**This is a re-published version of the attached final specification.**

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.

 O-RAN.WG5.Transport.0-v01.00

Technical Specification

O-RAN Open F1/W1/E1/X2/Xn Interfaces Working Group

Transport Specification

 O-RAN.WG5.Transport.0-v01.00

Technical Specification

O-RAN Open F1/W1/E1/X2/Xn Interfaces Working Group

Transport Specification

Prepared by the O-RAN Alliance. Copyright © 2020 by the O-RAN Alliance.

By using, accessing or downloading any part of this O-RAN specification document, including by copying, saving, distributing, displaying or preparing derivatives of, you agree to be and are bound to the terms of the O-RAN Adopter License Agreement contained in Annex ZZZ of this specification. All other rights reserved.

Copyright © 2020 by the O-RAN Alliance.

Your use is subject to the terms of the O-RAN Adopter License Agreement in Annex ZZZ 1

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Revision** | **Author** | **Description** |
| 2020.03.09 | 1.00 | Ole Reinartz (Nokia) | First published version 1.00 |
|  |  |  |  |

Contents

Revision History 2

1 Scope 4

2 References 5

3 Definitions and abbreviations 7

3.1 Definitions 7

3.2 Abbreviations 7

4 Interface classification 8

4.1 General 8

4.2 Class 1: Basic network interoperability 8

4.2.1 Network Layer Interface (layer 3) 8

4.2.2 Transport Layer Interface (layer 4) 11

4.2.3 Security 11

4.3 Class 2: UNI type interfaces 13

4.3.1 Class 2.1: Ethernet 14

4.3.2 Class 2.2: [Vn-Nf]/N/L3 Service 15

5 Annex ZZZ : O-RAN Adopter License Agreement 15

Section 1: DEFINITIONS 15

Section 2: COPYRIGHT LICENSE 16

Section 3: FRAND LICENSE 16

Section 4: TERM AND TERMINATION 17

Section 5: CONFIDENTIALITY 17

Section 6: INDEMNIFICATION 17

Section 7: LIMITATIONS ON LIABILITY; NO WARRANTY 17

Section 8: ASSIGNMENT 18

Section 9: THIRD-PARTY BENEFICIARY RIGHTS 18

Section 10: BINDING ON AFFILIATES 18

Section 11: GENERAL 18

# 1 Scope

This document complements existing standards specific for F1-, W1-, E1-, X2- and Xn- transport (currently TS 38.472 [1], TS 38.474 [23], TS 36.424 [22], TS 38.462 [48] and TS 36.422 [21]) as they apply to O-CU and O-DU.

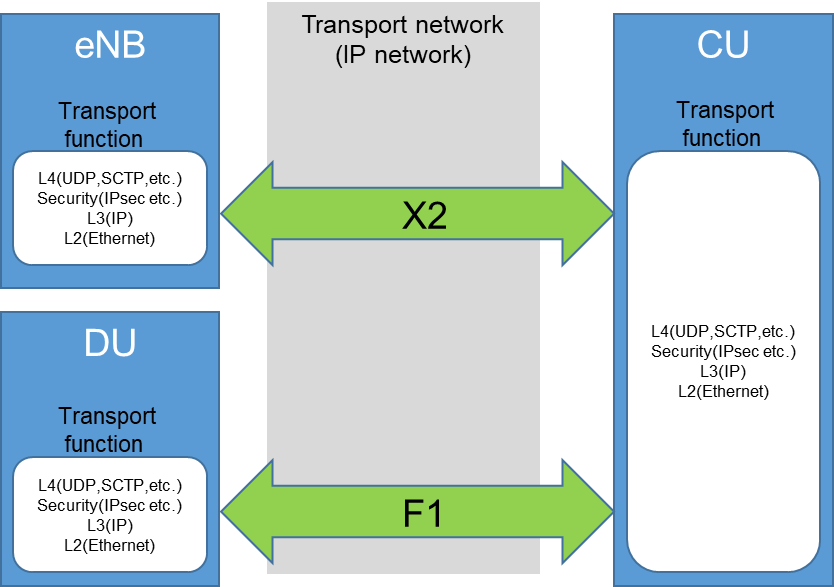


Figure Interfaces covered by ORAN WG5

Note: at the time of writing only F1- and X2- interfaces are covered by ORAN WG5 specifications.

It also covers transport aspects relevant for M-plane and S-plane. In addition, it defines a number of support classes.

Differences to referred standards are explicitly noted throughout the document.

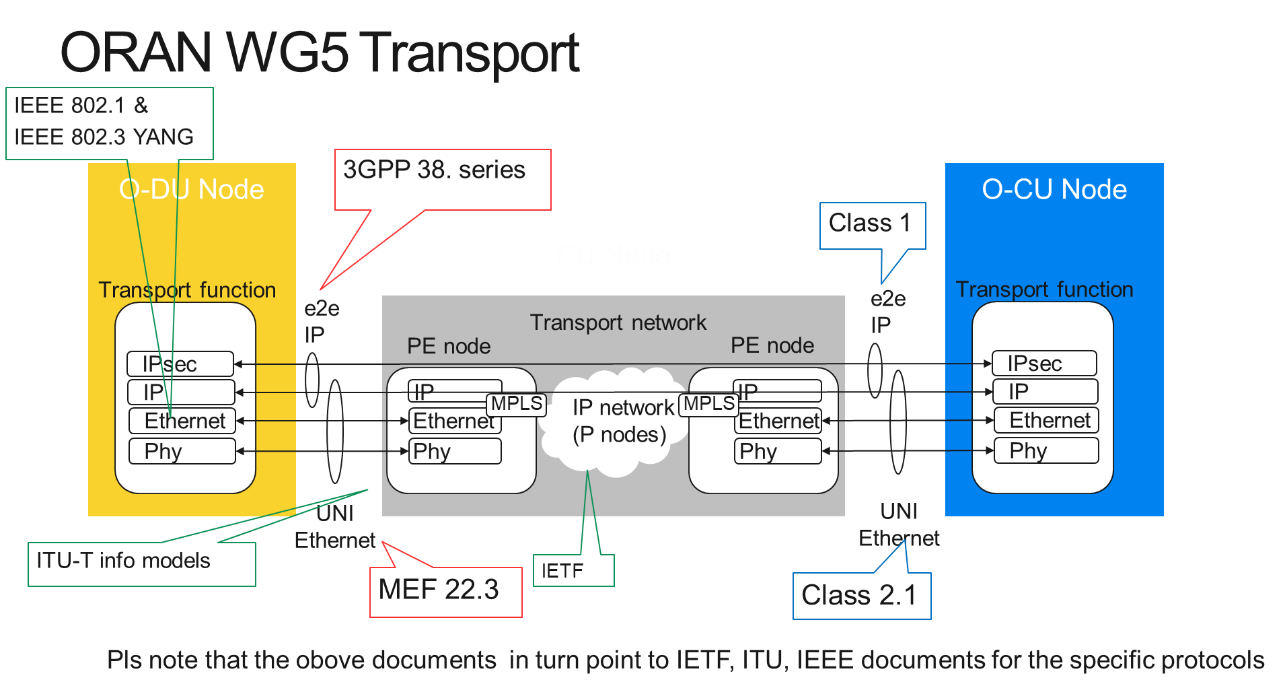


Figure 2 ORAN WG5 Transport

As stated above, while this document does not make requirement to the transport networks between O-DUs and O-CUs, Figure 2 also indicates existing standards documents making requirements to such transport networks that are possible to be used between O-DU and O-CUs, i.e. MEF 22.3, BBF TR-221,224,350 and WT-521.

# 2 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 TS 38.472 V15.5.0: " F1 signalling transport (Release 15)".

[2] IEEE 802.1Q-2018: “IEEE Standard for Local and metropolitan area networks— Bridges and Bridged Networks”

[3] IETF RFC 2474: “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”

[4] IETF RFC 2598: “An Expedited Forwarding PHB”

[5] IETF RFC 2597: “Assured Forwarding PHB Group”

[6] IETF RFC 4594: “Configuration Guidelines for DiffServ Service Classes”

[7] IETF RFC 826: “An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses”

[8] IETF RFC 792: “INTERNET CONTROL MESSAGE PROTOCOL”

[9] IETF RFC 8200: “Internet Protocol, Version 6 (IPv6) Specification”

[10] IETF RFC 4861: “Neighbor Discovery for IP version 6 (IPv6)”

[11] IETF RFC 4443: “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”

[12] IETF RFC 6890: “Special-Purpose IP Address Registries”

[13] IETF RFC 8190: “Updates to the Special-Purpose IP Address Registries”

[14] IETF RFC 2131: “Dynamic Host Configuration Protocol”

[15] IETF RFC 4361: “Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)”

[16] IETF RFC3315: “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”

[17] IETF RFC4862: “IPv6 Stateless Address Autoconfiguration”

[18] IETF RFC768: “User Datagram Protocol”

[19] 3GPP TS 29.060 V15.0.0: “GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 15)”

[20] 3GPP TS 29.274 V16.1.0: “GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 15)”

[21] 3GPP TS TS 36.422 version 15.1.0: “X2 signalling transport (Release 15)”

[22] 3GPP TS TS 36.424 version 15.0.0: “X2 data transport (Release 15)”

[23] 3GPP TS 38.474 V15.3.0: " F1 data transport (Release 15)".

[24] 3GPP TS 33.117 V16.2.0: “Catalogue of general security assurance requirements (Release 16)”

[25] IETF RFC 2119: “Key words for use in RFCs to Indicate Requirement Levels”

[26] IEEE 802.3-2018: “IEEE Standard for Ethernet”

[27] IETF RFC 791: “INTERNET PROTOCOL”

[28] IETF RFC 1918: “Address Allocation for Private Internets”

[29] IETF RFC 5357: “A Two-Way Active Measurement Protocol (TWAMP)”

[30] IETF RFC 4656: “A One-way Active Measurement Protocol (OWAMP)”

[31] ITU-T G.8013/Y.1731(08/2015): “Operation, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks”

[32] IETF RFC 4960. “Stream Control Transmission Protocol”

[33] 3GPP TS 29.281 V15.6.0: “General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) (Release 15)”

[34] IETF RFC 1034: “DOMAIN NAMES - CONCEPTS AND FACILITIES”

[35] IETF RFC 1035: “DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION”

[36] IETF RFC 4210: “Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)”

[37] IETF RFC 6083: “Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)”

[38] 3GPP TE 33.501 V15.6.0: “Security architecture and procedures for 5G system (Release 15)”

[39] IETF RFC 4301: “Security Architecture for the Internet Protocol”

[40] 3GPP TS 33.210 V16.2.0: “Network Domain Security (NDS); IP network layer security (Release 16)”

[41] 3GPP TS 33.310 V16.2.0: “Network Domain Security (NDS); Authentication Framework (AF) (Release 16)”

[42] 3GPP TS 33.401 V16.0.0: “3GPP System Architecture Evolution (SAE); Security architecture (Release 15)”

[43] 3GPP TR 33.821 V9.0.0: “Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE) (Release 9)”

[44] IETF RFC 4303: “IP Encapsulating Security Payload (ESP)”

[45] IETF RFC 8221: “Cryptographic Algorithm Implementation Requirements and Usage Guidancefor Encapsulating Security Payload (ESP) and Authentication Header (AH)”

[46] IETF RFC 7296: “Internet Key Exchange Protocol Version 2 (IKEv2)”

[47] ETSI GS NFV-INF 005 V1.1.1 (2014-12): Network Functions Virtualisation (NFV); Infrastructure; Network Domain

[48] 3GPP TS 38.462 V15.5.0: “E1 signalling transport (Release 15)”

[49] MEF 22.3: “Transport Services for Mobile Networks, January 2018”

[50] 3GPP TS 29.303 V16.0.0: “Domain Name System Procedures; Stage 3 (Release 16)”

# 3 Definitions and abbreviations

## 3.1 Definitions

The key words "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in IETF RFC 2119 [25]. All key words must be in upper case, bold text.

Items that are **REQUIRED** (contain the words **SHALL** or **SHALL NOT**) will be labeled as **[Rx]** for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) will be labeled as **[Dx]** for desirable. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) will be labeled as **[Ox]** for optional**.**

Items, if supported, are not meant to be active at all times, but should be available for use. Their state (active or not active) should be based on configuration.

In this document the phrase ‘equipment’ generally refers to entities implementing F1- and/or X2- interfaces.

## 3.2 Abbreviations

Abbreviations defined in this document take precedence over the definition of 3GPP

ARP Address Resolution Protocol

CBS committed burst size

CIR committed information rate

DHCP Dynamic Host Configuration Protocol

DSCP Differentiated Services Codepoint

ICMP Internet Control Message Protocol

MAC Media Access Control

OAM Operation, Administration and Maintenance

O-CU O-RAN Central Unit

O-DU O-RAN Distributed Unit

PHB Per-hop behaviour

QoS Quality of Service

TBD To Be Defined

FFS For Further Study

# 4 Interface classification

## 4.1 General

This chapter provides for a classification of Interface types, grouping different sets of mandatory features according to them into interface classes.

## 4.2 Class 1: Basic network interoperability

This class provides mandatory support for basic network interoperability.

### 4.2.1 Network Layer Interface (layer 3)

This section complies with and reuses the relevant parts of 3GPP TS 38.472 [1], TS 38.474 [23], TS 36.424 [22] and TS 36.422 [21].

#### 4.2.1 1 IP version 4

##### 4.2.1.1.1 General

1. IP version 4 **SHALL** be supported according to RFC791 [27] and RFC1918 [28].

Note: Address ranges specified in [28] are commonly used in operator networks.

1. O-RAN equipment **SHALL** **NOT** send IPv4 packets with any IPv4 header option field. If the IPv4 header option field is detected in the received packet, the contents of this option field **SHALL** be ignored at the receiving equipment.
2. IP addresses **SHALL** be supported on

* Logical interfaces: network interfaces that do not have a physical representation, e.g. Ethernet VLAN terminations
* Physical interfaces: Network interfaces that have a physical representation, e.g. a Network Interface Controller (a.k.a. plain Ethernet interfaces)
* Virtual IP interfaces (loopback interfaces). These IP addresses are not attached to any network interface

These may be located in the same or in different subnets.

1. For a particular Network Interface Controller IP addresses **SHALL** be supported on either the physical or the logical interface(s).
2. The resolution of Ethernet MAC addresses is done via ARP according to [7].

##### 4.2.1.1.2 ICMP for IPv4

1. The equipment **SHALL** support the function of sending and receiving ICMP according to [8]. Clause 4.2.4.1.1.2 in [24] shall generally be adhered to, with the differences as defined in [R7]:
2. The following message types **SHALL** be supported:

* destination unreachable (‘Permitted’ in [24])
* time exceeded with Code field=1 (‘Optional’ in [24])[[1]](#footnote-2)
* echo request/reply (echo request ‘Permitted’ and echo reply ‘Optional’ in [24])

1. The following message types **SHALL NOT** be supported, i.e. shall never be sent, and shall be discarded (existence of packet may be logged) when received:

* Source quench (not listed in [24])
* Information request/reply (not listed in [24])

1. The support of all other types of ICMP messages is optional.
2. Depending on the type of the received ICMP message the equipment **SHALL** terminate the ICMP messages, create and send the correct responses, or drop it. Incoming fragmented ICMP messages will be reassembled as necessary.
3. For IPsec tunnels ICMP messages towards and from inner IP address and outer IP address **SHALL** be supported.

##### 4.2.1.1.3 DHCPv4

1. DHCP according to [14] **SHOULD** be supported. In addition, the equipment **SHOULD** support the behavior specified in [15], using stable DHCPv4 node identifiers in their dhcp-client-identifier option.

#### 4.2.1.2 IP version 6

##### 4.2.1.2.1 General

1. IP version 6 **SHOULD** be supported according to [9].

If IP version 6 is supported,

1. All header fields **SHALL** be supported.
2. The following extension headers **SHALL** be supported:

* Fragment Header
* Encapsulating Security Payload Header
* Hop-by-Hop Options Header
* No Next header

1. IP addresses **SHALL** be supported on

* Logical interfaces: network interfaces that do not have a physical representation, e.g. Ethernet VLAN terminations
* Physical interfaces: Network interfaces that have a physical representation, e.g. a Network Interface Controller (a.k.a. plain Ethernet interfaces)
* Virtual IP interfaces (loopback interfaces). These IP addresses are not attached to any network interface

These may be located in the same or in different subnets.

1. For a particular interface, IP addresses **SHALL** be supported on either the physical or the logical interface(s).

##### 4.2.1.2.2 ICMP for IPv6

If IP version 6 is supported,

1. The equipment **SHALL** support the function of sending and receiving ICMPv6 according to [11] and Neighbor Discovery as defined in [10]. Clause 4.2.4.1.1.2 in [24] shall generally be adhered to, with the differences as defined in [R16]:.
2. The following message types **SHALL** be supported:

* neighbor solicitation/advertisement
* router solicitation
* router advertisement (only receive)
* destination unreachable
* time exceeded with Code field=1 [[2]](#footnote-3)
* echo request/reply

1. Depending on the type of the received ICMPv6 message the equipment **SHALL** terminate the ICMP messages, create and send the correct responses, or drop it. Incoming fragmented ICMPv6 will be reassembled as necessary.
2. The support of all other types of ICMPv6 messages is **OPTIONAL**.
3. For IPsec tunnels ICMPv6 messages towards and from inner IP addresses and outer IP addresses **SHALL** be supported.

##### 4.2.1.2.3 DHCPv6

1. DHCP according to [16] **SHOULD** be supported.

##### 4.2.1.2.4 SLAAC

1. SLAAC according to [17] **SHOULD** be supported.

#### 4.2.1.3 Address space

1. The whole IP address space **SHALL** be supported by all O-RAN nodes. However, the special purpose of some IP ranges as defined in [12] (updated by [13]) **SHALL** be respected.

#### 4.2.1.4 Packet marking

1. IP packets **SHALL** be marked with up to 64 different DSCP values according to [3], as also defined in [23] section 5.3 and [1] section 6.

#### 4.2.1.5 Traceroute

1. Traceroute based on UDP **SHALL** be supported by the equipment.

Traceroute is done at the indication from the m-plane application. A sequence of UDP packets is being sent, with the TTL of first packet being set to 1. This field is gradually incremented, usually with every third packet sent.

1. The Source IP address **SHALL** be indicated by the m-plane application and **SHALL** be one of the addresses assigned to the equipment.

#### 4.2.1.6 Network OAM

##### 4.2.1.6.1 TWAMP

1. TWAMP according to [29] **SHOULD** be supported, or its variant TWAMP-light as defined in Appendix 1 of [29].

##### 4.2.1.6.2 OWAMP

1. OWAMP according to [30] **SHOULD** be supported.

##### 4.2.1.6.3 ITU-T Y.1731

1. ITU-T Recommendation G.8013/Y.1731 according to [31] **SHOULD** be supported.
2. Support should be limited to:
   * Ethernet continuity check (ETH-CC) ([31] section 7.1)
   * Ethernet loopback (ETH-LB) ([31] section 7.2)
   * Ethernet link trace (ETH-LT) ([31] section 7.3)
3. All features not listed in [D8] are **OPTIONAL**.

#### 4.2.1.7 Nework layer setup

1. Networking parameters (IP addresses, IP routing entries, …) **SHALL** be assigned to interfaces based on one of the following methods, with 1. at the highest and 4. at the lowest priority:
2. Manual assignment
3. SLAAC (IP address, default route) with optional DHCPv6-support for additional parameters
4. DHCPv6
5. DHCPv4

Note: a more detailed automatic setup procedure is FFS.

### 4.2.2 Transport Layer Interface (layer 4)

#### 4.2.2.1 UDP

1. UDP **SHALL** be supported according to [18], as defined in [22] and [23].

#### 4.2.2.2 SCTP

1. SCTP **SHALL** be supported according to [32], as defined in [1], section 7.
2. A node **SHALL** support a single SCTP association per node pair
3. Multiple SCTP associations per node pair **SHOULD** be supported.
4. The minimum size of the receive buffer per socket shall be 128 Kilobytes.
5. The SCTP implementation **SHALL** allow any endpoint to be the initiator of an SCTP association.

Note: the application should define client- and server role of an SCTP association.

#### 4.2.2.3 PTP

The content of this section is FFS.

#### 4.2.2.4 GTP-U

1. GTP-U **SHALL** be supported according to [33].

#### 4.2.2.5 DNS

1. DNS according to [50] **SHOULD** be supported.

### 4.2.3 Security

#### 4.2.3.1 PKI

1. A Public Key Infrastructure according to [36] **SHOULD** be supported.

#### 4.2.3.2 DTLS

1. DTLSaccording to [37] **SHALL** be supported for the SCTP association(s) of the F1-C interface, as defined in [38] subsections 9.8.2, 9.8.3 and 9.4.

#### 4.2.3.3 IPsec

##### 4.2.3.3.1 Overview

The security of the F1/W1/E1/X2/Xn - interface control, user, synchronization and management plane protocols is increased by providing encryption, integrity protection and communication peer authentication with IPsec according [39]. IPSec can be applied to all IP traffic. It is possible to enable / disable IPsec and to configure IPsec connections to peer-entities independently in terms of security settings for each remote IPsec peer, e.g. per neighbor node or per plane. Further, it is possible to define connections to remote peers which shall not be covered by IPsec although IPsec is enabled (bypassing traffic).

The supported IPsec capabilities follow [40] for interworking purposes and further appliance rules given in [41], [42], [38] and [43]. Since IPsec standards include a high number of selectable security parameters options, 3GPP has recommended to cut down the number of these options in order to guarantee interoperability between different security domains.

##### 4.2.3.3.2 Supported IPsec capabilities

1. **Services that SHALL be supported (see also [38],** **section 9.8.2):**

* Confidentiality, can be enabled/disabled (via ENCR\_NULL)
* integrity protection, always enabled
* data origin authentication, always enabled
* anti-replay protection, can be enabled/disabled
* extended sequence numbers, can be enabled/disabled

1. **Protocol that SHALL be supported: ESP ([44]**, **as profiled by [40])**

* IPsec mode: Tunnel mode
* for encrypted packets the DSCP value of the inner packet will be copied to the outer packet
* NAT traversal

1. **ESP encryption transforms that SHALL be supported (including authenticated encryption transforms, see also [40], section 5.3.3):**

* as in [45] (the ones marked with ‘MUST’)

1. **ESP authentication transforms that SHALL be supported:**

* as in [45] (the ones marked with ‘MUST’ or “MUST-”)
* AES-GMAC with AES-128 shall be supported.
* NULL authentication algorithm is explicitly not allowed for use, unless an authenticated encryption algorithm is used.

1. **Identification that SHALL be supported:**

* IP address
* Fully Qualified domain name (FQDN) (if DNS is supported)

1. **Authentication that SHALL be supported:**

* Pre-shared Keys
* Digital certificates in X.509v3 format provided by a Certificate Authority solution. (optional)

1. **Key exchange that SHALL be supported:**

* IKEv2 (RFC 4306)
* profile as described in [41]
* certificate-based authentication according to [41]
* certificates according to the profile described by [41]
* DH groups 14 and 19

1. **Security Association multiplicity that SHALL be supported:**

* multiple IKE SAs (multiple IPsec tunnels)
* multiple IPsec SAs
* multiple IPsec SAs per IPsec tunnel

1. IKE SA(s) and IPSEC SA(s) **SHALL** be regularly re-established.
2. When the full sequence number space of an IPSEC SA(s) is used, the transmission for that SA **SHALL** stop.
3. Dead-Peer-Detection (DPD) **SHALL** be supported as defined in [46].
4. Each node **SHALL** support a traffic narrowing function for the traffic selector ([46]): If the traffic selector notified from the peer (e.g. Security GW or neighboring node) is wider than the Local/Remote Address range in the SPD information set on the node side, the peers set the traffic selector values to the narrower range.

##### 4.2.3.3.3 Parallel usage of IPsec and other secure transport protocols

1. The equipment **SHALL** support configuration of IPsec (one or more dedicated connections) in parallel with other secure transport protocols like SSH.

For instance, it is possible to run SSH connections within an IPsec tunnel or in parallel to IPsec tunnel(s).

##### 4.2.3.3.4 Responder mode and Initiator/Responder mode support

1. The equipment **SHALL** support a configurable option per IKE Security Association to use "Responder mode" instead of "Responder/Initiator mode".

The mode is related to IKE SA establishment only. The introduction of "Responder mode" does not change the IKE SA rekeying behavior: Each node operates as initiator and responder in IKE\_SA rekeying.

## 4.3 Class 2: UNI type interfaces

1. Support of this class **SHALL** include all mandatory features supported in class 1.

### 4.3.1 Class 2.1: Ethernet

#### 4.3.1.1 Data link layer Interface (layer 2)

##### 4.3.1.1.1 General

1. The only data link layer to be supported **SHALL** be Ethernet as defined in IEEE 802.3-2018 [26]
2. The supported frame format **SHALL** be Ethernet frame with type interpretation of the type length field (see [2] section 3). The Length-interpretation and multiplexing data with LLC (IEEE 802.2 LLC standard) **SHALL NOT** be supported.
3. The Ethernet termination feature **SHALL** support frames with an MTU (i.e. Ethernet SDU) of up to 1500 bytes as in [2], Section 3.2.7 item a).
4. The Ethernet termination feature **SHOULD** support frames with an MTU (i.e. Ethernet SDU) of 1982 bytes as in [2], Section 3.2.7 item c).[[3]](#footnote-4)
5. A single VLAN tag for the traffic (i.e. a C-VLAN tag) **SHALL** be supported according to IEEE 802.1Q-2018 [2].
6. Priority tagged frames (i.e, frames tagged with VLAN ID=0) **SHALL** always be received, as required by the standard.
7. Transmitting priority tagged frames is **OPTIONAL**.
8. The UNI to a transport network depicted in Figure 2, specified in MEF 22.3 [49] and amended by MEF 22.3.1, **MAY** be supported.

##### 4.3.1.1.2 QoS Marking

1. VLAN- tagged frames **SHALL** be marked with up to 8 different PCP values (see [2] for details on the PCP field), to allow for proper traffic scheduling in a VLAN- aware Ethernet network.

##### 4.3.1.1.3 Packet Queuing, -scheduling and -shaping

1. Traffic Queuing and -scheduling **SHALL** be provided for outgoing traffic. At the minimum, a single stage of queuing/scheduling per outgoing interface **SHALL** be supported.
2. Traffic shaping **SHOULD** be provided for outgoing traffic. At the minimum, a single stage of shaping per outgoing interface **SHOULD** be supported.
3. Scheduling/shaping **SHOULD** account for all bytes of the IP packet.
4. Scheduling/shaping **SHALL** account for all bytes of the Ethernet frame, including Ethernet header and FCS.
5. Schedulers **SHALL** support at least 6 different per-hop behaviours (PHB):

* EF: at least one class of Expedited Forwarding PHB (Defined in [4])
* AF1-4: 4 classes of Assured Forwarding PHB (Defined in [5])
* BE: Default PHB (Defined in [3])

1. PHBs **SHALL** be selected based on the DSCP value of the packet.
2. PHBs **SHOULD** be selected based on the PCP values of the frame.
3. The scheduling discipline to be supported by the scheduler **SHALL** be priority queueing and, if supported, rate queuing as defined in [6], where AF1-4 are scheduled using a either a priority or a rate queuing scheduling discipline. The result of this scheduling discipline, EF and BE are being scheduled using the priority queuing discipline with EF scheduled at the highest priority and BE scheduled at the lowest priority.



Figure 3 Example structure of scheduling disciplines (L2)

1. If implemented, the traffic shaping functionality **SHALL** allow to configure an average rate (CIR: committed information rate) and a burst size (CBS: committed burst size) to be committed. Range and granularity of these parameters depend on the implementation. In its default state (i.e. without any configuration done) the traffic shaping function **SHALL** be inacticve.

### 4.3.2 Class 2.2: [Vn-Nf]/N/L3 Service

1. A VNF **SHOULD** be able to use the network services provided by the Vn-Nf/N/L3 service as defined in [47] subsection 5.1.1.2.

# 5 Annex ZZZ : O-RAN Adopter License Agreement

BY DOWNLOADING, USING OR OTHERWISE ACCESSING ANY O-RAN SPECIFICATION, ADOPTER AGREES TO THE TERMS OF THIS AGREEMENT.

This O-RAN Adopter License Agreement (the “Agreement”) is made by and between the O-RAN Alliance and the entity that downloads, uses or otherwise accesses any O-RAN Specification, including its Affiliates (the “Adopter”).

This is a license agreement for entities who wish to adopt any O-RAN Specification.

## Section 1: DEFINITIONS

1.1 “Affiliate” means an entity that directly or indirectly controls, is controlled by, or is under common control with another entity, so long as such control exists. For the purpose of this Section, “Control” means beneficial ownership of fifty (50%) percent or more of the voting stock or equity in an entity.

1.2 “Compliant Implementation” means any system, device, method or operation (whether implemented in hardware, software or combinations thereof) that fully conforms to a Final Specification.

1.3 “Adopter(s)” means all entities, who are not Members, Contributors or Academic Contributors, including their Affiliates, who wish to download, use or otherwise access O-RAN Specifications.

1.4 “Minor Update” means an update or revision to an O-RAN Specification published by O-RAN Alliance that does not add any significant new features or functionality and remains interoperable with the prior version of an O-RAN Specification. The term “O-RAN Specifications” includes Minor Updates.

1.5 “Necessary Claims” means those claims of all present and future patents and patent applications, other than design patents and design registrations, throughout the world, which (i) are owned or otherwise licensable by a Member, Contributor or Academic Contributor during the term of its Member, Contributor or Academic Contributorship; (ii) such Member, Contributor or Academic Contributor has the right to grant a license without the payment of consideration to a third party; and (iii) are necessarily infringed by a Compliant Implementation (without considering any Contributions not included in the Final Specification). A claim is necessarily infringed only when it is not possible on technical (but not commercial) grounds, taking into account normal technical practice and the state of the art generally available at the date any Final Specification was published by the O-RAN Alliance or the date the patent claim first came into existence, whichever last occurred, to make, sell, lease, otherwise dispose of, repair, use or operate a Compliant Implementation without infringing that claim. For the avoidance of doubt in exceptional cases where a Final Specification can only be implemented by technical solutions, all of which infringe patent claims, all such patent claims shall be considered Necessary Claims.

1.6 “Defensive Suspension” means for the purposes of any license grant pursuant to Section 3, Member, Contributor, Academic Contributor, Adopter, or any of their Affiliates, may have the discretion to include in their license a term allowing the licensor to suspend the license against a licensee who brings a patent infringement suit against the licensing Member, Contributor, Academic Contributor, Adopter, or any of their Affiliates.

## Section 2: COPYRIGHT LICENSE

2.1 Subject to the terms and conditions of this Agreement, O-RAN Alliance hereby grants to Adopter a nonexclusive, nontransferable, irrevocable, non-sublicensable, worldwide copyright license to obtain, use and modify O-RAN Specifications, but not to further distribute such O-RAN Specification in any modified or unmodified way, solely in furtherance of implementations of an ORAN

Specification.

2.2 Adopter shall not use O-RAN Specifications except as expressly set forth in this Agreement or in a separate written agreement with O-RAN Alliance.

## Section 3: FRAND LICENSE

3.1 Members, Contributors and Academic Contributors and their Affiliates are prepared to grant based on a separate Patent License Agreement to each Adopter under Fair Reasonable And Non- Discriminatory (FRAND) terms and conditions with or without compensation (royalties) a nonexclusive, non-transferable, irrevocable (but subject to Defensive Suspension), non-sublicensable, worldwide patent license under their Necessary Claims to make, have made, use, import, offer to sell, lease, sell and otherwise distribute Compliant Implementations; provided, however, that such license shall not extend: (a) to any part or function of a product in which a Compliant Implementation is incorporated that is not itself part of the Compliant Implementation; or (b) to any Adopter if that Adopter is not making a reciprocal grant to Members, Contributors and Academic Contributors, as set forth in Section 3.3. For the avoidance of doubt, the foregoing licensing commitment includes the distribution by the Adopter’s distributors and the use by the Adopter’s customers of such licensed Compliant Implementations.

3.2 Notwithstanding the above, if any Member, Contributor or Academic Contributor, Adopter or their Affiliates has reserved the right to charge a FRAND royalty or other fee for its license of Necessary Claims to Adopter, then Adopter is entitled to charge a FRAND royalty or other fee to such Member, Contributor or Academic Contributor, Adopter and its Affiliates for its license of Necessary Claims to its licensees.

3.3 Adopter, on behalf of itself and its Affiliates, shall be prepared to grant based on a separate Patent License Agreement to each Members, Contributors, Academic Contributors, Adopters and their Affiliates under Fair Reasonable And Non-Discriminatory (FRAND) terms and conditions with or without compensation (royalties) a nonexclusive, non-transferable, irrevocable (but subject to Defensive Suspension), non-sublicensable, worldwide patent license under their Necessary Claims to make, have made, use, import, offer to sell, lease, sell and otherwise distribute Compliant Implementations; provided, however, that such license will not extend: (a) to any part or function of a product in which a Compliant Implementation is incorporated that is not itself part of the Compliant Implementation; or (b) to any Members, Contributors, Academic Contributors, Adopters and their Affiliates that is not making a reciprocal grant to Adopter, as set forth in Section 3.1. For the avoidance of doubt, the foregoing licensing commitment includes the distribution by the Members’, Contributors’, Academic Contributors’, Adopters’ and their Affiliates’ distributors and the use by the Members’, Contributors’, Academic Contributors’, Adopters’ and their Affiliates’ customers of such licensed Compliant Implementations.

## Section 4: TERM AND TERMINATION

4.1 This Agreement shall remain in force, unless early terminated according to this Section 4.

4.2 O-RAN Alliance on behalf of its Members, Contributors and Academic Contributors may terminate this Agreement if Adopter materially breaches this Agreement and does not cure or is not capable of curing such breach within thirty (30) days after being given notice specifying the breach.

4.3 Sections 1, 3, 5 - 11 of this Agreement shall survive any termination of this Agreement. Under surviving Section 3, after termination of this Agreement, Adopter will continue to grant licenses (a) to entities who become Adopters after the date of termination; and (b) for future versions of ORAN Specifications that are backwards compatible with the version that was current as of the date of termination.

## Section 5: CONFIDENTIALITY

Adopter will use the same care and discretion to avoid disclosure, publication, and dissemination of O-RAN Specifications to third parties, as Adopter employs with its own confidential information, but no less than reasonable care. Any disclosure by Adopter to its Affiliates, contractors and consultants should be subject to an obligation of confidentiality at least as restrictive as those contained in this Section. The foregoing obligation shall not apply to any information which is: (1) rightfully known by Adopter without any limitation on use or disclosure prior to disclosure; (2) publicly available through no fault of Adopter; (3) rightfully received without a duty of confidentiality; (4) disclosed by O-RAN Alliance or a Member, Contributor or Academic Contributor to a third party without a duty of confidentiality on such third party; (5) independently developed by Adopter; (6) disclosed pursuant to the order of a court or other authorized governmental body, or as required by law, provided that Adopter provides reasonable prior written notice to O-RAN Alliance, and cooperates with O-RAN Alliance and/or the applicable Member, Contributor or Academic Contributor to have the opportunity to oppose any such order; or (7) disclosed by Adopter with O-RAN Alliance’s prior written approval.

## Section 6: INDEMNIFICATION

Adopter shall indemnify, defend, and hold harmless the O-RAN Alliance, its Members, Contributors or Academic Contributors, and their employees, and agents and their respective successors, heirs and assigns (the “Indemnitees”), against any liability, damage, loss, or expense (including reasonable attorneys’ fees and expenses) incurred by or imposed upon any of the Indemnitees in connection with any claims, suits, investigations, actions, demands or judgments arising out of Adopter’s use of the licensed O-RAN Specifications or Adopter’s commercialization of products that comply with O-RAN Specifications.

## Section 7: LIMITATIONS ON LIABILITY; NO WARRANTY

EXCEPT FOR BREACH OF CONFIDENTIALITY, ADOPTER’S BREACH OF SECTION 3, AND ADOPTER’S INDEMNIFICATION OBLIGATIONS, IN NO EVENT SHALL ANY PARTY BE LIABLE TO ANY OTHER PARTY OR THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES RESULTING FROM ITS PERFORMANCE OR NON-PERFORMANCE UNDER THIS AGREEMENT, IN EACH CASE WHETHER UNDER CONTRACT, TORT, WARRANTY, OR OTHERWISE, AND WHETHER OR NOT SUCH PARTY HAD ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. O-RAN SPECIFICATIONS ARE PROVIDED “AS IS” WITH NO WARRANTIES OR CONDITIONS WHATSOEVER, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. THE O-RAN ALLIANCE AND THE MEMBERS, CONTRIBUTORS OR ACADEMIC CONTRIBUTORS EXPRESSLY DISCLAIM ANY WARRANTY OR CONDITION OF MERCHANTABILITY, SECURITY, SATISFACTORY QUALITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, ERROR-FREE OPERATION, OR ANY WARRANTY OR CONDITION FOR O-RAN SPECIFICATIONS.

## Section 8: ASSIGNMENT

Adopter may not assign the Agreement or any of its rights or obligations under this Agreement or make any grants or other sublicenses to this Agreement, except as expressly authorized hereunder, without having first received the prior, written consent of the O-RAN Alliance, which consent may be withheld in O-RAN Alliance’s sole discretion. O-RAN Alliance may freely assign this Agreement.

## Section 9: THIRD-PARTY BENEFICIARY RIGHTS

Adopter acknowledges and agrees that Members, Contributors and Academic Contributors (including future Members, Contributors and Academic Contributors) are entitled to rights as a third-party beneficiary under this Agreement, including as licensees under Section 3.

## Section 10: BINDING ON AFFILIATES

Execution of this Agreement by Adopter in its capacity as a legal entity or association constitutes that legal entity’s or association’s agreement that its Affiliates are likewise bound to the obligations that are applicable to Adopter hereunder and are also entitled to the benefits of the rights of Adopter hereunder.

## Section 11: GENERAL

This Agreement is governed by the laws of Germany without regard to its conflict or choice of law provisions.

This Agreement constitutes the entire agreement between the parties as to its express subject matter and expressly supersedes and replaces any prior or contemporaneous agreements between the parties, whether written or oral, relating to the subject matter of this Agreement.

Adopter, on behalf of itself and its Affiliates, agrees to comply at all times with all applicable laws, rules and regulations with respect to its and its Affiliates’ performance under this Agreement, including without limitation, export control and antitrust laws. Without limiting the generality of the foregoing, Adopter acknowledges that this Agreement prohibits any communication that would violate the antitrust laws.

By execution hereof, no form of any partnership, joint venture or other special relationship is created between Adopter, or O-RAN Alliance or its Members, Contributors or Academic Contributors. Except as expressly set forth in this Agreement, no party is authorized to make any commitment on behalf of Adopter, or O-RAN Alliance or its Members, Contributors or Academic Contributors.

In the event that any provision of this Agreement conflicts with governing law or if any provision is held to be null, void or otherwise ineffective or invalid by a court of competent jurisdiction, (i) such provisions will be deemed stricken from the contract, and (ii) the remaining terms, provisions, covenants and restrictions of this Agreement will remain in full force and effect.

Any failure by a party or third party beneficiary to insist upon or enforce performance by another party of any of the provisions of this Agreement or to exercise any rights or remedies under this Agreement or otherwise by law shall not be construed as a waiver or relinquishment to any extent of the other parties’ or third party beneficiary’s right to assert or rely upon any such provision, right or remedy in that or any other instance; rather the same shall be and remain in full force and effect.

1. The Time Exceeded message with Code 1 is used to report a fragment reassembly timeout, as specified in [8] [↑](#footnote-ref-2)
2. The Time Exceeded message with Code 1 is used to report a fragment reassembly timeout, as specified in [11] [↑](#footnote-ref-3)
3. This does not preclude equipment supporting Ethernet SDUs larger than that. [↑](#footnote-ref-4)