सत्यमेव जयते

अनंतिम टेस्ट गाइड

टीईसी सं: ३८०२१:२०२२

PROVISIONAL TEST GUIDE

TEC No. : 38021:2022

for

वाईफ़ाईऐक्सेसपॉइंट (एपी)

Wi-Fi Access Point (AP)

(Standard No.: TEC 38020:2021)

ISO 9001:2015

दूरसंचारअभियांत्रिकीकेंद्र
खुर्शीदलालभवन, जनपथ, नईदिल्ली-110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release : May, 2022

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

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

ABSTRACT

This test guide enumerates detailed test schedule and procedure for evaluating conformance / functionality / requirements / performance of Wi-Fi Access Point as per standard for Generic Requirements No. TEC 38020:2021

CONTENTS

Section	*Item*	*Page No.*
A.	Introduction	5
B.	History Sheet	5
C.	General information	6
D.	Testing team	7
E.	List of the test instruments	7
F.	Equipment Configuration offered	8
G.	Equipment/System Manuals	8
H.	Clause-wise Test Type and Test No.	9
I.	Test Setup & Procedures	40
J.	Summary of test results	113

A. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance / functionality / requirements / performance of Wi-Fi Access Point as per standard for Generic Requirements No. TEC 38020:2021.

B. HISTORY SHEET

Sl. No.	TSTP No.	Equipment/Interface	Issue
1.	TEC/TSTP/GR/CP/Wi-Fi-002/01/SEP-11	Wi-Fi Access Point (AP)	Release 1: September, 2011
2.	TEC/TS/RS/WFS-232/02/JUN-17	Wi-Fi Access Point (AP)	Release 2: June, 2017
3.	TEC 38021:2021	Wi-Fi Access Point (AP)	Release 3: November, 2021
4.	TEC 38021:2022	Wi-Fi Access Point (AP)	Release 4: May, 2022

C. General information:

Sn.	General Information	Details *(to be filled by testing team)*	
1	Name and Address of the Applicant		
2	Date of Registration		
3	Name and No. of GR/IR/Applicant’s Spec. against which the approval sought		
4	Details of Equipment		
	Type of Equipment	Model No.	Serial No.
(i)			
(ii)			
5	Any other relevant Information:-		

D.Testing team: *(to be filled by testing team)*

S.No.	Name	Designation	Organization	Signature
1.				
2.				

E. List of the Test Instruments:

S.no.	Name of the test instrument	Make /Model *(to be filled by testing team)*	Validity of calibration *(to be filled by testing team)*
1			dd/mm/yyyy
2			
3			
4			
5			
6			
7			
8			

F. Equipment Configuration Offered: *(to be filled by testing team)*

(a) <Equipment/product name> Configuration:

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

(b) <Other equipment name> Configuration:

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

G. Equipment/System Manuals: *(to be filled by testing team)*

Availability of Maintenance manuals, Installation manual, Repair manual & User Manual etc. (Y/N)

H.Clause-wise Test Type and Test No.:

Clause No.	*Clause*	*Type of Test / Test No. etc. **
1.1	This document specifies the Generic Requirements (GR) of Wi-Fi Access Point (AP) used for accessing Wireless Local Area Network (WLAN) services provided by Wi-Fi networks. The schematic of Wi-Fi Network (WLAN) is given in Annexure-I. Definitions: i) Access Point (AP):- Any entity that has station (STA) functionality and provides access to the distribution, via the wireless medium (WM) for associated STAs. ii) Station (STA) :- Any device that contains an IEEE 802.11- conformant and media access control (MAC) physical layer (PHY) interface to the wireless medium (WM).	No test required.
2.1	This GR covers requirements for interoperability, Quality, Electromagnetic Compatibility, Safety and Security.	Certificate from Accredited lab to be submitted.
2.2	This GR may be used for certification of following Types of Wi-Fi Access points: Type A: Wi-Fi Access Point without Router functionality Type B: Wi-Fi Access Point with Router functionality Note: i) Bridge functionality is available in all APs.	Declaration from the manufacturer about the type of Wi-Fi Access Point (A or B).

	ii) For Type B AP supporting routing functionality, the supplier must indicate the essential protocols (like for static routing or dynamic routing etc.) that enable routing.	
2.3	This document covers Wi-Fi APs based on suitability for Indoor, Outdoor, Mixed (Indoor & outdoor) applications, LAN capabilities (Optional).	Declaration from the manufacturer to be submitted regarding outdoor, indoor or mixed usage.
2.4	For all TEC GRs / IRs and International Standards referred to in this document, latest issue shall be applicable unless specified otherwise.	No test required.
2.5	Prevailing National Regulations shall apply in case of VoIP and Internet telephony.	Declaration from the manufacturer to be submitted.
2.6	The equipment shall support dual stack (IPv4 & IPv6) traffic.The equipment shall conform to IETF RFC 2460 and IETF RFC 791.	Test No. :- GR_WiFiAP_025
2.7	Information to be mentioned on the TEC Certificate is given in Clause 13.0	No test required.
3.0	**Functional/Operational Requirements**	
3.1	**Operating Frequency Range** The operation of equipment shall be in the license free bands of 2.4 and/or 5 GHz bands and as per latest National Frequency Allocation Plan (NFAP) and published WPC GSRs as specified below and further subject to, revision from time to time.	i. Test No.: - GR_WiFiAP_001 i. Data sheet of the equipment (specific to Radio Card) to be submitted.

S.No.	Frequency Range	Title of the Rule	GSR No. IND	IND Remarks as per NFAP 2018
1.	2400-2483.5 MHz	Use of Low Power Equipment in the frequency band 2.4 GHz to 2.4835 GHz (Exemption from Licensing Requirement) Rules, 2005	GSR No. 45 (E) dated 28-Jan-2005, and subsequent amendments, if any.	
2.	5150 - 5250 MHz 5250 - 5350 MHz 5470-	Use of Wireless Access Systems (WAS) including Radio	GSR No. 1048(E) dated 18-Oct.2018 and	IND 29

	5725 MHz 5725 - 5875 MHz	Local Area Network (RLAN) in 5GHz (Exemption from Licensing Requirement) Rules, 2018	subsequent amendments, if any		

3.2	**Conformance to Standards** The equipment shall conform to relevant IEEE 802.11 standard (IEEE 802.11 a/b/g/n/ac/ax). Note: The procurer may refer to Annexure IVof this document for the possible deployment scenarios of Wi-Fi Access Points and the suitability of different IEEE 802.11 standards in them.	i. Test No.: - GR_WiFiAP_002 i. Data sheet of the equipment (specific to Radio Card and antenna data sheet) to be submitted.
3.3	**Association rates and Throughput** The Access Point in accordance with the technology used ((IEEE 802.11 a/b/g/n/ac/ax) should support the association rates/bit rates and minimum throughput for the different technologies in different configurations as specified in the Annexures mentioned below: §In case of IEEE 802.11a: Annexure IIa §In case of IEEE 802.11b: Annexure II b	i. Test No. :- GR_WiFiAP_003 i. Link budget calculation shall be submitted by Manufacturer/ Supplier.

	§ In case of IEEE 802.11g: Annexure II c §In case of IEEE 802.11n : Annexure II d §In case of IEEE 802.11ac: Annexure II e §In case of IEEE 802.11ax: Annexure II f The procurer shall specify/choose the configuration (bandwidth, frequency, bit rate etc) and the technology used (IEEE 802.11 a/b/g/n/ac/ax). Link budget calculation shall be submitted by Manufacturer/ Supplier.	
3.4	**Radio** The equipment shall comply with radio requirements specified in Clause 15.4.6 of IEEE 802.11 / clause 18.4.6 of IEEE 802.11b / clause 19.4 of IEEE 802.11g (IEEE 802.11-2007) / clause 20 of IEEE 802.11n-2009/Clause 22 of IEEE 802.11ac-2013 standards/clause 27 of IEEE 802.11 ax, as applicable.	i. Data sheet of the equipment (specific to Radio Card and antenna data sheet) to be submitted. i.Declaration for conformance to the standards mentioned in Clause 3.4 to be submitted.
3.5	**RF Technology** It shall use Direct Sequence Spread Spectrum (DSSS) technology and/or Orthogonal Frequency Division Multiplexing (OFDM). In Case of IEEE802.11ax AP, as it uses OFDM as well as Orthogonal Frequency Division Multiple Access (OFDMA),	i. Data sheet of the equipment (specific to Radio Card and antenna data sheet) to be submitted. i.Declaration for

	there shall be following mandatory features supported in the IEEE 802.11ax AP:	conformance to the standards mentioned in Clause 3.5 to be submitted.
3.5 i.	Downlink (DL) OFDMA : The AP shall successfully transmit DL OFDMA PPDUs to minimum 4 STAs in all supported bandwidths. The AP shall support all Resource Unit (RU) sizes for its operating bandwidth.	Test No. :- GR_WiFiAP_004
3.5 ii.	Uplink (UL) OFDMA : The AP shall successfully receive the corresponding data frames from minimum 4 STAs using OFDMA in all supported bandwidths. The AP shall support all Resource Unit (RU) sizes for its operating bandwidth.	Test No. :- GR_WiFiAP_005
3.5 iii.	Single User (SU) MIMO with 2 Spatial Streams: The AP shall transmit and receive successfully with 2 spatial streams in all supported bandwidths.	Test No. :- GR_WiFiAP_006
3.5 iv.	DL MU MIMO: This feature shall be mandatory only if the AP declared support for greater than or equal to four Spatial Stream (SS) Downlink (DL) transmission.	Test No. :- GR_WiFiAP_007
3.5 v.	Uplink (UL) Multi User (MU) MIMO: The AP shall	Test No. :- GR_WiFiAP_008

	support Uplink Multi user MIMO functionality.	
3.5 vi	Preamble Format: a. HE_SU is a new HE SU PPDU format to be used for communication between the AP and a single STA. The AP shall successfully transmit and receive HE SU PPDUs in all supported bandwidths and number of spatial streams. b. HE_MU preamble is used when the AP intends to transmit data simultaneously to multiple client devices. This PPDU format is designed for OFDMA and/or DL MU-MIMO transmission. The AP shall successfully transmit HE MU PPDUs. c. HE TB PPDU preamble format including the HE_TRIG preamble format, is used for UL MU transmission that is a response to a Trigger frame, including UL OFDMA. The AP shall successfully receive HE TB PPDUs.	Test No. :- GR_WiFiAP_005 GR_WiFiAP_006 GR_WiFiAP_007 GR_WiFiAP_008
3.5 vii	The AP shall support MCSs 0-7 for all supported bandwidths and all supported numbers of spatial streams.	Test No. :- GR_WiFiAP_050

3.5 viii	The AP shall successfully transmit and receive BCC-coded PPDUs in all supported modes for which LDPC is not mandatory for STAs.	Test No. :- GR_WiFiAP_049
3.5 ix	20MHz only mode: The AP shall support 20 MHz bandwidth operating mode.	Test No. :- GR_WiFiAP_009
3.5 x	TWT(Target Wake Time) : The AP shall support Target Wake Time functionality.	Test No.: GR_WiFiAP_010
3.5 xi	Spatial Reuse Operation: The AP shall set the BSS Color field in its transmitted High efficiency (HE) frames.	Test No.: GR_WiFiAP_011
3.6	**Transmitter parameters**	
3.6.1	**Effective isotropic radiated power** EIRP limit shall be as per NFAP. The tendering authority may specify EIRP as per requirements but considering interference issues. EIRP specified for 2.4 GHz band and for 5 GHz band as per NFAP 2018 and latest GSR issued by WPC should be complied to. The EIRP specifications must be in conformance to the latest NFAP as and when it is revised.	Test No. :- GR_WiFiAP_012

S.No.	Frequency Range	Title of the Rule	GSR No.	Requirements as per GSR IND	Remaks a per NFAP 2018
1.	2400-2483.5 MHz	Use of Low Power Equipment in the frequency band 2.4 GHz to 2.4835 GHz (Exemption from Licensing Requirement) Rules, 2005	As per Section 3) GSR No. 45 (E) dated 28-Jan-2005 , and subsequent amendments, if any: 4w (36 dbm)	4w (36 dbm)	-
2.	5150 - 5250	Use of Wirele	Section 3).	Please refer	IND 2

	MHz 5250 - 5350 MHz 5470-5725 MHz 5725 - 5875 MHz	ss Access Systems (WAS) including Radio Local Area Network (RLAN) in 5GHz (Exemption from Licensing Requirement) Rules, 2018	GSR No. 1048(E) dated 18-Oct.2018 and subsequent amendments, if any.	*Note		

*Note:

(i) in the band 5 150-5 250 MHz, for access points operating with transmitting antennas of antenna gain of 6 dBi and less, the maximum conducted output power over the frequency band of operation shall not exceed 30 dBm (1 Watt) and; the maximum power spectral density shall not exceed

	17 dBm (50 mW) in any 1 MHz band. If transmitting antennas of directional gain greater than 6 dBi are used, the maximum conducted output power and the maximum power spectral density shall be reduced by the amount in dB that the antenna gain exceeds 6 dBi. When used for outdoor access point applications, the maximum e.i.r.p. at any elevation angle above 30 degrees as measured from the horizontal direction shall not exceed 21 dBm (125 mW); (ii) fixed point-to-point access points operating in the frequency band 5 150-5 250 MHz may employ antennas with directional gain up to 23 dBi and use the maximum conducted output power and maximum power spectral density as indicated at sub-paragraph (i) above. With access points'/ devices' directional antenna gain higher than of 23 dBi, maximum conducted output power and maximum power spectral density shall be reduced by the amount in dB that the antenna gain exceeds 23 dBi; point-to-multipoint systems, omni directional applications, and multiple collocated transmitters transmitting the same information shall not be considered as point-to-point systems for the purpose of these rules; (iii) for mobile and portable client devices in the 5 150-5 250 MHz band, the maximum conducted output power over the frequency band of operation shall not exceed 250 mW provided the maximum antenna gain does not exceed 6 dBi and in addition, the maximum power spectral density shall not exceed 11 dBm in any 1 MHz band; if transmitting antennas of directional gain greater	

	than 6 dBi are used, both the maximum conducted output power and the maximum power spectral density shall be reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi; (iv) in the frequency bands 5 250 – 5 350 MHz and 5 470- 5 725 MHz for access points operating with transmitting antennas of antenna gain 6 dBi and less, the maximum conducted output power over the frequency band of operation shall not exceed 24 (250 mW) or 11dBm + 10 log B, whichever is less, where ‘B’ is the emission bandwidth in MHz. In addition, the maximum power spectral density shall not exceed 11dBm in any 1 MHz band. If transmitting antennas of directional gain greater than 6 dBi are used, the maximum conducted output power and the maximum power spectral density shall be reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi. The use of appropriate interference mitigation technique dynamic frequency selection and or transmit power control shall be mandatory. Transmit power control mechanism may not be required for systems with an e.i.r.p. of less than 500 mW. (v) in the band 5 725-5 875 MHz, the minimum 6 dB bandwidth of the devices shall be at least 500 kHz and with transmitting antennas of antenna gain 6 dBi and less, the maximum conducted output power over the frequency band of operation shall not exceed 30 dBm (1 W). In addition, the maximum power spectral density shall not exceed 30 dBm in any 500 kHz band. If the transmitting antennas of directional gain greater than 6 dBi are	

<table>
<tr><td></td><td>used, both the maximum conducted output power and the maximum power spectral density shall be reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi;
(vi) Fixed point-to-point access points operating in the 5 725-5 875 MHz band may employ antennas with directional gain up to 23 dBi and use the maximum conducted output power and maximum power spectral density as indicated at sub-paragraph (iv) above. With access point devices directional antenna gain higher than of 23 dBi, maximum conducted output power and maximum power spectral density shall be reduced by the amount in dB that the antenna gain exceeds 23 dBi.</td><td></td></tr>
<tr><td><b>3.6.2</b></td><td><b>Peak power density</b>
For direct sequence systems, the peak power spectral density shall not be greater than 8 dBm in any 3 kHz band during any time interval of continuous transmission.</td><td>Test No. :- GR_WiFiAP_013</td></tr>
<tr><td><b>3.6.3</b></td><td><b>Processing gain</b>
The processing gain (the ratio in dB of the signal-to-noise ratio with the system spreading code turned off to the signal-to-noise ratio with the system spreading code turned on) of the equipment shall be at least 10 dB. This shall be applicable only for direct-sequence spread spectrum (DSSS) Technology.</td><td>Test No. :- GR_WiFiAP_014</td></tr>
<tr><td><b>3.6.4</b></td><td><b>Field Strength</b>
The field strength of emissions from the equipment shall comply with the following:
<b>Table 1: Field strength of emissions</b><table><tr><th>Fundamental</th><th>Field Strength of</th></tr></table></td><td>Test No. :- GR_WiFiAP_015</td></tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr><th>Frequency</th><th>Harmonics</th></tr>
<tr><td>2.4 GHz and 5 GHz band as per NFAP</td><td>≤0.5 mV/ meter</td></tr>
</table>

Field strength limits are specified at a distance of 3 meters. Emissions radiated outside of the specified frequency bands, except for harmonics, shall be attenuated by at least 50 dB below the level of the fundamental.
</td>
<td></td>
</tr>
<tr>
<td><b>3.6.5</b></td>
<td>
<b>Spurious emissions of the transmitter</b>
Spurious emissions are emissions outside the frequency range (s) of the equipment as defined in clause 3.6.4.
The level of spurious emissions shall be measured either as:
a) (i) Its power in a specified load (conducted spurious emissions); and
(ii) Its effective radiated power when radiated by the cabinet or structure of the equipment
OR
b) Its effective radiated power when radiated by cabinet and antenna.
The spurious emissions of the equipment shall not exceed the values in tables 2 and 3 in the indicated bands.

<b>Table 2: Transmitter limits for narrowband spurious emissions</b>

<table>
<tr><th>Frequency Range</th><th>Limit when operating</th><th>Limit when in standby</th></tr>
</table>
</td>
<td>i. Test No. :- GR_WiFiAP_016</td>
</tr>
</table>

30 MHz -1000 MHz	-36 dBm	-57 dBm	
Above 1 GHz —12.75 GHz	-30 dBm	-47 dBm	
1.8 GHz — 1.9 GHz 5 .15 GHz — 5.3 GHz	-47 dBm	-47 dBm	

Wideband spurious emission shall not exceed the values given in table 3.

Table 3: Transmitter limits for wideband spurious emissions

Frequency Range	Limit when operating	Limit when in standby
30 MHz -1000 MHz	-86 dBm/Hz	- 107 dBm/Hz
Above 1 GHz —12.75 GHz	-80 dBm/Hz	-97 dBm/Hz
1.8 GHz — 1.9 GHz 5 .15 GHz — 5.3 GHz	-97 dBm/Hz	-97 dBm/Hz

3.7	**Receiver Parameters**	
3.7.1	**Receiver Sensitivity**	i. Test No. :-

<table>
<tr><td></td><td>As per clause 17.3.10.1 of IEEE 802.11-2007 (for 802.11a/ b/g), clause 20.3.22.1 of IEEE 802.11n - 2009 and clause 22.3.19.1 of IEEE 802.11ac-2013 (Refer Annexure –III of this document) and clause 27.3.20.1 of IEEE 802.11 ax.</td><td>GR_WiFiAP_017</td></tr>
<tr><td><b>3.7.2</b></td><td><b>Spurious emissions of the Receiver</b>
The level of spurious emissions shall be measured either as:
a) (i) Its power in a specified load (conducted spurious emissions); and
(ii) Its effective radiated power when radiated by the cabinet or
Structure of the equipment (cabinet radiation);
or
b) Its effective radiated power when radiated by cabinet and antenna.
The spurious emissions of the receiver shall not exceed the values in tables 4 and 5 in the indicated bands.

<b>Table 4: Narrowband spurious emissions limits for receivers</b>
<table>
<tr><th>Frequency Range</th><th>Limit</th></tr>
<tr><td>30 MHz -1000 MHz</td><td>-57 dBm</td></tr>
<tr><td>Above 1 GHz - 12.75 GHz</td><td>- 47 dBm</td></tr>
</table>

Note: The limit values of Table 4 apply to narrowband emission, e.g. as caused by local oscillator leakage. The measurement bandwidth for such emission may be as small as necessary to get a reliable</td><td>Test No. :- GR_WiFiAP_018</td></tr>
</table>

<table>
<tr>
<td></td>
<td>measurement result.
Wideband emission shall not exceed the values given in table 5.
Table 5: Wideband spurious emissions limits for receivers
<table>
<tr><th>Frequency Range</th><th>Limit</th></tr>
<tr><td>30 MHz- 1000MHz</td><td>-107 dBm/Hz</td></tr>
<tr><td>Above 1 GHz - 12.75 GHz</td><td>- 97 dBm/Hz</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td><b>3.8</b></td>
<td><b>Bit Rates</b>

It shall support channel bit rates up to:-
As per Clause 3.3 (Annexure II)
• 1, 2, 5.5, and 11 Mbps with feature of automatic data rate selection as per IEEE 802.11b
• 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48 and 54 Mbps of IEEE 802.11g
• Upto 300Mbps as per IEEE 802.11n-2009 with channel bonding.
<b>• For IEEE 802.11ac</b>
▪ Upto 86 Mbps as per IEEE 802.11ac-2013 and 20 MHz channel bandwidth, 1 spatial stream.
▪ Upto 200 Mbps as per IEEE 802.11ac-2013 and 40 MHz channel bandwidth,1 spatial stream.
▪ Upto 433 Mbps as per IEEE 802.11ac-2013 and 80 MHz channel bandwidth,1 spatial stream.
▪ Upto 867 Mbps as per IEEE 802.11ac-2013 and 160 MHz channel bandwidth, 1 spatial stream.
▪ Upto 173.3 Mbps as per IEEE 802.11ac-2013 and 20 MHz channel bandwidth, 2 spatial streams.
▪ Upto 400Mbps as per IEEE 802.11ac-2013 and 40</td>
<td>Test No. :- GR_WiFiAP_050</td>
</tr>
</table>

	MHz channel bandwidth,2 spatial streams ▪ Upto 866.7 Mbps as per IEEE 802.11ac-2013 and 80 MHz channel bandwidth,2 spatial streams. ▪ Upto 1733.3 Mbps as per IEEE 802.11ac-2013 and 160 MHz channel bandwidth, 2 spatial streams. ▪ Upto 346.7 Mbps as per IEEE 802.11ac-2013 and 20 MHz channel bandwidth, 4 spatial streams. ▪ Upto 800Mbps as per IEEE 802.11ac-2013 and 40 MHz channel bandwidth,4 spatial streams ▪ Upto 1733.3 Mbps as per IEEE 802.11ac-2013 and 80 MHz channel bandwidth,4 spatial streams. ▪ Upto 3446.7 Mbps as per IEEE 802.11ac-2013 and 160 MHz channel bandwidth, 4 spatial streams. **• For IEEE 802.11ax** ▪ Upto 143.4Mbps as per IEEE 802.11ax and 20MHz channel bandwidth, 1 spatial stream ▪ Upto 286.8Mbps as per IEEE 802.11ax and 40MHz channel bandwidth, 1 spatial stream ▪ Upto 600.5Mbps as per IEEE 802.11ax and 80MHz channel bandwidth, 1 spatial stream ▪ Upto 1201Mbps as per IEEE 802.11ax and 160MHz channel bandwidth, 1 spatial stream ▪ Upto 286.8 Mbps as per IEEE 802.11ax and 20MHz channel bandwidth, 2 spatial streams ▪ Upto 573.5Mbps as per IEEE 802.11ax and 40MHz channel bandwidth, 2 spatial streams ▪ Upto 1201Mbps as per IEEE 802.11ax and 80MHz channel bandwidth, 2 spatial streams ▪ Upto 2402Mbps as per IEEE 802.11ax and 160MHz channel bandwidth, 2 spatial stream ▪ Upto 573.5Mbps as per IEEE 802.11ax and 20MHz channel bandwidth, 4 spatial streams ▪ Upto 1147.1Mbps as per IEEE 802.11ax and 40MHz	

	channel bandwidth, 4 spatial streams ▪ Upto 2402Mbps as per IEEE 802.11ax and 80MHz channel bandwidth, 4 spatial streams ▪ Upto 4803.9Mbps as per IEEE 802.11ax and 160MHz channel bandwidth, 4 spatial streams ▪ Upto 1147.1Mbps as per IEEE 802.11ax and 20MHz channel bandwidth, 8 spatial streams ▪ Upto 2294.1Mbps as per IEEE 802.11ax and 40MHz channel bandwidth, 8 spatial streams ▪ Upto 4803Mbps as per IEEE 802.11ax and 80MHz channel bandwidth, 8 spatial streams ▪ Upto 9607.8Mbps as per IEEE 802.11ax and 160MHz channel bandwidth, 8 spatial streams	
3.9	**Antenna** Antenna arrangement depends on application (Indoor and/or Outdoor). The details of antenna (like gain, frequency-range, beamwidth, integrated/external, size, etc.), interconnecting cables and interfaces depending on application requirements (like type of configuration, data rates, path profile, etc.) shall be indicated by the supplier.	i. Data sheet of the equipment (specific to antenna) to be submitted.
3.10	It shall have visual status indication on the unit in case of indoor deployment and on EMS/ WLAN controller in case of outdoor deployment for i) Activity over Radio ii) Activity over the Ethernet iii) Operating / Faulty State iv) Power indicator As an option, audio status indication can also be provided.	i. Test No. :- GR_WiFiAP_019

3.11	**Power supply requirements** The equipment should be able to operate on AC/DC/PoE(Power over Ethernet). The AC power supply shall be of 230 V + 10% to -15% and frequency 50 Hz ± 2 Hz. DC/PoE Supply details to be given by the supplier / manufacturer. Solar/Wind Power option may also be provided.	i. Test No. :- GR_WiFiAP_020
3.12	**Interference detection and avoidance.** The equipment should dynamically sense the spectrum and select the clean channel for effective throughput.	i. Test No. :- GR_WiFiAP_021
3.13	**Channel bonding** The AP may support channel bonding mode as per IEEE 802.11n/ac/ax TEC Standard No. TEC 38020:2021 standards with fallback mechanisms in case of collisions	Test No. :- GR_WiFiAP_047
3.14	It shall be possible to configure AP to support backward compatibility with IEEE 802.11 a/b/g/n/ac based CPEs.	Test No. :- GR_WiFiAP_048
4.0	**Interface Requirements**	
4.1	The equipment should adhere to the Clause no. 2.0 and the sub-clauses under it of TEC IR No. TEC/IR/R/WiFiAP/001/01. MARCH 2015.	i. Document to be submitted with the requisite test results for conformity as per the IR mentioned under Clause 4.1. ii. The tests prescribed in the IR and not covered under the GR must be identified and tested as per the TSTP of IR.
4.2	The Equipment shall be "Wi-Fi CERTIFIED™".	Wi-Fi CERTIFIED

	Note: - ● If the equipment is “Wi-Fi CERTIFIED™” clauses/parameters already tested may not be tested again for TEC certification. ● If the equipment is not “Wi-Fi CERTIFIED™”, then equipment shall be tested by TEC against this GR, for TEC certification purposes.	certificate if available shall be submitted.
4.3	Radio interface shall conform to IEEE standards 802.11a/b/g/n/ac/ax as applicable.	Test No. :- GR_WiFiAP_022
4.4	SNMP v2, v3 or above, or XML or CAPWAP or JSON shall be supported for management by a central NOC/EMS/WLAN Controller.	Test No. :- GR_WiFiAP_023
4.5	Interfaces: Equipment shall support 10/100/1000/2500/10000 Mbps electrical or optical Ethernet Interface.	Test No. :- GR_WiFiAP_024
4.6	Interface Ports:Auto sensing IEEE 802.3 10/100/1000/2500/10000 BASE-T Ethernet.	i. Test No. :- GR_WiFiAP_024
4.7	IPv4 and IPv6 addressing shall be supported.	i. Test No. :- GR_WiFiAP_025
5.0	**Quality Requirements**	
5.1	The manufacturer shall have a valid ISO 9001:2008 or any other equivalent ISO certificate.	Certificate should be submitted.
5.2	The equipment shall meet the environmental requirements as per ‘Category B-2’ (in case of Indoor equipment) and ‘Category D’ (in case of Outdoor equipment) of QM-333 March 2010	Test results/certificate from Accredited lab to be submitted.

	Standard for Environmental Testing of Telecommunication Equipment.	
5.3	The MTBF (Mean Time between Failure) and MTTR (Mean Time To Restore) predicted shall be provided and the manufacturer shall furnish observed values.	Details to be provided by manufacturer.
5.4	In case of outdoor deployment of Wi-Fi Access Point, it should be minimum IP-65 compliant. The equipment may be IP-67 compliant as per user/procurer's requirement.	Test results/certificate for IP-65 compliance from Accredited lab to be submitted.
6.0	**EMI/EMC Requirements** The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report from accredited test lab shall be furnished from a test agency. a) Conducted and radiated emission (applicable to telecom equipment): Name of EMC Standard: "CISPR 32 (2015) with amendments - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment". Limits:- i) To comply with Class B of CISPR 32 (2015) with amendments for indoor deployments and Class A of CISPR 32 (2015) with amendments for outdoor deployments. b) Immunity to Electrostatic discharge: Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test". Limits: -	Report from NABL/ILAC accredited test lab to be submitted.

	i) Contact discharge level 2 {± 4 kV} or higher voltage; ii) Air discharge level 3 {± 8 kV} or higher voltage; c) Immunity to radiated RF: Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques- Radiated RF Electromagnetic Field Immunity test" Limits:- For Telecom Terminal Equipment without Voice interface (s) Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz. d) Immunity to fast transients(burst): Name of EMC Standard: IEC 61000- 4- 4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test" Limits:- Test Level 2 i.e. a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal / control / data / telecom lines; e) Immunity to surges: Name of EMC Standard: IEC 61000-4-5 (2014) “Testing & Measurement techniques for Surge immunity test"	

	Limits:- i) For mains power input ports : (a)2 kV peak open circuit voltage for line to ground coupling (b) 1 kV peak open circuit voltage for line to line coupling ii) For telecom ports : (a) 2kV peak open circuit voltage for line to ground (b) 0.5KV peak open circuit voltage for line to line coupling. f) Immunity to conducted disturbance induced by Radio frequency fields: Name of EMC Standard: IEC 61000-4-6 (2013) with amendments) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields” Limits:- Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines. g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any): Name of EMC Standard: IEC 61000-4-11 (2014) “Testing & measurement techniques-voltage dips, short interruptions and voltage variations immunity tests” Limits:- i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e. 70 % supply voltage for 500 ms) ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e.	

	40% supply voltage for 200ms) and iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s. iv) a voltage interruption corresponding to a reduction of supply voltage of >95% for 10s. h) Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any): Name of EMC Standard: IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests Limits: i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B. ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C. iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B. iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000ms. Applicable Performance Criteria shall be C. v. Voltage variations corresponding to 80% and 120%of supply for 100 ms to10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B. Note: - For checking compliance with the above EMC requirements, the method of measurements shall	

<table>
<tr>
<td></td>
<td>be in accordance with TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16 and the referenced base standards i.e. IEC and CISPR standards and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (h) and TEC Standard TEC/SD/DD/EMC-221/05/OCT-16. The details of IEC/CISPR and their corresponding Euro Norms are as follows:
<table>
<tr><td>IEC/CISPR</td><td>Euro Norm</td></tr>
<tr><td>CISPR 11</td><td>EN 55011</td></tr>
<tr><td>CISPR 32</td><td>EN55032</td></tr>
<tr><td>IEC 61000-4-2</td><td>EN 61000-4-2</td></tr>
<tr><td>IEC 61000-4-3</td><td>EN 61000-4-3</td></tr>
<tr><td>IEC 61000-4-4</td><td>EN 61000-4-4</td></tr>
<tr><td>IEC 61000-4-5</td><td>EN 61000-4-5</td></tr>
<tr><td>IEC 61000-4-6</td><td>EN 61000-4-6</td></tr>
<tr><td>IEC 61000-4-11</td><td>EN 61000-4-11</td></tr>
<tr><td>IEC 61000-4-29</td><td>EN 61000-4-29</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td><b>7.0</b></td>
<td><b>Safety Requirements</b>
The equipment shall conform to:
a) IS 13252 part 1: 2010 “Information Technology Equipment –Safety- Part 1: General Requirements” [equivalent to IEC 60950-1 {2005} “Information Technology Equipment –Safety- Part 1: General Requirements”]
OR
IEC 62368-1: 2018 “Audio/video, information and</td>
<td>Report from NABL/ILAC accredited test lab to be submitted.</td>
</tr>
</table>

	communication technology equipment - Part 1: Safety requirements" b) IS 10437{1986} "Safety requirements for radio transmitting equipments" [equivalent to IEC 60215].	
8.0	**Security Requirements**	
8.1	Equipment shall conform to WPA2 based on IEEE 802.11i standard, access control authentication based on 802.1X / EAP Standard and in case of IEEE 802.11ax, equipment shall conform to WPA3 personal and WPA 3 enterprise as well.	Test No. :- GR_WiFiAP_026 GR_WiFiAP_027
8.2	Equipment shall conform to Media Access control security based on 802.1 AE as an optional requirement.	Test No. :- GR_WiFiAP_028
8.3	Service Set Identifier (SSID) shall be definable by Administrator.	Test No. :- GR_WiFiAP_029
8.4	In case of authentication and authorization is implemented through a RADIUS server, IETF RFC 2865 should be supported and optionally if required IETF RFC 2866, 2867 may also be supported.	GR_WiFiAP_030
9.0 Other Requirements		
9.1	**Identification of Equipment** i) Equipment shall be marked with supplier's or manufacturer's logo/name. ii) The Model No., serial No., Month and year of manufacture shall be indicated by screen printing on the body of equipment or by tamper-proof sticker	Physical check and relevant document to be submitted.

	pasted on the body of equipment. iii) Power Supply requirements shall be indicated on the body. iv) Above markings shall be legible, indelible and easily visible.	
9.2	**Documentation** Detailed documentation in English or Hindi shall be provided, including: i) Self-explanatory user manual giving details of all functions, facilities and procedures ii) Set-up and configuration parameters and procedures iii) Trouble shooting guide including fault dictionary. iv) Repair manual (Optional)	Relevant document to be submitted.
10.0 Optional Requirements		
10.1	Requirements for Type-'A' Type 'A' Access Point without routing but bridging functionality with Ethernet LAN/WAN ports, may also support, as per the procurer's requirements, some or all of the functionalities as below: i) IEEE 802.1q VLAN tagging (SSID to VLAN Mapping) ii) Mesh (Easy Mesh or 802.11s) and repeater modes of operation iii) ARP (IETF RFC 826) iv) IEEE 802.1p priority v) Spectrum sensing and reporting capability vi) Multiple SSID support for operator sharing. vii) Support for VAP (Virtual Access Point) viii) Configuration of parameters through web interface when link to NOC/EMS/WLAN Controller is not	Testing as listed below corresponding to the specifications under the roman numerals of Clause 10.1. i. Test No.: - GR_WiFiAP_031 ii. Test No.: - GR_WiFiAP_032 iii. Test No.: - GR_WiFiAP_033 iv. Test No.: - GR_WiFiAP_034 v. Test No.: - GR_WiFiAP_035 vi. Test No.: - GR_WiFiAP_036 vii. Test No.: -

	available. ix) NavIC support on board x) Concurrent clients per radio xi) Support of dying gasp (DG) feature for Outdoor deployment	GR_WiFiAP_037 viii. Test No. :- GR_WiFiAP_038 ix. Test No. GR_WiFiAP_039 x. Test No. GR_WiFiAP_040 xi. Test No. GR_WiFiAP_041
10.2	**Requirements for Type- 'B'** Type 'B' Access Point with built in routing and bridging functionality with Ethernet LAN/WAN ports, may also support, as per the procurer's requirements, some or all of the functionalities as below: i) IEEE 802.1q VLAN tagging ii) PPPoE for WAN port. iii) DHCP Server, client(optional),relay (RFC 2131, 951 and 3046) iv) ARP (IETF RFC 826) v) IEEE 802.1p priority vi) VPN Client vii) Firewall Support viii) NAT ix) NavIC support on board x) Concurrent clients per radio xi) Support of dying gasp (DG) feature for Outdoor deployment	Testing as listed below corresponding to the specifications under the roman numerals of Clause 10.1. i. Test No.: - GR_WiFiAP_031 ii. Test No.: - GR_WiFiAP_042 iii. Test No.: - GR_WiFiAP_043 iv. Test No.: - GR_WiFiAP_033 v. Test No.: - GR_WiFiAP_034 vi. Test No.: - GR_WiFiAP_044 vii. Test No.: - GR_WiFiAP_045 viii. Test No. :- GR_WiFiAP_046

		ix. Test No. :- GR_WiFiAP_039 x. Test No. :- GR_WiFiAP_040 xi. Test No. :- GR_WiFiAP_041
+10.3	In case of Hotspot 2.0 deployment, relevant features of IEEE 802.11u should be supported by the AP.	Wi-Fi Alliance's Wi-Fi Certified Passpoint certificate to be submitted.
10.4	In case of SIM based authentication EAP-SIM, AKA, EAP-AKA' should be supported while for non-SIM based authentication EAP-TLS, EAP- TTLS, EAP- should be supported by the AP..	Compliance to the following RFCs to be submitted: i. RFC 4186 i. RFC 5216 i. RFC 5281 v. RFC 4167
11.	**Additional Requirements for WANI compliant Wi-Fi Access Point.**	
11.1	In case of standalone operation wherein a single Wi-Fi AP has been deployed as a PDO and parented by PDOA a) The Access Point must be configured in Router mode. b) The Access Point must have DHCP server for IP allocation to the connected devices.	Test No.: - GR_WiFiAP_051
11.2	In case of cluster deployment of multiple Wi-Fi APs under a single PDO network, requirement of router mode of operation and DHCP server functionality may be provisioned for the cluster instead of a single Wi-Fi AP.	Test No.: - GR_WiFiAP_052
11.3	In case of cluster deployment of Wi-Fi APs under a single PDO network, they must support SSID	Test No.: - GR_WiFiAP_053

	based roaming/Fast BSS Transition (802.11r) for faster reassociation with roaming.	
11.4	The Access Point must support a minimum of 20 connected devices concurrently.	Test No.: - GR_WiFiAP_054
11.5	The Access Point must be deployed with storage facility so as to be able to transfer IP Detail Record to PDOA after end of session or periodically after every 24 hours.	Test No.: - GR_WiFiAP_055
11.6	The Access point must support network clock synchronization.	Test No.: - GR_WiFiAP_056
11.7	As backup, the Access Point must be deployed with a minimum storage to ensure IPDR logging for minimum 3 days.	Test No.: - GR_WiFiAP_057
11.8	The Access Point shall be able to present a uniquely branded user interface called Captive Portal when the wireless client device connects to it.	Test No.: - GR_WiFiAP_058
11.9	Provision for Whitelisting of PDOA related IPs/URLs.	Test No.: - GR_WiFiAP_059
11.10	The operation of Wireless Access Point shall be in the license free bands of 2.4 and/or 5 GHz bands and as per latest National Frequency Allocation Plan (NFAP) and published WPC GSRs as mentioned in Clause 3.1	Data sheet of the equipment (specific to Radio Card) to be submitted.

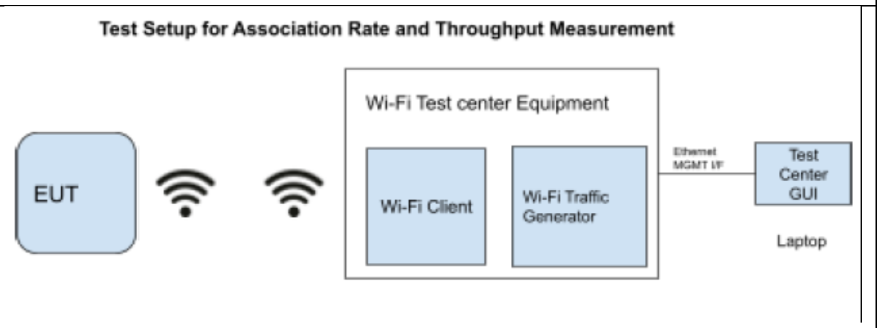
-

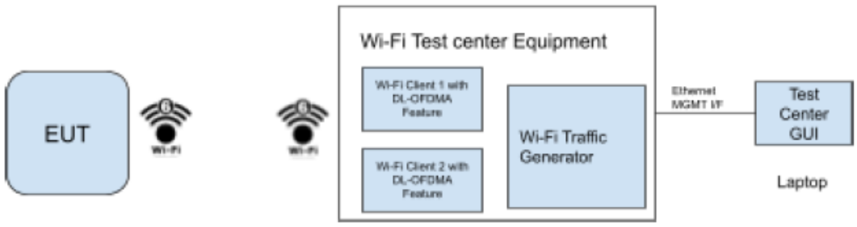
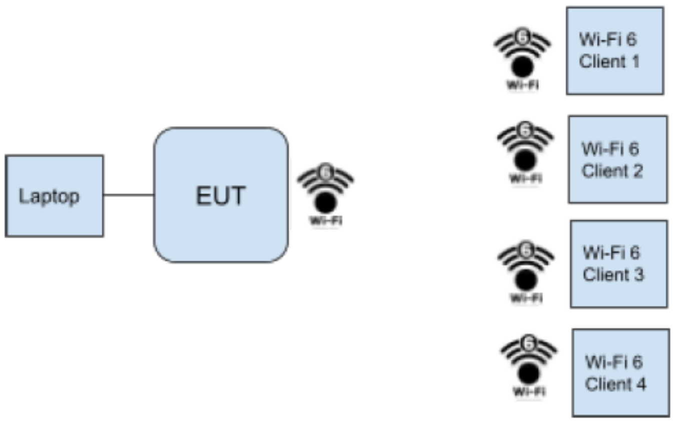
I. TEST SETUP & PROCEDURES:

Test No.	GR_WiFiAP_001
Test Details	To check the operating frequency of the Wi-Fi Access Point.
Test Instruments Required	1. Equipment under test 2. Laptop with open source tools like Inssider etc. OR Licensed tools etc. 3. Connecting cables.
Test Setup	Test setup for frequency range test EUT Wi-Fi Client
Test Procedure	1. Configure the EUT for the desired mode of operation (802.11 a/b/g/n/ac/ax) one at a time in a desired frequency band of 5GHz band or 2.4GHz 2. Connect a licensed equipment or a laptop OR 3. Verify using open source tools like Inssider, laptop or licensed equipment that the EUT is in the desired frequency of operation
Test Limits	Frequency of operation should be as per Clause 3.1
Expected Results	The EUT should operate in the prescribed frequency band.

--Test No.	GR_WiFiAP_002
Test Details	To check compliance to Conformance to Standards as per Clause 3.2.
Test Instruments Required	1. Equipment under test (EUT) 2. Laptop with open source tools like Inssider, Iperf etc. OR Licensed tools etc. 3. Connecting cables.
Test Setup	Test setup for mode of operation IEEE 802.11 a/b/g/n/ac/ax EUT Wi-Fi Client
Test Procedure	1. Configure the EUT for the desired mode of operation (802.11 a/b/g/n/ac/ax) one at a time 2. Connect a licensed equipment Test Center or a laptop as a Wi-Fi Client. 3. Ping between the laptop/equipment to the EUT 4. Verify open source tools like Inssider, laptop or licensed equipment that the EUT is associating at the desired bitrates
Test Limits	As per applicable Tables under Clause 3.2.
Expected Results	The EUT should comply with all the standards listed in Clause 3.2 but one at a time as configured.

Test No.	GR_WiFiAP_003
Test Details	To check the compliance for bit rates as per Clause no. 3.3.

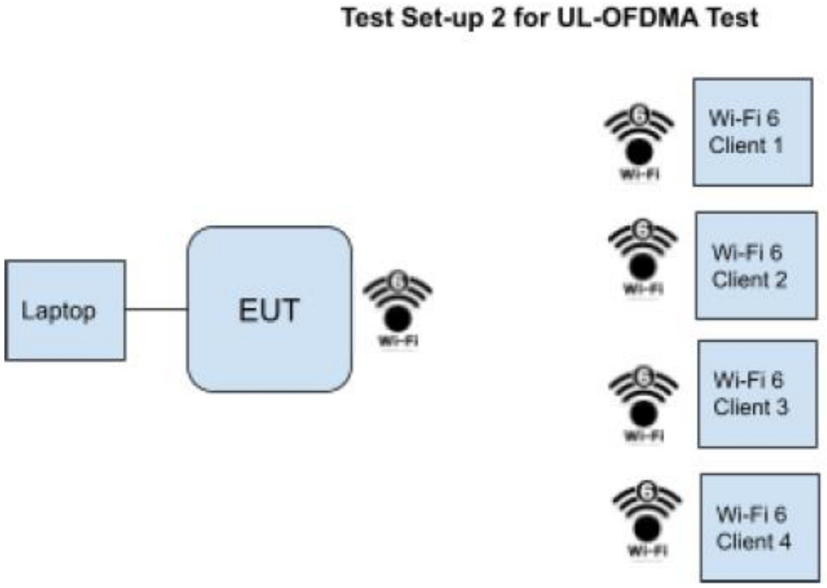
Test Instruments Required	● Equipment under test (EUT) ● Licensed Wi-FI Test Equipment ● Laptop with open source tools like iperf,ethereal,tcpdump or wireshark etc. ● Connecting cables.
Test Setup	 Test Setup for Association Rate and Throughput Measurement Wi-Fi Test center Equipment EUT Wi-Fi Client Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop
Test Procedure	1. Place the entire setup - EUT, licensed equipment or laptop - in a controlled environment such as a RF tent. 2. Configure the EUT for one of the desired mode of operation (802.11 a/b/g/n/ac/ax) 3. Configure the EUT for the desired bit rate as per the different IEEE 802.11 a/b/g/n/ac/ax one at a time 4. Connect a licensed equipment or a laptop and measure the minimum average data throughput over 60 seconds using licensed equipment or open-source tools like 'iperf'.
Test Limits	As per applicable Tables under Clause 3.3.
Expected Results	The data rates should be as per the specifications under Clause 3.3.

Test No.	GR_WiFiAP_004
Test Details	To check the functionality of DL-OFDMA feature as per Clause no. 3.5(i) and 3.5(vi) b.
Test Instruments Required	● Equipment under test (EUT) ● 4 Wi-Fi 6 Clients with DL-OFDMA Feature or Licensed Equipment (Wi-Fi Test Center) with DL-OFDMA feature enabled ● Laptop with open source tools like iperf,ethereal,tcpdump or wireshark etc. ● Connecting cables.
Test Setup	**Test Setup-1 for DL-OFDMA Test**  EUT Wi-Fi Wi-Fi Wi-Fi Test center Equipment Wi-Fi Client 1 with DL-OFDMA Feature Wi-Fi Client 2 with DL-OFDMA Feature Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop **Test Set-up 2 for DL-OFDMA Test**  Laptop EUT Wi-Fi Wi-Fi 6 Client 1 Wi-Fi 6 Client 2 Wi-Fi 6 Client 3 Wi-Fi 6 Client 4

Test Procedure	1. Place the entire setup - EUT, licensed equipment/Wi-Fi6 clients in a controlled environment such as a RF tent. 2. Configure the EUT in 802.11 ax mode with DL-OFDMA feature disabled. 3. Configure Test Equipment and simulate 4 Wi-Fi 6 clients in 802.11ax mode. 4. Connect a licensed equipment or Wi-Fi 6 Clients with EUT over wireless interface.Run ping between AP and Clients to verify connection. 5. Measure the latency using licensed equipment or open-source tools like 'iperf between AP and all the four connected clients simultaneously and note aggregate throughput'. 6. Now, configure the EUT in 802.11 ax mode with DL-OFDMA feature enabled. 7. Connect a licensed equipment or Wi-Fi 6 Clients with EUT over wireless interface.Run ping between AP and Client to verify connection. 8. Measure the latency using licensed equipment or open-source tools like 'iperf' between AP and all the connected clients simultaneously and note aggregate throughput. 9. Compare latency measured in step 5 and step 8 to verify the gain of DL-OFDMA feature. 10. Capture Packets in the Laptop using Wireshark

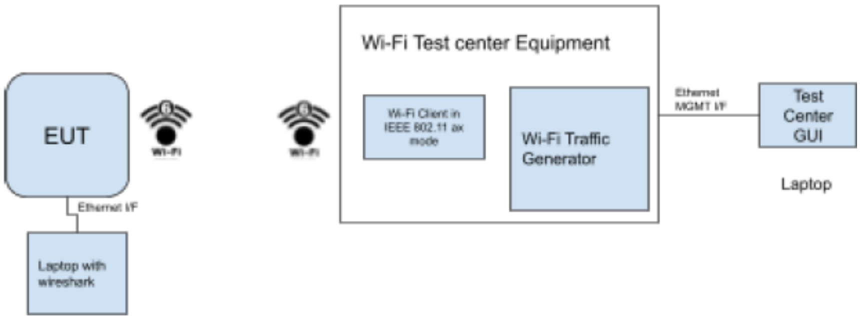
	application to verify preamble type HE_MU in the PPDU header
Test Limits	As per applicable Tables under Clause 3.5(i) and 3.5(vi) b.
Expected Results	The results should be as per the specifications under Clause 3.5(i) and 3.5(vi) b.

Test No.	GR_WiFiAP_005
Test Details	To check the functionality of UL-OFDMA features as per Clause no. 3.5(ii) and 3.5(vi) c.
Test Instruments Required	● Equipment under test (EUT) ● 4 Wi-Fi 6 Clients with UL-OFDMA Feature or Wi-Fi Test Center with UL-OFDMA feature enabled ● Licensed Wi-Fi Test Equipment,Laptop with open source tools like iperf,ethereal,tcpdump or wireshark etc. ● Connecting cables.

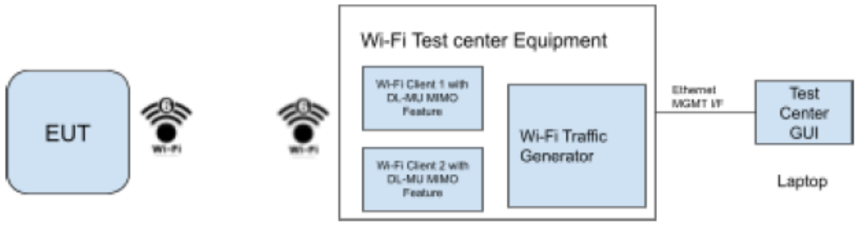
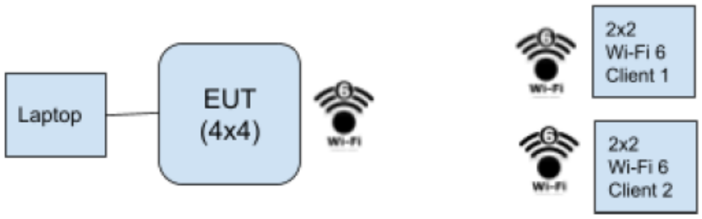
Test Setup	 Test Set-up 2 for UL-OFDMA Test Laptop EUT Wi-Fi Wi-Fi 6 Client 1 Wi-Fi 6 Client 2 Wi-Fi 6 Client 3 Wi-Fi 6 Client 4
Test Procedure	1. Place the entire setup - EUT, licensed equipment/Wi-Fi6 clients in a controlled environment such as a RF tent. 2. Configure the EUT in 802.11 ax mode with UL-OFDMA feature disabled. 3. Configure Test Equipment and simulate 4 Wi-Fi 6 clients in 802.11ax mode. 4. Connect a licensed equipment or Wi-Fi 6 Clients with EUT over wireless interface.Run ping between AP and Clients to verify connection. 5. Measure the latency ut using licensed equipment or open-source tools like 'iperf between AP and all the four connected clients simultaneously and note aggregate throughput'.

	6. Now, configure the EUT in 802.11 ax mode with UL-OFDMA feature enabled. 7. Connect a licensed equipment or Wi-Fi 6 Clients with EUT over wireless interface.Run ping between AP and Client to verify connection. 8. Measure the latency using licensed equipment or open-source tools like 'iperf' between AP and all the connected clients simultaneously and note aggregate throughput. 9. Compare latency measured in step 5 and step 8 to verify the gain of UL-OFDMA feature. 10. Capture Packets in the Laptop using Wireshark application to verify preamble type HE_TRIG in the PPDU header
Test Limits	As per applicable Tables under Clause 3.5(ii) and 3.5(vi) c.
Expected Results	The results should be as per the specifications under Clause 3.5(ii) and 3.5(vi) c.

Test No.	GR_WiFiAP_006
Test Details	To check the functionality of SU-MIMO feature as per Clause no. 3.5(iii) and 3.5(vi) a.
Test Instruments Required	● Equipment under test (EUT) ● Single Wi-Fi 6 Client or Licensed Wi-Fi Test Equipment ● Laptop with open source tools like iperf,ethereal,tcpdump or wireshark etc. ● Connecting cables.

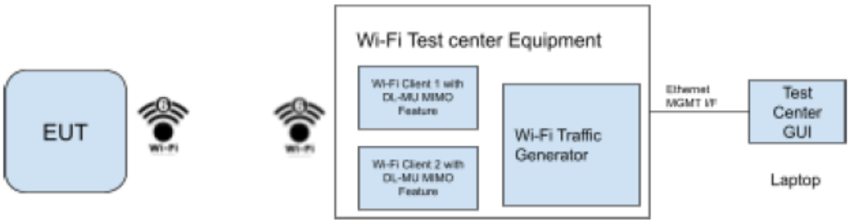
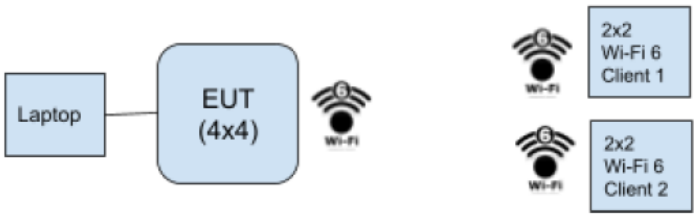
Test Setup	Test Setup for SU-MIMO Test  Wi-Fi Test center Equipment EUT Wi-Fi Wi-Fi Wi-Fi Client in IEEE 802.11 ax mode Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop Ethernet I/F Laptop with wireshark
Test Procedure	1. Place the entire setup - EUT, licensed equipment/Wi-Fi6 client 2. Configure the EUT in 802.11 ax mode with OFDMA and MU-MIMO feature disabled. 3. Configure Test Equipment and simulate single Wi-Fi 6 client in 802.11ax mode. 4. Connect a licensed equipment or Wi-Fi 6 Client with EUT over wireless interface.Run ping between AP and Client to verify connection. 5. Measure the data throughput using licensed equipment or open-source tools like 'iperf between AP and connected client. 6. Capture Packets in the Laptop using Wireshark application to verify preamble type HE_SU in the PPDU header
Test Limits	As per applicable Tables under Clause 3.5(iii) and 3.5(vi) a.
Expected Results	The results should be as per the specifications under Clause 3.5(iii) and 3.5(vi) a.

Test No.	GR_WiFiAP_007
Test Details	To check the functionality of DL-MU MIMO feature as per Clause no. 3.5(iv) and 3.5(vi) b. EUT should have 4 or more spatial streams.

Test Instruments Required	● Equipment under test (EUT) ● Two 2x2 MIMO Wi-Fi 6 Clients with DL-MU MIMO Feature or Wi-Fi Test Center with DL- MU MIMO feature enabled ● Laptop with open source tools like iperf,ethereal,tcpdump or wireshark etc. ● Connecting cables.
Test Setup	**Test Setup-1 for DL-MU MIMO Test**  EUT Wi-Fi Wi-Fi Wi-Fi Test center Equipment Wi-Fi Client 1 with DL-MU MIMO Feature Wi-Fi Client 2 with DL-MU MIMO Feature Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop **Test Set-up 2 for DL-MU MIMO Test**  Laptop EUT (4x4) Wi-Fi Wi-Fi 2x2 Wi-Fi 6 Client 1 Wi-Fi 2x2 Wi-Fi 6 Client 2
Test Procedure	1. Place the entire setup - EUT, licensed equipment/Wi-Fi6 clients in a controlled environment such as a RF tent.

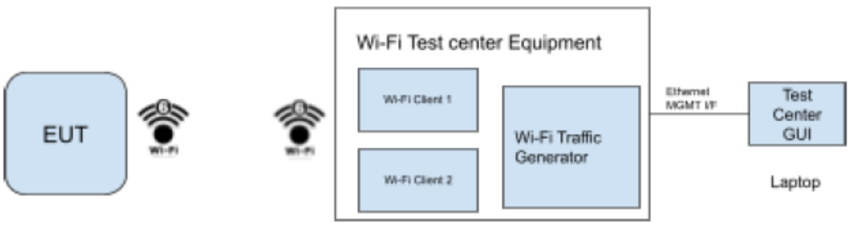
	2. Configure the EUT in 802.11 ax mode with DL-MU MIMO feature disabled. 3. Configure Test Equipment and simulate two 2x2 Wi-Fi 6 clients in 802.11ax mode with DL-MU MIMO feature disabled. 4. Connect simulated clients in a licensed equipment or Wi-Fi 6 Clients with EUT over wireless interface.Run ping between AP and Clients to verify connection. 5. Measure the data throughput using licensed equipment or open-source tools like 'iperf between AP and all the four connected clients simultaneously and note aggregate throughput'. 6. Now, configure the EUT in 802.11 ax mode with DL-MU MIMO feature enabled. 7. Configure Test Equipment and simulate two 2x2 Wi-Fi 6 clients in 802.11ax mode with DL-MU MIMO feature enabled. 8. Connect a licensed equipment or Wi-Fi 6 Clients with EUT over wireless interface.Run ping between AP and Client to verify connection. 9. Measure the data throughput using licensed equipment or open-source tools like 'iperf' between AP and all the connected clients simultaneously and note aggregate throughput. 10. Compare throughput measured in step 5 and step 9 to verify the gain of DL-MU MIMO feature. 11. Capture Packets in the Laptop using Wireshark application to verify preamble type HE_MU in the PPDU header
Test Limits	As per applicable Tables under Clause 3.5(iv) and 3.5(vi) b.

Expected Results	The results should be as per the specifications under Clause 3.5(iv) and 3.5(vi) b.

Test No.	GR_WiFiAP_008
Test Details	To check the functionality of UL-MU MIMO feature as per Clause no. 3.5(v) and 3.5(vi) c. EUT should have 4 or more spatial streams.
Test Instruments Required	● Equipment under test (EUT) ● Two 2x2 MIMO Wi-Fi 6 Clients with UL-MU MIMO Feature or Licensed Wi-Fi Test Center with UL- MU MIMO feature enabled ● Laptop with open source tools like iperf,ethereal,tcpdump or wireshark etc. ● Connecting cables.
Test Setup	**Test Setup-1 for UL-MU MIMO Test**  EUT Wi-Fi Wi-Fi Wi-Fi Test center Equipment Wi-Fi Client 1 with DL-MU MIMO Feature Wi-Fi Client 2 with DL-MU MIMO Feature Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop **Test Set-up 2 for UL-MU MIMO Test**  Laptop EUT (4x4) Wi-Fi Wi-Fi 2x2 Wi-Fi 6 Client 1 Wi-Fi 2x2 Wi-Fi 6 Client 2

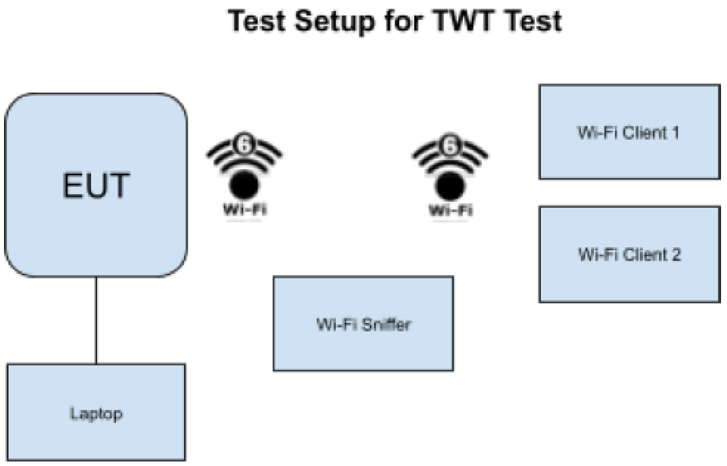
Test Procedure	1. Place the entire setup - EUT, licensed equipment/Wi-Fi6 clients in a controlled environment such as a RF tent. 2. Configure the EUT in 802.11 ax mode with UL-MU MIMO feature disabled. 3. Configure Test Equipment and simulate two 2x2 Wi-Fi 6 clients in 802.11ax mode with UL-MU MIMO feature disabled. 4. Connect simulated clients in a licensed equipment or Wi-Fi 6 Clients with EUT over wireless interface.Run ping between AP and Clients to verify connection. 5. Measure the data throughput using licensed equipment or open-source tools like 'iperf between AP and both the connected clients simultaneously and note aggregate throughput'. 6. Now, configure the EUT in 802.11 ax mode with UL-MU MIMO feature enabled. 7. Configure Test Equipment and simulate two 2x2 Wi-Fi 6 clients in 802.11ax mode with UL-MU MIMO feature enabled. 8. Connect a licensed equipment or Wi-Fi 6 Clients with EUT over wireless interface.Run ping between AP and Client to verify connection. 9. Measure the data throughput using licensed equipment or open-source tools like 'iperf' between AP and both the connected clients simultaneously

	and note aggregate throughput. 10. Compare throughput measured in step 5 and step 9 to verify the gain of UL-MU MIMO feature. 11. Capture Packets in the Laptop using Wireshark application to verify preamble type HE_TRIG in the PPDU header
Test Limits	As per applicable Tables under Clause 3.5(v) and 3.5(vi) c.
Expected Results	The results should be as per the specifications under Clause 3.5(v) and 3.5(vi) c.

Test No.	GR_WiFiAP_009
Test Details	To check the functionality of 20MHz only mode as per Clause no. 3.5(ix).
Test Instruments Required	● Equipment under test (EUT) ● Wi-Fi 6 Test Center Equipment ● Laptop with open source tools like iperf,ethereal,tcpdump or wireshark etc. ● Connecting cables.
Test Setup	**Test Setup for 20MHz only mode Test**  Wi-Fi Test center Equipment EUT Wi-Fi Wi-Fi Wi-Fi Client 1 Wi-Fi Client 2 Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop
Test Procedure	1. Place the entire setup - EUT, licensed equipment/Wi-

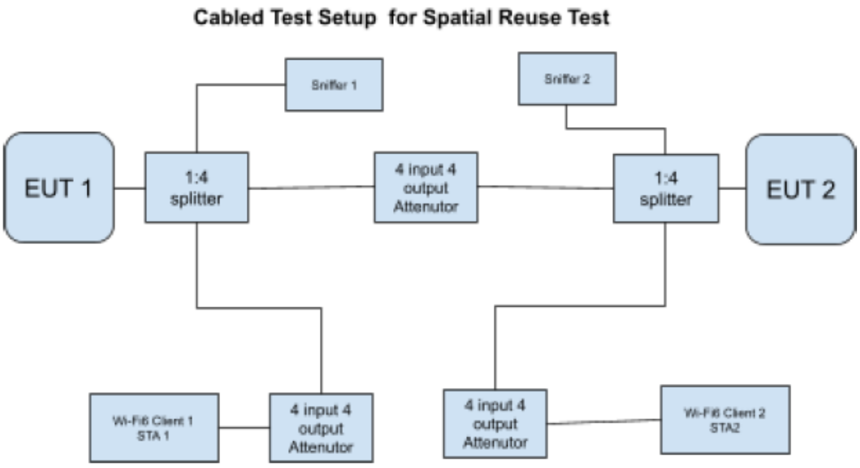
	Fi6 clients in a controlled environment such as a RF tent. 2. Configure the EUT in 802.11 ax mode in 40MHz or 80 MHz channel in 5GHz band. 3. Enable 20MHz mode in the Wi-Fi6 Test Equipment and simulate two clients or configure 20MHz bandwidth in Wi-Fi 6 clients.. 4. Connect simulated clients in a licensed equipment with EUT over wireless interface.Run ping between AP and Clients to verify connection.Note Association rate, it should be as per 20MHz mode only. 5. Measure the data throughput using licensed equipment or open-source tools like 'iperf between AP and both the connected clients simultaneously and note aggregate throughput'. 6. Capture Packets in the Laptop using Wireshark application to monitor Management frames in which simulated clients will inform EUT that they are operating in the 20MHz mode only.
Test Limits	As per applicable Tables under Annexure II f for 20 MHz.
Expected Results	The results should be as per the specifications under Annexure II f for 20 MHz.

Test No.	GR_WiFiAP_010
Test Details	To check the functionality of TWT(Target Wake Time) mode as per Clause no. 3.5(x).
Test Instruments Required	● Equipment under test (EUT) ● Licensed Wi-Fi 6 Test Center Equipment ● Laptop with open source tools like

	iperf,ethereal,tcpdump or wireshark etc. ● Connecting cables.
Test Setup	 Test Setup for TWT Test EUT Wi-Fi Wi-Fi Wi-Fi Client 1 Wi-Fi Client 2 Wi-Fi Sniffer Laptop
Test Procedure	1. Place the entire setup - EUT and Wi-Fi6 clients in a controlled environment such as a RF tent. 2. Configure the EUT in 802.11 ax mode in 20MHz and TWT feature. 3. Enable 20MHz mode in the Wi-Fi6 Test Equipment and simulate two clients with TWT feature. 4. Connect simulated clients in a licensed equipment with EUT over wireless interface.Run ping between AP and Clients to verify connection. 5. Capture Packets in the Laptop using Wireshark application or Wi-FI Sniffer to monitor frames for

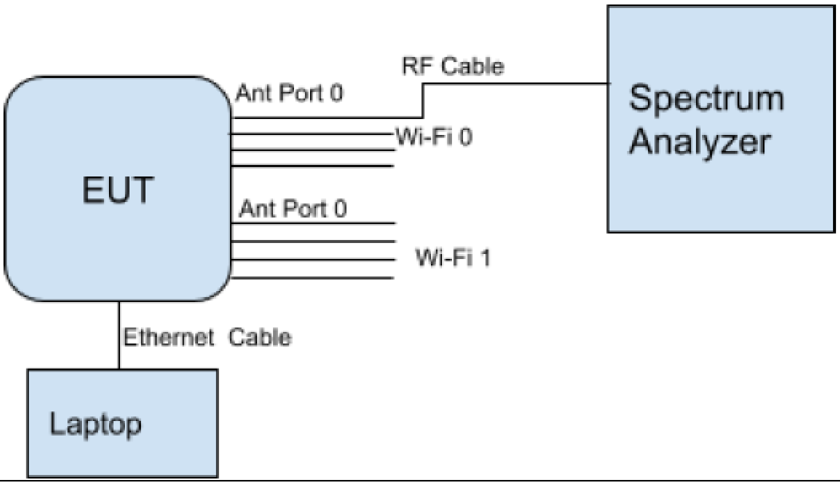
	TWT. a. Note Target wake up time, TWT Session interval in case of individual TWT agreement between EUT and STA. b. Note parameters for the TWT session, including the minimum TWT wake duration, TWT wake interval and TWT channel in the TWT Request message.
Test Limits	Noted values should be as per the configured values.
Expected Results	The results should be as per the configured values.

Test No.	GR_WiFiAP_011
Test Details	To check the functionality of Spatial Reuse as per Clause no. 3.5(xi).
Test Instruments Required	● Equipment under test (EUT) in AP mode : 2Nos. ● EUT in client mode or WI-Fi 6 clients : 2Nos. ● Power combiner or splitter : 1:4 ● 4:4 Programmable Variable attenuator: 3 Nos. ● Laptop with open source tools like iperf, ethereal, tcpdump or wireshark etc. ● Connecting RF and Ethernetcables.

Test Setup	 Cabled Test Setup for Spatial Reuse Test Sniffer 1 Sniffer 2 EUT 1 1:4 splitter 4 input 4 output Attenutor 1:4 splitter EUT 2 Wi-Fi6 Client 1 STA 1 4 input 4 output Attenutor 4 input 4 output Attenutor Wi-Fi6 Client 2 STA2
Test Procedure	1. Configure: a. EUT1 and EUT2 as 20MHz, 11axa, 1x1 at the same channel. b. Configure STA1 and let it associate to EUT1. c. Configure STA2 and let it associate to EUT2. 2. Adjust the attenuator between EUT1 and STA1 and check EUT1 and STA1 DL UDP throughput. The target RSSI is 40~50 and throughput is ~120 Mbps. Do not run throughput between EUT2 and STA2. 3. Adjust the attenuator between EUT2 and STA2 and check EUT2 and STA2 DL UDP throughput. The target RSSI is 40~50 and throughput is ~120 Mbps. Do not run throughput between EUT1 and STA1. 4. Run DL UDP throughput between EUT2 and STA2. Adjust the attenuator between EUT1 and EUT2 and check RSSI level on EUT1. This step checks the inter-BSS level. The target RSSI is 25~29. The EUT2 network both

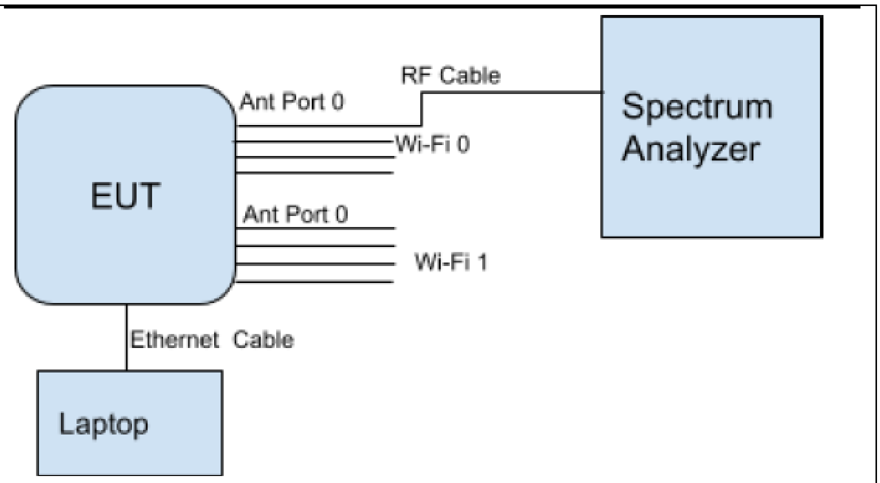
	and check the throughput difference between the spatial reuse on and off. 5. Run DL traffic on both networks, EUT1 and EUT2. 6. Enable the spatial reuse on EUT1 and set the threshold to 30 using the commands to check EUT1 DL UDP throughput. 7. Disable OBSS_PD and check EUT1 DL UDP throughput. If the throughput readings show no real difference, change the PPDU duration, AMPDU, and AMSDU on both EUT1 and EUT2. 8. Rerun the same test to check the gain between the spatial reuse on and off.
Test Limits	As per configured .
Expected Results	The results should be as per the configured values.

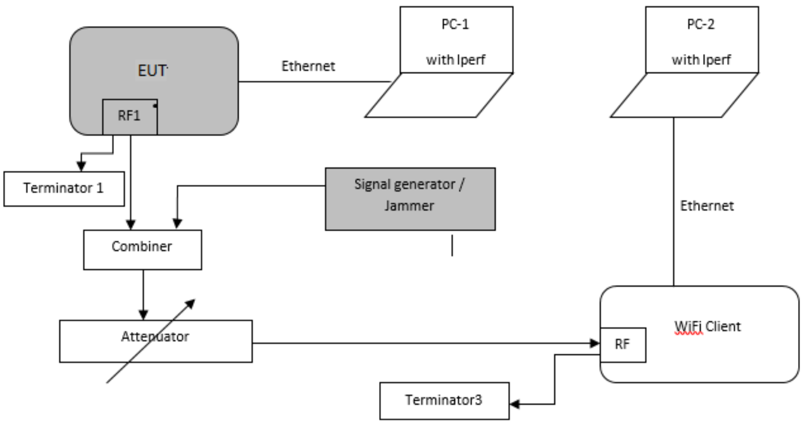
Test No.	GR_WiFiAP_012
Test Details	To check compliance for EIRP as per Clause 3.6.1.
Test Instruments Required	1. Equipment under test(EUT) 2. Spectrum Analyzer such as R&S Handheld (FSH06) 3. Power Adaptor 4. Connecting cables(RF cable and Ethernet Cable) 5. Laptop

Test Setup	
Test Procedure	1. Make the set up as shown in the test setup diagram and switch ON the EUT. 2. Connect the EUT output (wireless interface wlan0/1/2, port0/1) to the Spectrum Analyzer with a RF cable and if required use suitable Attenuator for safe operation of spectrum analyser 3. Configure the EUT as AP operating in one of the IEEE802.11 a/b/g/n/ac/ax modes with Tx Power set at maximum or at value which is required to meet EIRP limits with specified Antenna Gain. . 4. Follow the below steps to configure the Spectrum Analyzer for Band Power Test. a. Press Preset button on spectrum Analyser. b. Set Centre Frequency as per desired channel number, set in EUT configured for 2GHz or 5GHz wireless radio one at a time . c. Press Channel Power measurment button on spectrum analyser. d. Set channel BW as 20MHz in spectrum analyser for band power measurment of 20MHz channel BW selected in EUT. e. The spectrum analysr will automatically set the span and sweep time according to the channel

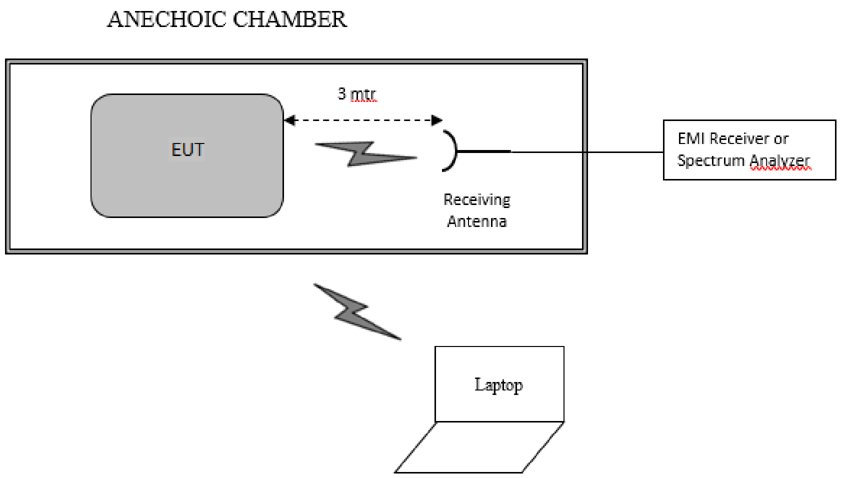
	BW selection. f. Adjust amplitude Reference Level of spectrum Analyser so that the signal spectrum is clearly visible on screen. g. Now in Trace Mode select clear option then press Max Hold option. h. Spectrum Analyzer will take few minutes to smooth the trace with minimal spikes 5. Note down the Band Power reading. 6. Now calculate the EIRP which will be the sum of conducted power and antenna gain. This should be less than the EIRP Limit (Max 4W). 7. Similarly for EUT band power measurement in 40MHz/80MHz/160MHz channel bandwidth, set channel bandwidth of Spectrum analyser to 40MHz/80MHz/160Mhz and take the measurement.
Test Limits	As per Clause 3.6.1.
Expected Results	The EIRP value should not exceed the limits as per Clause 3.6.1.

Test No.	GR_WiFiAP_013
Test Details	To check compliance for Peak Power Density as per Clause 3.6.2.
Test Instruments Required	1. Equipment under test 2. Laptop with open source tools like Inssider etc. OR Licensed tools. 3. Connecting cables. 4. Power Adaptor 5. Spectrum Analyzer

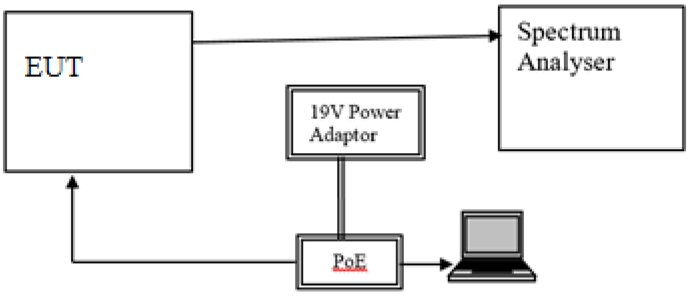
Test Setup	 RF Cable Ant Port 0 Wi-Fi 0 EUT Spectrum Analyzer Ant Port 0 Wi-Fi 1 Ethernet Cable Laptop
Test Procedure	1. Make the setup as shown above. 2. Configure the Spectrum Analyzer for a) Center Frequency of 2.412GHz, 2.437GHz or 2.462GHz b) SPAN of 40MHz c) RBW of 3KHz 3. Configure EUT in 802.11b for DSSS (channel 1, 6 or 11) one at a time 4. Connect a licensed equipment or a laptop 5. Measure peak power shown in Spectrum analyzer
Test Limits	As per Clause 3.6.2.
Expected Results	The limits for Power density shall not exceed the values prescribed under Clause 3.6.2.

Test No.	GR_WiFiAP_014
Test Details	To check compliance for Processing Gain as per Clause 3.6.3.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools. 3. Combiner 4. Attenuator 5. Signal Generator 6. Connecting cables.
Test Setup	 EUT RF1 Ethernet PC-1 with Iperf PC-2 with Iperf Terminator 1 Signal generator / Jammer Ethernet Combiner Attenuator WiFi Client RF Terminator3 Terminator:-50 Ω terminator for the unused antenna port of the radio card.
Test Procedure	1. Make the setup as shown above 2. Configure the EUT in IEEE 802.11b mode of operation. 3. Increase the jamming signal amplitude in pass band till BER/PER rates. 4. Find the jammer to signal ratio(J/S) 5. Calculate Processing Gain by Processing gain formula for DSSS-BPSK rates.
Test Limits	As per Clause 3.6.3.

Expected Results	The result for Processing Gain shall be as per Clause 3.6.3.

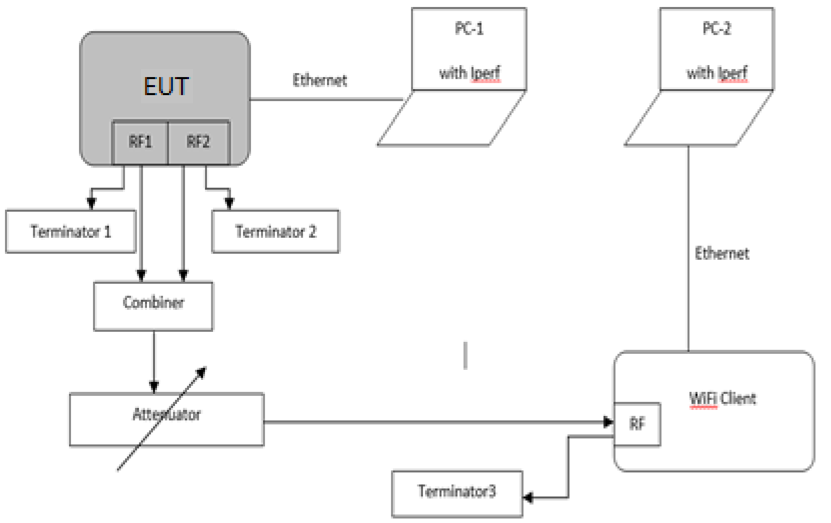
Test No.	GR_WiFiAP_015
Test Details	To check compliance for Field Strength as per Clause 3.6.4.
Test Instruments Required	1. Equipment under test(EUT) 2. Laptop with open source tools like Inssider etc. OR Licensed tool. 3. Spectrum Analyzer/EMI Receiver. 4. Connecting cables.
Test Setup	 ANECHOIC CHAMBER 3 mtr EUT Receiving Antenna EMI Receiver or Spectrum Analyzer Laptop
Test Procedure	1. Make the setup as shown above. 2. Configure the EUT for the desired mode of operation (802.11 a/b/g/n/ac/ax) 3. Connect a licensed equipment or a laptop 4. Observe on the Spectrum Analyzer or EMI Receiver the field strength of emissions.

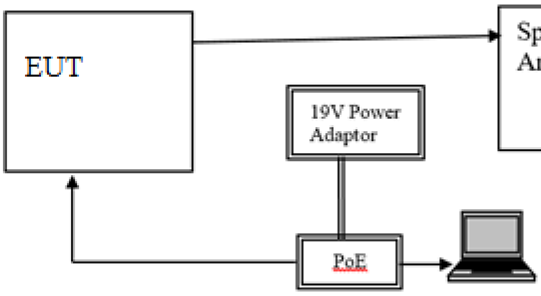
Test Limits	As per limits under Clause 3.6.4.
Expected Results	The limits of Field Strength should be as per the Clause 3.6.4.

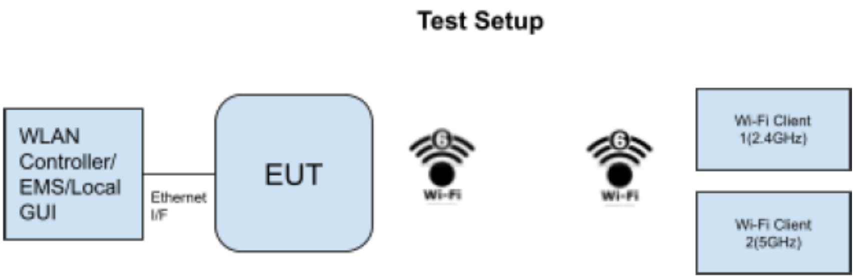
Test No.	GR_WiFiAP_016
Test Details	To check compliance for Transmitter Spurious Emissions as per Clause 3.6.5.
Test Instruments Required	1. Equipment under test 2. Laptop with open source tools like Inssider etc. OR Licensed tools etc. 3. Spectrum Analyzer. 4. Power Adaptor 5. Connecting cables.
Test Setup	
Test Procedure	1. Make the setup as shown above. 2. Configure the EUT for any one desired mode of operation (802.11 a/b/g/n/ac/ax)

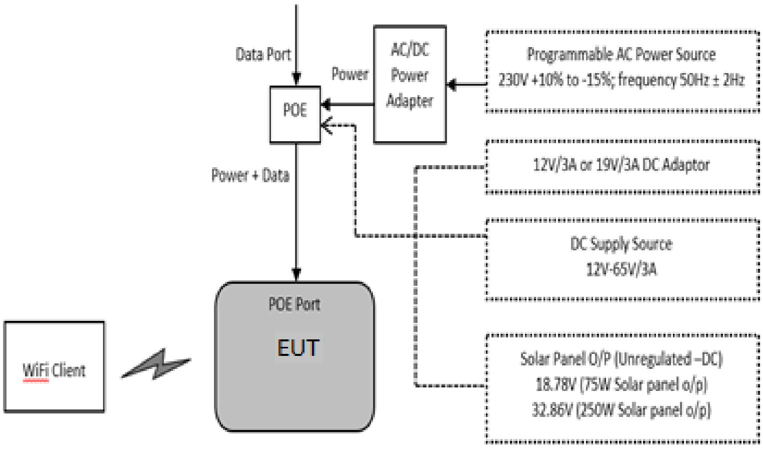
	3. Connect a licensed equipment or a laptop 4. Observe on the Spectrum Analyzer or EMI Receiver that the spurious emissions of the EUT
Test Limits	As per limits under Clause 3.6.5.
Expected Results	The limits of Transmitter Spurious Emissions should be as per the Clause 3.6.5.

Test No.	GR_WiFiAP_017
Test Details	To check compliance for Receiver Sensitivity as per Clause 3.7.1.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools. 3. Combiner 4. Attenuator 5. Signal Generator 6. Connecting cables.

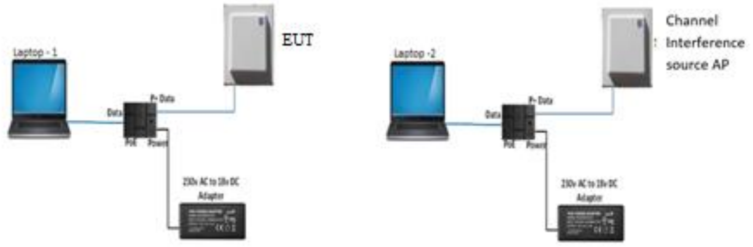
Test Setup	 EUT RF1 RF2 Ethernet PC-1 with Iperf PC-2 with Iperf Terminator 1 Terminator 2 Ethernet Combiner Attenuator WiFi Client RF Terminator3
Test Procedure	1. Configure the EUT for the desired mode of operation (802.11 a/b/g/n/ac/ax). 2. Connect a licensed equipment or IPerf tool using a RF cable and attenuator 3. Set the rejection level, RSSI at -3dB down point and find the channel capacity. 4. Set back the required RSSI as per table, Measure the receiver sensitivity by running the IPerf with found channel capacity data rate. 5. Verify data transfer between EUT and connected equipment within 10% PER.
Test Limits	As per limits under Clause 3.7.1.
Expected Results	The limits of Receiver Sensitivity should be as per the Clause 3.7.1.

Test No.	GR_WiFiAP_018
Test Details	To check compliance for Receiver Spurious Emissions as per Clause 3.7.2.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Spectrum Analyzer 4. Power Adaptor 5. Connecting cables.
Test Setup	
Test Procedure	1. Make the setup as shown above 2. Configure the EUT for any desired mode of operation (802.11 a/b/g/n/ac/ax) 3. Connect a licensed equipment or a laptop 4. Observe on the Spectrum Analyzer or EMI Receiver the spurious emissions of the EUT.
Test Limits	As per Clause 3.7.2.
Expected Results	The limits of Receiver Spurious Emissions should be as per the Clause 3.7.2.

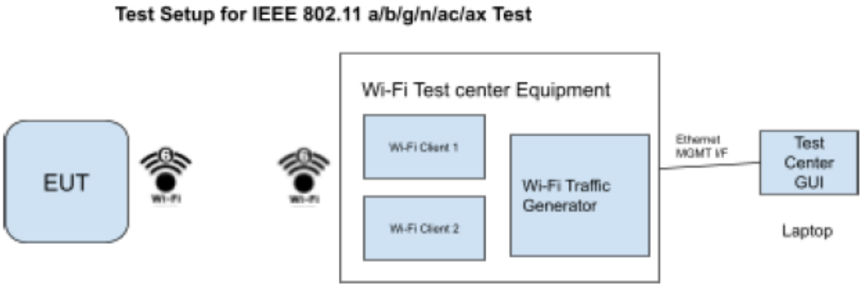
Test No.	GR_WiFiAP_019
Test Details	To check compliance as per Clause 3.10.
Test Instruments Required	1. Equipment under test 2. Laptop with EMS setup. 3. WLAN Controller.
Test Setup	 Test Setup WLAN Controller/ EMS/Local GUI Ethernet I/F EUT Wi-Fi Wi-Fi Wi-Fi Client 1(2.4GHz) Wi-Fi Client 2(5GHz)
Test Procedure	1. Check the link connectivity between EUT & EMS 2. Check EMS/WLAN controller displays specified visual indications for the configured EUT i) Activity over Radio ii) Activity over the Ethernet iii) Operating / Faulty State iv) Power Indicator
Test Limits	As per Clause 3.10.
Expected Results	The visual indications should be as per Clause 3.10.

Test No.	GR_WiFiAP_020
Test Details	To check compliance for Power Supply Requirements as per Clause 3.11.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Power Adaptor 4. AC/DC/Solar Power supply 5. Connecting cables.
Test Setup	 Data Port Power AC/DC Power Adapter Programmable AC Power Source 230V +10% to -15%; frequency 50Hz ± 2Hz POE 12V/3A or 19V/3A DC Adaptor Power + Data DC Supply Source 12V-65V/3A POE Port EUT WiFi Client Solar Panel O/P (Unregulated –DC) 18.78V (75W Solar panel o/p) 32.86V (250W Solar panel o/p)
Test Procedure	1. Connect a AC power supply of 230 V + 10% to -15% and frequency 50 Hz ± 2 Hz . 2. Verify the EUT is powered on. 3. Connect a licensed equipment/laptop in client mode. 4. Verify that the client is connected successfully. 5. Check that no Fault alarm or indication is given by the EUT. 6. Change the source of power supply to DCand repeat steps 2 to 5. 7. Change the source of power supply to Solar Power/adaptor and repeat steps 2 to 5.

Test Limits	As per Clause 3.11.
Expected Results	The EUT should be able to operate under the different Power Supply Requirements as per Clause 3.11.

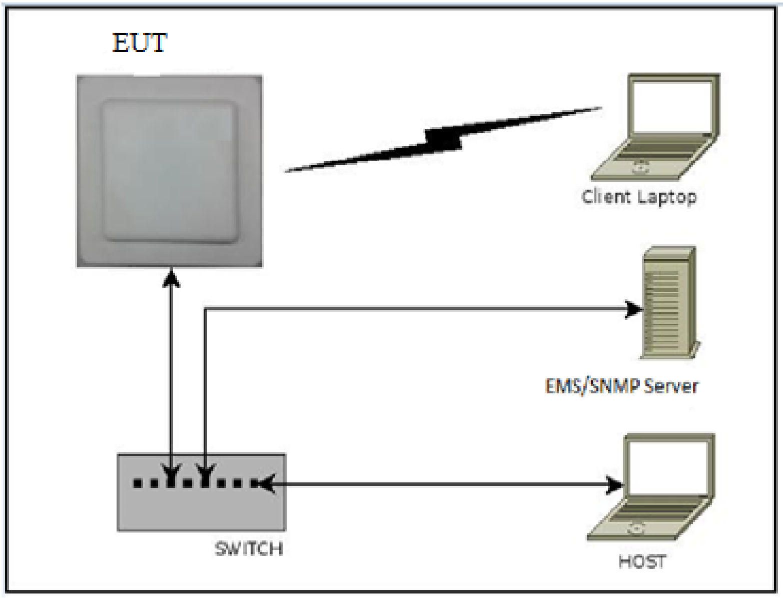
Test No.	GR_WiFiAP_021
Test Details	To check compliance for Interference Detection and Avoidance as per Clause 3.12.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Power Adaptor 4. Connecting cables.
Test Setup	 Laptop - 1 Data P+ Data PoE Power EUT 230v AC to 18v DC Adaptor Laptop -2 Data P+ Data PoE Power Channel Interference source AP 230v AC to 18v DC Adaptor
Test Procedure	1. Place the entire setup - EUT, other active Interference generator, - in a controlled environment such as a RF tent. 2. Configure the EUT in an interference free channel. 3. Verify using open source tool like Inssider that EUT is operating in the configured channel 4. Now, introduce interference on the channel in which

	EUT is configured by other interference source 5. Verify using an open source tool like Inssider that the EUT is switching to a clean channel 6. Verify step 4&5 for other possible scenarios of interference.
Test Limits	As per Clause 3.12.
Expected Results	The EUT should be able to operate as per the requirements of Clause 3.12.

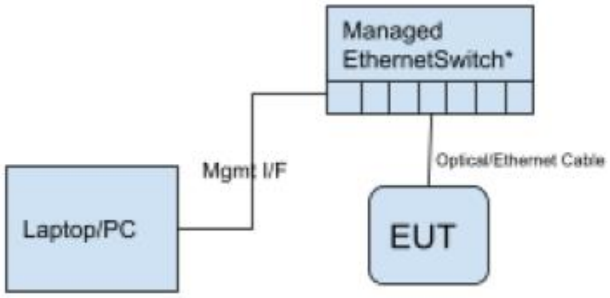
Test No.	GR_WiFiAP_022
Test Details	To check compliance for Radio interface requirements as per Clause 4.3.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tool 3. Connecting cables.
Test Setup	 Test Setup for IEEE 802.11 a/b/g/n/ac/ax Test Wi-Fi Test center Equipment EUT Wi-Fi Wi-Fi Wi-Fi Client 1 Wi-Fi Client 2 Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop
Test Procedure	1. Configure the EUT for the desired mode of operation

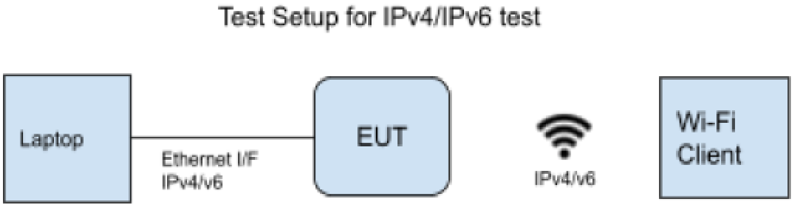
	(802.11 a/b/g/n/ac/ax) one at a time 2. Configure the EUT for the desired bit rate as per the different IEEE 802.11 a/b/g/n/ac/ax one at a time. 3. Connect a licensed equipment or a laptop. 4. Ping between the laptop/equipment to the EUT 5. Verify using open source tools like Inssider, laptop or licensed equipment that the EUT is associating at the desired bitrates.
Test Limits	As per Clause 4.3
Expected Results	The EUT should adhere to at least one or more than one of the following protocols: IEEE 802.11a/b/g/n/ac/ax protocols

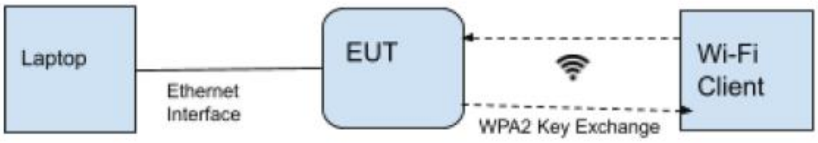
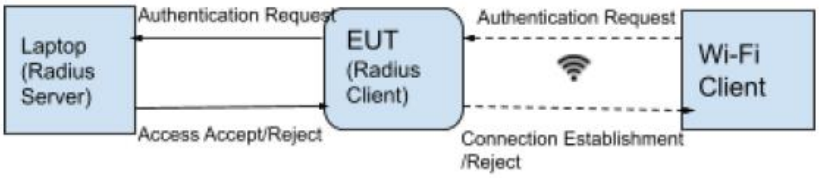
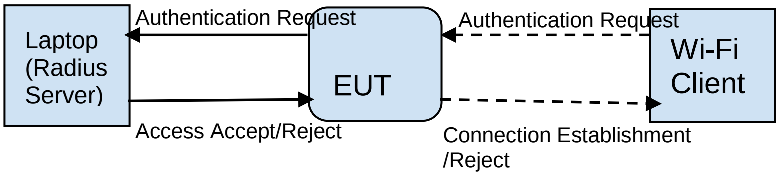
Test No.	GR_WiFiAP_023
Test Details	To check compliance for management protocols as per Clause 4.4.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Switch. 4. Connecting cables.

Test Setup	
Test Procedure	1. Configure EMS IP in EUT & enable SNMP 2. Ensure that the IP of EMS/NMS is reachable from EUT 3. Configure EUT for SSID, Mode, Channel, Tx power, etc from EMS 4. Verify/Modify for the configured parameters. (or Verify with SNMPWALK/GET/SET commands if EMS not available)
Test Limits	As per Clause 4.4
Expected Results	The EUT should support the management protocols as per Clause 4.4.

Test No.	GR_WiFiAP_024

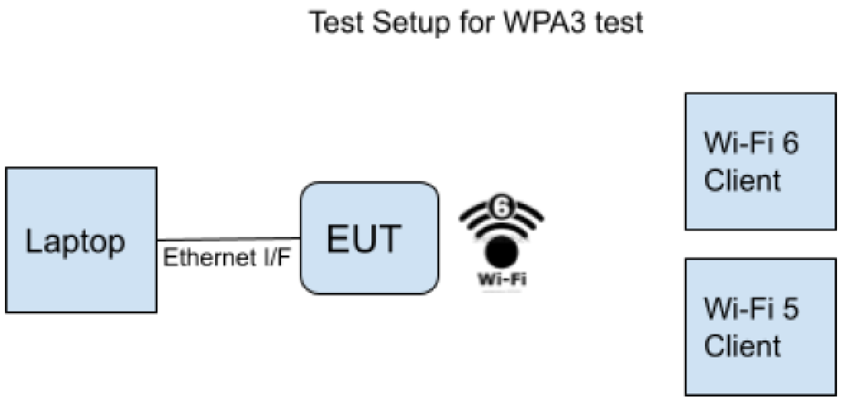
Test Details	To check compliance for Interfaces and Interface Ports requirements as per Clause 4.5 and 4.6.
Test Instruments Required	1. Equipment under test 2. Laptop with open source tools like Inssider etc. OR Licensed tools etc. 3. Managed Ethernet switch. 4. Connecting cables.
Test Setup	Test Setup for Ethernet/Optical Interface test  Managed EthernetSwitch* Mgmt I/F Optical/Ethernet Cable Laptop/PC EUT *Use Managed optical port switch and SFP cable for Optical Interface Test
Test Procedure	1. Connect the EUT to 10/100/1000/2500/10000 Mbps managed Ethernet switch or 1000 Mbps optical port one at a time. 2. Configure the speed of the port to 10 or 100 or 1000 or 2500 Mbps or 10000 Mbps on Ethernet switch or 1000/2500/10000Mbps optical port, one at a time 3. Observe in the EUT that the link has come up in the respective speed. 4. Perform Ping test.
Test Limits	As per Clause 4.5 and 4.6
Expected Results	The link should have come up in the respective speed 10/100/1000/2500/10000 Mbps electrical or 1000/2500/10000 Mbps optical

Test No.	GR_WiFiAP_025
Test Details	To check compliance for IPv4 and IPv6 addressing requirements as per Clause 4.7.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Connecting cables.
Test Setup	 Test Setup for IPv4/IPv6 test Laptop Ethernet I/F IPv4/v6 EUT IPv4/v6 Wi-Fi Client
Test Procedure	1. Configure EUT with IPv4 and IPv6 addresses. 2. Configure laptop to have IPv4 and IPv6 addresses. 3. Ping both IPv4 and IPv6 address between the EUT and the equipment/laptop.
Test Limits	Compliance for IPv4 and IPv6 addressing requirements as per Clause 4.7.
Expected Results	The ping operation should be successful for both IPv4 and IPv6 addressing schemes.

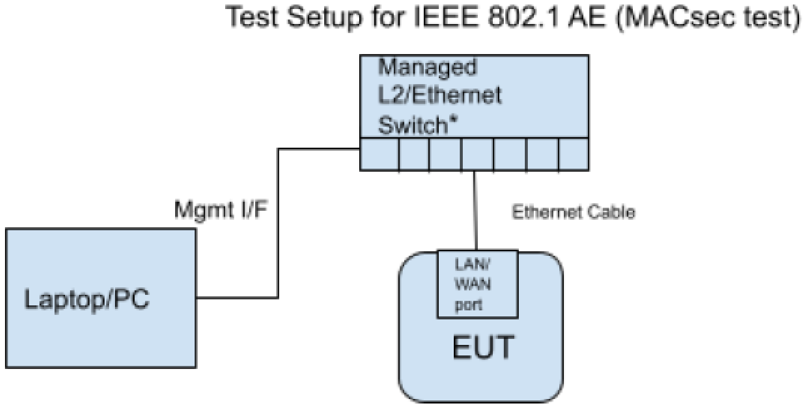
Test No.	GR_WiFiAP_026
Test Details	To check compliance for Security Requirements as per Clause 8.1.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Wireless clients which support WPA2/WPA3/802.1x 4. Connecting cables.
Test Setup	Test Setup for WPA2 test  Laptop Ethernet Interface EUT WPA2 Key Exchange Wi-Fi Client Test Setup for IEEE802.1x Security test  Laptop (Radius Server) Authentication Request Access Accept/Reject EUT (Radius Client) Authentication Request Connection Establishment /Reject Wi-Fi Client Test Setup for IEEE802.1x Security test  Laptop (Radius Server) Authentication Request Access Accept/Reject EUT Authentication Request Connection Establishment /Reject Wi-Fi Client
Test Procedure	1. Configure the EUT to have WPA2 (802.11i) and 2. 802.1X/EAP authentication mechanism one at a time 3. Configure a licensed equipment/laptop as a client to connect to EUT using the shared passphrase or EAP. 4. Observe using tools like ethereal, tcpdump or wireshark that the WPA2/802.1X messages are exchanged.

	5. Observe that the client is connected successfully.
Test Limits	Compliance for Security Requirements as per Clause 8.1
Expected Results	The WPA2/802.1X messages should be exchanged between the EUT and client.

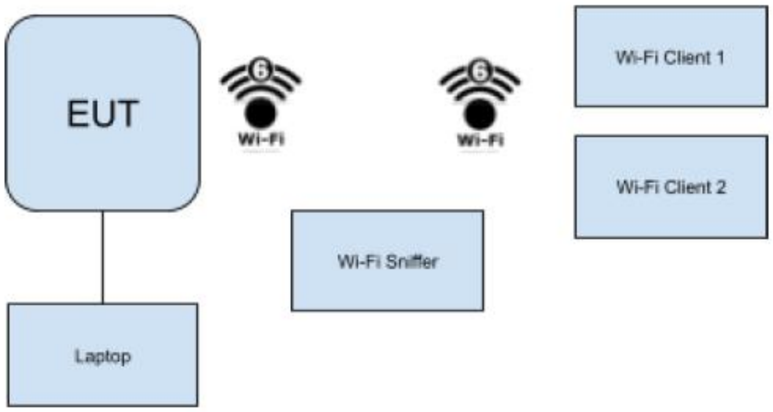
Test No.	GR_WiFiAP_027
Test Details	To check compliance for WPA3 Security Requirements as per Clause 8.1.Three tests are conducted for WPA3 capabilities. 1.WPA3-SAE 2.WPA3PSK2+SAE 3.WPA3 OWE
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Wireless clients which support WPA2/WPA3/802.1x 4. Connecting cables.

Test Setup	 Test Setup for WPA3 test Laptop Ethernet I/F EUT Wi-Fi Wi-Fi 6 Client Wi-Fi 5 Client
Test Procedure	1. Configure the EUT to have WPA3-SAE, WPA3-PSK2+SAE and WPA3-OWE security mechanism one at a time 2. Configure a licensed equipment/laptop as a client to connect to EUT using the shared passphrase. 3. Observe using tools like ethereal, tcpdump or wireshark that the WPA3 messages are exchanged. 4. Observe that the client is connected successfully.
Test Limits	compliance for WPA3 Security Requirements as per Clause 8.1.
Expected Results	The WPA3 messages should be exchanged between the EUT and client.

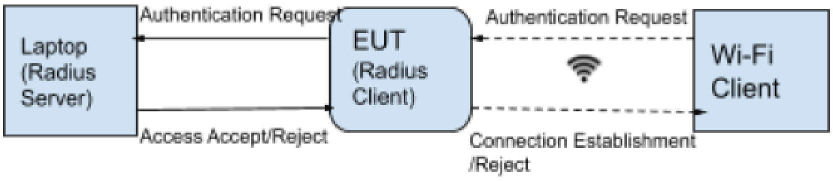
Test No.	GR_WiFiAP_028
Test Details	To check compliance for Mac Security IEEE802.1AE Requirements as per Clause 8.2.
Test Instruments Required	1. Equipment under test 2. Laptop.

	3. Managed L2/Ethernet switch with MACsec support 4. Connecting cables.
Test Setup	 Test Setup for IEEE 802.1 AE (MACsec test) Managed L2/Ethernet Switch* Mgmt I/F Ethernet Cable Laptop/PC LAN/ WAN port EUT
Test Procedure	1. Power on EUT and configure one of the Ethernet interfaces with MACsec. 2. Configure one of the LAN ports of L1 switch with MACsec and connect this port to the configured LAN port of the EUT. 3. Run ping test between L2 switch and EUT to verify connection with MACsec.
Test Limits	Compliance for Mac Security IEEE802.1AE Requirements as per Clause 8.2
Expected Results	The ping operation should be successful.

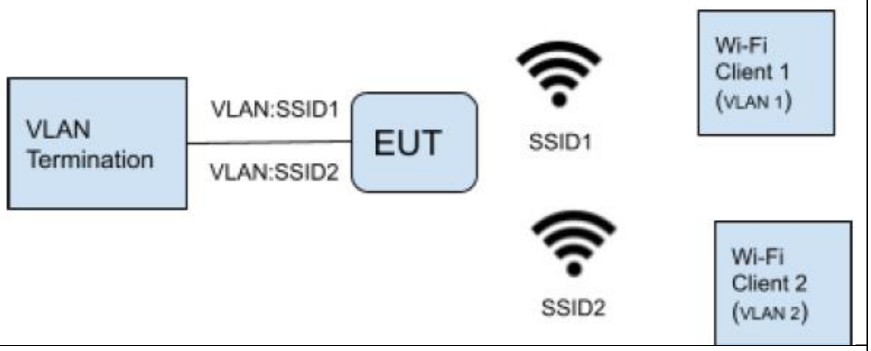
Test No.	GR_WiFiAP_029
Test Details	To check compliance for SSID requirements as per Clause 8.3.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Wi-Fi Client or Wi-Fi Sniffer 4. Connecting cables.

Test Setup	 EUT Wi-Fi Wi-Fi Wi-Fi Client 1 Wi-Fi Client 2 Wi-Fi Sniffer Laptop
Test Procedure	1. Login with Administrator Credentials to manage the EUT. 2. Configure the SSID of the EUT 3. Verify using standard open source tools like Inssider or licensed equipment that the configure SSID is visible 4. Verify the connectivity from Wi-Fi client.
Test Limits	compliance for SSID requirements as per Clause 8.3
Expected Results	The SSID should be definable by the administrator.

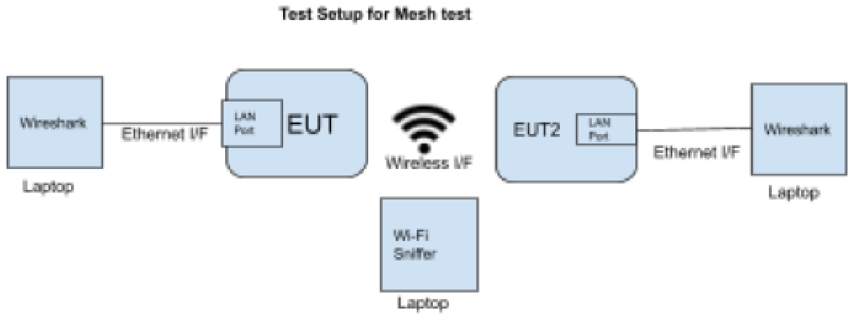
Test No.	GR_WiFiAP_030
Test Details	To check compliance for Security Requirements as per Clause 8.4.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	Test Setup for IEEE802.1x Security test  Laptop (Radius Server) Authentication Request Access Accept/Reject EUT (Radius Client) Authentication Request Connection Establishment /Reject Wi-Fi Client
Test Procedure	1. Configure EUT with 802.1X 2. Configure a standard licensed equipment/laptop as a client to connect to EUT 3. Observe using standard tools like ethereal/Wireshark/tcpdump that the RADIUS messages are exchanged between EUT and Radius Server 4. Observe that the client is connected successfully
Test Limits	compliance for Security Requirements as per Clause 8.4
Expected Results	The RADIUS AAA messages should be exchanged between EUT and AAA Server.

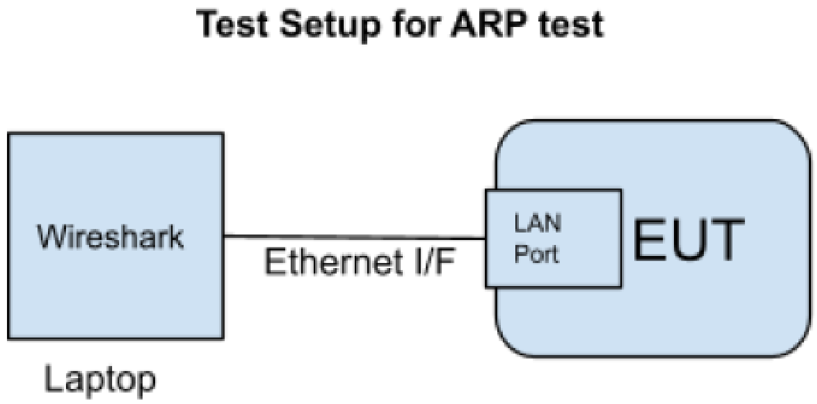
Test No.	GR_WiFiAP_031
Test Details	To check compliance for IEEEE 802.1q VLAN Tagging requirements as per Clause 10.1 i).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	Test Setup for IEEE802.1q VLAN Tagging test  VLAN Termination VLAN:SSID1 VLAN:SSID2 EUT SSID1 SSID2 Wi-Fi Client 1 (VLAN 1) Wi-Fi Client 2 (VLAN 2)
Test Procedure	1. Configure EUT with two (or more) SSIDs each in separate VLAN 2. Configure licensed equipment /laptop to connect as client to each SSID 3. Configure licensed equipment like Spirent Test Centre/standard Linux box for terminating the VLANs and initiate data transfer from the clients 4. Verify at licensed equipment like Spirent Test Centre/standard Linux box (using tools like Wireshark) that the packets from the clients are VLAN tagged.
Test Limits	compliance for IEEEE 802.1q VLAN Tagging requirements as per Clause 10.1 i).
Expected Results	The EUT should support the IEEE 802.1q VLAN Tagging functionality.

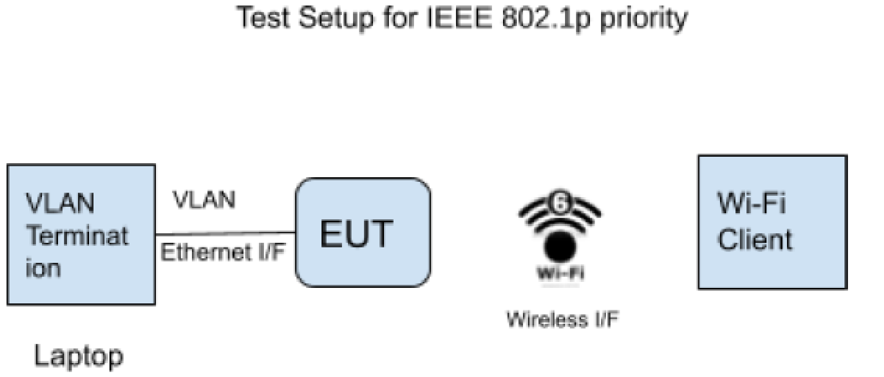
Test No.	GR_WiFiAP_032
Test Details	To check compliance for Mesh (802.11s) and repeater modes of operation requirements as per Clause 10.1 ii).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	 Test Setup for Mesh test Wireshark Laptop Ethernet I/F LAN Port EUT Wireless I/F Wi-Fi Sniffer Laptop EUT2 LAN Port Ethernet I/F Wireshark Laptop
Test Procedure	1. Configure EUT in MESH mode of operation 2. Configure a licensed equipment or another EUT in MESH mode 3. Ping between the two devices 4. Verify using a standard laptop (with tools like Wireshark) that the Mesh Frames are exchanged.
Test Limits	compliance for Mesh (802.11s) and repeater modes of operation requirements as per Clause 10.1 ii).
Expected Results	The EUT should support the Mesh (802.11s) and repeater modes of operation.

Test No.	GR_WiFiAP_033
Test Details	To check compliance for ARP (IETF RFC 826) as per Clause 10.1 iii).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	 Test Setup for ARP test Wireshark Laptop Ethernet I/F LAN Port EUT
Test Procedure	1. Connect the Ethernet interface of EUT to a licensed equipment /laptop 2. Configure the IP addresses of EUT and standard equipment so that both devices are in the same subnet 3. Ping from EUT to laptop/licensed equipment 4. Verify on the laptop (with tools like Wireshark) or on the licensed equipment that the ARP packets are exchanged
Test Limits	compliance for ARP (IETF RFC 826) as per Clause 10.1 iii).
Expected Results	The EUT should comply to requirements of ARP (IETF RFC 826) as per Clause 10.1 iii).

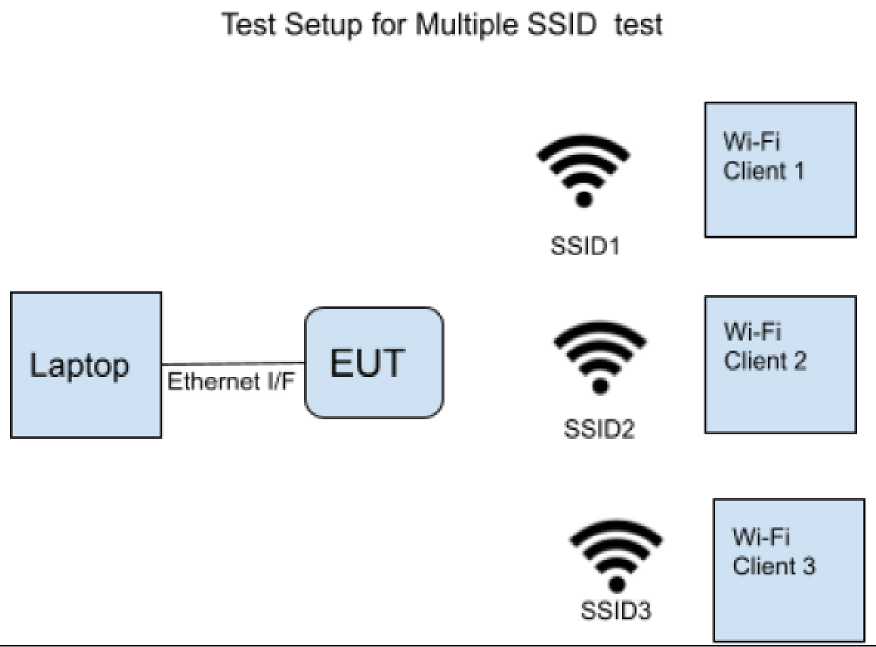
Test No.	GR_WiFiAP_034
Test Details	To check compliance for IEEE 802.1p priority requirements as per Clause 10.1 iv).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	Test Setup for IEEE 802.1p priority  VLAN Terminat ion VLAN Ethernet I/F EUT Wi-Fi Wireless I/F Wi-Fi Client Laptop
Test Procedure	1. Configure EUT for 802.1q VLAN. 2. Connect licensed equipment/laptop to EUT on WiFi. 3. Connect Ethernet port of EUT to Linux box/licensed equipment configured in the same VLAN. 4. Ping between equipment connected on WiFi to equipment connected on Ethernet interface of EUT. 5. On the equipment connected to Ethernet interface of EUT, capture packets using tools like wireshark and check for 802.1p header in Ethernet frame.
Test Limits	compliance for IEEE 802.1p priority requirements as per Clause 10.1 iv).
Expected Results	The EUT should satisfy the IEEE 802.1p priority requirements as per Clause 10.1 iv).

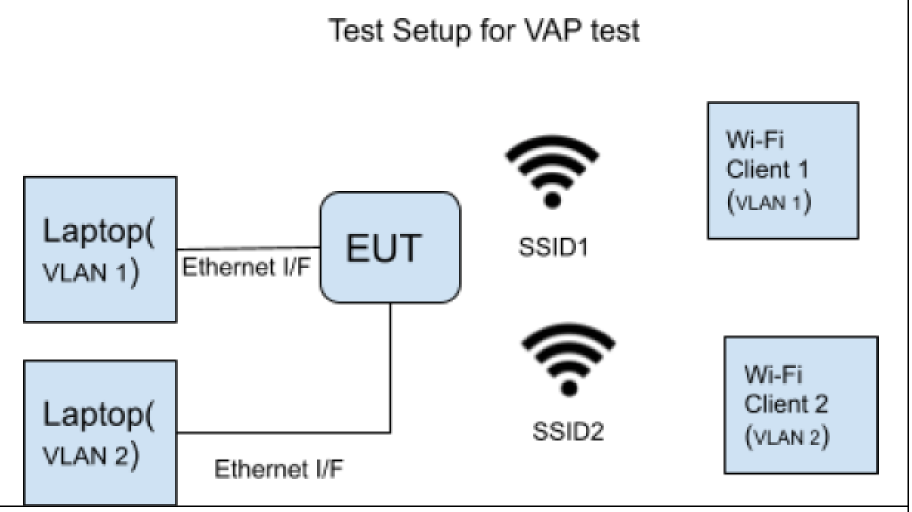
Test No.	GR_WiFiAP_035
Test Details	To check compliance for Spectrum sensing and reporting capability requirements as per Clause 10.1 v).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	NA
Test Procedure	1. Configure EUT to sense the spectrum. 2. Spectrum data (like channel number, power sensed on each channel) shall be captured and displayed locally or reported to remote monitoring unit like EMS
Test Limits	compliance for Spectrum sensing and reporting capability requirements as per Clause 10.1 v).
Expected Results	The EUT should support Spectrum sensing and reporting capability.

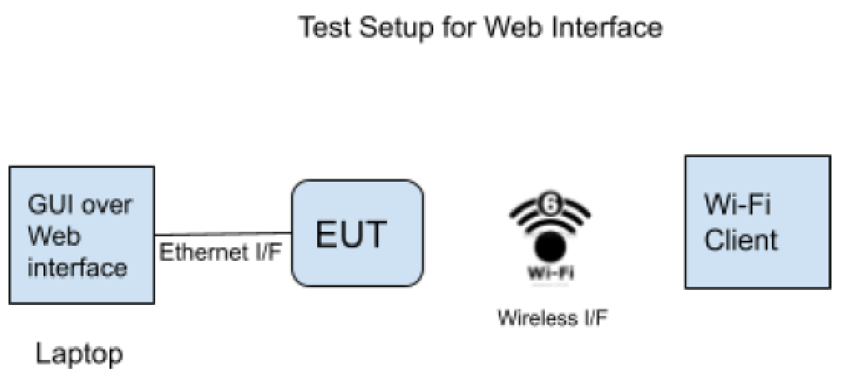
Test No.	GR_WiFiAP_036
Test Details	To check compliance for Multiple SSID support for operator sharing requirements as per Clause 10.1 vi).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	 Test Setup for Multiple SSID test Laptop Ethernet I/F EUT SSID1 SSID2 SSID3 Wi-Fi Client 1 Wi-Fi Client 2 Wi-Fi Client 3
Test Procedure	1. Configure EUT's each radio card with a distinct SSID 2. Configure licensed equipment/laptop to connect to each SSID one at a time 3. Verify that the client is connected successfully
Test Limits	compliance for Multiple SSID support for operator sharing requirements as per Clause 10.1 vi).
Expected Results	The EUT should support Multiple SSID support for operator sharing.

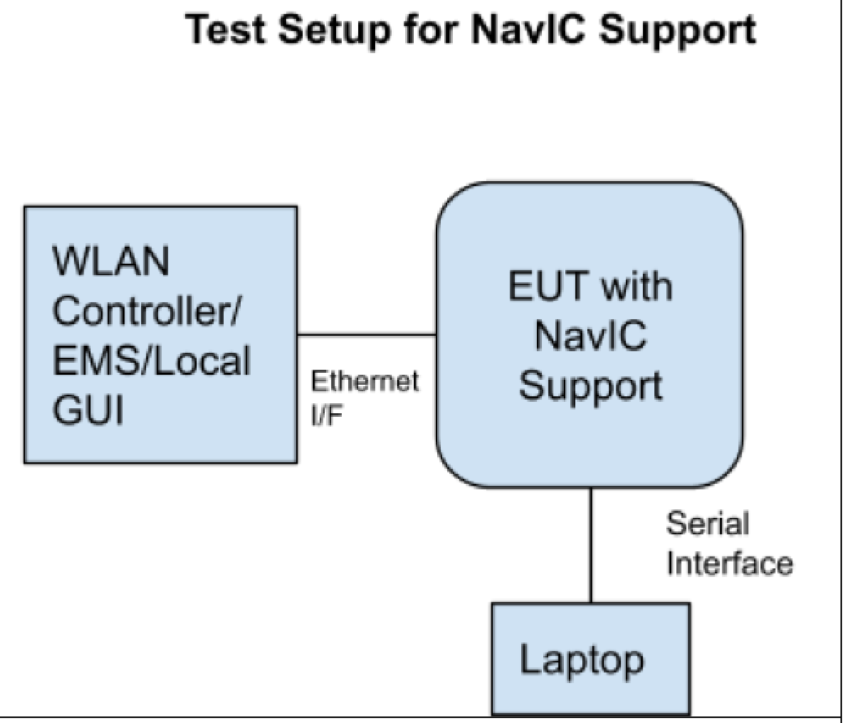
Test No.	GR_WiFiAP_037
Test Details	To check compliance for Support for VAP (Virtual Access Point) requirements as per Clause 10.1 vii).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	 Test Setup for VAP test Laptop(VLAN 1) Ethernet I/F EUT SSID1 Wi-Fi Client 1 (VLAN 1) Laptop(VLAN 2) Ethernet I/F SSID2 Wi-Fi Client 2 (VLAN 2)
Test Procedure	1. Configure EUT with multiple SSID on a single radio card 2. Configure licensed equipment/laptop to connect to each SSID one at a time 3. Verify that the client is connected successfully
Test Limits	NA
Expected Results	The EUT should support for VAP (Virtual Access Point) requirements as per Clause 10.1 vii).

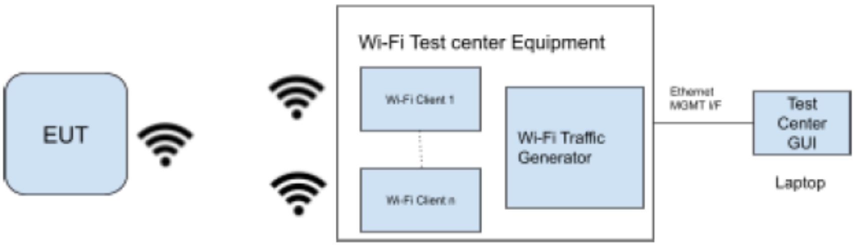
Test No.	GR_WiFiAP_038
Test Details	To check compliance for Configuration of parameters through web interface when link to EMS is not available requirements as per Clause 10.1 viii).
Test Instruments Required	1. Equipment under testEM 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	 Test Setup for Web Interface GUI over Web interface Laptop Ethernet I/F EUT Wi-Fi Wireless I/F Wi-Fi Client
Test Procedure	1. Connect a laptop to the EUT and access its web interface through http. 2. Change any of the parameters like SSID or channel number. 3. Verify that the change is successful (using open source tools such as Inssider)
Test Limits	compliance for Configuration of parameters through web interface when link to EMS is not available requirements as per Clause 10.1 viii).
Expected Results	The EUT should support configuration of parameters through a web interface when a link to EMS is not available.

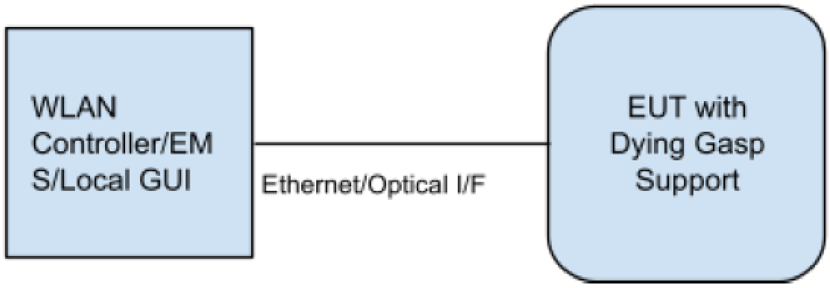
Test No.	GR_WiFiAP_039
Test Details	To check compliance for NAVIC Support Requirements as per Clause 10.1(ix).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	 Test Setup for NavIC Support WLAN Controller/ EMS/Local GUI Ethernet I/F EUT with NavIC Support Serial Interface Laptop
Test Procedure	1. Power On EUT and make connection with Laptop over serial interface/WLC/EMS over Ethernet interface. 2. Enable GPS support in EUT if required. 3. Check GPS data/coordinates in the Serial Prompt/Local GUI/WLC/EMS.
Test Limits	Compliance for NAVIC Support Requirements as per Clause 10.1(ix).
Expected Results	The EUT should have NavIC support.

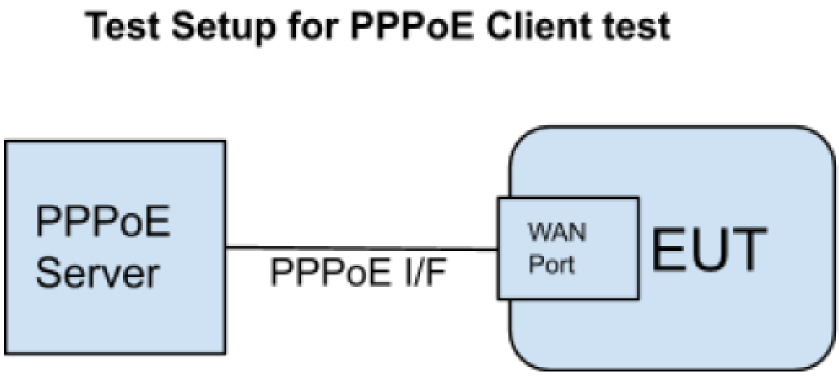
Test No.	GR_WiFiAP_040
Test Details	To check compliance for Concurrent clients per Radio Requirements as per Clause 10.1(x).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed Wi-Fi Test Centre.

	3. Connecting cables.
Test Setup	Test Setup for Concurrent Clients Test  EUT Wi-Fi Test center Equipment Wi-Fi Client 1 Wi-Fi Client n Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop
Test Procedure	1. Enable and configure one radio in the EUT with one of the IEEE 802.11 n/ac/ax modes. Other radios should be disabled. 2. Configure multiple Wi-Fi clients in the Wi-Fi Test Center equipment and connect with EUT. 3. Perform ping test between EUT and Wi-Fi clients to verify connection 4. Perform throughput test to check the EUT performance for concurrent clients.
Test Limits	EUT should have concurrent wifi connections with clients as per the maximum supported wi-fi clients in the data sheet.
Expected Results	Multiple Wi-Fi clients should have stable connection with EUT.

Test No.	GR_WiFiAP_041
Test Details	To check compliance for Dying gasp as per Clause 10.1(xi).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Iperf etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	**Test Setup for Dying gasp Support**  WLAN Controller/EMS/Local GUI Ethernet/Optical I/F EUT with Dying Gasp Support
Test Procedure	1. Power on EUT and establish connection with WLAN Controller/EMS/Local GUI. 2. Remove power cable or switch off EUT. 3. Verify message received at EMS/Wireless Controller from EUT about power off activity. If the dying gasp feature is enabled, then EUT will send a message to EMS/Wireless controller as soon as it switches off.
Test Limits	Power off message should be received by EMS/Wireless controller as soon as EUT switches off or within specified reporting time.
Expected Results	Power off message should be received by EMS/Wireless controller from EUT.

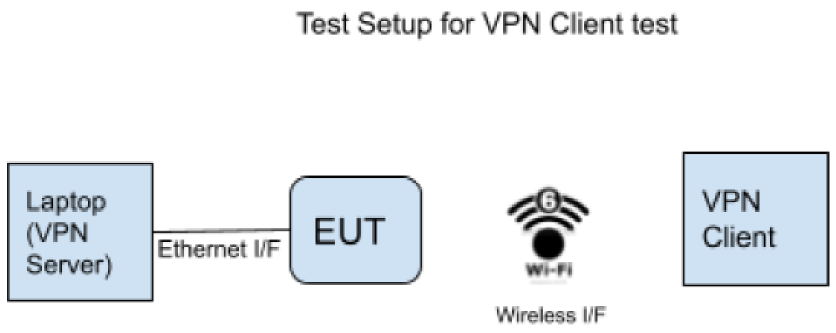
Test No.	GR_WiFiAP_042
Test Details	To check compliance for PPPoE for WAN port requirements as per Clause 10.2 ii).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	 Test Setup for PPPoE Client test PPPoE Server PPPoE I/F WAN Port EUT
Test Procedure	1. Connect WAN port of EUT to a PPPoE server 2. Authenticate EUT with PPPoE server with required credentials 3. Verify that PPPoE server is providing IP address, gateway, DNS etc to the WAN port of EUT after authentication.
Test Limits	compliance for PPPoE for WAN port requirements as per Clause 10.2 ii).
Expected Results	The EUT should support PPPoE for WAN port requirements as per Clause 10.2 ii).

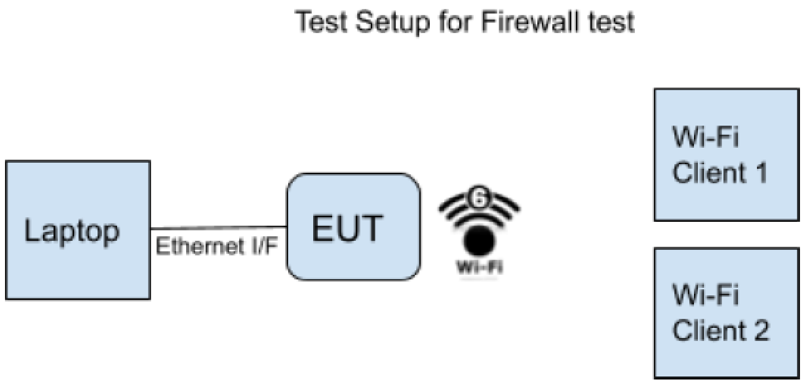
Test No.	GR_WiFiAP_043
Test Details	To check compliance for DHCP Server, client (optional), relay (RFC2131, 951 and 3046) requirements as per Clause 10.2 iii).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	NA
Test Procedure	A. DHCP Server 1. Run DHCP server on EUT 2. Connect clients to EUT 3. Verify using standard network protocol analyzer tool that clients are getting IP from DHCP range defined in EUT B. DHCP Relay 1. Configure EUT as DHCP relay 2. Run DHCP server on standard equipment connected to the LAN of EUT 3. Connect Wi-Fi clients to EUT 4. Observe using standard network protocol analyzer tool that clients are getting IP from DHCP range defined in EUT
Test Limits	compliance for DHCP Server, client (optional), relay (RFC2131, 951 and 3046) requirements as per Clause 10.2 iii).
Expected Results	The EUT should support the DHCP related functionalities as per Clause 10.2 iii).

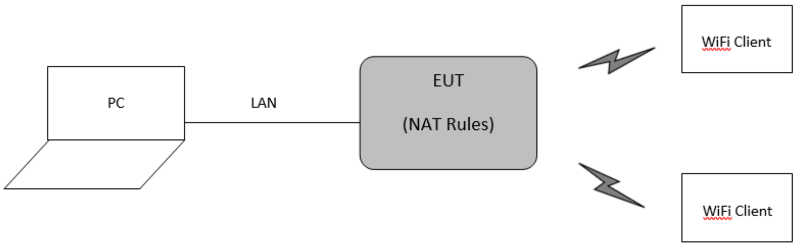
Test No.	GR_WiFiAP_044
Test Details	To check compliance for VPN Client requirements as per Clause 10.2 vi).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

Test Setup	ss  Test Setup for VPN Client test Laptop (VPN Server) Ethernet I/F EUT Wi-Fi Wireless I/F VPN Client
Test Procedure	1. Connect the Ethernet interface of the EUT to a VPN network. 2. Connect a laptop with VPN client credentials to the EUT on the WiFi. 3. Ping between VPN client and any system in VPN network. 4. Observe that the ping is successful
Test Limits	NA
Expected Results	The EUT should support the VPN client related functionalities as per Clause 10.2 vi).

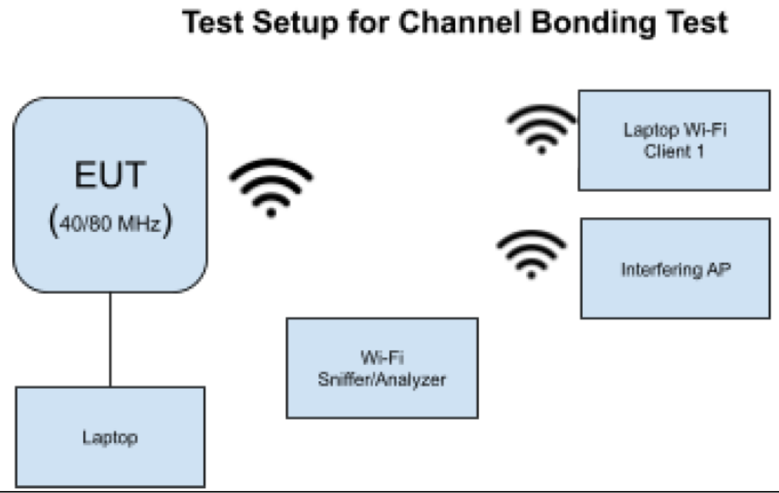
Test No.	GR_WiFiAP_045
Test Details	To check compliance for Firewall Support requirements as per Clause 10.2 vii).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.

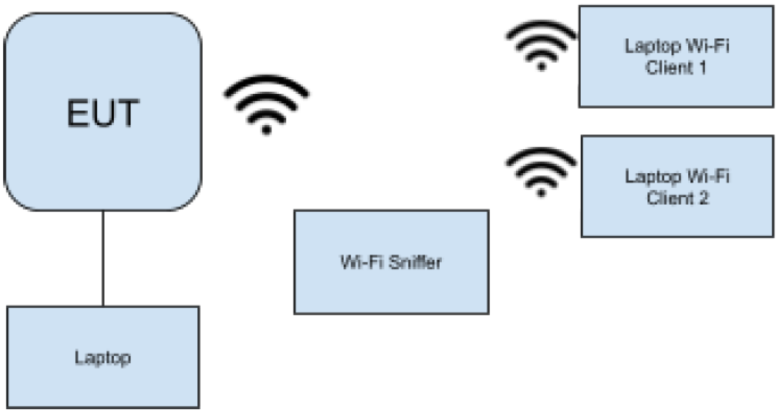
Test Setup	 Test Setup for Firewall test Laptop Ethernet I/F EUT Wi-Fi Wi-Fi Client 1 Wi-Fi Client 2
Test Procedure	A. IP address blocking 1. Connect two licensed equipments/laptops to EUT on WiFi 2. Connect one licensed equipment/laptop to EUT on Ethernet interface 3. Ping from both the licensed equipments/laptops connected on WiFi to that connected on the Ethernet interface 4. Verify that ping from licensed equipments/laptops on WiFi is successful 5. Configure the EUT to block the IP address of one of the licensed equipment/laptop connected on WiFi 6. Observe that ping to the blocked licensed equipment/laptop is failing.
Test Limits	NA
Expected Results	The EUT should support the Firewall support related functionalities as per Clause 10.2 vii).

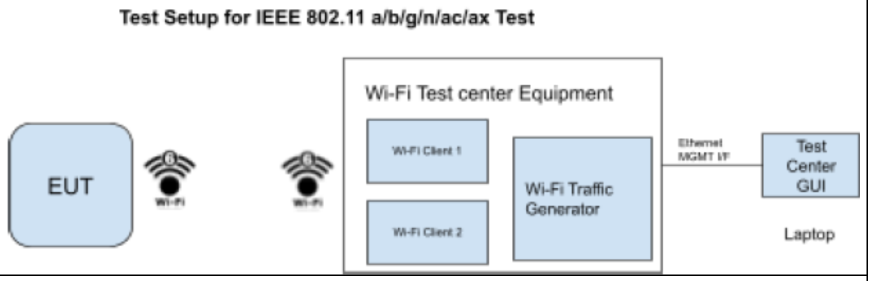
Test No.	GR_WiFiAP_046
Test Details	To check compliance for NAT requirements as per Clause

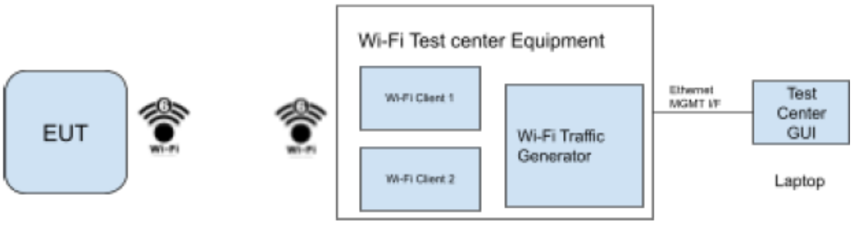
	10.2 viii).
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Wireshark etc. OR Licensed tools etc. 3. Connecting cables.
Test Setup	 PC LAN EUT (NAT Rules) WiFi Client WiFi Client
Test Procedure	1. Configure EUT for router mode with NAT rules 2. Connect two licensed equipments/laptops to EUT on WiFi 3. Connect one licensed equipment/laptop to EUT on Ethernet interface 4. Ping from Wi-Fi device to licensed equipment/laptop connected on Ethernet interface 5. Observe on the licensed equipment/laptop connected on Ethernet interface that NAT'ted packets are received.
Test Limits	compliance for NAT requirements as per Clause 10.2 viii).
Expected Results	The EUT should support the NAT related functionalities as per Clause 10.2 viii).

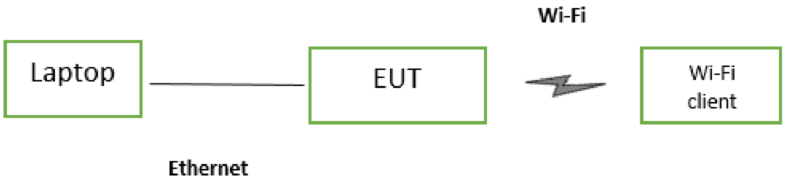
Test No.	GR_WiFiAP_047
Test Details	To check compliance for Channel Bonding requirements as

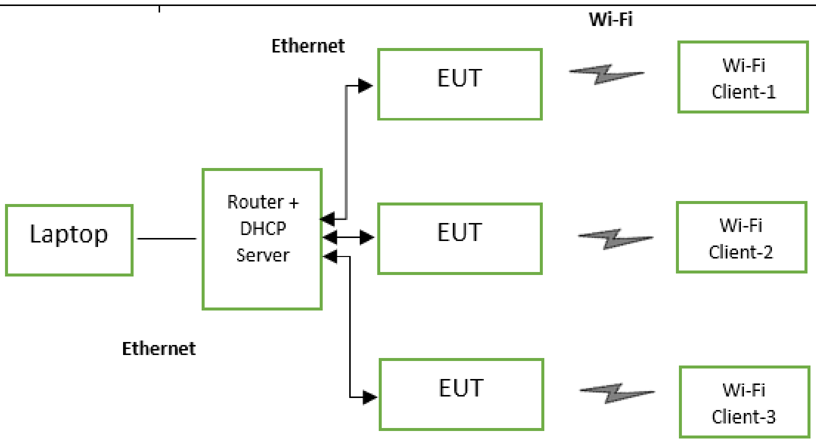
	per Clause 3.13.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Inssider etc. OR Licensed tools etc. 3. Connecting cables.
Test Setup	 Test Setup for Channel Bonding Test EUT (40/80 MHz) Laptop Wi-Fi Client 1 Interfering AP Wi-Fi Sniffer/Analyzer Laptop
Test Procedure	1. Configure EUT in 40Mhz bandwidth and connect a licensed equipment/laptop to connect as client 2. Verify using standard tools like Inssider that the EUT is operating in 40Mhz bandwidth 3. Power off the EUT 4. Configure another system/RF generator to cause interference in one of the 20MHz bands 5. Power On the EUT 6. Observe that the EUT is falling back to 20MHz bandwidth
Test Limits	compliance for Channel Bonding requirements as per Clause 3.13.
Expected Results	The EUT should support Channel Bonding related functionalities as per Clause 3.13.

Test No.	GR_WiFiAP_048
Test Details	To check compliance for backward compatibility requirements as per Clause 3.14.
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Inssider etc. OR Licensed tools etc. 3. Connecting cables.
Test Setup	Test Setup for Backward Compatibility Test  EUT Laptop Wi-Fi Client 1 Laptop Wi-Fi Client 2 Wi-Fi Sniffer Laptop
Test Procedure	1. Configure the EUT to be in n/ac/ax modes one at a time 2. Configure a licensed equipment/laptop in a/b/g mode one at a time and connect as WiFi client to EUT 3. Observe using standard tools like Inssider that the EUT is operating in desired mode. 4. Observe the association rate/link rate at the Wi-Fi Client. It should be as per the configured mode.
Test Limits	IEEE 802.11 a/b/g devices should connect to EUT with legacy data rates.
Expected Results	The EUT should support backward compatibility related functionalities as per Clause 3.14.

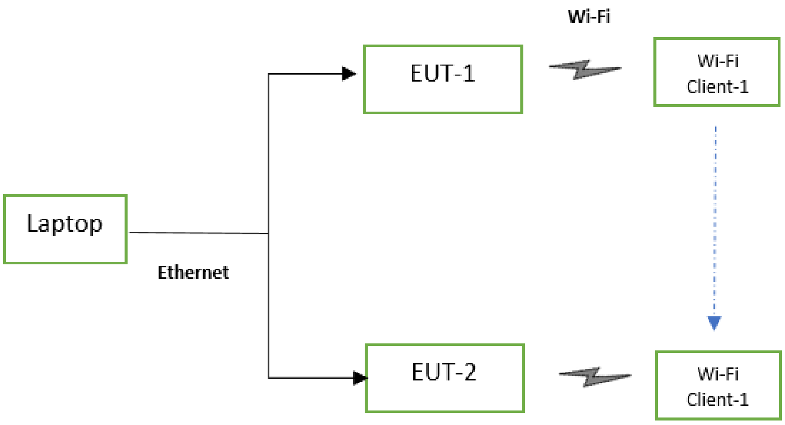
Test No.	GR_WiFiAP_049
Test Details	To check compliance for BCC-coded PPDUs in all supported modes for which LDPC is not mandatory for STAs as per clause 3.5 (viii)
Test Instruments Required	1. Equipment under test 2. Laptop with open-source tools like Inssider and Wireshark OR Licensed Wi-Fi Test Centre 3. Connecting cables.
Test Setup	 Test Setup for IEEE 802.11 a/b/g/n/ac/ax Test Wi-Fi Test center Equipment EUT Wi-Fi Wi-Fi Wi-Fi Client 1 Wi-Fi Client 2 Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop
Test Procedure	1. Configure the EUT to be in n/ac/ax modes one at a time with BCC coded PPDU Transmit and Receive capability. 2. Configure a licensed equipment/laptop and connect as WiFi client to EUT 3. Observe using standard tools like Inssider that the EUT is operating in desired mode. 4. Capture Packets at Wireless interface using Wireshark from the laptop or check in the Wi-Fi Test Center GUI for HT Capabilities info. 5. Observe HT/VHT Capabilities Info to check Coding type whether LDPC or BCC in the field “HT LDPC capability” or ”Rx LDPC”:
Test Limits	HT LDPC capability or Rx LDPC should be 0.
Expected Results	The EUT should support BCC coded PPDUs as per Clause 3.5 (viii).

Test No.	GR_WiFiAP_050
Test Details	To check compliance for Bit rates as per Clause 3.8.
Test Instruments Required	1. Equipment under test 2. Licensed Wi-Fi Test Center 3. Laptop with open-source tools like Iperf etc. OR Licensed tools like LANforge etc. 4. Power Adaptor 5. Connecting cables..
Test Setup	Test Setup for Bit Rates Test  EUT Wi-Fi Wi-Fi Wi-Fi Test center Equipment Wi-Fi Client 1 Wi-Fi Client 2 Wi-Fi Traffic Generator Ethernet MGMT I/F Test Center GUI Laptop
Test Procedure	1. LANforge or laptop - in a controlled environment such as a RF tent. 2. Configure the EUT for the desired mode of operation (802.11 a/b/g/n/ac/ax) one at a time 3. Configure the EUT for the desired bit rate as mentioned 4. Connect a licensed equipment like LANforge or a laptop 5. Ping between the laptop/equipment to the EUT 6. Run the data throughput measurement from LANforge & observe that EUT is associating at the desired bit rates.
Test Limits	As per Clause 3.8.
Expected Results	The supported data rates should be as per Clause 3.8.

Test No.	GR_WiFiAP_051
Test Details	To check router and dhcp functionality on Access point wherein single Wi-Fi AP is deployed by a PDO and parented by PDOA
Test Instruments Required	1. Equipment under test (Access point) 2. Laptop with open-source tools like ping 3. Power Adaptor 4. Connecting cables.
Test Setup	
Test Procedure	1. Configure EUT in router mode with NAT rules 2. Configure EUT with DHCP server. Assign IP Range. 3. Connect two laptops to EUT on WiFi 4. Connect one laptop to EUT on Ethernet interface 5. Check IP assigned to Wi-Fi Client devices is in the Range defined in the EUT. 6. Ping from Wi-Fi Client device to laptop connected on Ethernet interface 7. Observe on laptop connected on Ethernet interface that NAT'ted packets are received.
Test Limits	Compliance to Router and DHCP server functionality
Expected Results	The EUT should support Router and DHCP server functionality.

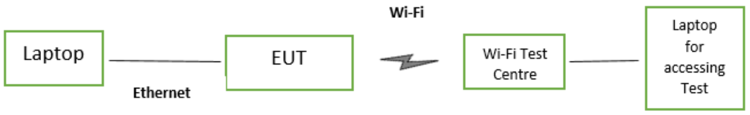
Test No.	GR_WiFiAP_052
Test Details	To check router and dhcp functionality in one of cluster nodeswherein multiple Wi-Fi APsare deployed by a PDO with single internet backhaul point and parented by PDOA
Test Instruments Required	1. Equipment under test (Access point) 2. Cluster node with Routing & DHCP server functionality 3. Laptops with open-source tools like ping 4. Power Adaptor 5. Connecting cables.
Test Setup	 Wi-Fi Ethernet EUT Wi-Fi Client-1 Router + DHCP Server Laptop EUT Wi-Fi Client-2 Ethernet EUT Wi-Fi Client-3
Test Procedure	1. Configure EUT for bridge mode 2. Configure a new node asRouter and DHCP server. Assign IP Range. 3. Connect two laptops to EUT on WiFi 4. Connect laptop to Router on Ethernet interface 5. Check IP assigned to Wi-Fi Client devices is in the Range defined in the NAS. 6. Ping from Wi-Fi Client device to laptop connected on Ethernet interface of Router 7. Observe on laptop connected on Ethernet interfaceof Router that NAT'ted packets are received.
Test Limits	Compliance to Router and DHCP server functionality in one of cluster nodes with multiple Access points deployment by

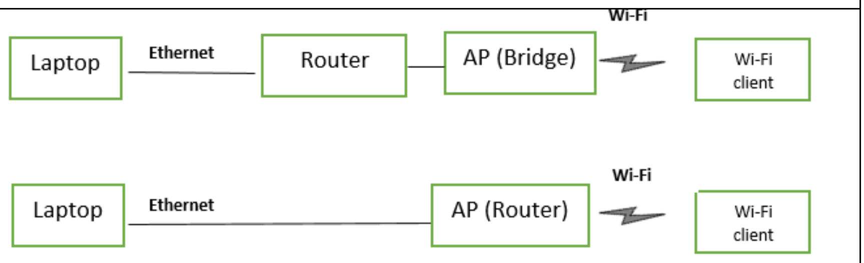
	PDO
Expected Results	The Cluster deploymentof PDO should support Router and DHCP server functionality.

Test No.	GR_WiFiAP_053
Test Details	To check Roaming of Wi-Fi clients in the cluster of Access points wherein multiple Wi-Fi APs are deployed by a PDO and parented by PDOA
Test Instruments Required	1. Equipment under test (Access point) 2. Laptops with open-source tools like ping, Iperf, Wireshark, 802.11r Wi-Fi support 3. Power Adaptor 4. Connecting cables.
Test Setup	 Wi-Fi EUT-1 Wi-Fi Client-1 Laptop Ethernet EUT-2 Wi-Fi Client-1
Test Procedure	SSID Based Roaming 1. Configure EUT-1 for with an SSID 2. Configure EUT-2 for with same SSID as configured on EUT-1 3. Place EUT-1 & EUT-2 with overlapping coverage region. 4. Connect onelaptop to EUT-1 on WiFi

	5. Verify the Wi-Fi Client laptop connection to EUT-1 6. Ping from Wi-Fi Client laptop to laptop connected on Ethernet interface and verify ping response 7. Move Laptop away from EUT-1 coverage and toward EUT-2 coverage. 8. Verify Wi-Fi Client laptop connection to EUT-2 9. Verify Ping (started in step 6) response FAST Roaming 1. Configure EUT-1 for with 802.11r and SSID 2. Configure EUT-2 for with 802.11r 3. Place EUT-1 & EUT-2 with overlapping coverage region. 4. Connect one laptop to EUT-1 on WiFi 5. Verify the Wi-Fi Client laptop connection to EUT-1 6. Ping from Wi-Fi Client laptop to laptop connected on Ethernet interface 7. Move Laptop away from EUT-1 coverage and toward EUT-2 coverage. 8. Verify Wi-Fi Client laptop connection to EUT-2 9. Verify Ping (started in step 6) response 10. Verify Wireshark captures on Wi-Fi client laptop to capture 802.11r packets
Test Limits	Compliance to SSID based roaming or Fast roaming
Expected Results	The Access points deployed by PDOA should support SSID based roaming or fast roaming.

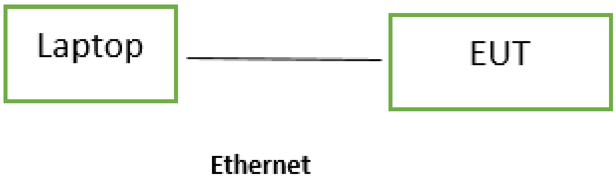
Test No.	GR_WiFiAP_054
Test Details	To check concurrent multiple Wi-Fi client’s connection to the Access point

Test Instruments Required	1. Equipment under test (Access point) 2. Laptops with open-source tools like ping, Iperf, Wireshark 3. Licensed Wi-Fi Test Center for multiple client simulation 4. Power Adaptor 5. Connecting cables.
Test Setup	 Laptop Ethernet EUT Wi-Fi Wi-Fi Test Centre Laptop for accessing Test
Test Procedure	1. Configure EUT (Access point in router or bridge mode)with an SSID 2. Configure Wi-Fi Test Centre to simulate a minimum 20 Wi-Fi clients 3. Connect the Wi-Fi Clients to the EUT 4. Verify the number of Wi-Fi Clients connected to EUT 5. Verify the IP assignment to each Wi-Fi Clients 6. Verify ping from each Wi-Fi client to the laptop connected to ethernet interface of EUT
Test Limits	Compliance to concurrent Wi-Fi client's connection to Access point
Expected Results	The Access point deployed by PDO should support a minimum 20 concurrent Wi-Fi client's connection to Access point.

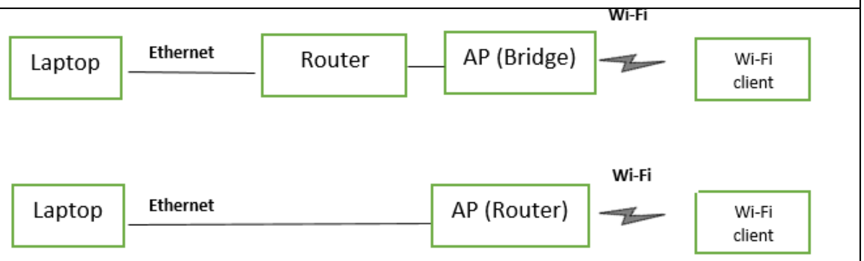
Test No.	GR_WiFiAP_055
Test Details	To check capability of Access point or equivalent cluster node to store and transfer IP detail record to PDOA after end of each session or periodically after every 24 hours
Test Instruments Required	1. Equipment under test (Access point or AP plus router node) 2. Cluster node with Router and DHCP server function 3. Laptops with open-source tools like ping, Iperf, Wireshark 4. Laptops with Wi-Fi client support 5. Power Adaptor 6. Connecting cables.
Test Setup	 Laptop Ethernet Router AP (Bridge) Wi-Fi Wi-Fi client Laptop Ethernet AP (Router) Wi-Fi Wi-Fi client
Test Procedure	1. Configure EUT (Access point or AP plus router node) in Router mode with an SSID as per network deployment 2. Configure the EUT with Laptop IP as PDOA IP 3. Connect the Wi-Fi Clients to the Access point 4. Verify the number of Wi-Fi Clients connected to Access point 5. Verify the IP assignment to each Wi-Fi Clients 6. Verify Iperf (TCP) from each Wi-Fi client to the laptop connected to ethernet interface of EUT

	7. Verify the IP detail record generated for each Wi-Fi session. 8. Verify the IP detail record size stored for each Wi-Fi session on the EUT 9. Verify the IP detail record transferred to Laptop connected on ethernet interface of AP/Router on configurable time interval (1 hour, 2 hours etc.) 10. Reboot the AP/Router 11. Verify the IP detail record still retained on the Ap/Router.
Test Limits	Compliance to storage and transfer capability of IP Detail records on the Access point (standalone) or router node to PDOA.
Expected Results	The Access point or equivalent cluster node in PDO network should be able to generate and store the IP detail records on Access point or router and should be able to transfer it to PDOA.

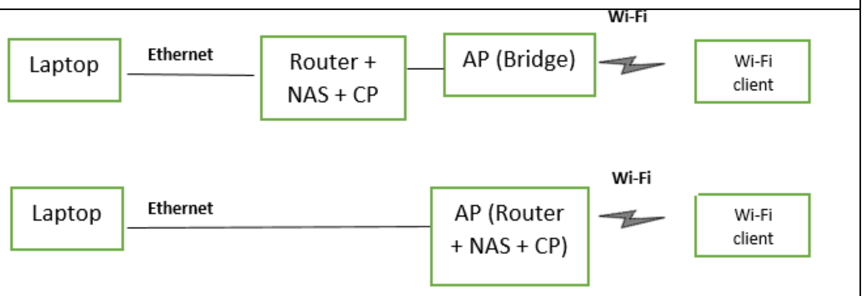
Test No.	GR_WiFiAP_056
Test Details	To check support of Network clock synchronization function on the Access point
Test Instruments Required	1. Equipment under test(Access point) 2. Laptops with open-source tools like ping, Iperf, Wireshark, NTP server 3. Laptops with Wi-Fi client support 4. Power Adaptor 5. Connecting cables.

Test Setup	
Test Procedure	1. Configure the EUT with Laptop (connected on ethernet interface of EUT) IP as NTP server IP. 2. Configure the Laptop (connected on ethernet interface of EUT) with NTP server and current date & time. 3. Verify the Date and Time on the Laptop. 4. Configure a different time than current time on EUT. 5. Enable NTP client functionality on EUT 6. Check the Date and Time on the EUT. 7. Verify if the Date and Time on EUT automatically sets to current time (or time set on the laptop in step 3). 8. Reboot the EUT 9. Verify if the Date and Time on EUT automatically sets to current time (or time set on the laptop in step 3).
Test Limits	Compliance to Network clock synchronization functionality on Access point
Expected Results	The Access points deployed by PDO should support network clock synchronization functionality.

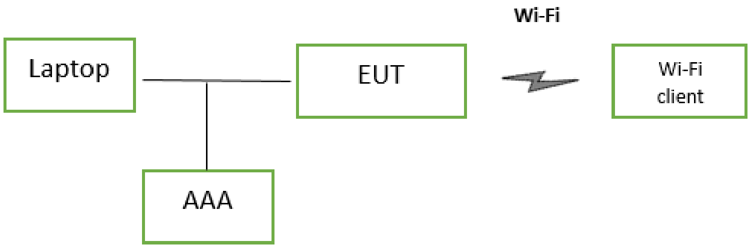
Test No.	GR_WiFiAP_057
Test Details	To check capability of Access point or equivalent cluster node of PDO to store IPDR logging for minimum 3 days

Test Instruments Required	1. Equipment under test (Access point or AP plus Router node) 2. Cluster node with Router and DHCP server function 3. Laptops with open-source tools like ping, Iperf, Wireshark 4. Laptops with Wi-Fi client support 5. Power Adaptor 6. Connecting cables.
Test Setup	 Laptop Ethernet Router AP (Bridge) Wi-Fi Wi-Fi client Laptop Ethernet AP (Router) Wi-Fi Wi-Fi client
Test Procedure	1. Configure EUT (Access point or AP plus Router node) in Router mode. 2. Configure the EUT with Laptop IP as PDOA IP 3. Define total number of clients served by EUT in a day. 4. Define average data consumed by the client in a day 5. Define size of IPDR record generated by each client in a day. 6. Calculate average storage required to store the IPDR records of a day. Multiply it by 3. It provides total storage required on the EUT for 3 days. 7. Copy a file of equivalent size on the defined storage location in the EUT. 8. Reboot the EUT 9. Verify if the file is retained on the EUT.
Test Limits	Compliance to storage of IPDR record on minimum 3 days

	on Access point (standalone) or equivalent in the cluster deployment.
Expected Results	The Access point or equivalent cluster node should be able to generate and store the IP detail records on Access point and should be able to transfer it to PDOA.

Test No.	GR_WiFiAP_058
Test Details	To check capability of Access point or equivalent cluster node of PDO to present a uniquely branded user interface called captive portal when the wireless client device connects to it.
Test Instruments Required	1. Equipment under test (Access Point or AP plus (Router & NAS & CP) node) 2. Cluster node with Router, NAS (Network Access Server) and CP (Captive Portal) function 3. Laptops with open-source tools like ping, Iperf, Wireshark 4. Laptops with Wi-Fi client support 5. Power Adaptor 6. Connecting cables.
Test Setup	 Laptop Ethernet Router + NAS + CP AP (Bridge) Wi-Fi Wi-Fi client Laptop Ethernet AP (Router + NAS + CP) Wi-Fi Wi-Fi client
Test Procedure	1. Configure EUT(Access point or AP plus cluster node) in Router mode with a SSID

	2. Configure the EUT(Access point or equivalent cluster node) with captive portal functionality. 3. Connect Wi-Fi client laptop to EUT over Wi-Fi. 4. Verify the captive portal page displayed on the Wi-Fi client laptop
Test Limits	Compliance to presenting uniquely branded captive portal page to Wi-Fi clients when connected to Access point.
Expected Results	The Access point or equivalent cluster node in PDO network deployment should be able to present uniquely branded captive portal page to the Wi-Fi clients.

Test No.	GR_WiFiAP_059
Test Details	To check capability of Access point or equivalent cluster node of PDO to whitelist PDOA related IPs/URLs
Test Instruments Required	1. Equipment under test 2. Laptops with open-source tools like ping, Iperf, Wireshark 3. Laptops with Wi-Fi client support 4. Power Adaptor 5. Connecting cables.
Test Setup	
Test Procedure	1. Configure EUT (Access point and equivalent cluster node with NAS function) in router mode with whitelist

	functionality. 2. Connect Wi-Fi client laptop to Access point (open SSID) over Wi-Fi. 3. The Wi-Fi client should get IP address 4. The Wi-Fi client should not be authenticated through AAA. 5. The Wi-Fi client should not be able to send http request to Laptop. 6. Configure the Laptop (connected to ethernet interface of EUT) IP as PDOA IP in the whitelist pool of Ips in EUT 7. The Wi-Fi client should be able to send http request to Laptop.
Test Limits	Compliance to whitelisting IPs capability in Access point or equivalent cluster node with NAS function
Expected Results	The Access point or equivalent cluster node in PDO network deployment should be able to whitelist the PDOA IPs/URLs.

J. SUMMARY OF TEST RESULTS

GR/IR No.______________________________

TSTP No.________________________________

Equipment name & Model No._____________

Clause No.	***Compliance*** *(Complied /Not Complied / Submitted/Not Submitted / Not Applicable)*	***Remarks / Test Report Annexure No.***

[Add as per requirement]

Date:

Place: ***Signature & Name of TEC testing Officer /***

**** Signature of Applicant / Authorized Signatory***

**** Section J as given above is also to be submitted by the Applicant/ Authorised signatory as part of in-house test results along with Form-A. The Authorised signatorssy shall be the same as the one for Form 'A'.***