GUJARAT GAS

SECTION-II
SCOPE OF WORK AND SOR WITH TECHNICAL SPECIFICATIONS

FOR

WIFI- WIRELESS SOLUTION

TABLE OF CONTENTS

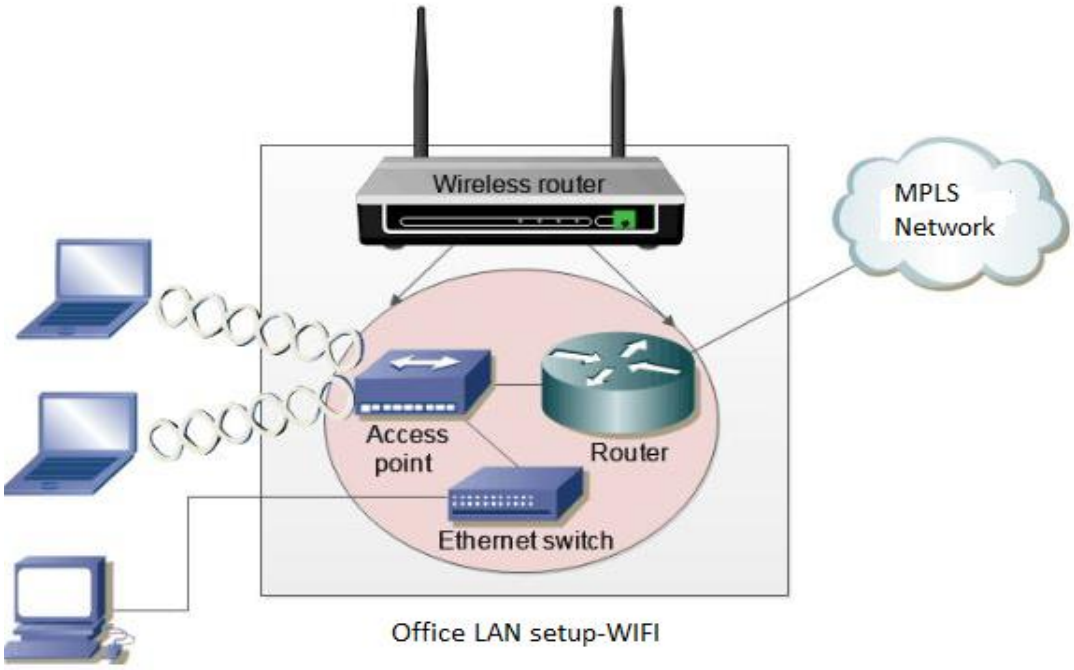
1. GGL Requirements

Gujarat Gas invites proposals from competent and authorized vendors /partners for Implementation of enterprise Grade WIFI solution which provides fast and reliable connections for all employees and visitors to ensure that productivity doesn't suffer.

2. Background and Objective

At Gujarat gas ltd , we have WIFI solution deployed almost 9-10 years ago . The Cisco make AIR-CT5508-K9 is old and technology need to be upgraded .

IT team propose to deploy latest ENTERPRISE GRADE WIFI technology for wireless LAN connectivity at VC room and critical offices across GGL locations. WIFI Access point uses radio signals for connectivity. Any device which falls in its signal range can connect with it. This feature makes it more flexible.



Office LAN setup-WIFI

Network connectivity within the area of range from anywhere within office
No need for network cabling for PC/Laptop device usage within VC room: ...
Wireless routers ,networks can serve a suddenly-increased number of clients with the existing equipment
In small office users can use WIFI to connect to GGL network, LAN cabling can be avoided /reduced

3. Scope of Work

I. Supply and installation of WIFI solution with Compatible Controller complying with the technical specifications given in Annexure –I, along with accessories and necessary documentation at GGL Datacenter GIFT City Gandhinagar.
II. The proposed WIFI Solution shall be compatible /Integral with GGL Network which is primarily Cisco platform.
III. Configuration and Integration of WIFI Solution with existing LAN/WAN at respective Datacenter.
IV. Prior to configuration and Integration, the bidder needs to study the existing setup GGL DC at Surat and GIFT City Gandhinagar and prepare detailed implementation plan. On approval of the same by GGL network SME, integration of WIFI needs to be carried out.
V. The O.E.M should provide a license copy (hard copy) or license document.
VI. The OEM should provide 24x7 technical support through phone and Web, Product Upgrades, Updates, Patches and access to Technical Library and Product Documentation
VII. Periodic preventive maintenance of hardware, once in half year by the bidder
VIII. The bidder shall impart complete administration training to at least two officials of the Gujarat Gas by OEM / authorized partner of OEM. The training should include Perform seamless product upgrades, Back-up and restore, monitor suspicious network activities and analyze attacks, troubleshoot network connections, Implement Identity Awareness(Minimum) for more granular access levels, Configure permanent tunnels for remote access to corporate resources etc
IX. WIFI Controller and Access points shall be from the same OEM only. AP must be thin AP's & must not be available to manage standalone in any given condition.
X. One Wireless controller (HA port and Management port) which cater minimum 100 access point seamlessly
XI. Bidders to check and provide Virtual software based Wireless controller at DR site without any additional cost
XII. All access point shall have at least 1 Port gigabit POE injector which generate at least 30 watts which cater the access point power.
XIII. AC Power adaptor for wireless access points with Indian style power plug
XIV. GGL location to be bifurcated in below 3 type and access point to be deployed as per below chart as per feasibility.

Access Point for location	**Approximate number of users**	**Tentative distance covered (Minimum)**
Type A	>=40 and <= 60	60 to 70 Mtrs diagonal
Type B	>=20 and <=40	50 to 60 Mtrs diagonal
Type C	>=10 and <=20	40 to 50 Mtrs diagonal

XV. **Delivery period of material** ,3 months from the date LOA/PO is awarded to BIDDER
XVI. **Project implementation period** ,6 months from the date LOA/PO is awarded to BIDDER.

4. Post Go live Support, Warranty

1. Support to be considered for 5 years from OEM /Bidders
2. During this period of 5 years, bidders shall provide comprehensive warranty (Parts,Labour,Configuration,Software upgrade) all upgrades for firmware, operating system upgrades , version upgrades, quick fixes and security patches to be made available to GGL at no extra cost
3. OEM to provide support for 8*5 over telephone, remote, onsite support .
4. The product upgrade to be supported by any nominated implementation partner by OEM
5. Vendor will provide contacts of all the resources and a clear escalation matrix for the support period.

5. Payment terms

Description	Payment Terms
Material cost	• 70% On material delivery • 30% On completion of work.
Support cost	• Yearly in advance

6. Service Level Agreement (SLA)

1) Breakdown and preventive maintenance of WIFI solution (Access point and Controllers) will be in the scope of vendor during support period
2) The support must be comprehensive in nature covering spares, labour and logistics onsite to GGL.
3) Required critical spare listing must be prepared by vendor to meet the deliverables as mentioned in the SLA.
4) Vendor must give escalation matrix with all the details as per following. There has to be minimum 3 level of escalation.

Escalation Level	Name / Team	Availability (24x7 OR 8x5 etc)	Mobile	Telephone	E-mail	Address

5) There has to be call logging, response, update, and resolution and closure process.
6) There has to be performance monitoring during support with all the support calls escalated and their response and resolution.
7) In case of failure i.e. either the device or any parts the vendor should respond to the incident within 4 hours and resolution should be given within 24 hours
8) There will be Performance Review Yearly.
9) GGL Required Response Time : 4 hour
10) GGL Required Resolution Time : 24 hours
11) GGL Required Uptime of WIFI Solution /Service 99.0 % during Support period.

7. Performance Review

Once in a year SLA review, MOM, Presentation, documentation, List of Calls attended during last one year with achievements of SLA with penalties agreements.

8. Penalty clause

1. **Material Delivery delay** – penalty of 0.5 % of the overall material cost per week of delay, maximum penalty of 10% of overall Material cost.
2. **Implementation delay** - penalty of 0.5 % of the overall material cost per week of delay, maximum penalty of 10% of overall project implementation cost
3. **SLA Violation** -GGL shall impose a penalty of INR 5,000/- (Indian rupees) per instance for not meeting the agreed SLA, Maximum Penalty in year shall not exceed 10% of total yearly support cost .

9. Documentation & Product training

Bidder shall prepare the following Documents and submit to Company.

1. Complete configuration guide
2. Complete operation document on daily check lists
3. Complete test plans signed off
4. Basic and Advanced Level of trainings to GGL representatives at least 2 nos for:

    a. Hardware setup and configuration
    b. Software configuration
    c. System /Device Management
    d. Report generation

10. Project Management

Bidder needs to take this as a turnkey project, this will require bidder to provide resources for implementation of project.
Significant weightage will be given to the vendor that submits the detailed thought proposal, in terms of completeness of BOM considering our existing setup, project planning and scheduling, risks and mitigation and implementation plan.

Following are some of the expectations:

a. All technical specifications for configuration at least 1 week in advance before delivery
of material and services
b. Advance notification for dependencies with GGL and any other vendor required during installation/configuration.
c. Overall weekly updates on the activity progress throughout the implementation tenure.
d. All the installation & configuration services have to be delivered by Certified OEM engineers or Certified Partners having Certified Engineers of the proposed solution only.
e. Proper handover to GGL team and vendor operational team with complete documentation on each configuration and setup.
f. A Vendor would be responsible for identifying bottlenecks for the performance and deliver appropriate solution for that.
g. Testing for all parameters / configurations

11. QHSE REQUIREMENTS

SCOPE AND APPLICATION

Contractor/Service providers are the key stake holder and an integral part of Gujarat Gas Ltd (GGL's) business. Contractors'/Service provider' Quality, Health, Safety and Environment (QHSE) performance reflects on the company's business performance and reputation. GGL has established QHSE Management Systems, Procedures & Guidelines to ensure compliance with GGL's QHSE requirements. These requirements apply to all jobs whilst conducting work for GGL including; Project, Construction, Operation & Maintenance, Field Operations and Services within any given contract or agreement.

The overall objective of QHSE management in contract/agreement is to improve the company and Contractor's/Service providers' QHSE performance in all aspects of activities. Active and on-going participation by both the GGL and Contractor/Service provider is essential to achieve this objective.

RESPONSIBILTIES

It is responsibility of GGL management and staffs to ensure that all Contractors/Service providers work under their direction & control are provided with relevant Integrated Management System (IMS) Policies, Procedures & Guidelines that describe the GGL requirements for undertaking work within the company. It is also the responsibility of Contractors/Service providers to ensure that their staff are informed of and comply with GGL's requirement whilst working for the company.

GGL HSE department provides advice and assistance on QHSE requirements across the complete spectrum of all work activities. Contract Owner (Department Head) and Contract Holder (Work in-charge) are responsible to ensure safe execution of work/service include the following:

- Ensuring that the QHSE Policy, Procedures & Guidelines are known and understood by all contractors'/service providers' staff and work force
- Monitoring, Inspecting & Auditing execution of work, activities to ensure adherence to the QHSE compliance requirements

The Contractors'/Service provider' will take the responsibility for implementation of GGL's QHSE Policy, Procedures, Guidelines and other requirements with the advice and support of the GGL's Contract Owner / Contract Holder and HSE representative.

Contractor/Service provider to ensure that all aspects relating to QHSE are adequately addressed and implemented in accordance with the GGL QHSE requirements and QHSE Management Plan, which shall include the management processes and activities to be implemented during the course of work with GGL.

Contractor/Service provider shall be responsible for ensuring that adequate HSE resources are put in place to enable satisfactory implementation of QHSE Management Plan.

This responsibility also applies to ensure the Health and Safety of the people are directly and indirectly engaged / involved whilst working or present at GGL's work area / sites.

MOBILIZATION

- Post selection and awarding of contract, GGL shall arrange a kick-off meeting with Contractor/Service provider where GGL team members Contract Owner (CO), Contract Holder (CH) & HSE representative) will discuss on QHSE Management aspects / plan and requirements in order to make sure that Contractor/Service provider and their team are fully understanding the expectation of GGL. During the meeting, QHSE Management Plan shall be discussed and agreed between GGL and Contractor/Service provider
- Contractor/Service Provider shall ensure that all tools, tackles, equipment, machineries & instruments are adequately deployed and are 'Fit for Purpose'. Pre mobilization checks/inspection shall be carried out by GGL team for the same before the start of work.
- GGL emphasizes on the importance of the Health and Fitness of all staff/work force deployed at GGL work sites. Contractor/Service provider shall adhere to medical check-up as per the GGL Health check-up matrix (as applicable)
- A proper HSE orientation and training will be organized by GGL for the Contractor/Service provider workforce before the start of work; under no circumstances should the Contractor/Service provider commence the work unless they have undergone the HSE training (as applicable)
- Contractor/Service provider shall ensure that all their staff/work force are provided required Personal Protective Equipment (PPEs) as per GGL PPE matrix (as applicable)
- Contractor/Service Provider shall ensure all required emergency arrangements like Medical treatment, FIRST AID box and Firefighting equipment (as applicable)

EXECUTION

- Contractor/Service provider is responsible to ensure the compliance with GGL QHSE requirements. GGL overall QHSE performance is directly influenced by the contractors' performance.
- Contractor/Service provider is responsible for QHSE compliance monitoring at site/work activities to ensure that work/activity is performed in a safe manner. Moreover, they are responsible for reporting of all incidents, Hazard and Near Miss that might happen during work/activity
- Contractor/Service provider shall follow and comply with GGL ''Work Permit'' system
- During work execution and activities, GGL team will regularly monitor and evaluate the performance of the Contractor/Service provider to identify the shortfalls and weaknesses and assist to improve the overall performance including QHSE performance through CPAR process (as applicable).

We believe that everyone at GGL, Employees, Contractors, Service providers and Associates have the right to go home safely to their families.

QHSE Defaults and Penalties (As applicable)		
Sr No	Description	Penalty amount (will be decided by Contract Owner)
1	LTI	Rs. 2500 / Instance
2	Non-compliance - HSE Engineer	NA
3	Un authorized work	NA
4	Work without PtW/WA	Rs. 1000 / Instance
5	Non-compliance - Safety Training Card (STC)	NA
6	Non-compliance - Health Check up	NA
7	Non-compliance - PPEs	NA

Remark: Issuance of MEMO against HSE non compliances including above mentioned defaults shall be decided by Contract Holder

QHSE GUIDELINE (AS APPLICABLE) FOR ALL TYPE OF CONTRACTS

- Contractor/Service provider…

a) Shall ensure that all staff/work force comply with the requirements of the GGL HSE Management System, QHSE policy, standard, procedures, guideline, plan & Life Savers at work site

b) Shall ensure issuance of Identity Card to their team members

c) Shall apply and obtain Permit to work (PtW/WA) before start of the work

d) Shall arrange work related Personal Protective Equipment (PPEs) for their staff/work force and ensure proper use during the execution of job

e) Shall carry out the work within the duty hours/office hours. No Work shall be carried out without permission of GGL's representative beyond the official duty hours unless otherwise agreed upon prior to start of work and recorded appropriately

f) Shall ensure that all tools, tackles, appliances, machines, vehicles, instruments or other equipment are Fit for Purpose and maintained safe working condition at all times and are used only by authorized and competent persons

g) Shall ensure that all the QHSE requirements are properly discussed for any sub-contracted activities with GGL. No such activity shall be performed without clearance from GGL management

h) Shall ensure that all Hazards, Near miss, accident, incident, injuries are reported promptly to GGL. Action arises due to reported Hazards, Near miss, incident investigation; audit/inspection shall be closed out as per agreed timelines with site in-charge

i) Shall deploy staff & work force trained, qualified and competent for the work and well aware of risks and mitigation action/s for the activities undertaken

j) Shall make necessary arrangements for safe custody of equipment, materials in stores/warehouse and at site

k) Shall ensure safe transportation, storage and handling of materials to prevent any damage which may impair safe performance of the equipment / material etc.

l) Shall initiate immediate actions to hospitalize injured person(s)

m) Shall ensure an injury free, incident free workplace and protect people from harm caused by work activities

n) Shall ensure use of seatbelts while driving four-wheeler and use of crash helmet for Two wheeler riders during job execution

o) Shall ensure Lock out and Tag out (LOTO) after de-energizing and double check before starting any jobs. In case of conducting job for the purpose of fault finding & monitoring of voltage & current it is to be considered live working and all PPE'S to be worn to avoid exposure of flash arc current

p) Shall take note that the use of open wires in sockets, use of wires with tape joints shall not be accepted at work site.

q) Shall ensure proper collection, storage and disposal of solid / liquid waste as per GGL procedure and guideline

r) Staff/work force shall not smoke or resort to misuse of drugs, medicines or alcohol while on duty

s) In case of any incident like fire, gas leakage etc. due to gross negligence of the Contractor's staff/work force, GGL reserves the right to impose penalty up to actual damage cost and or termination of work order depending upon the gravity of the situation.

t) Any breach of the QHSE requirements shall be deemed by the company to be a material breach of the terms & condition of the contract. GGL shall be entitled to take appropriate actions including instructing the contractor to (a) remedy the breach; (b) suspend the work or (c) terminate the contract.

u) All activities shall be carried out as per GGL's documented procedures and QHSE requirements, deviation from it shall be dealt with very strictly .

12. Annexure –I Technical specifications- Wireless controllers

Features	Sr no	Specifications	Compliance (Yes/No)
General	**1**	The Solution must be appliance based from the same Access Point OEM proposed.	
	2	Below specifications are minimum asked. Bidder are free to propose extra if solution need to incorporate the same. Also if below all features are not possible to achieve via single WLC than bidder are free to propose additional solution to match the compliance asked.	
	3	Controller must support IP4 & IPv6 Dual stack ,IPv6 routing from day 1 for management access & route the traffic	
	4	Proposed controller must have 2FA enable for atleast 2 admin to access controller GUI with 2FA for security reasons. If 2FA is not inbuilt, bidder are free to propose its integration tools & license from day 1.	
Wireless Controller	**1**	Proposed appliance must manage atleast 50 AP's from day 1 & must be scalable upto 100 Access Points in Bridge mode by adding just a license to the device.	
	2	It must have option to deploy AP's in Tunnel mode and Bridge mode for easy management	
	3	Controller should support deep packet inspection for all user traffic across Layer 4-7 network to analyses information about applications usage, peak network usage times for all access points from day one	
	4	Tunnel between AP & WLC must be encrypted in nature via IPSEC/CAPWAP or equivalent protocol	
	5	The appliance should support IEEE 802.11a/b/g/n/ac/Wave 2 standards-based wireless Access Points from day1.	
	6	Supports strong Authentication and Encryption Standards Include Open/ WEP64/ WEP128/ Shared, Guest Captive Portal, WPA /WPA2 802.11i Preshared key,WPA / WPA2 802.11i with Radius support.Wireless solution should support CCMP/AES ,WEP 64- and 128-bit,TKIP,SSL and TLS,RC4 128-bit,RSA 1024-bit,RSA 2048-bit,L2TP/IPsec (RFC 3193), XAUTH/Ipsec and PPTP (RFC 2637) Encryption protocols	

	7	The solution should have the capability to use an AP infrastructure and terminate two different SSIDs on two different controllers while maintaining complete separation and security for all networks, policies, management and visibility.	
	8	**The wireless controller support the following types of client load balancing:**	
	8.1	a)Access Point Hand-off - the wireless controller signals a client to switch to another access point.	
	8.2	b)Frequency Hand-off - the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency automatically	
	9	For smooth, seamless and easy manageability, operation, interoperability and maintenance, the bidder should offer/quote WLC & WAPs of the same make (OEM).	
	10	The solution should Live Upgrades and multiple version support to upgraded alongside active user sessions and eliminate the need for planned maintenance windows or downtime. Each Controller Cluster or individual service modules can also be selectively upgraded without impacting the rest of the network.	
	11	It must be feasible to detect AP on L2 & L3 discovery as & when required	
	12	**User Authentication features:**	
	12.1	AD, LDAP, RADIUS & Local user authentication	
	12.1	SSO should be done with AD user on windows system	
	12.2	2FA should be optional & must integrate with SMS/Email system for wireless users	
	12.3	Should support Soft/Hard Token based two-factor Authentication for all type of users (Inbuilt or Integrated with 3rd party)	
	13	**The wireless controller should include the following features.**	
	13.1	Wireless guest management with dedicated reception portal to create Guest users	

	13.2	Captive portal with Email capture login	
	13.3	Wireless Mesh, Bridging Features	
	13.4	BYOD (Bring Your Own Device) Support	
	13.5	User and application control	
	13.6	Wireless IDS feature from day 1	
	14	**The wireless Controller should support the following RF Management features**	
	14.1	a) Having Automatic Channel Allocation	
	14.2	b) Having Automatic Power Control	
	14.3	c) Supporting Neighborhood scanning of RF environment to minimize neighboring AP interference and leakage across floors.	
	14.4	d) Having Coverage Hole Detection	
	14.5	e) Providing alerts when APs are down or compromised RF environment is detected	
	14.6	f) Having Self-healing - Automatic neighboring AP power increase to fill in for coverage losses	
	15	The wireless Controller should support Rogue AP detection technology enabled	
	16	The solution must offer WIDS from day 1	
Hardware	**1**	Proposed solution must have atleast 4 GE RJ45 & 2GE SFP interface with Short range Transceivers included from day 1	
	2	Proposed solution must have dedicated console & USB interface	
	3	Proposed solution must offer atleast 2TB of storage for logging & reporting. Bidder are free to propose external server/appliance for logging/reporting if required.	
	4	Intergration & license for external Logging/reporting solution must be part of bidders offer from day 1	
	1	Controller must be security enabled with AV, IPS, WCF, AS, App-control, DoS protection, DLP from day 1,Controller should support deep packet inspection for all user traffic across Layer 4-7 network to analyses	

		information about applications usage, peak network usage times for all access points from day one	
	2	WIPS solution should Automatically blacklist clients when it attempt any attack.	
	3	WIPS solution should be capable of wireless intrusion detection & prevention .The WLAN should be able to detect Rogue AP and take corrective action to prevent the rogue AP. The system should detect and prevent an organization's wireless client connecting to rogue AP and also prevent an outside client trying to connect to organizational WLAN.	
	4	WIPS solution should detect & prevent an Ad-hoc connection (i.e. clients forming a network amongst themselves without an AP) as well as windows bridge (client that is associated to AP is also connected to wired network and enabled bridging between two interfaces)	
	5	The wireless solution should support Active/Active (1:1) or Active/Standby (1+1) or N+1 High Availability Deployment Modes	
Security	**6**	The system should detect an invalid AP broadcasting valid SSID and should prevent valid clients getting connected from these AP's.	
	7	WIPS Solution should track the location of interferer objects.	
	8	For advance forensic WIPS solution should perform spectrum analysis to detect and classify sources of interferences. System should provide chart displays and spectrograms for real-time troubleshooting and visualization.	
	9	The WIPS solution should able to detect and locate the rogue access point on floor maps once detected.	
	10	The WIPS solution should able to detect and prevent if a client use FATA-Jack 802.11 DoS tool (Available free on internet) and tries to disconnect other stations using spoofed authentication frames that contain an invalid authentication algorithm number.	
	11	The WIPS solution should detect and protect if a client probe-request frame will be answered by a probe response containing a null SSID to crash or lock up the firmware of any 802.11 NIC.	

	12	The WIPS solution should detect and protect if a client/tool try to flood an AP with 802.11 management frames like authenticate/associate frames which are designed to fill up the association table of an AP.	
	13	The WIPS solution should detect and protect if a client/tool keep on sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF) disconnect all stations on a network for a widespread DoS.	
	14	The WIPS solution should detect and protect if somebody try to spoof mac address of client or AP for unauthorized authentication.	
	15	The WIPS solution should detect and protect if a client/tool try de-authentication broadcast attempts to disconnect all clients in range rather than sending a spoofed deauth to a specific MAC address.	
	16	Should provide real-time charts/log showing interferers per access point, on a per- radio, per-channel basis.	
	17	The WIPS solution should detect and protect if an attacker attempts to lure a client to a malicious AP using SSID on fake AP in close proximity of the premises. It should detect When the Valid Client probes for Valid SSID and these malicious APs respond and invite the client to connect to them.	
	18	When client radio is in sleep mode to save battery and AP then begins buffering traffic bound for that client until it indicates that it is awake. The WIPS solution should detect and protect if intruder try sending spoofed frames to the AP on behalf of the original client to trick the AP into believing the client is asleep to buffer the AP beyond limit.	
Routing	**1**	Controller must have capacity to act as a SD-WAN solution.	
Virtualization	**1**	Controller must have option to virtualized its OS into multiple part so that it can divide in Firewall, SD-WAN, WLC as & when required. It must have at least 10 Virtualized context from day 1	
Eligibility	**1**	If above is only possible in single WLC, than bidder may need to propose additional Hardware for Firewall & SD-WAN which must be listed in both respective Gartner report	

13. Annexure –II Technical specifications- Access point Type A

Indoor dual radio Wireless Access Point covers minimum distance of approx. 60-70 meter diagonal and suffice approx. 40-60 user load		
Sr No	**Specifications**	**Compliance (Yes/No)**
1	Access Point radio should be minimum dual/tri-radio 5GHz 4x4 MIMO with 4 spatial streams and 4x4 MIMO with 4 spatial streams on 2.4 Ghz radio. The AP should have Dual Radio 802.11ax access point with OFDMA and Multi-User MIMO (MU-MIMO).	
2	Access Point should be 802.11ax ready from day one and support WPA3 and Enhanced Open security from day one	
3	AP should have 2 x 10/100/1000 interface RJ45/SFP interface with 1 Console port have one SmartRate port (RJ-45, maximum negotiated speed 5Gbps) and one 2.5Gbps and 5Gbps speeds comply with NBase-T and 802.3bz specifications	
4	Access point should support Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices	
5	Access point should support OFDMA and MU-MIMO for enhanced multi-user efficiency	
6	Access point should IoT-ready Bluetooth 5 and Zigbee support	
7	Minimum aggregate data rate should be 6 Gbps	
8	Access Point can have integrated internal antenna	
9	The Max transit power of the AP + Antenna should be as per WPC norms for indoor Access Points. OEM to give a undertaking letter stating that the AP will configured as per WPC guidelines for indoor AP and also submit the WPC certificate showing approval.	
10	Access point should have Internal/External Bluetooth Low energy beacon to support advance location based services for Mobile engagement solutions and Applications.	
11	Should support 16x BSSID per AP radio.	
12	The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio.	
13	Should support BPSK, QPSK, 16-QAM, 64-QAM, 256 QAM and 1024 QAM modulation types	

14	Access point Should support Power over Ethernet (PoE) 802.3af/at from day 1	
15	Intelligent Power Monitoring (IPM) to continuously monitor and report hardware energy consumption. AP can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.	
16	The AP should support Link aggregation (LACP) between both network ports for redundancy and increased capacity	
17	Access point should have option of external power adaptor as well.	
18	Access point should have console port.	
19	Must operate as a sensor for wireless IPS	
20	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services	
21	The Access Point should have the technology to improve downlink performance to all mobile devices.	
22	Access point must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	
23	AP mounting kit should be with locking mechanism so that AP cannot be removed without using special tools.	
24	AP should support standalone mode/ Inbuilt Virtual controller mode for specific requirements.	
25	The AP should support Supports priority handling and policy enforcement for unified communication apps, including Skype for Business with encrypted videoconferencing, voice, chat and desktop sharing	
26	The AP should support deep packet inspection to classify and block, prioritize, or limit bandwidth for thousands of applications in a range of categories	
27	The AP should support Spectrum analysis and capable of part-time or dedicated air monitoring, the spectrum analyzer remotely scans the 2.4GHz and 5GHz radio bands to identify sources of RF interference from 20MHz through 160MHz operation	
28	The Access point should support maximum ratio combining (MRC) for improved receiver performance	
29	The Access point should support cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance	

30	The Access point should support Space-time block coding (STBC) for increased range and improved reception	
31	The Access point should support Low-density parity check (LDPC) for high-efficiency error correction and increased throughput	
32	The Access point should support Transmit beam-forming (TxBF) for increased signal reliability and range	
33	The Access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices	
34	Feasible for AC Power adaptor for wireless access points with Indian style power plug	
35	Operating Temperature 0–40°C,	
	Mobility features	
1	Should support L2 and L3 wireless controller discovery	
2	WME Multimedia Extensions support 4 priority queues for voice, video, data and background traffic	
3	Should support 24 Simultaneous SSIDs	
4	Support EAP-TLS EAP-TTLS/MSCHAPv2 EAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM EAP-AKA EAP-FAST	
5	Should support Tx power of 22dBm or higher	
6	Solution should have support for Captive portal for guest authentication	
	Management features	
1	Solution should have managed by proposed controller from the same OEM only. AP must thin AP's & must not be available to manage standalone in any given condition.	
2	Should support web-based secured management GUI	
3	Support Wall mounting & ceiling mount options with included accessories from day 1	
	Interfaces for connectivity	
1	2 x 10/100/1000/2500/5000Base-T port supporting 2.5Gbps & 5Gbps speed and PoE-PD – 48Vdc 802.3at/bt	
2	DC power interface – 48V dc	
3	USB 2.0 host interface,Bluetooth 5 and Zigbee radio	

GUJARAT GAS

14. Annexure –III Technical specifications- Access point Type B

Indoor dual radio Wireless Access Point covers minimum distance of approx. 40-60 meter diagonal and suffice approx. 20-40 user load		
Sr No	**Specifications**	**Compliance (Yes/No)**
1	Access Point radio should be minimum dual/tri-radio 5GHz 4x4 MIMO with 4 spatial streams and 4x4 MIMO with 4 spatial streams on 2.4 Ghz radio. The AP should have Dual Radio 802.11ax access point with OFDMA and Multi-User MIMO (MU-MIMO)	
2	Access Point should be 802.11ax ready from day one and support WPA3 and Enhanced Open security from day one	
3	AP should have 2 x 10/100/1000 interface RJ45/SFP interface with 1 Console port have one SmartRate port (RJ-45, maximum negotiated speed 5Gbps) and one 2.5Gbps and 5Gbps speeds comply with NBase-T and 802.3bz specifications	
4	Access point should support Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices	
5	Access point should support OFDMA and MU-MIMO for enhanced multi-user efficiency	
6	Access point should IoT-ready Bluetooth 5 and Zigbee support	
7	Minimum aggregate data rate should be 3.55 Gbps or above	
8	Access Point can have integrated internal antenna	
9	The Max transit power of the AP + Antenna should be as per WPC norms for indoor Access Points. OEM to give a undertaking letter stating that the AP will configured as per WPC guidelines for indoor AP and also submit the WPC certificate showing approval.	
10	Access point should have Interna/External Bluetooth Low energy beacon to support advance location based services for Mobile engagement solutions and Applications.	
11	Should support at least 8x BSSID per AP radio.	
12	The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio.	
13	Should support BPSK, QPSK, 16-QAM, 64-QAM, 256 QAM and 1024 QAM modulation types	

14	Access point Should support Power over Ethernet (PoE) 802.3af/at from day 1	
15	Intelligent Power Monitoring (IPM) to continuously monitor and report hardware energy consumption. AP can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.	
16	The AP should support Link aggregation (LACP) between both network ports for redundancy and increased capacity	
17	Access point should have option of external power adaptor as well.	
18	Access point should have console port.	
19	Must operate as a sensor for wireless IPS	
20	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services	
21	The Access Point should have the technology to improve downlink performance to all mobile devices.	
22	Access point must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	
23	AP mounting kit should be with locking mechanism so that AP cannot be removed without using special tools.	
24	AP should support standalone mode/ Inbuilt Virtual controller mode for specific requirements.	
25	The AP should support Supports priority handling and policy enforcement for unified communication apps, including Skype for Business with encrypted videoconferencing, voice, chat and desktop sharing	
26	The AP should support deep packet inspection to classify and block, prioritize, or limit bandwidth for thousands of applications in a range of categories	
27	The AP should support Spectrum analysis and capable of part-time or dedicated air monitoring, the spectrum analyzer remotely scans the 2.4GHz and 5GHz radio bands to identify sources of RF interference from 20MHz through 160MHz operation	
28	The Access point should support maximum ratio combining (MRC) for improved receiver performance	
29	The Access point should support cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance	

30	The Access point should support Space-time block coding (STBC) for increased range and improved reception	
31	The Access point should support Low-density parity check (LDPC) for high-efficiency error correction and increased throughput	
32	The Access point should support Transmit beam-forming (TxBF) for increased signal reliability and range	
33	The Access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices	
34	Feasible for AC Power adaptor for wireless access points with indian style power plug	
35	Operating Temperature 0–40°C,	
	Mobility features	
1	Should support L2 and L3 wireless controller discovery	
2	WME Multimedia Extensions support 4 priority queues for voice, video, data and background traffic	
3	Should support 24 Simultaneous SSIDs	
4	Support EAP-TLS EAP-TTLS/MSCHAPv2 EAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM EAP-AKA EAP-FAST	
5	Should support Tx power of 22dBm or higher	
6	Solution should have support for Captive portal for guest authentication	
	Management features	
1	Solution should have managed by proposed controller from the same OEM only. AP must thin AP's & must not be available to manage standalone in any given condition.	
2	Should support web-based secured management GUI	
3	Support Wall mounting & ceiling mount options with included accessories from day 1	
	Interfaces for connectivity	
1	2 x 10/100/1000/2500/5000Base-T port supporting 2.5Gbps & 5Gbps speed and PoE-PD – 48Vdc 802.3at/bt	
2	DC power interface – 48V dc	
3	USB 2.0 host interface, Bluetooth 5 and Zigbee radio	

GUJARAT GAS

15. Annexure –IV Technical specifications- Access point Type C

Indoor dual radio Wireless Access Point covers minimum distance of approx. 30-40 meter diagonal and suffice approx. 10-20 user load		
Sr No	**Technical Specifications**	**Compliance (Yes/No)**
1	Access Point radio should be minimum 2X2 MIMO with 2 special stream on 2.4 Ghz and minimum 4x4 MIMO with 4 special streams 2.4 Ghz radio. The AP should have Dual Radio 802.11ax access point with OFDMA and Multi-User MIMO (MU-MIMO)	
2	Access Point should be 802.11ax ready from day one and support WPA3 and Enhanced Open security from day one	
3	AP should have 2 x 10/100/1000 interface RJ45/SFP interface with 1 Console port have one Smart Rate port (RJ-45, maximum negotiated speed 5Gbps) and one 2.5Gbps and 5Gbps speeds comply with NBase-T and 802.3bz specifications	
4	Access point should support Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices	
5	Access point should support OFDMA and MU-MIMO for enhanced multi-user efficiency	
6	Access point should IoT-ready Bluetooth 5 and Zigbee support	
7	Minimum aggregate data rate should be 3 Gbps or above	
8	Access Point can have integrated internal antenna	
9	The Max transit power of the AP + Antenna should be as per WPC norms for indoor Access Points. OEM to give a undertaking letter stating that the AP will configured as per WPC guidelines for indoor AP and also submit the WPC certificate showing approval.	
10	Access point should have Internal/External Bluetooth Low energy beacon to support advance location based services for Mobile engagement solutions and Applications.	
11	Should support at least 8 BSSID per AP radio.	
12	The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio.	
13	Should support BPSK, QPSK, 16-QAM, 64-QAM, 256 QAM and 1024 QAM modulation types	

14	Access point Should support Power over Ethernet (PoE) 802.3af/at from day 1	
15	Intelligent Power Monitoring (IPM) to continuously monitor and report hardware energy consumption. AP can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.	
16	The AP should support Link aggregation (LACP) between both network ports for redundancy and increased capacity	
17	Access point should have option of external power adaptor as well.	
18	Access point should have console port.	
19	Must operate as a sensor for wireless IPS	
20	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services	
21	The Access Point should have the technology to improve downlink performance to all mobile devices.	
22	Access point must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	
23	AP mounting kit should be with locking mechanism so that AP cannot be removed without using special tools.	
24	AP should support standalone mode/ Inbuilt Virtual controller mode for specific requirements.	
25	The AP should support Supports priority handling and policy enforcement for unified communication apps, including Skype for Business with encrypted videoconferencing, voice, chat and desktop sharing	
26	The AP should support deep packet inspection to classify and block, prioritize, or limit bandwidth for thousands of applications in a range of categories	
27	The AP should support Spectrum analysis and capable of part-time or dedicated air monitoring, the spectrum analyzer remotely scans the 2.4GHz and 5GHz radio bands to identify sources of RF interference from 20MHz through 160MHz operation	
28	The Access point should support maximum ratio combining (MRC) for improved receiver performance	
29	The Access point should support cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance	

30	The Access point should support Space-time block coding (STBC) for increased range and improved reception	
31	The Access point should support Low-density parity check (LDPC) for high-efficiency error correction and increased throughput	
32	The Access point should support Transmit beam-forming (TxBF) for increased signal reliability and range	
33	The Access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices	
34	Feasible for Ac Power adaptor for wireless access points with indian style power plug	
35	Operating Temperature 0–40°C,	
	Mobility features	
1	Should support L2 and L3 wireless controller discovery	
2	WME Multimedia Extensions support 4 priority queues for voice, video, data and background traffic	
3	Should support 24 Simultaneous SSIDs	
4	Support EAP-TLS EAP-TTLS/MSCHAPv2 EAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM EAP-AKA EAP-FAST	
5	Should support Tx power of 22dBm or higher	
6	Solution should have support for Captive portal for guest authentication	
	Management features	
1	Solution should have managed by proposed controller from the same OEM only. AP must thin AP's & must not be available to manage standalone in any given condition.	
2	Should support web-based secured management GUI	
3	Support Wall mounting & ceiling mount options with included accessories from day 1	
	Interface connectivity	
1	10/100/1000 Base-T Ethernet network interface (RJ-45)	
2	10/100/1000/2500Base-T port supporting 2.5Gbps speed and PoE-PD – 48Vdc 802.3af/at/bt	
3	DC power interface – 12V dc , USB 2.0 host interface	

16. Annexure - Schedule of Rates (SOR)

Sr. No.	Material/Service SAP Master Code*	Description	UoM	Quantity for requirement period
1	400000405	Indoor access point (wave2) with dual radio and multi MIMO streaming capabilities which tentatively covers minimum distance of 60-70 meter diagonal and suffice 40-60 user load, internal antennas, 2 x 10/100/1000 RJ45 port, BT / BLE. Ceiling/wall mount kit included. For power: 802.3at PoE and AC adapter SP-FAP200-PA., Ceiling/wall mount with 1 year of 24x7 support.	EA	30
2	400000405	Indoor access point (wave2) with dual radio and multi MIMO streaming capabilities which tentatively covers minimum distance of 50-60 meter diagonal and suffice 20-40 user load, internal antennas, 2 x 10/100/1000 RJ45 port, BT / BLE. Ceiling/wall mount kit included. For power: 802.3at PoE and AC adapter SP-FAP200-PA.Ceiling/wall mount with 1 year of 24x7 support.	EA	10
3	400000405	Indoor access point (wave2) with dual radio and multi MIMO streaming capabilities which tentatively covers minimum distance of 40-50 meter diagonal and suffice 10-20 user load, internal antennas internal antennas, 2 x 10/100/1000 RJ45 port, BT / BLE. Ceiling/wall mount kit included. For power: 802.3at PoE and AC adapter SP-FAP200-PA., Ceiling/wall mount with 1 year of 24x7 support.	EA	10
4	500320	Additional Contract of 24 X 7 to support Wireless controller and Indoor access points (50 N0s) - 4 Years	EA	4
5	400000404	Wireless controller (HA port and Management port) which cater minimum 100 access point seamlessly along with 1 year of support.	EA	1
6	902090	One Time Implementation charges	AU	1

Bidder seal & sign

GUJARAT GAS

17. Annexure V- List of locations for WIFI deployment

SR	GA Location	Location	AREA	Nos of WIFI	WIFI Type - A/B/C
1	AMRELI	AMRELI	VC Room	1	B
2	AMRITSAR	AMRITSAR	VC Room	1	B
3	Bharuch	Ankleshwar	THIRD FLOOR	3	A
4	Bharuch		FIRST FLOOR		A
5	Bharuch		SECOND FLOOR		A
6	Bharuch	BHARUCH	VC Room	1	A
7	Bharuch	DAHEJ	A BLOCK SECOND FLOOR	1	C
8	BHATINDA	BHATINDA	VC Room	1	C
9	BHAVNAGAR	BHAVNAGAR	VC room	1	A
10	BHUJ	BHUJ	VC Room	1	B
11	Corporate office	Ahmedabad Parimal	MANAGING DIRECTOR ROOM	7	A
12	Corporate office		SECOND FLOOR		A
13	Corporate office		CAFETERIA		A
14	Corporate office		THIRD FLOOR		A
15	Corporate office		SECOND FLOOR		A
16	Corporate office		FIRST FLOOR		A
17	Corporate office		FOURTH FLOOR		A
18	Corporate office	Ahmedabad Avdhesh	AVDESH HOUSE A wing	2	A
19	Corporate office		AVDESH HOUSE B wing		A
20	Corporate office	Ahmedabad GSFC	GSFC HOUSE	1	A
21	DAHOD	DAHOD	A BLOCK GROUND FLOOR	1	C
22	DNH	SILVASSA	VC Room	1	B
23	GANHINAGAR	GANDHINAGAR	VC Room	1	A
24	JAMNAGAR	JAMNAGAR	VC Room	1	A

SR	GA Location	Location	AREA	Nos of WIFI	WIFI Type - A/B/C
25	MORBI	MORBI	VC Room	1	A
26	NAVSARI	NAVSARI	VC Room	1	A
27	RAJKOT	RAJKOT	VC Room	1	A
28	SURAT	SURAT	ADMIN BUILDING	5	A
29	SURAT		ADMIN BUILDING THIRD FLOOR		A
30	SURAT		CUSTOMER CALL CENTER		A
31	SURAT		CENTRALISED CONTROL ROOM		A
32	SURAT		A BLOCK FIRST FLOOR		A
33	SURENDRANAGAR	SURENDRANAGAR	VC Room	1	A
34	THANE	THANE	VC Room	1	A
35	VALASAD	VAPI	VC Room	1	A
36	Valsad GA	Billimora	floor	1	B
37	Bhavnagar GA	Botad	floor	1	B
38	Gandhinagar GA	Chandkheda	floor	1	B
39	Nadiad GA	Dabhan	floor	1	A
40	Nadiad GA	Halol	floor	1	A
41	SURENDRANAGAR	Jamvadi	floor	1	B
42	Nadiad GA	Khambhat	floor	1	C
43	SURENDRANAGAR	Limdi	floor	1	C
44	Nadiad GA	Nadiad	floor	1	B
45	Valsad GA	Valsad	floor	1	B
46	Nadiad GA	Memnabad	floor	1	C
47	Valsad GA	Bhilad and Sarigam	floor	**1**	C
48	rajkot	Rajkot CNG Green	floor	**1**	C

49	Valsad GA	Umargam	floor	**1**	C
50	Valsad GA	pardi	floor	**1**	C