NATIONAL INSTITUTE OF TECHNOLOGY
ROURKELA – 769 008, ODISHA

Advertised Tender Enquiry

Department: Computer Centre

Tender Notice No: NITR/PW/CC/2020/63 **Dated: 01/06/2020**

To

Bidding Through
e-Procurement Portal of Ministry of HRD, Govt. of India
https://mhrd.euniwizarde.com/

Important Dates

Event	Date	Time
Pre-bid Conference	**NA**	**NA**
Last Date of submission of bid	**24/06/2020**	**11:00 AM**
Date of opening of techno-commercial bid	**25/06/2020**	**11:00 AM**

Dear Sir,

We intend to purchase the commodities specified below and invite quotations in accordance with the terms and conditions detailed in the bid document. If you are interested, kindly send your offer with prices and complete terms within the time mentioned above.

For any query, you may contact

Attention:-
Prof. Bibhudatta Sahoo
HOD, Computer Centre
NATIONAL INSTITUTE OF TECHNOLOGY
ROURKELA – 769 008, ODISHA
Phone : (0661) – 246-2671

E-mail: hod-cc@nitrkl.ac.in
eprocurementcell@nitrkl.ac.in

Yours sincerely,

Sd/-
Prof. Bibhudatta Sahoo
HOD, Computer Centre

Encl:

(1) Schedule of requirement, specifications, dates etc.

(2) Bid document containing detail terms and conditions.

1. **Schedule of requirements**

Sl. No.	Description of Goods	Quantity
1.	Wireless Controller (In Higher Availability)	2
2.	Access Point Type 1(Low Density)	40
3.	Access Point Type 2 (High Density)	80

2. **Specifications and allied Technical Details**

As per Annexure – I

3. **Format of Quotation**

It is a two-part bid with separate techno-commercial and price bids

4. **The bid should be submitted through**

https://mhrd.euniwizarde.com/HomePage/ebidSites?siteName=mhrd

5. **Quotations should be valid for a period of 90 days from the closing date of opening of techno-commercial bid.**

6. **Some important dates**

i. Pre-bid Conference	Date: NA	Time: NA
ii. Last date for submission of bid	Date: 24/06/2020	Time: 11:00 AM
iii. Opening of Techno-commercial bid	Date: 25/06/2020	Time: 11:00 AM

7. **Warranty:** 5 years comprehensive warranty from OEM.

8. **Technical Evaluation Criteria**: As per the detailed equipment technical specifications given in Annexure –I. If required, the bidder may be asked to provide clarification regarding the technical aspects.

9. **Other Qualification criteria:**

Eligibility of Bidders:

i. Firms should quote products that are not expected to go into end of sale in next 3 years and end of support in next 5 years

ii. The bidder must have valid authorization from the OEM specific to this tender. Documentary proof regarding this must be attached.

iii. The bidder should be a Private/ Public Limited company registered under the Companies Act, 1956 or a registered firm. The company/firm should be in existence for more than 5 years as on date. Copy of Certificate of incorporation/commencement should be submitted.

iv. The bidder should have GST registration. GST details should be submitted.

v. The average annual financial turnover of the tenderer for last three consecutive financial years ending on 31st March, 2019 should be minimum **Rs 50 Crores**. Copy of Audited Balance Sheet and P/L Account to be submitted.

vi. The bidder must have supplied & installed Wireless Network Solution in any Govt./PSU/Education Institute/Corporate in India in last 5 years ending on 31st March, 2019. The minimum order value should be INR 50 lac. Copy of the PO & Installation report to be submitted.

vii. Considering primary support from the bidder, the bidder should have office cum service support setup of 24X7 customer support service form smooth support in Eastern India. Supporting documents like office address and phone no. should be submitted.

viii. The bidder should have valid ISO 9001 & 27001 certifications. Copy of the same to be submitted.

ix. Bidders must submit a declaration on their letter head that they are not black listed in any Govt. body, undertaking, and PSU or Autonomous bodies. If found the declaration is false their offer will be out rightly rejected and their EMD amount will be forfeited.

x. The Vendor shall provide the following information with the bid to provide background information on vendor to Tender Committee.

a. ***The list of clients*** (contact details of a person phone/ mob. no. with e-mail ids should be attached) where the bidder/OEM had supplied the similar type of materials (as mentioned in schedule of requirements) with successful installation in last three years.

b. ***Quality certificate*** from a recognized institution for their manufacturing/ assembly/ system integration facilities anywhere located in India or abroad.

c. ***Delivery period*** from the date of placement of the Purchase Order.

d. ***Customer support*** strength by the vendor.

e. Possible quicker ***availability*** of the vendor when problem occurs.

f. ***Mode of handling complains*** (whether by fault ticket/complain even by email or by phone etc.)

g. ***Validity period*** of cost of equipment.

h. ***Necessary documents*** as mentioned in **Annexure -II**

i. Any other points may deemed fit by the committee at time of technical evaluation of bid documents.

j. Details of Hardware included in offer.

k. Details of Technical Specification and other specifications so as to enable technical assessment of the proposal. Unpriced bid document exactly same as the price bid with full break up without the costs mentioned.

10. **Financial Bid Evaluation Criteria:** The comparison will be made for the award of contract on the overall price basis.

11. (a) All prices to be quoted on FOR basis (NIT Rourkela) in INR.

(b) GST: GST should be charged at applicable rates against DSIR certificate.

12. **Bid Security (EMD) and Tender Cost: EMD (Earnest Money Deposit)** of **INR 1,00,000/- (Rupees One Lacs only)** through online mode and Tender cost (Non-refundable) through online mode for **INR 1,000/- (Rupees One Thousand only)**. The EMD (Earnest Money Deposit) of unsuccessful bidders should be returned to them at the earliest and latest on or before the 30th days after the award of the contract. EMD shall bear no interest. Any bid without accompanying with EMD & Tender Cost is liable to be treated as non-responsive and rejected.

13. **Performance Security: 5% of contract value** in shape of Bank Guarantee/Demand Draft (DD) in favor of Director, NIT Rourkela payable at Rourkela from any Scheduled Commercial Bank except Co-operative and Gramin bank. Performance security should remain valid for a period of 60 days beyond the date of completion of all contractual obligations of the supplier including warranty obligation. And EMD (Earnest Money deposit) amount of successful bidder will be returned after the receipt of performance security in case of award of contract to successful bidder.

14. Please send your quotations through
https://mhrd.euniwizarde.com/HomePage/ebidSites?siteName=mhrd

15. For technical details, you may contact

Prof. Bibhudatta Sahoo
HOD, Computer Centre
National Institute of Technology, Rourkela – 769 008
Ph. No: 0661-246-2671
Email Id: bdsahu@nitrkl.ac.in

NB: ***Please furnish your Dealership Certificate (must) and Proprietary Nature Certificate (If applicable)***

NATIONAL INSTITUTE OF TECHNOLOGY ROURKELA – 769 008, ODISHA

BID DOCUMENT

1. Instructions to the bidders

1.1 Bids are invited on behalf of the Director, National Institute of Technology (NIT), Rourkela – 769008, Odisha, from the intending bidders for supply of the goods/stores/ equipments for the Institute as detailed in the enquiry letter.

1.2 The bidders should quote their offer/rates in **BOQ** in clear terms without ambiguity.

1.3 In case of any discrepancy between the rates in figures and that in words, the rate in words will be accepted as correct.

1.4 The last date for receipt of the bid is marked in the enquiry.

1.5 The Bid should be uploaded in https://eprocure.gov.in/eprocure/app Please follow the guideline of the site.

1.6 If a prospective bidder requires any clarification in regard to the bidding documents, he may make a request the concerned officer or faculty member at least 15 days before the deadline for receipt of bids.

1.7 Bids received after the deadline of receipt indicated in Para 1.4 above shall not be taken into consideration.

1.8 Each bidder shall submit only one bid. A bidder, who submits more than one bid, shall be disqualified and considered nonresponsive.

1.9 (In respect of high value plant, machinery etc. of a complex and technical nature). The bids may be submitted in two parts, viz., techno-commercial bid and financial bid.

1.10 The bidder has to sign in full at all pages of the scanned part of the bidding document. No over-writing in those pages are acceptable.

1.11 Bidders registered with any of the following agencies/ bodies as per Public procurement policy for Micro & Small Enterprises (MSE) order 2012 are exempted categories from payment of EMD provided that the registration Certificate issued by any one of these below mentioned agencies must be valid as on close date of tender. Micro small or medium enterprises who have applied for registration or renewal of registration with any of these agencies/bodies but have not obtained the valid Certificate as on close date of tender are not eligible for exemption.

i) Khadi and Village Industries Commission (KVIC)

ii) National Small Industries Corporation (NSIC)

iii) Any other body specificed by Ministry of MSME/GOI

2. INSTRUCTIONS FOR ONLINE BID SUBMISSION

The bidders are required to submit soft copies of their bid electronically on the e-Wizard Portal (https://mhrd.euniwizarde.com) using valid Digital Signature Certificates. Below mentioned instructions are meant to guide the bidders for registration on the e-Wizard Portal, prepare their bids in accordance with the requirements and submitting their bids online on the e-Wizard Portal. For more information, bidders may visit the e-Wizard Portal https://mhrd.euniwizarde.com

2.1 REGISTRATION PROCESS ON ONLINE PORTAL

1. Bidders to enroll on the e-Procurement module of the portal https://mhrd.euniwizarde.com by clicking on the link "Bidder Enrollment". Enrolment on the e-wizard Portal.
2. The bidders to choose a unique username and assign a password for their accounts. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the e-Wizard Portal. Bidders to register upon enrolment their valid Digital Signature Certificate (Only Class III Certificates with signing + encryption key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / TCS / nCode / eMudhra etc.), with their profile.
3. Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSCs to others which may lead to misuse. Foreign bidders are advised to refer "DSC details for Foreign Bidders" for Digital Signature requirements on the portal.
4. Bidder then logs in to the site through the secured log-in by entering their user ID / password and the password of the DSC / eToken.
5. Bidders must ensure that they have the latest version of Java installed in their local system.
6. The scanned copies of all original documents should be uploaded in pdf format on portal https://mhrd.euniwizarde.com
7. After completion of registration payment, you need to sends your acknowledgement copy on our help desk mail id ewizardhelpdesk@gmail.com for activation of your account.

2.2 TENDER DOCUMENTS SEARCH

1. Various built in options are available in the e-Wizard Portal to facilitate bidders to search active tenders by several parameters. These parameters include Tender ID, organization, location, date, value, etc.
2. There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as organization name, form of contract, location, date, other keywords etc. to search for a tender published on the Online Portal.
3. Once the bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective 'My Tenders' folder. This would enable the Online Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.
4. The bidder should make a note of the unique Tender ID assigned to each tender, in case they want to obtain any clarification / help from the Helpdesk.

2.3 BID PREPARATION

1. Bidder should take into account any corrigendum published on the tender document before submitting their bids.
2. Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.

3. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid.
4. Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / PNG etc. formats. Bid documents may be scanned with 100 dpi with black and white option.

2.4 BID SUBMISSION

1. Bidder to log into the site well in advance for bid submission so that he/she upload the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
2. The bidder to digitally sign and upload the required bid documents one by one as indicated in the tender document.
3. Bidder to select the payment option as Online" to pay the tender fee/ EMD wherever applicable and enter details of the instrument.
4. A standard BoQ format has been provided with the tender document to be filled by all the bidders. Bidders to note that they should necessarily submit their financial bids in the prescribed format and no other format is acceptable. Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BOQ format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BOQ file, open it and complete the unprotected cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BOQ file is found to be modified by the bidder, the bid will be rejected.
5. The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.
6. All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data, which cannot be viewed by unauthorized persons until the time of bid opening.
7. The uploaded tender documents become readable only after the tender opening by the authorized bid openers.
8. Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.
9. Kindly add scanned PDF of all relevant documents in a single PDF file of compliance sheet.

2.5 AMENDMENT OF BID DOCUMENT

At any time prior to the deadline for submission of proposals, the institutions reserve the right to add/modify/delete any portion of this document by issuance of a Corrigendum, which would be published on the website and will also be made available to the all the Bidder who have been issued the tender document. The Corrigendum shall be binding on all bidders and will form part of the bid documents.

2.6 ASSISTANCE TO BIDDERS

1. Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.

2. e-Procurement support any queries relating to the process of online bid submission or queries relating to e-Wizard Portal in general may be directed to the **24x7 e-Wizard Helpdesk**. **The contact number for the helpdesk is 011-49606060, 23710092, 23710091, Er Sanjeet Kumar Jha (+91-8882495599), 9355030626. Amit Kumar Jha 9355030627, 9205898226**

   Email Support:

   For any eProcurement Application Service Requests and Technical issues related to Document Uploads, Tender Publishing, Issue of Corrigendum, Encryption/Decryption Key issues, Bid Evaluation, Bidder Login issues, New Registration issues, Key Uploads, DSC Key installation, Bid Submission, system users may please mail to Sanjeet Kumar Jha ewizardsanjeet.kumar@gmail.com

3. Conditions of the bid

3.1 The rates quoted should preferably be net, inclusive of all taxes and duties, packing, forwarding, freight, Insurance and all other incidental charges. In case these charges are quoted extra in addition to the quoted rates, the amount thereof or Ad Valorem rate must be specified. Packing, forwarding, freight etc., when quotes separately are reimbursable at actuals. If external agencies are employed, their receipts must be enclosed with the invoice.

3.2 Duties and Taxes are to be quoted separately. Ad Valorem rates thereof should be clearly indicated with reference to the relevant Acts and Rules.

It may be noted that the Institute is availing custom duty exemption in terms of Notification No. 51/96 – Customs dt. 23.07.1996, Notification No. - 47/2017- Integrated Tax (Rate) dt. 14.11.2017 and Notification No- 45/2017 – Integrated tax (Rate) dt. 14/11/2017 & Notification No. - 45/2017- Central tax (Rate) dt. 14.11.2017, Notification No. - 45/2017- Union Territory Tax (Rate) dt. 14/11/2017 [Vide DSIR, Ministry of Science and Technology, Government of India, Registration No.: TU/V/RG- CDE (227)/2016, dated: 13.11.2018]

3.3 The goods are required to be delivered at the indenting Department of NIT, Rourkela, and must be reached within **90 days** from the date of placement of the supply of order under the risk and arrangement of the bidder and offers with delivery beyond the above period shall be treated as unresponsive. In case the delivery time is higher, the same must be mentioned clearly in the quotation.

3.4 The bid should remain valid for a period of **90 days** from the date of opening. In case your offer has a different validity period that should be clearly mentioned in the quotation.

3.5 Conditional discount, if any, offered by the bidder shall not be considered at the time of evaluation.

3.6 The goods offered should strictly conform to the specification and technical details mentioned in Annexure-I.

3.7 The Institute may like to conduct pre-dispatch inspection of goods, where applicable.

3.8 Period of guarantee/warranty, where applicable, should be specified in the bid.

3.9 If the successful bidder, on receipt of the supply order, fails to execute the order within the stipulated period, in full or part, it will be open to the Director, NIT Rourkela to recover liquidated damage from the firm at the rate of 1 percent of the value of undelivered goods per month or part thereof, subject to a maximum of 5 percent of the value of undelivered goods. Alternatively, it will also be

opened to the Director, to arrange procurement of the required goods from any other source at the risk and expenses of the bidder.

3.10 The successful bidder may be required to execute a contract, where applicable.

3.11 The bidder has to furnish up to date Income Tax Clearance Certificate along with the bid.

3.12 Payment (100 percent) will be made by Account Payee Cheque/Bank Draft, within 30 days from the date of receipt of the goods in good condition or receipt of the bill, commissioning of the equipment, where applicable, whichever is later/latest.

3.13 In case of Advance payment, the payment will be made on either in Foreign Demand Draft or Wire Transfer only. The proforma invoice copy need to be sent for advance payment.

3.14 In the event of any dispute arising out of the bid or from the resultant contract, the decision of the Director, NIT, Rourkela shall be final.

3.15 The bid document/resultant contract will be interpreted under Indian Laws.

Annexure-I

General Clauses:

1. Firms should quote products that are not expected to go into end of sale in next 3 years and end of support in next 5 years.

2. Wireless controller, Access Points and the fibre modules (If required for the deployment) should be from the same OEM.

3. The OEM should have R&D centre in India. The OEM should have at least 2 RMA depot in India and should have India Toll free number with India TAC centre - reflected on the official website.

4. The OEM should be globally reputed and presence/recommendation in Latest Gartner report in leader quadrant for wired and wireless will be preferred.

5. **Warranty:** 5 years comprehensive warranty from OEM. Should provide advance replacement of the faulty/defective devices on Advance Hardware Replacement (AHR) basis. Replacement should be provided from Indian Warehouse within 10 days of complain reported. Replacement expenses (pickup of faulty device and delivery of the replacement device) will be completely on the OEM.

6. **Technical Support:** 24x7 or 8x5 technical support (telephoney and web support) must be provided by the OEM from Support Centre in India.

7. **Configuration & Installation:** Configuration & Installation of Wireless Controller and Access Points must be done by the certified engineer of OEM.

8. **Training:** 2 days on site training on Configuration & Maintenance of Wireless Controller and Access Points must be provided by the certified trainer of OEM.

Technical Specification of Load Balancer

1. Access Point Type 1 (Low density)

S. NO	SPECIFICATION
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave-2 or higher.
2	AP should Support MU-MIMO 256QAM.
3	Mounting bracket should be supplied with every AP and should be from the AP OEM
4	LED should be available for activity indication
5	Must have 1x IEEE 802.3 Gigabit Ethernet auto-sensing with One console Serial Port.
6	The access point must have integrated antenna or External Antenna
7	Operating temperature should be in the range 0° C to 40° C
8	Should support 802.11 a/b/g/n/ac standard.
9	AP should have Dual band radios; supports 256-QAM 2X2 MIMO with 2 Spatial Streams on both radio or higher.
10	AP should support 20, 40, and 80 MHz Channels
11	AP have minimum 1100 Mbps data rates on dual concurrent radio operations or better.
12	Support Packet Aggregation (AMSDU, AMPDU) Reduced Interface Spacing
13	Should support MIMO Power Save (Static and Dynamic) Advanced forward error correction coding: STBC, LDPC
14	should support 802.11ac transmit beamforming Maximal Ratio Combining (MRC)

15	Maximum conducted transmit power shall be 20 dBm on both 2.4 and 5 GHz with
	two antennas and EIRP complying to regulatory requirements
16	Should support minimum 4dBi on 2.4 GHz band and 6 dBi on 5GHz band or better
17	AP should support Radio Share and Off-Channel Scan, Enables a single to perform double duty as an access point and a sensor.
18	AP should Increases reliability and resilience of the wireless network to support mission-critical applications.
19	Should support Load Balancing, Pre-Emptive Roaming, and Rate Scaling
20	Should support Gap-Free Security, Protects your network 24x7x365 with integrated security features.
21	Should support an unprecedented number of users and applications—including voice and video—allowing you to confidently deploy Bring Your Own Device (BYOD) initiatives and empower new workgroups with mobility.
22	AP should support comprehensive integrated security features that include layer 2-7 stateful packet filtering firewall, AAA RADIUS services, a VPN gateway and location-based access control.
23	The AP secures all your wireless transmissions, ensuring compliance with the government or industry regulations your business may be subject to, such as PCI in retail and HIPAA in healthcare
24	AP should support Air Defense Network Assurance features
25	AP should support dedicated sensor, Radio Share and Off-Channel Scan features work hand-in-hand to allow either or both radios to carry client data and act as a sensor, providing dual-band sensing without adding cost.
26	AP should support for Voice-over-wireless LAN (VoWLAN) quality of service (QoS) ensures toll quality, even with many simultaneous calls on a single access point.
27	AP should easily provide hotspot and guest access
28	AP should be capable of managed by controller, Controller-less and Standalone Mode.
29	AP should be capable of serving the client, if Hardware controller will be faulty or power fail without any human intervention.
30	AP should support Layer 3 routing, 802.1q, DynDNS, DHCP server/client, BOOTP client, PPPoE and LLDP
31	Should support Stateful Firewall, IP filtering, NAT, 802.1x, 802.11i, WPA2, WPA Triple-Methodology Rogue Detection: 24x7 dual-band WIPS sensing, on-board IDS, and secure guest access (hotspot) with captive portal, IPSec, and RADIUS Server
32	AP should support captive portal with time-based access, Customize Guest page and must have option for self-guest registration options, so that guest can automatic register self from day 1. Bidder should provide the external supported device also if required.
33	should support WMM, WMM-UAPSD, 802.1p, DiffServ, and TOS
34	Should support wireless medium Direct Sequence Spread Spectrum (DSSS), Orthogonal Frequency Division Multiplexing (OFDM), and Spatial Multiplexing (MIMO)
35	Should support IEEE 802.11a/b/g/n/ac, 802.11d/r/v/k/w/e/d and 802.11i WPA2, WMM, and WMM-UAPSD, L2TPv3, Client VPN, MESH and Captive Portal server
36	AP should have Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac and Safety- UL / cUL 60950-1, IEC / EN60950-1, UL2043, RoHS
37	Should have Radio Approval FCC (USA), EU, TELEC
38	Should support receiver sensitivity up to -97 or better.
39	AP should support Dynamic Vlan, Bridge and Tunnel Vlan, Vlan Load Balancing and Vlan Pool.
40	AP should support User, AP and Band Load Balancing.
41	Ap should support customized WIPS signature and Rouge AP detection and Rouge AP Termination manual and automatic.

2. Access Point Type 2 (High density)

S. NO	SPECIFICATION
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave-2 or higher.
2	AP should Support MU-MIMO 256QAM.
3	Mounting bracket should be supplied with every AP and should be from the AP OEM
4	LED should be available for activity indication
5	Must have 1x IEEE 802.3 Gigabit Ethernet auto-sensing with One console Serial Port.
6	The access point must have integrated antenna or External Antenna
7	Operating temperature should be in the range 0° C to 40° C
8	Should support 802.11 a/b/g/n/ac standard.
9	AP should have Dual band radios; supports 4X4 MIMO with 4 Spatial Streams on 802.11a/802.11n/802.11ac or higher.
10	AP should support 20, 40, and 80 MHz Channels
11	AP have minimum 2300 Mbps data rates on dual concurrent radio operations or better.
12	Support Packet Aggregation (AMSDU, AMPDU) Reduced Interface Spacing
13	Should support MIMO Power Save (Static and Dynamic) Advanced forward error
	correction coding: STBC, LDPC
14	should support 802.11ac transmit beamforming Maximal Ratio Combining (MRC)
15	Maximum conducted transmit power shall be 28 dBm on both 2.4 and 5 GHz with two antennas and EIRP complying to regulatory requirements
16	Should support minimum 4dBi on 2.4 GHz band and 6 dBi on 5GHz band or better
17	AP should support Radio Share and Off-Channel Scan, Enables a single to perform double duty as an access point and a sensor.
18	AP should Increases reliability and resilience of the wireless network to support mission-critical applications.
19	Should support Load Balancing, Pre-Emptive Roaming, and Rate Scaling
20	Should support Gap-Free Security, Protects your network 24x7x365 with integrated security features.
21	Should support an unprecedented number of users and applications—including voice and video—allowing you to confidently deploy Bring Your Own Device (BYOD) initiatives and empower new workgroups with mobility.
22	AP should support comprehensive integrated security features that include layer 2-7 stateful packet filtering firewall, AAA RADIUS services, a VPN gateway and location-based access control.
23	The AP secures all your wireless transmissions, ensuring compliance with the government or industry regulations your business may be subject to, such as PCI in retail and HIPAA in healthcare
24	AP should support Air Defense Network Assurance features
25	AP should support dedicated sensor, Radio Share and Off-Channel Scan features work hand-in-hand to allow either or both radios to carry client data and act as a sensor, providing dual-band sensing without adding cost.
26	AP should support for Voice-over-wireless LAN (VoWLAN) quality of service (QoS) ensures toll quality, even with many simultaneous calls on a single access point.
27	AP should easily provide hotspot and guest access
28	AP should be capable of managed by controller, Controller-less and Standalone Mode.
29	AP should be capable of serving the client, if Hardware controller will be faulty or power fail without any human intervention.
30	AP should support Layer 3 routing, 802.1q, DynDNS, DHCP server/client, BOOTP client, PPPoE and LLDP
31	Should support Stateful Firewall, IP filtering, NAT, 802.1x, 802.11i, WPA2, WPA Triple-Methodology Rogue Detection: 24x7 dual-band WIPS sensing, on-board IDS, and secure guest access (hotspot) with captive portal, IPSec, and RADIUS Server

32	Ap should support captive portal with time-based access, Customize Guest page and must have option for self-guest registration options, so that guest can automatic register self from day 1. Bidder should provide the external supported device also if required.
33	should support WMM, WMM-UAPSD, 802.1p, DiffServ, and TOS
34	Should support wireless medium Direct Sequence Spread Spectrum (DSSS), Orthogonal Frequency Division Multiplexing (OFDM), and Spatial Multiplexing (MIMO)
35	Should support IEEE 802.11a/b/g/n/ac, 802.11d/r/v/k/w/e/d and 802.11i WPA2, WMM, and WMM-UAPSD, L2TPv3, Client VPN, MESH and Captive Portal server
36	AP should have Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac and Safety- UL / cUL 60950-1, IEC / EN60950-1, UL2043, RoHS
37	Should have Radio Approval FCC (USA), EU, TELEC
38	Should support receiver sensitivity up to -97 or better.
39	AP should support Dynamic Vlan, Bridge and Tunnel Vlan, Vlan Load Balancing and Vlan Pool.
40	AP should support User, AP and Band Load Balancing.
41	Ap should support customized WIPS signature and Rouge AP detection and Rouge AP Termination manual and automatic.
42	Wireless controller, Access Points and the fibre modules (If required for the deployment) should be from the same OEM. The OEM should have R&D centre in India. The OEM should have atleast 2 RMA depot in India and should have India Toll free number with India TAC centre - reflected on the official website. The OEM should be globally reputed and presence/recommendation in Latest Gartner report in leader quadrant for wired and wireless will be preferred.

2. Wireless Controller

S. NO	SPECIFICATION
1	The OEM should be globally reputed and presence/recommendation in Latest Gartner report in leader quadrant for wired and wireless will be preferred.
2	Proposed Solution Controller & AP should be of the same OEM.
3	Controller should have 1U rack size with minimum 4 nos. 10/100/1000 Base-T Port.
4	Controller should support min. 256 AP from Day 1 and upgradable up to 500 AP without changing Hardware.
5	Controller should support minimum up to 16K Client.
6	Should have at least with 4GB RAM and 32 GB SSD or more.
7	Controller should support 256 WLANs.
8	Controller should support IPV4 and IPV6 from day 1.
9	Controller architecture offers a software-defined networking (SDN)-ready operating system that can distribute controller functionality to every access point in your network
10	All wireless LAN infrastructure can work together to ensure every transmission is routed through the most efficient path, every time.
11	Solutions should have with Maximum network uptime and security with minimal management. And true seamless and dependable mobility for users.
12	Should supports all Wi-Fi protocols, including 802.11a/b/g/n/ac, allowing to a cost-effective migration plan based on the needs of business.
13	Solutions should support from a small WLAN network in a single location to a large multi-site network
14	Solution should be ready to support for all type of deploy infrastructure, i.e. standalone independent access points or adaptive access points that can be adopted by a controller but can switch to independent mode; virtual controllers; physical controllers in branch offices, the network operating centre (NOC) or the cloud from day 1
15	Controller and access point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time **for Staff/ Employee and Guest Traffic.**
16	Controller should support hierarchical management that delivers a new level of management simplicity and resiliency by enabling controllers to manage other controllers and access points,
17	Controller shall have comprehensive security capabilities keep network and data safe, ensuring compliance with PCI, HIPAA and other government and industry security regulations.
18	Controller should support Mesh connectivity for Large Indoor and Outdoor Space, where not have any possibility to reach the cable.
19	Support single powerful windowpane enables for zero touch infrastructure deployment
20	Provide visibility & control over layer-7 applications with an embedded DPI engine that inspects every flow of every user at the access point.
21	Controller is capable of detecting and identifying thousands of applications real time.
22	Should have options to configure your access points to report this real-time, network statistics to the NMS
23	Support features so that Network administrators can get in-depth insight into every dimension of the network including layer-7 application visibility, client devices, device & OS types and users.
24	Administrators can discern, at a glance, the top applications by usage or by count at every level of the network from site level to access points and clients.
25	System should be capable of enables all WLAN infrastructure with the intelligence required to work together to determine the most efficient path for every transmission
26	Solutions should be capable to route all traffic through a controller is eliminated, along with the resulting congestion and latency, resulting in higher throughput and superior network performance.

27	All controller feature should available at the access layer, they remain available even when the controller is offline, for example, due to a WAN outage, ensuring site survivability and extraordinary network resilience.
28	Controller have capability to enables the creation of highly reliable networks, with several levels of redundancy and failover mechanisms to ensure continuous network service in case of outages
29	AP should support APs in remote sites coordinate with each other to provide optimized routing and self-healing, delivering a superior quality of experience for operational/business-critical applications.
30	When APs lose communication with the controller, they continue to function, able to bridge traffic while still enforcing QoS and security policies, including stateful inspection of Layer2 (locally bridged) or Layer 3 traffic.
31	Controller should have built-in DHCPv4 and DHCPv6 server to serve the IP address to client.
32	should support AAA server and routing protocols like policy-based routing and OSPF.
33	Should support STP, RSTP, MSTP and Link Aggregation.
34	Access Point and controller should support CLI and GUI for manage or troubleshoot the Network.
35	Solutions should able to show the health & inventory report of Client, Access point and Controller.
36	An administrator can capture connected client packet data based on the packet's address type or port on which received.
37	Should support 802.1x authentication and providing the capability to permit or deny connectivity based on user or device identity from day 1.
38	Controllers and service platforms must support WIPS to provides continuous protection against wireless threats, Bidder should quote all licenses from day 1.
39	should detect and locate unauthorized AP devices, able to block device using manual termination, air lockdown or port suppression.
40	Controllers and service platforms support dedicated sensor devices, designed to actively detect and locate unauthorized AP devices
41	An access point support CPLD (complex programmable logic device) to manage power.
42	CPLD determines the maximum power provided by the POE device and the budget available to the access point.
43	Should support IPV4 and IPV6 Firewall Rules.
44	Controller should support Virtual Interface to a controller or service platform or provide to layer 3 service on a VLAN
45	Controller should support Bonjour for Apple's implementation of zero configuration networking (Zeroconf).
46	Controller must have support 802.1s, 802.1p, RA Guard, 802.11r, 802.11w, 802.11s
47	Should support A highly-scalable built-in captive portal server with customizable pages, Pages can be customized easily for the form factor of the target device like smartphones, tablets, and laptops and also have options to hosted on an external web server.
48	support Authentication/accounting via external RADIUS server or built-in guest user database
49	support Mobile-friendly Web portal Customizable templates (Colour, Banner with preview option)
50	Includes support for bandwidth tracking and rate limiting/enforcement
51	Should have provide Guest Self Registration, Device Registration, Registration using Social Logins, Customizable Registration Form with support for Name, Email, Mobile, Member, DOB, Age, Gender, and more. Bidder can go with external device to achieve this features.
52	should support Passcode notification through email, SMS, or SMS through SMTP, Built-in Analytics, Redirection for Proxy Ports, Device fingerprinting, Dynamic VLAN support, Walled Garden (DNS or Host IP white list), Granular day of week and time of day access.

53	To prevent congestion in the network, and ensure that mission critical traffic is not impacted, controller provides the capability to limit traffic per user, or enable rate limiting per WLAN, so that all users on that WLAN are rate-limited.
54	Clients are distributed among APs on association by client count or AP throughput, which is useful for dense deployments, such as conferences and stadiums. Neighbouring APs are automatically computed and do not require manual identification.
55	Allows a web admin to generate and print a voucher for a guest user that grants the user access for a specified period of time. Contains the capability to generate vouchers in bulk for multiple users. Useful in retail and enterprise guest access scenarios, where admins want to pre-generate these vouchers to be handed out later
56	Controller Provides the following native capabilities: Extensive WIPS Event Detection, Customized WIPS Signatures, Device Categorization, Unauthorized AP Detection and Anomaly Analysis with Client Blacklisting. Rogue AP classification using wired side detection, termination, and rogue detection of APs leaking wired traffic from a sanctioned network supported both with part-time scanning and off-channel scanning
57	Controller should support layer 2 and at layer 3 (IP), Application Layer Gateways, Association ACL, Centralized Association ACL, Client Disassociate on Excessive Denies, DHCP Broadcast to Unicast Conversion, Dos Attack Detection, Dynamic ARP Inspection (DAI), Hole 196 Detection/Protection, IPv4 ACL and Rules, MAC ACL and Rules, Per VLAN Enable/Disable, Rogue DHCP Server Detection, Storm Controls.
58	Controller should have Firewall policy enforcement based on user roles, besides the standard firewall policies by subnet, port, etc. Role can be assigned based on various parameters, such as AP Location, Active Directory Attributes, OpenLDAP Attributes, Authentication State, Authentication Type, DHCP Fingerprint, Encryption Type, Group Membership, MAC Address, SSID Name and User Defined LDAP Attributes.
59	WLAN client should work continuously without any changes required if Hardware controller will be fail or Power Off

Annexure-II

Sl. No.		Page No. of the Bid Document
1	**Eligibility:**	
a.	Firms should quote products that are not expected to go into end of sale in next 3 years and end of support in next 5 years	
b.	The bidder must have valid authorization from the OEM specific to this tender. Documentary proof regarding this must be attached.	
c.	The bidder should be a Private/ Public Limited company registered under the Companies Act, 1956 or a registered firm. The company/firm should be in existence for more than 5 years as on date. Copy of Certificate of incorporation/commencement should be submitted.	
d.	The bidder should have GST registration. GST details should be submitted.	
e.	The average annual financial turnover of the tenderer for last three consecutive financial years ending on 31st March, 2019 should be minimum **Rs 50 Crores**. Copy of Audited Balance Sheet and P/L Account to be submitted.	
f.	The bidder must have supplied & installed similar solution i.e. load balancer in any Govt./PSU/Education Institute/Corporate in India in last 5 years ending on 31st March, 2019. The minimum order value should be INR 30 lac. Copy of the PO & Installation report to be submitted.	
g.	Considering primary support from the bidder, the bidder should have office cum service support setup of 24X7 customer support service form smooth support in Eastern India. Supporting documents like office address and phone no. should be submitted.	
h.	The bidder should have valid ISO 9001 & 27001 certifications. Copy of the same to be submitted.	
i.	Bidders must submit a declaration on their letter head that they are not black listed in any Govt. body, undertaking, and PSU or Autonomous bodies. If found the declaration is false their offer will be out rightly rejected and their EMD amount will be forfeited.	

4. Technical compliance for Access Point Type 1(Low density)

S. NO	SPECIFICATION	Page No. of the Bid Document
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave-2 or higher.	
2	AP should Support MU-MIMO 256QAM.	
3	Mounting bracket should be supplied with every AP and should be from the AP OEM	
4	LED should be available for activity indication	
5	Must have 1x IEEE 802.3 Gigabit Ethernet auto-sensing with One console Serial Port.	
6	The access point must have integrated antenna or External Antenna	
7	Operating temperature should be in the range 0° C to 40° C	
8	Should support 802.11 a/b/g/n/ac standard.	
9	AP should have Dual band radios; supports 256-QAM 2X2 MIMO with 2 Spatial Streams on both radio or higher.	
10	AP should support 20, 40, and 80 MHz Channels	
11	AP have minimum 1100 Mbps data rates on dual concurrent radio operations or better.	
12	Support Packet Aggregation (AMSDU, AMPDU) Reduced Interface Spacing	
13	Should support MIMO Power Save (Static and Dynamic) Advanced forward error correction coding: STBC, LDPC	
14	should support 802.11ac transmit beamforming Maximal Ratio Combining (MRC)	
15	Maximum conducted transmit power shall be 20 dBm on both 2.4 and 5 GHz with	
	two antennas and EIRP complying to regulatory requirements	
16	Should support minimum 4dBi on 2.4 GHz band and 6 dBi on 5GHz band or better	
17	AP should support Radio Share and Off-Channel Scan, Enables a single to perform double duty as an access point and a sensor.	
18	AP should Increases reliability and resilience of the wireless network to support mission-critical applications.	
19	Should support Load Balancing, Pre-Emptive Roaming, and Rate Scaling	
20	Should support Gap-Free Security, Protects your network 24x7x365 with integrated security features.	
21	Should support an unprecedented number of users and applications—including voice and video—allowing you to confidently deploy Bring Your Own Device (BYOD) initiatives and empower new workgroups with mobility.	
22	AP should support comprehensive integrated security features that include layer 2-7 stateful packet filtering firewall, AAA RADIUS services, a VPN gateway and location-based access control.	
23	The AP secures all your wireless transmissions, ensuring compliance with the government or industry regulations your business may be subject to, such as PCI in retail and HIPAA in healthcare	
24	AP should support Air Defense Network Assurance features	
25	AP should support dedicated sensor, Radio Share and Off-Channel Scan features work hand-in-hand to allow either or both radios to carry client data and act as a sensor, providing dual-band sensing without adding cost.	
26	AP should support for Voice-over-wireless LAN (VoWLAN) quality of service (QoS) ensures toll quality, even with many simultaneous calls on a single access point.	
27	AP should easily provide hotspot and guest access	
28	AP should be capable of managed by controller, Controller-less and Standalone Mode.	

29	AP should be capable of serving the client, if Hardware controller will be faulty or power fail without any human intervention.	
30	AP should support Layer 3 routing, 802.1q, DynDNS, DHCP server/client, BOOTP client, PPPoE and LLDP	
31	Should support Stateful Firewall, IP filtering, NAT, 802.1x, 802.11i, WPA2, WPA Triple- Methodology Rogue Detection: 24x7 dual-band WIPS sensing, on-board IDS, and secure guest access (hotspot) with captive portal, IPSec, and RADIUS Server	
32	AP should support captive portal with time-based access, Customize Guest page and must have option for self-guest registration options, so that guest can automatic register self from day 1. Bidder should provide the external supported device also if required.	
33	should support WMM, WMM-UAPSD, 802.1p, DiffServ, and TOS	
34	Should support wireless medium Direct Sequence Spread Spectrum (DSSS), Orthogonal Frequency Division Multiplexing (OFDM), and Spatial Multiplexing (MIMO)	
35	Should support IEEE 802.11a/b/g/n/ac, 802.11d/r/v/k/w/e/d and 802.11i WPA2, WMM, and WMM-UAPSD, L2TPv3, Client VPN, MESH and Captive Portal server	
36	AP should have Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac and Safety- UL / cUL 60950-1, IEC / EN60950-1, UL2043, RoHS	
37	Should have Radio Approval FCC (USA), EU, TELEC	
38	Should support receiver sensitivity up to -97 or better.	
39	AP should support Dynamic Vlan, Bridge and Tunnel Vlan, Vlan Load Balancing and Vlan Pool.	
40	AP should support User, AP and Band Load Balancing.	
41	Ap should support customized WIPS signature and Rouge AP detection and Rouge AP Termination manual and automatic.	

5. Technical compliance for Access Point Type 2(High density)

S. NO	SPECIFICATION	Page No. of the Bid Document
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave-2 or higher.	
2	AP should Support MU-MIMO 256QAM.	
3	Mounting bracket should be supplied with every AP and should be from the AP OEM	
4	LED should be available for activity indication	
5	Must have 1x IEEE 802.3 Gigabit Ethernet auto-sensing with One console Serial Port.	
6	The access point must have integrated antenna or External Antenna	
7	Operating temperature should be in the range 0° C to 40° C	
8	Should support 802.11 a/b/g/n/ac standard.	
9	AP should have Dual band radios; supports 4X4 MIMO with 4 Spatial Streams on 802.11a/802.11n/802.11ac or higher.	
10	AP should support 20, 40, and 80 MHz Channels	
11	AP have minimum 2300 Mbps data rates on dual concurrent radio operations or better.	
12	Support Packet Aggregation (AMSDU, AMPDU) Reduced Interface Spacing	
13	Should support MIMO Power Save (Static and Dynamic) Advanced forward error	
	correction coding: STBC, LDPC	
14	should support 802.11ac transmit beamforming Maximal Ratio Combining (MRC)	
15	Maximum conducted transmit power shall be 28 dBm on both 2.4 and 5 GHz with two antennas and EIRP complying to regulatory requirements	
16	Should support minimum 4dBi on 2.4 GHz band and 6 dBi on 5GHz band or better	
17	AP should support Radio Share and Off-Channel Scan, Enables a single to perform double duty as an access point and a sensor.	
18	AP should Increases reliability and resilience of the wireless network to support mission-critical applications.	
19	Should support Load Balancing, Pre-Emptive Roaming, and Rate Scaling	
20	Should support Gap-Free Security, Protects your network 24x7x365 with integrated security features.	
21	Should support an unprecedented number of users and applications—including voice and video—allowing you to confidently deploy Bring Your Own Device (BYOD) initiatives and empower new workgroups with mobility.	
22	AP should support comprehensive integrated security features that include layer 2-7 stateful packet filtering firewall, AAA RADIUS services, a VPN gateway and location-based access control.	
23	The AP secures all your wireless transmissions, ensuring compliance with the government or industry regulations your business may be subject to, such as PCI in retail and HIPAA in healthcare	
24	AP should support Air Defense Network Assurance features	
25	AP should support dedicated sensor, Radio Share and Off-Channel Scan features work hand-in-hand to allow either or both radios to carry client data and act as a sensor, providing dual-band sensing without adding cost.	
26	AP should support for Voice-over-wireless LAN (VoWLAN) quality of service (QoS) ensures toll quality, even with many simultaneous calls on a single access point.	
27	AP should easily provide hotspot and guest access	
28	AP should be capable of managed by controller, Controller-less and Standalone Mode.	
29	AP should be capable of serving the client, if Hardware controller will be faulty or power fail without any human intervention.	

30	AP should support Layer 3 routing, 802.1q, DynDNS, DHCP server/client, BOOTP client, PPPoE and LLDP	
31	Should support Stateful Firewall, IP filtering, NAT, 802.1x, 802.11i, WPA2, WPA Triple- Methodology Rogue Detection: 24x7 dual-band WIPS sensing, on-board IDS, and secure guest access (hotspot) with captive portal, IPSec, and RADIUS Server	
32	Ap should support captive portal with time-based access, Customize Guest page and must have option for self-guest registration options, so that guest can automatic register self from day 1. Bidder should provide the external supported device also if required.	
33	should support WMM, WMM-UAPSD, 802.1p, DiffServ, and TOS	
34	Should support wireless medium Direct Sequence Spread Spectrum (DSSS), Orthogonal Frequency Division Multiplexing (OFDM), and Spatial Multiplexing (MIMO)	
35	Should support IEEE 802.11a/b/g/n/ac, 802.11d/r/v/k/w/e/d and 802.11i WPA2, WMM, and WMM-UAPSD, L2TPv3, Client VPN, MESH and Captive Portal server	
36	AP should have Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac and Safety- UL / cUL 60950-1, IEC / EN60950-1, UL2043, RoHS	
37	Should have Radio Approval FCC (USA), EU, TELEC	
38	Should support receiver sensitivity up to -97 or better.	
39	AP should support Dynamic Vlan, Bridge and Tunnel Vlan, Vlan Load Balancing and Vlan Pool.	
40	AP should support User, AP and Band Load Balancing.	
41	Ap should support customized WIPS signature and Rouge AP detection and Rouge AP Termination manual and automatic.	
42	Wireless controller, Access Points and the fibre modules (If required for the deployment) should be from the same OEM. The OEM should have R&D centre in India. The OEM should have atleast 2 RMA depot in India and should have India Toll free number with India TAC centre - reflected on the official website. The OEM should be globally reputed and presence/recommendation in Latest Gartner report in leader quadrant for wired and wireless will be preferred.	

7. Technical compliance for Wireless Controller

Sl. NO	SPECIFICATION	Page No. of the Bid Document
1	The OEM should be globally reputed and presence/recommendation in Latest Gartner report in leader quadrant for wired and wireless will be preferred.	
2	Proposed Solution Controller & AP should be of the same OEM.	
3	Controller should have 1U rack size with minimum 4 nos. 10/100/1000 Base-T Port.	
4	Controller should support min. 256 AP from Day 1 and upgradable up to 500 AP without changing Hardware.	
5	Controller should support minimum up to 16K Client.	
6	Should have at least with 4GB RAM and 32 GB SSD or more.	
7	Controller should support 256 WLANs.	
8	Controller should support IPV4 and IPV6 from day 1.	
9	Controller architecture offers a software-defined networking (SDN)-ready operating system that can distribute controller functionality to every access point in your network	
10	All wireless LAN infrastructure can work together to ensure every transmission is routed through the most efficient path, every time.	
11	Solutions should have with Maximum network uptime and security with minimal management. And true seamless and dependable mobility for users.	
12	Should supports all Wi-Fi protocols, including 802.11a/b/g/n/ac, allowing to a cost-effective migration plan based on the needs of business.	
13	Solutions should support from a small WLAN network in a single location to a large multi-site network	
14	Solution should be ready to support for all type of deploy infrastructure, I.e. standalone independent access points or adaptive access points that can be adopted by a controller but can switch to independent mode; virtual controllers; physical controllers in branch offices, the network operating centre (NOC) or the cloud from day 1	
15	Controller and access point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time **for Staff/Employee and Guest Traffic.**	
16	Controller should support hierarchical management that delivers a new level of management simplicity and resiliency by enabling controllers to manage other controllers and access points,	
17	Controller shall have comprehensive security capabilities keep network and data safe, ensuring compliance with PCI, HIPAA and other government and industry security regulations.	
18	Controller should support Mesh connectivity for Large Indoor and Outdoor Space, where not have any possibility to reach the cable.	
19	Support single powerful windowpane enables for zero touch infrastructure deployment	
20	Provide visibility & control over layer-7 applications with an embedded DPI engine that inspects every flow of every user at the access point	
21	Controller is capable of detecting and identifying thousands of applications real time.	
22	Should have options to configure your access points to report this real-time, network statistics to the NMS	
23	support features so that Network administrators can get in-depth insight into every dimension of the network including layer-7 application visibility, client devices, device & OS types and users.	
24	Administrators can discern, at a glance, the top applications by usage or by count at every level of the network from site level to access points and clients.	

25	System should be capable of enables all WLAN infrastructure with the intelligence required to work together to determine the most efficient path for every transmission	
26	Solutions should be capable to route all traffic through a controller is eliminated, along with the resulting congestion and latency, resulting in higher throughput and superior network performance.	
27	All controller feature should available at the access layer, they remain available even when the controller is offline, for example, due to a WAN outage, ensuring site survivability and extraordinary network resilience.	
28	Controller have capability to enables the creation of highly reliable networks, with several levels of redundancy and failover mechanisms to ensure continuous network service in case of outages	
29	AP should support APs in remote sites coordinate with each other to provide optimized routing and self-healing, delivering a superior quality of experience for operational/business-critical applications.	
30	When APs lose communication with the controller, they continue to function, able to bridge traffic while still enforcing QoS and security policies, including stateful inspection of Layer2 (locally bridged) or Layer 3 traffic.	
31	Controller should have built-in DHCPv4 and DHCPv6 server to serve the IP address to client.	
32	should support AAA server and routing protocols like policy-based routing and OSPF.	
33	Should support STP, RSTP, MSTP and Link Aggregation.	
34	Access Point and controller should support CLI and GUI for manage or troubleshoot the Network.	
35	Solutions should able to show the health & inventory report of Client, Access point and Controller.	
36	An administrator can capture connected client packet data based on the packet's address type or port on which received.	
37	Should support 802.1x authentication and providing the capability to permit or deny connectivity based on user or device identity from day 1.	
38	Controllers and service platforms must support WIPS to provides continuous protection against wireless threats, Bidder should quote all licenses from day 1.	
39	should detect and locate unauthorized AP devices, able to block device using manual termination, air lockdown or port suppression.	
40	Controllers and service platforms support dedicated sensor devices, designed to actively detect and locate unauthorized AP devices	
41	An access point support CPLD (complex programmable logic device) to manage power.	
42	CPLD determines the maximum power provided by the POE device and the budget available to the access point.	
43	Should support IPV4 and IPV6 Firewall Rules.	
44	Controller should support Virtual Interface to a controller or service platform or provide to layer 3 service on a VLAN	
45	Controller should support Bonjour for Apple's implementation of zero configuration networking (Zeroconf).	
46	Controller must have support 802.1s, 802.1p, RA Guard, 802.11r, 802.11w, 802.11s	
47	Should support A highly-scalable built-in captive portal server with customizable pages, Pages can be customized easily for the form factor of the target device like smartphones, tablets, and laptops and also have options to hosted on an external web server.	
48	support Authentication/accounting via external RADIUS server or built-in guest user database	
49	support Mobile-friendly Web portal Customizable templates (Colour, Banner with preview option)	

50	Includes support for bandwidth tracking and rate limiting/enforcement	
51	Should have provide Guest Self Registration, Device Registration, Registration using Social Logins, Customizable Registration Form with support for Name, Email, Mobile, Member, DOB, Age, Gender, and more. Bidder can go with external device to achieve this features.	
52	should support Passcode notification through email, SMS, or SMS through SMTP, Built-in Analytics, Redirection for Proxy Ports, Device fingerprinting, Dynamic VLAN support, Walled Garden (DNS or Host IP white list), Granular day of week and time of day access.	
53	To prevent congestion in the network, and ensure that mission critical traffic is not impacted, controller provides the capability to limit traffic per user, or enable rate limiting per WLAN, so that all users on that WLAN are rate-limited.	
54	Clients are distributed among APs on association by client count or AP throughput, which is useful for dense deployments, such as conferences and stadiums. Neighbouring APs are automatically computed and do not require manual identification.	
55	Allows a web admin to generate and print a voucher for a guest user that grants the user access for a specified period of time. Contains the capability to generate vouchers in bulk for multiple users. Useful in retail and enterprise guest access scenarios, where admins want to pre-generate these vouchers to be handed out later	
56	Controller Provides the following native capabilities: Extensive WIPS Event Detection, Customized WIPS Signatures, Device Categorization, Unauthorized AP Detection and Anomaly Analysis with Client Blacklisting. Rogue AP classification using wired side detection, termination, and rogue detection of APs leaking wired traffic from a sanctioned network supported both with part-time scanning and off-channel scanning	
57	Controller should support layer 2 and at layer 3 (IP), Application Layer Gateways, Association ACL, Centralized Association ACL, Client Disassociate on Excessive Denies, DHCP Broadcast to Unicast Conversion, Dos Attack Detection, Dynamic ARP Inspection (DAI), Hole 196 Detection/Protection, IPv4 ACL and Rules, MAC ACL and Rules, Per VLAN Enable/Disable, Rogue DHCP Server Detection, Storm Controls.	
58	Controller should have Firewall policy enforcement based on user roles, besides the standard firewall policies by subnet, port, etc. Role can be assigned based on various parameters, such as AP Location, Active Directory Attributes, OpenLDAP Attributes, Authentication State, Authentication Type, DHCP Fingerprint, Encryption Type, Group Membership, MAC Address, SSID Name and User Defined LDAP Attributes.	
59	WLAN client should work continuously without any changes required if Hardware controller will be fail or Power Off	