

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](#_Toc184886455)

[History 5](#_Toc184886456)

[Keywords: 5](#_Toc184886457)

[Foreword 5](#_Toc184886458)

[Modal verbs terminology 5](#_Toc184886459)

[Executive summary 5](#_Toc184886460)

[1. Scope 6](#_Toc184886461)

[2. References 6](#_Toc184886462)

[2.1 Normative References 6](#_Toc184886463)

[3 Definitions of Terms and Abbreviations 9](#_Toc184886464)

[3.1 Terms 9](#_Toc184886465)

[3.3 Abbreviations 11](#_Toc184886466)

[4. General 13](#_Toc184886467)

[4.1 Conventions 13](#_Toc184886468)

[4.2 Topics for Future Specification Versions 13](#_Toc184886469)

[4.3 Revision and Compatibility Handling 13](#_Toc184886470)

[4.4 Namespace Compatibility Handling 14](#_Toc184886471)

[5 High Level Description 15](#_Toc184886472)

[5.1 Top level functional description, terminology, including hybrid, hierarchical 15](#_Toc184886473)

[5.1.1 Architecture for O-RAN WG4 Fronthaul functional split 15](#_Toc184886474)

[5.1.2 M-Plane architecture model 16](#_Toc184886475)

[5.1.3 Transport Network 20](#_Toc184886476)

[5.1.4 M-Plane functional description 21](#_Toc184886477)

[5.2 Interfaces 26](#_Toc184886478)

[5.3 YANG Module Introduction 27](#_Toc184886479)

[5.4 Security 28](#_Toc184886480)

[6 “Start-up” installation 30](#_Toc184886481)

[6.1 General 30](#_Toc184886482)

[6.2 Management Plane Transport aspects 37](#_Toc184886483)

[6.2.1 Transport Establishment 37](#_Toc184886484)

[6.2.2 O-RU identification in DHCP 42](#_Toc184886485)

[6.2.3 Management Plane VLAN Discovery Aspects 44](#_Toc184886486)

[6.2.4 O-RU Management Plane IP Address Assignment 47](#_Toc184886487)

[6.2.5 O-RU Controller Discovery 48](#_Toc184886488)

[6.2.6 Multi-Vendor Plug-and-Play 53](#_Toc184886489)

[6.2.7 Event-Collector Discovery 56](#_Toc184886490)

[6.3 **NETCONF Call Home to O-RU Controller(s)** 60](#_Toc184886491)

[6.4 **NETCONF Connection Establishment** 64](#_Toc184886492)

[6.4.1 NETCONF Security 65](#_Toc184886493)

[6.4.2 NETCONF Authentication 66](#_Toc184886494)

[6.4.3 User Account Provisioning 69](#_Toc184886495)

[6.5 NETCONF Access Control 72](#_Toc184886496)

[6.6 NETCONF capability discovery 74](#_Toc184886497)

[6.7 Monitoring NETCONF connectivity 76](#_Toc184886498)

[6.8 Closing a NETCONF Session 81](#_Toc184886499)

[6.9 PNF Registration 81](#_Toc184886500)

[6.9.1 Introduction 81](#_Toc184886501)

[6.9.2 PNF Registration Procedure 81](#_Toc184886502)

[6.10 Encoding of PNF Registration Notification 82](#_Toc184886503)

[7 O-RU to O-DU Interface Management 82](#_Toc184886504)

[7.1 O-RU Interfaces 82](#_Toc184886505)

[7.2 Transceiver 83](#_Toc184886506)

[7.3 C/U Plane VLAN Configuration 84](#_Toc184886507)

[7.4 O-RU C/U Plane IP Address Assignment 84](#_Toc184886508)

[7.5 Definition of processing elements 85](#_Toc184886509)

[7.6 O-DU Verification of C/U Plane Transport Connectivity 86](#_Toc184886510)

[7.6.1 C/U Plane Transport Connectivity Verification 86](#_Toc184886511)

[7.6.2 Ethernet connectivity monitoring procedure 86](#_Toc184886512)

[7.6.3 IP connectivity monitoring procedure 87](#_Toc184886513)

[7.7 C/U-Plane Delay Management 88](#_Toc184886514)

[7.7.1 Introduction 88](#_Toc184886515)

[7.7.2 Delay Parameters 88](#_Toc184886516)

[7.8 O-RU Adaptive Delay Capability 88](#_Toc184886517)

[7.9 Measuring transport delay parameters 88](#_Toc184886518)

[7.10 O-RU Monitoring of C/U Plane Connectivity 88](#_Toc184886519)

[7.11 Bandwidth Management 88](#_Toc184886520)

[8 Software Management 89](#_Toc184886521)

[9 Configuration Management 89](#_Toc184886522)

[10 Performance Management 89](#_Toc184886523)

[11 Fault Management 89](#_Toc184886524)

[12 File Management 89](#_Toc184886525)

[13 Synchronization Aspects - ING 89](#_Toc184886526)

[13.1 Introduction 89](#_Toc184886527)

[13.2 Sync Status Object 90](#_Toc184886528)

[13.3 Sync Capability Object 90](#_Toc184886529)

# 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

<Perplexity>

네임스페이스 형식

* O-RAN YANG 모델의 네임스페이스 형식: "urn:o-ran:<model-name>:<model-number>"
* 새로 정의된 YANG 모델의 초기 <model-number>는 "1.0"입니다.
* 문서에서 모델을 일반적으로 참조할 때는 <model-number>를 "x.y"로 표시하여 특정 <model-name>의 모든 버전을 포함합니다.

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

<Perplexity>

하위 계층 기능 분할

O-RAN 프론트홀 사양은 하위 계층 기능 분할을 다룹니다. 이 분할은 O-DU(O-RAN Distributed Unit)와 O-RU(O-RAN Radio Unit) 사이의 인터페이스를 정의합니다.

주요 평면(Plane)

O-RAN 프론트홀 아키텍처는 다음과 같은 주요 평면으로 구성됩니다:

1. **C-Plane (Control Plane)**:
   * O-DU와 O-RU 사이의 실시간 제어를 담당합니다.
   * 스케줄링 및 빔포밍 명령 전송 절차를 정의합니다.
2. **U-Plane (User Plane)**:
   * O-DU와 O-RU 사이의 데이터 전송을 처리합니다.
   * 엄격한 시간 제한 내에서 효율적인 데이터 전송을 보장합니다.
3. **S-Plane (Synchronization Plane)**:
   * O-DU와 O-RU 간의 시간 및 주파수 동기화를 보장합니다.
4. **M-Plane (Management Plane)**:
   * O-RU의 초기화, 구성 및 관리를 담당합니다.
   * 하위 계층 분할 M-plane (LLS-M)은 명시된 기능 분할을 지원하기 위한 O-RU의 초기화, 구성 및 관리를 용이하게 합니다.

프로토콜 스택

각 평면은 이더넷 상에서 서로 다른 프로토콜 스택을 사용합니다. 예를 들어, C/U-Plane은 eCPRI over Ethernet 또는 RoE(Radio over Ethernet)를 지원합니다.

멀티벤더 지원

이 아키텍처는 다양한 벤더의 O-DU와 O-RU 간 상호 연결을 가능하게 하여 진정한 멀티벤더 Open RAN을 실현합니다.

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

<Perplexity>

O-RAN의 M-Plane은 NETCONF/YANG 기반 프로토콜을 사용하여 O-RU(O-RAN Radio Unit)의 다양한 관리 기능을 지원합니다. 이 M-Plane은 두 가지 아키텍처 모델을 지원합니다:

계층적 모델 (Hierarchical Model)

* O-RU는 하나 이상의 O-DU(O-RAN Distributed Unit)에 의해 전적으로 관리됩니다.
* NETCONF 기반 M-Plane 인터페이스를 사용합니다.
* 여러 O-DU가 O-RU를 관리하는 경우, 주로 O-DU 및/또는 전송 연결의 중복성 기능을 위한 것입니다.

하이브리드 모델(Hybrid Model)

* O-DU와 O-RU 사이의 논리적 인터페이스 외에도, 관리 시스템과 O-RU 사이에 하나 이상의 직접적인 논리적 인터페이스를 제공합니다.
* O-RU에 연결되는 NETCONF 클라이언트는 다양한 클래스(예: O-DU 및 SMO)일 수 있습니다.
* 관리 시스템이 직접 다음과 같은 기능을 관리할 수 있습니다:
  + O-RU 소프트웨어 관리
  + 성능 관리
  + 구성 관리
  + 장애 관리

두 모델 모두 다음과 같은 관리 기능을 지원합니다:

* "시작" 설치
* 소프트웨어 관리
* 구성 관리
* 성능 관리
* 장애 관리
* 파일 관리

O-RAN의 M-Plane 사양은 O-RU(O-RAN Radio Unit)가 계층적 구성과 하이브리드 구성을 모두 지원할 수 있도록 설계되었습니다. 이에 대한 주요 특징은 다음과 같습니다:

1. 명시적 신호 없음: O-RU가 계층적 또는 하이브리드 구성으로 작동하고 있음을 나타내는 명시적인 신호가 없습니다.
2. 다중 NETCONF 세션 지원: 이 M-Plane 사양을 지원하는 모든 NETCONF 서버는 여러 NETCONF 세션을 지원해야 합니다.
3. 유연한 구성: 모든 규격 준수 O-RU는 계층적 배포와 하이브리드 배포를 모두 지원할 수 있어야 합니다.
4. NETCONF 서버 위치: NETCONF 서버는 O-RU에 존재합니다.
5. NETCONF 클라이언트: NETCONF 클라이언트는 O-RU 컨트롤러(O-DU 또는 NMS)에 존재합니다.
6. 하이브리드 아키텍처 지원: NETCONF는 O-RU의 NETCONF 서버에서 발생하는 정보를 여러 클라이언트가 구독하고 수신할 수 있는 하이브리드 아키텍처를 기본적으로 지원합니다.

이러한 설계는 O-RU가 다양한 관리 시나리오에 유연하게 대응할 수 있도록 하며, 네트워크 운영자에게 관리 옵션의 선택권을 제공합니다.

텍스트, 스크린샷, 도표, 폰트이(가) 표시된 사진

자동 생성된 설명

NETCONF/YANG는 O-RAN 아키텍처에서 네트워크 요소 관리 프로토콜 및 데이터 모델링 언어로 사용됩니다. 이 표준화된 프레임워크와 공통 모델링 언어의 사용은 다음과 같은 이점을 제공합니다:

O-DU와 O-RU 간 통합 간소화

* NETCONF/YANG은 O-DU와 O-RU 사이의 통합을 단순화합니다.
* 공통 기능을 공유하는 요소들 간의 운영자 네트워크 통합을 용이하게 합니다.

다양한 제품 통합 지원

* 잘 정의된 공개 데이터 모델을 통해 서로 다른 기능을 가진 제품들의 통합을 지원합니다.
* 이는 다양한 벤더의 장비를 사용하는 멀티벤더 환경에서 특히 유용합니다.

하이브리드 아키텍처 지원

* NETCONF는 기본적으로 하이브리드 아키텍처를 지원합니다.
* 여러 클라이언트가 O-RU의 NETCONF 서버에서 발생하는 정보를 구독하고 수신할 수 있습니다.
* 이를 통해 O-DU와 SMO 같은 다양한 관리 엔티티가 O-RU와 직접 통신할 수 있습니다.

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

<Perplexity>

O-RAN의 M-Plane 연결성에 대한 주요 요구사항과 특징은 다음과 같습니다:

기본 요구사항

* O-RU와 관리 요소(O-DU, SMO, "O-RU 컨트롤러") 간 종단간 IP 연결성이 필요합니다.

IP 버전 지원

* O-RU는 IPv4 또는 IPv6 중 하나를 반드시 지원해야 합니다.
* 선택적으로 듀얼 스택(IPv4와 IPv6 동시 지원)을 지원할 수 있습니다.

이전 버전과의 호환성

* 이전 사양 버전에서는 IPv4만 필수였습니다.
* 이전 버전 장비와의 호환성을 위해, 운영자와 벤더는 O-RU, O-DU, 기타 O-RU 컨트롤러에서 공통 IP 버전을 사용하기로 합의할 수 있습니다.

</Perplexity>

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

<Perplexity>

M-Plane은 NETCONF 기능을 사용하여 O-RU에 다음과 같은 주요 기능을 제공합니다:

O-RAN의 **"Start-up" 설치** 과정은 다음과 같은 주요 단계를 포함합니다:

네트워크 매개변수 획득

O-RU는 시작 시 네트워크 계층 매개변수를 획득합니다:

* 정적 방식: O-RU에 사전 구성된 매개변수 사용
* 동적 방식: DHCP 또는 DHCPv6를 통한 매개변수 획득

O-RU 컨트롤러 연결

* O-RU는 O-RU 컨트롤러의 IP 주소를 획득할 수 있습니다.
* "Call home" 기능을 사용하여 NETCONF 연결을 설정합니다.

SMO 환경에서의 동작

O-RAN 정의 SMO가 포함된 환경에서 작동할 경우:

* O-RU는 이벤트 수집기의 IP 주소를 획득할 수 있습니다.
* pnfRegistration을 수행하여 SMO가 NETCONF 연결을 설정하도록 트리거합니다.

기능 교환

* 클라이언트와 서버 간의 기능 교환은 초기 NETCONF Hello 교환의 일부로 수행됩니다.

주의 사항

* 이 사양에서 "start up"이라는 용어는 NETCONF 환경에서 장치가 별도의 실행 중인 구성과 시작 구성 데이터 저장소를 지원함을 나타내는 "start-up" 기능과는 구별됩니다.
* O-RU는 "리셋 지속 메모리"에 저장된 구성을 "시작" 구성으로 사용해야 합니다.

이러한 단계들의 세부 사항은 6절에서 제공됩니다.

O-RAN의 M-Plane은 O-RU 컨트롤러의 요청에 따라 **소프트웨어 관리**를 담당합니다. 소프트웨어 관리 절차는 다음과 같은 주요 단계를 포함합니다:

1. 소프트웨어 인벤토리
2. 소프트웨어 다운로드
3. 소프트웨어 설치/업그레이드
4. 소프트웨어 활성화

소프트웨어 다운로드 과정은 두 단계로 나뉩니다:

1. NETCONF RPC 절차를 통한 다운로드 트리거
2. 실제 소프트웨어 패키지 다운로드

실제 소프트웨어 패키지 다운로드는 다음 두 가지 방법 중 하나를 사용하여 수행됩니다:

* SSH를 사용한 sFTP (Secure File Transfer Protocol)
* TLS를 사용한 FTPES (FTP over explicit TLS/SSL)

이러한 보안 프로토콜을 사용함으로써 소프트웨어 다운로드 과정에서 데이터의 기밀성과 무결성을 보장할 수 있습니다.

O-RAN의 **구성 관리**는 O-RU(O-RAN Radio Unit)의 리소스와 매개변수를 관리하기 위한 여러 핵심 시나리오를 다룹니다. 구성 관리의 주요 측면은 다음과 같습니다:

리소스 상태 관리

* 리소스 상태 검색
* 리소스 상태 수정

매개변수 관리

* 매개변수 수정
* 매개변수 검색

이러한 구성 관리 작업을 수행하기 위해 O-RAN은 NETCONF(Network Configuration Protocol) 원격 프로시저 호출(RPC)을 사용합니다. 구체적으로:

1. NETCONF <get-config> RPC: O-RU에서 구성 매개변수를 검색하는 데 사용됩니다.
2. NETCONF <edit-config> RPC: O-RU의 구성 매개변수를 업데이트하는 데 사용됩니다.

이러한 RPC를 통해 O-RU 컨트롤러는 표준화된 방식으로 O-RU의 구성과 상호 작용할 수 있습니다. NETCONF의 사용으로 O-RAN 생태계에서 다양한 벤더의 장비 간 일관된 구성 관리 접근 방식이 가능해집니다.

구성 데이터 저장소

O-RU는 다양한 구성 데이터 저장소를 지원합니다:

1. 실행 중인(running) 데이터 저장소: 현재 활성화된 구성을 포함합니다.
2. 후보(candidate) 데이터 저장소: 실행 중인 데이터 저장소에 커밋하기 전에 구성 변경사항을 저장하는 데 사용됩니다.

후보 데이터 저장소를 통해 사용자는 실행 중인 시스템에 영향을 주지 않고 대량의 구성을 편집하고 검증할 수 있습니다.

구성 수정 프로세스

O-RU 구성을 수정할 때 O-RU 컨트롤러는 다음 단계를 따라야 합니다:

1. 다른 NETCONF 클라이언트와의 충돌을 방지하기 위해 대상 구성을 잠급니다.
2. 후보 구성 데이터 저장소에서 수정 작업을 수행합니다(지원되는 경우).
3. 검증된 구성을 실행 중인 구성 데이터 저장소에 커밋합니다.
4. 대상 구성의 잠금을 해제합니다.

이 프로세스는 O-RAN 네트워크 전반에 걸쳐 안전하고 일관된 구성 변경을 보장합니다.

O-RAN의 **성능 관리**는 O-RU(O-RAN Radio Unit) 운영과 관련된 측정 및 카운터 데이터를 수집하는 데 중점을 둡니다. 성능 관리의 주요 목적은 O-RU의 운영을 최적화하는 것입니다.

측정 결과는 다음 두 가지 옵션을 통해 보고됩니다:

1. YANG 알림:
   * 이 옵션은 각 측정 그룹에 대한 YANG 모델의 통계 정의를 활용합니다.
   * get RPC 및/또는 알림 메커니즘을 사용합니다.
   * 이 옵션에 대한 자세한 내용은 사양의 10절에서 확인할 수 있습니다.
2. 파일 업로드:
   * 이 옵션은 파일 관리 섹션에 정의된 파일 업로드 절차를 사용합니다.
   * 측정 결과는 주기적으로 데이터 파일에 저장됩니다.
   * 파일 업로드 절차는 사양의 12절에 설명되어 있습니다.

이러한 보고 옵션들은 성능 데이터를 수집하고 분석하는 방법에 유연성을 제공하여, O-RAN 아키텍처에서 O-RU 운영을 효과적으로 모니터링하고 최적화할 수 있게 합니다.

O-RAN의 **장애 관리**는 네트워크의 건강 상태를 모니터링하고 유지하는 데 중요한 구성 요소입니다. 주요 특징은 다음과 같습니다:

알람 통지

* NETCONF 클라이언트에게 알람 통지를 전송합니다.
* 구성된 구독 기능을 지원하는 O-RU의 경우, 구독자는 이벤트 수집기일 수 있습니다.
* O-RU는 특정 심각도의 새로운 활성 알람이나 취소된 알람에 대해서만 통지를 보냅니다.

알람 제어

* 알람 통지를 활성화하거나 비활성화할 수 있습니다.
* 이는 장애 관리 관리 요소를 통해 제어됩니다.

알람 구독

* NETCONF 클라이언트는 create-subscription 요청을 NETCONF 서버에 보내 장애 관리 요소를 "구독"할 수 있습니다.
* 이를 통해 클라이언트는 지속적으로 알람 통지를 받을 수 있습니다.

활성 알람 목록

* NETCONF 서버는 "active-alarm-list"를 관리합니다.
* "경고" 심각도의 알람은 이 목록에서 제외됩니다.
* 알람이 감지되면 목록에 추가되고, 알람 원인이 사라지면 목록에서 제거됩니다.

알람 통지 내용

* 알람 통지에는 O-RU 내 알람의 출처를 나타내는 "fault-source" 요소가 포함됩니다.
* 장애의 영향을 받는 요소를 나타내는 "affected objects"도 포함됩니다.
* 알람은 "fault-id", "fault-source", "fault-severity"로 식별됩니다.

장애 관리 활성화

* O-RU 컨트롤러는 o-ran-fm.yang 모델에 정의된 YANG 통지에 대한 구독을 생성하여 장애 관리를 활성화합니다.

이러한 종합적인 장애 관리 접근 방식은 O-RAN 네트워크의 효율적인 모니터링과 문제 해결을 가능하게 하여 신속한 문제 식별과 해결을 지원합니다.

O-RAN의 **파일 관리** 기능은 다음과 같은 특징을 가집니다:

1. 다양한 파일 제공:
   * O-RU는 여러 종류의 파일을 제공할 수 있습니다.
   * 이러한 파일들은 다양한 목적으로 사용될 수 있습니다.
2. 파일 검색:
   * 검색된 파일들은 여러 용도로 활용될 수 있습니다.
3. 동시 다중 파일 업로드:
   * O-RU에서 O-DU/SMO로의 파일 전송 시 동시에 여러 파일을 업로드할 수 있습니다.
   * 이는 단일 sFTP 또는 FTPES 연결을 통해 지원됩니다.
4. 보안 프로토콜 사용:
   * sFTP(SSH File Transfer Protocol)나 FTPES(FTP over explicit TLS/SSL)와 같은 보안 프로토콜을 사용합니다.
   * 이를 통해 파일 전송 시 데이터의 기밀성과 무결성을 보장합니다.

</Perplexity>

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

<Perplexity>

M-Plane 인터페이스는 O-RU 컨트롤러와 O-RU 사이에 정의됩니다. M-Plane 인터페이스의 프로토콜 스택은 다음과 같은 특징을 가집니다:

전송 계층 구조

* IP 전송 기반으로 구축됨
* SSH/TCP를 사용하여 M-Plane 메시지 전달
* 선택적으로 TLS 사용 가능

비동기 알림 지원 (선택 사항)

* O-RU는 HTTPS를 사용한 비동기 알림 전송 기능을 지원할 수 있음
* 이 옵션은 O-RU 컨트롤러가 SMO에 해당하고 O-RU와 비영구적 NETCONF 세션으로 작동하는 경우 시스템 최적화를 가능하게 함

</Perplexity>

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

<Perplexity>

M-Plane을 나타내는 데이터 모델은 재사용 가능한 YANG 모듈 세트로 구성됩니다. 또한 O-RAN 특화 모듈을 개발하는 대신 가능한 한 공개적으로 사용 가능한 일반 YANG 모델을 재사용하는 것이 목적입니다.

각 모듈에 대한 자세한 내용은 다음을 참조하십시오:

1. 다양한 장(chapter)
2. 부록 D (Annex D)
3. YANG 모델 저장소

이러한 참조를 통해 각 모듈의 구조, 기능 및 사용 방법에 대한 상세한 정보를 얻을 수 있습니다. 이는 O-RAN 아키텍처에서 M-Plane의 효율적인 구현과 관리를 위한 중요한 리소스입니다.

</Perplexity>

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

<Perplexity>

제공된 정보에 따르면, O-RAN M-Plane 초기화를 위한 **사전 조건**은 다음과 같이 충족되었습니다:

1. O-RU/NETCONF 서버의 전원 켜짐 또는 O-RU 재시작 작업:
   * O-RU 전원 상태: 켜짐
   * NETCONF 서버 상태: 활성화
2. O-RU 컨트롤러/NETCONF 클라이언트의 전원 켜짐:
   * O-RU 컨트롤러 상태: 켜짐
   * NETCONF 클라이언트 상태: 활성화
3. pnfRegistration 이벤트 수집기의 전원 켜짐:
   * pnfRegistration 이벤트 수집기 상태: 활성화
4. 물리적 인터페이스 연결:
   * 물리적 인터페이스 연결 상태: 연결됨

O-RAN M-Plane 초기화 과정의 **사후 조건**은 다음과 같습니다:

1. O-RU의 무선 전송 준비 상태:
   * O-DU로부터 패킷 전송을 받으면 최소 하나의 캐리어에서 공중으로 무선 전송할 준비가 되어 있습니다.
2. O-RU의 패킷 전송 준비 상태:
   * 공중에서 최소 하나의 캐리어로 무선 수신이 이루어지면 O-DU로 패킷을 전송할 준비가 되어 있습니다.
3. O-RU 제어 권한:
   * "super-user" 또는 "hybrid-odu" 접근 권한을 가진 최소 하나의 O-RU 컨트롤러/NETCONF 클라이언트가 O-RU/NETCONF 서버의 캐리어 구성을 제어할 수 있습니다.

이러한 사후 조건들은 O-RAN 시스템이 정상적으로 초기화되어 운영 준비가 완료되었음을 나타냅니다.

</Perplexity>

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.

텍스트, 스크린샷, 폰트, 도표이(가) 표시된 사진

자동 생성된 설명

[Table 6.1.1: Overall of Start-Up Installation]

<GPT>

O-RU(Open Radio Unit)\*\*가 전원 켜짐(Power-ON) 또는 재시작(Restart) 이후 수행하는 초기화 절차와 관련된 상세 단계를 설명합니다. 해당 절차는 O-RAN 아키텍처에서 O-RU가 정상적으로 서비스 가능한 상태가 되기 위한 일련의 작업입니다.

O-RU 초기화 절차 (Figure 6.1.1에 따른 주요 단계)

**1. M-Plane 전송 계층 해상 및 IP 복구**

* **작업 내용**:
  + O-RU는 DHCP를 통해 네트워크 계층(MAC 주소, VLAN, IP 주소 등)을 구성.
  + O-RU 컨트롤러 및 pnfRegistration 이벤트 수집기의 IP 주소를 확인.
* **목적**:
  + 네트워크에서 통신을 시작할 수 있는 기본적인 연결 설정.

**2. O-RU와 기본 참조 클럭(Primary Reference Clock) 동기화**

* **작업 내용**:
  + O-RU는 클럭 동기화를 시작하여 네트워크 타이밍을 맞춤.
* **특징**:
  + 일부 O-RU 구현에서는 동기화가 네트워크 계층 설정(1단계)과 병렬로 수행될 수 있음.
* **목적**:
  + 네트워크에서 시간 동기화가 필요한 통신 및 서비스 제공 준비.

**3. NETCONF Call Home 및 pnfRegistration 수행**

* **작업 내용**:
  + O-RU는 네트워크에서 발견된 O-RU 컨트롤러와 이벤트 수집기에 NETCONF Call Home을 통해 연결.
  + Call Home은 O-RU가 클라이언트(O-RU 컨트롤러)와 연결을 초기화.
* **목적**:
  + O-RU가 관리 시스템과 상호작용하기 위한 통신 채널 생성.

**4. SSH/TLS 연결 설정**

* **작업 내용**:
  + O-RU 컨트롤러는 O-RU와의 안전한 연결을 위해 SSH 또는 TLS를 사용하여 세션을 설정.
* **목적**:
  + 보안이 유지된 상태에서 관리 및 데이터 전송 수행.

**5. NETCONF 기능 탐색**

* **작업 내용**:
  + O-RU와 O-RU 컨트롤러 간에 지원되는 NETCONF 기능 및 모델(YANG 모델) 확인.
* **목적**:
  + 관리자가 O-RU에서 사용할 수 있는 기능 및 데이터 모델 파악.

**6. 관리 계정 프로비저닝 (선택적)**

* **작업 내용**:
  + O-RU 컨트롤러가 새로운 관리 계정을 설정. (일반적으로 사전 준비 단계에서 수행)
* **목적**:
  + 관리 권한 및 사용자 계정을 설정하여 안전한 관리 수행.

**7. NETCONF 연결 상태 감독**

* **작업 내용**:
  + O-RU와 O-RU 컨트롤러는 NETCONF 연결 상태를 지속적으로 모니터링.
* **목적**:
  + 연결의 안정성과 신뢰성을 보장.

**8. O-RU 정보 검색**

* **작업 내용**:
  + O-RU 컨트롤러는 O-RU의 상태, 구성, 하드웨어 및 소프트웨어 정보를 검색.
* **목적**:
  + O-RU의 초기 상태 및 기능 확인.

**9. 소프트웨어(SW) 관리**

* **작업 내용**:
  + O-RU 컨트롤러가 O-RU 소프트웨어를 관리(업데이트, 설치 등).
* **목적**:
  + 최신 소프트웨어로 O-RU를 유지.

**10~15. CU-Plane 구성 및 성능 확인**

* **작업 내용**:
  + O-RU와 O-DU 간의 CU-Plane 데이터 전송 구성을 수행.
  + 필요 시, CU-Plane 연결 상태 및 전송 지연 측정.
* **목적**:
  + 데이터 전송 경로를 구성하고 성능을 보장.

**16. 장애 관리(Fault Management) 활성화**

* **작업 내용**:
  + O-RU 컨트롤러는 NETCONF 이벤트 스트림에 구독하여 장애 이벤트를 수신.
  + O-RU의 활성 알람 목록을 검색.
* **목적**:
  + 초기화 과정에서 발생하는 문제를 신속히 감지.

**17. 성능 관리 활성화**

* **작업 내용**:
  + O-RU 컨트롤러는 성능 측정을 시작.
* **목적**:
  + O-RU의 성능 상태를 모니터링.

**18. O-RU 상태 검색**

* **작업 내용**:
  + O-RU 컨트롤러는 동기화 상태 등 운영 상태를 검색.
* **목적**:
  + 서비스 제공 준비 상태 확인.

**19. 운영 파라미터 설정**

* **작업 내용**:
  + O-RU 컨트롤러가 O-RU의 작동 파라미터를 설정.
* **목적**:
  + O-RU가 요구사항에 따라 동작하도록 설정.

**20. 서비스 가용성**

* **작업 내용**:
  + 모든 초기화 절차가 완료되고, O-RU가 정상적인 서비스를 제공할 준비가 완료.
* **특이사항**:
  + 클럭 동기화(2단계)는 서비스 가용성 전 반드시 완료되어야 함.

</GPT>

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

<GPT>

O-RU(Open Radio Unit)와 O-RU 컨트롤러(예: O-DU 및/또는 SMO) 간 **M-Plane(관리 평면) 전송 계층**을 설정하는 시나리오를 설명합니다. 여기서는 M-Plane의 전송 계층 주소 설정에 초점을 맞추며, C-Plane 및 U-Plane의 전송 관련 내용은 7장에서 다룹니다.

**전제 조건(Pre-condition):**

1. **물리적 인터페이스가 연결됨.**
   * O-RU와 O-RU 컨트롤러 간 물리적 연결이 활성화되어 있어야 합니다.
2. **NETCONF Call Home 환경에서의 포트 일치:**
   * NETCONF 서버와 클라이언트는 동일한 NETCONF Call Home 포트를 사용하도록 설정되어야 합니다. 이를 통해 NETCONF 클라이언트가 서버가 사용하는 포트를 올바르게 청취(listen)할 수 있습니다.

**사후 조건(Post-condition):**

1. **M-Plane 전송 계층 주소를 O-RU 및 컨트롤러가 인지.**
   * O-RU와 O-RU 컨트롤러가 M-Plane 통신에 필요한 전송 계층 주소를 인식해야 합니다.
2. **M-Plane 물리적 포트 정보 인지:**
   * O-RU는 M-Plane에 사용되는 물리적 포트(복수 포트 가능)를 알고 있어야 합니다.
3. **VLAN 정보 인지:**
   * 네트워크에서 VLAN이 사용된다면, O-RU는 M-Plane에 사용되는 VLAN을 인식해야 합니다.
4. **TCP 연결 준비 완료:**
   * O-RU는 NETCONF Call Home 및/또는 PNF(Physical Network Function) 등록을 위한 TCP 연결 준비를 완료합니다.

**M-Plane 전송 설정 시나리오:**

M-Plane 전송 계층 주소를 설정하는 방법은 다음 세 가지 대안 중 하나를 사용할 수 있습니다(그림 6.2.1.1 참조).

**a) 수동 전송 계층 주소 구성**

* **방법**:
  + O-RU와 NETCONF 클라이언트 및/또는 이벤트 수집기에 대한 주소를 수동으로 설정합니다.
  + 이 방법에서 수동 구성 절차는 이 명세의 범위를 벗어납니다.
* **결과**:
  + 수동 구성이 성공하면, NETCONF 서버는 구성된 정보를 복구하고 o-ran-mplane-int.yang 모델을 사용하여 이 정보를 NETCONF 클라이언트에 전달할 수 있습니다.

**b) DHCP를 통한 IPv4 기반 구성**

* **방법**:
  + DHCP 서버가 O-RU의 전송 계층 주소 정보와 NETCONF 클라이언트 및/또는 이벤트 수집기의 식별 정보를 제공합니다.
  + 식별 정보에는 NETCONF 클라이언트/이벤트 수집기의 전송 계층 주소 또는 FQDN(정규화된 도메인 이름)이 포함됩니다.
  + FQDN이 제공되면, O-RU는 DHCP 서버에서 제공한 DNS 서버 주소를 사용하여 해당 FQDN의 IP 주소를 확인합니다.

**c) DHCPv6를 통한 IPv6 기반 구성**

* **방법**:
  + SLAAC(Stateless Address Auto-Configuration)를 사용하여 O-RU의 전송 계층 주소를 구성합니다.
  + DHCPv6 서버는 NETCONF 클라이언트 및/또는 이벤트 수집기의 식별 정보를 제공합니다(FQDN 또는 전송 계층 주소).
  + FQDN이 제공되면, O-RU는 DNS 서버 주소를 사용하여 FQDN에 해당하는 IP 주소를 확인합니다.

**참고 사항**

* **IP 버전 지원 여부 확인**:
  + NETCONF 클라이언트는 O-RU가 지원하는 IP 버전을 확인하기 위해 **get RPC**를 사용하여 O-RU가 지원하는 인터페이스 목록을 검색할 수 있습니다.
  + **o-ran-interfaces** 모듈에서 IPv4 또는 IPv6 컨테이너가 있는지 확인하여 지원 여부를 판단합니다.
* **DHCP 정보 노출**:
  + O-RU는 **o-ran-dhcp.yang** 모델을 사용하여 DHCP 서버에서 제공된 정보를 노출합니다.

**M-Plane 전송 계층 정보**

M-Plane의 전송 계층 인터페이스 정보에는 다음이 포함됩니다:

* 물리적 포트 번호
* 이더넷 포트의 하드웨어 주소(MAC 주소)
* VLAN ID
* 로컬 IP 주소
* 원격 IP 주소
* 기본 게이트웨이 주소
* 서브넷 마스크

**b) 및 c) 옵션 관련 추가 작업**

1. **DHCP 메시지를 통한 O-RU 식별**
2. **M-Plane VLAN 탐색**
3. **O-RU IP 주소 할당**
4. **O-RU 컨트롤러 및/또는 이벤트 수집기의 주소 정보 검색**

</GPT>

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.

텍스트, 스크린샷, 평행, 폰트이(가) 표시된 사진

자동 생성된 설명

[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

<GPT>

O-RU(Open Radio Unit)가 DHCP 서버에 자신을 식별하는 방법과 관련된 명세를 설명합니다. 이를 통해 O-RU가 네트워크에서 IP 주소를 할당받거나 관리 평면(M-plane) 컨트롤러 정보를 구성할 수 있도록 지원합니다.

**O-RU의 DHCP 식별 방법**

O-RU는 DHCP 메시지에 포함된 vendor-class-data 문자열을 사용하여 자신을 O-RU로 식별합니다. 이 문자열은 **o-ran-dhcp YANG 모델**에서 정의됩니다.  
O-RU가 지원하는 IP 버전에 따라 아래 옵션 중 하나를 사용합니다.

**1. IPv4를 사용하는 경우**

O-RU는 다음 두 가지 옵션 중 하나를 통해 자신을 식별할 수 있습니다:

1. **옵션 60: Vendor Class Identifier (RFC2132)**
2. **옵션 124: Vendor-Identifying Vendor Class Option (RFC3925)**

**옵션 60 (Vendor Class Identifier)**

* **옵션 번호**: 60
* **Vendor Class Identifier 형식**:  
  vendor-class-data 문자열은 아래 세 가지 중 하나의 형식을 따라야 합니다:
  1. "o-ran-ru2/<vendor>"  
     예: "o-ran-ru2/vendorA"
  2. "o-ran-ru2/<vendor>/<product-code>"  
     예: "o-ran-ru2/vendorA/ORUAA100"
  3. "o-ran-ru2/<vendor>/<product-code>/<serial-number>"  
     예: "o-ran-ru2/vendorA/ORUAA100/FR1918010111"

**옵션 124 (Vendor-Identifying Vendor Class Option)**

* **옵션 번호**: 124
* **Enterprise 번호**: O-RAN Alliance (53148)
* **Vendor-Class-Data 형식**:
  + 문자열 형식은 위 **옵션 60**에서 정의된 규칙과 동일합니다.

**2. IPv6를 사용하는 경우**

O-RU는 **DHCPv6 Vendor Class Option**을 사용하여 자신을 식별합니다:

* **옵션 번호**: 16
* **Enterprise 번호**: O-RAN Alliance (53148)
* **Vendor-Class-Data 형식**:
  + 문자열 형식은 **옵션 60**에서 정의된 규칙과 동일합니다.

**DHCP 서버에서의 역할**

* DHCP 서버는 O-RU가 제공한 vendor-class-data 정보를 사용하여 아래 작업을 수행할 수 있습니다:
  1. **IP 주소 풀 선택**:
     + DHCP 서버는 O-RU의 식별 정보를 기반으로 적절한 IP 주소 풀에서 IP를 할당합니다.
  2. **M-Plane O-RU 컨트롤러 정보 선택**:
     + 관리 평면에서 사용할 O-RU 컨트롤러 정보를 O-RU에 구성할 때 활용합니다.

**요약**

* **IPv4**: 옵션 60 또는 옵션 124 중 하나를 사용하여 O-RU 식별.
* **IPv6**: 옵션 16을 사용하여 O-RU 식별.
* **문자열 형식**: "o-ran-ru2/<vendor>/<product-code>/<serial-number>"와 같은 구조로 구성.
* 이 정보를 통해 DHCP 서버는 네트워크 설정(주소 할당, 컨트롤러 구성 등)을 효율적으로 수행할 수 있습니다.

</GPT>

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

<GPT>

O-RAN Radio Unit (O-RU)이 이더넷 포트를 통해 **관리 플레인(M-Plane)** 연결을 설정하는 과정을 설명합니다.

**1. 이더넷 포트 설정**

* O-RU는 하나 이상의 이더넷 포트를 통해 네트워크에 연결됩니다.
* 이 포트는 두 가지 모드로 설정될 수 있습니다:
  + **액세스 포트**: 태그가 없는(ununtagged) 이더넷 프레임을 사용하는 모드.
  + **트렁크 포트**: 여러 VLAN(Virtual LAN)이 구성된 모드.

**2. 부팅 시 초기 상태**

* O-RU가 부팅을 완료하고 이더넷 연결이 감지되면 관리 플레인 연결을 설정하기 시작합니다.
* 초기 상태에서는 포트가 액세스 모드인지 트렁크 모드인지 즉시 판단할 수 없습니다.

**3. VLAN ID 확인 과정**

1. **트렁크 포트 연결 시**:
   * 관리 플레인 통신에 사용되는 VLAN ID를 알아내야 합니다.
   * 이를 위해 DHCP 서버로 **DHCP DISCOVER** 메시지를 전송합니다.
   * DHCP 서버의 응답(DHCP OFFER)을 통해 VLAN ID를 확인합니다.
2. **IPv6 지원 시**:
   * 만약 O-RU가 IPv6를 지원하고, IPv6 라우터 광고(Router Advertisement)를 받을 때 "관리 주소 구성(managed address configuration)" 또는 "기타 구성(other configuration)" 비트가 설정되지 않았다면, 관리 플레인에 VLAN이 사용되지 않는다고 추론할 수 있습니다.
3. **사전 구성된 정보가 없는 경우**:
   * O-RU는 모든 이더넷 포트에서 태그가 없는(ununtagged) 프레임을 사용하여 DHCP 서버를 검색합니다.
4. **사전 구성된 VLAN 정보가 있는 경우**:
   * 이전에 사용된 관리 플레인 VLAN 정보 또는 NETCONF 클라이언트를 통해 설정된 VLAN 범위를 활용해 검색을 최적화할 수 있습니다.

**4. 검색 실패 시 동작**

* 태그가 없는 프레임이나 사전 구성된 VLAN을 통해 DHCP OFFER를 받지 못할 경우:
  + O-RU는 \*\*VLAN ID 전체 범위(1~4094)\*\*를 사용하여 모든 포트에서 DHCP 서버를 검색합니다.

**5. 검색 알고리즘과 스캔 주기**

* O-RU는 **개별 VLAN 검색 알고리즘**을 사용하여 M-Plane의 신속한 활성화를 보장해야 합니다.
* 간헐적 또는 일시적인 연결 문제로 인해 DHCP 응답을 받지 못할 경우를 대비하여 다음과 같은 동작을 수행합니다:
  + 태그가 없는 프레임과 사전 구성된 VLAN을 반복적으로 검색합니다.
  + VLAN ID 전체 범위를 스캔할 때도 이를 포함합니다.
* **스캔 주기(scan-interval)**:
  + O-RU 컨트롤러는 스캔 주기의 최대 간격을 권장할 수 있습니다.
  + 예: 기본 스캔 주기가 60초일 경우, O-RU가 개별 VLAN 검색에 1초를 사용한다면 60개의 VLAN을 스캔한 뒤 다시 태그가 없는 프레임과 구성된 VLAN에 대해 검색을 반복합니다.

요약

O-RU는 부팅 이후 관리 플레인 연결을 설정하기 위해 포트가 액세스 모드인지 트렁크 모드인지 확인하며, 필요한 경우 DHCP를 통해 VLAN ID를 탐색합니다. 스캔 알고리즘은 효율적이고 반복적인 방식으로 설계되어, 네트워크 연결 문제에도 M-Plane 연결을 안정적으로 활성화할 수 있도록 합니다.

</GPT>

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

<GPT>

O-RU(Open Radio Unit) 관리 plane의 IP 주소를 자동 할당하는 방법에 대한 설명입니다.

**IPv4 설정:**

1. **DHCPv4 (RFC 2131)**:
   * IPv4 네트워크 주소를 할당하는 방법입니다.
   * O-RU는 DHCP 클라이언트 식별자 옵션에서 안정적인 노드 식별자를 사용하도록 **RFC 4361**의 동작을 따라야 합니다.
   * **참고 사항**:
     + 여러 DHCP 서버가 있는 네트워크에서는, O-RU가 서로 다른 인터페이스를 통해 여러 DHCPv4 응답을 받을 경우 공통된 기본 게이트웨이가 제공되도록 서버 구성의 조정이 필요합니다.
     + O-RU는 **RFC 3442**를 통해 정적 라우팅 정보를 설정하도록 지원할 수 있으며, 이는 O-RU가 여러 인터페이스를 지원하는 경우 상향 패킷을 라우팅할 때 사용됩니다.

</GPT>

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

<GPT>

O-RU(Open Radio Unit) 컨트롤러 주소를 자동으로 발견하는 방법에 대한 내용입니다.

**O-RU의 관리 plane 구성 정보 획득:**

1. \*\*IPv6 Stateless Address Auto-Configuration(SLAAC)\*\*를 통해 IPv6 주소를 할당받은 O-RU:
   * Stateless DHCPv6 (RFC 3736)을 사용하여 관리 plane 구성 정보를 획득해야 합니다.
2. **IPv4 또는 IPv6 상태 저장 주소 할당**을 사용하는 O-RU:
   * IP 주소 할당 과정에서 관리 plane 구성 정보를 획득해야 합니다.

**NETCONF 클라이언트 정보 복구:**

O-RU는 NETCONF 서버로 동작하며, 다음 DHCP 옵션을 사용해 NETCONF 클라이언트 정보를 복구할 수 있어야 합니다 (RFC 8572):

* **DHCPv4 옵션 V4\_SZTP\_REDIRECT [143]**
* **DHCPv6 옵션 V6\_SZTP\_REDIRECT [136]**

**DHCP 옵션으로 제공된 정보:**

* 서버 URI 리스트 형식: https://<IP 주소 또는 호스트 이름>[:<포트>].
* DHCP 서버는 NETCONF 클라이언트 정보를 IANA가 지정한 포트를 포함해 인코딩해야 합니다 (RFC 8071 참조).
* 포트 정보가 포함되지 않은 경우, O-RU는 기본적으로 NETCONF/SSH를 사용하여 "Call Home"을 시도합니다.

**수동 구성:**

* 수동으로 IP 주소가 설정된 O-RU는 O-RU 컨트롤러도 수동으로 구성해야 합니다.

**DHCP 옵션 요청:**

* IPv4: **OPTION\_V4\_SZTP\_REDIRECT**를 요청하려면 DHCP Discover/Request 메시지의 Parameter Request List(55)에 옵션 코드를 포함합니다.
* IPv6: **OPTION\_V6\_SZTP\_REDIRECT**를 요청하려면 Option Request Option에 요청된 옵션 코드를 포함합니다.

**참고:**

* DHCP 서버는 이미 O-RU의 Vendor Class Option을 통해 통신 중인 장치가 O-RU임을 알고 있으므로, 이러한 작업은 선택 사항입니다.

**레거시 환경 지원:**

IANA가 정의한 DHCP 옵션을 사용할 수 없는 환경에서는 O-RAN 정의 벤더 특화 옵션을 사용할 수 있습니다.

* **DHCPv4 Option 43** 또는 **DHCPv6 Option 17**을 통해 NETCONF 클라이언트 정보를 신호화 가능.
* 정보는 Type/Length/Value(TLV) 필드로 인코딩됩니다.

**벤더 클래스에 따른 타입 정의:**

* **"o-ran-ru"**:
  + Type 0x01: O-RU 컨트롤러 IP 주소
  + Type 0x02: O-RU 컨트롤러 FQDN (Fully Qualified Domain Name)
* **"o-ran-ru2"**:
  + Type 0x81: O-RU 컨트롤러 IP 주소
  + Type 0x82: O-RU 컨트롤러 FQDN
  + Type 0x86: O-RU Call Home 프로토콜

**예시:**

1. **O-RU 컨트롤러 IP 주소 (IPv4)**:
   * IPv4 주소: 198.185.159.144
   * DHCPv4 옵션 43 TLV 인코딩:  
     Type: 0x81  
     Length: 0x04  
     Value: C6 B9 9F 90
2. **O-RU 컨트롤러 FQDN**:
   * FQDN: controller.operator.com
   * DHCPv4 옵션 43 TLV 인코딩:  
     Type: 0x82  
     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
3. **Call Home 프로토콜 (NETCONF/TLS)**:
   * DHCPv4 옵션 43 TLV 인코딩:  
     Type: 0x86  
     Length: 0x01  
     Value: 01

**DHCPv6 옵션 17:**

* DHCPv6 인코딩은 DHCPv4와 유사하지만, TLV 데이터 이전에 IANA 지정 기업 번호(53148)가 포함됩니다.

이 내용은 O-RU의 관리 자동화를 지원하며, 레거시 및 현대 네트워크 환경 모두를 고려한 방식입니다.

</GPT>

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

<GPT>

다음은 O-RU(Open Radio Unit)에서 CMPv2를 사용한 인증서 등록과 관련된 내용입니다.

**CMPv2를 사용한 인증서 등록 지원:**

1. **IPv4 환경**:
   * O-RU가 IPv4를 지원하는 경우, DHCP 옵션 43을 사용하여 하나 이상의 인증 기관(CA/RA) 서버의 IP 주소 또는 FQDN(Fully Qualified Domain Name)을 발견할 수 있습니다.
   * 이 방식은 **3GPP 32.509**에서 정의된 절차를 따릅니다.
2. **IPv6 환경**:
   * CMPv2를 사용한 인증서 등록을 지원하는 IPv6 기반 O-RU는 DHCPv6 옵션 17을 사용하여 벤더 특화 옵션을 신호화할 수 있어야 합니다.
   * **DHCPv6 옵션 17 형식**:
     + DHCPv4 인코딩 형식을 따르며, 추가적으로 TLV(Type-Length-Value) 데이터 이전에 **Enterprise Number**가 포함됩니다.
     + O-RAN Alliance에 의해 IANA가 할당한 **기업 번호**는 53148입니다.

**포인트 투 포인트 연결(P2P) 환경:**

* O-RU와 O-DU(Open Distributed Unit) 간에 P2P 연결이 있는 경우, O-DU는 다음과 같은 기능을 제공해야 합니다.
  1. **IP 주소 기반**:
     + O-RU가 위에서 설명한 방식으로 전달된 IP 주소를 사용해 운영자 CA/RA 서버에 접근할 수 있는 수단.
  2. **FQDN 기반**:
     + O-RU가 운영자 DNS 서버에 접근하여 FQDN을 해석할 수 있는 추가 수단.

**YANG 모델을 통한 보고:**

* O-RU는 발견된 다중 벤더 플러그 앤 플레이 서버에 대한 정보를 **o-ran-dhcp YANG 모델**을 사용하여 보고해야 합니다.

이 내용은 O-RU의 인증서 등록 자동화를 지원하며, 다양한 네트워크 환경과 운영 요건을 충족하기 위한 방법을 제공합니다.

</GPT>

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

<GPT>

다음은 O-RU(Open Radio Unit)의 \*\*인증서 등록(Certificate Enrolment)\*\*에 관한 상세 내용입니다.

**CMPv2 기반 인증서 등록:**

* **3GPP 33.310**에서 정의:
  + CMPv2를 사용하여 기지국이 운영자 서명 인증서를 획득.
  + 인증서 요청은 기지국의 벤더 서명 인증서와 CA/RA 서버에 사전 설치된 벤더 루트 인증서를 기반으로 안전하게 이루어짐.
  + 이 방식은 IPSec 또는 TLS 인증서를 발급하는 데 사용되며, 동일한 기법이 SSHv2 기반 M-Plane 연결의 보안을 위한 인증서 발급에도 사용됨.

**NETCONF 클라이언트 및 서버 인증서 발급:**

* **TLS 클라이언트 CA**:
  + TLS 또는 SSHv2로 보호되는 NETCONF 클라이언트 인증서 발급 담당.
* **TLS 서버 CA**:
  + TLS 또는 SSHv2로 보호되는 NETCONF 서버 인증서 발급 담당.

**인증서 처리 및 프로필:**

* 인증서 및 인증서 프로필 처리는 **3GPP 33.310**의 TLS CA 인증서 규칙을 준수.
* 추가적으로 다음 조건 포함:

**1. 인증서 서명 요청(Certificate Signing Request, CSR):**

* **Subject Distinguished Name 필드**:
  + O-RU 제조업체 이름, 모델, 시리얼 번호를 포함한 문자열로 구성.
  + 사용되는 정확한 Subject DN 하위 필드는 CA/RA 서버 운영자의 인증서 정책에 의해 정의됨.

**참고 사항**:

* **향후 O-RAN 인증서 정책**:
  + O-RAN 생태계 전반에서 하위 필드 정의를 표준화할 수 있음.
* **허용되지 않는 문자**:
  + Subject DN 필드에 포함될 수 없는 문자: :(콜론), .(마침표), \_(밑줄), #(해시), £(파운드), \*(별표), "(따옴표) 등.
  + 제조업체 이름, 모델, 시리얼 번호에 이러한 문자가 포함된 경우, 필드에 포함하기 전에 제거해야 함.

**2. CA/RA 서버와의 통신:**

* **DHCP 옵션 기반 구성**:
  + O-RU는 3GPP 32.509에서 정의된 DHCP 옵션을 사용하여 CA/RA 서버의 포트 번호와 디렉토리 경로를 신호화.
* **기본값 사용**:
  + DHCP 기반 구성을 수신하지 못한 경우, 기본 포트 **443**과 기본 디렉토리 \*\*"/pkix/"\*\*를 사용.

**3. 초기화 응답 메시지에서의 신뢰 앵커 포함:**

* CA/RA 서버는 다음 정보를 초기화 응답 메시지에 포함해야 함:
  + 운영자가 발급한 인증서의 신뢰 앵커.
  + 적절한 인증서 체인.

**참고 사항**:

* O-RU에서 인증서 등록 중에 프로비저닝된 신뢰 앵커는 NETCONF 클라이언트(O-DU 및 선택적으로 SMO)에 프로비저닝된 신뢰 앵커와 동일할 가능성이 높음.

</GPT>

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

<GPT>

다음은 \*\*O-RU(Event-Collector Discovery)\*\*의 이벤트 수집기(Event-Collector) 탐지와 관련된 내용입니다.

O-RU가 이벤트 수집기를 자동으로 발견하고, PNF Registration 알림을 전송하는 방법을 설명합니다.  
이 기능은 선택 사항이며, 이 옵션을 지원하는 O-RU에만 해당됩니다.

**IP 주소 할당 방식에 따른 이벤트 수집기 정보 탐지 방법:**

1. **IPv6 Stateless Address Auto-Configuration(SLAAC)**:
   * SLAAC를 사용해 IPv6 주소를 획득한 O-RU는 **Stateless DHCPv6** (RFC3736)을 이용해 이벤트 수집기 정보를 탐지.
2. **Stateful IPv4 또는 IPv6**:
   * IP 주소 할당 중 이벤트 수집기 정보를 함께 획득.
3. **수동 IP 설정**:
   * IP 주소가 수동으로 설정된 O-RU는 이벤트 수집기와 알림 형식(Event-Collector Notification Format)도 수동으로 설정.

**DHCP를 통한 이벤트 수집기 정보 전달:**

* **O-RAN 정의 벤더별 옵션**:
  + DHCPv4 옵션 43 및 DHCPv6 옵션 17을 사용해 이벤트 수집기 정보를 O-RU에 신호화.
* **DHCP 옵션 타입 정의**:
  + 0x83: 이벤트 수집기 IP 주소.
  + 0x84: 이벤트 수집기 완전한 도메인 이름(Fully Qualified Domain Name, FQDN).
  + 0x85: 이벤트 수집기 알림 형식.

**DHCPv4 옵션 43 예시:**

1. **이벤트 수집기 IP 주소**:
   * IP 주소 198.185.159.144인 이벤트 수집기 예시:  
     Type: 0x83  
     Length: 0x04  
     Value: C6 B9 9F 90
2. **이벤트 수집기 FQDN**:
   * 도메인 이름 collector.operator.com인 이벤트 수집기 예시:  
     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
3. **알림 형식**:
   * **ONAP VES 이벤트 리스너** 사양에 따른 알림 형식 사용:  
     Type: 0x85   
     Length: 0x01   
     Value: 00

**DHCPv6 옵션 17 형식:**

* DHCPv4 형식과 유사하되, **Enterprise Number**가 TLV 데이터 앞에 추가.
* IANA에서 O-RAN Alliance에 할당된 Enterprise Number: **53148**.

**미정의 상황:**

* **다중 IP 주소**:
  + 이벤트 수집기 FQDN이 여러 IP 주소로 해석되는 경우에 대한 처리 방식 미정.
* **다중 이벤트 수집기 정보**:
  + 이벤트 수집기 IP 주소 또는 FQDN이 여러 개로 제공되는 경우의 동작 미정.

**알림 형식 지정:**

* 현재 규격에서는 단일 형식만 정의:
  + 값 00: **ONAP VES 이벤트 리스너** 사양에 따른 알림을 기대.

</GPT>

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)**

<GPT>

다음은 **NETCONF Call Home to O-RU Controller(s)** 절의 내용을 요약하고 설명한 것입니다:

이 섹션은 O-RU가 알려진 O-RU 컨트롤러와 **NETCONF 세션**을 설정하기 위한 절차를 다룹니다.

**NETCONF 세션 설정 방법:**

1. **O-RU 컨트롤러 정보 획득**:
   * DHCP 옵션(6.2.5 참조)을 통해 O-RU 컨트롤러 탐지.
   * 기존 NETCONF 클라이언트로부터 설정 정보 제공.
   * 수동으로 구성된 컨트롤러 정보 사용.
2. **컨트롤러 주도 NETCONF 세션**:
   * O-RU 컨트롤러는 PNF Registration 절차를 통해 NETCONF 세션을 시도할 수 있음.
   * 그러나 NAT(Network Address Translation) 제한 등으로 인해 컨트롤러가 세션을 시작하지 못할 수 있음.
3. **O-RU 주도 NETCONF 세션(Call Home)**:
   * 활성 NETCONF 세션이 없는 경우, O-RU는 알려진 모든 O-RU 컨트롤러에 **Call Home** 요청을 전송.
   * Call Home 과정은 **RFC 8071**에 따라 TCP 연결을 통해 NETCONF 세션을 시작.

**NETCONF 세션 재시도 규칙:**

* **“re-call-home-no-ssh-timer”** 사용:
  + NETCONF 세션이 설정되지 않은 O-RU 컨트롤러에 대해 주기적으로 Call Home 절차 수행.
  + SSH 또는 TLS 여부에 관계없이 동일한 타이머 값 사용.
* **최대 시도 횟수**:
  + 알려진 O-RU 컨트롤러당 설정된 최대 재시도 횟수(max-call-home-attempts) 초과 시 O-RU는 자율적으로 리셋 수행.

**TCP 연결 및 포트:**

* **포트 신호**:
  + RFC 8572 DHCP 옵션을 통해 NETCONF 클라이언트와 연결할 포트 정보 제공.
  + DHCP 옵션이 없는 경우:
    - 포트 4334: SSHv2를 통한 NETCONF 연결.
    - 포트 4335: TLS를 통한 NETCONF 연결.
* **프로세스 흐름**:
  + O-RU(NETCONF 서버)가 TCP 연결을 시작.
  + NETCONF 클라이언트가 할당된 포트에서 TCP 연결 수락.
  + 클라이언트가 SSH/TLS 세션을 시작.
  + SSH/TLS 연결을 통해 NETCONF 세션 설정.

**지속적인 연결 유지:**

* **Keep-Alive 메커니즘**:
  + RFC 8071에 정의된 방식으로 연결의 생존 여부를 테스트.
  + "sudo" 권한이 있는 NETCONF 클라이언트와의 연결을 유지해야 함.

**중요 참고사항:**

* **세션 실패 시**:
  + 모든 O-RU 컨트롤러와 NETCONF 세션을 설정하지 못할 경우, O-RU는 자율 리셋을 수행.
* **NETCONF 클라이언트 권한 관리**:
  + NETCONF 클라이언트의 권한 부여와 관련된 사항은 6.5절에서 다룸.

</GPT>

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.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

**[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**

<GPT>

이 섹션은 NETCONF 클라이언트와 O-RU(NETCONF 서버) 간 연결 설정 시의 인증 및 보안 절차를 정의합니다.

**NETCONF 서버의 인증**

1. **클라이언트의 서버 인증 요구사항**:
   * NETCONF 클라이언트는 O-RU로부터 데이터를 송수신하기 전에 **서버의 신원을 검증 및 인증**해야 함.
   * 인증 방식은 로컬 정책에 따라 결정.
2. **SSHv2 사용 시**:
   * **공개 키 기반 호스트 인증**:
     + 클라이언트는 서버(O-RU)를 RFC 4253에 정의된 공개 키 인증 방식으로 인증.
   * **X.509 인증서 기반 서버 인증**(선택 사항):
     + 추가적인 서버 인증 옵션으로 제공 가능.
3. **TLS 사용 시**:
   * **X.509 인증서 기반 상호 인증**:
     + NETCONF 클라이언트와 서버 간 상호 인증 필수.

**SSHv2의 공개 키 기반 호스트 인증**

* **사전 키 프로비저닝 요구사항**:
  + O-RU의 공개 키는 NETCONF 클라이언트(O-DU 및/또는 SMO)에 **사전 프로비저닝**되어야 함.
* **대체 인증 전략 (RFC 4251)**:
  + 초기 연결 시 서버의 호스트 키를 **검증 없이 허용**한 뒤, 이를 로컬 데이터베이스에 저장.
  + 이후 연결 시 저장된 키와 비교하여 인증.
  + 이 방식은 키 관리 절차를 단순화하지만, 보안이 저하될 가능성이 있음.
* **구성 가능 옵션**:
  + 위 대체 전략의 사용 여부는 구성 가능하며, **운영자의 선택에 따라** 활성화 여부를 결정.

**요약**

* NETCONF 연결 과정에서 O-RU의 신원을 인증하기 위한 엄격한 절차가 요구됨.
* 인증 방식은 사용 중인 보안 프로토콜(SSHv2 또는 TLS)에 따라 다르며, TLS는 강제적인 X.509 인증서를 사용.
* SSHv2에서는 공개 키 기반 인증이 기본이며, 보안과 편의성을 조율하는 대체 옵션도 제공됨.

이 절차는 NETCONF 통신의 보안과 신뢰성을 보장하기 위한 핵심입니다.

</GPT>

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

</GPT>

본 섹션은 NETCONF 연결 시 사용되는 보안 프로토콜 및 다중 세션 관리 요건을 설명합니다.

**보안 프로토콜**

1. **지원되는 프로토콜**:
   * **TLS 1.2**:
     + O-RU와 NETCONF 클라이언트(O-DU 또는 SMO) 간 **상호 인증**을 위한 선택적 프로토콜.
   * **SSHv2**:
     + 상호 인증을 위한 **필수 프로토콜**로 지정됨.
2. **프로토콜 지원 요약**:
   * **Table 5.4.2**에 따라 TLS 1.2는 선택적이며, SSHv2는 모든 구현에서 반드시 지원되어야 함.

**다중 세션 관리**

* **세션 분리**:
  + O-RU에서 여러 NETCONF 세션이 설정된 경우, **각 세션은 개별 SSH 터널 또는 TLS 연결**을 통해 설정되어야 함.
  + 이를 통해 세션 간 격리를 보장하고 보안 위협을 최소화.

요약

O-RU의 NETCONF 통신은 SSHv2를 필수적으로 지원하며, TLS 1.2는 선택적으로 사용할 수 있습니다. 다중 세션은 반드시 독립적인 SSH 터널 또는 TLS 연결로 설정되어야 하며, 이는 NETCONF 연결의 안전성과 신뢰성을 유지하기 위한 중요한 요구사항입니다.

</GPT>

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

<GPT>

이 섹션에서는 O-RU 관리 평면 사양에서 정의된 NETCONF 인증 메커니즘을 설명합니다.

**지원되는 인증 메커니즘**

1. **SSHv2**:
   * **Password-based Authentication**: SSHv2를 사용하여 클라이언트 인증 지원.
   * **X.509 Certificate-based Authentication**: X.509 인증서를 기반으로 클라이언트 인증을 선택적으로 지원.
2. **TLS 1.2** (선택 사항):
   * **X.509 Certificate-based Mutual Authentication**: TLS 1.2를 사용하는 경우 클라이언트와 서버 간 상호 인증.

**서버 및 클라이언트 인증 요건**

1. **NETCONF 서버(O-RU) 인증**:
   * NETCONF 클라이언트(O-DU 또는 SMO)가 로컬 정책에 따라 서버의 ID를 확인 및 인증.
   * 인증 데이터를 교환하거나 구성/상태 데이터를 전송받기 전에 인증 완료 필요.
2. **NETCONF 클라이언트(O-DU 또는 SMO) 인증**:
   * NETCONF 서버(O-RU)가 클라이언트의 ID를 확인 및 인증.
   * 인증 방식:
     + **X.509 인증서** 또는
     + **Username/Password**를 통해 인증.
   * 인증 후 클라이언트 요청에 대해 적절한 권한 확인 수행.
3. **X.509 인증서 매핑**:
   * 사용자 이름은 인증서의 **SubjectAltName** 필드를 통해 매핑.
   * 사용자 이름 결정 규칙: RFC 7589에 정의된 규칙 적용.
   * 서버 ID 검증: RFC 7589 및 RFC 6125에 기반.

**초기 시스템 초기화**

1. **기본 계정**:
   * O-RU는 초기화 시 **기본 계정**을 제공:
     + **계정 유형: PASSWORD**:
       - 예: 사용자 이름: oranuser, 기본 비밀번호: o-ran-password.
     + **계정 유형: CERTIFICATE**:
       - 예: 사용자 이름 매핑: san-rfc822-name에 oranuser@o-ran.org.
   * 기본 계정은 **sudo 액세스 그룹**의 멤버로, 추가 계정 생성 가능.
2. **인증서 기반 인증**:
   * O-RU는 플러그 앤 플레이 중 **X.509v3 인증서**를 통한 자동 매핑 지원.
   * O-RU는 초기 설정 시 인증서를 설치하거나, CMPv2 프로토콜을 사용해 운영자의 CA 서버에서 인증서를 자동으로 획득 가능.

**특별 고려 사항**

1. **운영자별 기본 계정**:
   * 기본 계정 설정은 운영자 요구 사항에 따라 조정 가능.
   * 초기 설치 시 안전한 기본 계정 설정을 위한 O-RU 제공 기능 필요.
2. **Zero Touch 지원**:
   * 플러그 앤 플레이 첫 NETCONF 연결을 위해 기본 NETCONF 계정과 인증서의 자동 매핑 지원.
3. **신뢰 앵커**:
   * O-RU와 O-RU 컨트롤러 간 동일한 신뢰 앵커를 사용하여 수동 설정 없이 보안 연결 지원.

O-RU의 NETCONF 인증은 SSHv2와 TLS 1.2 기반으로 설계되어 있으며, 플러그 앤 플레이 및 초기 시스템 초기화를 포함한 다양한 시나리오에서 강력한 인증 및 보안 메커니즘을 제공합니다. 기본 계정 및 자동 인증서 매핑은 운영자 요구 사항과 보안 고려 사항을 충족하기 위해 세부적으로 조정됩니다.

</GPT>

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

<GPT>

다음은 NETCONF 클라이언트를 사용하여 O-RU(개방형 RAN 라디오 장치)에서 사용자 계정을 프로비저닝하는 방식에 대한 설명입니다.

**주요 사항**

1. **사용자 계정 세부 정보**:
   * **사용자 이름**:
     + 3~32자의 문자열.
     + 첫 번째 문자는 소문자여야 함.
     + 나머지 문자는 소문자 또는 숫자만 사용 가능.
   * **계정 유형**:
     + 인증 방식 지정: 비밀번호 기반 또는 인증서 기반.
2. **비밀번호**:
   * 8~128자의 문자열.
   * 허용되는 문자:
     + 소문자 및 대문자.
     + 숫자.
     + 특수 문자: ! $ % ^ ( ) \_ + ~ { } [ ] .
   * **인증서 기반 계정**의 경우 비밀번호 필드가 필요하지 않음.
3. **액세스 제어 그룹**:
   * 계정과 연결된 그룹 지정 (권한 및 그룹 세부 정보는 6.5절 참조).
4. **계정 활성화/비활성화**:
   * 계정이 활성화되었는지 여부 지정.
   * O-RU에는 항상 최소한 하나의 활성 사용자 계정이 있어야 함.
5. **데이터 저장**:
   * 계정 정보(사용자 이름, 비밀번호, 액세스 그룹, 활성화 여부)는 **리셋 지속 메모리**에 저장.
6. **인증서 기반 인증**:
   * 비밀번호 없이 인증 가능.
   * SSH 연결 시, X.509 인증서의 SubjectAltName 필드에 기반하여 사용자를 인증.
7. **기본 계정 관리**:
   * 새로운 관리자 계정(sudo 계정)이 생성되면 기존 NETCONF 세션이 닫히고 기본 계정이 비활성화됨.
   * 기본 계정은 공장 초기화 절차(8.8절 참조)를 통해 다시 활성화 가능.
   * 기본 계정을 활성화하는 다른 방법은 O-RU 벤더 구현에 따라 다를 수 있음.
8. **보안 원칙**:
   * 기본 계정 및 매핑에 정의된 보안 원칙을 따름.
   * O-RU 컨트롤러는 새로운 매핑을 생성해야 함.
   * EE/CA 인증서와 관련된 매핑은 특정 인증서의 지문(fingerprint)이나 SubjectAltName 필드를 기반으로 정의됨(6.4.2절 참조).

</GPT>

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

<GPT>

NETCONF 접근 제어

**개요**

NETCONF 접근 제어는 다수의 NETCONF 클라이언트(사용자)가 정의되었을 때, NETCONF 서버가 각 클라이언트에 대해 특정 작업을 제한하거나 전체 권한을 허용할 수 있도록 합니다. 특히 **하이브리드 관리 구성**(5절 참조)에서는 O-DU의 NETCONF 클라이언트와 SMO의 NETCONF 클라이언트 간의 권한을 다르게 설정할 수 있습니다.

**기준**

* NETCONF 서버는 **IETF NETCONF Access Control Model** (RFC8341)을 사용하여 상호 운용 가능한 접근 제어를 지원해야 합니다.

**접근 제어 그룹**

현재 NETCONF 세션별로 6개의 접근 제어 그룹이 정의됩니다:

1. **sudo**
2. **smo**
3. **hybrid-odu**
4. **nms**
5. **fm-pm**
6. **swm**

**표 6.5.1**에서는 각 그룹 이름과 다양한 권한을 매핑합니다.  
권한은 네임스페이스(namespace)별로 다음과 같이 정의됩니다:

* **읽기 (R)**
* **쓰기 (W)**
* **실행 (X)**
* 알림 구독(Notifications)

**하이브리드 관리 모드에서의 권한**

* 하이브리드 관리 모드에서는 \*\*중앙화된 네트워크 관리 시스템(NMS)\*\*의 NETCONF 클라이언트가 **sudo** 권한을 가지는 것이 허용될 수 있습니다.
  + 이를 통해 O-RU의 설정을 편집할 수 있습니다.
* 그러나 이 경우, O-DU의 동작은 명확히 정의되지 않을 수 있습니다.  
  예를 들어, 중앙화된 NMS가 O-RU에 **autonomous reset RPC**를 트리거한 경우:
  + O-DU가 O-RU로부터 restart-cause 정보를 가져와 NMS가 리셋을 수행했음을 인지하지 못할 수 있습니다.

**권장 사항**

* 하이브리드 모드에서는 다음과 같은 권한 그룹을 사용하는 것이 권장됩니다:
  + O-DU의 NETCONF 클라이언트 → **“hybrid-odu”** 그룹.
  + SMO의 NETCONF 클라이언트 → **“smo”** 그룹.

**권한 및 사용자-그룹 매핑 관리**

* 이 매핑은 **ietf-netconf-acm.yang** 모델의 **rule list**에 인코딩되어야 합니다.
* **rule list**는 어떤 NETCONF 클라이언트도 수정할 수 없도록 설정되어야 합니다.
* 동일한 모델은 **사용자 이름과 그룹 간 매핑**을 구성하는 데에도 사용됩니다.

이 접근 제어 메커니즘은 다양한 NETCONF 클라이언트의 작업을 제한하거나 허용함으로써 시스템의 보안과 관리 효율성을 강화하는 데 목적이 있습니다.

</GPT>

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

<GPT>

**기능 광고**

* O-RU는 NETCONF **Hello 메시지**에서 자신의 NETCONF 기능을 광고합니다.
  + 이 메시지는 NETCONF RFCs에서 정의된 표준 기능 지원 여부와 특정 네임스페이스 지원 여부를 나타냅니다.
* NETCONF 기능은 O-RU와 NETCONF 클라이언트 간에 교환됩니다.

**기능 예시**

다음은 지원되는 NETCONF 기능의 예입니다:

* **Writable-running** 기능
* **Candidate Configuration** 기능 및 관련 **Commit** 작업
* 변경 사항 폐기(Discard change) 작업
* 잠금 및 잠금 해제(Lock and Un-lock) 작업
* **Confirmed Commit** 기능
* **Cancel Commit** 작업
* **Rollback on Error** 기능
* **Validate** 기능
* 시작 구성(Startup Configuration) 기능
* **URL** 기능
* **XPATH** 기능
* **알림(Notifications)** 기능
* **Interleave** 기능

**필수 지원 기능**

모든 O-RAN O-RU는 다음 기능을 지원해야 합니다:

1. **XPATH 기능**
2. **NETCONF 알림(Notifications)**
3. **Writable-running** 또는 **Candidate Configuration** 중 하나 이상

**데이터 검색**

* NETCONF 클라이언트는 **get RPC**와 함께 **sub-tree 기반 <filter>** 및 \*\*XPATH 기반 <filter>\*\*를 사용하여 O-RU로부터 특정 하위 트리를 검색할 수 있습니다.
* NETCONF 기반 구성 관리에 대한 자세한 내용은 **9절**을 참조하세요.

**타이머 간 상호작용 관리**

* **NETCONF Confirmed Commit** 기능 사용 시, \*\*확인 타이머(confirmed-timeout)\*\*와 **감시 타이머(supervision-notification-interval)** 간의 상호작용을 피해야 합니다.
  + RFC 6241에 따라 기본 확인 타이머 값은 **600초**로 설정됩니다.
  + \*\*감시 타이머(supervision-notification-interval)\*\*는 **o-ran-supervision.yang**에서 기본값이 **60초**로 정의됩니다.
* **sudo 권한**을 가진 NETCONF 클라이언트는 확인 타이머(confirmed-timeout)를 \*\*감시 타이머(supervision-notification-interval)\*\*보다 작게 설정해야 합니다.

이 내용은 O-RU가 NETCONF 클라이언트와 상호작용할 때 지원하는 기능을 정의하고, 타이머 간 충돌을 방지하기 위한 관리 지침을 제공합니다.

</GPT>

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

<GPT>

**개요**

* **NETCONF 연결 모니터링**은 지속적인 NETCONF 세션을 유지하기 위한 메커니즘입니다.
* O-RU와 NETCONF 클라이언트 간 연결 상태를 확인하기 위해 **watchdog 타이머**(supervision timer와 notification timer)를 사용합니다.
* O-RU는 클라이언트가 **supervision-notification** 알림에 가입하면 타이머를 작동시켜 연결을 모니터링합니다.
* O-RU 클라이언트는 **<supervision-watchdog-reset> RPC**를 사용하여 O-RU에 연결 상태를 확인시키고 타이머를 재설정합니다.

**감시 타이머(Watchdog Timers)**

* **Notification Timer**
  + **기본값**: supervision-notification-interval (60초)
  + **동작**: O-RU는 클라이언트에게 주기적으로 **supervision-notification**을 전송합니다.
  + 클라이언트는 알림을 수신하여 연결 상태가 정상임을 확인합니다.
* **Supervision Timer**
  + **기본값**: supervision-notification-interval (60초) + guard-timer-overhead (10초)
  + **동작**: 클라이언트가 주기적으로 타이머를 재설정하지 않으면 타이머가 만료되고 "supervision failure(감시 실패)" 상태가 됩니다.

**타이머 작동 절차**

1. **타이머 시작**
   * 클라이언트가 **<create-subscription> RPC**를 보내 **supervision-notification** 스트림에 가입하면 타이머가 시작됩니다.
   * 타이머가 활성화되면 O-RU는 주기적으로 알림을 전송하고 클라이언트는 이를 수신합니다.
2. **타이머 재설정**
   * 클라이언트는 **<supervision-watchdog-reset> RPC**를 사용하여 타이머를 재설정하거나 새 값을 설정할 수 있습니다.
   * 새 값은 즉시 적용됩니다.
3. **알림 종료**
   * 클라이언트가 세션을 종료하거나 알림 스트림 구독을 취소하면 O-RU는 알림 전송을 중단합니다.

**감시 실패 조건**

* **Supervision Timer 만료**:
  + O-RU는 **supervision failure** 상태로 전환하며, 이 상황은 14.1.1 절에서 정의된 절차에 따라 처리됩니다.
* **알림 구독 종료**:
  + 클라이언트가 알림 스트림 구독을 종료하면 O-RU는 **Supervision Termination(감시 종료)** 절차를 수행합니다(14.1.2 절 참조).

**오류 처리**

* 클라이언트가 타이머 값을 설정하려 할 때, 다른 클라이언트가 running configuration을 잠궜다면:
  + **<supervision-watchdog-reset> RPC**는 성공할 수 있으나 타이머 값 변경은 실패할 수 있습니다.
  + O-RU는 RPC 출력에 오류 메시지를 포함해 클라이언트에게 이를 알립니다.

**참고 사항**

* O-RU는 여러 알림 스트림에 대해 개별적으로 구독 메시지를 처리해야 합니다(11.3 절 참조).
* 감시 실패 또는 구독 종료에 따른 구체적인 절차는 14.1.1 및 14.1.2 절에 정의되어 있습니다.

</GPT>

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.

텍스트, 스크린샷, 평행, 도표이(가) 표시된 사진

자동 생성된 설명

**[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

<Perplexity>

NETCONF 세션을 종료하는 과정은 다음과 같이 정의됩니다:

종료 명령

* NETCONF 클라이언트는 세션을 종료하기 위해 <close-session/> RPC 명령을 발행합니다.

O-RU의 응답

* O-RU는 이 명령에 응답하고 SSH 세션 또는 TLS 연결을 종료합니다.
* 이후 O-RU는 "call home" 절차를 재개합니다. 이는 O-RU가 관리 시스템과의 연결을 유지하기 위한 절차입니다.

정상 운영 시 주의사항

* 일반적으로 "sudo" 또는 "hybrid-odu" 권한을 가진 최소 한 개의 NETCONF 세션이 장기적으로 유지되며, 이 세션은 O-RU의 감독 워치독 타이머를 반복적으로 재설정하는 데 사용됩니다.
* 다른 권한 그룹에 속하는 NETCONF 클라이언트는 지속적인 NETCONF 세션을 운영할 것으로 기대되지 않습니다.

클라이언트 제거 시 처리

* 만약 NETCONF 클라이언트가 이전에 O-RU에 의해 NETCONF를 사용하여 구성되었고, 이후 해당 클라이언트가 O-RU의 구성에서 제거된다면, 예를 들어 "sudo" 권한을 가진 다른 NETCONF 클라이언트에 의해 제거된 경우, NETCONF 서버는 제거된 클라이언트의 NETCONF 세션을 강제로 종료해야 합니다.

예시

세션 종료를 위한 RPC 호출 예시는 다음과 같습니다:

<rpc>

<close-session/>

</rpc>

이 호출에 대한 응답은 다음과 같이 나타납니다:

<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">

<ok/>

</rpc-reply>

결론

NETCONF 세션 종료는 관리 및 보안 측면에서 중요한 절차로, 이를 통해 시스템 자원의 효율적인 관리를 도모하고, 불필요한 연결을 해소하여 보안을 강화할 수 있습니다.

</Perplexity>

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

<GPT>

PNF(Physical Network Function) 등록 및 Event-Collector와의 통신 채널 모니터링 지원에 대한 선택적 기능을 다루고 있습니다.

O-RU(Open Radio Unit)가 Event-Collector에 대해 PNF(Physical Network Function) 등록을 지원하는 것은 선택 사항입니다. 따라서, Clause 6.9의 내용은 이 선택적 기능을 지원하는 O-RU에만 적용됩니다.

또한, PNF 등록 기능을 지원하는 O-RU는 Clause 18.6에서 정의된 Event-Collector와의 통신 채널 모니터링 기능도 반드시 지원해야 합니다.

</GPT>

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

<GPT>

**pnfRegistration** 알림은 O-RU(Open Radio Unit)가 발견된 Event-Collector에 REST/HTTPS를 통해 전송하는 JSON 형식의 메시지입니다.  
PNF 등록을 수행하기 위한 사전 조건으로, O-RU는 먼저 **Clause 6.2.7**에 설명된 대로 DHCP/DHCPv6 옵션에 인코딩된 Event-Collector 정보를 수신해야 합니다.

O-RU는 다음의 절차를 통해 PNF 등록을 수행합니다:

1. **HTTP 연결 설정**: O-RU는 TLS를 사용하여 발견된 Event-Collector와 HTTP 연결을 설정하고, TLS를 통해 연결을 인증합니다.
2. **pnfRegistration 알림 전송**: HTTP/TLS 연결을 통해 pnfRegistration 알림을 신호로 전송합니다.
3. **반복 전송**: SMO(Service Management and Orchestration)가 O-RU와 NETCONF 세션을 설정할 때까지, pnfRegistration 알림 전송을 주기적으로 반복합니다.
4. **절차 도식**: 이러한 절차는 **Figure 6.9.2.1**에 도식화되어 있습니다.

O-RU가 **Clause 6.3**에서 설명된 **Call Home 절차**를 동시에 수행하면서 PNF 등록 절차를 수행하는 경우, SMO가 O-RU와 NETCONF 세션을 설정했음을 확인할 수 있어야 합니다.

이 확인은 다음 방식으로 이루어집니다:

* O-RU는 NETCONF 세션이 시작된 원본 IP 주소를 분석합니다.
* 이는 SMO의 NETCONF 세션이 O-RU가 Call Home 절차를 수행하고 있는 “알려진 O-RU 컨트롤러”의 IP 주소와 구별되는 IP 주소에서 시작된다는 가정에 기반합니다.

</GPT>

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.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

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

## 6.10 Encoding of PNF Registration Notification

<GPT>

이 명세 버전에서는 **pnfRegistration 알림의 인코딩 방식**이 ONAP(Open Network Automation Platform) 정의 [37]를 따릅니다.

**포함해야 할 정보**

pnfRegistration 알림에는 NETCONF 클라이언트가 O-RU의 NETCONF 서버와 IP 연결을 설정하기 위해 필요한 IP 주소 정보가 포함되어야 합니다.

* **IPv4 인터페이스가 구성된 경우**: oamV4IpAddress 필드를 포함해야 합니다.
* **IPv6 인터페이스가 구성된 경우**: oamV6IpAddress 필드를 포함해야 합니다.

**알림 내용의 출처**

* 알림의 세부 내용은 O-RU의 \*\*구성 데이터베이스(Configuration Database)\*\*에서 파생됩니다.
* 관련 정보는 \*\*표 6.10.1(Table 6.10.1)\*\*을 참고하여 구성됩니다.

**O-RU의 지원 요구 사항**

O-RU는 다음 YANG 모델의 특정 버전 또는 그 이상의 버전을 지원해야 합니다:

1. **o-ran-hardware.yang**:
   * 리비전 5.0.0 이상.
   * 이 모델은 unitFamily 및 unitType 값과 관련된 스키마 노드를 정의합니다.
2. **o-ran-operations.yang**:
   * 리비전 5.0.0 이상.
   * 이 모델은 pnfRegistration 필드의 버전과 관련된 스키마 노드를 정의합니다.

</GPT>

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

<GPT>

O-RU(Open Radio Unit)에는 여러 네트워크 인터페이스가 포함되며, 이들에는 **Ethernet, VLAN, IP 인터페이스** 등이 있습니다. 이 섹션에서는 O-RU의 네트워크 인터페이스 관리를 설명합니다.

**인터페이스 구성**

* O-RU의 인터페이스 구성은 **o-ran-interfaces.yang** 모듈을 사용하여 정의됩니다.
* 이 모듈은 표준 **ietf-interfaces.yang** 및 **ietf-ip.yang** 모듈을 확장(augment)하여 사용됩니다.
* O-RU의 인터페이스는 \*\*계층적 설계(layering principle)\*\*를 기반으로 하며, 각 인터페이스는 고유한 이름을 가집니다.

**인터페이스 계층 구조**

1. **기본 인터페이스(Base Interface)**:
   * **Ethernet 인터페이스**가 기본 인터페이스로 사용됩니다.
   * 이 인터페이스는 다음 정보를 포함합니다:
     + 최대 전송 단위(l2-mtu)
     + 하드웨어 주소(hardware-address)
     + 선택적으로 CU-plane 전송에 사용할 수 있는 별칭 MAC 주소(alias MAC addresses)
2. **VLAN 인터페이스**:
   * Ethernet 인터페이스 위에 정의됩니다.
3. **IP 인터페이스**:
   * VLAN 및 Ethernet 인터페이스 모두 IP 인터페이스를 지원할 수 있습니다.
   * IP 인터페이스는 표준 **ietf-ip.yang** 모델을 기반으로 정의됩니다.
   * 각 IP 인터페이스는 IPv4 및/또는 IPv6 인터페이스를 포함할 수 있습니다.

**운영 상태(Operational State)**

* 계층 3(Layer 3) 구성 정보를 제공합니다:
  + 네트워크 접두사(prefix)
  + 도메인 이름 서버(DNS)
  + 기본 게이트웨이 주소(default gateway addresses)

**CoS 및 DSCP 마킹**

* **CoS(Class of Service)** 및 **DSCP(Differentiated Services Code Point)** 마킹을 지원합니다.
* u-plane, c-plane, m-plane 트래픽에 대해 독립적으로 설정 가능하며, 기본적으로 O-RU는 모든 사용자 평면 트래픽(user-plane flows)을 동일하게 마킹합니다.
* 선택적으로 업링크 트래픽에 대해 향상된 사용자 평면 마킹을 지원할 수 있습니다.
  + 이를 통해 O-RU의 개별 수신 엔드포인트에서 다른 CoS 또는 DSCP 값을 설정하고, 전송 시스템에서 업링크 트래픽을 차별화된 방식으로 처리할 수 있습니다.

**운영 상태 보고 및 RPC**

* **o-ran-interfaces.yang** 모델은 **ietf-interfaces.yang** 모델을 확장하여, 각 인터페이스의 패킷 및 바이트 수를 보고할 수 있는 기능을 제공합니다.
* 또한, o-ran-interfaces 모듈은 이러한 카운터를 재설정할 수 있는 단일 RPC를 정의합니다.

</GPT>

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

<GPT>

**o-ran-transceiver YANG 모듈**은 SFP, SFP+, SFP28, XFP, QSFP, QSFP+, QSFP28, QSFP56 등의 **플러그형 트랜시버 모듈**의 운영 상태를 정의합니다.  
각 트랜시버는 고유한 \*\*인터페이스 이름(interface-name)\*\*과 \*\*포트 번호(port number)\*\*와 연관됩니다.

**디지털 진단 모니터링 인터페이스**

* 광학 트랜시버의 **디지털 진단 모니터링 인터페이스**를 통해 디바이스의 작동 파라미터에 접근할 수 있습니다.
* **SFF-8472** [16] 및 **SFF-8636** [34]에 따라 데이터는 보통 파일 형태로 트랜시버 모듈에서 검색됩니다.
* 이 파일은 O-RU를 통해 NETCONF 클라이언트가 획득할 수 있습니다.
  + 추가 정보는 **Clause 9**를 참조하세요.

**QSFP 폼팩터**

* **QSFP 폼팩터**는 다중 파장(4xTx 및 4xRx) 또는 다중 섬유(MPO - Multifibre Parallel Optic)를 지원할 수 있습니다.
* QSFP 디지털 진단 인터페이스 [34]는 광학 레인의 사용법을 설명하며, O-RU 인터페이스 관리에서는 모든 미디어 레인에 대한 \*\*"transceiver fault"(경고 29)\*\*를 정의합니다.

**트랜시버 데이터 처리**

1. **데이터 저장 형식**:
   * **바이너리 파일 형식**으로 데이터가 저장됩니다.
   * 메모리 주소에 따라 다음과 같이 바이트를 읽습니다:
     + **i < 256**: 0xA0 주소에서 데이터 주소 i의 바이트 읽기.
     + **i ≥ 256**: 0xA2 주소에서 데이터 주소 i-256의 바이트 읽기.
2. **데이터 저장 및 파일 생성**:
   * O-RU는 트랜시버 모듈을 감지하면 부팅 시 해당 데이터를 저장하고 파일로 작성합니다.
   * NETCONF 클라이언트는 **Clause 12**에서 정의된 **File Upload 절차**를 통해 파일을 업로드할 수 있습니다.
   * O-RU는 런타임 동안 트랜시버 메모리와 파일 내용을 동기화하지 않습니다. 따라서 **동적 정보**는 오래된 값일 수 있습니다.
   * 트랜시버 모듈 제거 시에도 O-RU는 파일을 삭제하지 않습니다.
3. **파일 업로드 및 실패 처리**:
   * 트랜시버 모듈이 없는 경우 O-RU는 파일을 생성하지 않거나 기존 파일을 제거합니다.
   * 업로드 절차 중 트랜시버가 삽입되면:
     + 이전 내용이 포함된 파일이 제공되거나, 실패 메시지가 반환될 수 있습니다.
   * 존재하지 않는 파일 요청 시 업로드 절차는 실패합니다.

**파일 명명 규칙**

파일 이름은 다음과 같은 형식을 따릅니다:  
sfp\_{portNumber}.sffcap

* {portNumber}는 해당 포트 트랜시버 데이터 리스트의 **port-number** 필드 값을 나타냅니다.
* **예시**: sfp\_0.sffcap, sfp\_1.sffcap

</GPT>

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

<GPT>

**o-ran-interfaces YANG 모델**에서 각 Ethernet 인터페이스는 VLAN 태깅 지원 여부를 나타내는 leaf를 포함합니다.

**기본 동작**

* 기본적으로 모든 인터페이스에서 **VLAN 태깅**이 활성화되어 있습니다.
* 이는 O-RU가 **Clause 6.2.3**에서 설명된 대로 스스로 \*\*트렁크 포트(trunk port)\*\*에 연결되었음을 감지할 수 있게 합니다.

**C/U Plane VLAN 할당**

* O-RU가 트렁크 포트에 연결된 경우, C/U Plane 연결을 위해 VLAN이 할당됩니다.
* **관리 평면(management plane)** 연결에 사용되는 VLAN과는 다른 VLAN이 C/U Plane 트래픽에 사용될 수 있습니다.
* **규칙**:
  + 특정 eAxC\_ID에 대해 U-Plane에 할당된 VLAN은 C-Plane에 할당된 VLAN과 동일해야 합니다.
  + 만약 다른 VLAN을 사용하는 경우, NETCONF 클라이언트가 O-RU에서 C/U Plane VLAN을 구성해야 합니다.

**VLAN 인터페이스 구성**

* **o-ran-interfaces** 모델에 따라, NETCONF 클라이언트는 각 활성 VLAN에 대해 별도의 이름이 지정된 인터페이스(named interfaces)를 구성해야 합니다.
* **구성 방식**:
  + **C/U Plane VLAN 인터페이스**는 상위 계층 인터페이스(higher-layer-if)로 정의됩니다.
  + 이 상위 계층 인터페이스는 기본 Ethernet 인터페이스를 하위 계층 인터페이스(lower-layer-if)로 참조합니다.

이 요약은 C/U Plane VLAN 구성의 주요 내용을 명확히 설명하며, VLAN 태깅, 트렁크 포트 감지, 그리고 VLAN 인터페이스 관리 방식에 대한 이해를 돕기 위해 작성되었습니다.

</GPT>

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

<GPT>

**적용 범위**

* UDP/IP를 통한 **C/U Plane 트래픽 전송**은 선택적 기능입니다.
* 따라서 이 섹션은 **UDP/IP 기반 C/U Plane 트랜스포트를 지원하는 O-RU**에만 적용됩니다.

**IPv4/IPv6 지원**

* UDP/IP 기반 C/U Plane 전송을 지원하는 O-RU는 **IPv4** 및/또는 **IPv6**를 기반으로 하는 전송을 지원해야 합니다.
* NETCONF 클라이언트는 **get RPC**를 사용하여 O-RU가 지원하는 인터페이스 목록을 조회할 수 있습니다.
  + 인터페이스 내의 **IPv4 컨테이너** 또는 **IPv6 컨테이너**가 존재하면 해당 IP 버전을 지원하는 것으로 간주됩니다.

**C/U Plane 및 관리 Plane의 IP 인터페이스 구분**

* **UDP/IP 기반 C/U Plane 트래픽**에 사용되는 IP 인터페이스는 관리 Plane 연결에 사용되는 IP 인터페이스와 다를 수 있습니다.
* 이 경우, NETCONF 클라이언트는 **ietf-ip YANG 모델**을 사용하여 IPv4 및/또는 IPv6 컨테이너를 구성하여 C/U Plane IP 인터페이스를 설정해야 합니다.

**인터페이스 구성**

* NETCONF 클라이언트가 정의한 C/U Plane 인터페이스는 다음 중 하나로 구성될 수 있습니다:
  + **Ethernet 인터페이스**: interface type이 ianaift:ethernetCsmacd로 설정됨.
  + **VLAN 인터페이스**: interface type이 ianaift:l2vlan로 설정됨.
  + VLAN이 IP 기반 C/U Plane 트래픽을 지원하는지에 따라 결정됩니다.
* NETCONF 클라이언트는 이 인터페이스에 대해 정적 IP 주소를 설정할 수 있습니다.
  + 정적 IP 주소가 설정되지 않은 경우, O-RU는 IP 주소 할당 절차를 수행해야 합니다.

**IP 주소 할당 절차**

1. **IPv4를 지원하는 경우**:
   * **DHCPv4**를 사용하여 IP 주소를 설정합니다.
2. **IPv6을 지원하는 경우**:
   * \*\*IPv6 Stateless Address Auto-Configuration (SLAAC)\*\*를 사용.
   * **DHCPv6**를 통한 상태 기반(State-full) 주소 구성을 사용.

</GPT>

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

<GPT>

**C/U Plane 데이터 흐름과 처리 요소**

* **CU-plane 애플리케이션**은 특정 데이터 흐름과 고유하게 연결되어야 합니다.
* 이를 위해 \*\*O-RU "처리 요소(processing element)"\*\*가 정의됩니다.
  + 이 요소는 특정 **C/U Plane 엔드포인트 주소** 또는 **지연 측정 작업**과 연결됩니다.
  + 특별히 명시되지 않는 한, 동일한 eAxC\_ID에 관련된 \*\*제어(C-plane)\*\*와 **사용자(User-plane)** 애플리케이션 구성 요소는 **공통 처리 요소**를 사용해야 합니다.

**처리 요소의 엔드포인트 정의 방식**

O-RU 관리 Plane은 특정 처리 요소에 사용되는 **전송 기반 엔드포인트 식별자**를 정의하는 여러 옵션을 지원합니다.  
**3가지 주요 옵션**:

1. **(별칭) MAC 주소**를 사용하는 처리 요소 정의.
2. **VLAN ID**와 **MAC 주소의 조합**을 기반으로 한 처리 요소 정의.
3. **UDP 포트와 IP 주소**를 기반으로 한 처리 요소 정의.

* **주의**: 현재 IANA에서 o-ran 애플리케이션을 위해 할당된 명확한 소스 포트 번호는 없습니다.  
  따라서 NETCONF 클라이언트가 O-RU에서 해당 포트 번호를 구성해야 합니다.

**처리 요소의 구성**

* 처리 요소는 특정 데이터 흐름과 관련된 **로컬 및 원격 엔드포인트**를 정의합니다.
* 처리 요소 정의에는 고유한 \*\*요소 이름(element name)\*\*이 포함되며, 다른 시스템에서 해당 처리 요소 인스턴스를 참조할 때 사용됩니다.
* **o-ran-interfaces YANG 모델**:
  + 별칭 MAC 주소 및 UDP/IP를 기반으로 한 C/U Plane 전송 지원 기능 정의.
  + NETCONF 기능 교환을 통해 O-RU가 지원하는 선택적 기능을 신호합니다(Annex C에 설명).
* **o-ran-processing-elements YANG 모델**:
  + 처리 요소 목록을 정의하는 **processing-elements 컨테이너**를 사용.
  + 각 처리 요소는 고유한 **요소 이름**으로 식별됨.
  + 각 처리 요소는 데이터 흐름 지원에 사용되는 특정 **인터페이스 이름**을 참조.
  + C/U Plane 전송 세션 유형에 따라 추가적인 leaf 구성 요소가 설정됩니다:
    - **MAC 주소**
    - **VLAN**
    - **IP 주소**
    - **UDP 포트**

**처리 요소의 메시지 필터링**

* O-RU는 처리 요소가 구성되지 않은 상태로 전송된 CU-plane 메시지(eCPRI/IEEE 1914 프레임/패킷)를 **폐기**할 수 있습니다.

</GPT>

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

<GPT>

7.6 O-DU의 C/U Plane 전송 연결 확인

**7.6.1 C/U Plane 전송 연결 확인 절차**

**O-DU**와 **O-RU** 간에는 여러 **C/U Plane 데이터 흐름**이 교환될 가능성이 있습니다. 이를 위해 **종단 간 전송 연결성**을 확인할 수 있는 절차가 필요합니다.

**O-RU는 요청/응답 기능을 활용하여 전송 연결 확인 기능을 지원해야 합니다.**  
해당 절차는 **Figure 7.6.1.1**에 설명된 방식으로 수행됩니다.

**연결 확인 절차의 주요 기능**

O-DU는 사용자 Plane 엔드포인트 간의 도달 가능성 및 연결성을 확인하기 위해 다음과 같은 작업을 수행합니다:

1. **O-RU 구성 중**: 전송 구성의 유효성을 확인.
2. **운영 중**: 네트워크 연결 상태를 지속적으로 모니터링.

**연결 확인 방법**

* 패킷 네트워크에서 연결 확인은 일반적으로 \*\*프로브 메시지(probe message)\*\*를 엔드포인트 간에 교환하여 수행됩니다.
* 이 메시지 교환의 주기는 사용 사례에 따라 다릅니다.
  + \*\*가용성 측정(availability measurement)\*\*의 경우, 주기는 보통 **1초에서 60초 사이**입니다.

**지원 프로토콜**

전송 연결 확인 절차를 수행하기 위해 다음 두 가지 네트워크 프로토콜이 정의되었습니다:

1. **Ethernet 기반 C/U 세션**:
   * **Loop-back Protocol (LB/LBM)**
   * IEEE 802.1Q (수정안 802.1ag)에서 정의됨【17】.
2. **IP 기반 C/U 세션 (O-RU가 지원 시)**:
   * **UDP Echo**
   * RFC 862에서 정의됨【18】.

**요약**

* O-RU는 O-DU와의 전송 연결 상태를 확인할 수 있는 기능을 제공해야 하며, 이를 위해 요청/응답 기반의 프로브 메시지를 주기적으로 교환합니다.
* 지원 프로토콜은 Ethernet의 **LB/LBM** 또는 IP 기반의 **UDP Echo**로 구성됩니다.
* 이 기능은 O-RU 구성 및 운영 중 네트워크 상태를 확인하고 유지하기 위한 핵심입니다.

</GPT>

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].

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

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

### 7.6.2 Ethernet connectivity monitoring procedure

#### 7.6.2.1 Monitoring Procedure

<GPT>

**C/U Plane 세션이 Ethernet에서 운영되는 경우**, 전송 연결 확인은 Ethernet 계층에서 수행됩니다.  
이 사양에 따라, **Ethernet 연결 모니터링 프로토콜**은 \*\*IEEE 802.1Q (수정안 802.1ag)\*\*에서 정의된 \*\*Loop-back Protocol (LBP)\*\*을 기반으로 합니다【17】.

**연결 모니터링의 구성 요소**

1. **C/U Plane 메시징 엔드포인트**는 프론트홀 네트워크에서 동일한 \*\*Maintenance Entity (ME)\*\*의 일부로 간주됩니다.
2. 각 엔드포인트는 **Maintenance Association End Point (MEP)** 역할을 맡아 LBM(Loop-back Message)을 처리합니다.

**LBM 요청 관리**

* **LBM 전송 및 중지는 O-DU에서 관리적으로(Administratively) 수행**됩니다.
* LBM 요청을 전송하기 위해, 관리 엔터티는 다음 정보를 O-DU에 제공해야 합니다:
  + LBM 요청을 시작할 명령
  + 응답자로 설정된 O-RU의 **Ethernet MAC 주소**

**LBM 요청 전송**

* 이 사양에서는 **모든 LBM 요청이 O-DU에서 O-RU로 전송**됩니다.
* 요청은 항상 **O-RU의 유니캐스트 Ethernet MAC 주소**를 대상으로 합니다.

**요약**

* O-RU와 O-DU 간 Ethernet 연결 확인은 \*\*Loop-back Protocol (LBP)\*\*을 사용해 수행됩니다.
* O-DU는 관리적으로 LBM 요청을 시작하며, 각 요청은 O-RU의 유니캐스트 MAC 주소로 전송됩니다.
* 이 절차는 C/U Plane 세션의 안정적인 Ethernet 연결을 보장하는 데 필수적입니다.

</GPT>

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.

#### 7.6.2.2 Validating the transport configuration

<GPT>

이 내용은 O-RAN 시스템에서 O-DU(Open Distributed Unit)와 O-RU(Open Radio Unit) 간의 전송 구성(Transport Configuration)을 검증하는 방법에 대한 설명입니다.

**전송 구성 검증 과정**

1. **U/C-plane 세션 설정**  
   O-DU와 O-RU 간에 U-plane(User Plane) 또는 C-plane(Control Plane) **세션이 설정되면**, 연결이 올바르게 구성되었는지 확인해야 합니다.
2. **LBM 응답자(LBM Responder) 활성화**
   * O-RU에서는 U/C-plane **메시징 엔드포인트가 활성화**되면, **LBM(Loopback Message) 응답자** 애플리케이션이 자동으로 실행됩니다.
   * 이 응답자는 해당 엔드포인트로 들어오는 LBM 요청에 자동으로 응답합니다.
3. **O-DU에서 LBM 요청 전송**
   * O-DU는 구성 명령에 따라 미리 정해진 수의 LBM 요청을 정해진 간격으로 O-RU로 전송합니다.
   * O-DU는 O-RU로부터 받은 LBM 응답 정보를 내부 데이터베이스에 저장합니다.
   * O-RU는 **이더넷 MAC 주소**와 **CU-plane VLAN**을 기반으로 식별됩니다.
4. **연결 상태 확인**
   * 올바르게 구성된 세션에서는 O-DU가 O-RU로부터 LBM 응답을 네트워크 지연 시간(network latency)과 O-RU의 응답 시간에 따라 적절한 시간 내에 받아야 합니다.
   * O-DU가 O-RU로부터 LBM 응답을 정상적으로 수신하면 세션이 "운영 상태"로 간주됩니다.

**주의 사항**

* O-RU는 서로 다른 원격 유지 관리 엔드포인트(Remote Maintenance Association Endpoint)에서 들어오는 LBM 메시지에도 응답할 수 있어야 합니다.

**목적**

이 과정은 O-DU와 O-RU 간의 연결 상태를 확인하고, 구성된 세션이 제대로 작동하는지 보장하기 위한 것입니다. 정상적인 LBM 응답이 오지 않을 경우, 연결 문제 또는 구성 오류를 의심할 수 있습니다.

</GPT>

After setting up a U/C-plane session between an O-DU and an O-RU, the O-DU can test whether connectivity exists as per the configuration. To achieve that, at the time a U/C-plane messaging endpoint becomes operational at an O-RU, it starts an LBM responder application which automatically responds to incoming LBM requests on that endpoint. Based on a configuration command the O-DU starts sending out a predefined number of LBM requests to its O-RU(s) at a predefined interval, storing the information received in LBM responses from the O-RU(s) in an internal database. O-RU(s) are identified by both Ethernet MAC address and the CU plane VLAN. NOTE : The O-RU shall be able to respond to Loopback Messages received from different remote Maintenance Association Endpoints In case the configuration of the session is indeed correct, the O-DU should receive LBM responses from the O-RU(s) within a time frame dependent on the network latency and the O-RU’s reaction time. If LBMs from the O-RU(s) are being received, the session is determined to be operational.

#### 7.6.2.3 Monitor network connectivity

<GPT>

O-RAN 시스템에서 O-DU가 O-RU와의 네트워크 연결 상태를 지속적으로 모니터링하는 방법에 대해 설명합니다.

**네트워크 연결 상태 모니터링 절차**

1. **초기 검증 완료 후 지속 모니터링 시작**
   * **7.6.2.2 절차**에서 연결 상태가 성공적으로 검증된 이후, O-DU는 네트워크 연결 상태를 유지하기 위해 **지속적인 모니터링** 절차를 실행합니다.
2. **LBM 요청 지속 전송**
   * O-DU는 설정된 간격에 따라 LBM(Loopback Message) 요청을 계속해서 O-RU로 전송합니다.
   * LBM 응답을 수신하면 이를 기록하여 연결 상태를 추적합니다.
3. **연결 상태 판별 기준**
   * O-DU는 수신된 LBM 응답을 기반으로 O-RU와의 연결 상태를 판단합니다:
     + **연결 상태 정상**: 설정된 간격에 따라 O-RU로부터 LBM 응답이 계속 수신되는 경우, 연결이 유지되고 있다고 간주합니다.
     + **연결 상태 비정상**: 특정 O-RU로부터 설정된 LBM 요청 간격의 **3배 시간** 이상 동안 LBM 응답이 수신되지 않으면 연결이 끊어진 것으로 간주합니다.

**목적**

이 과정은 O-DU와 O-RU 간의 네트워크 연결 상태를 지속적으로 모니터링하여 연결 문제를 빠르게 감지하고, 네트워크 안정성을 유지하기 위함입니다.

* 설정된 간격과 기준은 네트워크의 성능과 요구사항에 따라 조정될 수 있습니다.
* 연결이 비정상으로 판별되면 적절한 장애 조치가 필요합니다.

</GPT>

After the procedure described in clause 7.6.2.2 has been executed successfully, a further procedure may be executed continuously to maintain the connectivity status. To achieve this the O-DU continues to send out LBM requests at the configured interval. It also keeps track of LBM responses received. Based on the LBM responses received the O-DU shall decide on the connectivity status. Connectivity shall be assumed to be available as long as LBM responses from the O-RU(s) are being received at the configured interval. Connectivity shall be assumed not available if no LBM response from the particular O-RU has been received for an interval that is as long as 3 x the configured LBM request interval or longer.

#### 7.6.2.4 Managing Ethernet connectivity monitoring procedure

<GPT>

O-RAN 시스템에서 이더넷 연결 모니터링 절차를 관리하기 위한 방법을 설명합니다.

**이더넷 연결 모니터링 절차 관리**

1. **이더넷 인터페이스 지원**
   * O-DU는 하나 이상의 이더넷 인터페이스를 가질 수 있으며, 이 인터페이스들은 **이더넷 연결 모니터링 절차**를 지원해야 합니다.
2. **절차 관리의 기본 개념**
   * 이 관리 절차는 Metro Ethernet Forum(MEF)에서 정의한 **MEF-CFM** 모듈을 기반으로 설계되었습니다.
   * 현재 사용되는 모듈은 MEF-CFM의 전체 기능 집합이 아닌, 하위 집합(subset)만을 구현합니다.
   * 이 접근 방식은 미래에 MEF-CFM 전체 기능 세트로 확장 가능하도록 설계되었습니다.
3. **지원되는 YANG 모듈**
   * O-RAN 시스템에서 사용되는 YANG 모듈은 IEEE 802.1Q(수정판 802.1ag)에서 정의된 **Loop-back Protocol**의 구성(configuration)과 장애 관리(fault management)를 지원합니다.
   * **o-ran-lbm.yang** 모듈의 일부로, MEF CFM YANG 모듈에서 파생된 데이터 유형의 하위 집합(subset)이 정의됩니다.

**목적**

이 절차는 O-DU의 이더넷 인터페이스 연결 상태를 효율적으로 모니터링하고 관리하기 위한 것입니다.

* **구성 관리**: Loop-back Protocol 설정을 지원하여 이더넷 연결을 효과적으로 제어할 수 있습니다.
* **장애 관리**: 네트워크 연결 중단이나 성능 문제를 감지하고 이를 처리할 수 있도록 설계되었습니다.
* 이 모듈은 확장 가능성이 있어, 이후 필요에 따라 더 많은 기능을 추가할 수 있습니다.

이러한 절차를 통해 O-DU와 O-RU 간의 이더넷 연결 상태를 안정적으로 유지하며, 네트워크 안정성과 가용성을 보장합니다.

</GPT>

An O-DU may have one or more Ethernet interfaces that have to support the Ethernet connectivity monitoring procedure. This section describes the management of this function. The module described here is based on (i.e., a subset of) the mef-cfm module defined by the Metro Ethernet Forum [19]. This is to allow for a later extension of the module to the full feature set of mef-cfm. The YANG module provided below supports the configuration and fault management of the Loop-back Protocol as defined by IEEE 802.1Q (amendment 802.1ag). Derived from MEF CFM YANG, the subset of type definitions is defined as part of the o-ran-lbm.yang.

### 7.6.3 IP connectivity monitoring procedure

#### 7.6.3.1 Monitoring Procedure

<GPT>

O-RU와 O-DU가 IP 기반 연결(특히 C/U plane에 UDP/IP를 사용하는 경우)에서 전송 연결 상태를 확인하는 모니터링 절차에 대해 설명합니다.

**모니터링 절차 (Layer 3 기반)**

1. **IP 기반 연결**
   * O-RU와 O-DU가 IP(특히 UDP/IP)를 통해 연결된 경우, 전송 연결 확인 작업은 \*\*3계층(Layer 3)\*\*에서 수행됩니다.
2. **UDP 에코 서버 기반 검증**
   * 연결 검증은 O-RU가 **UDP 에코 서버** 기능을 지원하는 것을 기반으로 합니다.
   * 이 기능은 **RFC 862**(UDP Echo Protocol)에 정의된 동작을 따릅니다.
3. **UDP 에코 서버 활성화**
   * O-RU에서 UDP 에코 서버를 활성화하려면 **NETCONF 클라이언트**가 이를 제어합니다.
     + NETCONF 클라이언트는 O-RU에서 UDP 에코 서버를 활성화하는 명령을 보냅니다.
     + 이 명령은 O-RU가 \*\*포트 7(Well-Known Port)\*\*에서 UDP 데이터그램을 수신하도록 트리거합니다.
4. **UDP 데이터그램 송수신**
   * O-DU에서 O-RU로 UDP 데이터그램을 전송하면, O-RU는 이를 수신한 뒤, 데이터 내용을 다시 송신자(O-DU)로 되돌려 보냅니다.
   * 송신자가 이 에코 응답을 수신함으로써 두 엔드포인트 간의 UDP/IP 연결 상태를 확인할 수 있습니다.

**목적**

이 절차는 UDP/IP 기반의 연결 상태를 검증하여 O-DU와 O-RU 간의 안정적인 데이터 통신을 보장하기 위한 것입니다.

* **Layer 3 검증**: 네트워크 계층에서 연결 상태를 확인함으로써 물리적 연결뿐만 아니라 논리적 연결의 안정성을 점검합니다.
* **RFC 862 표준 준수**: UDP 에코 프로토콜을 통해 간단하면서도 표준화된 방식으로 연결을 검증할 수 있습니다.
* **NETCONF 활용**: O-RU에서 기능을 제어하고 관리할 수 있는 체계적인 방법을 제공합니다.

이를 통해 연결 문제가 발생할 경우 빠르게 감지하고 적절한 조치를 취할 수 있도록 지원합니다.

</GPT>

If the O-RU and O-DU are connected using IP (and UDP/IP is being used to transport the C/U plane), these transport connectivity verification checks operate at layer 3. Layer 3 connection verification is based on the O-RU supporting the UDP echo server functionality, RFC 862 [18]. The NETCONF client is responsible for enabling the UDP echo server in the O-RU, triggering the O-RU to listen for UDP datagrams on the well-known port 7. When a datagram is received by the O-RU, the data from it is sent back towards the sender, where its receipt can be used to confirm UDP/IP connectivity between the endpoints.

#### 7.6.3.2 Managing IP Connectivity Monitoring Procedure

<GPT>

O-RAN 시스템에서 **UDP 에코 기능**을 관리하고, 이를 통해 O-DU와 O-RU 간의 IP 연결 상태를 모니터링하는 방법을 설명합니다.

**IP 연결 모니터링 관리 절차**

1. **UDP 에코 기능 관리**
   * O-RU의 **UDP 에코 서버** 동작은 **udp-echo YANG 모델**에 정의된 enable-udp-echo 리프(leaf)를 사용하여 NETCONF 클라이언트가 제어합니다.
   * NETCONF 클라이언트는 이를 통해 UDP 에코 서버의 작동을 활성화하거나 비활성화할 수 있습니다.
2. **DSCP 마킹 제어**
   * UDP 에코 응답 데이터그램에 사용되는 **DSCP(Differentiated Services Code Point)** 값을 제어하려면 dscp-config 리프를 설정합니다.
   * 이를 통해 네트워크 품질(QoS) 정책에 따라 데이터 패킷 우선순위를 조정할 수 있습니다.
3. **운영 상태 확인**
   * NETCONF 클라이언트는 echo-replies-transmitted 운영 상태 값을 사용하여 O-RU에서 전송한 UDP 에코 응답 메시지의 수를 확인할 수 있습니다.
   * 이를 통해 에코 기능이 정상적으로 작동하는지 모니터링합니다.
4. **O-DU와 O-RU 간 IP 연결 지원**
   * O-DU는 하나 이상의 IP 인터페이스를 가질 수 있으며, 이 인터페이스들은 UDP/IP 연결 모니터링 절차를 지원해야 합니다.
   * UDP 에코 서버가 활성화된 O-RU는 **유효한 모든 송신 IP 주소**로부터 오는 UDP 데이터그램에 응답할 수 있어야 합니다.

**결론**

이 절차는 O-DU와 O-RU 간 IP 연결 상태를 효과적으로 관리하고, 장애를 빠르게 감지할 수 있도록 설계되었습니다.  
UDP 에코 기능을 기반으로 한 연결 모니터링은 간단하면서도 신뢰성 있는 방법으로, 네트워크 연결의 안정성과 성능을 보장하는 데 중요한 역할을 합니다.

</GPT>

This section describes the management of the UDP echo functionality. The NETCONF client uses the enable-udp-echo leaf in the udp-echo YANG model to control operation of the UDP echo server in the O-RU. The NETCONF client is able to control the DSCP marking used by the O-RU when it echoes back datagrams using the dscp-config leaf. Additionally, the NETCONF client can recover the number of UDP Echo messages sent by the O-RU by using echo-replies-transmitted operational state. An O-DU may have one or more IP interfaces that have to support the UDP/IP connectivity monitoring procedure. An O-RU with its UDP echo server enabled shall be able to respond to UDP datagrams originated from any valid source IP address.

## 7.7 C/U-Plane Delay Management

### 7.7.1 Introduction

<GPT>

\*\*C/U-Plane 지연 관리(C/U-Plane Delay Management)\*\*의 중요성과 이를 관리하기 위한 절차를 설명하고 있습니다.

1.**Intra-PHY 하위 계층 프론트홀 분할의 특성**

* Intra-PHY 계층에서의 프론트홀 분할은 높은 대역폭 요구와 엄격한 지연(latency) 요구 사항을 특징으로 합니다.
* O-DU와 O-RU 간의 물리적 거리가 지연을 초래하며, 이는 전체 시스템 성능에 중요한 영향을 미칩니다.

**2.CUS-Plane 사양의 역할**

* **CUS-Plane 사양**에 따르면, O-DU와 O-RU 간의 \*\*전파 지연(propagation delay)\*\*은 다음과 같은 요소들에 중요한 영향을 미칩니다:
  + **윈도잉(windowing)**: 데이터 수신 시 적절한 시간 창을 설정하여 데이터의 정합성을 유지.
  + **수신 측 버퍼링(receive-side buffering)**: 데이터 손실 방지 및 동기화를 위한 버퍼 관리.
* 전파 지연은 이러한 요소를 최적화하는 데 핵심적인 매개변수로 작용합니다.

3.**지연 관리의 목적**

* O-DU와 O-RU 간의 프론트홀 인터페이스에서 지연을 측정하고 제어하여 시스템 안정성과 성능을 유지합니다.
* 이 섹션에서는 프론트홀 분할의 지연 파라미터를 관리하기 위한 절차를 설명합니다.

**주요 고려사항**

* **엄격한 지연 요구 사항**:
  + Intra-PHY 분할 구조는 시간 동기화와 낮은 지연이 중요한 5G 네트워크에서 필수적입니다.
* **전파 지연 영향**:
  + 지연 시간이 길어질수록 데이터 처리 및 동기화에 추가적인 부담이 발생하며, 이는 네트워크의 전반적인 성능 저하로 이어질 수 있습니다.

**결론**

C/U-Plane 지연 관리는 프론트홀 네트워크의 효율성과 성능을 보장하기 위해 필수적입니다.

* 이 절차를 통해 전파 지연을 측정하고 조정하여, O-DU와 O-RU 간의 통신이 신속하고 정확하게 이루어질 수 있도록 합니다.
* 지연 관리는 네트워크 설계 및 운영 최적화에 핵심적인 역할을 합니다.

</GPT>

### 7.7.2 Delay Parameters

<GPT>

O-RU의 \*\*지연 관리(delay management)\*\*를 위해 정의된 다양한 지연 파라미터를 설명하며, 하향링크(DL)와 상향링크(UL) 데이터 방향에 따른 주요 파라미터와 그 의미를 다룹니다.

**1. 지연 관리의 기준점**

* 지연 관리를 위한 기준점은 **CUS-Plane 사양**의 "지연 요구사항(Latency Requirements)" 및 "O-RU 외부 지연 처리(O-RU External Delay Handling)" 섹션에서 정의됩니다.
* O-RU의 지연 특성은 \*\*O-RU 지연 프로파일(**O-RU delay profile**)\*\*로 나타내며, 이는 서브캐리어 간격(**SCS**) 및 **채널 대역폭** 조합에 따라 달라질 수 있습니다.

**2. 하향링크(DL) 지연 파라미터**

* **T2a\_min**:
  + 프론트홀 인터페이스에서 마지막 데이터 샘플을 수신한 후, 안테나에서 첫 번째 IQ 샘플을 송신하기까지의 최소 O-RU 데이터 처리 지연.
* **T2a\_max**:
  + 데이터 패킷이 수신된 후, 첫 번째 IQ 샘플을 안테나에서 송신하기까지 허용되는 최대 시간.
* **T2a\_max – T2a\_min**:
  + O-RU의 **수신 창(reception window)** 범위를 나타냅니다.
* **T2a\_min\_cp\_dl**:
  + 프론트홀에서 하향링크 실시간 제어 메시지를 수신한 후, 첫 번째 IQ 샘플을 안테나에서 송신하기까지의 최소 지연.
* **T2a\_max\_cp\_dl**:
  + 하향링크 실시간 제어 메시지를 수신한 후 첫 번째 IQ 샘플을 송신하기까지 허용되는 최대 시간.
* **Tcp\_adv\_dl**:
  + 하향링크 실시간 제어 메시지와 해당 IQ 데이터 메시지의 수신 창 간 시간 차이(advance).
* **Tda**:
  + O-RU 안테나 커넥터에서 DL 신호가 출력된 후, 전파로 송신되기까지의 시간 차이.

**3. 상향링크(UL) 지연 파라미터**

* **Ta3\_min**:
  + 안테나에서 IQ 샘플을 수신한 후, 프론트홀 인터페이스로 첫 번째 데이터 샘플을 송신하기까지의 최소 O-RU 데이터 처리 지연.
* **Ta3\_max**:
  + 안테나에서 IQ 샘플을 수신한 후, 프론트홀 인터페이스로 마지막 데이터 샘플을 송신하기까지의 최대 O-RU 데이터 처리 지연.
* **Ta3\_max – Ta3\_min**:
  + O-RU의 **전송 창(transmission window)** 범위를 나타냅니다.
* **T2a\_min\_cp\_ul**:
  + 프론트홀에서 실시간 UL 제어 메시지를 수신한 후, 첫 번째 IQ 샘플을 안테나에서 수신하기까지의 최소 지연.
* **T2a\_max\_cp\_ul**:
  + 실시간 UL 제어 메시지를 수신한 후, 첫 번째 IQ 샘플이 안테나에서 수신되기까지 허용되는 최대 시간.
* **Tau**:
  + 전파를 통해 신호를 수신한 후, O-RU 안테나 커넥터에 UL 신호가 입력되기까지의 시간 차이.

**4. 파라미터 테이블 및 초기화**

* O-RU는 초기 시작 단계에서, 지원하는 서브캐리어 간격(SCS)과 채널 대역폭 조합에 따라 위 파라미터의 **정적으로 정의된 값(pre-defined values)** 테이블을 관리 인터페이스를 통해 제공해야 합니다.

**요약 및 목적**

1. **O-RU 지연 특성 관리**
   * 하향링크 및 상향링크 지연 파라미터를 정의하여, 데이터 송수신 과정에서의 처리 지연과 동기화를 세부적으로 관리할 수 있습니다.
2. **지연 최적화**
   * 지연 파라미터를 기반으로 프론트홀 인터페이스에서 윈도잉(windowing)과 버퍼링(buffering) 동작을 최적화하여 네트워크 성능을 유지합니다.
3. **파라미터 보고**
   * **초기 설정 시 O-RU가 지원하는 지연 특성을 명확히 제공함**으로써, O-DU와의 협력 및 동기화를 강화합니다.

</GPT>

### 7.7.3 Reception Window Monitoring

<GPT>

\*\*O-RU가 프론트홀 인터페이스에서 수신 창(reception window)\*\*의 동작을 모니터링해야 한다는 내용을 설명하고 있습니다.

**수신 창 모니터링(Operation of Reception Window)**

**1. 모니터링 개요**

* **O-RU는 프론트홀 인터페이스를 통해 수신되는 패킷의 도착 시점을 모니터링**해야 합니다.
  + 이 도착 시점은 수신 창의 허용 범위 내에 있어야 합니다.
  + 수신 창의 허용 범위는 다음 값들로 정의됩니다:
    - **T2a\_min**: 패킷이 도착 가능한 **최소 허용 시간**.
    - **T2a\_max**: 패킷이 도착 가능한 **최대 허용 시간**.

**2. 지연 관리의 중요성**

* O-RU가 수신 창의 동작을 모니터링하는 이유:
  + 수신 창의 외부에서 도착하는 패킷은 데이터 처리를 방해할 수 있음.
  + 지연 관리를 통해 **정확한 데이터 동기화**를 보장하고 네트워크의 성능을 유지.

**3. 부속서 B.3 참조**

* \*\*부속서 B.3(Annex B.3)\*\*에서 \*\*수신 창 카운터(reception window counters)\*\*와 관련된 추가 정보가 제공됩니다.
  + 카운터를 통해 수신 창 내외로 도착하는 패킷의 수를 기록하고 이를 기반으로 네트워크 상태를 분석.

**요약**

* **O-RU는 T2a\_min과 T2a\_max로 정의된 수신 창 내에서만 패킷을 수신해야 함**.
* 수신 창 모니터링을 통해 패킷 도착 시간의 허용 여부를 확인하고, 네트워크 성능 및 안정성을 유지.
* 자세한 카운터 동작 및 분석 방법은 부속서 B.3에서 제공됨.

</GPT>

### 7.7.4 External Antenna Delay Control

<GPT>

외부 안테나 지연 제어 (External Antenna Delay Control)\*\*는 O-RU에서 외부 안테나의 지연을 관리 및 제어할 수 있는 기능을 설명합니다.

**외부 안테나 지연 제어 기능 개요**

1. **옵션 지원**:
   * O-RU는 **외부 안테나 지연 제어(EXTERNAL ANTENNA DELAY CONTROL)** 기능을 지원할 수 있습니다.
   * 이 기능을 지원하는 O-RU는 **o-ran-wg4-features YANG 모델**에서 이를 나타냅니다.
2. **기능 표시**:
   * O-RU는 **o-ran-module-cap YANG 모델**의 ext-ant-delay-capability 스키마 노드를 사용하여, O-RU 컨트롤러에 지원하는 외부 지연 구성의 유형을 알립니다.

**외부 지연 구성 유형**

외부 안테나 지연 제어에서 지원되는 구성 유형은 다음과 같습니다:

1. **PER-O-RU**:
   * O-RU는 **모든** **송신 배열(tx-array carriers)** 및 \*\*수신 배열(rx-array carriers)\*\*에서 단일 값의 지연 보정(offset)만 지원합니다.
   * 이 경우, t-da-offset(송신 지연 보정) 및 t-au-offset(수신 지연 보정)의 값이 O-RU 전반에 걸쳐 동일하게 적용됩니다.
2. **PER-ARRAY**:
   * O-RU는 **개별** **송신 배열(tx-arrays)** 및 \*\*수신 배열(rx-arrays)\*\*에 대해 서로 다른 값을 지원합니다.
   * 각각의 배열에 따라 \*\*t-da-offset\*\*과 **t-au-offset** 값을 독립적으로 설정할 수 있습니다.
3. **PER-ARRAY-CARRIER**:
   * O-RU는 **개별** **송신 배열의 캐리어(tx-array carriers)** 및 \*\*수신 배열의 캐리어(rx-array carriers)\*\*에 대해 서로 다른 값을 지원합니다.
   * 가장 세분화된 제어 방식으로, 각각의 배열 캐리어 단위로 \*\*t-da-offset\*\*과 \*\*t-au-offset\*\*을 독립적으로 설정할 수 있습니다.

**적용 목적**

* **외부 안테나 지연 보정**은 송신 및 수신 경로에서 발생하는 시간 지연을 조정하여 네트워크 동기화 및 성능을 최적화하는 데 사용됩니다.
* 다양한 **구성 옵션**을 통해 네트워크 설계 요구 사항에 맞춰 유연하게 대응할 수 있습니다.

**요약**

* 외부 안테나 지연 제어는 O-RU가 지원 여부를 나타내고, 지원 수준에 따라 **PER-O-RU**, **PER-ARRAY**, **PER-ARRAY-CARRIER**로 세분화됩니다.
* 이 기능은 네트워크의 지연 조정 및 동기화 품질을 개선하는 데 핵심적인 역할을 합니다.

</GPT>

## 7.8 O-RU Adaptive Delay Capability

<GPT>

\*\*7.8 O-RU 적응형 지연 기능 (O-RU Adaptive Delay Capability)\*\*은 O-RU가 O-DU의 구성 정보와 전송 네트워크의 지연 정보를 기반으로 \*\*버퍼를 최적화(adaptive buffer optimization)\*\*할 수 있는 기능을 설명합니다.

**적응형 지연 기능 개요**

1. **기능 지원 여부 표시**:
   * **O-RU가 적응형 타이밍 기능을 지원**하는 경우, NETCONF 기능 교환을 통해 **ADAPTIVE-O-RU-PROFILE** 지원 여부를 O-RU Controller 클라이언트에 알립니다.
   * 자세한 내용은 **9.2절 및 Annex C**를 참조.
2. **O-DU와 네트워크의 지연 정보 제공**:
   * O-RU Controller는 O-RU에 O-DU 지연 프로필 및 전송 네트워크 지연 파라미터를 제공합니다.
   * 이를 통해 O-RU는 버퍼를 최적화하고 지연 제약 조건을 충족할 수 있습니다.

**O-DU 지연 프로필 구성 요소**

O-RU Controller가 제공하는 O-DU 지연 프로필은 다음과 같은 파라미터를 포함합니다:

1. **T1a\_max\_up**:
   * O-DU가 **IQ 데이터 메시지**를 안테나에서 IQ 샘플이 전송되기 전에 보낼 수 있는 가장 이른 시간.
2. **TXmax**:
   * **O-DU가 심볼에 대한 모든 다운링크 user plane IQ 데이터 메시지를 전송**하는 데 필요한 최대 시간.
3. **Ta4\_max**:
   * O-DU가 **업링크 user plane IQ 데이터 메시지의 마지막 메시지**를 수신할 수 있는 가장 늦은 시간.
4. **RXmax**:
   * **O-DU가 동일한 심볼에 대한 첫 번째와 마지막 user plane IQ 데이터 메시지를 수신**하는 데 허용되는 최대 시간 차이.
5. **T1a\_max\_cp\_dl**:
   * O-DU가 **다운링크 실시간 제어 메시지**를 안테나에서 IQ 샘플이 전송되기 전에 보낼 수 있는 가장 이른 시간.

**전송 네트워크 타이밍 파라미터**

O-RU Controller는 O-RU에 다음 전송 네트워크 타이밍 파라미터를 제공합니다:

1. **T12\_min**:
   * **O-DU와 O-RU 처리 요소** 사이에서 발생하는 최소 지연.
2. **T12\_max**:
   * **O-DU와 O-RU 처리 요소** 사이에서 발생하는 최대 지연.
3. **T34\_min**:
   * **O-RU와 O-DU 처리 요소** 사이에서 발생하는 최소 지연.
4. **T34\_max**:
   * **O-RU와 O-DU 처리 요소** 사이에서 발생하는 최대 지연.

**참고:**

* O-RU Controller는 **외부 지연이 없는 상태**(Tau = 0, Tda = 0)를 가정하여 T12\_max 및 T34\_max 값을 구성해야 합니다.

**적응형 프로파일 구성 절차**

1. **O-RU의 시작 시**:
   * O-RU Controller는 적응형 지연 구성 정보를 제공.
   * 이 정보는 O-RU가 \*\*지연 프로파일을 조정(adapt)\*\*하는 데 사용됩니다.
2. **캐리어 작동 중일 때**:
   * O-RU가 **적응형 지연 구성 정보를 수신**하더라도, 현재 작동 중인 캐리어가 모두 비활성화될 때까지 프로파일을 변경하지 않습니다.
3. **프로파일 업데이트 후**:
   * O-RU가 새로운 지연 프로파일로 적응한 후, NETCONF 클라이언트에 지연 파라미터를 신호로 제공합니다.

**주요 목적**

* **O-DU 지연 프로필**과 **전송 네트워크 지연 정보**를 활용하여 O-RU의 버퍼를 최적화.
* 지연 제약 조건(Annex B의 불평등식)을 준수하며 네트워크 성능을 유지.

**요약**

O-RU 적응형 지연 기능은 네트워크의 지연 정보를 활용하여 O-RU가 **동적으로 버퍼를 최적화**할 수 있도록 지원하는 선택적 기능입니다. 이는 네트워크 동기화 및 성능 최적화에 기여하며, 적응형 프로파일은 캐리어 작동 상태와 관계없이 안전하게 업데이트됩니다.

</GPT>

## 7.9 Measuring transport delay parameters

<GPT>

\*\*7.9 전송 지연 파라미터 측정 (Measuring Transport Delay Parameters)\*\*은 O-RU가 O-DU와 O-RU 간의 전송 지연을 측정하는 기능을 설명합니다.

**eCPRI 기반 전송 지연 측정 지원**

1. **기능 지원 여부**:
   * O-RU는 **eCPRI(evolved Common Public Radio Interface)** 기반으로 전송 지연 측정을 지원할 수 있으며, 이 경우 해당 기능을 명시적으로 알립니다.
   * O-RU가 전송 지연 측정을 지원한다면, \*\*CUS-Plane Specification [2]\*\*에서 정의된 프로토콜을 구현해야 합니다.
2. **전송 지연 측정 수행 조건**:
   * O-RU는 \*\*7.5절에서 설명된 대로 구성된 처리 요소(processing element)\*\*에 대해 전송 지연 측정을 수행할 수 있어야 합니다.

**O-RU의 기능 및 요구 사항**

1. **메시지 처리 및 응답**:
   * O-RU는 구성된 각 처리 요소에 대해 **수신한 메시지에 응답**할 수 있어야 합니다.
   * O-RU는 요청 메시지, 응답 메시지, 후속 메시지에 대해 각각 기록을 유지해야 합니다.
2. **기록 유지**:
   * O-RU는 자신이 전송한 **응답, 요청, 후속 메시지**의 개수를 기록으로 관리해야 합니다.

**주요 목적**

* **전송 지연 측정 데이터의 정확성 보장**: eCPRI 기반 측정을 통해 O-DU와 O-RU 간 전송 지연을 평가.
* **효율적인 전송 지연 관리**: 처리 요소별 메시지 응답 및 기록을 통해 네트워크 상태를 모니터링하고 최적화.

**요약**

O-RU가 전송 지연 측정을 지원할 경우, **eCPRI 프로토콜**을 따라야 하며, 요청 및 응답 메시지를 처리하는 동시에 이러한 메시지의 기록을 유지해야 합니다.

</GPT>

## 7.10 O-RU Monitoring of C/U Plane Connectivity

<GPT>

**7.10 O-RU의 C/U Plane 연결 모니터링**은 O-RU가 C/U Plane 연결 상태를 모니터링하고 연결 실패 시 경고를 발생시키는 방법을 설명합니다.

**C/U Plane 연결 모니터링 기능**

1. **O-RU의 책임**:
   * O-RU는 **C/U Plane 연결 상태를 모니터링**하며, 처리 요소(processing-element)와 연결된 논리적 C/U Plane 연결이 실패할 경우 경고(alarm)를 발생시켜야 합니다.
2. **타이머 기반 모니터링**:
   * O-RU는 각 처리 요소별로 \*\*타이머(timer)\*\*를 사용하여 C/U Plane 연결을 감시합니다.
   * **타이머 작동 조건**:
     + 처리 요소에 연결된 최소 하나의 array-carrier가 \*\*활성 상태(active state)\*\*여야 타이머가 작동합니다.
     + 특정 처리 요소와 연결된 C/U Plane 데이터 흐름이 수신될 때마다 타이머는 \*\*초기화(reset)\*\*됩니다.

**타이머 설정 및 기본값**

1. **타이머 기본값**:
   * O-RU는 기본적으로 **160ms**를 타이머 값으로 사용하여 C/U Plane 연결을 모니터링합니다.
   * 이는 O-RU가 PHY 및 C/U Plane 구성에 따라 메시지 전송 최소 빈도를 독립적으로 결정할 수 없기 때문입니다.
2. **타이머 값 조정**:
   * O-RU는 **o-ran-supervision.yang** 모델의 cu-plane-monitoring **컨테이너**를 통해 타이머 값을 조정할 수 있음을 나타낼 수 있습니다.
   * NETCONF 클라이언트를 사용하여 타이머 값을 **재구성**하거나, **C/U Plane 모니터링 기능을 비활성화**할 수 있습니다.

**중요 사항 및 권장사항**

* **타이머 초기 비활성화 권장**:
  + O-DU가 C/U Plane 데이터 흐름 전송을 시작하는 데 시간이 걸릴 경우, 초기 타이머 값(기본 160ms)을 초과하여 O-RU가 잘못된 경고를 발생시킬 수 있습니다.
  + 이를 방지하기 위해, **NETCONF 클라이언트**는 캐리어 활성화 전에 타이머 작동을 일시적으로 비활성화(disable)하는 것이 좋습니다.
  + C/U Plane 데이터 흐름이 시작된 후 타이머를 **필요한 값으로 재설정**하여 C/U Plane 연결 모니터링을 활성화할 수 있습니다.

**요약**

* O-RU는 타이머를 사용하여 C/U Plane 연결 상태를 감시하고, 연결 실패 시 경고를 발생시킵니다.
* 기본 타이머 값은 160ms로 설정되지만, NETCONF 클라이언트를 통해 조정 및 비활성화가 가능합니다.
* O-DU의 초기 데이터 흐름 지연으로 인한 잘못된 경고를 방지하려면 타이머를 초기 비활성화한 후 데이터 흐름이 시작되면 다시 활성화하는 방식이 권장됩니다.

</GPT>

## 7.11 Bandwidth Management

<GPT>

\*\*7.11 대역폭 관리 (Bandwidth Management)\*\*에서는 O-RU가 지원 가능한 최대 비트 전송 속도와 물리적 인터페이스 그룹을 기반으로 대역폭 관리를 수행하는 방법을 설명합니다.

**O-RU의 대역폭 관리 기능**

1. **최대 지원 비트 전송 속도(nominal bitrate)**:
   * O-RU는 특정 물리적 포트와 연결된 인터페이스에서 지원할 수 있는 \*\*최대 비트 전송 속도(nominal bitrate)\*\*를 나타낼 수 있습니다.
   * 이를 위해 **o-ran-transceiver YANG 모듈**의 nominal-bitrate 노드를 사용합니다.
2. **지속 가능한 비트 전송 속도(sustainable bitrate)**:
   * O-RU가 지원 가능한 지속 가능한 비트 전송 속도가 모든 물리적 포트의 **최대 비트 전송 속도 합산치보다 낮은 경우**:
     + O-RU는 **o-ran-interfaces YANG 모델**의 interface-grouping 컨테이너를 사용하여 \*\*인터페이스 그룹(interface-group-id)\*\*과 연관된 최대 지속 가능한 속도를 정의할 수 있습니다.
     + 이 인터페이스 그룹은 하나 이상의 물리적 인터페이스로 구성될 수 있습니다.
3. **인터페이스 그룹 구성**:
   * 동일한 YANG 모델(o-ran-interfaces)은 **ietf-interfaces**의 interface list를 확장하여 각 인터페이스가 속한 interface-group-id를 지정할 수 있습니다.

**중요 사항**

* **최대 지속 가능한 대역폭(sustainable bandwidth)**:
  + 이는 **하나의 무선 프레임 단위**로 계산됩니다.
  + **단기적인 기간(하나의 무선 프레임보다 짧은 시간)** 동안에는 **최대 대역폭을 초과**할 수 있지만, 지속 가능한 비트 전송 속도를 초과하지 않도록 관리됩니다.

**요약**

* O-RU는 물리적 인터페이스에서 지원 가능한 최대 비트 전송 속도를 YANG 모듈을 통해 정의할 수 있습니다.
* 지속 가능한 비트 전송 속도가 낮을 경우, 인터페이스 그룹을 구성하고 그룹 단위로 대역폭 제한을 정의할 수 있습니다.
* 대역폭 관리는 평균적으로 **무선 프레임 단위**에서 지속 가능한 속도를 유지하도록 설계되어 있습니다.

</GPT>

# 8 Software Management - TODO

# 9 Configuration Management

## 9.1 Baseline configuration

### 9.1.1 NETCONF Operatins

<GPT>

NETCONF(Network Configuration Protocol)은 네트워크 장치 구성 및 관리에 사용되는 표준 프로토콜입니다. NETCONF의 **운영(Operation)** 중 **Configuration Management(CM)** 관련 작업에 대해 설명하고 있습니다.

**NETCONF Standard Operations**

NETCONF는 네트워크 장치의 설정을 \*\*변경(Modify)\*\*하거나 \*\*검색(Retrieve)\*\*하기 위해 표준 작업을 제공합니다.  
예시로 아래 작업들이 포함됩니다:

1. **edit-config**: YANG 모델에 정의된 파라미터 값을 수정.
2. **get-config**: 특정 데이터스토어에서 구성 값을 가져옴.
3. **get**: 장치의 현재 상태 정보를 가져옴.

**Configuration Management(CM) 시나리오**

CM(구성 관리) 작업에서는 두 가지 주요 시나리오가 존재합니다:

**1. 2-Phase Operation (Modify/Commit):**

* **Running datastore**를 직접 수정합니다.
* 두 단계로 구성:
  1. **Modify**: edit-config 명령을 통해 설정 변경.
  2. **Commit**: 변경 내용을 장치에 영구 적용.
* **확인(Confirm)** 단계가 없습니다.
* 모든 O-RU(오픈 라디오 유닛)는 이 방식을 **필수적으로 지원**해야 합니다.

**2. 3-Phase Operation (Modify/Commit/Confirm):**

* **Candidate datastore**를 사용하여 변경 사항을 임시로 적용한 후, 확인 단계를 추가합니다.
* 세 단계로 구성:
  1. **Modify**: edit-config 명령으로 임시 데이터스토어(Candidate datastore)에 변경 적용.
  2. **Commit**: 변경 내용을 확정.
  3. **Confirm**: 설정이 의도대로 작동하는지 확인.
     + 설정이 유효하지 않으면 롤백 가능.
* **3단계 방식은 선택 사항**으로, O-RU가 지원할 필요는 없습니다.

**Running Datastore와 Candidate Datastore**

* **Running datastore**:
  + NETCONF의 주요 데이터 저장소.
  + 실행 중인 시스템에서 현재 사용되는 구성 정보를 저장.
  + 2-Phase Operation에서 직접 수정.
* **Candidate datastore**:
  + 임시로 수정 작업을 수행할 수 있는 저장소.
  + 설정을 검증한 뒤 Running datastore로 적용.
  + 3-Phase Operation에서 사용.

2-Phase vs. 3-Phase 비교

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

**YANG 모델과 연관성**

* YANG은 네트워크 장치의 데이터 및 동작을 모델링하기 위한 언어입니다.
* 위 예제에서는 **o-ran-hardware**라는 YANG 모듈이 사용되었습니다.
  + NETCONF 작업은 이 YANG 모듈의 매개변수를 수정하거나 검색하는 데 사용됩니다.

**결론**

NETCONF를 사용한 구성 관리에서:

1. **2-Phase Operation**은 간단하고 필수적으로 지원됩니다.
2. **3-Phase Operation**은 안정성을 높이지만 선택 사항입니다.

이는 네트워크 장치의 설정 변경 중 오류를 방지하거나 안정성을 높이기 위한 방법론적 차이를 나타냅니다.

</GPT>

### 9.1.2 Retrieve State

<GPT>

NETCONF 프로토콜을 사용하여 **O-RU Controller**가 \*\*O-RU의 상태 정보를 검색(Retrieve)\*\*하는 작업 과정을 나타냅니다. 이 작업은 NETCONF의 <get> 명령을 사용하여 수행되며, YANG 모델에서 정의된 상태 정보(예: o-ran-hardware의 특정 상태)를 가져옵니다.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

**작업 과정 설명**

1. **Preconditions (사전 조건)**:
   * O-RU Controller와 O-RU 간에 NETCONF 연결이 이미 설정되었습니다.
   * NETCONF 연결 설정 과정에서 두 장치는 각자의 \*\*NETCONF 기능(Capabilities)\*\*을 교환하였습니다.
     + 예: 지원하는 데이터스토어, YANG 모델 등.
2. **작업 흐름**:
   * **[1단계: 요청]**
     + O-RU Controller는 <get> RPC 호출을 사용하여 O-RU로 상태 데이터를 요청합니다.
     + 요청 형식: <get><source><running/></source><filter>...</filter></get>
       - **<source><running/>**: 요청 데이터의 출처가 running datastore임을 지정.
       - **<filter>**: 검색하고자 하는 상태 정보의 범위나 필터를 설정.
   * **[2단계: 응답]**
     + O-RU는 요청받은 필터에 해당하는 상태 데이터를 NETCONF <rpc-reply> 메시지로 반환합니다.
     + 응답 데이터는 YANG 모델에 정의된 포맷에 맞춰 제공됩니다.
3. **Postconditions (결과 조건)**:
   * O-RU Controller는 요청한 상태 정보를 성공적으로 검색하여 사용할 수 있습니다.

**상황 예시**

* O-RU Controller가 O-RU의 하드웨어 상태(예: 온도, 전원 상태)를 모니터링하기 위해 <get> 명령을 실행.
* 예시 RPC 요청:  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명
* O-RU 응답 예시:  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명

<GPT>

### 9.1.3 Modify State

<GPT>

**O-RU Controller**가 NETCONF의 <edit-config> 명령을 사용하여 \*\*O-RU의 상태를 변경(Modify)\*\*하는 작업 과정을 보여줍니다. 이 작업은 O-RU를 리셋하지 않고 수행되며, 예시로 YANG 모델에서 정의된 \*\*admin-state\*\*와 \*\*power-state\*\*를 변경할 수 있습니다.

**작업 과정 설명**

1. **작업 시나리오**
   * O-RU Controller는 O-RU의 구성 가능한 상태(예: admin-state 및 power-state)를 변경합니다.
   * NETCONF <edit-config> 프로시저를 사용하여 Running datastore에 직접 변경 사항을 적용합니다.
2. **구성 가능한 상태 예시**
   * **admin-state**: 관리 상태를 나타내며, 활성화 또는 비활성화 상태 설정 가능.
   * **power-state**: 전원 상태 설정 가능(예: 켜짐, 꺼짐).
3. **작업 흐름**
   * **[1단계: 요청]**
     + O-RU Controller는 **<edit-config>** 명령을 사용하여 O-RU의 Running datastore에 상태 변경 요청을 보냅니다.
     + 요청 형식:  
       텍스트, 스크린샷, 폰트이(가) 표시된 사진

       자동 생성된 설명
   * **[2단계: 성공 응답]**
     + O-RU는 상태 변경에 성공하면 <rpc-reply> 메시지로 <OK>를 반환합니다.
   * **[3단계: 실패 응답]**
     + 상태 변경이 실패하면 **<rpc-error>** 메시지를 반환하며, RFC6241 Appendix A에서 정의된 에러 코드와 함께 응답합니다.
4. **에러 처리**
   * 에러 발생 시:
     + **RFC6241 Appendix A**에 정의된 표준 에러 코드를 반환합니다.  
       예: **invalid-value**, **operation-failed** 등.
     + 벤더는 에러 발생 시의 동작(예: 롤백, 경고 메시지 출력)을 정의할 수 있습니다.

**O-RU Controller와 O-RU 간 작업 흐름**

1. O-RU Controller가 <edit-config>를 통해 상태 변경 요청을 전송합니다.
2. O-RU가 요청을 처리:
   * 성공 시 <rpc-reply>로 <OK>를 반환.
   * 실패 시 <rpc-error>와 함께 에러 코드 반환.
3. 작업 결과에 따라 O-RU Controller는 후속 작업을 수행합니다.

**중요 사항**

1. **상태 변경 가능 여부**:
   * 상태 변경은 YANG 모델에서 \*\*구성 가능(Configurational)\*\*한 항목에만 적용됩니다.
   * 예: admin-state, power-state.
2. **에러 처리 정책**:
   * NETCONF는 에러가 발생한 경우 명확한 에러 코드와 함께 응답하도록 설계되었습니다.
   * 벤더마다 에러 발생 시의 동작(예: 롤백, 경고 메시지 표시)을 다르게 정의할 수 있습니다.
3. **O-RU 리셋 없이 상태 변경**:
   * 이 작업은 O-RU를 리셋하지 않고도 상태 변경이 가능하다는 점에서 효율적입니다.

**활용 예시**

* 네트워크 유지보수 중 특정 O-RU의 admin-state를 "disabled"로 설정하여 유지보수 모드로 전환.
* O-RU의 power-state를 "off"로 설정하여 전력 소비를 줄임.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

**admin-state**는 \*\*O-RU의 관리 상태를 나타내는 상태(machine state)\*\*로, 각 상태는 O-RU의 자원 활성화 및 비활성화 조건을 정의합니다. 아래는 각 상태와 상태 전이에 대한 설명입니다.

**admin-state의 상태 정의**

1. **locked**:
   * 이 상태에서는 O-RU의 모든 자원이 비활성화됩니다.
   * **자원 활성화가 금지**됩니다.
   * 관리자가 명시적으로 모든 자원을 비활성화한 상태입니다.
   * 예: 네트워크 유지보수를 위해 O-RU를 잠금 상태로 전환.
2. **shutting-down** (선택 사항, 필수 아님):
   * 이 상태에서는 현재 사용 중인 자원은 유지되지만, 새로운 자원 사용이 **제한**됩니다.
   * 예: O-RU를 점진적으로 비활성화하려는 중간 상태.
3. **unlocked**:
   * 이 상태에서는 모든 자원이 활성화될 수 있습니다.
   * **자원 활성화가 허용**됩니다.
   * O-RU가 초기화(reset)된 후 기본 상태로 설정됩니다.

**상태 전이 다이어그램**

O-RU의 상태 전이(transition)는 아래와 같이 동작합니다:

* **locked → unlocked**:
  + 관리자가 O-RU를 활성화하여 모든 자원 사용을 허용.
* **unlocked → locked**:
  + 관리자가 O-RU를 비활성화하여 모든 자원을 비활성화.
* **unlocked → shutting-down** (선택 사항):
  + 관리자가 점진적으로 자원을 비활성화하거나 제한하려는 경우.
* **shutting-down → locked**:
  + shutting-down 상태에서 모든 자원을 완전히 비활성화.
* **reset 후 상태**:
  + O-RU가 초기화되면 기본적으로 **unlocked** 상태로 설정.

**상태 전환 사용 예시**

1. **네트워크 유지보수**:
   * O-RU를 locked 상태로 전환하여 자원을 비활성화하고 유지보수 작업 수행.
2. **시스템 초기화 후 기본 상태**:
   * O-RU가 재부팅되거나 초기화되면 unlocked 상태로 전환하여 자원을 활성화 가능.
3. **점진적 비활성화** (선택 사항):
   * O-RU의 특정 자원만 제한적으로 비활성화하려면 shutting-down 상태 사용.

**상태 관리의 중요성**

* O-RU의 상태 전이는 **운영 안정성**과 **네트워크 관리 효율성**을 보장하는 데 중요한 역할을 합니다.
* 관리자는 적절한 상태 전이를 통해 네트워크 성능을 유지하고 장애를 방지할 수 있습니다.

텍스트, 폰트, 라인, 스크린샷이(가) 표시된 사진

자동 생성된 설명

위 그림은 **O-RU Admin State**의 상태 전이 다이어그램을 나타냅니다. 이 다이어그램은 O-RU의 admin-state가 NETCONF의 <edit-config> 명령을 통해 어떻게 전이되는지 보여줍니다.

**다이어그램에 나타난 상태 전이**

1. **unlocked → shutting-down**
   * <edit-config> 명령을 사용하여 admin-state를 shutting-down으로 변경.
   * 이 상태에서는 제한적으로 자원을 사용하거나 점진적으로 비활성화 가능.
2. **shutting-down → locked**
   * <edit-config> 명령을 통해 shutting-down 상태에서 locked로 변경.
   * 이 상태에서는 모든 자원이 비활성화되고 자원 사용이 금지.
3. **unlocked → locked**
   * shutting-down 단계를 거치지 않고 unlocked에서 직접 locked 상태로 전환 가능.
   * 네트워크나 자원을 즉시 비활성화해야 하는 경우 사용.
4. **locked → unlocked**
   * <edit-config> 명령을 통해 locked 상태에서 다시 unlocked로 변경.
   * 모든 자원이 활성화 가능하며, O-RU의 정상 작동 상태로 돌아감.
5. **shutting-down → unlocked**
   * <edit-config> 명령으로 shutting-down 상태에서 unlocked로 복구.
   * 제한적으로 비활성화된 자원을 다시 활성화 가능.

**상태 전이 명령 사용 예시**

* O-RU 관리자는 **NETCONF <edit-config>** 명령을 사용하여 아래와 같은 XML 요청으로 상태를 전환할 수 있습니다:
* 상태 변경 요청 예시 (unlocked → locked):  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명
* 응답 예시:
  + 성공 시:  
    텍스트, 스크린샷, 폰트이(가) 표시된 사진

    자동 생성된 설명
  + 실패 시:  
    텍스트, 스크린샷, 폰트이(가) 표시된 사진

    자동 생성된 설명

**핵심 요약**

* admin-state는 **unlocked**, **shutting-down**, **locked**의 세 가지 상태로 구성.
* 상태 전이는 **NETCONF <edit-config>** 명령을 통해 수행.
* **unlocked**는 초기화 후 기본 상태이며, 네트워크 및 자원이 활성화 가능.
* **locked**는 모든 자원을 비활성화하여 사용을 제한.
* **shutting-down**은 선택 사항이며 점진적인 자원 비활성화를 지원.

이 상태 전이 관리는 O-RU의 운영 상태를 효율적으로 관리하고 제어하는 데 필수적입니다.

**power-state 상태 및 전이 설명**

power-state는 O-RU의 전원 관리 상태를 나타내며, 에너지 절약 모드와 일반 작동 모드 간의 전이를 관리합니다. 아래는 각 상태 및 상태 전이에 대한 설명입니다.

텍스트, 폰트, 스크린샷, 원이(가) 표시된 사진

자동 생성된 설명

**power-state 상태 정의**

1. **awake**:
   * O-RU가 정상적으로 작동 중임을 나타냅니다.
   * **에너지 절약 모드가 비활성화**된 상태.
   * 이 상태는 **O-RU가 초기화(reset)된 후 기본 상태**로 설정됩니다.
   * 예: 네트워크 트래픽이 많거나 시스템이 최대 성능을 발휘해야 할 때.
2. **sleeping** (선택 사항):
   * O-RU가 **에너지 절약 모드**에 진입했음을 나타냅니다.
   * M-Plane 연결 및 일부 기본 관리 기능은 유지되지만, **C/U/S Plane 기능은 중단**될 수 있습니다.
   * 전력 소비를 줄이기 위해 사용.
   * 예: 네트워크 트래픽이 적거나 비활성 시간 동안.

**상태 전이 다이어그램**

* 상태 전이는 아래와 같이 **energy-saving-enabled** 파라미터를 수정하여 수행됩니다:
  1. **awake → sleeping**:
     + energy-saving-enabled 파라미터를 활성화(true)하여 O-RU를 에너지 절약 모드로 전환.
  2. **sleeping → awake**:
     + energy-saving-enabled 파라미터를 비활성화(false)하여 O-RU를 일반 모드로 복구.

**상태 전환 명령 사용 예시**

* O-RU 관리자는 **NETCONF <edit-config>** 명령을 사용하여 아래와 같은 XML 요청으로 상태를 전환할 수 있습니다.
* 상태 변경 요청 예시 (awake → sleeping):  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명
* 응답 예시:
  + **성공 시**:  
    텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

    자동 생성된 설명
  + **실패 시**:  
    텍스트, 스크린샷, 폰트이(가) 표시된 사진

    자동 생성된 설명

**oper-state 상태 및 전이 설명**

oper-state는 O-RU의 동작 상태(operational state)를 나타내며, O-RU가 운영 가능한 상태인지, 아니면 비활성 상태인지 관리합니다. 이 상태는 NETCONF의 \*\***reset RPC**(Remote Procedure Call)\*\*를 통해 제어됩니다.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

**oper-state 상태 정의**

1. **enabled**:
   * O-RU가 부분적으로 또는 완전히 운영 중임을 나타냅니다.
   * 네트워크 트래픽 처리가 가능하며 모든 주요 기능이 활성화된 상태.
2. **disabled**:
   * O-RU가 비활성 상태이며 운영 불가능.
   * **reset** 후 기본 상태로 설정됩니다.

**상태 전이 특성**

1. **초기 상태**:
   * O-RU가 **reset** 명령을 수신하면, 이전 상태에 관계없이 disabled 상태로 시작합니다.
2. **전이 가능성**:
   * disabled 또는 enabled 상태 모두에서 **reset RPC**를 실행할 수 있습니다.

**상태 전환 다이어그램**

* reset 명령을 통해 상태가 초기화되고, O-RU는 disabled 상태로 시작합니다.
* 이후, 내부 로직이나 별도의 NETCONF 명령을 통해 enabled 상태로 전환될 수 있습니다.

**상태 전환 명령 사용 예시**

* O-RU 관리자는 **NETCONF <rpc>** 명령을 사용하여 O-RU의 상태를 재설정할 수 있습니다.
* 상태 변경 요청 예시 (reset 실행):  
  텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

  자동 생성된 설명
* 응답 예시:
  + **성공 시**:  
    텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

    자동 생성된 설명
  + O-RU 초기화 후:  
    O-RU는 자동으로 oper-state를 **disabled**로 설정.

**상태 전이 다이어그램**

아래 다이어그램은 oper-state의 전이 과정을 설명합니다:

1. **enabled → reset → disabled**:
   * O-RU가 활성 상태에서 reset 명령을 수신하면 disabled로 전환.
2. **disabled → reset → disabled**:
   * 이미 비활성 상태여도 reset 명령 실행 가능하며, 초기 상태를 유지.

텍스트, 폰트, 스크린샷, 원이(가) 표시된 사진

자동 생성된 설명

**핵심 요약**

* **enabled**:
  + O-RU가 운영 가능하며 네트워크 트래픽 처리가 가능한 상태.
* **disabled**:
  + O-RU가 비활성화된 상태로, **reset** 후 기본 상태.
* O-RU의 동작 상태는 **NETCONF reset RPC**로 초기화 가능.

**availability-state 상태 및 전이 설명**

availability-state는 O-RU의 가용성 상태를 나타내며, O-RU의 작동 가능 여부와 신뢰성 상태를 정의합니다. 이 상태는 **내부적으로 감지된 결함**과 그 결함이 O-RU의 작동에 미치는 영향을 기반으로 결정됩니다.

**availability-state 상태 정의**

1. **normal**:
   * O-RU에 **결함이 없으며** 정상적으로 작동 가능.
   * 모든 서비스와 기능이 정상적으로 수행되는 상태.
2. **degraded**:
   * **주요 또는 치명적인 결함이 활성화된 경우**, O-RU의 일부 구성 요소 또는 모듈에 영향을 미침.
     + 예: 송신기(transmitter) 또는 다른 하위 구성 요소에 오류 발생.
   * O-RU는 제한된 용량이나 기능으로 작동 가능.
3. **faulty**:
   * O-RU 전체에 영향을 미치는 **치명적인 결함이 활성화된 경우**.
   * O-RU는 더 이상 서비스를 제공할 수 없는 상태.

**상태 전이 다이어그램**

1. **normal → degraded**:
   * 주요 또는 치명적인 하위 구성 요소 결함이 발생하여 작동 상태가 일부 저하됨.
2. **degraded → faulty**:
   * 전체 시스템에 치명적인 영향을 미치는 결함이 발생하여 O-RU가 더 이상 작동 불가.
3. **faulty → degraded**:
   * 치명적인 결함이 복구되었지만 일부 주요 결함은 여전히 남아 있을 때.
4. **degraded → normal**:
   * 모든 주요 결함이 복구되었을 때 O-RU는 정상 상태로 복구.

텍스트, 폰트, 원, 스크린샷이(가) 표시된 사진

자동 생성된 설명

**상태 결정 요인**

* **내부 감지된 결함**:
  + 하드웨어 또는 소프트웨어 결함의 감지.
  + 예: 송신기 오류, 전원 문제 등.
* **외부 요인 제외**:
  + O-RU의 가용성 상태는 외부 네트워크 조건이나 외부 환경적 오류에 의해 영향을 받지 않음.

**운영 중 고려 사항**

* availability-state는 NETCONF 명령어로 직접 수정되지 않으며, O-RU의 내부 결함 관리 시스템에 의해 동적으로 설정됩니다.
* O-RU 관리자는 이 상태를 주기적으로 조회하여 시스템의 신뢰성과 작동 가능성을 평가해야 합니다.

**usage-state 상태 및 전이 설명**

usage-state는 O-RU의 현재 자원 사용 상태를 나타냅니다. 이 상태는 O-RU가 주파수 운용(carrier configuration)을 어떻게 처리하고 있는지를 반영하며, 사용 가능한 자원의 상태에 따라 변화합니다.

**usage-state 상태 정의**

1. **idle**:
   * \*\*O-RU에 주파수 운용(carrier)\*\*이 구성되지 않은 상태.
   * 자원이 할당되지 않았으며, 대기 중인 상태.
   * 초기 상태로 설정될 가능성이 높음.
2. **active**:
   * \*\*주파수 운용(carrier)\*\*이 하나 이상 구성된 상태.
   * 자원이 사용 중이나 추가 자원 할당이 가능한 상태.
3. **busy**:
   * \*\*추가 주파수 운용(carrier)\*\*을 구성할 수 없을 정도로 자원이 모두 사용된 상태.
   * O-RU의 최대 용량에 도달했음을 의미.

**상태 전이 다이어그램**

1. **idle → active**:
   * O-RU에 하나 이상의 주파수 운용(carrier)이 설정되면 상태가 active로 변경.
2. **active → busy**:
   * O-RU 자원이 모두 소진되어 추가 주파수 운용(carrier)을 구성할 수 없게 되면 busy로 전환.
3. **busy → active**:
   * 기존 주파수 운용(carrier)이 해제되어 일부 자원이 확보되면 active 상태로 돌아감.
4. **active → idle**:
   * 모든 주파수 운용(carrier)이 제거되면 상태가 다시 idle로 변경.

텍스트, 폰트, 원, 그래픽이(가) 표시된 사진

자동 생성된 설명

**운영 중 고려 사항**

* usage-state는 O-RU 자원의 동적 활용을 반영하며, 주파수 운용(carrier) 구성 및 해제 작업에 따라 자동으로 변경됩니다.
* 상태는 **NETCONF 명령어**로 조회 가능하며, 관리자는 이를 사용해 자원 상태를 확인하고 적절히 관리할 수 있습니다.

**상태 전환 예시**

**1. 상태 변경: idle → active**

* O-RU에 첫 번째 주파수 운용이 설정됨.  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명

2. **상태 조회:**

* **현재** usage-state  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명
* **응답 예시:**텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명

</GPT>

### 9.1.4 Retrieve Parameters

O-RU Controller는 NETCONF 프로토콜의 <get> 또는 <get-config> 명령어를 사용하여 YANG 모듈에 정의된 매개변수를 검색할 수 있습니다. 이 작업은 O-RU(장치)로부터 특정 데이터를 조회하는 데 사용되며, 결과는 NETCONF 서버가 클라이언트에 전달합니다.

**절차 및 구조**

1. **Preconditions (사전 조건)**:
   * O-RU Controller와 O-RU 간에 NETCONF 연결이 이미 설정되어 있어야 하며, 이를 위해 **NETCONF capabilities 교환**이 완료되어야 합니다.
   * 이 교환 과정은 각 시스템에서 지원하는 기능이 상호 확인되는 단계입니다.
2. **Post conditions (결과 조건)**:
   * O-RU Controller는 요청된 매개변수를 성공적으로 검색합니다.
   * 매개변수 검색은 <get> 또는 <get-config> 요청과 함께 적절한 **필터**가 포함되어야 하며, 반환되는 **데이터는 O-RU의 실행 데이터 저장소(running datastore)**에서 가져옵니다.

**NETCONF 명령어 구성**

**1. <get> 사용 예시**

* **사용 목적**: 특정 상태 정보를 실시간으로 검색.
* **예시**:  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명
* **응답 예시**:  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명

**2. <get-config> 사용 예시**

* **사용 목적**: 구성 정보를 검색.
* **예시**:  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명
* **응답 예시**:  
  텍스트, 스크린샷, 폰트이(가) 표시된 사진

  자동 생성된 설명

**작업 흐름**

1. **O-RU Controller → O-RU**: <get> 또는 <get-config> 요청 전송.
2. **O-RU → O-RU Controller**: 요청한 데이터가 포함된 <rpc-reply> 응답 전송.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

**Figure 9.1.4.1**

이 그림은 다음 흐름을 나타냅니다:

1. **클라이언트 요청**:
   * <get> 또는 <get-config> 명령어 전송.
   * 필터를 포함하여 특정 데이터만 요청 가능.
2. **서버 응답**:
   * 요청된 데이터를 <rpc-reply> 형식으로 클라이언트에게 반환.

**핵심 요약**

* **사용 목적**: O-RU의 상태 및 구성 매개변수 검색.
* **명령어**:
  + <**get**>: **실시간** 데이터 조회.
  + **<get-config>: 구성 데이터 조회**.
* **사전 조건**: NETCONF 연결 설정 및 기능 교환 완료.
* **필터 사용**: 특정 매개변수만 선택적으로 조회 가능.

### 9.1.5 Modify Parameters

이 섹션은 O-RU(Open RAN Radio Unit)의 구성을 NETCONF 프로토콜을 통해 수정하는 절차를 설명합니다. 이 과정은 데이터 일관성을 유지하고 동시 액세스로 인한 충돌을 방지하기 위해 설계되었습니다.

**절차 상세 설명**

1. **구성 데이터스토어 잠금 (Lock)**:
   * O-RU Controller는 구성을 수정하기 전에 \*\*대상 구성 데이터스토어(예: candidate 또는 running)\*\*를 잠가야 합니다.
   * 잠금은 다른 NETCONF 클라이언트가 Controller의 작업 중 구성 데이터스토어를 변경하지 못하도록 방지합니다.
   * 만약 다른 클라이언트가 이미 데이터스토어를 잠갔다면, O-RU는 **잠금 거부**를 나타내는 NETCONF 오류를 반환합니다.
     + **참고 1**: 이 경우, O-RU Controller는 일정 시간 대기 후 다시 시도해야 합니다.
2. **구성 수정 (Edit-Config)**:
   * O-RU Controller는 YANG 모듈의 매개변수를 NETCONF <edit-config> 절차를 사용하여 수정할 수 있습니다(Figure 9.1.5.1 참조).
   * **Candidate Datastore 사용**:
     + O-RU가 candidate 구성 데이터스토어를 지원하는 경우, 수정 작업은 반드시 candidate 데이터스토어에서 수행한 후 검증된 구성을 running 데이터스토어에 커밋(commit)해야 합니다.
   * **Running Datastore 사용**:
     + O-RU가 candidate 데이터스토어를 지원하지 않을 경우, running 데이터스토어에서 수정해야 합니다. 그러나 이는 시스템 운영에 영향을 미칠 가능성이 높으므로 각별한 주의가 필요합니다.
3. **구성 검증 (Validation)**:
   * 수정된 구성은 다음을 기반으로 검증됩니다:
     + 기본 YANG 제약 조건(예: min-elements, range, pattern).
     + XPATH 기반 YANG 제약 조건(예: leafref, must 및 when 구문).
     + YANG 제약 조건을 구현하는 외부 코드(O-RAN 사양에 정의됨).
   * 실패 시, 오류가 반환되며 RFC6241 부록 A를 참조하여 오류 코드를 확인할 수 있습니다.
4. **구성 잠금 해제 (Unlock)**:
   * 수정 작업이 완료된 후, O-RU Controller는 대상 구성 데이터스토어의 잠금을 해제해야 합니다.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

**조건**

* **사전 조건**:
  1. O-RU Controller와 O-RU 간의 NETCONF 기능 교환을 완료해야 합니다(연결 설정 과정의 일부).
  2. O-RU Controller가 대상 구성을 잠가야 합니다.
* **사후 조건**:
  1. O-RU Controller는 <edit-config> 요청에 따라 O-RU 리소스 상태를 업데이트합니다.
     + **성공 시**: 수정이 O-RU Controller에 확인됩니다.
     + **실패 시**: 실패 이유가 O-RU Controller에 제공됩니다.

**추가 고려사항**

1. **순차 처리**:
   * 각 <edit-config> 요청은 순차적으로 처리되며, 이전 요청의 응답을 받은 후에만 다음 요청을 수행할 수 있습니다.
   * 이로 인해 동시성 문제를 방지합니다.
2. **수정 거부**:
   * O-RU는 지원되지 않는 기능(예: 대역 외 캐리어 설정)과 관련된 내용이 포함된 경우 <edit-config> 요청을 거부할 수 있습니다.
3. **벤더 정의 동작**:
   * 벤더는 오류 발생 후의 동작을 정의할 수 있습니다.

### 9.1.6 Deleting Parameters

이 섹션은 O-RU(Open RAN Radio Unit)의 구성 데이터를 삭제하는 절차를 설명하며, 데이터 일관성을 유지하고 충돌을 방지하기 위한 안전 메커니즘을 포함합니다.

**절차 상세 설명**

1. **구성 데이터스토어 잠금 (Lock)**:
   * O-RU Controller는 \*\*대상 구성 데이터스토어(예: candidate 또는 running)\*\*를 잠가야 삭제 작업을 수행할 수 있습니다.
   * 잠금을 통해 다른 NETCONF 클라이언트가 구성 데이터스토어를 변경하지 못하도록 방지합니다.
   * 다른 클라이언트가 이미 데이터스토어를 잠갔다면, O-RU는 **잠금 거부**를 나타내는 NETCONF 오류를 반환합니다.
     + **참고**: 이 경우, O-RU Controller는 일정 시간 대기 후 삭제 작업을 재시도해야 합니다.
2. **삭제 작업 (Edit-Config with Delete)**:
   * O-RU Controller는 NETCONF <edit-config> 절차를 사용하여 YANG 모듈의 매개변수를 삭제할 수 있습니다.
   * **operation 속성**을 delete로 설정하여 삭제 작업을 지정합니다(Figure 9.1.6.1 참조).
   * **데이터가 없는 경우**:
     + 삭제 대상 데이터가 존재하지 않을 경우, **<rpc-error>** 요소와 함께 **<error-tag>** 값으로 "**data-missing**"이 반환됩니다.
3. **Candidate Datastore 우선 사용**:
   * O-RU가 candidate 데이터스토어를 지원하는 경우, 삭제 작업은 candidate 데이터스토어에서 수행한 후 검증된 구성을 running 데이터스토어에 커밋(commit)해야 합니다.
   * O-RU가 candidate 데이터스토어를 지원하지 않는 경우, running 데이터스토어에서 작업을 수행해야 합니다. 그러나 이는 시스템 운영에 영향을 미칠 가능성이 높으므로 각별히 주의해야 합니다.
4. **구성 잠금 해제 (Unlock)**:
   * 삭제 작업이 완료된 후, O-RU Controller는 구성 데이터스토어의 잠금을 해제해야 합니다.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

**조건**

* **사전 조건**:
  1. O-RU Controller와 O-RU 간 NETCONF 기능 교환이 완료되어야 합니다(연결 설정 과정의 일부).
  2. O-RU Controller가 대상 구성을 잠가야 합니다.
* **사후 조건**:
  1. O-RU Controller는 <edit-config> 요청에 따라 O-RU 리소스 상태를 업데이트합니다.
     + **성공 시**: 삭제 작업이 확인됩니다.
     + **실패 시**: 실패 이유가 O-RU Controller에 제공됩니다.

**추가 고려사항**

1. **순차 처리**:
   * 모든 <edit-config> 요청은 순차적으로 처리되어야 하며, 이전 요청의 응답을 받은 후에만 다음 요청을 수행할 수 있습니다.
2. **데이터 일관성**:
   * 삭제 작업은 구성 데이터스토어의 무결성과 일관성을 유지해야 하며, 삭제 대상이 없는 경우에도 적절한 오류 메시지를 반환하여 처리 상태를 명확히 해야 합니다.
3. **사용 사례**:
   * 기존 구성의 매개변수를 삭제하여 불필요한 설정을 제거하거나, 특정 설정을 초기화할 수 있습니다.

## 9.2 Framework for optional feature handling - TODO

## 9.3 M-Plane Operational State

## 9.4 Notification of Updates to Configuration Datastore

### 9.4.1 Introduction

### 9.4.2 Subscribing to updates from an O-RU

# 10 Performance Management - TODO

## 10.1 General

## 10.2 Measurement Activation and De-activation

## 10.3 Collection and Reporting of Measurement Result

### 10.3.1 NETCONF process

### 10.3.2 File Management process

### 10.3.3 Configured Subscription Process

# 11 Fault Management - TODO

## 11.1 Introduction

## 11.2 Alarm Notification

## 11.3 Manage Alarms Request to NETCONF Clients

## 11.4 Fault Sources

## 11.5 Manage Alarms Request to Event-Collector

# 12 File Management - TODO

## 12.1 Introduction

## 12.2 File System Structure

## 12.3 File Management Operation: upload

## 12.4 File Management Operation: retrieve file list

## 12.5 File Management Operation: download

# 13 Synchronization Aspects - ING

## 13.1 Introduction

이 절은 O-RU 시간 동기화의 다양한 측면과 Management Plane의 상호 작용을 제공합니다. 일반적으로 O-RU는 동기화 상태를 관리하고, 공급업체별 구현에 따라 하나 이상의 동기화 입력 소스를 선택하고, 그 결과 정확도가 구현 중인 무선 액세스 기술에서 요구하는 정확도를 충족하는지 확인하는 역할을 합니다.

## 13.2 Sync Status Object

이 sync 컨테이너는 모듈의 동기화 상태를 제공합니다. 동기화 상태에 관심이 있는 경우 O-RU 컨트롤러는 synchronization-state-change 알림에 대한 구독을 O-RU에 구성할 수 있습니다. 이벤트 알림은 O-RU 동기화 상태가 변경될 때마다 전송됩니다.

O-RU 동기화 상태는 다음과 같은 허용 값으로 표시됩니다:

* LOCKED: O-RU는 ITU-T G.810에 정의된 대로 locked 모드에 있습니다.
* HOLDOVER: O-RU 클럭이 보류 모드에 있습니다.
* FREERUN: O-RU 클럭은 입력 reference에 고정되어 있지 않으며 holdover 모드에 있지 않습니다.

그림 13.2.1은 상태 전환을 보여줍니다.

sync 컨테이너는 O-RU가 지원할 수 있는 동기화 소스를 배열을 통해 나열할 수 있도록 합니다.

* GNSS
* PTP
* SYNCE

텍스트, 도표, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

그림 13.2.1: Allowed sync state transitions

NOTE : HOLDOVER mode is optional and depends on internal O-RU design.

## 13.3 Sync Capability Object

## 13.4 PTP Configuration

### 13.4.1 Introduction

### 13.4.2 G.8275.1 specific parameters

### 13.4.3 G.8275.2 specific parameters

## 13.5 PTP Status

## 13.6 SyncE Configuration

## 13.7 SyncE Status

## 13.8 GNSS Configuration

## 13.9 GNSS Status

# 14 Operations Use Cases - TODO

## 14.1 Supervision Failure Handling and Supervision Termination Handling

### 14.1.1 Supervision Failure handling

### 14.1.2 Supervision Termination handling

## 14.2 Log management

### 14.2.1 Introduction

### 14.2.2 Troubleshooting

## 14.3 Trace

## 14.4 Operational aspects of Antenna Line Devices

### 14.4.1 Introduction

### 14.4.2 HDLC Interworking

### 14.4.3 ALD Operations

## 14.5 Operational aspects of external IO

### 14.5.1 Introduction

### 14.5.2 External input

### 14.5.3 External output

# 15 Details of O-RU Operations – \*\*TODO

## 15.1 Retrieval of O-RU Information

## 15.2 User plane message routing

### 15.2.1 Introduction

### 15.2.2 Configurable format for eAxC\_ID

### 15.2.3 U-Plane endpoint addressing

### 15.2.4 General configuration scenario

## 15.3 Carrier Configuration

### 15.3.1 Carrier creation

### 15.3.2 Activation, deactivation and sleep

### 15.3.3 Carriers relation to sync

#### 15.3.3.1 Transitions and Combinations

#### 15.3.3.2 Synchronization lost and HOLDOVER mode expired

#### 15.3.3.3 External timing source restored

## 15.4 Beamforming

### 15.4.1 Beamforming Configuration

### 15.4.2 Pre-Defined Beamforming Configuration

### 15.4.3 Beamforming Configuration Update

### 15.4.4 Tilting Pre-defined Beams

### 15.4.5 Dynamic Beamforming Control option

## 15.5 Antenna Calibration

### 15.5.1 Background

### 15.5.2 Overall Operation

#### 15.5.2.1 General

#### 15.5.2.2 Initiation

#### 15.5.2.3 Self-Calibration Operation

#### 15.5.2.4 Calibration Completion

#### 15.5.2.5 Antenna Calibration Procedure

### 15.5.3 O-RU Antenna Calibration Capability Parameter Configuration

### 15.5.4 antenna-calibration-required Notification Parameters

### 15.5.5 Start-antenna-calibration RPC Request Parameters

### 15.5.6 Example Antenna Calibration Operation

### 15.5.7 Calibration with multiple timing resource sets

### 15.5.8 antenna-calibration-multiple-time-resource-params Notification Parameters

## 15.6 Static configuration for PRACH and SRS

### 15.6.1 Background

### 15.6.2 Static configuration for PRACH processing

### 15.6.3 Frequency domain configuration

### 15.6.4 Time domain configuration

### 15.6.5 Operation

### 15.6.6 Static configuration for raw SRS processing

### 15.6.7 Operation

## 15.7 TDD pattern configuration

## 15.8 C-Plane Message Limits

# 16 Licensed-Assisted Access - TODO

## 16.1 Introduction

## 16.2 LAA-initiation Process

### 16.2.1 LAA Module Capabilities

### 16.2.2 LAA O-RU Parameter Configuration

## 16.3 Carrier-Selection

### 16.3.1 LAA Measurements

### 16.3.2 LAA Carrier Frequency Configuration

# 17 Shared Cell - \*\*TODO

## 17.1 Introduction

## 17.2 Architecture

## 17.3 Start-up and Installation

## 17.4 Performance Management

## 17.5 Delay Management

## 17.6 Details of O-RU operations for shared cell

### 17.6.1 O-RU Information for Shared Cell

### 17.6.2 Topology Discovery procedure

### 17.6.3 Shared Cell Configuration

### 17.6.4 U-plane Configuration for FHM mode

### 17.6.5 Support of Selective Transmission and Reception Function

## 17.7 Cascade-FHM mode

## 17.7.1 Background

## 17.7.2 Shared Cell Configuration on cascaded FHMs

# 18 Configured Subscriptions - TODO

## 18.1 Introduction

## 18.2 Description

## 18.3 Procedure

## 18.4 Notification Encoding

## 18.5 Notification Transport

## 18.6 Monitoring the Communications Channel between O-RU and Event-Collector

### 18.6.1 Background

### 18.6.2 Heartbeat Encoding

### 18.6.3 Heartbeat Control

### 18.6.4 Heartbeat Procedure

# Annex A Common Alarm definition (Normative) - TODO

## A.1 Introduction

# Annex B Counters (Normative) - TODO

## B.1 Counter Definition

## B.2 Transceiver Statistics

### B.2.1 Transceiver Measurements

### B.2.2 Statistics Calculation

### B.2.3 Frequency Table Generation

## B.3 Rx Window Statistics

### B.3.1 Rx Window Measurement

## B.4 Tx Statistics

## B.5 Energy, Power and Environmental Statistics

## B.6 Symbol RSSI Statistics

### B.6.1 Statistics Calculation

### B.6.2 Frequency Table Generation

# Annex C Optional Multi-Vendor Functionality (Informative) - TODO

## C.1: Optional Namespace

## C.2: Optional YANG Features

## C.3: Optional Capabilities Exposed Using O-RAN YANG Models

# Annex D YANG Module Graphical Representation (Informative) - TODO

## D.1 Introduction

## D.2 System Folder

### D.2.1 o-ran-supervision.yang Module