सत्यमेव जयते

वर्गीय आवश्यकताओं के लिए मानक

टी.ई.सी XXXX:२०२५

STANDARD FOR GENERIC REQUIREMENTS

TEC XXXX:2025

फिक्स्ड वायरलेस एक्सेस ग्राहक परिसर उपकरण

Fixed Wireless Access Customer Premises Equipment

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नई दिल्ली–110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release: XXXX, 2025

FOREWORD

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Standards for Generic Requirements (GR), Interface Requirements (IR) and Service Requirements (SR) as well as Test guides for Telecom Products and Services;
- Issue of Technical regulations in the form of essential Requirements (ER);
- Field evaluation of products and Systems;
- National Fundamental Plans;
- Support to DOT on technology issues;
- Testing & Certification of Telecom products; and
- Designation of Conformance Assessment Bodies (CABs) for testing.

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document is the standard for Generic Requirements (GR) of Fixed Wireless Access Customer Premises Equipment (FWA CPE), covering common features across 4G, 5G Non-Standalone (NSA), and 5G Standalone (SA) technologies. It also includes specific requirements that apply only to certain technologies. The requirements are grouped into important areas such as Radio/RRC/NAS, support for multiple APNs to separate different services, Quality of Service, Voice Services, Networking Features, Wi-Fi, IDU/ODU Interworking and Resilience, Device Management, and Security. For each area, it is clearly mentioned whether the requirement applies to Indoor FWA devices, Outdoor FWA devices, or both.

CONVENTIONS

In this document, requirements are classified as follows:

- The keywords "shall" or “is/are required to” indicate a requirement or requirements, which must be mandatorily complied and from which no deviation is permitted, if conformance to this document is to be claimed;
- The keyword "should" indicates a recommended requirement, which is not mandatory for claiming conformance to this document. However, its implementation is strongly advised as it represents best practices or preferred functionality; and
- The keywords “Optional” or “may” indicate an optional requirement, which is permissible for exclusion from mandatory compliance, unless the said requirement is claimed to be complied by the vendor. These terms are not intended to imply that the vendor's implementation must provide the option; it means the vendor may optionally provide the feature and still claim conformance with this document.

HISTORY SHEET

Sl. No.	Standard/Document No.	Title	Remarks
1.	TEC XXXX:2025	Fixed Wireless Access Customer Premises Equipment	New Standard

Table of Contents

References

S. No	*Document No*	*Title / Document Name*
1.	3GPP TS 23.207 V16.0.0 or later	End-to-end Quality of Service (QoS) concept and architecture
2.	3GPP TS 23.203 V16.0.0 or later	Policy and charging control architecture
3.	GSMA IR.92 Version 15.0 or later	IMS Profile for Voice and SMS - Version 15.0
4.	GSMA IR.114	IMS Profile for Voice, Video and Messaging over 5GS
5.	GSMA TS.64	FWA Devices Architecture and Requirements Version 1.0
6.	3GPP TS 24.229 V15.2.0 or later	IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
7.	3GPP TS 23.003 V16.3.0 or later	Numbering, addressing and identification.
8.	3GPP TS 23.228 V16.5.0 or later	IP Multimedia Subsystem (IMS); Stage 2
9.	3GPP TS 24.607 version 15.0.0 or later	Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
10.	ETSI EN 300 659-3 V1.3.1	Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Subscriber line protocol over the local loop for display (and related) services; Part 3: Data link message and parameter codings
11.	3GPP TS 24.604 version 15.1.0 or later	Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem.

		Protocol specification
12.	3GPP TS 24.611 version 11.3.0 or later	Anonymous Communication Rejection (ACR) and Communication Barring (CB) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
13.	3GPP TS 24.610 version 15.1.0 or later	Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
14.	3GPP TS 24.615 version 15.0.0 or later	Communication Waiting (CW) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol Specification
15.	3GPP TS 24.147 version 10.1.0 or later	Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem. Stage 3
16.	3GPP TS 24.642 version 10.2.0 or later	Completion of Communications to Busy Subscriber (CCBS) and Completion of Communications by No Reply (CCNR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol Specification
17.	3GPP TS 24.629 version 15.0.0 or later	Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
18.	3GPP TS 24.608 version 10.0.0 or later	Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification
19.	3GPP TS 24.616 version 10.0.0 or	LTE; Malicious Communication Identification

	later	(MCID) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification

Chapter 1

1 Introduction

1.1 Scope

This document is the standard for Generic Requirements (GR) of Fixed Wireless Access Customer Premises Equipment (FWA CPE), covering common features across 4G, 5G Non-Standalone (NSA), and 5G Standalone (SA) technologies. It also includes specific requirements that apply only to certain technologies. The requirements are grouped into important areas such as Radio/RRC/NAS, support for multiple APNs to separate different services, Quality of Service, Voice Services, Networking Features, Wi-Fi, IDU/ODU Interworking and Resilience, Device Management, and Security. For each area, it is clearly mentioned whether the requirement applies to Indoor FWA devices, Outdoor FWA devices, or both.

1.2 Overview

Fixed Wireless Access (FWA) has emerged as a widely adopted and cost-effective solution for providing ultrabroadband Internet, especially in areas where wireline infrastructure like FTTx has not been deployed. FWA uses wireless radio links to connect customers to a service provider’s mobile network using standardized 4G/4G+/5G technologies. A typical FWA setup includes either an indoor unit (1-box) or a combination of an indoor and outdoor unit (2-box solution). These devices offer end-users high-speed internet through Wi-Fi, Ethernet ports, and voice connectivity via FXS ports for analog phones.

While the radio interface (4G/5G) is standardized, several other critical features of FWA devices remain unstandardized. For example, remote management practices vary, with some operators using BBF TR-069/TR-369 and ACS platforms, while others rely on proprietary solutions. Voice service is another complex area—many FWA devices use VoLTE (IR.92 stack)/VoNR Stack, which is ideal for mobile phones but often lacks features needed for PSTN-like landline services. As a result, many operators deploy VoIP stacks, which require custom design, integration, and testing, increasing complexity and cost.

In 2-box FWA setups, the Outdoor Unit (ODU) connects to the mobile network, while the Indoor Unit (IDU) provides Wi-Fi, Ethernet, and voice services. These units typically connect via a Gigabit Ethernet cable with Power-over-Ethernet (PoE) to power the ODU. However, there is no open standard for the interface between IDU and ODU. Often, both units come from the same vendor and use proprietary protocols, limiting interoperability. Many operators now advocate for an open and standardized IDU-ODU interface to allow mixing and matching devices based on specific needs—such as consumer, ~~SMB~~, or enterprise use cases—thereby enabling greater flexibility and innovation.

1.3 Architecture

A FWA Device offers the typical features of a Home Router (also known as Residential Gateway) and connects to a 3GPP-based network via a Radio Interface.

The two architectural models considered in this document are: indoor FWA solution and outdoor FWA solution.

In the indoor FWA solution, a single box comprises all the functions and interfaces needed to deliver the Ultrabroadband Internet services to the end user.

In the outdoor FWA solution, the functions are split between an Outdoor Unit (ODU), which connects to the mobile network with the radio interface, and an Indoor Unit (IDU), which offers all the functions and interfaces for the LAN network: Wi-Fi access point, Voice interface, networking functions (e.g. port mapping, Firewall), etc.

While the indoor solution is clearly a single-tenant solution, different architectural alternatives are possible for outdoor FWA solutions.

In particular, outdoor solutions can be single-tenant or multi-tenant: in a single-tenant solution, an Outdoor Unit is dedicated to a single customer and is connected with a point-to-point link with an Indoor Unit. In a multi-tenant solution, an Outdoor Unit serves multiple customers, and several Indoor Units are connected to it.

Another possible option of the architecture of outdoor solutions is the interface between ODU and IDU. This document defines an open, standard interface between ODU and IDU; therefore, ODUs and IDUs from different manufacturers can be matched and combined.

1.3.1 Indoor FWA Solution

The Indoor FWA solution reference architecture is depicted in Figure 1.

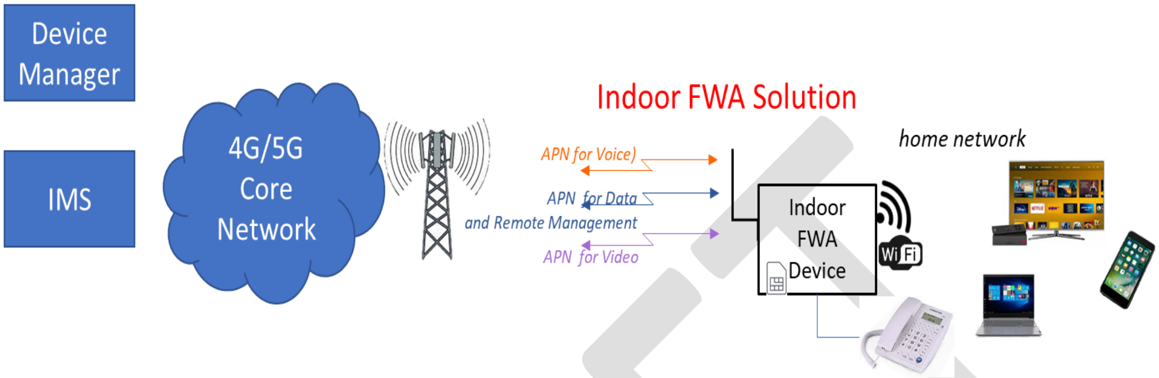

Figure 1: Indoor FWA Device Reference Architecture

The indoor FWA Device offers the following services:

- Internet Service (mandatory): ultra-broadband connectivity to the Internet. Ancillary functions to this connectivity are the possibility to configure VPN, Port Mapping, Firewall rules, NAT helpers (ALG, Application Layer Gateway), and to customize DNS servers.
- Voice Service (mandatory): the service is provided by the operator by means of VoIP or VoLTE technologies. In both cases, the Indoor FWA Device offers one or more Voice Interfaces to the end-user (typically, an FXS port) and interacts with the IMS Core of the Operator. These two flavours are both foreseen in this document as they represent valid industry standards for Voice service. The choice between the two standards may depend on legacies in the Operator's network, specific voice features requested by the market or regulatory obligations.
- Managed Video services (optional): Video on Demand (VOD) or Video Streaming service, managed by the Operator (also in partnership with one or more OTT Service Providers), which controls some of the transport features, in order to maximize the Quality of Experience (QoE) for the end user and the efficiency in network resources utilization.

An Indoor FWA Device may provide further services, e.g. Smart Home control, but they're outside the scope of this document, which focuses on the three services above.

The indoor FWA Device normally offers the following interfaces:

- LAN:
  - Ethernet: an FWA Device offers some Ethernet LAN interfaces, of which at least one LAN interface should be Gigabit Ethernet
  - Wi-Fi: an FWA Device offers Wi-Fi interface. Minimum performance requirements for Wi-Fi are detailed in the specific section.
- Voice Interfaces: an FWA Device must offer at least one analog FXS (Foreign eXchange Station) port, to be used in association with a single-line (that is, single-number, single-channel) profile. The availability of two or more FXS interfaces or more complex interfaces such as ISDN BRI (Basic Rate Interface) are normally associated to the use with more complex multi-line (multiple-number, multiple-channel) profiles.
- WAN: an FWA Device connects to the network via a radio/mobile interface (4G, 5G NSA, 5G SA). Different PDN connections are used to differentiate quality of service. The requirements are detailed in the specific section of this document.

An Indoor FWA Device is managed through a centralized Device Management platform. An example is a TR-069/TR-369 AutoConfiguration Server (ACS), operated by the Operator. The remote management serves different purposes, including:

- Provisioning: used to configure VoIP account and other VoIP-related parameters (such provisioning is not needed in case of VoLTE-based voice service), APN configurations, Wi-Fi customization and other provisioning activities.
- Assurance: used to perform assurance activities such as re-provisioning, reboot, factory reset, firmware upgrade.
- Monitoring: used to monitor Device operation and performance, for example Device status, VoIP registration status, Wi-Fi statistics and performance, Internet access performance measurements, radio parameters.

The Indoor FWA Device hosts one SIM which allows line identification and authorization to access the network.

1.3.2 Outdoor FWA Solution

The Outdoor FWA solution reference architecture is depicted in Figure 2.

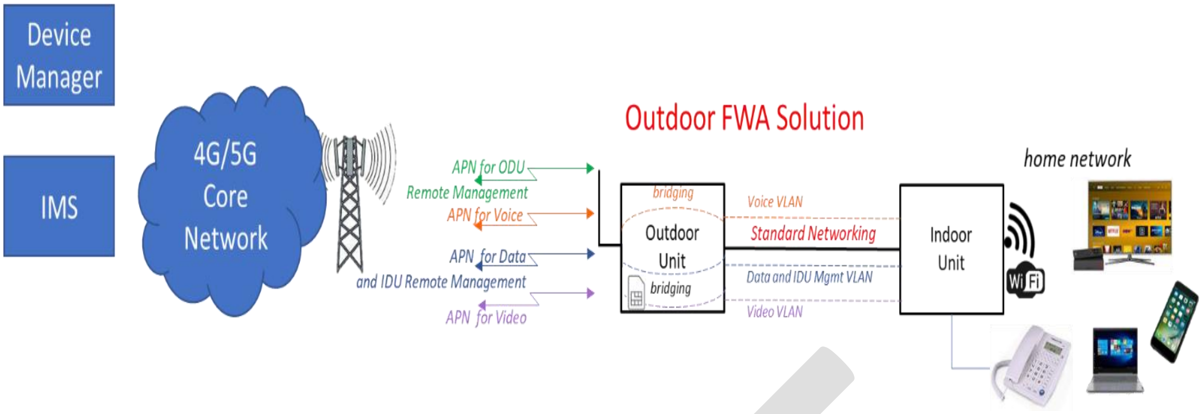

Figure 2: Outdoor FWA Device Reference Architecture

As mentioned at the beginning of the section, this document focuses only on an open, standard architecture between the Outdoor Unit (ODU) and Indoor Unit (IDU), so that ODU and IDU also from different manufacturers can be used together to achieve the Outdoor FWA Solution.

The Outdoor Unit:

- Hosts one physical SIM which allows line identification and authorization to access the network;
- Provides connectivity to the network, via a radio interface (4G, 5G NSA, 5G SA). Different PDN connections are used to differentiate quality of service. The requirements are detailed in the specific section of this document;
- Connects to the Indoor Unit, by means of an Ethernet Interface (at least Gigabit Ethernet), differentiating services by means of VLANs dedicated to Voice, Video and Data services, where each VLAN maps 1 :1 with a PDN connection;
- Is managed through a centralized Device Management platform. An example is a TR-069/TR-369 AutoConfiguration Server (ACS), operated by the Operator. The remote management serves different purposes, including:
  - Provisioning: used for APN configurations, VLAN configurations and other provisioning activities.
  - Assurance: used to perform assurance activities such as re-provisioning, reboot, factory reset, firmware upgrade, …

    - Monitoring: used to monitor Device operation and performance, for example Device status, Internet access performance measurements, radio parameters.
- Is normally powered through Power over Ethernet from a POE PSU to be installed indoor, which connects via Ethernet to the IDU;
- The AC power adapter shall be 3 pin and operate PoE power till 170v-260v
- Is suitable for outdoor installation. That is, the ODU and its accessories have Hardware, EMC and Security features suitable for outdoor installation and compliant to the current regulations of the country where they are installed.

The Indoor Unit:

- Connects to the Outdoor Unit, by means of an Ethernet Interface (at least Gigabit Ethernet), differentiating services by means of VLANs dedicated to Voice, Video and Data services, where each VLAN is mapped by the ODU 1:1 with a PDN connection;
- Offers the services normally offered from a Home Router/ Residential Gateway, that is the same services foreseen for the Indoor FWA Device: Internet access (mandatory), Voice (mandatory), managed Video service (optional);
- Offers the same LAN interfaces foreseen for the Indoor FWA Device;
- Is managed through a centralized Device Management platform. An example is a TR-69 AutoConfiguration Server (ACS), operated by the Operator. The remote management serves different purposes, including:
    - Provisioning: used to configure VoIP account and other VoIP-related parameters, VLAN configurations, Wi-Fi customization and other provisioning activities.
    - Assurance: used to perform assurance activities such as re-provisioning, reboot, factory reset, firmware upgrade etc.
    - Monitoring: used to monitor Device operation and performance, for example Device status, VoIP registration status, Wi-Fi statistics and performance, Internet access performance measurements.

In summary, the Indoor Unit of the Outdoor FWA Solution can be any Home Router/Residential Gateway compliant to the requirements detailed in the following sections, and in particular to the requirements for IDU/ODU interconnection. It is also very similar to an Indoor FWA Device, with the difference that the IDU of an Outdoor FWA Solution does not need a SIM and does not connect directly to the mobile network.

Chapter 2

2 Functional Requirements (Common)

2.1 Radio/RRC/NAS common requirements

2.1.1 The FWA device shall support one (1) SIM/USIM. FWA Devices with multiple SIMs are outside the scope of this document.

2.1.2 The FWA device may be equipped with one (1) eSIM, instead of a physical SIM.

2.1.3 The Indoor FWA Device (1-box solution) shall support the establishment of at least 3 PDNs/PDUs (e.g. for data/remote management, video, and voice services).

2.1.4 The Outdoor Unit of an Outdoor FWA Solution (2-box) shall support the establishment of at least 4 PDNs/PDUs (e.g. for remote management of ODU, data/remote management of IDU, video, and voice services).

2.1.5 The FWA Device shall allow configurable associations between PDN/PDU connections and services/applications (e.g. voice, video; VLAN settings via Web UI).

2.1.6 The FWA device should support the establishment of at least 6 PDNs/PDUs.

2.1.7 For each PDNs/PDUs, the FWA Device shall allow to configure:

a. Protocol stack (IPv4, IPv6, IPv4/v6);
b. Authentication option (PAP/CHAP);
c. MTU/MSS

2.2 Quality of Service

2.2.1 The FWA Device shall comply with the 3GPP standards 3GPP TS 23.207 and 3GPP TS 23.203, regardless of deployment scenario (e.g., 4G, 5G NSA, 5G SA).

2.2.2 If a wireless service provider utilizes customized QoS for specific category of subscribers including mission critical organizations, government entities and enterprise customers, the FWA device should comply with the wireless service provider’s requirements and mandates.

2.3 Voice Service

Voice Service requirements apply to the Indoor FWA Device and to the Indoor Unit of an Outdoor FWA Solution.

2.3.1 The Indoor FWA Device (1-box solution) shall support voice service either by means of VoLTE /VoNR technology or VoIP technology.

2.3.2 The Indoor Unit of an Outdoor FWA Solution (2-box) shall support voice service uniquely by means of VoIP technology.

2.3.3 In case of VoLTE/VoNR Technology, the FWA Device shall be compliant to GSMA IR.92 profile.

2.3.4 In case of VoNR Technology, the FWA Device shall be compliant to GSMA NG.114 profile.

2.3.5 In case of VoIP technology, the FWA Device shall be compliant to 3GPP specification 24.229, with the profile defined in the following sections 3.3.2, 3.3.3 and, optionally, 3.3.5 of GSMA TS.64 FWA Devices Architecture and Requirements Version 1.0.

2.3.6 In case of VoIP technology, the FWA Device shall request a dedicated PDN Connection. The PDN Connection for VoIP traffic may be characterized with a dedicated QCI.

Note: Voice Traffic includes SIP, RTP, RTCP and DNS traffic used to resolve the P-CSCF FQDN in order to get the P-CSCF addresses.

2.3.7 It shall be possible to disable all voice features.

2.3.8 The FWA Device shall be customizable in order not to have any FXS port or other voice interfaces

2.4 Networking Features

2.4.1 Interfaces

2.4.1.1 The indoor FWA Device and the Indoor Unit of an Outdoor FWA Solution shall support at least two Gigabit Ethernet LAN ports, compliant to IEEE 802.3ab standard.

2.4.1.2 For the physical interfaces for LAN Ethernet, the 10 100 1000BASE-T electrical interface should be used.

2.4.1.3 Different physical interfaces for LAN Ethernet, compliant to the standards, e.g. 10 100 1000BASE-TX, may be used in alternative to 10 100 1000BASE-T, depending on market and MNOs needs.

2.4.1.4 The Indoor Unit and the Outdoor Unit of an Outdoor FWA Solution shall have a connection coherent with the LAN-WAN capability of the Device.

2.4.1.5 For the physical interfaces for the IDU-ODU, if Ethernet is used, the BASE-T electrical interface should be used.

2.4.1.6 If Ethernet is used for the IDU-ODU connection, different physical interfaces, compliant to the standards, e.g. 1000BASE-TX, may be used in place of BASE-T, depending on market and MNOs needs.

2.4.2 Performance

2.4.2.1 The 4G FWA Device shall offer an aggregate throughput of at least 1 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.

2.4.2.2 The 4G FWA Device should offer an aggregate throughput of at least 2.5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.

2.4.2.3 The 5G FWA Device shall offer an aggregate throughput of at least 2.5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.

2.4.2.4 The 5G FWA Device should offer an aggregate throughput of at least 5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.

2.4.2.5 The 4G FWA Device shall offer a throughput LAN-WAN coherent with the LTE UE Category of the Device, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length and not affected by the local LAN-LAN throughput.

2.4.2.6 The 5G FWA Device shall offer a throughput LAN-WAN coherent with 5G cellular bandwidth of the FWA Device, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length and not affected by the local LAN-LAN throughput.

2.4.3 Protocols

2.4.3.1 The FWA Device shall support Internet Protocol version 4 (IPv4), defined in IETF RFC 791.

2.4.3.2 The FWA Device shall support Internet Protocol version 6 (IPv6), defined in IETF RFC 8200 and further amendments defined by IETF.

2.4.3.3 The FWA Device shall support Address Resolution Protocol (ARP), defined in IETF RFC 826 and further amendments (IETF RFC 5227, IETF RFC 5494).

2.4.3.4 The FWA Device shall support Network Discovery Protocol for IPv6 (NDP) defined in IETF RFC 4861 and further amendments defined by IETF.

2.4.3.5 The FWA Device shall support Internet Control Message Protocol (ICMP) defined in IETF RFC 792 and further amendments defined by IETF (RFC 950, RFC 4884, RFC 6633, RFC 6918).

2.4.3.6 The FWA Device shall support Internet Control Message Protocol version 6 for IPv6 (ICMPv6) defined in IETF RFC 4443.

2.4.3.7 The FWA Device shall implement a Network Time Protocol (NTP) client as defined in IETF RFC 5905 and further amendments.

2.4.3.8 The FWA Device shall support Internet Group Management Protocol, version 3 (IGMPv3), defined in IETF RFC 3376.

2.4.3.9 The FWA Device shall support IGMP Proxy as defined in IETF RFC 4605.

2.4.3.10 The FWA Device shall supports QoS Treatment both at level 2 (p-bits of 802.1q VLAN Tag) and at level 3 (Differentiated Services Code Point of the IP header).

2.4.3.11 The FWA Device shall support the Differentiated Services (DiffServ) architecture and behaviors defined in RFC 2474, 2475, 2597, 3246 and 3260.

2.4.3.12 The behaviors of traffic classification, marking, remarking, queuing, scheduling, policing, shaping shall be applicable both to internally generated traffic and to traffic coming from LAN and destined to the WAN.

2.4.3.13 At least four queues shall be supported on the WAN interface, of which one with Strict Priority scheduling, and the others with configurable scheduling mechanisms (e.g. Weighted Fair Queuing, Weighted Round Robin).

2.4.3.14 The FWA Device should support a secondary IPv4 addressing on LAN, in order to enable the assignment of public IP addresses to hosts in LAN.

2.4.3.15 The FWA Device shall support VLAN Tagging, compliant to IEEE 802.1q standard.

2.4.4 DHCP

2.4.4.1 The FWA Device shall support Dynamic Host Configuration Protocol (DHCP) defined in IETF RFC 2131.

2.4.4.2 The FWA Device shall support DHCP Options defined in IETF RFC 2132.

2.4.4.3 The FWA device may implement DHCP options 60 and 43 for automatic provision of ACS parameters.

2.4.4.4 In case of multiple connections from the same FWA device, FWA device shall implement DHCP option 82 and 37 for client identifications and policy enforcement.

2.4.4.5 The DHCP Server implemented by the FWA Device shall manage at least 254 addresses.

2.4.4.6 It shall be possible to define any IPv4 Unicast subnet for the private LAN and DHCP pool.

2.4.4.7 The DHCP Server implemented by the FWA Device shall support Duplicate Address Detection (DAD) functionality.

2.4.4.8 The DHCP Server implemented by the FWA Device shall provide a mechanism for IP reservation on MAC Address basis, assigning the same IP address (if available) at the same MAC Address.

2.4.4.9 The FWA Device shall support hostnames presented by the hosts (DHCP clients) with DHCP Option 12.

2.4.4.10 The FWA Device shall properly manage the cases of overlapping hostnames and hostnames not presented by clients, by assigning to client’s unambiguous hostnames by means of Option 12.

2.4.4.11 The FWA Device shall support Dynamic Host Configuration Protocol for IPv6 (DHCPv6) defined in IETF RFC 8415.

2.4.4.12 The FWA Device shall support Prefix Delegation for IPv6 (DHCPv6) defined in IETF RFC 8415.

2.4.4.13 The FWA Device shall support Prefix Exclude for IPv6 (DHCPv6) defined in IETF RFC 8415.

2.4.5 NAT & Bridge operation

2.4.5.1 The FWA Device shall support IP Network Address Translator (NAT) as defined in IETF RFC 3022.

2.4.5.2 The Network Address Translator functionality implemented by the FWA Device shall be compliant to the behaviors defined in IETF RFC 4787.

2.4.5.3 The FWA Device shall implement a configurable Port Mapping/Virtual Server functionality, allowing the creation of entries for mapping protocols/ports on the WAN side of the FWA Device to an IP address and protocols/ports on the private LAN.

2.4.5.4 It shall be possible to configure at least 32 Port Mapping entries.

2.4.5.5 The FWA Device shall support Customer-side Translator (CLAT) functionality according to IETF RFC 6145

2.4.5.6 The FWA Device shall support operation in Bridge Mode. In this configuration both DHCP and NAT operations are provided by the network being bridged to.

2.4.5.7 The FWA Device shall implement a configurable Application Layer Gateway functionality (ALG), as defined in IETF RFC 2663, at least for the following protocols: SIP, IPSec, PPTP, L2TP.

2.4.6 MTU

2.4.6.1 The FWA Device shall support a default MTU size of 1380 bytes.

2.4.6.2 The FWA Device shall support network override of the default MTU size in IPv4 operation via Protocol Configuration Options (3GPP TS 24.008).

2.4.6.3 The FWA Device shall support network override of the default MTU size in IPv6 operation via Router Advertisement.

2.4.7 DNS

2.4.7.1 The FWA Device shall support Domain Name System (DNS) compliant to IETF RFC 1034, RFC 1035 and further amendments defined by IETF

2.4.7.2 The FWA Device shall be able, on a configuration basis, to act as DNS Server for the Hosts in LAN.

2.4.7.3 The FWA Device shall be able to advertise the DNS server(s) to the Hosts in LAN via DHCP protocol. On a configuration basis, the advertised DNS server(s) can be:

a. The FWA Device itself, if it’s configured to act as a DNS Server;

b. The DNS server addresses received from the network, if the FWA Device is not configured to act as a DNS Server;

c. Optionally, other DNS Server addresses configured on the FWA Device.

2.4.7.4 The FWA Device shall support a configurable Dynamic DNS (DDNS) Service, allowing the FWA Device to be addressable from the Internet with an FQDN.

2.4.7.5 For the Dynamic DNS service, the FWA Device shall send updates to the DDNS server not periodically, but only whenever an IP address change is detected on the Data WAN Interface.

2.4.7.6 For Static DNS operation the FWA Device shall support Recursive DNS and not Iterative DNS.

2.4.7.7 The FWA Device shall support unencrypted DNS access.

2.4.7.8 The FWA Device shall support DNS access via HTTPS (IETF RFC 8484).

2.4.7.9 The FWA Device shall support DNS access via TLS.

2.4.7.10 The FWA device shall be protected against DNS Rebind Vulnerability.

2.4.7.11 To prevent DNS spoofing, source ports and Transaction-IDs shall be selected randomly by the CPE.

2.4.8 Security

2.4.8.1 The FWA Device shall implement a configurable DeMilitarized Zone (DMZ) functionality, allowing an internal host in LAN to be fully exposed on WAN.

2.4.8.2 The FWA Device shall implement a configurable Port Binding functionality, allowing binding of the WAN connections to none, one or more LAN interfaces (including Wi-Fi SSIDs).

2.4.8.3 The FWA Device shall implement a configurable Filtering functionality, allowing the creation of entries for blocking/allowing the communication of MAC Addresses on LAN towards specific IP address/range, on specific protocols/ports/port range.

2.4.8.4 It shall be possible to configure at least 32 Filtering entries.

2.4.8.5 The FWA Device should implement a configurable (on/off) UPnP Discovery functionality, compliant with the UPnP Forum's Device Architecture and Device Control Protocols standards.

2.4.8.6 UPnP functionality shall be blocked on the WAN side.

2.4.8.7 If the FWA Device supports UPnP, it should be disabled in Factory default configuration.

2.4.8.8 If the FWA Device supports UPnP, rules created for one client device shall apply only to that device and not to other LAN clients (also for the FWA Device itself).

2.4.8.9 The FWA Device should implement a configurable VPN functionality, both as a VPN-client and a VPN-server, with L2TP/IPSec PSK or PPTP.

2.4.8.10 The FWA Device shall implement a Parental Control functionality, letting the user to configure a list of URLs which access must be denied to all (or a configurable subset of) LAN hosts.

2.4.8.11 The FWA Device shall implement a per-user device configurable Internet access control functionality, letting the user to configure, for a selected user device, which days of the week/which hours of the day or how many hours per day the Internet access must be allowed/denied.

2.4.8.12 The FWA Device shall implement a configurable (at least with on/off behaviors) stateful IPv4 Firewall.

2.4.8.13 The FWA Device shall implement Denial of Service (DoS) protection functionality.

2.4.8.14 The DoS functionality shall remain enabled even when the Firewall has been disabled by user configuration.

2.4.8.15 The behavior of the FWA Device to ICMP messages coming from WAN interface shall be configurable.

2.4.8.16 The FWA Device shall implement a configurable (at least with on/off behaviors) stateful IPv6 Firewall.

2.4.8.17 The IPv6 and IPv4 firewall shall be independently configurable.

2.4.8.18 The IPv6 and IPv4 firewall status shall be presented independently.

2.4.8.19 The FWA Device shall NOT allow outgoing traffic originated from a LAN IP address outside the range defined by the FWA Device itself.

2.4.8.20 In Factory Reset condition, the status of the firewall shall be enabled.

2.4.8.21 The FWA CPE device shall comply to the security requirements mentioned in the applicable Indian Telecommunication Security Assurance Requirements (ITSAR) as and when notified by National Centre for communication Security (NCCS).

2.4.9 Customisation

2.4.9.1 It shall be possible for a MNO to customize a FWA Device in addition to the requirements mentioned.

2.4.10 USB Port

2.4.10.1 The FWA Device may support a Universal Serial Bus (USB) interface.

2.4.10.2 The USB interface shall be compliant to the Universal Serial Bus Specification version 3.1 or higher.

2.4.10.3 The USB Interface receptacle shall be any of Type-A, Type-Micro B or Type-C.

2.4.10.4 The USB Interface should supply a current of at least 1.5A.

2.4.10.5 The FWA Device shall integrate the USB Mass Storage Device Class driver, to provide the automatic detection of an USB Mass Storage (such as Hard Disk, CD/DVD ROM, USB memory stick, etc.) connected to the USB Host Port.

2.4.10.6 The FWA Device shall integrate the USB Printer Device Class driver, to provide the automatic detection of an USB Printer connected to the USB Host Port.

2.4.10.7 The FWA Device should use SMBv2 (or higher) protocol to enable the sharing of an USB Mass Storage Hard Disk Devices between LAN hosts.

2.4.10.8 The FWA Device should use SMBv2 (or higher) protocol to enable the print sharing between the LAN hosts, supporting the standard error messages via SMB protocol.

2.4.10.9 The FWA Device shall NOT support SMBv1 protocol.

2.4.10.10 The USB Interface shall block firmware upgrade, logging, tracing and similar local management and troubleshooting activities on the FWA Device.

2.5 WIFI (As per tenderer requirements)

2.5.1 Standards

2.5.1.1 The FWA Device shall integrate a Wi-Fi 4 (IEEE 802.11n) Access Point (AP), or later standards, operating on 2.4 GHz bands.

2.5.1.2 The FWA Device shall integrate a Wi-Fi 5 (IEEE 802.11ac) Access Point (AP), or later standards, operating on 5 GHz bands.

2.5.1.3 The FWA Device should integrate a Wi-Fi 6 (IEEE 802.11ax) Access Point (AP), or later standards, operating on both 2.4 and 5 GHz bands.

2.5.1.4 The FWA Device may integrate a Wi-Fi 6E (IEEE 802.11ax) Access Point (AP), or later standards, operating on 2.4, 5 and 6 GHz bands.

2.5.1.5 The FWA Device may integrate a Wi-Fi 7 (IEEE 802.11be) Access Point (AP), or later standards, operating on 2.4,5 and 6 GHz bands.

2.5.1.6 The Wi-Fi AP of a FWA Device shall comply to the TEC ER of WiFi Access Point and CPE.

2.5.1.7 The FWA Device shall be certified (WFA Certification Program): Wi-Fi CERTIFIED 5.

2.5.1.8 If Wi-Fi 6 is supported, the FWA Device shall be certified (WFA Certification Program): Wi-Fi CERTIFIED 6.

2.5.1.9 The FWA Device shall be certified (WFA Certification Program): WPA3.

2.5.1.10 The FWA Device shall be certified (WFA Certification Program): Wi-Fi Protected Setup (PBC).

2.5.2 MIMO Capabilities, Bandwidth, Modulation and Coding schemes

2.5.2.1 The Wi-Fi AP of a FWA Device shall support at least MIMO 2x2 on all supported frequency bands.

2.5.2.2 The Wi-Fi AP of a FWA Device should support MIMO 4x4 on all supported frequency bands.

2.5.2.3 The Wi-Fi AP of a FWA Device may support MIMO higher than 4x4 on some or all supported frequency bands.

2.5.2.4 An 802.11n AP of a FWA Device shall support a bandwidth of 40 MHz.

2.5.2.5 An 802.11ac AP of a FWA Device shall support a bandwidth of 80 MHz in the 5 GHz band.

2.5.2.6 An 802.11ax AP of a FWA Device shall support a bandwidth of 40 MHz in the 2.4 GHz band.

2.5.2.7 An 802.11ax AP of a FWA Device shall support a bandwidth of 80 MHz in the 5 GHz band.

2.5.2.8 An 802.11ax AP of a FWA Device should support a bandwidth of 160 MHz in the 5 GHz band.

2.5.2.9 An 802.11ax (Wi-Fi 6E) AP of a FWA Device shall support a bandwidth of 160 MHz in the 6 GHz band, if supported.

2.5.2.10 An 802.11n AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 64-QAM with coding 5/6.

2.5.2.11 An 802.11ac AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 256-QAM with coding 5/6.

2.5.2.12 An 802.11ax AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 1024-QAM with coding 5/6.

2.5.3 Performance

2.5.3.1 The AP of a FWA Device shall offer a throughput coherent with the theoretical maximum physical bit rate attainable by the AP characteristics, at least 70% of Maximum Physical Speed with TCP and UDP traffic in a “clean” environment.

2.5.3.2 All the Wi-Fi interfaces shall NOT exceed the regulatory limits as defined by WPC regards output power level (EIRP).

2.5.3.3 FWA device shall have the capability to perform the speedTest or other equivalent measures of initiating throughput tests by the Service Provider.

2.5.4 Service Set Identifier (SSID)

2.5.4.1 The AP of a FWA Device shall permit the configuration of one main SSID for each supported band.

2.5.4.2 The AP of a FWA Device shall permit the configuration of at least one guest SSID.

2.5.4.3 The guest SSID(s) shall NOT permit the access to the configuration of the FWA Device.

2.5.4.4 The guest SSID(s) shall NOT permit traffic between hosts in LAN.

2.5.4.5 Each SSID shall be configurable to operate on one or more frequency bands.

2.5.4.6 Each SSID shall be configurable as regards the Authentication and Security mechanisms adopted.

2.5.4.7 Each SSID shall be configurable as regards the SSID broadcasting.

2.5.4.8 The default configuration of the FWA Device shall be with the same SSID for all supported bands.

2.5.4.9 Based on MNO requirements, in the default configuration, the SSIDs may have an unambiguous, not-repeating value for each deployed FWA Device and not contain any information that consist of or are derived from data or parts of data that depend on the FWA device model itself.

2.5.5 Channel and Bandwidth Selection

2.5.5.1 The AP of a FWA Device shall permit the manual channel selection on all supported bands.

2.5.5.2 The AP of a FWA Device shall support Automatic Channel Selection on all supported bands, in order to select the less interfered channels.

2.5.5.3 If enabled, the Automatic Channel Selection shall be performed every time the AP is turned on.

2.5.5.4 The AP of a FWA Device shall support Periodic Automatic Channel Selection.

2.5.5.5 The default value for Periodic Automatic Channel Selection should be 24 hours.

2.5.5.6 The Periodic Automatic Channel Selection shall be configurable by the MNO through customization.

2.5.5.7 The AP of a FWA Device shall permit the manual Bandwidth selection on all supported bands.

2.5.5.8 The AP of a FWA Device shall support Automatic Bandwidth Selection on all supported bands.

2.5.6 Clients

2.5.6.1 The AP of a FWA Device shall support at least 64 clients.

2.5.7 Security

The Security related requirements for the WiFi Access point shall comply with ITSAR Number: ITSAR702042504 (Group-IV Devices Common Security Requirements ITSAR) which covers Wi-Fi CPE (Customer Premises Equipment) device.

2.5.8 The AP of a FWA Device may support WPS with Push Button mode in order to facilitate the association between clients and the AP of the FWA Device. If present, WPS shall be disabled by default and enabled only with full awareness of risks and only when physical access is strictly controlled.

2.5.9 The AP of a FWA Device shall support IEEE 802.11k industry standard for radio resource measurement

2.5.10 The AP of a FWA Device shall support Band Steering to steer clients from the more congested 2.4 GHz band to the less congested bands (5 GHz, and 6GHz if supported).

2.5.11 The Band Steering feature shall be manually configurable (ON/OFF selection).

2.5.12 The AP of a FWA Device shall comply to the Wi-Fi Alliance Easy Mesh™ R2 (or later) standard.

2.5.13 The Wi-Fi Diagnostic solution shall collect data also from the other APs connected in mesh, as well as from the clients connected to those APs.

2.5.14 The AP of a FWA Device should support Wi-Fi Alliance Wireless Multimedia Extensions™ (WME™), also known as Wi-Fi Multimedia™ (WMM™), in order to prioritize traffic in the Wireless Network according to Access Categories.

2.5.15 If WMM™ is supported; the FWA Device shall provide the mechanism to enable/disable the feature and to configure the mappings (Access Categories vs DSCP).

2.5.16 It shall be possible for a MNO to customize the settings of a FWA Device as regards Wi-Fi region/country of operation, enabled bands and channels, power transmission limits, SSIDs, passphrases.

2.6 IDU/ODU Interworking and Resilience

2.6.1 Common requirements to bridged and routed modes of operation

2.6.1.1 The Outdoor Unit (ODU) in an Outdoor FWA Solution, shall be able to map the traffic received on each PDN Connection / PDU Session, on different VLANs over the interface with the Indoor Unit (IDU), and vice versa.

2.6.1.2 The IDU shall be able to map the different traffic generated by the IDU itself or by hosts in LAN, and destined to the WAN, on different VLANs over the interface with the ODU, based on Service/VLAN mapping rules defined on the IDU.

2.6.1.3 The ODU shall be configurable in order to operate on each VLAN, either in bridged mode or in routed mode.

2.6.1.4 The ODU shall allow to configure one PDN connection / PDU session to be locally terminated in the ODU itself, that is to operate in routed mode without being mapped on a VLAN with the IDU.

Note: for example, this connection may be dedicated to ODU Remote Management.

2.6.2 ODU Bridged mode operation.

2.6.2.1 The Outdoor Unit (ODU) shall be able to operate in bridged mode, over one or more PDNs-PDUs/VLANs.

2.6.2.2 In bridged mode operation, the ODU shall use DHCP/DHCPv6 to assign to the IDU, on each VLAN, the network parameters received from the mobile network over a PDN/PDU

a. IP Address

b. DNS Servers IP Addresses (DHCP Option 6)

Therefore, in bridge mode operation, the IP Address received on each PDN/PDU from the network, is not retained on the ODU itself, but is assigned to the IDU on the VLAN corresponding to that PDN/PDU.

2.6.2.3 The ODU shall define, for each VLAN, the following parameters:

a. Subnet Mask

b. Default Gateway

c. and assign them to the IDU by means of DHCP/DHCPv6.

Note 1: this is needed because the mobile network does not provide a UE (specifically, the ODU) with such parameters over a PDN/PDU, while they are needed to properly configure the IDU with DHCP/DHCPv6.

Note 2: Subnet Mask is DHCP Option 1, Default Gateway is DHCP Option 3 (Router).

2.6.2.4 The ODU may define:

a. For the Subnet Mask, a /30 (255.255.255.252)

b. For the Default Gateway, the IP Address immediately after or before the one assigned to the IDU on each VLAN, following the rules of the Classless Inter-Domain Routing (CIDR).

2.6.3 Reliability of IDU-ODU operation

2.6.3.1 If an APN is configured in bridged mode, the ODU shall guarantee that the IDU IP configuration will always be the same of the WAN (mobile) IP configuration.

2.6.3.2 As soon as the WAN (mobile) IP connection state changes, the ODU shall trigger the IDU IP Address renewal by means of a reset of the physical interface with the IDU.

2.6.4 ODU Routed mode operation

2.6.4.1 The Outdoor Unit (ODU) shall be able to operate in routed mode, over one or more PDNs-PDUs/VLANs.

2.6.4.2 In routed mode operation, the ODU shall retain for itself the IP Address received from the mobile network over a APN/DNN.

2.6.4.3 In routed mode operation, the ODU shall be able to configure the IP Address of the IDU, on each VLAN configured in routed mode, by means of DHCP, using a private IP address pool.

2.6.4.4 In routed mode operation, if DHCP is used, then ODU shall provide via DHCP also:

a. The DNS Server IP Address(es), which can be either the ODU itself or the Servers received from network;

b. The Default Gateway (Router), which is the IP Address of the ODU over the IDU-ODU connection.

2.6.4.5 In routed mode operation, the ODU shall be able to manage statically configured addresses for:

a. The IP Address of the IDU over the IDU-ODU connection: this is a directly connected interface

b. The LAN of the IDU: this will be a subnet routed through the IP Address of the IDU.

Note: static IP Addressing, for the IDU-ODU connection, can be used as an alternative to DHCP.

2.6.4.6 In routed mode operation, the ODU shall perform NAT of traffic coming from the IDU and destined to the Network.

2.6.5 Tunnels / VPNs

2.6.5.1 The IDU shall be able to establish, through the ODU, one or more Tunnels or VPN connections, based on IPSec or PPTP or GRE, over one or more VLANs, towards Tunnel/VPN Terminators in the network.

CHAPTER 3

3 Specific Functional Requirements

3.1 For 5G NSA FWA Devices

3.1.1 The FWA device shall support standardized QCIs as specified in 3GPP TS 23.203

3.1.2 The FWA device should support operator-specific QCIs as specified in 3GPP TS 23.203

3.1.3 The FWA device shall be compliant with 3GPP E-UTRAN and NR Access Stratum Release 16 baseline or later.

3.1.4 The FWA device shall support periodical ANR measurements for reporting via the 4G network the Strongest NR Cells and related CGI (Cell Global Identity) when in ENDC operation.

3.1.5 The FWA device should support periodical inter-RAT ANR measurements for reporting via the 4G network the Strongest NR Cells and related CGI (Cell Global Identity) when not in ENDC operation.

3.1.6 The FWA device shall support periodical inter-RAT ANR measurements for reporting via the NR network the Strongest 4G Cells and related CGI (Cell Global Identity).

3.1.7 The FWA device shall support periodical intra-RAT ANR measurements for reporting via the NR network the Strongest NR Cells and related CGI (Cell Global Identity).

3.1.8 The FWA device shall be compliant to GSMA TS.24 for Antenna Performance acceptance values

3.1.9 Radio/RRC/NAS specific requirements for 5G-FR1 NSA FWA devices

3.1.9.1 The FWA device shall support EN-DC (Option 3x).

3.1.9.2 The FWA device shall support DSS technology.

3.1.9.3 The FWA device shall support rateMatchingResrcSetSemi-Static Information element in the Capability Information message.

3.1.9.4 The FWA device shall support rateMatchingResrcSetDynamic Information element in the Capability Information message.

3.1.9.5 The FWA device shall support rateMatchingLTE-CRS Information element at least for one FDD mid-band (e.g. n1, n3) in the Capability Information message.

3.1.9.6 The FWA device should support AdditionalDMRS-DL-Alt Information element in the Capability Information message.

3.1.9.7 The FWA device shall support NR SRS antenna switching 1T4R in 5G NR TDD high-bands (e.g. n77/n78).

3.1.9.8 The FWA device shall support NR SRS antenna switching 1T2R in 5G NR TDD mid- and low-bands.

3.1.9.9 The FWA device should support 2DL NR Inter-Band Carrier Aggregation.

3.1.9.10 The FWA device shall support UL split bearer to transmit concurrently on LTE and NR.

3.1.9.11 The FWA device shall support MIMO 4x4 DL capability on NR mid-bands (e.g. NR bands n77/n78).

3.1.9.12 The FWA device shall support 4Rx diversity on NR bands.

3.1.9.13 The FWA device should support 8Rx diversity on NR bands.

3.1.9.14 The FWA device may support more than 8Rx diversity on NR bands.

3.1.9.15 The FWA device shall support 256QAM modulation for downlink.

3.1.9.16 The FWA device shall support 64QAM modulation for uplink.

3.1.9.17 The FWA device should support 256QAM modulation for uplink.

3.1.9.18 The FWA device shall support power class 3 (23 dBm).

3.1.9.19 The FWA device should support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1

3.1.9.20 The FWA device should support power class 1.5 (29 dBm) in compliance with 3GPP TS 38.101-1

3.1.9.21 The FWA device shall support 15 kHz Sub-Carrier Spacing in FR1 NR bands.

3.1.9.22 The FWA device shall support 30 kHz Sub-Carrier Spacing in FR1 NR bands. The FWA device shall support 30 kHz Sub-Carrier Spacing in FR1 NR bands.

3.1.9.23 The FWA device Should support all 3GPP Channel Bandwidths defined for N78/N77

3.1.10 Radio/RRC/NAS specific requirements for 5G-FR2 NSA FWA devices

3.1.10.1 The FWA device shall support EN-DC (Option 3x)

3.1.10.2 The FWA device shall support 2DL contiguous NR Carrier Aggregation.

3.1.10.3 The FWA device should support 2UL contiguous NR Carrier Aggregation

3.1.10.4 The FWA device shall support UL split bearer to transmit concurrently on LTE and NR.

3.1.10.5 The FWA device shall support MIMO 2 x 2 DL capabilities on NR FR2 bands (e.g., NR bands n257/n258).

3.1.10.6 The FWA device should support MIMO 4 x 4 DL capabilities on NR FR2 bands (e.g., NR bands n257/n258).

3.1.10.7 The FWA device shall support 64QAM modulation for downlink

3.1.10.8 The FWA device should support 256QAM modulation for downlink.

3.1.10.9 The FWA device shall support 64QAM modulation for uplink.

3.1.10.10 The FWA device should support 256QAM modulation for uplink.

3.1.10.11 The FWA device shall support power class 3 (23 dBm).

3.1.10.12 The FWA device should support power class 2 (26 dBm).

3.1.10.13 The FWA device should support power class 1 (31 dBm).

3.1.10.14 The FWA device shall support 100 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).

3.1.10.15 The FWA device should support 200 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).

3.1.10.16 The FWA device should support 400 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).

3.1.10.17 The FWA device shall support Cell Carriers with ax50Mhz + bx100MHz channel bandwidth in FR2 NR TDD bands (i.e N258 , N257) , where a & b represents integer numbers

3.1.10.18 The FWA device shall support 60 KHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).

3.1.10.19 The FWA device shall support 120 KHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).

3.1.11 Antenna Performance Acceptance Values for 5G NSA FWA devices

3.1.11.1 The FWA device shall be compliant to TS.24for Antenna Performance acceptance values

3.2 For 5G SA FWA Devices

3.2.1 The FWA device shall support Option 2 SA deployment option

3.2.2 The FWA device should support Option 4 NSA deployment option.

3.2.3 The FWA device shall be compliant with 3GPP NR Access Stratum Release 16 baseline or later

3.2.4 The FWA device shall support standardized 5QIs as specified in 3GPP TS 23.501

3.2.5 The FWA device shall support NEA0 Null Encryption Algorithm

3.2.6 The FWA device shall support 128-NEA1 New radio Encryption Algorithm (based on SNOW 3G algorithm).

3.2.7 The FWA device shall support 128-NEA2 New radio Encryption Algorithm (based on AES algorithm)

3.2.8 The FWA device should support 128-NEA3 New radio Encryption Algorithm (based on ZUC algorithm).

3.2.9 The FWA device shall support 128-NIA1 New radio Integrity Algorithm (based on SNOW 3G algorithm).

3.2.10 The FWA device shall support 128-NIA2 New radio Integrity Algorithm (based on AES algorithm).

3.2.11 The FWA device should support 128-NIA3 New radio Integrity Algorithm (based on ZUC algorithm).

3.2.12 The FWA device shall support 5G-AKA Authentication Protocol Algorithm.

3.2.13 The FWA device shall support EAP-AKA Authentication Protocol Algorithm.

3.2.14 The FWA device shall support Initial 5GC Registration with SUCI, as per 3GPP TS 24.501

3.2.15 The FWA device may support 5G Slicing User Equipment Route Selection Policy (URSP) parameters.

3.2.16 The FWA device shall be compliant to GSMA TS.24 for Antenna Performance acceptance values

3.2.17 The FWA device may support 5G Slicing Network Slice Selection Assistance Information (NSSAI) parameters, as per 3GPP TS 24.501

3.2.18 The FWA device may support SST (Slice/Service Type) and SD (Slice Differentiator) parameters.

3.2.19 The FWA device may support standardized SST values, as specified in 3GPP TS 23.501

3.2.19.1 The FWA device should support all 3GPP Channel Bandwidths defined for N78/N77

3.2.20 Radio/RRC/NAS specific requirements for 5G-FR1 SA FWA devices

3.2.20.1 The FWA device shall support SA option of connectivity to 5GC with Option-2 Architecture

3.2.20.2 The FWA device shall support 2DL NR Carrier Aggregation.

3.2.20.3 The FWA Device shall support all combinations of FDD and TDD duplexing (i.e., 2F, 2T, F+T and T+F) in 2DL NR Carrier Aggregation.

3.2.20.4 The FWA device should support 3DL NR Carrier Aggregation.

3.2.20.5 The FWA device may support 4DL NR Carrier Aggregation or higher order.

3.2.20.6 The FWA device should support 2UL NR Carrier Aggregation

3.2.20.7 The FWA device shall support 15 kHz Sub-Carrier Spacing in FR1 NR bands.

3.2.20.8 The FWA device shall support 30 kHz Sub-Carrier Spacing in FR1 NR bands.

3.2.20.9 The FWA device shall support MIMO 4x4 DL capability on NR high-bands (e.g. NR bands n77/n78).

3.2.20.10 The FWA device shall support MIMO 2x2 UL capability on NR high-bands (e.g. NR bands n77/n78).

3.2.20.11 The FWA device shall support 4Rx diversity on NR bands.

3.2.20.12 The FWA device should support 8Rx diversity on NR bands

3.2.20.13 The FWA device may support more than 8Rx diversity on NR bands

3.2.20.14 The FWA device shall support 256QAM modulation for downlink

3.2.20.15 The FWA device may support 1024QAM modulation for downlink on NR TDD FR1 high-bands (e.g. n77/n78).

3.2.20.16 The FWA device shall support 64QAM modulation for uplink.

3.2.20.17 The FWA device should support 256QAM modulation for uplink

3.2.20.18 The FWA device shall support power class 3 (23 dBm).

3.2.20.19 The FWA device should support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1

3.2.20.20 The FWA device should support power class 1.5 (29 dBm) in compliance with 3GPP TS 38.101-1.

3.2.21 Radio/RRC/NAS specific requirements for 5G-FR2 SA FWA devices

3.2.21.1 The FWA device shall support SA option of connectivity to 5GC with Option-2 Architecture

3.2.21.2 The FWA device shall support 2DL intra-band contiguous NR Carrier Aggregation

3.2.21.3 The FWA device should support 4DL intra-band contiguous NR Carrier Aggregation

3.2.21.4 The FWA device should support 8DL intra-band contiguous NR Carrier Aggregation

3.2.21.5 The FWA device should support 2UL intra-band contiguous NR Carrier Aggregation.

3.2.21.6 The FWA device may support 4UL intra-band contiguous NR Carrier Aggregation

3.2.21.7 The FWA device shall support 100 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).

3.2.21.8 The FWA device should support 200 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).

3.2.21.9 The FWA device should support 400 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).

3.2.21.10 The FWA device shall support Cell Carriers with [a x 50Mhz + b x100MHz] channel bandwidth in FR2 NR TDD bands (i.e N258 , N257) , where a & b represents integer numbers

3.2.21.11 The FWA device shall support 60 kHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).

3.2.21.12 The FWA device shall support 120 kHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).

3.2.21.13 The FWA device shall support MIMO 2x2 DL capability on NR FR2 bands (e.g., NR bands n257/n258)

3.2.21.14 The FWA device should support MIMO 4x4 DL capability on NR FR2 bands (e.g., NR bands n257/n258).

3.2.21.15 The FWA device shall support 64QAM modulation for downlink

3.2.21.16 The FWA device should support 256QAM modulation for downlink

3.2.21.17 The FWA device shall support 64QAM modulation for uplink

3.2.21.18 The FWA device should support 256QAM modulation for uplink

3.2.21.19 The FWA device shall support power class 3 (23 dBm).

3.2.21.20 The FWA device should support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1

3.2.21.21 The FWA device should support power class 1 (31 dBm) in compliance with 3GPP TS 38.101-1.

3.3 For 4G FWA Devices

3.3.1 Radio/RRC/NAS specific requirements for 4G FWA devices

3.3.1.1 The FWA device shall be compliant with 3GPP E-UTRAN Access Stratum Release 12 baseline or later

3.3.1.2 The FWA device shall support EEA0 Null Encryption Algorithm.

3.3.1.3 The FWA device shall support 128-EEA1 EPS Encryption Algorithm (based on SNOW 3G algorithm) for both RRC signalling ciphering and User Plane ciphering.

3.3.1.4 The FWA device shall support 128-EEA2 EPS Encryption Algorithm (based on AES algorithm) for both RRC signalling ciphering and User Plane ciphering.

3.3.1.5 The FWA device should support 128-EEA3 EPS Encryption Algorithm (based on ZUC algorithm) for both RRC signalling ciphering and User Plane ciphering.

3.3.1.6 The FWA device shall support EIA0 Null Integrity Algorithm.

3.3.1.7 The FWA device shall support 128-EIA1 EPS Integrity Algorithm (based on SNOW 3G algorithm) for both RRC and NAS signalling integrity protection.

3.3.1.8 The FWA device shall be compliant to GSMA TS.24 for Antenna Performance acceptance values

3.3.1.9 The FWA device shall support 128-EIA2 EPS Integrity Algorithm (based on AES algorithm) for both RRC and NAS signalling integrity protection.

3.3.1.10 The FWA device should support 128-EIA3 EPS Integrity Algorithm (based on ZUC algorithm) for both RRC and NAS signalling integrity protection.

3.3.1.11 The FWA device shall support EPS-AKA Authentication Protocol.

3.3.1.12 In order to support the transmission techniques reported above, the FWA device shall support ue-CategoryDL 11 and ue-CategoryUL 5 or higher and all fallback configurations foreseen by the standard.

3.3.1.13 The FWA device should support ue-CategoryDL 12 and ue-CategoryUL 13 (Uplink CA support) or higher and all fallback configurations foreseen by the standard.

3.3.1.14 The FWA device shall support at least 3DL LTE Carrier Aggregation capability

3.3.1.15 The FWA device should support 2UL LTE Carrier Aggregation capability

3.3.1.16 The FWA device shall support MIMO 4x4 capability at least on one LTE mid-band (e.g., LTE B3 for Europe/Asia or B2 for US

3.3.1.17 The FWA device shall support 256QAM modulation for downlink

3.3.1.18 The FWA device shall support 64QAM modulation for uplink.

3.3.1.19 The FWA device should support 256QAM modulation for uplink

3.3.1.20 The FWA device shall support standardized QCIs as specified in 3GPP TS 23.203

3.3.1.21 The FWA device should support operator specific QCIs as specified in 3GPP TS 23.203

3.3.1.22 The FWA device shall support periodical intra-frequency ANR measurements for reporting to the network the Strongest Cells and related CGI (Cell Global Identity).

3.3.1.23 The FWA device shall support periodical inter-frequency ANR measurements for reporting to the network the Strongest Cells and related CGI (Cell Global Identity).

CHAPTER 4

4 Hardware, Safety, EMC requirements and environment operating conditions

4.1 Quality Requirements

4.1.1 The supplier/manufacturer shall conform to ISO 9001:2015 certifications. A quality plan describing the quality assurance system followed by the manufacturer shall be required to be submitted.

4.1.2 The failure of any component/ sub-system in the system may not result in the failure of complete system.

4.1.3 Provision shall be made for continuous testing of the system to allow both system qualities check and fault indication as a fault arises.

4.1.4 In case a fault is detected requiring reloading of the program, this shall be carried out automatically. In case of manual re-loading, it shall be possible to stop and start at any particular point in the program

4.1.5 The components used shall be available from multiple sources with adequate qualification. Number of proprietary components used shall be minimum. List of such components shall be indicated.

4.1.6 All the equipment shall have a tropical finish and coated to protect against saline atmosphere.

4.1.7 The FWA Device shall comply with the eco-design and energy efficiency regulations of the market where it is meant to be used.

4.1.8 The FWA Device shall comply to the restrictions of use of hazardous materials and waste management regulations of the market where it is meant to be used

4.1.9 The FWA Device shall have a MTBF (Mean Time Between Failure) not shorter than 7 years at 30 °C.

4.2 Device Management (Common for IDU and ODU)

4.2.1 The System shall support following methods:

a. RPC methods

b. Data model structure

c. Security

d. Performance monitoring

e. Data model parameters

4.3 Stability

4.3.1 In case of loss of power, when the power is restored the FWA Device shall return automatically to the operational state, with all services (e.g., data, voice) restored according to the configuration of the device prior the power interruption.

4.3.2 In case of loss of radio signal(s), when the radio signal is restored the FWA Device shall return automatically to the operational state, with all services (e.g., data, voice) restored according to the configuration of the device prior the radio signal interruption.

4.3.3 For data service, in normal operating conditions, the FWA Device shall offer a service availability equal or greater than 99.95%.

Note: this objective considers only the availability of the Device itself, not the availability of the network.

4.3.4 In normal operating conditions, the FWA Device shall offer a service availability for voice service of at least 99.5%.

4.3.5 The FWA Device shall maintain uninterrupted voice (SIP protocol) registration for at least 72 consecutive hours, during which the Device is idle for Voice.

4.3.6 the FWA Device shall be able to receive and make phone calls regularly, as well as to transmit and receive IP data user packets regularly.

4.3.7 If voice service is supported, the FWA Device shall be able to support long-lasting voice calls (1.5 hours at least).

4.4 User interface

4.4.1 The FWA Device shall offer a Web UI to the end user for customizing the configuration of the FWA Device.

4.4.2 The Web UI should permit the configuration of all the service features relevant for the end user.

4.4.3 The Web UI shall be customizable based on MNO requirements.

4.5 Safety Requirements

The equipment shall conform to relevant safety requirements as per (IS/IEC 62368-1:2018 or Latest & IS 10437: 2019/IEC 60215: 2016) as prescribed under Table no. 1 of the TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT": TEC10009: 2024. These requirements are applicable for purposely built hardware or a physical entity only.

4.6 Electromagnetic Compatibility (EMC)

These requirements are applicable for purposely built hardware or a physical entity only. (These requirements shall be as per TEC Standard No. TEC11016:2016 as modified/ amended from time to time)

Clause	Parameter	Standard
1.	Conducted and Radiated Emission	CISPR 32 Class-A
2.	Immunity to Electrostatic discharge: Contact discharge level 2 {± 4 kV}	IEC-61000-4-2 Performance Criteria-B, Clause 9
3.	Immunity to Electrostatic discharge: Air discharge level 3 {± 8 kV}	IEC-61000-4-2 Performance Criteria-B, Clause 9

4.	Immunity to radiated RF: a) Radio Frequency: 80 MHz to 1 GHz, Electromagnetic field: 3V/m b) Radio Frequency: 800 MHz to 960 MHz, Electromagnetic field: 10V/m c) Radio Frequency: 1.4 GHz to 6 GHz, Electromagnetic field: 10V/m	IEC 61000-4-3 (2010);
5.	Immunity to fast transients (burst): Test Level 2: a) 1 kV for AC/DC power port b) 0. 5 kV for signal / control / data / telecom lines.	IEC 61000- 4- 4 {2012); Performance Criteria-B, Clause 9
6.	Immunity to surges: AC/DC ports a) 2 kV peak open circuit voltage for line to ground b) 1kV peak open circuit voltage for line to line	IEC 61000-4-5 (2014) Performance Criteria-B, Clause 9
7.	Immunity to surges: Telecom ports a) 2 kV peak open circuit voltage for line to ground coupling. b) 2 kV peak open circuit voltage for line-to-line coupling.	IEC 61000-4-5 (2014) Performance Criteria-C, Clause 9
8.	Immunity to conducted disturbance induced by Radio frequency fields: Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz- 80	IEC 61000-4-6 (2013) Performance Criteria-A, Clause 9

	MHz for AC / DC lines and Signal /Control/telecom lines.	
9.	Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any): Limits: - a) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e., 70% supply voltage for 500ms) b) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e.,40% supply voltage for 200ms) c) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s. d) a voltage interruption corresponding to a reduction of supply voltage of >95% for 10ms.	IEC 61000-4-11 (2004): a) Performance Criteria B for Reduction of Supply 30% for 500ms or Dip to reduction of 60% for 100ms b) Performance Criteria C for Reduction of 60% for 200ms c) Performance criteria C for Voltage Interruption>95% for 5 s (Note: In case of Battery back-up performance criteria A is applicable). d) Performance Criteria B for Voltage Interruption >95% duration :10ms (Note: In case of Battery back-up Performance Criteria A is applicable for above conditions.)
10	Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any): a) Voltage Interruption with 0% of supply for 10ms. b) Voltage Interruption with 0% of supply for 30ms, 100ms,	IEC 61000-4-29(2000) a) Applicable Performance Criteria shall be B. b) Applicable Performance Criteria shall be C. c) Applicable Performance Criteria shall be B.

	300ms and 1000ms. c) Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. d) Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000 ms. e) Voltage variations corresponding to 80% and 120%of supply for 100 ms to 10s as per Table 1c of IEC 61000-4-29.	d) Applicable Performance Criteria shall be C. Applicable Performance Criteria shall be B.

4.7 System Radio Operating Environments

4.7.1 Availability

a. The facility shall be available for introduction of centralized Operation and Maintenance Control (OMC).

b. The maintenance spares supplies shall take in to account the MTBF and MTTR.

4.7.2 Diagnostic Capability

a. The diagnostic capability of the system shall be such as to minimize the human efforts required. The diagnostic programs which are normally resident in the on-line program shall be indicated. Details of the off-line diagnostic programs shall be given. The procedure for invoking such programs shall be described. The procedure for consulting fault dictionary for diagnostic programs shall be made available.

b. The system shall provide facility for automatic restart under severe fault conditions. Where automatic restart fails to restore system sanity, facility shall be provided for manual restart of the system.

4.7.3 **Environmental Test Conditions:**

a. Indoor entity (such as CU, DU, RIC, SMO): Category A SD: QM-333

b. Outdoor entity (such as O-RU): Category D SD: QM-333 and IP65

c. Antenna & Feeders: Category E as per SD: QM-333

4.8 General Requirements

4.8.1 General

4.8.1.1 The operation of the equipment shall be in the frequency band allotted.

4.8.1.2 Support of Multiple Equipment Vendors as per tender requirement

4.8.1.3 The system shall support the possibility of using equipment and sub-systems of different vendors as per defined industry standards, wherever relevant.

4.8.2 Hardware

4.8.2.1 The system hardware shall be modular in design and shall permit growth in steps. The arrangement shall be such that failure/ deterioration of service shall not occur when implementing the growth.

4.8.2.2 Design precautions shall be taken to minimize the possibility of equipment damage arising from the insertion of an electronic package into the wrong connector or the removal of any package from any connector.

4.8.2.3 The system hardware shall not pose any problem, due to changes in date and time caused by events such as changeover of leap year etc., in the normal functioning of the system.

4.8.3 Processors

4.8.3.1 Provision shall be made to prevent the loss/alteration of memory contents due to power failures, improper operating procedures and the procedure for restoring the system to its normal state, etc.

4.8.4 Input-Output Devices

4.8.4.1 The communication facilities provided for exchange of information between the elements of FWA device and the maintenance and operating personnel shall include facilities for a system test, control and alarm indication at OMC.

4.8.4.2 Input / output terminals shall be capable of transmitting/ receiving characters of a subset of the ITU-T T.50 alphabet. The printing/display device shall print/display different graphic symbols for the digit zero and the capital letter O. The input/output terminal shall have the English Keyboard.

4.8.4.3 Adequate number of man-machine interfaces shall be available.

4.8.4.4 If provision is made for monitoring from a remote terminal, it shall be ensured that the data links conform to the ITU-T Recommendation Q.513. Care shall be taken that the reliability of the data links towards remote terminal does not, in any way, affect the reliability of the device. Special provision shall also be made for storage of failure event even when the system is unable to transmit an output message.

4.8.4.5 A suitable alarm and display system at OMC shall be provided for a continuous indication of the system status.

4.8.5 Equipment Practice

4.8.5.1 It shall be indicated whether printed board connectors are of edge-type or plug-and-socket type. They shall not be easily damaged during replacements and removals. The contact particulars as well as life test performance on contact resistance for each type of connector shall be supplied.

4.8.5.2 All components and material used in the equipment shall be non-inflammable or in absence of it, self-extinguishable. They shall be fully tropicalised.

4.8.5.3 The method used for connection of permanent wiring outside the printed cards shall be indicated.

4.8.5.4 The buses, if any, shall be suitably protected against electrical and magnetic interference from neighbouring systems (like electromechanical systems, fluorescent tubes, motors, etc.).

4.8.5.5 The different plug-in cards shall have suitable mechanical safeguards to prevent damage due to accidental interchange of cards.

4.8.5.6 The requirement at the external interface against induced voltages and currents due to lightning, high power system, etc. shall be indicated.

4.8.5.7 The system shall provide for human isolation and protection from accidental high voltage power contact.

4.9 Software

4.9.1 The software shall be written in a High-Level Language. The software shall be modular and structured.

4.9.2 The software shall include the following characteristics:

a. The design of the software shall be such that the system is easy to handle both during installation and normal operations as well as during extensions.

b. The functional modularity of the software shall permit introduction of changes wherever necessary with least impact on other modules.

c. It shall be open-ended to allow addition of new features.

d. Adequate flexibility shall be available to easily adopt changes in service features & facilities and technological evolution in hardware.

e. The design shall be such that propagation of software faults is contained.

f. Test programs shall include fault tracing for detection and localization of system faults.

4.9.3 Software Maintenance

4.9.3.1 All software updates, for a period as specified, shall be supplied on continuing basis. These updates shall include new features and services and other maintenance updates.

4.9.3.2 Integration of software updates without posing any problem to the existing functionality shall be possible.

CHAPTER 5

INFORMATION FOR THE PROCURER/VENDOR OF PRODUCT

Interfaces and features which are optional needs to be examined by the procurer and suitably specified in the tender conditions as per their requirement based on the deployment scenario specific to the procurer.

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
5QI	5G QoS Identifier
ACS	Auto-Configuration Server
AKA	Authentication and Key Agreement
ALG	Application Layer Gateway
ANR	Automatic Neighbour Relation
AP	Access Point
APN	Access Point Name
ARP	Address Resolution Protocol
BBF	BroadBand Forum
BRI	Basic Rate Interface
CABs	Conformance Assessment Bodies
CGI	Cell Global Identity
CHAP	Challenge-Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CISPR	International Special Committee on Radio Interference
CLAT	Customer-Side Translator

CN	Core Network
CPE	Customer Premises Equipment
DAD	Duplicate Address Detection
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DL	Downlink
DMZ	DeMilitarized Zone
DNN	Data Network Name
DNS	Domain Name System
DoS	Denial of Service
DSCP	Differentiated Services Code Point
DSS	Dynamic Spectrum Sharing
EAP	Extensible Authentication Protocol
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
EIRP	Effective Isotropic Radiated Power
EMC	Electromagnetic Compatibility

EN-DC	E-UTRA-NR Dual Connectivity
ER	Essential Requirements
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FDD	Frequency Division Duplex
FQDN	Fully Qualified Domain Name
FR1	Frequency Range 1
FR2	Frequency Range 2
FWA	Fixed Wireless Access
FXS	Foreign eXchange Station
GR	Generic Requirements
GRE	Generic Routing Encapsulation
GSMA	GSM Association
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDU	Indoor Unit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
IR	Interface Requirements
IS	Indian Standard
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MIMO	Multiple-Input Multiple-Output
MNO	Mobile Network Operator
MSS	Maximum Segment Size
MTBF	Mean Time Between Failure

MTU	Maximum Transmission Unit
NAS	Non-Access Stratum
NAT	Network Address Translator
NDP	Network Discovery Protocol
NEA	New Radio Encryption Algorithm
NIA	New Radio Integrity Algorithm
NR	New Radio
NSA	Non-Standalone
NSSAI	Network Slice Selection Assistance Information
NTP	Network Time Protocol
ODU	Outdoor Unit
OTT	Over-The-Top
PAP	Password Authentication Protocol
PBC	Push Button Configuration
P-CSCF	Proxy-Call Session Control Function
PDN	Packet Data Network
PDU	Protocol Data Unit
PoE	Power-over-Ethernet

PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
PSU	Power Supply Unit
QAM	Quadrature Amplitude Modulation
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
RFC	Request for Comments
RPC	Remote Procedure Call
RRC	Radio Resource Control
RTP	Real-time Transport Protocol
Rx	Receive
SA	Standalone
SCS	Sub-Carrier Spacing
SD	Slice Differentiator
SDP	Session Description Protocol
SIM	Subscriber Identity Module

SIP	Session Initiation Protocol
SMB	Server Message Block
SR	Service Requirements
SRS	Sounding Reference Signal
SSID	Service Set Identifier
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
TDD	Time Division Duplex
TLS	Transport Layer Security
TR	Technical Report
UDP	User Datagram Protocol
UI	User Interface
UL	Uplink
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
URSP	User Equipment Route Selection Policy
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module

VLAN	Virtual Local Area Network
VOD	Video on Demand
VoIP	Voice over IP
VoLTE	Voice over LTE
VPN	Virtual Private Network
WAN	Wide Area Network
WFA	Wi-Fi Alliance
WME	Wireless Multimedia Extensions
WMM	Wi-Fi Multimedia
WPS	Wi-Fi Protected Setup
WPA3	Wi-Fi Protected Access 3