TS.64 FWA Devices Architecture and Requirements

Version 1.0

02 October 2023

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction 4
1.1 Overview 4
1.2 Scope 5
1.3 Definitions 5
1.4 Abbreviations 6
1.5 References 9
1.6 Conventions 17
2 FWA Devices Architectures 17
2.1 Indoor FWA Solution 18
2.2 Outdoor FWA Solution (single tenant) 19
3 FWA Devices Requirements (Common section) 21
3.1 Radio/RRC/NAS common requirements 21
3.2 Quality of Service 22
3.3 Voice Service 22
3.3.1 Voice General Requirements 22
3.3.2 VoIP service: registration and basic call for single-line profile 23
3.3.3 VoIP service: supplementary services for single-line profile 26
3.3.4 FXS interface requirements 29
3.3.5 FAX and POS (Point of Sale) Requirements 30
3.4 Networking Features 31
3.4.1 Interfaces 31
3.4.2 Performance 32
3.4.3 Protocols 33
3.4.4 DHCP 34
3.4.5 NAT & Bridge operation 35
3.4.6 MTU 35
3.4.7 DNS 35
3.4.8 Security 36
3.4.9 Customisation 37
3.4.10 USB Port 37
3.5 Wi-Fi 38
3.5.1 Standards 38
3.5.2 MIMO capabilities, Bandwidth, Modulation and Coding schemes 39
3.5.3 Performance 39
3.5.4 Service Set Identifier (SSID) 40
3.5.5 Channel and Bandwidth Selection 41
3.5.6 Clients 41
3.5.7 Security 41
3.5.8 Wi-Fi protected Setup (WPS) 42
3.5.9 Band Steering 42
3.5.10 Mesh Networks 43
3.5.11 Wi-Fi Diagnostics 43
3.5.12 Wireless Multimedia Extension 43

3.5.13 Customisation 43
3.6 IDU/ODU Interworking and Resilience 44
3.6.1 Common requirements to bridged and routed modes of operation 44
3.6.2 ODU Bridged mode operation. 45
3.6.3 Reliability of IDU-ODU operation 46
3.6.4 ODU Routed mode operation. 46
3.6.5 Tunnels/VPNs 47
3.7 Device Management 47
3.7.1 Common Requirements for IDU and ODU 47
3.7.2 Technical Adaptation of FWA Device 52
3.8 Security 52
3.8.1 Passwords 53
3.8.2 Web UI security requirements 54
3.9 User Data Protection and Privacy 54
3.10 Hardware, Safety, EMC requirements and environment operating conditions 56
3.10.1 General 56
3.11 Stability 57
3.12 User Interface 58
4 Specific Requirements for 4G FWA Devices 58
4.1 Radio/RRC/NAS specific requirements for 4G FWA devices 58
4.2 Antenna Performance Acceptance Values for 4G FWA devices 59
5 Specific Requirements for 5G NSA FWA Devices 60
5.1 Radio/RRC/NAS specific requirements for 5G-FR1 NSA FWA devices. 60
5.2 Radio/RRC/NAS specific requirements for 5G-FR2 NSA FWA devices 61
5.3 Antenna Performance Acceptance Values for 5G NSA FWA devices 62
6 Specific Requirements for 5G SA FWA Devices 63
6.1 Radio/RRC/NAS specific requirements for 5G-FR1 SA FWA devices 64
6.2 Radio/RRC/NAS specific requirements for 5G-FR2 SA FWA devices 65
6.3 Antenna Performance Acceptance Values for 5G SA FWA devices 65
Annex A Hardware, Safety and EMC normative references for European Market 66
A.1 Safety 66
A.2 EMC 66
A.3 Radio Spectrum 66
A.4 Environment Protection and Energy Efficiency 67
A.5 Environment Operating Conditions 68
Annex B Example of Wi-Fi metrics for Wi-Fi diagnostic 68
Annex C Document Management 69
C.1 Document History 69
C.2 Other Information 69

1 Introduction

1.1 Overview

The use of Fixed Wireless Access (FWA) solutions has become quite popular in the Ultrabroadband Internet Access market as a cost-effective solution to provide a good connectivity service to customers, especially in areas in which wireline (FTTx) solutions have not been yet deployed.

A typical FWA Device is an indoor (1-box) or outdoor (2-box) solution that connects via Radio Interface to the network of the Service Provider, and offers to the end-user Wi-Fi connectivity, Fast- or Gigabit-Ethernet ports, and one or two FXS (Foreign eXchange Station) ports for connecting analog telephones to provide voice service to the end-user.

Several options are available as regards the radio technology for the communication between the FWA Device and the Network, including WiMax. However, in this context we will focus on Devices connecting to the mobile network of service operators via standard 4G/4G+/5G interfaces, as this technology is the natural choice for MNOs and is quickly becoming very popular in the market.

Provided that the 4G/4G+/5G mobile interface through which the FWA Devices connect to the network is well defined and standardized, many other functionalities of FWA Devices have not been standardized so far; this implies that both Operators and Manufacturers need to define and implement in a customized way many features of the FWA Device and the way the services are delivered to the end-user.

So, for example, Remote Management of FWA Devices is an area not clearly defined in standards, although some operators manage such devices via BBF TR-069 ACS (Auto-Configuration Server).

Voice service is another area in which there isn’t a clearly defined standard for FWA Devices. Many Devices offer voice service through the adoption of an IR.92 VoLTE stack, but this often does not fit the needs of a typical land-line service with PSTN Emulation requirements; for this reason, many Operators prefer to implement a VoIP-based stack, but this is a customized development which requires a lot of effort in specification definition, implementation and testing.

Another area still not covered by standards so far is the definition of an open architecture for outdoor (2-box) FWA Devices. An outdoor solution is typically made of an external Antenna, also called OutDoor Unit (ODU), providing connection to the mobile network, and an InDoor Unit (IDU), providing Wi-Fi, networking, Ethernet and Voice Service. The connection between the two Units is normally done via a Gigabit-Ethernet connection, with Power-over-Ethernet to provide power supply to the ODU.

Sometimes, the 2 boxes (IDU and ODU) are provided from the same manufacturer as a whole solution and the protocol used between the two boxes is proprietary or, in general, not public. Instead, many Operators may want to open the interface between IDU and ODU, as for example different market segments (consumer, small business, and enterprise) may need different types of IDU with very different features and services.

1.2 Scope

This document specifies a minimum set of requirements for FWA Devices. The proposed approach is to define requirements common to the various mobile technologies (4G, 5G NSA, 5G SA), and delta requirements for the requirements specific to each technology.

The requirements are grouped in functional areas (e.g. Radio, Device Management, Voice); for each area it is indicated where the requirements apply to Outdoor or Indoor FWA solutions (or both).

An initial section of the document is dedicated to an overview of FWA Device architectures. This section introduces the Indoor and Outdoor architectures and identifies the areas of requirements to be defined in detail in the subsequent sections. Future enhancements to the FWA architecture are possible, such as the evolution from single-tenant solution to multi-tenant.

The main areas of requirements covered in the document are:

- Radio/RRC/NAS
- Use of multiple APNs for differentiating the various services
- Quality of Service
- Voice Service
- Networking Features
- Wi-Fi
- IDU/ODU Interworking and Resilience
- Device Management
- Security

Please note that 3G FWA Devices and multi-SIM FWA Devices are outside the scope of this document.

1.3 Definitions

Term	Description
Bridged mode	In an OutDoor FWA Solution, in Bridged mode operation the OutDoor Unit (ODU) transfers frames (i.e. IP Packets) between each VLAN on the link with the Indoor Unit to the correspondent PDN/PDU Connection on the mobile network, and vice versa. Therefore, in this operation mode, the behaviour of the ODU corresponds to a Layer 2 bridge between networks with different encapsulations.
Routed mode	In an OutDoor FWA Solution, in Routed mode operation the OutDoor Unit (ODU) routes frames (i.e., IP Packets) between each VLAN on the link with the Indoor Unit to the PDN/PDU Connections on the mobile network, and vice versa, by means of IP routing and IP routing table. Therefore, in this operation mode, the behaviour of the ODU corresponds to an IP (Layer 3) router. This operation mode normally involves the use of Network Address Translation (NAT) to route IP packets coming from the private IP addressing space with the IDU, to the mobile network, and vice versa.
NR FR1 low-bands	Operating bands below 1GHz for NR.

Term	Description
NR FR1 mid-bands	Operating bands between 1GHz and 2GHz for NR.
NR FR1 high-bands	Operating bands above 2 GHz for NR.
Upspeed	A procedure for changing the voice codec during the active phase of a call, done usually to change to a codec that requires more bandwidth than the one needed for the original codec.

1.4 Abbreviations

Term	Description
3GPP	3rd Generation Partnership Project
4G	Fourth-generation technology standard for broadband cellular networks
5G	Fifth-generation technology standard for broadband cellular networks
5QI	5G QoS Identifier
ACS	AutoConfiguration Server
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
ANR	Automatic Neighbour Relation
AP	Access Point
APN	Access Point Name
ARP	Address Resolution Protocol
BBF	BroadBand Forum
BRI	Basic Rate Interface
CA	Carrier Aggregation
CB	Communication Barring
CCBS	Completion of Communications to Busy Subscriber
CDIV	Communication Diversion
CGI	Cell Global Identity
CPE	Customer Premise Equipment
CSCF	Call Session Control Function
CW	Communication Waiting
CWMP	CPE WAN Management Protocol
DC	Direct Current
DLNA	Digital Living Network Alliance
DNS	Domain Name System
DSCP	Differentiated Service Code Point
DSS	Dynamic Spectrum Sharing
DTMF	Dual-Tone Multi-Frequency signaling
ECT	Explicit Communication Transfer

Term	Description
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
EIRP	Equivalent Isotropic Radiated Power
EMC	ElectroMagnetic Compatibility
EN-DC	E-UTRAN/New Radio Dual Connectivity
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access
FDD	Frequency Division Duplex
FQDN	Fully Qualified Domain Name
FR	Frequency Range
FS	Free Space
FTP	File Transfer Protocol
FWA	Fixed Wireless Access
FXS	Foreign eXchange Station
GSM / E-GSM	Global System for Mobile Communication/ Extended-GSM
GSMA	GSM Association
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDU	InDoor Unit
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union – Telecommunication Standardization Bureau
LAN	Local Area Network
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Media Access Control
MCID	Malicious Communication Identification
MIMO	Multiple Input Multiple Output
MSS	Maximum Segment Size
MTBF	Mean Time Between Failure
MTU	Maximum Transmission Unit
MWI	Message Waiting Indication

Term	Description
NAS	Non-Access Stratum
NAT	Network Address Translation
NEA	New radio Encryption Algorithm
NIA	New radio Integrity Algorithm
NR	New Radio
NSA	Non Stand-Alone
NSSAI	Network Slice Selection Assistance Information
NTP	Network Time Protocol
ODU	OutDoor Unit
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
OTA	Over The Air (without cable)
OTT	Over The Top
PC	Power Class
PCI	Physical layer Cell Identifier
P-CSCF	Proxy-CSCF
PDN	Packet Data Network
PDSCH	Physical Downlink Shared Channel
POE	Power Over Ethernet
PSK	Pre-Shared Key
PSU	Power Supply Unit
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
RFC	Request For Comments
RPC	Remote Procedure Call
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SA	Stand-Alone
SDP	Session Description Protocol
SIM/USIM	Subscriber Identity Module / Universal Subscriber Identity Module (in this document, includes eSIM)
SINR	Signal to Interference plus Noise Ratio
SIP	Session Initiation Protocol

Term	Description
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TIP	Terminating Identification Presentation
TIR	Terminating Identification Restriction
TLS	Transport Layer Security
TRP	Total Radiated Power
TRS	Total Radiated Sensitivity
TSG	Terminal Steering Group
TWAMP	Two-Way Active Measurement Protocol
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URSP	UE Route Selection Policy
VLAN	Virtual LAN
VOD	Video On Demand
VoLTE	Voice over LTE
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WFA	Wi-Fi Alliance
Wi-Fi	A wireless local area networking technology that uses radio waves to provide wireless high-speed Internet access, defined by IEEE 802.11 standards.
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

1.5 References

Ref	Doc Number	Title
[1]	<e.g., PRD AA.34>	<PRD or document title e.g., “Policy and Procedures for Official Documents”. For non-binding documents with no reference entries, this section may be deleted >
[2]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[3]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words

Ref	Doc Number	Title
		https://www.rfc-editor.org/info/rfc8174
[4]	3GPP TS 23.207 V16.0.0 or later	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; End-to-end Quality of Service (QoS) concept and architecture (Release 16)
[5]	3GPP TS 23.203 V16.0.0 or later	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 16)
[6]	GSMA IR.92 Version 15.0 or later	IMS Profile for Voice and SMS - Version 15.0

[7]	3GPP TS 24.229 V15.2.0 or later	3rd Generation Partnership Project;
		Technical Specification Group Core Network and Terminals;
		IP multimedia call control protocol based on
		Session Initiation Protocol (SIP)
		and Session Description Protocol (SDP);
		Stage 3 (Release 15)

[8]	3GPP TS 23.003 V16.3.0 or later	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification. (3GPP TS 23.003 version 16.3.0 Release 16)
[9]	3GPP TS 23.228 V16.5.0 or later	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 version 16.5.0 Release 16)
[10]	RFC 3263	Session Initiation Protocol (SIP): Locating SIP Servers
[11]	RFC 5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
[12]	RFC 3261	SIP: Session Initiation Protocol
[13]	RFC 5341	The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry
[14]	RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
[15]	RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
[16]	RFC 3311	The Session Initiation Protocol (SIP) UPDATE Method
[17]	RFC 4733	RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
[18]	ITU-T G.711 (11/88)	Pulse code modulation (PCM) of voice frequencies
[19]	ITU-T G.729 (06/12) or later	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)
[20]	ITU-T G.729 Annex A (11/96) or later	Reduced complexity 8 kbit/s CS-ACELP speech codec

Ref	Doc Number	Title
[21]	ITU-T G.722 (09/12) or later	7 kHz audio-coding within 64 kbit/s
[22]	ITU-T G.131 (11/03) or later	Talker echo and its control
[23]	RFC 3550	RTP: A Transport Protocol for Real-Time Applications
[24]	RFC 3551	RTP Profile for Audio and Video Conferences with Minimal Control
[25]	RFC 3605	Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)
[26]	RFC 2198	RTP Payload for Redundant Audio Data.
[27]	RFC 4961	Symmetric RTP / RTP Control Protocol (RTCP)
[28]	RFC 5009	Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media
[29]	RFC 3960	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
[30]	RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
[31]	3GPP TS 24.607 version 15.0.0 or later	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.607 version 15.0.0 Release 15)
[32]	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
[33]	3GPP TS 24.604 version 15.1.0 or later	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.604 version 15.1.0 Release 15)
[34]	RFC 3842	A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
[35]	3GPP TS 24.611 version 11.3.0 or later	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Anonymous Communication Rejection (ACR) and Communication Barring (CB) using IP Multimedia (IM) Core Network (CN) subsystem;

Ref	Doc Number	Title
		Protocol specification (3GPP TS 24.611 version 11.3.0 Release 11)
[36]	3GPP TS 24.610 version 15.1.0 or later	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.610 version 15.1.0 Release 15)
[37]	3GPP TS 24.615 version 15.0.0 or later	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Communication Waiting (CW) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol Specification (3GPP TS 24.615 version 15.0.0 Release 15)
[38]	3GPP TS 24.147 version 10.1.0 or later	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS);LTE; Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3 (3GPP TS 24.147 version 10.1.0 Release 10)
[39]	3GPP TS 24.642 version 10.2.0 or later	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS);LTE; 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 (3GPP TS 24.642 version 10.2.0 Release 10)
[40]	3GPP TS 24.629 version 15.0.0 or later	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.629 version 15.0.0 Release 15)
[41]	3GPP TS 24.608 version 10.0.0 or later	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS);LTE; Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.608 version 10.0.0 Release 10)
[42]	3GPP TS 24.616 version 10.0.0 or later	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Malicious Communication Identification (MCID)

Ref	Doc Number	Title
		using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.616 version 10.0.0 Release 10)

[43]	ETSI ES 201 970 V1.1.1	Access and Terminals (AT);
		Public Switched Telephone Network (PSTN);
		Harmonized specification of physical and electrical characteristics at a 2-wire analogue presented Network Termination Point (NTP)

[44]	ITU-T Q.522 (11/88)	Digital exchange connections, signalling and ancillary functions
[45]	ITU-T T.38 (09/10)	Procedures for real-time Group 3 facsimile communication over IP networks
[46]	ITU-T T.38 (11/15)	Procedures for real-time Group 3 facsimile communication over IP networks
[47]	BBF TR-069	CPE WAN Management Protocol Issue: 1 Amendment 6 Approval Date: March 2018 CWMP Version: 1.4
[48]	BBF TR-135	Data Model for a TR-069 Enabled STB Issue: 1 Amendment 3 Issue Date: November 2012
[49]	BBF TR-104	TR-069 Voice Service:2.0 Service Object definition
[50]	BBF TR-140	TR-069 Data Model for Storage Service Enabled Devices Issue: 1 Amendment 3 Issue Date: May 2017
[51]	BBF TR-196	FAP Service:2.0 Femto Access Point Service Data Model
[52]	BBF TR-098	TR-069 InternetGatewayDevice:1.14 Root Object definition
[53]	BBF TR-181	TR-069 Device:2.11 Root Object definition
[54]	RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
[55]	BBF TR-143	Enabling Network Throughput Performance Tests and Statistical Monitoring Issue: 1 Amendment 1 Corrigendum 2 Issue Date: February 2023
[56]	BBF TR-390	Performance Measurement from IP Edge to Customer Equipment using TWAMP Light Issue: 1 Issue Date: May 2017
[57]	GSMA TS.24 Version 6.0 or later	Operator Acceptance Values for Device Antenna Performance
[58]	3GPP TS 38.101-1 Version 17.5.0 or later	5G;NR; User Equipment (UE) radio transmission and reception;

Ref	Doc Number	Title
		Part 1: Range 1 Standalone (3GPP TS 38.101-1 version 17.5.0 Release 17)
[59]	IEEE 802.3ab-1999 or later	IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Physical Layer Parameters and Specifications for 1000 Mb/s Operation over 4 pair of Category 5 Balanced Copper Cabling, Type 1000BASE-T
[60]	RFC 791	INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION
[61]	RFC 8200	Internet Protocol, Version 6 (IPv6) Specification
[62]	RFC 826	An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware
[63]	RFC 5227	IPv4 Address Conflict Detection
[64]	RFC 5494	IANA Allocation Guidelines for the Address Resolution Protocol (ARP)
[65]	RFC 4861	Neighbour Discovery for IP version 6 (IPv6)
[66]	RFC 792	INTERNET CONTROL MESSAGE PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION
[67]	RFC 950	Internet Standard Subnetting Procedure
[68]	RFC 4884	Extended ICMP to Support Multi-Part Messages
[69]	RFC 6633	Deprecation of ICMP Source Quench Messages
[70]	RFC 6918	Formally Deprecating Some ICMPv4 Message Types
[71]	RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
[72]	RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification
[73]	RFC 3376	Internet Group Management Protocol, Version 3
[74]	RFC 4605	Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")
[75]	IEEE 802.1Q-2018 and later	IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks
[76]	RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
[77]	RFC 2475	An Architecture for Differentiated Services
[78]	RFC 2597	Assured Forwarding PHB Group

Ref	Doc Number	Title
[79]	RFC 3260	New Terminology and Clarifications for Diffserv
[80]	RFC 2663	IP Network Address Translator (NAT) Terminology and Considerations
[81]	3GPP TS 23.501 Version 16.5.0 or later	System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.5.0 Release 16)
[82]	3GPP TS 24.501 Version 16.5.1 or later	Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 3GPP TS 24.501 V16.5.1
[83]	IEEE 802.11n-2009	IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput
[84]	IEEE 802.11ac-2013	IEEE Standard for Information technology--Telecommunications and information exchange between systems–Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.
[85]	IEEE 802.11ax-2021	IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN
[86]	IEEE 802.11k-2008	IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs
[87]	IEEE 802.11v-2011	IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management
[88]	IEEE 802.11r-2008	IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition
[89]	IEC 60529:1989/AMD2:2013 /COR1:2019 or later	Degrees of protection provided by enclosures (IP Code)

Ref	Doc Number	Title
[90]	ITU-T K.21 (08/22)	Resistibility of telecommunication equipment installed in customer premises to overvoltages and overcurrents
[91]	ITU-T K.44 (10/19) – Cor.1 (12/20)	Resistibility tests for telecommunication equipment exposed to overvoltages and overcurrents – Basic Recommendation
[92]	ITU-T K.45 (11/22)	Resistibility of telecommunication equipment installed in the access and trunk networks to overvoltages and overcurrents
[93]	3GPP TS 36.101 Version 17.10.0 or later	Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception
[94]	3GPP TS 38.101-2 Version 17.5.0 or later	NR; User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone
[95]	3GPP TS 38.214 Version 17.6.0. or later	NR; Physical layer procedures for data
[96]	GSMA TS.32 Version 13.0 or later	Technical Adaptation of Devices through Late Customisation
[97]	GSMA TS.49 Version 1.1 or later	WLAN Antenna Performance Testing
[98]	RFC 2131	Dynamic Host Configuration Protocol
[99]	RFC 2132	DHCP Options and BOOTP Vendor Extensions
[100]	RFC 8415	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[101]	RFC 3022	Traditional IP Network Address Translator (Traditional NAT)
[102]	RFC 4787	Network Address Translation (NAT) Behavioural Requirements for Unicast UDP
[103]	RFC 6145	IP/ICMP Translation Algorithm
[104]	3GPP TS 24.008 Version 18.3.0 or later	Mobile radio interface Layer 3 specification; Core network protocols; Stage 3
[105]	RFC 1034	DOMAIN NAMES - CONCEPTS AND FACILITIES
[106]	RFC 1035	DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
[107]	RFC 8484	DNS Queries over HTTPS (DoH)
[108]	USB 3.1	USB Implementers Forum, Universal Serial Bus 3.1 Specification
[109]	IEEE 802.11i-2004	IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements
[110]	WPA3™ - 2022	Wi-Fi Alliance WPA3™ Specification Version 3.1
[111]	IEEE 802.1X-2020	IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control

1.6 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [2] and clarified by RFC 8174 [3], when, and only when, they appear in all capitals, as shown here.

2 FWA Devices Architectures

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.

In this version of the document, the focus is on single-tenant Outdoor solutions.

Another possible option of the architecture of outdoor solutions is the interface between ODU and IDU. In some cases, the ODU can only be connected to a specific IDU of the same manufacturer, and the interface between IDU and ODU is proprietary or, in general, not open. This case is not covered in this document.

Instead, this document defines an open, standard interface between ODU and IDU; therefore, ODUs and IDUs from different manufacturers can be matched and combined.

2.1 Indoor FWA Solution

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

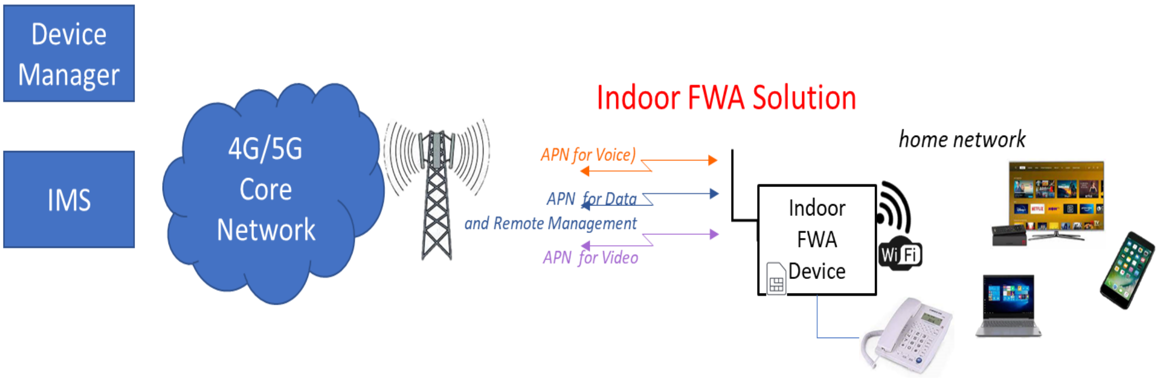

Figure 1: Indoor FWA Device Reference Architecture

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 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.

2.2 Outdoor FWA Solution (single tenant)

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

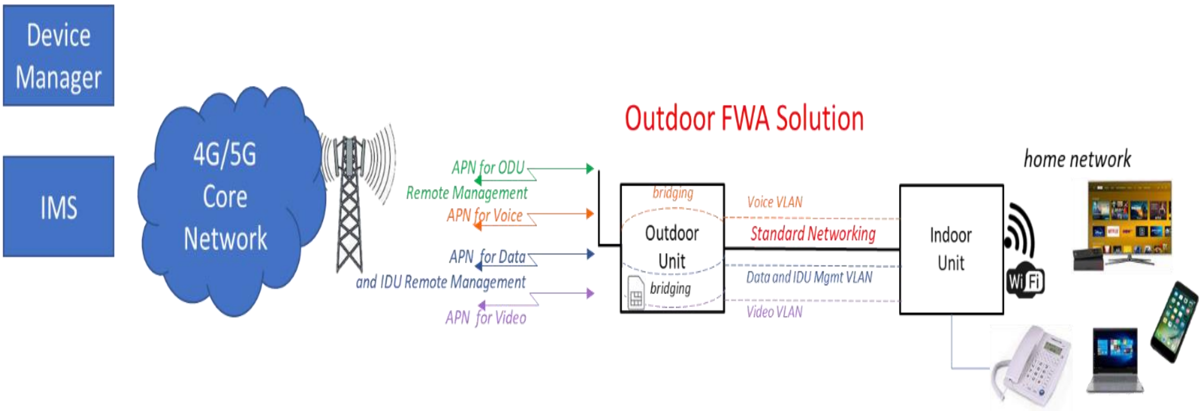

Figure 2: Outdoor FWA Device Reference Architecture

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.

In this version of the document, the single-tenant solution is considered: therefore, each ODU is coupled 1:1 with an IDU and the resultant FWA Solution is exclusively dedicated to a single user.

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-69 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;
- Is suitable for outdoor installation. That is, the ODU and its accessories have Hardware, EMC and Security featues 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, …
  - 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.

3 Error! Reference source not found.**FWA Devices Requirements (Common section)**

3.1 Radio/RRC/NAS common requirements

Typically, FWA devices share the radio access resources with other 4G and 5G device categories (e.g., smartphones, M2M modules) so it is essential for mobile operators to increase the spectral efficiency as much as possible, in order to optimize the usage of the valuable FDD and TDD frequency assets.

All this is possible thanks to some transmission techniques that are able to improve device performance and leading to an overall higher spectral efficiency:

- **Carrier Aggregation**: the ability of the device to receive and/or transmit on multiple bands at the same time.
- **MIMO** to use multiple antenna elements at the transmitter and the receiver to improve bit rates and channel quality estimation.
- **Higher-Order Modulations** provide higher data rates within a given bandwidth; the drawback is the reduced robustness to noise and interference.
- **Higher Maximum Output Power** to compensate propagation losses.

- **Uplink Power Class**

TS.64_3.1_REQ_001	The FWA device SHALL support one (1) SIM/USIM. FWA Devices with multiple SIMs are outside the scope of this document.
TS.64_3.1_REQ_002	The FWA device MAY be equipped with one (1) eSIM, instead of a physical SIM.
TS.64_3.1_REQ_003	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)
TS.64_3.1_REQ_004	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)
TS.64_3.1_REQ_005	The FWA Device SHALL allow configurable associations between PDN/PDU connections and services/applications (e.g. voice, video; VLAN settings via Web UI)
TS.64_3.1_REQ_006	The FWA device SHOULD support the establishment of at least 6 PDNs/PDUs
TS.64_3.1_REQ_007	The FWA Device SHALL support the establishment of PDNs/PDUs with the following stacks: • IPv4 only • IPv6 only • IPv4/IPv6
TS.64_3.1_REQ_008	For each PDNs/PDUs, the FWA Device SHALL allow to configure: • Protocol stack (IPv4, IPv6, IPv4v6); • Authentication option (PAP/CHAP);

	- MTU/MSS

Further detailed requirements for FWA Device in this area depend on the specific technology considered, therefore they are defined in the chapters dedicated to the various technologies (§ 4.1 for 4G, § 5.1 for 5G-FR1 NSA, § 5.2 for 5G-FR2 NSA, § 6.1 for 5G-FR1 SA, § 6.2 for 5G-FR2 SA).

3.2 Quality of Service

TS.64_3.2_REQ_001	For Quality of Service, the FWA Device SHALL comply with the 3GPP standards 3GPP TS 23.207 **Error! Reference source not found.** and 3 GPP TS 23.203 **Error! Reference source not found.** regardless of deployment scenario (e.g., 4G, 5G NSA, 5G SA).
TS.64_3.2_REQ_002	A wireless service provider utilizes customized QoS for specific category of subscribers including mission critical organizations, government entities and enterprise customers. For the latter case, the FWA Device SHOULD comply with the wireless service provider's requirements and mandates.

3.3 Voice Service

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

3.3.1 Voice General Requirements

TS.64_3.3.1_REQ_001	The Indoor FWA Device (1-box solution) SHALL support voice service either by means of VoLTE technology or VoIP technology.
TS.64_3.3.1_REQ_002	The InDoor Unit of an OutDoor FWA Solution (2-box) SHALL support voice service uniquely by means of VoIP technology.
TS.64_3.3.1_REQ_003	In case of VoLTE Technology, the FWA Device SHALL be compliant to GSMA IR.92 [6] profile.
TS.64_3.3.1_REQ_004	In case of VoIP technology, the FWA Device SHALL be compliant to 3GPP specification 24.229 [7], with the profile defined in the following sections 3.3.2, 3.3.3 and, optionally, 3.3.5.
TS.64_3.3.1_REQ_005	In case of VoIP technology, the FWA Device SHALL request a dedicated PDN Connection. Note 1: The PDN Connection for VoIP traffic may be characterized with a dedicated QCI. Note 2: Voice Traffic includes SIP, RTP, RTCP and DNS traffic used to resolve the P-CSCF FQDN in order to get the P-CSCF addresses.
TS.64_3.3,1_REQ_006	It SHALL be possible to disable all voice features.
TS.64_3.3,1_REQ_007	The FWA Device SHALL be customizable in order not to have any FXS port or other voice interfaces.

3.3.2 VoIP service: registration and basic call for single-line profile

TS.64_3.3.2_REQ_001	In case of VoIP technology, the FWA Device SHALL be compliant to 3GPP specification TS 24.229 [7].
TS.64_3.3.2_REQ_002	The FWA Device SHALL use the public user identity defined in 3GPP 23.003 [8]. In particular, the UE SHALL use a SIP URL format, with the username part in E.164 telephone number, in international format: e.g. sip:+390612345678@operatordomain.com.
TS.64_3.3.2_REQ_003	The FWA Device SHALL support the private user identity, as specified in 3GPP TS 23.228 [9] par. 4.3.3.1. This parameter is used as username in SIP Digest authentication procedure; it is different from public user identity.
TS.64_3.3.2_REQ_004	The FWA Device SHALL support RFC3263: Location of SIP Servers [10], for the resolution of FQDN of the outbound proxy. The outcome of the process of resolution of the P-CSCF FQDN is a set of P-CSCF IP addresses, ordered by priority.
TS.64_3.3.2_REQ_005	In order to support the P-CSCF FQDN resolution process, the FWA Device SHALL be configured with DNS Servers addresses. Such addresses can be obtained during the Voice PDN connection establishment process.
TS.64_3.3.2_REQ_006	SIP Digest Authentication SHALL be supported. The FWA Device SHALL use digest authentication for the following methods: REGISTER (first registration and registration refresh) and INVITE.
TS.64_3.3.2_REQ_007	The FWA Device SHALL support a password of at least 64 characters for Digest Authentication.
TS.64_3.3.2_REQ_008	The FWA Device SHALL offer a maximum expire time for Registration of 600000 seconds.
TS.64_3.3.2_REQ_009	In order to improve user experience, the FWA Device SHOULD be compliant to RFC5626 (Managing Client-Initiated Connections in SIP) [11], in particular, as regards the use of reg-id and +sip.instance tags. The latter tag is important in order to handle properly multiple registrations of a User Agent that may occur in case of IP address change of the Device.
TS.64_3.3.2_REQ_010	The FWA Device SHALL support the Retry-After header as defined in RFC3261 [12].
TS.64_3.3.2_REQ_011	In case of Failure of Registration, the FWA Device SHALL follow the procedures indicated at par. 5.1.1.2.1 of 3GPP TS 24.229 [7].
TS.64_3.3.2_REQ_012	The FWA Device SHOULD support Registration Event Package according to 3GPP TS 24.229 [7].
TS.64_3.3.2_REQ_013	The FWA Device SHOULD support P-Associated-URI as defined in 3GPP TS 24.229 [7].
TS.64_3.3.2_REQ_014	The FWA Device SHALL support Tel-URI in incoming requests, in compliance with RFC 5341 [13].
TS.64_3.3.2_REQ_015	The FWA Device MAY use Tel-URI in outgoing requests, instead of SIP-URI.

TS.64_3.3.2_REQ_016	The FWA Device SHALL be compliant with mandatory requirements of RFC3261 SIP protocol [12].
TS.64_3.3.2_REQ_017	The FWA Device SHALL be compliant with mandatory requirements of RFC3262 Reliability of Provisional Responses [14].
TS.64_3.3.2_REQ_018	The FWA Device SHALL be compliant mandatory requirements of with RFC3264 The Offer/Answer Model [15].
TS.64_3.3.2_REQ_019	The FWA Device SHALL be compliant with mandatory requirements of RFC3311 The UPDATE method [16].
TS.64_3.3.2_REQ_020	The FWA Device SHALL support an open numbering plan, that is the length of user selection is not predetermined.
TS.64_3.3.2_REQ_021	The FWA Device SHALL use en-bloc selection towards the IMS network. Overlap selection is not foreseen.
TS.64_3.3.2_REQ_022	In case of selections from user containing * or # digits, those digits SHALL be coded as defined in the Device configuration.
TS.64_3.3.2_REQ_023	The FWA Device SHALL support DSCP marking for SIP, RTP and RTCP traffic, with configurable values for DS Code Point.
TS.64_3.3.2_REQ_024	The FWA Device MAY insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity, as per 3GPP 24.229 [7].
TS.64_3.3.2_REQ_025	The FWA Device SHALL accept incoming INVITE without SDP, in this case the UE shall perform the SDP offer in the first reliable 1xx or 200 Response, as specified in RFC3262 [14].
TS.64_3.3.2_REQ_026	The FWA Device SHALL support at least the ITU-T G.711 codec (A-law and μ-law) [18], as specified in RFC3261 [12].
TS.64_3.3.2_REQ_027	The FWA Device SHOULD support ITU-T G.729a [19] [20] and G.722 [21] codecs.
TS.64_3.3.2_REQ_028	If FWA Device supports more than one codec, the order of Codecs in SDP Offer SHALL be configurable.
TS.64_3.3.2_REQ_029	The FWA Device SHALL send and receive DTMF tones complying with RFC4733 [17].
TS.64_3.3.2_REQ_030	The RTP Payload Type for DTMF Events SHALL be configurable.
TS.64_3.3.2_REQ_031	The FWA Device SHALL support an echo canceller compliant to ITU-T G.131 [22], for managing delays less than 150 ms.
TS.64_3.3.2_REQ_032	The FWA Device SHALL be compliant with mandatory requirements of RFC 3550 (RTP) [23].
TS.64_3.3.2_REQ_033	The FWA Device SHALL be compliant with mandatory requirements of RFC 3551 (RTP Profile for Audio and Video Conferences with Minimal Control) [24].
TS.64_3.3.2_REQ_034	The FWA Device SHALL be compliant with mandatory requirements of RFC 3605 (RTCP) [25].
TS.64_3.3.2_REQ_035	The FWA Device SHOULD be compliant with mandatory requirements of RFC 2198 (RTP Payload for Redundant Audio Data) [26].

TS.64_3.3.2_REQ_036	The FWA Device SHALL use Symmetric RTP and RTCP, i.e. the UE shall transmit RTP/RTCP packets using the same UDP port used for receiving RTP/RTCP packets, as stated in RFC 4961 [27].
TS.64_3.3.2_REQ_037	The FWA Device, for Early Media and Ringing Tone Generation, SHALL be compliant, either to RFC 5009 [28], about P-Early-Media header, or RFC 3960 [29], in particular with the "Gateway Model".
TS.64_3.3.2_REQ_038	When a FWA Device has sent the SDP offer, it SHALL be prepared to receive media for any streams described by that offer, as defined in RFC 3264 [15], even before receiving any SIP provisional response.
TS.64_3.3.2_REQ_039	In case the FWA Device is compliant to RFC 3960, the FWA Device, for ringing tone generation, SHOULD implement the following local policy, derived from the example contained in RFC 3960 [29]: 1. Unless a 180 (Ringing) response is received, never generate local ringing. 2. If a 180 (Ringing) has been received but there are no incoming media packets or incoming media packets containing silence, generate local ringing. 3. If a 180 (Ringing) has been received and there are incoming media packets, not containing silence, play them and do not generate local ringing.
TS.64_3.3.2_REQ_040	The FWA Device SHALL support RE-INVITE and UPDATE methods.
TS.64_3.3.2_REQ_041	The use of UPDATE method SHALL be accompanied by 100rel/PRACK.
TS.64_3.3.2_REQ_042	The FWA Device SHALL insert the following header in INVITEs: Supported:100rel
TS.64_3.3.2_REQ_043	The following parameters SHALL be provisionable for VoIP Service from the centralized management platform: • phone number/line identity: user part of the public user identity, to be used in SIP registration process and in all outgoing SIP Requests in the From header. • Authentication username: user part of the private user identity, to be used during SIP Digest Authentication. • Authentication password: to be used for user authentication during SIP Digest Authentication. • Outbound proxy: FQDN or IP Address of the proxy (P-CSCF) to which the FWA Device sends all outgoing SIP requests.
TS.64_3.3.2_REQ_044	The following parameters SHALL be configurable in the FWA Device: • SIP Domain: domain portion of SIP URL. • SIP Server Address: configurable as a FQDN or as an IP Address. • SIP Registrar Address: configurable as a FQDN or as an IP Address. • Expire Time for Registration. • VoIP Codec list and priority. • RTP payload type to be used for RTP-events.

	- DSCP values to be used for both SIP and RTP/RTCP. - Voice Activity Detection on/off. - Silence Suppression on/off. - Dejitter buffer controls: static/dynamic depth. - Coding to be used for * and # characters in SIP signalling (dialled sequences): normal ASCII or URL-encoded. - meaning of a trailing # in user selection not beginning with * or #: end-of-selection marker (speed dial) vs. part of the user selection. - Emergency numbers list. - Conference Factory URI.
TS.64_3.3.2_REQ_045	The FWA Device SHOULD discard silently any SIP/RTP/RTCP packet coming from IP source addresses different from the IP Address(es) of the P-CSCF discovered by the Registration Procedure.
TS.64_3.3.2_REQ_046	The FWA Device SHALL support multiple SIP dialogs within a single session, as specified in RFC3261 [12]. Note: as specified in RFC3261 [12], a dialog is defined by Call-ID, ‘From’ tag, and ‘To’ tag.
TS.64_3.3.2_REQ_047	The FWA Device SHALL support incoming INVITE with the Request-URI different from the ‘To’ header, as specified in RFC3261 [12]. Note: as an example, this occurs when the incoming INVITE has been diverted by the network due to some Diversion service.
TS.64_3.3.2_REQ_048	The FWA Device SHALL reply to an incoming INVITE with Request-URI different from the SIP identity(-ies) configured on the FWA Device itself, with a 404 Not Found response, as specified in RFC3261 [12].

3.3.3 VoIP service: supplementary services for single-line profile

TS.64_3.3.3_REQ_001	The procedures for activation, deactivation and interrogation of Supplementary Services through the FXS interface, are based on the use of specific Feature Access Codes (FAC), that is, dialled sequences normally containing * and # keys. The FWA Device SHALL support the signalling of such Supplementary Services codes towards the IMS network, by means of the Gm Interface, that is sending an INVITE with the Request URI containing the * and # sequence dialled by the user.
TS.64_3.3.3_REQ_002	If the FWA Device supports activation/deactivation/interrogation Supplementary Services via the Ut interface towards the IMS, the FAC for activation/deactivation/interrogation SHALL be configurable on the Device.

3.3.3.1 OIP/OIR - ORIGINATING IDENTITY PRESENTATION/ RESTRICTION

TS.64_3.3.3.1_REQ_001	The FWA Device SHALL support the P-Asserted-Identity header according to RFC 3325 [30].

TS.64_3.3.3.1_REQ_002	The FWA Device SHALL support OIP (Originating Identity Presentation) and OIR (Originating Identity Restriction) according to 3GPP TS 24.607 [31]. In particular: • If both From and P-Asserted-Identity headers are present, the UE has to provide the Originating Identity Presentation giving priority to P-A-I header with respect to From header. • If multiple P-A-I headers are present in the incoming messages, the UE SHALL provide OIP according to the P-A-I in tel-URI format.
TS.64_3.3.3.1_REQ_003	For the purpose of OIP Service, the FWA Device SHALL support ETSI EN 300 659 on FXS port. In particular, the cases of OIP service Unsubscribed and Identity Restricted SHALL be treated with the ad-hoc coding, defined in ETSI EN 300 659_3 par. 5.4.4 [32].
TS.64_3.3.3.1_REQ_004	For the purpose of OIP service on FXS port, the FWA Device SHOULD allow reformat the Identity to be displayed, so for instance to remove international prefix from domestic numbers.
TS.64_3.3.3.1_REQ_005	The FWA Device SHOULD perform OIP service on FXS port also in combination with Call Waiting service.

3.3.3.2 CDIV – COMMUNICATION DIVERSION

TS.64_3.3.3.2_REQ_001	The FWA Device SHALL support network-based communication diversion (CDIV) services according to 3GPP TS 24.604 (Communication Diversion Unconditional, No Reply, On Busy, to Voice Mail) [33].
TS.64_3.3.3.2_REQ_002	The FWA Device SHALL support RFC 3842 “A message summary and Message Waiting Indication Event Package for the Session Initiation Protocol” [34] in order to provide Centralized Voice Mail Service.

3.3.3.3 ACB/CB/DND – ANONYMOUS CALL REJECTION/COMMUNICATION BARRING/DO NOT DISTURB

TS.64_3.3.3.3_REQ_001	The FWA Device SHALL support Anonymous Call Rejection (ACR), Communication Barring (CB) and Do Not Disturb (DND) services according to 3GPP TS 24.611 [35].

3.3.3.4 HOLD - COMMUNICATION HOLD

TS.64_3.3.3.4_REQ_001	The FWA Device SHALL support Communication on Hold service according to 3GPP TS 24.610 [36].
TS.64_3.3.3.4_REQ_002	The Keypad procedures for holding an active call, switching between an active and a held call, terminating an active call and resuming an held call, SHALL be configurable.
TS.64_3.3.3.4_REQ_003	In order to provide PSTN emulation of the hold service, FWA Device SHOULD hold an active call when the local user presses the Register Recall (“R” key) on the telephone; after holding the call, offer dial tone to the telephone, in order to allow dialling a new call.

TS.64_3.3.3.4_REQ_004	When a FWA Device has a held call and user is dialling a new number, it SHOULD terminate new call attempt and return to the held call, if the user presses the Register Recall ("R") key on the telephone during: dial tone, dialling, ringing, busy, fast busy.
TS.64_3.3.3.4_REQ_005	In order to provide PSTN emulation of the hold service, when a FWA Device has an active call and a held call, if the user of the FWA Device hangs up the telephone, the FWA Device SHOULD: • terminate the active call. • ring back (recall) the FXS port • when the local user answers, resume the held call. • If the local user doesn't answer in 30 seconds, release the held call.
TS.64_3.3.3.4_REQ_006	In order to provide PSTN emulation of the hold service, when a FWA Device has an active call and a held call, if the remote user terminates the active call, the FWA Device SHOULD: • Play 5 seconds of fast-busy as a "guard tone", then • Resume held call.
TS.64_3.3.3.4_REQ_007	With reference to TS.64_3.3.3_REQ_015, if the local user hangs up the telephone during the guard tone, the FWA Device SHOULD: • ring back (recall) the FXS port • when the local user answers, resume the held call. • If the local user doesn't answer in 30 seconds, release the held call.

3.3.3.5 CW - COMMUNICATION WAITING

TS.64_3.3.3.5_REQ_001	The FWA Device SHALL support Communication Waiting service according to 3GPP TS 24.615 [37].
TS.64_3.3.3.5_REQ_002	The FWA Device SHOULD be able to recognize an "INVITE on waiting" when the incoming INVITE has the specific XML CW indication. Note: the ability to recognize the "INVITE on waiting" could be needed in order to avoid ringing all phones connected to UE when the Call Waiting service has to be provided.
TS.64_3.3.3.5_REQ_003	When required, the FWA Device SHALL generate a configurable Call Waiting Tone (Frequency, Cadence, Level).
TS.64_3.3.3.5_REQ_004	The Call Waiting service SHALL NOT be applied to FXS port in other states than active conversation (e.g., idle, dialling, ringing, hold, reorder/congestion.)
TS.64_3.3.3.5_REQ_005	The Keypad procedures for answering a waiting call while holding an active call, answering a waiting call while terminating an active call, rejecting a waiting call, SHALL be configurable.
TS.64_3.3.3.5_REQ_006	If the FWA Device supports FAX or POS/modem, it SHOULD a support configurable feature interaction between FAX/POS and Call Waiting

	service: if a FAX/POS call is ongoing, a new incoming call has not to be served with call waiting service but rejected with a 4xx answer.
TS.64_3.3.3.5_REQ_007	The FWA Device SHOULD allow enabling/disabling CW service on a per-FXS port basis.
TS.64_3.3.3.5_REQ_008	On a FXS port, at most one active call and one held can be handled simultaneously. Hence, the FWA Device equipped with one FXS port SHOULD reject an incoming call with Busy when there are simultaneously an active call and a held call.

3.3.3.6 CONF - CONFERENCE

TS.64_3.3.3.6_REQ_001	The FWA Device SHALL support N-Way Conference service according to 3GPP TS 24.147 [38].
TS.64_3.3.3.6_REQ_002	The Keypad procedures SHALL be configurable.

3.3.3.7 CCBS – COMMUNICATION COMPLETION ON BUSY SUBSCRIBER

TS.64_3.3.3.7_REQ_001	The FWA Device SHALL support CCBS service according to 3GPP TS 24.642 [39].
TS.64_3.3.3.7_REQ_002	The CCBS ring pattern SHALL be played in case the incoming INVITE contains the specific Alert-Info Header: Alert-Info: <urn:alert:service:auto-callback>

3.3.3.8 ECT – EXPLICIT COMMUNICATION TRANSFER

TS.64_3.3.3.8_REQ_001	The FWA Device SHOULD support Explicit Communication Transfer (ECT) service according to 3GPP TS 24.629 [40].
TS.64_3.3.3.8_REQ_002	The Keypad procedures SHALL be configurable.

3.3.3.9 TIP/TIR – TERMINATING IDENTIFICATION PRESENTATION/TERMINATING IDENTIFICATION RESTRICTION

TS.64_3.3.3.9_REQ_001	The FWA Device SHOULD support TIP/TIR services according to 3GPP TS 24.608 [41].

3.3.3.10 MCID – MALICIOUS COMMUNICATION IDENTIFICATION

TS.64_3.3.3.10_REQ_001	The FWA Device SHOULD support MCID service according to 3GPP TS 24.616 [42].

3.3.4 FXS interface requirements

Requirements in this section apply to FWA Devices supporting VoLTE profile and FWA Devices supporting VoIP Profile.

TS.64_3.3.4_REQ_001	The FWA Device SHALL support at least one FXS (Foreign eXchange Station) port, compliant to ETSI ES 201 970 [43].
TS.64_3.3.4_REQ_002	The FXS interface SHALL support DTMF Dialling.

TS.64_3.3.4_REQ_003	The FXS interface SHALL recognize Register Recall signal, as specified in ETSI ES 201 970 [43].
TS.64_3.3.4_REQ_004	The FXS interface SHALL support multiple terminals arrangements; in particular, as regards ringing, the FXS interface SHALL support a value of REN (Ringing Equivalence Number) >=4.
TS.64_3.3.4_REQ_005	The FXS interface SHALL support narrowband voice (3.1kHz net bandwidth, in the range 300-3400 Hz) in conformance to Rec. ITU-T Q.522 [44].
TS.64_3.3.4_REQ_006	The FXS interface SHOULD support wideband voice (8 kHz bandwidth).
TS.64_3.3.4_REQ_007	The following parameters related to the FXS interface SHALL be customizable: • Supervision Tones: for instance, Dial, Ringing, Busy, Congestion, Call Waiting. Customization shall be possible as regards cadence, frequency and level. • Timers: initial digit timeout, interdigit timeout (Note: interdigit timeout is used to infer the end of the user selection). • Ringing current: customization SHALL be possible as regards cadence, frequency and level. • Polarity Reversal. • Input impedance • TX-gain • RX-gain • DC feed voltage and current limit. • Howler tone control (on/off).

3.3.5 FAX and POS (Point of Sale) Requirements

The requirements in this section apply to a FWA Device supporting VoIP profile.

TS.64_3.3.5_REQ_001	The FWA Device SHOULD support FAX and/or POS service using the same FXS port for voice.
TS.64_3.3.5_REQ_002	The FWA Device SHOULD support FAX transmission, at least by means of upspeed to ITU-T G.711 [18].
TS.64_3.3.5_REQ_003	The FWA Device SHOULD support POS/modem transmission, at least by means of upspeed to ITU-T G.711 [18].
TS.64_3.3.5_REQ_004	The called FWA Device SHOULD send the ReINVITE (upspeed to G.711), when it detects the CED/ANSam in case of FAX; in case of modem/POS, the called FWA Device SHOULD send the ReINVITE (upspeed to G.711), when it detects the modem carrier signal.
TS.64_3.3.5_REQ_005	When performing upspeed to G.711, either initiated by the FWA Device or by the remote party, the FWA Device SHOULD disable, for the ongoing call, all voice signal processing features, such as echo canceller, voice activity detection. Note: this is needed as voice signal processing features introduce non-linearities in the coded signal; instead, for the transport of voice-band

	data over G.711, it is necessary to keep the original signals unmodified from the source to the destination.
TS.64_3.3.5_REQ_006	When performing upspeed to G.711, either initiated by the FWA Device or by the remote party, the FWA Device SHOULD use a static dejitter buffer.
TS.64_3.3.5_REQ_007	The FWA Device SHOULD support T.38 fax transmission, as specified in ITU-T T.38 (09/2010) [45]. In particular: a. The calling FWA Device SHOULD include, in the SDP Offer of the INVITE, the line a=cdsc:1 image udptl t38 b. The called FWA Device SHOULD perform an upspeed to T.38, when it detects the V.21 preamble, by sending a ReINVITE, if in the received INVITE is present the line a=cdsc:1 image udptl t38.
TS.64_3.3.5_REQ_008	The FWA Device MAY support the capabilities for T.38 defined by Annex D of ITU-T T.38 (11/2015) [46].
TS.64_3.3.5_REQ_009	In case a ReINVITE fails, for example because the remote party is unable to perform upspeed (i.e. a 488 Not Acceptable Here Response is received), the FWA Device SHALL continue the session using the previously negotiated codec(s). In this case, the FWA Device MAY send a ReINVITE to confirm again to the remote party the previously negotiated codecs.
TS.64_3.3.5_REQ_010	The FWA Device SHOULD allow, on a per-FXS port basis, the possibility to choose whether to use only the G.711 codec.
TS.64_3.3.5_REQ_011	When the configuration for use of the G.711 codec only is enabled, the FWA Device SHOULD disable all voice signal processing features, such as echo canceller, voice activity detection.
TS.64_3.3.5_REQ_012	When the configuration for use of the G.711 codec only is enabled, the FWA Device SHOULD use a static dejitter buffer.
TS.64_3.3.5_REQ_013	The FWA Device SHOULD allow the possibility to enable or disable T.38, on a device basis.

3.4 Networking Features

Except where explicitly indicated, the Requirements of this section apply to the Indoor FWA Device, the InDoor Unit and the OutDoor Unit of an OutDoor FWA Solution.

3.4.1 Interfaces

TS.64_3.4.1_REQ_001	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.
TS.64_3.4.1_REQ_002	For the physical interfaces for LAN Ethernet, the 1000BASE-T electrical interface SHOULD be used.
TS.64_3.4.1_REQ_003	Different physical interfaces for LAN Ethernet, compliant to the standards, e.g. 1000BASE-TX, MAY be used in alternative to 1000BASE-T, depending on market and MNOs needs.

TS.64_3.4.1_REQ_004	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 as defined in the performance requirements below.
TS.64_3.4.1_REQ_005	For the physical interfaces for the IDU-ODU, if Ethernet is used, the BASE-T electrical interface SHOULD be used.
TS.64_3.4.1_REQ_006	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.

3.4.2 Performance

TS.64_3.4.2_REQ_001	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.
TS.64_3.4.2_REQ_002	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.
TS.64_3.4.2_REQ_003	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.
TS.64_3.4.2_REQ_004	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.
TS.64_3.4.2_REQ_005	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.
TS.64_3.4.2_REQ_006	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.

Note: in the Outdoor FWA Solution, requirements TS.64_3.4.2_REQ_001, TS.64_3.4.2_REQ_002, TS.64_3.4.2_REQ_003 and TS.64_3.4.2_REQ_004 apply only to the Indoor Unit – LAN-LAN traffic is managed only by the Indoor Unit.

For TS.64_3.4.2_REQ_005 and TS.64_3.4.2_REQ_006, supported throughputs must align with the maximum WAN throughout. Figures for selected 4G and 5G device categories are as follows:

Device Category	Maximum Downlink (DL) throughput	Maximum Uplink (UL) throughput
LTE Category DL11UL5	600 Mbps	75 Mbps
LTE Category DL12UL13	600 Mbps	150 Mbps

Device Category	Maximum Downlink (DL) throughput	Maximum Uplink (UL) throughput
LTE Category DL16UL13	975 Mbps	150 Mbps
LTE Category DL18UL18	1200 Mbps	210 Mbps
NSA DL12UL13 LTE + 100MHz NR	2100 Mbps	200 Mbps
NSA DL12UL13 LTE + 140MHz NR	2700 Mbps	200 Mbps
NSA DL12UL13 LTE + 200MHz NR	3600 Mbps	200 Mbps
SA 100MHz NR	1500 Mbps	100 Mbps
SA 140MHz NR	2100 Mbps	140 Mbps
SA 200MHz NR	3000 Mbps	200 Mbps

Note: The table assumes NR channels are TDD configured as 70:30 DL:UL

3.4.3 Protocols

TS.64_3.4.3_REQ_001	The FWA Device SHALL support Internet Protocol version 4 (IPv4), defined in IETF RFC 791 [60].
TS.64_3.4.3_REQ_002	The FWA Device SHALL support Internet Protocol version 6 (IPv6), defined in IETF RFC 8200 [61] and further amendments defined by IETF.
TS.64_3.4.3_REQ_003	The FWA Device SHALL support Address Resolution Protocol (ARP), defined in IETF RFC 826 [62] and further amendments (IETF RFC 5227 [63], IETF RFC 5494 [64]).
TS.64_3.4.3_REQ_004	The FWA Device SHALL support Network Discovery Protocol for IPv6 (NDP) defined in IETF RFC 4861 [65] and further amendments defined by IETF.
TS.64_3.4.3_REQ_005	The FWA Device SHALL support Internet Control Message Protocol (ICMP) defined in IETF RFC 792 [66] and further amendments defined by IETF (RFC 950 [67], RFC 4884 [68], RFC 6633 [69], RFC 6918 [70]).
TS.64_3.4.3_REQ_006	The FWA Device SHALL support Internet Control Message Protocol version 6 for IPv6 (ICMPv6) defined in IETF RFC 4443 [71].
TS.64_3.4.3_REQ_007	The FWA Device SHALL implement a Network Time Protocol (NTP) client as defined in IETF RFC 5905 [72] and further amendments.
TS.64_3.4.3_REQ_008	The FWA Device SHALL support Internet Group Management Protocol, version 3 (IGMPv3), defined in IETF RFC 3376 [73].
TS.64_3.4.3_REQ_009	The FWA Device SHALL support IGMP Proxy as defined in IETF RFC 4605 [74].
TS.64_3.4.3_REQ_010	The FWA Device SHALL support QoS Treatment both at level 2 (p-bits of 802.1q VLAN Tag [75]) and at level 3 (Differentiated Services Code Point of the IP header).

TS.64_3.4.3_REQ_011	The FWA Device SHALL support the Differentiated Services (DiffServ) architecture and behaviours defined in IETF RFC 2474 [76], RFC 2475 [77], RFC 2597 [78], RFC 3260 [79]).
TS.64_3.4.3_REQ_012	The behaviours of traffic classification, marking, remarking, queueing, scheduling, policing, shaping SHALL be applicable both to internally generated traffic and to traffic coming from LAN and destined to the WAN.
TS.64_3.4.3_REQ_013	At least four queues SHALL be supported on the WAN interface, of which one Strict Priority scheduling, and the others with configurable scheduling mechanism (e.g. Weighted Fair Queueing, Weighted Round Robin, ..).
TS.64_3.4.3_REQ_014	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.
TS.64_3.4.3_REQ_015	The FWA Device SHALL support VLAN Tagging, compliant to IEEE 802.1q standard [75].

3.4.4 DHCP

TS.64_3.4.4_REQ_001	The FWA Device SHALL support Dynamic Host Configuration Protocol (DHCP) defined in IETF RFC 2131 [98].
TS.64_3.4.4_REQ_002	The FWA Device SHALL support DHCP Options defined in IETF RFC 2132 [99].
TS.64_3.4.4_REQ_003	The FWA device MAY implement DHCP options 60 and 43 for automatic provision of ACS parameters.
TS.64_3.4.4_REQ_004	The DHCP Server implemented by the FWA Device SHALL manage at least 254 addresses.
TS.64_3.4.4_REQ_005	It SHALL be possible to define any IPv4 Unicast subnet for the private LAN and DHCP pool.
TS.64_3.4.4_REQ_006	The DHCP Server implemented by the FWA Device SHALL support Duplicate Address Detection (DAD) functionality.
TS.64_3.4.4_REQ_007	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.
TS.64_3.4.4_REQ_008	The FWA Device SHALL support hostnames presented by the hosts (DHCP clients) with DHCP Option 12.
TS.64_3.4.4_REQ_009	The FWA Device SHALL properly manage the cases of overlapping hostnames and hostnames non presented by clients, by assigning to client’s unambiguous hostnames by means of Option 12.
TS.64_3.4.4_REQ_010	The FWA Device SHALL support Dynamic Host Configuration Protocol for IPv6 (DHCPv6) defined in IETF RFC 8415 [100].
TS.64_3.4.4_REQ_011	The FWA Device SHALL support Prefix Delegation for IPv6 (DHCPv6) defined in IETF RFC 8415 [100].

TS.64_3.4.4_REQ_012	The FWA Device SHALL support Prefix Exclude for IPv6 (DHCPv6) defined in IETF RFC 8415 [100].

3.4.5 NAT & Bridge operation

TS.64_3.4.5_REQ_001	The FWA Device SHALL support IP Network Address Translator (NAT) as defined in IETF RFC 3022 [101].
TS.64_3.4.5_REQ_002	The Network Address Translator functionality implemented by the FWA Device SHALL be compliant to the behaviours defined in IETF RFC 4787 [102].
TS.64_3.4.5_REQ_003	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.
TS.64_3.4.5_REQ_004	It SHALL be possible to configure at least 32 Port Mapping entries.
TS.64_3.4.5_REQ_005	The FWA Device SHALL support CLAT functionality according to IETF RFC 6145 [103].
TS.64_3.4.5_REQ_006	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.
TS.64_3.4.5_REQ_007	The FWA Device SHALL implement a configurable Application Layer Gateway functionality (ALG), as defined in IETF RFC 2663 [80], at least for the following protocols: SIP, IPSec, PPTP, L2TP.

3.4.6 MTU

TS.64_3.4.6_REQ_001	The FWA Device SHALL support a default MTU size of 1380 bytes.
TS.64_3.4.6_REQ_002	The default MTU size SHALL be customisable according to network requirements.
TS.64_3.4.6_REQ_003	The FWA Device SHALL support network override of the default MTU size in IPv4 operation via Protocol Configuration Options (3GPP TS24.008 [104]).
TS.64_3.4.6_REQ_004	The FWA Device SHALL support network override of the default MTU size in IPv6 operation via Router Advertisement (IETF RFC 4861 [65]).

3.4.7 DNS

TS.64_3.4.7_REQ_001	The FWA Device SHALL support Domain Name System (DNS) compliant to IETF RFC 1034 [105], RFC 1035 [106] and further amendments defined by IETF.
TS.64_3.4.7_REQ_002	The FWA Device SHALL be able, on a configuration basis, to act as DNS Server for the Hosts in LAN.

TS.64_3.4.7_REQ_003	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: • The FWA Device itself, if it's configured to act as a DNS Server; • The DNS server addresses received from the network, if the FWA Device is not configured to act as a DNS Server; • Optionally, other DNS Server addresses configured on the FWA Device.
TS.64_3.4.7_REQ_004	The FWA Device SHALL support a configurable Dynamic DNS (DDNS) Service, allowing the FWA Device to be addressable from the Internet with an FQDN. Note: some MNOs may wish to remove this service via customization.
TS.64_3.4.7_REQ_005	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.
TS.64_3.4.7_REQ_006	For Static DNS operation the FWA Device SHALL support Recursive DNS.
TS.64_3.4.7_REQ_007	For Static DNS operation the FWA Device SHALL NOT support Iterative DNS.
TS.64_3.4.7_REQ_008	The FWA Device SHALL support unencrypted DNS access.
TS.64_3.4.7_REQ_009	The FWA Device SHALL support DNS access via HTTPS (IETF RFC 8484 [107]).
TS.64_3.4.7_REQ_010	The FWA Device SHALL support DNS access via TLS.
TS.64_3.4.7_REQ_011	The FWA device SHALL be protected against DNS Rebind Vulnerability.
TS.64_3.4.7_REQ_012	To prevent DNS spoofing, source ports and Transaction-IDs SHALL be selected randomly by the CPE.

3.4.8 Security

TS.64_3.4.8_REQ_001	The FWA Device SHALL implement a configurable DeMilitarized Zone (DMZ) functionality, allowing an internal host in LAN to be fully exposed on WAN.
TS.64_3.4.8_REQ_002	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).
TS.64_3.4.8_REQ_003	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.
TS.64_3.4.8_REQ_004	It SHALL be possible to configure at least 32 Filtering entries.
TS.64_3.4.8_REQ_005	The FWA Device SHOULD implement a configurable (on/off) UPnP Discovery functionality, compliant to UPnP Forum Standard: Device Control Protocols.

TS.64_3.4.8_REQ_006	UPnP functionality SHALL be blocked on the WAN side.
TS.64_3.4.8_REQ_007	If the FWA Device supports UPnP, it SHOULD be disabled in Factory default configuration.
TS.64_3.4.8_REQ_008	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).
TS.64_3.4.8_REQ_009	The FWA Device SHOULD implement a configurable VPN functionality, both as a VPN-client and a VPN-server, with L2TP/IPSec PSK or PPTP.
TS.64_3.4.8_REQ_010	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.
TS.64_3.4.8_REQ_011	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.
TS.64_3.4.8_REQ_012	The FWA Device SHALL implement a configurable (at least with on/off behaviours) stateful IPv4 Firewall.
TS.64_3.4.8_REQ_013	The FWA Device SHALL implement a Denial of Service (DoS) protection functionality.
TS.64_3.4.8_REQ_014	The DoS functionality SHALL remain enabled even when the Firewall has been disabled by user configuration
TS.64_3.4.8_REQ_015	The behaviour of the FWA Device to ICMP messages coming from WAN interface SHALL be configurable.
TS.64_3.4.8_REQ_016	The FWA Device SHALL implement a configurable (at least with on/off behaviours) stateful IPv6 Firewall.
TS.64_3.4.8_REQ_017	The IPv6 and IPv4 firewall SHALL be independently configurable
TS.64_3.4.8_REQ_018	The IPv6 and IPv4 firewall status SHALL be presented independently.
TS.64_3.4.8_REQ_019	The FWA Device SHALL NOT allow outgoing traffic originated from a LAN IP address outside the range defined by the FWA Device itself.
TS.64_3.4.8_REQ_020	In Factory Reset condition, the status of the firewall SHALL be enabled.

3.4.9 Customisation

TS.64_3.4.9_REQ_001	It SHALL be possible for a MNO to customize a FWA Device in order to hide to the end-user any of the functionality detailed in requirements TS.64_3.4.3_REQ_014, TS.64_3.4.5_REQ_003, TS.64_3.4.5_REQ_004, TS.64_3.4.5_REQ_007, TS.64_3.4.7_REQ_004, TS.64_3.4.7_REQ_005, TS.64_3.4.8_REQ_001 to TS.64_3.4.8_REQ_011.

3.4.10 USB Port

TS.64_3.4.10_REQ_001	The FWA Device MAY support a Universal Serial Bus (USB) interface.

The following requirements apply ONLY IF the FWA Device supports a USB Interface for functions other than powering the FWA Device.

TS.64_3.4.10_REQ_002	The USB interface SHALL be compliant to the Universal Serial Bus Specification version 3.1 [108] or higher.
TS.64_3.4.10_REQ_003	The USB Interface receptacle SHALL be any of Type-A, Type-Micro B or Type-C.
TS.64_3.4.10_REQ_004	The USB Interface SHOULD supply a current of at least 1.5A
TS.64_3.4.10_REQ_005	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.
TS.64_3.4.10_REQ_006	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.
TS.64_3.4.10_REQ_007	The FWA Device SHOULD use SMBv2 (or higher) protocol to enable the sharing of an USB Mass Storage Hard Disk Devices between LAN hosts.
TS.64_3.4.10_REQ_008	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.
TS.64_3.4.10_REQ_009	The FWA Device SHALL NOT support SMBv1 protocol.
TS.64_3.4.10_REQ_010	The USB Interface SHALL block firmware upgrade, logging, tracing and similar local management and troubleshooting activities on the FWA Device.

3.5 Wi-Fi

Requirements in this section apply to the Indoor FWA Solution and to the InDoor Unit (IDU) of the Outdoor FWA Solution. There may be MNO or market specific Wi-Fi requirements for the outdoor unit (ODU).

3.5.1 Standards

TS.64_3.5.1_REQ_001	The FWA Device SHALL integrate a Wi-Fi 4 (IEEE 802.11n [83]) Access Point (AP), or later standards, operating on 2.4 GHz bands.
TS.64_3.5.1_REQ_002	The FWA Device SHALL integrate a Wi-Fi 5 (IEEE 802.11ac [84]) Access Point (AP), or later standards, operating on 5 GHz bands.
TS.64_3.5.1_REQ_003	The FWA Device SHOULD integrate a Wi-Fi 6 (IEEE 802.11ax [85]) Access Point (AP), or later standards, operating on both 2.4 and 5 GHz bands.
TS.64_3.5.1_REQ_004	The FWA Device MAY integrate a Wi-Fi 6E (IEEE 802.11ax [85]) Access Point (AP), or later standards, operating on 2.4, 5 and 6 GHz bands.
TS.64_3.5.1_REQ_005	The FWA Device SHALL be certified (WFA Certification Program): Wi-Fi CERTIFIED 5.

TS.64_3.5.1_REQ_006	If Wi-Fi 6 is supported, the FWA Device SHALL be certified (WFA Certification Program): Wi-Fi CERTIFIED 6.
TS.64_3.5.1_REQ_007	The FWA Device SHALL be certified (WFA Certification Program): WPA3.
TS.64_3.5.1_REQ_008	The FWA Device SHALL be certified (WFA Certification Program): Wi-Fi Protected Setup (PBC).

3.5.2 MIMO capabilities, Bandwidth, Modulation and Coding schemes

TS.64_3.5.2_REQ_001	The Wi-Fi AP of a FWA Device SHALL support at least MIMO 2x2 on all supported frequency bands.
TS.64_3.5.2_REQ_002	The Wi-Fi AP of a FWA Device SHOULD support MIMO 4x4 on all supported frequency bands.
TS.64_3.5.2_REQ_003	The Wi-Fi AP of a FWA Device MAY support MIMO higher than 4x4 on some or all supported frequency bands.
TS.64_3.5.2_REQ_004	An 802.11n [83] AP of a FWA Device SHALL support a bandwidth of 40 MHz.
TS.64_3.5.2_REQ_005	An 802.11ac [84] AP of a FWA Device SHALL support a bandwidth of 80 MHz in the 5 GHz band.
TS.64_3.5.2_REQ_006	An 802.11ax [85] AP of a FWA Device SHALL support a bandwidth of 40 MHz in the 2.4 GHz band.
TS.64_3.5.2_REQ_007	An 802.11ax AP of a FWA Device SHALL support a bandwidth of 80 MHz in the 5 GHz band.
TS.64_3.5.2_REQ_008	An 802.11ax AP of a FWA Device SHOULD support a bandwidth of 160 MHz in the 5 GHz band.
TS.64_3.5.2_REQ_009	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.
TS.64_3.5.2_REQ_010	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.
TS.64_3.5.2_REQ_011	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.
TS.64_3.5.2_REQ_012	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.

3.5.3 Performance

TS.64_3.5.3_REQ_001	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

TS.64_3.5.3_REQ_002	All the Wi-Fi interfaces SHALL NOT exceed the regulatory limits as regards output power level (EIRP).
TS.64_3.5.3_REQ_003	For Wi-Fi antenna performance, the FWA Device SHALL comply to the requirements specified in TS.49 [97].

Figures for selected Wi-Fi AP types are as follows:

Wi-Fi AP Type	Theoretical Maximum Physical bit rate
802.11n 2.4 GHz, MIMO 2x2, 40 MHz, 64-QAM	300 Mbps
802.11n 2.4 GHz, MIMO 4x4, 40 MHz, 64-QAM	600 Mbps
802.11ac 5 GHz, MIMO 2x2, 80 MHz, 256-QAM	866 Mbps
802.11ac 5 GHz, MIMO 4x4, 80 MHz, 256-QAM	1733 Mbps
802.11ax 2.4+5 GHz, MIMO 2x2 + 2x2, 80 MHz, 1024-QAM	600 + 1200 Mbps
802.11ax 2.4+5 GHz, MIMO 2x2 + 2x2, 160 MHz, 1024-QAM	600 + 2400 Mbps
802.11ax 2.4+5 GHz, MIMO 4x4 + 4x4, 160 MHz, 1024-QAM	1200 + 4800 Mbps

3.5.4 Service Set Identifier (SSID)

TS.64_3.5.4_REQ_001	The AP of a FWA Device SHALL permit the configuration of one main SSID for each supported band.
TS.64_3.5.4_REQ_002	The AP of a FWA Device SHALL permit the configuration of at least one guest SSID.
TS.64_3.5.4_REQ_003	The guest SSID(s) SHALL NOT permit the access to the configuration of the FWA Device.
TS.64_3.5.4_REQ_004	The guest SSID(s) SHALL NOT permit traffic between hosts in LAN.
TS.64_3.5.4_REQ_005	Each SSID SHALL be configurable to operate on one or more frequency bands.
TS.64_3.5.4_REQ_006	Each SSID SHALL be configurable as regards the Authentication and Security mechanisms adopted.
TS.64_3.5.4_REQ_007	Each SSID SHALL be configurable as regards the SSID broadcasting.
TS.64_3.5.4_REQ_008	The default configuration of the FWA Device SHALL be with the same SSID for all supported bands.
TS.64_3.5.4_REQ_009	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.

3.5.5 Channel and Bandwidth Selection

TS.64_3.5.5_REQ_001	The AP of a FWA Device SHALL permit the manual channel selection on all supported bands.
TS.64_3.5.5_REQ_002	The AP of a FWA Device SHALL support Automatic Channel Selection on all supported bands, in order to select the less interfered channels.
TS.64_3.5.5_REQ_003	If enabled, the Automatic Channel Selection SHALL be performed every time the AP is turned on.
TS.64_3.5.5_REQ_004	The AP of a FWA Device SHALL support Periodic Automatic Channel Selection.
TS.64_3.5.5_REQ_005	The default value for Periodic Automatic Channel Selection SHOULD be 24 hours.
TS.64_3.5.5_REQ_006	The Periodic Automatic Channel Selection SHALL be configurable by the MNO through customization.
TS.64_3.5.5_REQ_007	The AP of a FWA Device SHALL permit the manual Bandwidth selection on all supported bands.
TS.64_3.5.5_REQ_008	The AP of a FWA Device SHALL support Automatic Bandwidth Selection on all supported bands.

3.5.6 Clients

TS.64_3.5.6_REQ_001	The AP of a FWA Device SHALL support at least 64 clients.

3.5.7 Security

TS.64_3.5.7_REQ_001	The AP of a FWA Device SHALL support all encryption algorithms foreseen by the supported standards.
TS.64_3.5.7_REQ_002	The AP of a FWA Device SHALL support all security and authentication features foreseen by the supported standards.
TS.64_3.5.7_REQ_003	The AP of a FWA Device SHALL support Open Mode security.
TS.64_3.5.7_REQ_004	The AP of a FWA Device SHOULD support Wi-Fi Alliance Wi-Fi Protected Access 2 (WPA2) defined in IEEE 802.11i [109]. Note: the support of WPA2 is required for compatibility reasons, although it is recognized the security of WPA2 is already compromised.
TS.64_3.5.7_REQ_005	The AP of a FWA Device SHALL support Wi-Fi Alliance Wi-Fi Protected Access 3 (WPA3) [110].
TS.64_3.5.7_REQ_006	The AP of a FWA Device SHALL support Temporal Key Integrity Protocol (TKIP) security protocol.
TS.64_3.5.7_REQ_007	The AP of a FWA Device SHALL support CTR mode with CBC-MAC Protocol (CCMP) security protocol, also known as Advanced Encryption Standard (AES).
TS.64_3.5.7_REQ_008	The AP of a FWA Device SHALL support WPA2/WPA3 personal mixed mode of operation.

TS.64_3.5.7_REQ_009	The AP of a FWA Device SHOULD support WPA2/WPA3 Enterprise mode of operation.
TS.64_3.5.7_REQ_010	The FWA Device default configuration SHALL be personal mixed mode WPA2/WPA3 with AES.
TS.64_3.5.7_REQ_011	The passphrase (pre-shared key, PSK) configured in factory setting SHALL have a length of at least 20 characters.
TS.64_3.5.7_REQ_012	The passphrase (pre-shared key, PSK) configured in factory setting SHALL NOT contain information that consist of or are derived from data or parts of data that depend on the Device itself.
TS.64_3.5.7_REQ_013	The procedure to set the Wi-Fi passphrase to a different value SHALL be supported by a mechanism showing the strength of the new desired passphrase based on the number of characters and classes of characters (e.g. numbers, letters).
TS.64_3.5.7_REQ_014	The FWA Device SHALL implement a configurable overall Wi-Fi control functionality, letting the user to configure which days of the week/which hours of the day the wireless service is turned ON/OFF.
TS.64_3.5.7_REQ_015	The Wi-Fi control functionality MAY be implemented with finer granularity, e.g. on a per-radio interface basis or on a per-SSID basis.

3.5.8 Wi-Fi protected Setup (WPS)

TS.64_3.5.8_REQ_001	The AP of a FWA Device SHALL support WPS in order to facilitate the association between clients and the AP of the FWA Device.
TS.64_3.5.8_REQ_002	The AP of a FWA Device SHALL support WPS with Push Button mode.
TS.64_3.5.8_REQ_003	The WPS Push Button MAY be either physical or logical (i.e., in the Web UI of the FWA Device) or both.
TS.64_3.5.8_REQ_004	The AP of a FWA Device SHALL support WPS PIN mode, with PIN generated by client.
TS.64_3.5.8_REQ_005	The WPS PIN mode with PIN generated by the AP of the FWA Device SHALL be forbidden.
TS.64_3.5.8_REQ_006	WPS Push Button authentication SHALL only allow a limited number of attempts per period of time, to be protected against brute force attacks.
TS.64_3.5.8_REQ_007	The WPS nonce generated by the device SHALL be random.

3.5.9 Band Steering

TS.64_3.5.9_REQ_001	The AP of a FWA Device SHALL support IEEE 802.11k [86] industry standard for radio resource measurement.
TS.64_3.5.9_REQ_002	The AP of a FWA Device SHALL support IEEE 802.11v [87] industry standard to allow configuration of client devices while connected to wireless networks,
TS.64_3.5.9_REQ_003	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).

TS.64_3.5.9_REQ_004	The Band Steering feature SHALL be manually configurable (ON/OFF selection).
TS.64_3.5.9_REQ_005	The FWA Device SHALL provide a mechanism to manually or automatically configure SSIDs on all supported bands, accordingly with Band Steering settings (i.e. same SSIDs when Band Steering is active).

3.5.10 Mesh Networks

Requirements in this section apply to a FWA Device supporting Mesh capability.

TS.64_3.5.10_REQ_001	The AP of a FWA Device SHALL comply to the Wi-Fi Alliance Easy Mesh™ R2 (or later) standard.
TS.64_3.5.10_REQ_002	The FWA Device SHALL manage the connectivity of Wi-Fi clients and implement AP steering to guarantee that each client is always connected to the best AP and frequency band.
TS.64_3.5.10_REQ_003	The AP of a FWA Device SHALL support IEEE 802.11r [88] industry standard to allow fast transition of clients between BSS (Basic Service Sets),
TS.64_3.5.10_REQ_004	If supported, the 802.11r feature SHALL be configurable (ON/OFF) through customization.

3.5.11 Wi-Fi Diagnostics

TS.64_3.5.11_REQ_001	The FWA Device SHALL collect Wi-Fi metrics related to its AP and the connected clients as shown in Annex B.
TS.64_3.5.11_REQ_002	Wi-Fi Diagnostics data SHALL be available to be collected from the FWA Device by means of TR-069.
TS.64_3.5.11_REQ_003	Additional protocols for allowing the collection of Wi-Fi Diagnostics data from the network MAY be used.
TS.64_3.5.11_REQ_004	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.

3.5.12 Wireless Multimedia Extension

TS.64_3.5.12_REQ_001	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.
TS.64_3.5.12_REQ_002	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).

3.5.13 Customisation

TS.64_3.5.13_REQ_001	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.

TS.64_3.5.13_REQ_002	It SHALL be possible for a MNO to customize a FWA Device in order to hide to the end-user any of the functionality detailed in section 3.5.5, 3.5.7 and 3.5.8.
TS.64_3.5.13_REQ_003	It SHALL be possible for a MNO to customize a FWA Device in order to disable any of the functionality detailed in section 3.5.8, 3.5.9, 3.5.10, 3.5.11.

3.6 IDU/ODU Interworking and Resilience

3.6.1 Common requirements to bridged and routed modes of operation

3.6.1.1 APN/VLAN/Service mapping

TS.64_3.6.1.1_REQ_001	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.
TS.64_3.6.1.1_REQ_002	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.
TS.64_3.6.1.1_REQ_003	IDU and ODU SHALL be able to manage at least 4 VLANs over the IDU-ODU interface. An example of service/VLAN mapping is: • IDU remote management – VLAN ‘a’ • Data/Internet traffic – VLAN ‘b’ • Voice (VoIP) – VLAN ‘c’ • Video – VLAN ‘d’ Other services may be defined based on MNO and market needs.
TS.64_3.6.1.1_REQ_004	The IDU SHALL be able to manage Differentiated Services QoS Treatment, over the interface with the ODU, based on the Requirements TS.64_3.4.3_REQ_010 to TS.64_3.4.3_REQ_013.
TS.64_3.6.1.1_REQ_005	The ODU SHALL be able to manage Differentiated Services QoS Treatment, over both the interface with the IDU and the interface with the mobile network, based on the Requirements TS.64_3.4.3_REQ_010 to TS.64_3.4.3_REQ_013.

3.6.1.2 IDU-ODU Networking

TS.64_3.6.1.2_REQ_001	The ODU SHALL be configurable in order to operate on each VLAN, either in bridged mode or in routed mode.
TS.64_3.6.1.2_REQ_002	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.

TS.64_3.6.1.2_REQ_003	When using DHCP with the IDU, the ODU SHALL define an IP Address Lease Time and configure it to the IDU by means of DHCP Option 51.
TS.64_3.6.1.2_REQ_004	The ODU SHOULD define an IP Address Lease Time in the interval 1 hour (3600 seconds) - 12 hours (43200 seconds).
TS.64_3.6.1.2_REQ_005	When using DHCP with the IDU, the ODU SHALL be able to provide the IDU with the Interface MTU parameter, by means of DHCP Option 26, over each VLAN, using the IPv4 Link MTU received from the Mobile Network on the corresponding PDN/PDU.
TS.64_3.6.1.2_REQ_006	The ODU and the IDU SHALL use, on each VLAN, Address Resolution Protocol (ARP) or Network Discovery Protocol for IPv6 (NDP) in order to properly maintain the association between IP Addresses and MAC Addresses, on each VLAN.
TS.64_3.6.1.2_REQ_007	The ODU SHALL use a unique MAC Address per each VLAN; the same MAC Address is meant to be used, on a VLAN, both for data traffic exchange with the IDU and for ARP/NDP communications with the IDU.
TS.64_3.6.1.2_REQ_008	The IDU SHALL use a unique MAC Address per each VLAN; the same MAC Address is meant to be used, on a VLAN, both for data traffic exchange with the ODU and for ARP/NDP communications with the ODU.
TS.64_3.6.1.2_REQ_009	The ODU SHALL reply, on each VLAN, to ARP Requests generated by IDU, relating to the IP Address of the Default Gateway, with its own MAC Address dedicated to that VLAN.
TS.64_3.6.1.2_REQ_010	The ODU and the IDU SHOULD support 802.1X authentication [111], where the IDU has the role of the Supplicant, and the ODU has the Role of the Authenticator.
TS.64_3.6.1.2_REQ_011	For the purpose of 802.1X, the ODU MAY have also the role of local Authentication Server.

3.6.2 ODU Bridged mode operation.

TS.64_3.6.2_REQ_001	The OutDoor Unit (ODU) SHALL be able to operate in bridged mode, over one or more PDNs-PDUs/VLANs.
TS.64_3.6.2_REQ_002	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: • IP Address • 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.
TS.64_3.6.2_REQ_003	The ODU SHALL define, for each VLAN, the following parameters: • Subnet Mask • Default Gateway 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).
TS.64_3.6.2_REQ_004	The ODU MAY define: • For the Subnet Mask, a /30 (255.255.255.252) • 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).

3.6.3 Reliability of IDU-ODU operation

TS.64_3.6.3_REQ_001	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.
TS.64_3.6.3_REQ_002	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.
TS.64_3.6.3_REQ_003	In addition to the reset of the physical interface with the IDU, the ODU MAY trigger the IDU IP Address renewal by using the DHCP "ForceRenew" message as specified in RFC 3203.
TS.64_3.6.3_REQ_004	In case of Out-Of-Coverage condition of LTE/5G signal, when the ODU is back to coverage, it SHALL perform Tracking Area Update (TAU) until the relevant timer expires in order to recover its previous IP addresses.

3.6.4 ODU Routed mode operation.

TS.64_3.6.4_REQ_001	The OutDoor Unit (ODU) SHALL be able to operate in routed mode, over one or more PDNs-PDUs/VLANs.
TS.64_3.6.4_REQ_002	In routed mode operation, the ODU SHALL retain for itself the IP Address received from the mobile network over a APN/DNN.
TS.64_3.6.4_REQ_003	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.
TS.64_3.6.4_REQ_004	In routed mode operation, if DHCP is used, then ODU SHALL provide via DHCP also: • The DNS Server IP Address(es), which can be either the ODU itself or the Servers received from network; • The Default Gateway (Router), which is the IP Address of the ODU over the IDU-ODU connection.
TS.64_3.6.4_REQ_005	In routed mode operation, the ODU SHALL be able to manage statically configured addresses for: • The IP Address of the IDU over the IDU-ODU connection: this is a directly connected interface • 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.

TS.64_3.6.4_REQ_006	In routed mode operation, the ODU SHALL perform NAT of traffic coming from the IDU and destined to the Network.

3.6.5 Tunnels/VPNs

TS.64_3.6.5_REQ_001	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.

3.7 Device Management

For the proper maintenance of the FWA Devices it is crucial for operators to be able to manage them remotely through an application layer protocol.

For this purpose, TR-069 protocol provides the chance to execute Device management and monitoring operations such as read and write parameters, perform a firmware upgrade etc.

TS.64_3.7_REQ_001	The FWA Device SHALL support broadband forum (BBF) TR-069 Device WAN Management Protocol (Issue:6 corrigendum 1 CWMP Version 1.4 or later) [47].

All objects and parameters describing the many different functions and capabilities of the FWA Devices are hierarchically organised in a XML scheme called “data model”.

The BBF defines two types of CWMP data models:

- *Root*: used to describe the main functions necessary to CWMP (e.g. interfaces, SW/FW Diagnostics, basic Device information)
- *Service*: used to provide specific services (e.g. Voice, Set-Top-Box).
  For each of service please refer to the following BBF technical reports:
  - TR-135: Data Model for a TR-069 Enabled STB (Set-Top-Boxes), Issue 1, Amendment 3 [48]
  - TR-104: Provisioning Parameters for VoIP FWA Device, Issue 2 [49]
  - TR-140: TR-069 Data Model for Storage Service Enabled Devices, Issue 1, Amendment 3 [50]
  - TR-196: Femto Access Point Service Data Model, Issue 2 [51]

3.7.1 Common Requirements for IDU and ODU

In this chapter a set of common requirements for IDU and ODU FWA Devices has been identified and organised in five main sections:

1. RPC methods
2. Data model structure
3. Security
4. Performance monitoring
5. Data model parameters

This is a GSMA minimum set of requirements and then MNOs can add extra metrics according to their needs.

3.7.1.1 RPC methods

The technical report TR-069 FWA Device WAN Management Protocol (Issue:6 corrigendum 1 CWMP Version 1.4) provides a summary of all required RPC methods.

TS.64_3.7.1.1_REQ_001	The FWA Device SHALL support the following FWA Device RPC Methods, as reported in TR-069 (Issue:6 corrigendum 1 CWMP Version 1.4) technical report, section 3.6 [47]: • `GetRPCMethods` • `SetParameterValues` • `GetParameterValues` • `GetParameterNames` • `SetParameterAttributes` • `GetParameterAttributes` • `AddObject` • `DeleteObject` • `Reboot` • `Download`
TS.64_3.7.1.1_REQ_002	The FWA Device SHALL support the following ACS RPC Methods, as reported in TR-069 (Issue:6 corrigendum 1 CWMP Version 1.4) technical report, section 3.6 [47]: • `Inform` • `TransferComplete`
TS.64_3.7.1.1_REQ_003	The FWA Device SHOULD support the following FWA Device RPC Methods: • `Upload` • `FactoryReset`

3.7.1.2 Data model structure

Regarding the CWMP data model structure, two types of root data models have been defined:

- TR-098: Internet Gateway Device Data Model for TR-069 [52]. The data model defined in this specification is DEPRECATED since proved to be inflexible and caused problems in representing complex Device configurations; accordingly, it should be used only by legacy Devices.

- TR-181: Device Data Model for TR-069 [53]. This technical report covers the same functionality of TR-098 plus several extensions as well as IPv6 support and interface stacking mechanism.

TS.64_3.7.1.2_REQ_001	For all FWA Devices and upgrades of existing Devices the “Device:2” data model defined in TR-181 Issue 2 [53] SHALL be used.

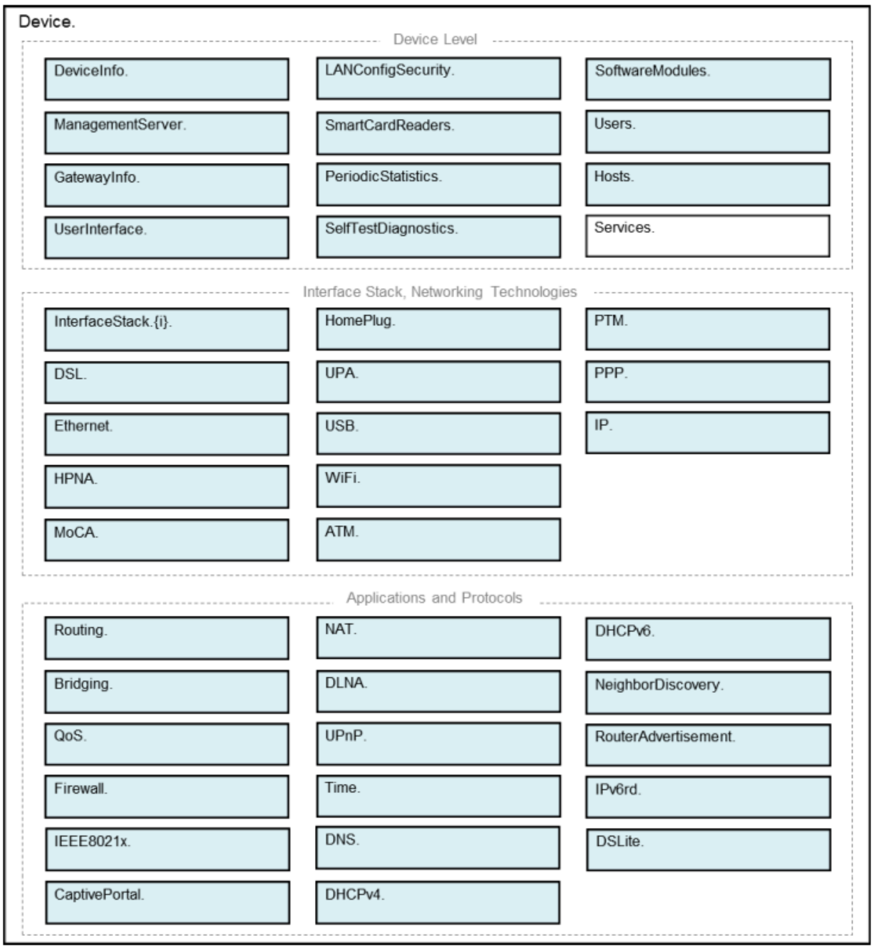

Figure 3: Device:2 Data Model Structure – Overview

3.7.1.3 Security

TS.64_3.7.1.3_REQ_001	The FWA Device SHALL support TLS 1.2 [54] and any earlier versions that are still valid in standards.
TS.64_3.7.1.3_REQ_002	TLS versions later than v1.2 MAY be supported.
TS.64_3.7.1.3_REQ_004	The FWA Device SHALL support the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite.
TS.64_3.7.1.3_REQ_005	Signalling request from the device to the ACS SHALL indicate the latest version of TLS that the device supports.
TS.64_3.7.1.3_REQ_006	The FWA Device SHALL fall back to an earlier version of TLS if that is requested by the ACS.
TS.64_3.7.1.3_REQ_007	The FWA Device SHALL support the mandatory cipher suites for all supported TLS versions.

3.7.1.4 Performance monitoring

TS.64_3.7.1.4_REQ_001	In order to measure the Device performance in terms of downlink and uplink throughput and latency, the FWA Device SHALL be compliant to BBF TR-143 [55] technical report.
TS.64_3.7.1.4_REQ_002	The FWA Device SHALL support both FWA Device initiated and Network Initiated diagnostics TR-143 approaches.
TS.64_3.7.1.4_REQ_003	The FWA Device SHALL support both size-based and time-based TR-143 throughput testing approaches.
TS.64_3.7.1.4_REQ_004	In order to increase the rate that a specific link can be tested, the FWA Device SHOULD support TCP multi-thread for TR-143 downlink and uplink throughput test.
TS.64_3.7.1.4_REQ_005	The FWA Device SHALL support both FTP and HTTP transport for Download and Upload diagnostics.
TS.64_3.7.1.4_REQ_006	The FWA Device SHALL support UDP Echo Plus methodology for latency and packet loss evaluation (One Way Packet Loss, Round Trip Delay, One Way IP Packet Delay Variation).
TS.64_3.7.1.4_REQ_007	The FWA Device SHOULD support TR-390 for Performance Measurement from IP Edge to Customer Equipment using TWAMP Light [56].

3.7.1.5 Data model parameters

This section presents a baseline data model. Please note that parameters will only be used if they are relevant to the operator's service offering.

TS.64_3.7.1.5_REQ_001	The Data model of the FWA Device SHALL contain a set of data object concerning the ACS parameter: • ACS Url • ACS Username • ACS Password • Connection Request URL • Connection Request Username • Connection Request Password • Periodic Inform Interval
TS.64_3.7.1.5_REQ_002	The Data model of the FWA Device SHALL contain a set of data object concerning APNs info, making a clear distinction between the various APN types (Management, Data, Voice): • APN Name • IP Address and Subnet Mask • IP stack (IPv4, IPv6, IPv4v6) • APN Authentication Type • APN Username • APN Password
TS.64_3.7.1.5_REQ_003	The Data model of the FWA Device SHALL contain a set of data object concerning FWA Device info: • Serial Number

	• IMEI • Software/Firmware Version
TS.64_3.7.1.5_REQ_004	The Data model of the FWA Device SHALL contain a set of data object concerning SIM info: • MSISDN • IMSI • ICCID
TS.64_3.7.1.5_REQ_005	The Data model of the FWA Device SHALL contain a set of data object concerning network info: • PLMN ID • Global Cell ID • TAC • PCI
TS.64_3.7.1.5_REQ_006	The Data model of the FWA Device SHALL contain a set of data object concerning radio condition, making a clear distinction between 4G and 5G NSA/SA parameter: • Connected bands • RSRP • RSRQ • SINR
TS.64_3.7.1.5_REQ_007	If the FWA Device supports VoIP, the Data model SHALL contain a set of data object concerning voice service, as specified in TS.64_3.3.2_REQ_043.
TS.64_3.7.1.5_REQ_008	If the FWA Device supports Voice service (VoIP or VoLTE), the Data model SHALL contain the status of SIP registration.
TS.64_3.7.1.5_REQ_009	If the FWA Device supports Wi-Fi access point, the Data model SHALL contain a set of data object concerning Wi-Fi service: • SSID • Channel • Password
TS.64_3.7.1.5_REQ_010	The Data model of the FWA Device SHALL contain a set of data object concerning networking (eg. VLAN ID).
TS.64_3.7.1.5_REQ_011	The Data model of the FWA Device SHALL contain a set of data object concerning Devices connected to the FWA Device, both via Wi-Fi or Ethernet: • Host name • Connected IP Address • MAC Address
TS.64_3.7.1.5_REQ_012	The Data model of the FWA Device SHALL contain a set of data object concerning TR-143 Diagnostic Parameter: • Download URL • Interface • Ethernet Priority • DSCP • BOM Time • EOM Time • Test Bytes Received • Diagnostic Max Connection for multi-thread connections

TS.64_3.7.1.5_REQ_013	The Data model of the FWA Device SHALL contain a set of data object concerning NTP service.

3.7.2 Technical Adaptation of FWA Device

TS.64_3.7.2_REQ_001	If the FWA Device implements autoconfiguration based on SIM insertion, this SHOULD be able to use the available settings as defined in GSMA TS.32 [96].

3.8 Security

TS.64_3.8_REQ_001	To prevent attacks on secured connections and on the CPE itself, the FWA Device SHALL have unique cryptographic keys and secrets per each sample in the factory setting condition.
TS.64_3.8_REQ_002	To be able to react to newly appearing exploits of soft- or hardware vulnerabilities of the FWA Device or any of its components, the FWA Device SHALL have a functionality to update the firmware (operating system and applications) using a firmware package.
TS.64_3.8_REQ_003	The FWA Device SHALL support remote firmware upgrade via the WAN connection.
TS.64_3.8_REQ_004	The FWA Device SHALL be able to verify the authenticity of the firmware package before it is installed on the FWA Device
TS.64_3.8_REQ_005	The FWA Device SHALL NOT install an unsigned firmware package
TS.64_3.8_REQ_006	The FWA Device SHALL support a Factory Reset feature, deleting all personal data and end-user setting from the FWA Device.
TS.64_3.8_REQ_007	The FWA Device SHALL provide at least two different methods to the end-user to request the factory reset, e.g. Web UI and pinhole/reset button on the case of the FWA Device.
TS.64_3.8_REQ_008	The FWA Device SHALL expose, on any interface, a defined and declared set of services, identified by specific TCP and/or UDP ports.
TS.64_3.8_REQ_009	The FWA Device SHALL allow the customization of the active services and corresponding open ports, based on MNOs requirements.
TS.64_3.8_REQ_010	Any other port on any interface of the FWA Device, out of those defined by MNO custom requirements, SHALL be closed at all times.
TS.64_3.8_REQ_011	If the FWA Device has a serial interface to access the Device, it SHALL be closed by default, unless differently required by the MNO.

3.8.1 Passwords

TS.64_3.8.1_REQ_001	Access to the configuration of the FWA Device SHALL be secured by a password, both in Factory Reset condition (preset password used with factory settings) and after user customization.
TS.64_3.8.1_REQ_002	The preset password used with factory settings SHALL NOT contain information derived from data or parts of data related to the FWA Device itself (e.g. manufacturer, model name, MAC address, IMEI, …)
TS.64_3.8.1_REQ_003	If the FWA Device does not implement a forced preset password customization at the first access of the user to the Web UI, the preset password SHALL be unique for each device of the same manufacturer.
TS.64_3.8.1_REQ_004	Preset passwords and customized passwords SHALL fulfil the following requirements: • SHALL contain at least 8 characters (12+ recommended) • SHALL contain at least: • one uppercase letters [A-Z] • one lowercase letters [a-z] • one special characters [e.g. ?, !, $, etc.] • one numeric characters [0-9]
TS.64_3.8.1_REQ_005	Different security requirements for passwords MAY be defined, based on MNO requirements.
TS.64_3.8.1_REQ_006	The FWA Device SHALL allow an authenticated end-user to change the password after entering the previous password.
TS.64_3.8.1_REQ_007	The FWA Device SHALL prevent the user from selecting a weak password without being warned about doing so.
TS.64_3.8.1_REQ_008	Password based authentication SHALL be protected against brute force attacks. A suitable solution is reducing the amount of login attempts in a certain time span (e.g. tarpit) or equivalent techniques.
TS.64_3.8.1_REQ_009	After authentication, the session of the authenticated end-user SHALL be protected against session hijacking attacks. Minimal requirements for such a protection are a session time out and the use of a CSRF token.
TS.64_3.8.1_REQ_010	IF the FWA device have SAMBA or DLNA the end-user SHALL be capable of setting a password to protect access to media devices connected to the device.

3.8.2 Web UI security requirements

TS.64_3.8.2_REQ_001	The FWA Device SHALL NOT have, in factory reset condition, accounts undocumented to the end-user.
TS.64_3.8.2_REQ_002	In factory setting condition, the FWA Device SHALL allow end-user access to the configuration only using the LAN or Wi-Fi interface.
TS.64_3.8.2_REQ_003	To maintain a secure operation, the FWA Device SHALL provide the necessary security relevant information to the authenticated end-user.
TS.64_3.8.2_REQ_004	The FWA Device MAY offer to the end-user remote access to the configuration via WAN interface, e.g. through a Web server.
TS.64_3.8.2_REQ_005	IF the FWA Device offers remote configuration, this communication SHALL be encrypted using strong protocols and cipher suites.
TS.64_3.8.2_REQ_006	IF the FWA Device offers remote configuration, the status of this functionality (active/ inactive) SHALL be made available to the end-user.
TS.64_3.8.2_REQ_007	IF the FWA Device offers remote configuration, the status of this functionality SHALL be disabled in factory setting condition.
TS.64_3.8.2_REQ_008	If the FWA Device provides an option to save and/or restore the configuration to a file, this function SHALL be available only to successfully authenticated users.
TS.64_3.8.2_REQ_009	Credentials and security-sensitive data SHALL be stored securely in the FWA Device.
TS.64_3.8.2_REQ_010	Hard-coded credentials in device software SHALL NOT be used.
TS.64_3.8.2_REQ_011	If the FWA Device provides an option to save and/or restore the configuration to a file, its content SHALL be encrypted.
TS.64_3.8.2_REQ_012	The FWA Device SHALL allow the end-user to display the version number of the firmware currently installed on the Device.

3.9 User Data Protection and Privacy

In the provision of the FWA service, the FWA Device processes user personal data, for which privacy requirements apply.

Such data fall into some categories:

- Data essential for the basic services of the FWA Device: for example, the MAC Addresses of the hosts connected in LAN to the FWA Device are needed in order to properly route data traffic to/from these hosts.
- Data useful to provide additional services of the FWA Device: for example, the call log, that is the list of received, placed and missed voice calls, may be a useful service provided by the FWA Device, although it is based on sensitive data.

- Data useful to provide additional services offered by the MNO using a combination of features local to the FWA Device and remotely located in the network: for example, MAC Addresses and hostnames may be used by Wi-Fi diagnostics applications, to provide the end-user hints and advice to optimize the Wi-Fi performance in the home network.

TS.64_3.9_REQ_001	The nature and amount of user personal data being stored, processed and transmitted by the FWA Device SHALL be clearly identified and declared.
TS.64_3.9_REQ_002	Personal data SHALL be processed by the FWA Device in compliance with the Data Protection and Privacy regulations in effect in the country where the FWA Device is deployed.
TS.64_3.9_REQ_003	Personal data SHALL be stored in the FWA Device ONLY IF permitted by the Data Protection and Privacy regulations in effect in the country where the FWA Device is deployed and following the mandatory prescriptions. Note: for example, a regulator might require to anonymize data to be presented, e.g. anonymizing the last digits of a phone number or a significant portion of a hostname/MAC Address.
TS.64_3.9_REQ_004	If permitted, the storage of personal data onboard the FWA Device SHALL be done in an encrypted manner.
TS.64_3.9_REQ_005	Personal data in the FWA Device SHALL be presented to the end user only upon authenticated access and by means of secure protocols.
TS.64_3.9_REQ_006	Personal data SHALL be transmitted by the FWA Device to the MNO ONLY IF permitted by the Data Protection and Privacy regulations in effect in the country where the FWA Device is deployed and following the mandatory prescriptions. Note: for example, a regulator might require to anonymize data to be transmitted, e.g. anonymizing the last digits of a phone number or a significant portion of a hostname/MAC Address.
TS.64_3.9_REQ_007	Personal data in the FWA Device SHALL NOT be shared with other parties other than the MNO providing the service and/or its business partners specifically identified by the MNO.
TS.64_3.9_REQ_008	If permitted, the transmission of personal data between the FWA Device and the MNO network SHALL happen only through authenticated sessions and encrypted protocols.

3.10 Hardware, Safety, EMC requirements and environment operating conditions

3.10.1 General

TS.64_3.10.1_REQ_001	The FWA Device SHALL comply to the safety, health and environmental protection regulations of the market where it is meant to be used.
TS.64_3.10.1_REQ_002	The FWA Device SHALL comply to the ElectroMagnetic Compatibility (EMC) regulations of the market where it is meant to be used.
TS.64_3.10.1_REQ_003	The FWA Device SHALL comply to the eco-design and energy efficiency regulations of the market where it is meant to be used.
TS.64_3.10.1_REQ_004	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.
TS.64_3.10.1_REQ_005	For the Indoor FWA Device and the InDoor Unit of the OutDoor FWA Solution, the maximum allowed temperature on the different parts of the enclosure, except the one on the bottom side, in any environmental condition during stationary use, shall be not higher than 55°C.
TS.64_3.10.1_REQ_006	The FWA Device SHALL comply to the noise emissions regulations of the market where it is meant to be used.
TS.64_3.10.1_REQ_007	Regarding the insulation against water and dust, the OutDoor Unit of the OutDoor FWA Solution SHALL be compliant at least to the class IP65 of the international standard IEC 60529 [89].
TS.64_3.10.1_REQ_008	Regarding the electrical resistibility, the Indoor FWA Device and the InDoor Unit of the OutDoor FWA Solution SHALL comply with basic requirements defined by Rec. ITU-T K.21 [90] (Resistibility of telecommunication equipment installed in customer premises to overvoltages and overcurrents) and K.44 [91] (Resistibility tests for telecommunication equipment exposed to overvoltages and overcurrents – Basic Recommendation).
TS.64_3.10.1_REQ_009	Regarding the electrical resistibility, the OutDoor Unit of the OutDoor FWA Solution, including the external power supply, SHALL comply with basic requirements defined by Rec. ITU-T K.21 [90] (Resistibility of telecommunication equipment installed in customer premises to overvoltages and overcurrents), K.44 [91] (Resistibility tests for telecommunication equipment exposed to overvoltages and overcurrents – Basic Recommendation) and K.45 [92] (Resistibility of telecommunication equipment installed in the access and trunk networks to overvoltages and overcurrents).
TS.64_3.10.1_REQ_010	The FWA Device SHALL have a MTBF (Mean Time Between Failure) not shorter than 7 years at 30 °C.

TS.64_3.10.1_REQ_011	In countries where there're no safety requirements, the FWA Device SHOULD comply with the requirements mandatory for the CE marking.

Note 1: examples or mandatory regulatory requirements for some markets:

- CE Marking for the operation in the Economic European Area (EEA).
- FCC regulatory requirements for the operation in the US market.

Note 2: some operators may require additional certifications.

Note 3: See Annex A for detailed list of European norms to be fulfilled in EU for EMC, Safety & Radio aspects.

3.11 Stability

TS.64_3.11_REQ_001	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.
TS.64_3.11_REQ_002	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.
TS.64_3.11_REQ_003	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.
TS.64_3.11_REQ_004	In normal operating conditions, the FWA Device SHALL offer a service availability for voice service of at least 99.5%. Note: this objective considers only the availability of the Device itself, not the availability of the network.
TS.64_3.11_REQ_005	The FWA Device SHALL maintain uninterrupted voice (SIP protocol) registration for at least 72 consecutive hours, during which the Device is idle for Voice.
TS.64_3.11_REQ_006	At the end of the idle period of req. TS.64_3.11.0_REQ_005, 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.
TS.64_3.11_REQ_007	If voice service is supported, the FWA Device SHALL be able to support long-lasting voice calls (1.5 hours at least).
TS.64_3.11_REQ_008	As regards the performance targets reported at sect. 3.4 and 3.5, with reference to 3GPP TS 36.101 [93] (for 4G), TS 38.101-1 [94] (5G FR1) and TS 38.101-2 [95] (5G FR2), the Indoor FWA Device and the InDoor Unit of the OutDoor FWA Solution SHALL offer: • 100% of the targets, in the "normal conditions" temperature range.

TS.64_3.11_REQ_009	As regards the performance targets reported at sect. 3.4 and 3.5, with reference to 3GPP TS 36.101 [93] (for 4G), TS 38.101-1 [94] (5G FR1) and TS 38.101-2 [95] (5G FR2), the Indoor FWA Device and the InDoor Unit of the OutDoor FWA Solution SHALL offer: • At least 85% of the targets, in “extreme conditions” temperature range (outside the “normal condition” range).
TS.64_3.11_REQ_010	As regards the performance targets reported at sect. 3.4, with reference 3GPP TS 36.101 [93] (for 4G), TS 38.101-1 [94] (5G FR1) and TS 38.101-2 [95] (5G FR2), the OutDoor Unit of the OutDoor FWA Solution SHALL offer: • 100% of the targets, in the “extreme conditions” temperature range.

3.12 User Interface

TS.64_3.12_REQ_001	The FWA Device SHALL offer a Web UI to the end user for customizing the configuration of the FWA Device.
TS.64_3.12_REQ_002	The FWA Device SHALL comply to the requirements defined in sect. 3.8.2 as regards Web UI Security.
TS.64_3.12_REQ_003	The Web UI SHOULD permit the configuration of all the service features relevant for the end user.
TS.64_3.12_REQ_004	The Web UI SHALL be customizable based on MNO requirements.

4 Specific Requirements for 4G FWA Devices

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

TS.64_4.1_REQ_001	The FWA device SHALL be compliant with 3GPP E-UTRAN Access Stratum Release 12 baseline or later.
TS.64_4.1_REQ_002	The FWA device SHALL support EEA0 Null Encryption Algorithm.
TS.64_4.1_REQ_003	The FWA device SHALL support 128-EEA1 EPS Encryption Algorithm (based on SNOW 3G algorithm) for both RRC signalling ciphering and User Plane ciphering.
TS.64_4.1_REQ_004	The FWA device SHALL support 128-EEA2 EPS Encryption Algorithm (based on AES algorithm) for both RRC signalling ciphering and User Plane ciphering.
TS.64_4.1_REQ_005	The FWA device SHOULD support 128-EEA3 EPS Encryption Algorithm (based on ZUC algorithm) for both RRC signalling ciphering and User Plane ciphering.
TS.64_4.1_REQ_006	The FWA device SHALL support EIA0 Null Integrity Algorithm.

TS.64_4.1_REQ_007	The FWA device SHALL support 128-EIA1 EPS Integrity Algorithm (based on SNOW 3G algorithm) for both RRC and NAS signalling integrity protection.
TS.64_4.1_REQ_008	The FWA device SHALL support 128-EIA2 EPS Integrity Algorithm (based on AES algorithm) for both RRC and NAS signalling integrity protection.
TS.64_4.1_REQ_009	The FWA device SHOULD support 128-EIA3 EPS Integrity Algorithm (based on ZUC algorithm) for both RRC and NAS signalling integrity protection.
TS.64_4.1_REQ_010	The FWA device SHALL support EPS-AKA Authentication Protocol.
TS.64_4.1_REQ_011	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.
TS.64_4.1_REQ_012	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. Note: if the FWA device supports this requirement, then TS.64_4.1_REQ_001 requirement does not apply.
TS.64_4.1_REQ_013	The FWA device SHALL support at least 3DL LTE Carrier Aggregation capability.
TS.64_4.1_REQ_014	The FWA device SHOULD support 2UL LTE Carrier Aggregation capability.
TS.64_4.1_REQ_015	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).
TS.64_4.1_REQ_016	The FWA device SHALL support 256QAM modulation for downlink.
TS.64_4.1_REQ_017	The FWA device SHALL support 64QAM modulation for uplink.
TS.64_4.1_REQ_018	The FWA device SHOULD support 256QAM modulation for uplink.
TS.64_4.1_REQ_019	The FWA device SHALL support standardized QCIs as specified in 3GPP TS 23.203 [5].
TS.64_4.1_REQ_020	The FWA device SHOULD support operator specific QCIs as specified in 3GPP TS 23.203 [5].
TS.64_4.1_REQ_021	The FWA device SHALL support periodical intra-frequency ANR measurements for reporting to the network the Strongest Cells and related CGI (Cell Global Identity).
TS.64_4.1_REQ_022	The FWA device SHALL support periodical inter-frequency ANR measurements for reporting to the network the Strongest Cells and related CGI (Cell Global Identity).

4.2 Antenna Performance Acceptance Values for 4G FWA devices

As described in GSMA TS.24 [57], the GSMA Terminal Steering Group have reviewed results of antenna performance tests, aligning test methods and performance values to be used as guidelines for acceptable performance of antennas in Mobile devices to facilitate alignment and agreement among the various operators representing America, Europe, and Asia.

GSMA TS.24 (Operator Acceptance Values for Device Antenna Performance) version 6 onwards has specific focus on FWA Devices, as they have different form factor which may improve Antenna performance.

TS.64_4.2_REQ_001	The FWA device SHALL be compliant to TS.24 for Antenna Performance acceptance values [57].

5 Specific Requirements for 5G NSA FWA Devices

TS.64_5_REQ_001	The FWA device SHALL support standardized QCIs as specified in 3GPP TS 23.203 [5].
TS.64_5_REQ_002	The FWA device SHOULD support operator-specific QCIs as specified in 3GPP TS 23.203 [5].
TS.64_5_REQ_003	The FWA device SHALL be compliant with 3GPP E-UTRAN and NR Access Stratum Release 16 baseline or later.
TS.64_5_REQ_004	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. (reportCGI-NR-EN-DC-r15) (nr-CGI-Reporting-ENDC)
TS.64_5_REQ_005	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. (reportCGI-NR-NoEN-DC-r15)
TS.64_5_REQ_006	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). (eutra-CGI-Reporting)
TS.64_5_REQ_007	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). (nr-CGI-Reporting)

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

TS.64_5.1_REQ_001	The FWA device SHALL support EN-DC (Option 3x).
TS.64_5.1_REQ_002	The FWA device SHALL support DSS technology.
TS.64_5.1_REQ_003	The FWA device SHALL support rateMatchingResrcSetSemi-Static Information element in the Capability Information message. Note: It indicates the UE supports receiving PDSCH with resource mapping that excludes the REs corresponding to resource sets configured with RB-symbol level granularity following the semi-static configuration as specified in TS 38.214.
TS.64_5.1_REQ_004	The FWA device SHALL support rateMatchingResrcSetDynamic Information element in the Capability Information message. Note: It indicates the UE supports receiving PDSCH with resource mapping that excludes the REs corresponding to resource sets

	configured with RB-symbol level granularity based on dynamic indication in the scheduling DCI as specified in TS 38.214.
TS.64_5.1_REQ_005	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. Note: It indicates the UE supports receiving PDSCH with resource mapping that excludes the REs determined by the higher layer configuration LTE-carrier configuring common RS, as specified in TS 38.214.
TS.64_5.1_REQ_006	The FWA device SHOULD support AdditionalDMRS-DL-Alt Information element in the Capability Information message. Note: It indicates the support of the alternative additional DMRS position for coexistence with LTE CRS.
TS.64_5.1_REQ_007	The FWA device SHALL support NR SRS antenna switching 1T4R in 5G NR TDD high-bands (e.g. n77/n78).
TS.64_5.1_REQ_008	The FWA device SHALL support NR SRS antenna switching 1T2R in 5G NR TDD mid- and low-bands.
TS.64_5.1_REQ_009	The FWA device SHOULD support 2DL NR Inter-Band Carrier Aggregation.
TS.64_5.1_REQ_010	The FWA device SHALL support UL split bearer to transmit concurrently on LTE and NR.
TS.64_5.1_REQ_011	The FWA device SHALL support MIMO 4x4 DL capability on NR mid-bands (e.g. NR bands n77/n78).
TS.64_5.1_REQ_012	The FWA device SHALL support 4Rx diversity on NR bands.
TS.64_5.1_REQ_013	The FWA device SHOULD support 8Rx diversity on NR bands.
TS.64_5.1_REQ_014	The FWA device MAY support more than 8Rx diversity on NR bands.
TS.64_5.1_REQ_015	The FWA device SHALL support 256QAM modulation for downlink.
TS.64_5.1_REQ_016	The FWA device SHALL support 64QAM modulation for uplink.
TS.64_5.1_REQ_017	The FWA device SHOULD support 256QAM modulation for uplink.
TS.64_5.1_REQ_018	The FWA device SHALL support power class 3 (23 dBm).
TS.64_5.1_REQ_019	The FWA device SHOULD support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1 [58].
TS.64_5.1_REQ_020	The FWA device SHOULD support power class 1.5 (29 dBm) in compliance with 3GPP TS 38.101-1 [58].
TS.64_5.1_REQ_021	The FWA device SHALL support 15 kHz Sub-Carrier Spacing in FR1 NR bands.
TS.64_5.1_REQ_022	The FWA device SHALL support 30 kHz Sub-Carrier Spacing in FR1 NR bands.

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

If the Device supports 5G FR2, the following requirements apply.

TS.64_5.2_REQ_001	The FWA device SHALL support EN-DC (Option 3x).
TS.64_5.2_REQ_002	The FWA device SHALL support 2DL contiguous NR Carrier Aggregation.
TS.64_5.2_REQ_003	The FWA device SHOULD support 2UL contiguous NR Carrier Aggregation.
TS.64_5.2_REQ_004	The FWA device SHALL support UL split bearer to transmit concurrently on LTE and NR.
TS.64_5.2_REQ_005	The FWA device SHALL support MIMO 2x2 DL capability on NR FR2 bands (e.g., NR bands n257/n258).
TS.64_5.2_REQ_006	The FWA device SHOULD support MIMO 4x4 DL capability on NR FR2 bands (e.g., NR bands n257/n258).
TS.64_5.2_REQ_007	The FWA device SHALL support 64QAM modulation for downlink.
TS.64_5.2_REQ_008	The FWA device SHOULD support 256QAM modulation for downlink.
TS.64_5.2_REQ_009	The FWA device SHALL support 64QAM modulation for uplink.
TS.64_5.2_REQ_010	The FWA device SHOULD support 256QAM modulation for uplink.
TS.64_5.2_REQ_011	The FWA device SHALL support power class 3 (23 dBm).
TS.64_5.2_REQ_012	The FWA device SHOULD support power class 2 (26 dBm).
TS.64_5.2_REQ_013	The FWA device SHOULD support power class 1 (31 dBm).
TS.64_5.2_REQ_014	The FWA device SHALL support 100 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
TS.64_5.2_REQ_015	The FWA device SHOULD support 200 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
TS.64_5.2_REQ_016	The FWA device SHOULD support 400 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
TS.64_5.2_REQ_017	The FWA device SHALL support 60 KHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).
TS.64_5.2_REQ_018	The FWA device SHALL support 120 KHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).

5.3 Antenna Performance Acceptance Values for 5G NSA FWA devices

TS.64_5.3_REQ_001	The FWA device SHALL be compliant to TS.24 [57] for Antenna Performance acceptance values.

6 Specific Requirements for 5G SA FWA Devices

TS.64_6_REQ_001	The FWA device SHALL support Option 2 SA deployment option.
TS.64_6_REQ_002	The FWA device SHOULD support Option 4 NSA deployment option.
TS.64_6_REQ_003	The FWA device SHALL be compliant with 3GPP NR Access Stratum Release 16 baseline or later.
TS.64_6_REQ_004	The FWA device SHALL support standardized 5QIs as specified in 3GPP TS 23.501 [5].
TS.64_6_REQ_005	The FWA device SHALL support NEA0 Null Encryption Algorithm.
TS.64_6_REQ_006	The FWA device SHALL support 128-NEA1 New radio Encryption Algorithm (based on SNOW 3G algorithm).
TS.64_6_REQ_007	The FWA device SHALL support 128-NEA2 New radio Encryption Algorithm (based on AES algorithm).
TS.64_6_REQ_008	The FWA device SHOULD support 128-NEA3 New radio Encryption Algorithm (based on ZUC algorithm).
TS.64_6_REQ_009	The FWA device SHALL support 128-NIA1 New radio Integrity Algorithm (based on SNOW 3G algorithm).
TS.64_6_REQ_010	The FWA device SHALL support 128-NIA2 New radio Integrity Algorithm (based on AES algorithm).
TS.64_6_REQ_011	The FWA device SHOULD support 128-NIA3 New radio Integrity Algorithm (based on ZUC algorithm).
TS.64_6_REQ_012	The FWA device SHALL support 5G-AKA Authentication Protocol Algorithm.
TS.64_6_REQ_013	The FWA device SHALL support EAP-AKA Authentication Protocol Algorithm.
TS.64_6_REQ_014	The FWA device SHALL support Initial 5GC Registration with SUCI, as per 3GPP TS 24.501 [82].
TS.64_6_REQ_015	The FWA device SHALL support 5G Slicing User Equipment Route Selection Policy (URSP) parameters.
TS.64_6_REQ_016	The FWA device SHALL support 5G Slicing Network Slice Selection Assistance Information (NSSAI) parameters, as per 3GPP TS 24.501 [82].
TS.64_6_REQ_017	The FWA device SHALL support SST (Slice/Service Type) and SD (Slice Differentiator) parameters.
TS.64_6_REQ_018	The FWA device SHALL support standardised SST values, as specified in 3GPP TS 23.501 [81].

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

TS.64_6.1_REQ_001	The FWA device SHALL support 2DL NR Carrier Aggregation.
TS.64_6.1_REQ_002	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.
TS.64_6.1_REQ_003	The FWA device SHOULD support 3DL NR Carrier Aggregation.
TS.64_6.1_REQ_004	The FWA device MAY support 4DL NR Carrier Aggregation or higher order.
TS.64_6.1_REQ_005	The FWA device SHOULD support 2UL NR Carrier Aggregation.
TS.64_6.1_REQ_006	The FWA device SHALL support 15 kHz Sub-Carrier Spacing in FR1 NR bands.
TS.64_6.1_REQ_007	The FWA device SHALL support 30 kHz Sub-Carrier Spacing in FR1 NR bands.
TS.64_6.1_REQ_008	The FWA device SHALL support MIMO 4x4 DL capability on NR high-bands (e.g. NR bands n77/n78).
TS.64_6.1_REQ_009	The FWA device SHALL support MIMO 2x2 UL capability on NR high-bands (e.g. NR bands n77/n78).
TS.64_6.1_REQ_010	The FWA device SHALL support 4Rx diversity on NR bands.
TS.64_6.1_REQ_011	The FWA device SHOULD support 8Rx diversity on NR bands.
TS.64_6.1_REQ_012	The FWA device MAY support more than 8Rx diversity on NR bands.
TS.64_6.1_REQ_013	The FWA device SHALL support 256QAM modulation for downlink.
TS.64_6.1_REQ_014	The FWA device MAY support 1024QAM modulation for downlink on NR TDD FR1 high-bands (e.g. n77/n78).
TS.64_6.1_REQ_015	The FWA device SHALL support 64QAM modulation for uplink.
TS.64_6.1_REQ_016	The FWA device SHOULD support 256QAM modulation for uplink.
TS.64_6.1_REQ_017	The FWA device SHALL support power class 3 (23 dBm).
TS.64_6.1_REQ_018	The FWA device SHOULD support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1 [58].
TS.64_6.1_REQ_019	The FWA device SHOULD support power class 1.5 (29 dBm) in compliance with 3GPP TS 38.101-1 [58].

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

TS.64_6.2_REQ_001	The FWA device SHALL support 2DL intra-band contiguous NR Carrier Aggregation.
TS.64_6.2_REQ_002	The FWA device SHOULD support 4DL intra-band contiguous NR Carrier Aggregation.
TS.64_6.2_REQ_003	The FWA device SHOULD support 8DL intra-band contiguous NR Carrier Aggregation.
TS.64_6.2_REQ_004	The FWA device SHOULD support 2UL intra-band contiguous NR Carrier Aggregation.
TS.64_6.2_REQ_005	The FWA device MAY support 4UL intra-band contiguous NR Carrier Aggregation.
TS.64_6.2_REQ_006	The FWA device SHALL support 100 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
TS.64_6.2_REQ_007	The FWA device SHOULD support 200 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
TS.64_6.2_REQ_008	The FWA device SHOULD support 400 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
TS.64_6.2_REQ_009	The FWA device SHALL support 60 kHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).
TS.64_6.2_REQ_010	The FWA device SHALL support 120 kHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).
TS.64_6.2_REQ_011	The FWA device SHALL support MIMO 2x2 DL capability on NR FR2 bands (e.g., NR bands n257/n258).
TS.64_6.2_REQ_012	The FWA device SHOULD support MIMO 4x4 DL capability on NR FR2 bands (e.g., NR bands n257/n258).
TS.64_6.2_REQ_013	The FWA device SHALL support 64QAM modulation for downlink.
TS.64_6.2_REQ_014	The FWA device SHOULD support 256QAM modulation for downlink.
TS.64_6.2_REQ_015	The FWA device SHALL support 64QAM modulation for uplink.
TS.64_6.2_REQ_016	The FWA device SHOULD support 256QAM modulation for uplink.
TS.64_6.2_REQ_017	The FWA device SHALL support power class 3 (23 dBm).
TS.64_6.2_REQ_018	The FWA device SHOULD support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1 [58].
TS.64_6.2_REQ_019	The FWA device SHOULD support power class 1 (31 dBm) in compliance with 3GPP TS 38.101-1 [58].

6.3 Antenna Performance Acceptance Values for 5G SA FWA devices

TS.64_6.3_REQ_001	The FWA device SHALL be compliant to TS.24 [57] for Antenna Performance acceptance values.

Annex A Hardware, Safety and EMC normative references for European Market

A.1 Safety

- EN 50385:2017 (Product standard to demonstrate the compliance of base station equipment with electromagnetic field exposure limits (110 MHz - 100 GHz), when placed on the market).

- EN 62311:2020. Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz).

- IEC EN 62368-1:2023 (Audio/video, information and communication technology equipment - Part 1: Safety requirements).

A.2 EMC

- IEC EN 55032:2015 + A1:2020 - class B limits (Electromagnetic compatibility of multimedia equipment - Emission requirements).

- IEC EN 55035:2017 + A11: 2020 (Electromagnetic compatibility of multimedia equipment. Immunity requirements).

- ETSI EN 301 489-1 V2.2.3 (EMNC Standard for Radio Equipment and services – Part1: Common Requirements).

- ETSI EN 301 489-17 V3.2.4 (Part 17: Specific conditions for Broadband Data Transmission Systems).

- ETSI EN 301 489-19 V2.2.1 Specific conditions for Receive Only Mobile Earth Stations (ROMES) operating in the 1,5 GHz band providing data communications and GNSS receivers operating in the RNSS band (ROGNSS) providing positioning, navigation, and timing data.

- ETSI EN 301 489-52 V1.2.2 (Part 52: Specific conditions for Cellular Communications User Equipment's).

- IEC EN 61000-3-2:2014 (limitation of harmonic currents injected into the public supply system).

A.3 Radio Spectrum

- ETSI EN 300 328 V2.2.2 (Data transmission equipment operating in the 2,4 GHz band; Harmonised Standard for access to radio spectrum).

- ETSI EN 301 893 V2.1.1 (5 GHz RLAN; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU).

- ETSI EN 301 908-1 V15.1.1 (IMT cellular networks; Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Part 1: Introduction and common requirements).

- ETSI EN 301 908-2 V13.1.1 MT cellular networks; Harmonised Standard for access to radio spectrum; Part 2: CDMA Direct Spread (UTRA FDD) User Equipment (UE).

- ETSI EN 301 908-13 V13.2.1 (IMT cellular networks; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU; Part 13: Evolved Universal Terrestrial Radio Access (E-UTRA) User Equipment (UE)).

- Draft ETSI 301 908-25 V15.1.1 IMT cellular networks - Harmonised Standard for access to radio spectrum - Part 1: Introduction and common requirements Release 15.

- EN 303 413 V1.2.1 Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) receivers; Radio equipment operating in the 1164 MHz to 1300 MHz and 1559 MHz to 1610 MHz frequency bands; Harmonised Standard for access to radio spectrum.

- ETSI TS 138 521-1 V17.5.0 5G; NR; User Equipment (UE) conformance specification; Radio transmission and reception; Part 1: Range 1 standalone (3GPP TS 38.521-1 version 17.5.0 Release 17).

- ETSI TS 138 521-3 V17.5.0 5G; NR; User Equipment (UE) conformance specification; Radio transmission and reception; Part 3: Range 1 and Range 2 Interworking operation with other radios (3GPP TS 38.521-3 version 17.5.0 Release 17).

- ETSI TS 38 521-3 V16.4.0 5G New Radio User Equipment Conformance Specification – Radio Transmission and Reception Part 3: Range 1 and Range 2 Interworking Operation with other Radios.

A.4 Environment Protection and Energy Efficiency

- EN 63000:2018 Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances

- EN 50564:2011: Electrical and electronic household and office equipment - Measurement of low power consumption

- Directive 2014/53/EU Radio equipment, and the related conformity assessment procedure.

- Energy related Products (ErP) Directive 2009/125/EC and related Commission Regulation (EC) no. 2023/826.

- Directives RoHS 2011/65/UE and WEEE 2012/19/UE, and the related conformity assessment procedures.

- For the operation in the European Union (EU), considering the obligations of the applicable Directives, the manufacturer of the FWA Device shall provide the full text of the Declaration of Conformity (DoC) and the Technical File, which shall include the Technical Documentation (TD) compliant with the conformity assessment procedure used under the applicable product Directives.

A.5 Environment Operating Conditions

- ETSI ETS 300 019-1-1 [] as regards storage for equipment in class 1.1 (Weather protected, partly temperature-controlled storage locations)
- ETSI ETS 300 019-1-2 [] as regards transportation for equipment in class 2.3 (Public transportation).
- For the Indoor FWA Device and the InDoor Unit of the OutDoor FWA Solution, ETSI EN 300 019-1-3 [] as regards stationary use in Environmental Class T 3.1 “Temperature-controlled locations”.
- For the OutDoor Unit of the OutDoor FWA Solution, ETSI EN 300 019-1-4 [] as regards stationary use in Environmental Class T 4.1 “Non-weather protected locations”.
- For the OutDoor Unit of the OutDoor FWA Solution, IEC EN 60068-2-52 as regards the corrosion produced by salt-laden atmosphere - severity (1).
- ETS 300 019-2-3 as regards the mechanical stress, (severity Class T3.2).

a. IEC EN 60068-2-27 Test Ea – Shock: according to, with test severity defined for the Class T3.2 by the standard ETS 300 019-2-3

b. IEC EN 60068-2-64 Test Fh – Random: according to, with test severity defined for the Class T3.2 by the standard

c. IEC EN 60068-2-6 Test Fc – Sinusoidal Vibration: according to, with test severity defined for the Class T3.2 by the standard ETS 300 019-2-3

d. IEC EN 60068-2-32 Test Ed – Free fall from a height of 1m.

Annex B Example of Wi-Fi metrics for Wi-Fi diagnostic

Wi-Fi metrics related to the AP of the FWA Device, and the connected clients are defined in Wi-Fi Data Elements™ specified by Wi-Fi Alliance and the corresponding TR-181 data model specified by BroadBand Forum.

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	Oct 2023	New PRD	TSG#53 ISAG#34	Paolo Ferrabone Telecom Italia

C.2 Other Information

Type	Description
Document Owner	GSMA Terminal Steering Group (TSG)
Editor / Company	Paolo Ferrabone / Telecom Italia

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.