG model per measurement group. In this case, get RPC and/or notification will be used (see clause 10 for more details).
2. **File Upload**: This option uses the file upload procedure defined in File management. The measurement results are saved to a data file periodically.

**Fault Management**

Fault management is responsible for sending alarm notifications to the NETCONF Client. Fault Management allows alarm notifications to be disabled or enabled as well as alarm subscription.

**File Management**

File management allows the O-RU Controller to trigger an O-RU to perform upload of files stored on O-RU to O-RU Controller. The O-RU may provide different kinds of files and retrieved files can be used for various purposes. Simultaneous multiple file upload operations can be supported under the same sFTP or FTPES [54] connection between O-RU to O-DU/SMO.

## 5.2 Interfaces

The M-Plane interface is defined between the O-RU Controller and the O-RU. The protocol stack of the M-Plane interface is shown in in the Figure 5.2.1 below. The transport network layer is built on IP transport and SSH/TCP, and optionally TLS, is used to carry the M-Plane message between the O-RU Controller and the O-RU. As an option, the O-RU may support the capability to support asynchronous notifications to be sent using HTTPS. This option enables system optimization when the O-RU Controller corresponds to the SMO which is operating with a non-persistent NETCONF session to the O-RU.

텍스트, 폰트, 스크린샷, 번호이(가) 표시된 사진

자동 생성된 설명

## 5.3 YANG Module Introduction

The data models representing the M-Plane are organized as a set of reusable YANG modules. It is also the intent to reuse the publicly available and generic YANG models as much as possible instead of developing customized O-RAN specific modules. Refer to the various chapters, Annex D and the repository of YANG models for more details on each of these modules.

## 5.4 Security

The M-Plane provides end to end security as a mandatory feature, see Table 5.4.1. M-Plane security shall support SSHv2 in accordance with RFC 6242 [5]. TLS 1.2 in accordance with RFC 7589 [41] may be optionally supported. TLS 1.3 in accordance with RFC 8446 [42] may also be optionally supported in addition to TLS 1.2. RFC 6242 [5] and RFC 7589 [41] provide the procedures for interoperability with NETCONF implementations. If there are multiple NETCONF sessions established with a single O-RU, either SSH tunnels or TLS connections may be used and each session should be established over a separate SSH tunnel or TLS connection. An O-RU shall support sFTP based file transfer over SSH. An O-RU that supports optional NETCONF/TLS shall also support FTPES based file transfer over TLS. For the O-DU, the operator may use SSH, TLS, or both. It is recommended that operators use NETCONF/TLS and FTPES in production networks.

NOTE : TLS versions 1.0 and 1.1 have been deprecated by the IETF [55] and shall not be used.

텍스트, 스크린샷, 번호, 폰트이(가) 표시된 사진

자동 생성된 설명

SSHv2 may be used to perform SSH server host authentication, key exchange, encryption, and integrity protection. It also derives a unique session ID that may be used by higher-level protocols. The end point (SSH client) authentication should be done as per RFC 4252 [6]. Clause 6 describes the authentication approach based on username and password as well as based on X.509 certificates.

The SSHv2 transport level security (encryption algorithms, data integrity algorithms) shall be based on RFC4253 [7]. As per aes128-ctr shall be the mandatory ciphering protocol, and rest of the ones listed as optional. For data integrity, hmac-sha2-256 shall be the mandatory algorithm, and rest of the listed algorithms shall be optional. Public key-based host authentication shall be used for authenticating the server (RFC 4253) by the clients, and username/password-based client authentication shall be done by the server as part of the SSH session establishment. The O-RU shall support the host key algorithms and key exchange methods defined in section 10.1 of RFC 5656 for securing the Secure Shell (SSH) transport.

NOTE 1: In order to ensure backwards compatibility with equipment supporting earlier versions of this specification, an operator and vendor may agree to use one of the optional ciphering protocols.

As an additional option, both client and server may implement authentication based on X.509 certificates. With this option, RSA 2048 bit shall be supported for the Public Key algorithm, aes128-ctr shall be supported for the cyphering algorithm and hmac-sha2-256 shall be supported for integrity algorithm.

NOTE 2: The above specification will be replaced with a cross reference to the O-RAN Security Task Group Guidelines once such is published.

TLS 1.2 based on RFC 5246[38] performs mutual authentication, key exchange, encryption, and integrity protection to ensure trusted communication between the NETCONF server (O-RU) and the NETCONF client (O-DU or SMO). NETCONF implementations may support X.509 certificate-based authentication using TLS 1.2 based on RFC 7589 [41]. When X.509 based authentication is used, NETCONF server identity is based on RFC 6125 [40] and NETCONF client identity is specified in RFC 7589[41].

TLS 1.2 implementations shall support the following TLS Cipher Suites with SHA-256 and AES Galois Counter Mode in accordance with RFC 7540 [42] and 3GPP TS 33.210 [46]:

* ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289 [47].
* DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288 [48].

It is mandatory that TLS implementations follow the rules on allowed cipher suites specified in the O-RAN Security Protocols Specifications [56]. Implementations may include additional TLS cipher suites that provide mutual authentication and confidentiality as required by NETCONF in RFC 6241 [3]. Only cipher suites with AEAD (e.g., GCM) and PFS (e.g., ECDHE, DHE) and recommended by IANA [45] may be optionally supported. The disallowed cipher suites in RFC 7540 [49], Appendix A, shall not be used. The vendor and operator need to be prepared to replace integrity and/or ciphering algorithms if the current algorithm in use is compromised or deprecated. TLS 1.2 shall follow TLS profiling defined in 3GPP TS 33.210 [46] section 6.2.3.

Operators may select the authentication mechanism and protocol to use as shown in Table 5.4.2

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

# 6 “Start-up” installation

## 6.1 General

This clause provides the overall start-up mechanism from the power-on of O-RU to available in service.

**Pre-condition:**

* Power-ON for O-RU/NETCONF Server or O-RU restart operation.  
  Power-ON for O-RU controller/NETCONF Client(s) and/or pnfRegistration event-collector.
* Physical interface(s) is(are) connected.

**Post-condition:**

* O-RU is ready for the radio transmission to the air on at least one carrier if packet transmission received from O-DU
* O-RU is ready for the packet transmission to the O-DU if radio reception received at the air on at least one carrier.
* At least one O-RU Controller/NETCONF client with either “super-user” or “hybrid-odu” access privileges can control the carrier configuration of the O-RU/NETCONF server in O-RU.

[Table 6.1.1: Overall of Start-Up Installation]

At the power-on of O-RU or following an O-RU restart, the following procedures are performed, as illustrated in Figure 6.1.1.

1. O-RU performs M-Plane transport layer resolution (DHCP, MAC, VLAN, IP, etc.) and recovers IP address(es) of O-RU controller(s) and/or pnfRegistration event-collector.
2. O-RU begins synchronization of the O-RU against a Primary Reference Clock. (NOTE 1: Step 2 may be in parallel with step 1 for some O-RU implementation.)
3. O-RU performs NETCONF Call Home to discovered O-RU controller(s) and/or performs pnfRegistration to discovered event-collector.
4. O-RU controller performs SSH or TLS connection establishment.
5. O-RU and O-RU controller perform NETCONF capability discovery.
6. O-RU controller performs optional provisioning of new management accounts (typically only performed once during prestaging)
7. O-RU and O-RU controller perform supervision of NETCONF connection.
8. O-RU controller performs retrieval of O-RU information.
9. O-RU controller performs SW management.
10. O-DU performs CU-Plane transport configuration
11. (opt) O-DU performs LBM configuration (CU-Plane over ETH) or enables UDP Echo (CU-Plane over IP).
12. (opt) O-DU performs initial C/U-Plane transport connectivity checking between O-DU and O-RU.
13. O-RU controller retrieves the O-RU delay profile from the O-RU.
14. O-RU controller performs U-Plane configuration between O-DU and O-RU. C/U-Plane transport connectivity between O-DU and O-RU is configured as part of this step.
15. O-DU optionally performs C/U-Plane delay measurements between O-DU and O-RU if the O-RU supports it.
16. O-RU controller performs Fault Management activation by creating subscription to fault management event stream if O-RU controller has not subscribed to default event stream. Additionally, O-RU controller retrieves list of O-RU’s active alarm
17. O-RU controller activates performance measurement (if required at start-up timing).
18. O-RU controller retrieves O-RU state, including synchronization information, from O-RU.
19. O-RU controller configures the O-RU operational parameters.
20. Service available.

NOTE 2: The synchronization procedures started in step 2 needs to be completed before service is available.

NOTE 3: Periodic CU-Plane connectivity check is not considered as the part of start-up. Once configured in start-up phase, CU-Plane connectivity check can later be performed periodically and at any time in run-time.

This clause mainly covers 1 and 3 to 7 as sub-sections.

Cross Reference of other clauses:

The detail of 2. Synchronization management is described in clause 13.

The method of 8 and 17 retrieval of O-RU information is described in clause 9.

The detail of 9. SW management is described in clause 8.

The detail of 12. C/U-Plane transport connectivity checking between O-DU and O-RU is described in clause 7.

The detail of 13. Retrieval of the O-RU delay profile and 13. C/U-Plane delay measurements are described in clause 74.

The detail of 14. U-plane configuration is described in clause 15, and C/U-Plane transportation configuration is described in clause 7.

The detail of 17. Performance management is described in clause 10.

The detail of 16. Fault management is described in clause 11.

The method of 19. Control to make service available is described in clause 15.

## 6.2 Management Plane Transport aspects

### 6.2.1 Transport Establishment

This clause provides the M-plane transport establishment scenario between O-RU and O-RU controller(s), such as O-DU and/or SMO. The transport layer address of M-plane is only the target in this section. Transport aspects of the C plane and U plane are covered in clause 7.

**Pre-condition:**

* Physical interface is connected.
* When operating in an environment using call-home, the NETCONF server and NETCONF Client(s) have an identical NETCONF call home port configured, to ensure the NETCONF client listens on the same port used by the NETCONF Server.

**Post-condition:**

* Transport Layer address(es) for M-plane are known to O-RU and O-RU controllers.
* O-RU is aware of the physical port(s) for M-plane, e.g., if there are multiple ports in the O-RU.
* O-RU is aware of the VLAN(s) to be used for M-Plane, e.g., if VLANs are used in the transport network.
* Then O-RU is ready to establish TCP connection for NETCONF call home and/or for PNF registration.

For the transport establishment, there are the following alternatives, as illustrated in Figure 6.2.1.1:

a) Manual transport layer address configuration in O-RU. This configuration contains the addresses for O-RU and NETCONF client(s) and/or the event-collector. The method to manually configure the O-RU is out of scope in this specification. Assuming manual configuration is successful, the NETCONF server shall be able to recover this configured information and use the o-ran-mplane-int.yang model to communicate this operational-state to a NETCONF client.

b) If IPv4 is supported, DHCP server provides O-RU’s transport layer address information together with the identity of the NETCONF client and/or the identity of the event-collector. This identity encodes either the transport layer address or FQDN of the NETCONF client or event-collector. If an FQDN is signalled, the O-RU shall use the DNS server address provided by the DHCP server to recover the IP address corresponding to FQDN of the NETCONF client or event-collector.

c) If IPv6 is supported, Stateless Address Auto-Configuration (SLAAC) is used to configure the O-RU’s transport address with the DHCPv6 server providing the identity of the NETCONF client and/or event-collector. This identity encodes either the transport layer address or FQDN of the NETCONF client or event-collector. If an FQDN is signalled, the O-RU shall use the DNS server address provided by the DHCPv6 server to recover the IP address corresponding to FQDN of the NETCONF client or event-collector.

NOTE : A NETCONF client can receive a hint as to whether an O-RU supports a particular IP version by using the get RPC to recover the list of interfaces supported by the O-RU and using the presence of the augmented ipv4 container or ipv6 container in the o-ran-interfaces module as an indication that a particular IP version is supported.

The O-RU uses the o-ran-dhcp.yang model to be able to expose information signalled by the DHCP server.

[Figure 6.2.1.1: Transport Layer Establishment for M-plane]

Transport Layer interface related information for M-plane contains at least the physical port number, the hardware address of the Ethernet port, VLAN-ID, local IP address, remote IP address, Default Gateway address and Subnet mask.

In the case of option b) and c), the following subsections are used:

* O-RU identification in DHCP messages from O-RU.
* VLAN discovery aspect for M-plane.
* IP address assignment to O-RU.
* Discovery of address information of O-RU controller(s) and/or Event-Collector.

### 6.2.2 O-RU identification in DHCP

The O-RU shall identify itself as an O-RU to DHCP servers by using DHCP option(s) using the vendor-class-data string within the o-ran-dhcp YANG model. If the O-RU supports IPv4, there are two alternatives. One uses option 60 Vendor Class Identifier, RFC2132 [8]. The other uses option 124 Vendor Identifying Vendor Class Option, RFC3925 [9]. An O-RU implementing IPv4 shall support at least one of these options. If the O-RU supports IPv6, then it shall identify itself using the DHCPv6 Vendor Class Option.

**DHCPv4 Vendor Class Option:**

* Option: 60
* Vendor Class Identifier Option 60: string

The format of the vendor class string shall be configured to one of the following three options:

1. ““o-ran-ru2/, e.g., “o-ran-ru2/vendorA”
2. “o-ran-ru2//”, e.g., “o-ran-ru2/vendorA/ORUAA100”
3. “o-ran-ru2///”, e.g., “o-ran-ru2/vendorA/ORUAA100/FR1918010111”

**DHCPv4 Vendor-Identifying Vendor Class Option:**

* Option: 124
* Enterprise number: O-RAN-alliance 53148
* Vendor-Class-Data: the format of the string shall follow the rules defined for the DHCPv4 Vendor Class Option

**DHCPv6 Vendor Class Option:**

* Option: 16
* Enterprise number: O-RAN-alliance 53148
* Vendor-Class-Data: the format of the string shall follow the rules defined for the DHCPv4 Vendor Class Option

The DHCP Server may use the information when selecting an address pool from which to allocate an IP address to the O-RU or when selecting which management plane O-RU Controller information to configure in the O-RU.

### 6.2.3 Management Plane VLAN Discovery Aspects

The O-RU will be connected to one or more Ethernet ports. The transport systems may be realized such that these Ethernet ports may be configured either as an access port, where untagged Ethernet frames are used, or as a trunk port, where multiple VLANs are configured. At start up, the O-RU will typically not be able to immediately determine whether its ports are attached to remote transport equipment configured for access or trunk mode operation.

Once an O-RU completes its boot-up sequence and Ethernet connectivity is detected on at least one of its Ethernet interfaces, the O-RU starts management plane connection establishment.

The O-RU needs to determine whether it is connected to an access port or a trunk port. In particular, when connected to a trunk port, the O-RU needs to additionally determine the VLAN identity/ies used to support the management plane communication(s). The VLAN(s) used to support management plane communications can be identified by the DHCP server replying to the DHCP DISCOVER message, as described in clause 6.2.5 and clause 6.2.7.

NOTE : An O-RU which supports IPv6 may infer that a VLAN is not used to support management plane communications if it receives an IPv6 Router Advertisement without either the “managed address configuration” or “other configuration” bits set.

If the O-RU does not have previously configured management plane VLAN information, the O-RU shall attempt to discover DHCP servers on all its Ethernet ports using untagged Ethernet frames.

When the O-RU has been previously configured with management plane VLAN information, the O-RU may use this information to optimize its discovery of the VLAN ID(s) used for management plane connectivity. Previously configured management plane VLAN information includes an O-RU that stores the last VLAN(s) used for management plane connectivity, and/or an O-RU which has been previously configured with a range of management plane VLANs by a NETCONF client using the contents of the searchable-mplane-access-vlans-info container that have been stored in reset-persistent memory. The ORU may use this information to optimize its discovery of the VLAN ID(s) used for management plane connectivity.

If the O-RU does not receive a DHCP OFFER from a DHCP server using untagged frames, or previously configured VLANs, the O-RU should attempt to contact a DHCP server using the full range of VLAN IDs (1~4094) on all its Ethernet ports.

The individual VLAN search algorithm used by an O-RU should ensure timely activation of the M-Plane while accommodating scenarios whereby there may be an intermittent or temporary connectivity problem between the O-RU and the DHCP server causing no DHCP response to be received on the M-Plane VLAN. The O-RU should repeatedly search using untagged frames and previously configured VLANs whenever it searches across the full range of VLAN IDs. The O-RU controller is able to recommend the maximum interval between repeatedly scanning for M-Plane connectivity on the untagged and configured VLANs using the scan-interval schema node.

For example, the default scan-interval is 60 seconds. If the O-RU takes 1 second to scan an individual VLAN, then after scanning every 60 out of the full range of VLAN IDs, the O-RU should repeat the scan for M-Plane connectivity on untagged and configured VLANs.

### 6.2.4 O-RU Management Plane IP Address Assignment

Automatic IP address assignment for the O-RU management plane can be achieved using different techniques:

1. IPv4 configuration using DHCPv4, RFC2131 [10] enables DHCP servers to configure IPv4 network address(es) on the ORU. An O-RU implementing IPv4 shall support the behaviour specified in RFC 4361 [33], using stable DHCPv4 node identifiers in their dhcp-client-identifier option.

NOTE 1: A network realized with multiple DHCP servers should ensure that their configurations are coordinated to ensure a common default gateway is provisioned in an O-RU which receives multiple DHCPv4 responses, e.g., when received over different interfaces.

NOTE 2: An O-RU may indicate that it supports configuration of routing information using RFC 3442, enabling static routes to be used by the O-RU when determining how to route uplink packets, e.g., when the O-RU supports multiple interfaces.

For O-RUs that support IPv6, both stateful and stateless address assignment procedures are supported:

2. IPv6 Stateless Address Auto-Configuration (SLAAC), RFC4862 [11] enables the O-RU to generate link-local and global addresses.

NOTE 3: A network realized with multiple IPv6-enabled routers that support dynamic address assignment is expected to use RFC 4191 to configure the preference of the default route prefixes learnt by the O-RU using SLAAC.

3. IPv6 State-full address configuration uses DHCPv6, RFC3315 [12] and enables DHCP servers to configure IPv6 network address(es) on the O-RU. DHCPv6 is transported using UDP, using the link-local address on the O-RU and a link-scoped multicast address on the DHCP server.

NOTE 4: The above does not restrict the realization of the DHCP server, which may be integrated with the O-DU, may be provided by the transport system, or may be accessed via a relay.

The DHCP server should operate using static bindings, i.e., ensuring an O-RU identified by a particular client hardware address will be re-allocated the same management plane IP address, e.g., after performing an O-RU reset procedure.

### 6.2.5 O-RU Controller Discovery

This clause provides how to automatically discover the O-RU Controller address(es).

O-RUs that have obtained their IPv6 addresses by stateless address auto-configuration, shall use stateless DHCPv6, RFC3736 [13], to obtain management plane configuration information.

Other O-RUs operating using stateful IPv4 or IPv6 address allocations shall obtain management plane configuration information during IP address allocation.

The O-RU as NETCONF Server shall be able to recover NETCONF Client information using the following DHCP Options, RFC8572 [14]:

* DHCPv4 OPTION V4\_SZTP\_REDIRECT [143]
* DHCPv6 OPTION\_V6\_SZTP\_REDIRECT [136]

These options are defined in [14] and are used to deliver bootstrap-server-list information to the O-RU. The O-RU shall use these options to recover the NETCONF client information using the above IANA defined DHCP options. The O-RU is not required to implement the remainder of the zerotouch capabilities defined in [14].

The above DHCP option provided information is encoded as a list of one or more server URIs, of the format “https://[:]” signalled to the O-RU. The DHCP server shall ensure that all NETCONF client information is encoded with these options, including the optional port information using the IANA assigned ports specified in RFC8071 [15]. The O-RU shall use the included port information to decide whether to call home using NETCONF/SSH or NETCONF/TLS. If no call home port is provided, the O-RU shall attempt to call home using NETCONF/SSH.

Other O-RUs which have had their IP address(es) manually configured, shall also have their O-RU Controller(s) manually configured.

For IPv4, the O-RU may request the OPTION\_V4\_SZTP\_REDIRECT by including its option code in the Parameter Request List (55) in DHCP discover/request messages.

For IPv6, the O-RU may request the OPTION\_V6\_SZTP\_REDIRECT option by including the requested option codes in the Option Request Option.

NOTE : These operations are optional because the DHCP server will already be aware that it is communicating with an O-RU based on the recovered vendor class option.

To enable O-RUs to operate in legacy environments where the DHCP server has not been enhanced with IANA defined DHCP options for zero touch NETCONF capability, an O-RAN defined vendor specific option can be used to signal all NETCONF client information to the O-RU using option 43 for DHCPv4 and option 17 for DHCPv6. Multiple instances of NETCONF client information may be signalled, encoded as a sequence of type/length/value fields.

The definition of the types used within the DHCPv4 option 43/DHCPv6 Option 17 depends on the vendor-class option reported by the O-RU in its DHCP messages.

When a legacy O-RU reports its vendor-class using the “o-ran-ru” prefix, the following types are defined:

Type: 0x01 – O-RU Controller IP Address

Type: 0x02 – O-RU Controller Fully Qualified Domain Name

When the O-RU reports its vendor-class using the “o-ran-ru2” prefix, the following types are defined:

Type: 0x81 – O-RU Controller IP Address

Type: 0x82 – O-RU Controller Fully Qualified Domain Name

Type: 0x86 – O-RU Call home protocol

In all cases, the Type is followed by the length, which is the hexadecimal encoding of length of value field in octets, and the Value.

When Type corresponds to an O-RU Controller IP Address, the value encodes IPv4 address(es) in hexadecimal format. For example, a single server with IPv4 address 198.185.159.144 will be encoded in an option 43 TLV as

Type 0x81 (or x01 for legacy)

Length: 0x04

Value: C6 B9 9F 90

When Type corresponds to an O-RU Controller Fully Qualified Domain Name, this encodes the string representation of domain name, using ACSII encoding (i.e., following for encoding used for the domain name in the Host Name DHCP Option 12). For example, a server with FQDN “controller.operator.com” will be encoded in an option 43 TLV as

Type 0x82 (or x02 for legacy)

Length: 0x17

Value: 63 6F 6E 74 72 6F 6C 6C 65 72 2E 6F 70 65 72 61 74 6F 72 2E 63 6F 6D

The format of the DHCPv6 option 17 follows the format of the DHCPv4 encoding, with the additional inclusion of an Enterprise Number prior to the TLV option data. The IANA allocated private enterprise number to be used with DHCPv6 option 17 is 53148.

When Type corresponds to the call home protocol, the value encodes whether an O-RU shall call home using NETCONF/SSH or NETCONF/TLS using the IANA defined ports in [15]. If no call home protocol type is provided, the O-RU shall use NETCONF/SSH. The format is encoded as follows:

Value 00 - O-RU shall attempt to call home using NETCONF/SSH

Value 01 - O-RU shall attempt to call home using NETCONF/TLS

For example, a DHCP server wanting to trigger the call home procedure using NETCONF/TLS will encode the option 43 TLV as

Type: 0x86

Length: 0x01

Value: 01

### 6.2.6 Multi-Vendor Plug-and-Play

#### 6.2.6.1 Introduction

As described in clause 6.4.2, an O-RU may optionally support certificate enrolment using CMPv2. 3GPP 32.509 [52] specifies how the O-RU supporting IPv4 can discover the IP address or FQDN of one or more Certification Authority (CA/RA) servers using DHCP Option 43.

An O-RU supporting IPv6 and certificate enrolment using CMPv2 shall additionally support the signalling of vendor specific options using DHCPv6 option 17. The format of the DHCPv6 option 17 follows the format of the DHCPv4 encoding, with the additional inclusion of an Enterprise Number prior to the TLV option data. The IANA allocated private enterprise number to be used with DHCPv6 option 17 is 53148 (as allocated by IANA to O-RAN Alliance).

An O-RU shall report any discovered multi-vendor plug-and-play servers using the o-ran-dhcp YANG model

#### 6.2.6.2 Certificate Enrolment

3GPP 33.310 [51] specifies the use of CMPv2 used by base stations to obtain an operator-signed certificate using a secured communication based on the vendor-signed certificate in the base station and a vendor root certificate pre-installed in the CA/RA server. While the approach has been defined for provisioning certificates for use in either IPSec or TLS, the same techniques defined for provisioning TLS certificates are specified to be re-used here to provision certificates for use in securing the SSHv2 RFC 6187 [31] based M-Plane connection. Hence, the TLS client CA is responsible for issuing certificates to NETCONF clients, irrespective of whether NECTONF is secured using TLS or SSHv2. Similarly, the TLS server CA is responsible for issuing certificates to NETCONF servers, irrespective of whether NECTONF is secured using TLS or SSHv2.

The handling of certificates, including certificate profiles, shall follow the rules defined in 3GPP 33.310 for TLS CA certificates. In addition:

* when an O-RU generates a certificate signing request it shall populate the Subject Distinguished Name field with a string that includes the O-RU manufacturer’s name, model and serial number. The exact Subject DN sub-field used is defined in the operator of the CA/RA server’s certificate policy.

NOTE 1: In future, an O-RAN defined certificate policy may be defined to normalize the sub-field definition across the O-RAN ecosystem.

NOTE 2: There are various characters that may not be permissible in the Subject Distinguished Name Field, e.g., “:” (colon, hexadecimal character 0x34), “.” (period, hexadecimal character 0x2E), "\_" (underscore, hexadecimal character 0x5F), “#” (hash, hexadecimal 0x23), “£” (pound, hexadecimal 0xa3), “\*” (asterisk, hexadecimal 0x2a) or “”” (double quote, hexadecimal 0x22). Manufacturers that include such characters in their name, model and/or serial number should ensure such characters are removed before including in the Subject Distinguished Name Field.

* when transferring messages to the CA/RA server, the O-RU shall use the “port number of the CA/RA server” and the “path to the CA/RA directory” as signalled using the DHCP options defined in 3GPP 32.509 [52]. If no DHCP based configuration is received by an O-RU, the O-RU shall use the default port 443 and default directory “/pkix/”.
* The CA/RA server shall include the trust anchor for the operator issued certificate and the appropriate certificate chains in the initialization response message.

NOTE 3: The trust anchor provisioned in the O-RU during certificate enrolment will typically be the same as the trust anchor provisioned in the NETCONF client(s), i.e., in O-DU and optionally SMO.

### 6.2.7 Event-Collector Discovery

This section describes how an O-RU automatically discovers the Event-Collector to which it shall send its pnfRegistration notification. The support by an O-RU of PNF Registration to a discovered Event-Collector is optional and hence this section only applies to those O-RUs that support this optional capability.

O-RUs that have obtained their IPv6 addresses by stateless address auto-configuration, shall use stateless DHCPv6, RFC3736 [13], to obtain Event-Collector information. Other O-RUs operating using stateful IPv4 or IPv6 address allocations shall obtain Event-Collector information during IP address allocation. Other O-RUs which have had their IP address(es) manually configured, shall also have their Event-Collector(s) and Event-Collector Notification Format manually configured.

The O-RU shall be able to recover Event-Collector information using O-RAN defined vendor specific option to signal Event-Collector information to the O-RU using option 43 for DHCPv4 and option 17 for DHCPv6.

The definition of the types used within the DHCPv4 option 43/DHCPv6 Option 17 are as follows:

Type: 0x83 – Event-Collector IP Address

Type: 0x84 – Event-Collector Fully Qualified Domain Name

Type: 0x85 – Event-Collector Notification Format

In this version of the specification, the operation of an O-RU when receiving multiple instances of the Event-Collector IP Address and/or Event-Collector FQDN information is not defined.

In all cases, the Type is followed by the length, which is the hexadecimal encoding of length of value field in octets, and the Value.

When Type corresponds to an Event-Collector IP Address, the value encodes IPv4 address(es) in hexadecimal format. For example, an Event-Collector with IPv4 address 198.185.159.144 will be encoded in an option 43 TLV as

Type 0x83

Length: 0x04

Value: C6 B9 9F 90

When Type corresponds to an Event-Collector Fully Qualified Domain Name, this encodes the string representation of domain name, using ACSII encoding (i.e., following for encoding used for the domain name in the Host Name DHCP Option 12). For example, a server with FQDN “collector.operator.com” will be encoded in an option 43 TLV as

Type 0x84

Length: 0x17

Value: 63 6F 6C 6C 65 63 74 6F 72 2E 6F 70 65 72 61 74 6F 72 2E 63 6F 6D

In this version of the specification, the operation of an O-RU when receiving an Event-Collector FQDN that is subsequently resolved by the O-RU to more than one IP address (i.e., returning multiple Address records) is not defined.

The format of the DHCPv6 option 17 follows the format of the DHCPv4 encoding, with the additional inclusion of an Enterprise Number prior to the TLV option data. The IANA allocated private enterprise number to be used with DHCPv6 option 17 is 53148.

When Type corresponds to an Event-Collector Notification Format, the value encodes in what format the Event-Collector expects to receive asynchronous notifications. In this version of the specification, only a single format is defined:

Value 00 - Event-Collector expects the notification to be signalled using the format as specified in the ONAP VES event listener specification [36].

For example, an Event-Collector expecting the pnfRegistration notification to be signalled using the ONAP defined format will encode the option 43 TLV as

Type 0x85

Length: 0x01

Value: 00

## 6.3 NETCONF Call Home to O-RU Controller(s)

The O-RU aims to have NETCONF sessions with all of the known O-RU Controller(s), either discovered using the DHCP options defined in clause 6.2.5, provisioned by an existing NETCONF client, or statically configured. An O-RU controller may attempt to autonomously initiate a NETCONF session with the O-RU, e.g., triggered by the pnfRegistration procedure. In order to support NETCONF clients corresponding to known O-RU Controllers that either do not attempt to initiate a NETCONF session with the O-RU, or are prohibited from doing so, e.g., because of Network Address Translation limitations, the O-RU shall call home to all known O-RU Controllers with which it does not already have an active NETCONF session.

If the O-RU is unable to establish a NETCONF session with some of the known O-RU Controller(s), the O-RU shall use the “re-call-home-no-ssh-timer” to repeatedly re-perform the call home procedure to all known O-RU Controllers with which the O-RU does not have an established NETCONF session.

NOTE: The same value of timer shall be used, irrespective of whether SSH or TLS is being used to transport the NETCONF session.

If the O-RU is unable to trigger the establishment of NETCONF session with at least one known O-RU Controller after having repeated the call home procedure a total of max-call-home-attempts per O-RU Controller, then the O-RU should perform an autonomous reset.

The O-RU shall use RFC 8071 [15] whereby the O-RU (NETCONF Server) initiates a TCP connection to the NETCONF client. The port used by the O-RU shall be the one signalled using the RFC 8572 DHCP option [14], else, if no port was signalled, the O-RU shall use the IANA-assigned port 4334 to indicate that the O-RU wants to use SSHv2 to secure the NETCONF connection and the IANA-assigned port 4335 to indicate that the O-RU wants to use TLS to secure the NETCONF connection. As illustrated in Figure 6.3.1, when the NETCONF client accepts a TCP connection on the allocated port, it initiates an SSH session/TLS connection with the NETCONF Server. Using this SSH session/TLS connection, the NETCONF client initiates a NETCONF session.

**[Figure 6.3.1: Outline of NETCONF call home procedure]**

The O-RU shall ensure that a persistent connection to any NETCONF client with “sudo” privileges is maintained by actively testing the aliveness of the connection using the keep-alive mechanism defined in [15]. The establishment of NETCONF client privileges is covered in clause 6.5.

## 6.4 NETCONF Connection Establishment

The identity of the NETCONF server (O-RU) shall be verified and authenticated by the NETCONF client according to local policy before password-based authentication data or any configuration or state data is sent to or received from the NETCONF server.

When using SSHv2, public key-based host authentication shall be used for authenticating the server (RFC 4253) by the clients. In addition, server authentication based on X.509 certificates may also be provided [31].

When using TLS, X.509 certificate-based authentication shall be used for mutual authentication between the NECTONF client and NETCONF server.

NOTE: SSHv2 based public key-based host authentication requires that the SSH server (O-RU) public keys are provisioned in the NETCONF client (e.g., O-DU and/or SMO). As an alternative, RFC4251 mentions that “a possible strategy is to only accept a host key without checking the first time a host is connected, save the key in a local database, and compare against that key on all future connections to that host.”. This option simplifies the key management procedure as it doesn’t require to pre-populate them in O-DU/SMO (SSH client) but obviously at the price of degraded security, therefore the support of this option shall be configurable and left to operator’s choice.

### 6.4.1 NETCONF Security

As specified in clause 5.4, this version of the O-RU Management Plane Specification uses TLS 1.2 or SSHv2 for mutual authentication between the NETCONF server (O-RU) and the NETCONF client (O-DU or SMO). Support for TLS 1.2 is optional and support for SSHv2 is mandatory as described in Table 5.4.2.

If multiple NETCONF sessions are established to an O-RU, those sessions shall be established over separate SSH tunnels/TLS connections.

### 6.4.2 NETCONF Authentication

This version of the O-RU Management Plane Specification supports SSHv2 using password authentication method for SSHv2 [6] and client authentication based on X.509 certificates [31], as well as optional support for TLS 1.2 using X.509 certificate-based authentication.

The identity of the NETCONF server (O-RU) shall be verified and authenticated by the NETCONF client (O-DU or SMO) according to local policy before authentication data or any configuration or state data is sent to or received from the server.

The identity of the NETCONF client (O-DU or SMO) shall be verified and authenticated by the NETCONF server (O-RU) according to local policy (X.509 certificate-based or username/password) to ensure that the incoming NETCONF client request is legitimate before any configuration or state data is sent to or received from the NETCONF client. The server shall also perform proper authorization of the client before accepting any request.

If authentication is based on X.509 certificates, for the purposes of user authentication, the mapping between certificates and user-name is provided by the SubjectAltName field of the X.509 certificate, which means that the user name is coded in the subjectAltName. The username is determined from the subjectAltName using the rules defined in RFC 7589. For the purposes of NETCONF server authentication, RFC 7589 [41] specifies server identity based on RFC 6125 [40].

Upon initial system initialization, the O-RU is configured with a default account. The specific details of the default account are to be agreed between operator and vendor. An example of a default user account for account-type PASSWORD is one with username “oranuser”. An example of a default user account for account-type CERTIFICATE is map type “san-rfc822-name” with an rfc822-name of “oranuser@o-ran.org”.

The default account may be of account-type PASSWORD, in which case a default password also needs to be defined and configured in the O-RU, for example “o-ran-password”.

NOTE 1: As the default account may be operator specific, this may require that the O-RU provides facilities to configure securely this default account at installation time (i.e., before the O-RU is connected to the O-RU Controller).

If user authentication is based on X.509v3 certificate during O-RU plug and play, to support zero touch for the first NETCONF connection, the O-RU shall support the default mapping between certificate and default NETCONF account which will map any authenticated X.509 v3 certificate to this default O-RAN account.

NOTE 2: The trust anchor for O-RU shall be provisioned automatically with online CA server during O-RU Plug and Play, and it shall be same as the trust anchor of the O-RU Controller(s), thus avoiding the need for manual configuration of the peer trust anchor for O-RU.

The default account is a member of the “sudo” access control group (see clause 6.5 for details of groups/privileges) as it can be used to create other accounts (see clause 6.4.3).

The identity of the SSH client (NETCONF client) shall be verified and authenticated by the SSH server (O-RU) according to local policy to ensure that the incoming SSH client request is legitimate before any configuration or state data is sent to or received from the SSH client.

Upon initial system initialization, the NETCONF client can authenticate itself to the O-RU using SSH Authentication, with the agreed default username and password.

If authentication based on X.509 certificates according to [31] is supported by SSH client and server, the certificates need to be installed at initial system initialization, or can be obtained through certificate enrolment with operator’s PKI (certificate enrolment as defined by 3GPP with CMPv2 protocol between the NE and the operator’s CA).

### 6.4.3 User Account Provisioning

The NETCONF client with suitable privileges may provision user accounts on the O-RU, including the accounts (users) name, password, group (see clause 6.5 for details of groups/privileges) and whether a particular account is enabled or disabled.

* The name for the user is a string which should be between 3-32 characters. The first character should be a lowercase letter. The remaining characters should be lowercase letters or numbers.
* The account-type is an enumeration, indicating whether password or certificate-based authentication is used for this account.
* The password is a string between 8-128 characters. Allowed characters in the password field include lowercase and uppercase letters, numbers and the special characters: ! $ % ^ ( ) \_ + ~ { } [ ] . – The password leaf is not present for those user accounts associated with certificate-based authentication.
* The access control group associated with an account (see clasue 6.5 for details of groups/privileges).
* Whether an account is enabled. The YANG model ensures that at least one user account is always enabled on the O-RU

The new account information (user name, password, access group and whether the account is enabled) shall be stored in reset persistent memory in O-RU.

If certificate-based client authentication is used no password needs to be provisioned. At time of SSH connection, user’s authorization is done based on the X.509 certificate’s SubjectAltName field that codes the associated account’s name.

When other user account (sudo) is created, the NETCONF client closes existing NETCONF session as described in clause 6.8. Then, the O-RU disables the default account and default account stays disabled over the resets. The default account becomes enabled when the O-RU is reset to the factory default software by following the procedures defined in clause 8.8. Any other way to enable the default account is not precluded as O-RU vendor implementation matter.

The security principle defined in this section shall follow those defined for the default account and default mapping, i.e., the O-RU Controller shall create a new mapping.

NOTE: Depending on the EE/CA certificate of the O-RU Controller, the map type can still be specified but with specific fingerprint of the EE/CA certificate or based on SubjectAltName of EE/CA certificate as specified in clause 6.4.2.

## 6.5 NETCONF Access Control

This subsection defines the access control for NETCONF clients. Its motivation is that when multiple NETCONF clients (users) are defined, the NETCONF access control mechanism enables the NETCONF server to limit some operations for one client but allow full access for another client. In particular, for hybrid access configuration as introduced in clause 5, this allows the privileges associated with the NETCONF client in the O-DU to be distinct and different from the privileges associated with the NETCONF client in the SMO.

In order to support interoperable access control management, the NETCONF Server shall use the IETF NETCONF Access Control Model [RFC8341].

Currently six access control groups are defined per NETCONF session: “sudo”, “smo”, “hybrid-odu”, “nms”, “fm-pm”, and “swm”. Table 6.5.1 maps the group name to different privileges. Privileges are defined per namespace for read “R”, write “W” and execute “X” RPC operations or subscribe to Notifications.

NOTE: When operating in hybrid management, the definition of above groupings does not preclude the NETCONF client in a centralized network management system from being configured “sudo” privileges that permit it to edit the configuration used by an O-RU. However, importantly the operation of the O-DU in those situations may not be defined. For example, an O-DU when operating with an O-RU which receives an autonomous reset RPC from a centralized NMS may not result in the O-DU recovering the o-ran-operations:operational-info/operational-state/restart-cause from the O-RU to then determine that an NMS triggered reset has been performed. In order to reduce the possibility of such a scenario, it is recommended that when operating in hybrid mode of operation, the NETCONF client in the O-DU is associated with the “hybrid-odu” privilege group and the NETCONF client in the SMO is associated with the “smo” privilege group.

**[Table 6.5.1: Mapping of account groupings to O-RU module privileges (continues over page)]**

This mapping shall be encoded in the rule list in ietf-netconf-acm.yang model. This rule list shall be unmodifiable by any NETCONF client.

The same model is responsible for configuring the mapping between different user-names and groups.

## 6.6 NETCONF capability discovery

The O-RU advertises its NETCONF capabilities in the NETCONF Hello message. The Hello message provides an indication of support for standard features defined in NETCONF RFCs as well as support for specific namespaces.

NETCONF capabilities are exchanged between the O-RU and the NETCONF client(s). Examples of capabilities include [3]:

* Writable-running Capability
* Candidate Configuration Capability and associated Commit operation
* Discard change operation
* Lock and un-lock operations
* Confirmed commit Capability
* Cancel commit operation
* Rollback on error capability
* Validate Capability
* Startup configuration capability
* URL capability
* XPATH capability
* Notifications
* Interleave capability

All O-RAN O-RUs shall support the XPATH capability, NETCONF Notifications and at least one of the writeable-running and candidate configuration capabilities.

The NETCONF client uses the get RPC together with sub-tree based and XPATH based to recover particular sub-trees from the O-RU. Please see clause 9 for more information on NETCONF based configuration management.

In order to avoid interactions between the operation of supervision watchdog timer (see clause 6.7) and the confirmed commit timer (default value set to 600 seconds in RFC 6241), when using the NETCONF confirmed commit capability, a NECTONF client with “sudo” privileges shall ensure the confirmed-timeout is less than the supervision-notification-interval timer (default value 60 seconds in o-ran-supervision.yang).

## 6.7 Monitoring NETCONF connectivity

This section provides description of NETCONF connectivity monitoring for persistent NETCONF session. Additional procedures for O-RUs that support the optional NON-PERSISTENT-MPLANE feature to monitor the communication path between the O-RU and Event-Collector are defined in clause 18.6.

When having a session with a NETCONF client that has subscribed to receive the supervision-notification, the O-RU operates watchdog timers (supervision timer and notification timer) to ensure that the session to the NECTONF client is persistent, as illustrated in Figure 6.7.1. The O-RU provides NETCONF Notifications to indicate to remote systems that its management system is operational.

An O-RU controller that has subscribed to the supervision-notification is expected to use the RPC to indicate to O-RU the O-RU controller is operational.

NOTE 1: This supervision is intended to be used with the NETCONF client associated with the operation of the peer to the O-RU’s lower layer split and clause 6.5 describes which NETCONF clients have privileges to subscribe to the supervisionnotification.

NOTE 2: A NETCONF server shall support the operation of individual supervision watchdog timers for each NETCONF client which has subscribed to supervision-notification.

The privileged NETCONF client is responsible for automatically enabling the operation of the watchdog timers by creating supervision-notification subscription. After operation of watchdog timers is enabled - the timers are considered as running.

The O-RU uses two timers, referred generically as watchdog timers, to support the bi-directional monitoring of NETCONF connectivity:

* Notification timer:  
  Value: Equal to supervision-notification-interval (default value: 60s)  
  Operation: The O-RU sends supervision-notification to those NETCONF clients that have subscribed to receive such notifications. The O-RU sends supervision-notification, at the latest when the timer expires. The O-RU Controller confirms that NETCONF connectivity to the O-RU is operational by receiving the notification.
* Supervision timer:  
  Value : Equal to supervision-notification-interval (default value: 60s) + guard-timer-overhead (default value: 10s)  
  Operation: The O-RU identifies supervision failure operation when the timer expires. To avoid supervision timer expiration, a NETCONF client who has subscribed to receive the supervision-notification should repeatedly reset this supervision timer. Such supervision timer reset is considered by O-RU as confirmation that NETCONF connectivity to the O-RU Controller is operational.

The O-RU enables dedicated watchdog timers for specific NETCONF client when it receives a RPC from a NETCONF client with required privileges. The notification timer shall be started when the O-RU receives a RPC, but how the O-RU treats the supervision timer is up to O-RU’s implementation based on the above definition. After the watchdog timers have been enabled, the O-RU is responsible for sending supervision-notification after the expiry of the notification timer. An O-RU Controller who has subscribed to the supervision-notification shall be prepared to receive the notification at any time when the watchdog timers are running.

The NETCONF client is responsible for sending supervision-watchdog-reset RPC in order not to cause the Supervision timer to expire, and the O-RU should send next notification timestamp as next-update-at in reply.

NOTE 3: next-update-at is just informative.

In the supervision-watchdog-reset RPC, the NETCONF client may configure new values for the watchdog timers using RPC parameters "supervision-notification-interval" and "guard-timer-overhead. When the O-RU receives the supervision-watchdog-reset RPC, it is responsible for resetting its supervision timer and notification timer. When the watchdog timers are running, the O-RU shall be prepared to receive supervision-watchdog-reset RPC at any time - also within supervision timer period.

The NETCONF client can set new value of watchdog timers without receiving supervision-notification from the O-RU. The new values are taken into use immediately with respect to supervision-watchdog-reset RPC content. The next notification should be expected not later than at the moment addressed in timestamp provided by RPC reply.

NOTE 4: If another NETCONF client has locked the running configuration, e.g., when operating in hybrid mode of operation, and if the O-RU Controller attempts to configure a new value of the watchdog timer(s) by sending the supervision-watchdog-reset RPC, then the RPC operation to reset the watchdog timer will succeed, but the related backend implementation to modify the watchdog timer(s) may fail. In such circumstances, the O-RU may use the error-message in the RPC output to indicate to the O-RU Controller that the configuration modification has failed.

If the supervision timer expires, the O-RU will enter “supervision failure” condition, as described in clause 141. If all NETCONF sessions to NECTONF clients with “sudo” privileges are closed, the O-RU shall immediately disable operation of the supervision timer.

**[Table 6.7.1: Monitoring NETCONF Connectivity]**

NOTE: This figure uses create-subscription for the single stream "supervision-notification". In order to subscribe multiple notifications, the appropriate create-subscription message is required. Please refer to clasue 11.3 for the appropriate example of create-subscription of multiple notifications.

The figure illustrates the O-RU ceasing supervision operation triggered by two options:

1. The supervision timer expires. In such case the O-RU performs Supervision Failure handling as described in clause 14.1.1.
2. The NETCONF client terminates the subscription to the supervision-notification. The NETCONF client can either close the subscription session, terminate the NETCONF session or remove subscription to supervision notification stream. In such case the O-RU performs Supervision Termination handling as described in clause 14.1.2

## 6.8 Closing a NETCONF Session

A NETCONF client closes an existing NETCONF session by issuing the RPC close-session command. The O-RU shall respond and close the SSH session or TLS connection. The O-RU shall then re-commence call home procedures, as described in clasue 6.3.

NOTE 1: Under normal operations, it is expected that at least one NETCONF session with “sudo” or “hybrid-odu” privileges are long-lived and used to repeatedly reset the O-RU’s supervision watchdog timer. NECTONF clients associated with other privilege groups are not expected to operate using persistent NETCONF sessions.

NOTE 2: If a NETCONF client has been previously become known to an O-RU by being configured using NETCONF, and the NETCONF client is subsequently removed from the O-RU’s configuration, e.g., by a second NETCONF client with “sudo” privileges, the NETCONF server shall force the termination of the NETCONF session to the removed client.

## 6.9 PNF Registration

### 6.9.1 Introduction

The support by an O-RU of PNF Registration to a discovered Event-Collector is optional and hence claue 6.9 only applies to those O-RUs that support this optional capability. An O-RU that support pnfRegistration shall also support the Monitoring the Communications Channel between O-RU and Event-Collector as defined in clause 18.6.

### 6.9.2 PNF Registration Procedure

The pnfRegistration notification is a JSON encoded message sent from the O-RU to the discovered Event-Collector using REST/HTTPS. As a pre-condition to performing PNF Registration, the O-RU first receives the Event-Collector information encoded in a DHCP/DHCPv6 option as described in clause 6.2.7. The O-RU shall attempt to establish a HTTP connection to the discovered Event-Collector using TLS to authenticate the connection. It shall then signal the pnfRegistration notification over the HTTP/TLS connection. The sending of the pnfRegistration notification is repeated periodically until the SMO establishes a NETCONF session with the O-RU. These procedures are illustrated in Figurew 6.9.2.1.

An O-RU that is performing the PNF registration procedure whilst simultaneously performing the call home procedure described in clause 6.3, shall be able to determine that the SMO has established a NETCONF session with the O-RU. This is identified by the O-RU analysing the source IP address from which the NETCONF originates, based on the assumption that the NETCONF session from the SMO originates from an IP address that is distinct from the IP address(es) of the “known O-RU Controller(s)” to which the O-RU is simultaneously performing the call home procedure.

**[Figure 6.9.2.1: PNF Registration Procedure]**

## 6.10 Encoding of PNF Registration Notification

In this version of the specification, the encoding of the pnfRegistration notification follows the ONAP definition [37].

The pnfRegistration notification shall include the IP address information necessary for a NETCONF client to establish IP connectivity to the NETCONF Server in the O-RU, i.e., shall include the field oamV4IpAddress when the O-RU has a configured IPv4 interface and/or the field oamV6IpAddress when the O-RU has a configured IPv6 interface.

The contents of the pnfRegistration notification are derived from the O-RU’s configuration database using Table 6.10.1. An O-RU shall support the o-ran-hardware.yang model revision 5.0.0, or later, which defines the schema nodes corresponding to unitFamily and unitType values and the o-ran-operations.yang model revision 5.0.0, or later, which defines the schema nodes corresponding to the version of pnfRegistration fields.

**[Table 6.10.1: Mapping from O-RU’s Operational Data to PnfRegistration fields]**

# 7 O-RU to O-DU Interface Management

## 7.1 O-RU Interfaces

An O-RU has a number of network interfaces, including Ethernet, VLAN and IP interfaces. This section describes the management of these network interfaces.

The O-RU’s configuration for its interfaces is defined using the o-ran-interfaces.yang module. This module augments the standard ietf-interfaces.yang and ietf-ip.yang modules. The O-RU’s interfaces are built on a layering principle where each interface has a unique **name**.

All interfaces are referenced by their **port-number** and **name**. The base interface corresponds to the Ethernet interface. These leafs describe the maximum transmission unit (**l2-mtu**), the hardware-address as well as optional alias mac addressees that may be used to transport the CU plane. Above the Ethernet interface are VLAN interfaces. Both Ethernet and VLAN interfaces can support IP interfaces. IP interfaces are defined using the standard ietf-ip.yang model. Accordingly, each IP interface can have an IPv4 and/or IPv6 interface(s) defined. Operational state associated with these interfaces provide additional detail of the layer 3 configuration, including prefix(es), domain name servers and default gateway addresses.

Finally, leafs associated with CoS and DSCP marking are defined, enabling independent configuration of CoS and DSCP markings for u-plane, c-plane and m-plane traffic. As a default, all user-plane flows are marked identically by the O-RU. Optionally, the interfaces can be configured to support enhanced user plane marking for up-link traffic whereby different CoS or DSCP values can be configured. This enables individual receive endpoints in the O-RU to be configured with different markings to then enable differentiated handling of up-link flows by the transport system.

Because the o-ran-interfaces model defines augments to the ietf-interfaces model, the O-RU can leverage the definition of operational state in ietf-interfaces to optionally report packet and byte counts on a per interface basis. A single RPC is defined in the o-ran-interfaces module, to enable these counters to be reset.

## 7.2 Transceiver

The o-ran-transceiver YANG module is used to define operational state for the pluggable transceiver module (like SFP, SFP+, SFP28, XFP and QSFP, QSFP+, QSFP28, QSFP56). Each transceiver is associated with a unique **interface-name** and **port-number**

A digital diagnostic monitoring interface for optical transceivers is used to allow access to device operating parameters. As specified in SFF-8472 [16] and SFF-8636 [34], data is typically retrieved from the transceiver module in a file. This file may be obtained from O-RU by the NETCONF client. Please see clause 9 for more details.

With QSFP form factor, the optical links may be multi-wavelengths (4xTx & 4xRx) and/or multi-fibres (MPO - Multifibre Parallel Optic). The QSFP digital diagnostic interface [34] describes the use of optical lanes and the O-RU interface management defines alarm 29:“transceiver fault” for all media lanes.

The byte with offset i (i=0, …, 511) from the beginning of the file is the byte read from data address i of the transceiver memory at two-wire interface address 0xA0 if i<256, otherwise it is the byte read from data address i-256 of the transceiver memory at two-wire interface address 0xA2. The retrieved data is stored in the file without any conversion in binary format.

The O-RU stores data from the transceiver module on transceiver module detection during start-up. The data from the transceiver module is saved in the file. A NETCONF client can upload it by using the File Upload procedure defined in clause 12. The O-RU does not synchronize contents of the file with transceiver memory in runtime, therefore bytes representing dynamic information are expected to be outdated. The O-RU does not remove the file on transceiver module removal. If a transceiver module is inserted during File Upload procedure, then the procedure may provide a file with previous content or fail (with failure reason as listed in File Upload procedure). If the O-RU is unable to retrieve the data from the transceiver module or it is not present, then the O-RU does not create the file or removes the file created earlier

NOTE: File Upload procedure requesting non-existing file shall fail.

The file name shall have the following syntax:

sfp\_{portNumber}.sffcap

where {portNumber} is the value of port-number leaf of the corresponding list of port-transceiver data. Examples: sfp\_0.sffcap, sfp\_1.sffcap.

## 7.3 C/U Plane VLAN Configuration

Within the o-ran-interfaces YANG model, each named Ethernet interface includes a leaf to indicate whether VLAN tagging is supported. By default, VLAN tagging is enabled on all interfaces. This permits an O-RU to autonomously discover that it is connected to a trunk port, as described in clause 6.2.3.

When an O-RU is connected to a trunk port, VLANs will also typically be assigned to the C/U plane connections. The VLAN(s) used to support C/U plane transport may be different from the VLAN(s) used to support management plane connectivity. The VLAN assigned to the U-Plane shall be the same as the VLAN assigned to the C-Plane for any given eAxC\_ID. When different VLANs are used, the C/U plane VLANs shall be configured in the O-RU by the NETCONF client. In such circumstances, as defined in o-ran-interfaces, the NETCONF client shall configure separate named interfaces for each active VLAN. This configuration will define a C/U-Plane named VLAN interface as being the higher-layer-if reference for the underlying Ethernet interface and the underlying Ethernet interface is defined as being the lower-layer-if reference for the named VLAN interface.

## 7.4 O-RU C/U Plane IP Address Assignment

In this release, the support for C/U plane transport over UDP/IP is optional and hence this section only applies to those O-RUs that support this optional capability.

An O-RU that supports C/U plane transport over UDP/IP shall support IPv4 and/or IPv6 based transport. A NETCONF client can receive a hint as to whether an O-RU supports a particular IP version by using the get RPC to recover the list of interfaces supported by the O-RU and using the presence of the augmented ipv4 container or ipv6 container in the o-ran-interfaces YANG module as an indication that a particular IP version is supported.

The IP interface(s) used to support UDP/IP based C/U plane transport may be different than the IP interface(s) used to support management plane connectivity. When different IP interface(s) is/are used, the C/U plane IP interfaces shall be configured in the O-RU by the NETCONF client by using the ietf-ip YANG model to configure the IPv4 container and/or IPv6 container. When defined by the NETCONF client, this interface shall be configured using either a named Ethernet interface (i.e., where the interface type is set to ianaift:ethernetCsmacd) and/or a named VLAN interface (i.e., where the interface type is set to ianaift:l2vlan), depending upon whether VLANs are used to support IP based C/U plane traffic.

When a separate C/U plane IP interface is configured by the NETCONF client, additionally the NETCONF client may statically configure the IP address(es) on this/these interface(s). If the NETCONF client does not statically configure an IP address, the O-RU shall be responsible for performing IP address assignment procedures on the configured interfaces.

When an O-RU has not been configured with a static IP address, the O-RU shall support the IP address assignment using the following techniques:

When the O-RU supports IPv4:

1. IPv4 configuration using DHCPv4 [10].

and when the O-RU supports IPv6:

2. IPv6 Stateless Address Auto-Configuration (SLAAC) [11].

3. IPv6 State-full address configuration uses DHCPv6 [12].

## 7.5 Definition of processing elements

The CU-plane application needs to be uniquely associated with specific data flows. This association is achieved by defining an O-RU “processing element” which can then be associated with a particular C/U plane endpoint address [2] or delay measurement operation. Unless specified otherwise, a common processing element is required to be configured for the control and user-plane application components associated with any individual eAxC\_ID.

The O-RU management plane supports different options for defining the transport-based endpoint identifiers used by a particular processing element (used depending on transport environment), supporting the following 3 options:

* Processing element definition based on usage of different (alias) MAC addresses;
* Processing element definition based on a combination of VLAN identity and MAC address; and
* Processing element definition based on UDP-ports and IP addresses.

NOTE : There is no well-defined source port currently allocated by IANA for the o-ran application and hence the NETCONF client is responsible for configuring this port number in the O-RU.

A processing element defines both the local and remote endpoints used with a specific data flow. The processing element definition includes its element **name** which is then used by other systems to refer to a particular processing element instance.

The o-ran-interfaces YANG model is used to define feature support for C/U plane transport based on alias MAC addresses and UDP/IP. The exchange of NETCONF capabilities is used to signal which optional capabilities are supported by the O-RU, as described in Annex C.

The o-ran-processing-elements YANG model uses a processing-elements container to define a list of processing elements. Each processing element is identified by a unique element name. Each processing element references a particular interfacename used to support the data flows associated with a particular processing element. Depending upon the type of C/U plane transport session, additionally leafs are configured that specify MAC addresses, and/or VLANs and/or IP addresses and/or UDP ports used to identify a particular processing element.

The O-RU may discard any received CU-plane messages , i.e., eCPRI/IEEE 1914 frames/packets, which are not transported using a configured processing element.

## 7.6 O-DU Verification of C/U Plane Transport Connectivity

### 7.6.1 C/U Plane Transport Connectivity Verification

As described above, there will likely be multiple C/U-plane data flows being exchanged between the O-DU and the O-RU. In order to enable checks verifying end-to-end transport connectivity between the O-DU and O-RU, the O-RU shall support transport connectivity check capabilities using a request/reply function, as illustrated in Figure 7.6.1.1.

Using that connectivity monitoring procedure, reachability/connectivity checks between user plane endpoints can be performed by the O-DU:

* During O-RU configuration, to validate the transport configuration
* At runtime to monitor network connectivity

In packet networks connectivity checking is usually done by exchanging probe-messages between the endpoints. The periodicity of this exchange depends on the use case. For availability measurement, the only use case relevant for this specification, the periodicity is usually between 1 and 60 seconds.

Two different network protocols are defined for performing the transport connectivity check procedure:

* For C/U sessions over Ethernet: Loop-back Protocol (LB/LBM) as defined by IEEE 802.1Q (amendment 802.1ag) [17].
* When the O-RU supports C/U sessions over IP: UDP echo, RFC 862 [18].

**[Figure 7.6.1.1: C/U Plane Transport Connectivity Verification]**

### 7.6.2 Ethernet connectivity monitoring procedure

#### 7.6.2.1 Monitoring Procedure

If the O-RU and O-DU are operating their C/U sessions on Ethernet, the transport connectivity verification checks operate at the Ethernet layer. In this O-RU Management Plane Specification, the protocol for Ethernet connectivity monitoring is based on the Loop-back Protocol as defined by IEEE 802.1Q (amendment 802.1ag) [17].

For the purpose of connectivity monitoring all C/U -plane messaging endpoints in the fronthaul network are part of the same Maintenance Entity (ME). They each get the assigned the role of a Maintenance association End Point (MEP) for LBM.