NIT NO.:/MDU-R/MAR/2018/004

TENDER DOCUMENT

NAME OF WORK: PROCUREMENT & RATE CONTRACT FOR 1 YEAR OF WI-FI EQUIPMENT FOR STRENGTHENING WI-FI COVERAGE

VIKAS

Last date submission of the filled Tender document: 23.04.2018 up to 2:30 pm.
(The Tender document is to be submitted duly signed in blue/black ink on each page and stamped with official seal on each page)

Table of Contents

CONTENTS

Maharshi Dayanand University, Rohtak

[Established in Act No. 25 of 1975 of the Haryana Legislative Assembly in 1976]

NAAC Accredited 'A' Grade

No. UCC/2017/ Dated :31/03/2018

University Computer Center

Phone: 01262-393548 **E-mail: dir.ucc@mdurohtak.ac.in**

STANDARD BIDDING DOCUMENT FOR PROCUREMENT & RATE CONTRACT FOR 1 YEAR OF WI-FI EQUIPMENT FOR STRENGTHENING WI-FI COVERAGE ON BEHALF OF REGISTRAR, MAHARSHI DAYANAND UNIVERSITY, ROHTAK.

PART1: COMPLETE BIDDING DOCUMENT

PRESS NOTICE

M. D. UNIVERSITY, ROHTAK **Notice Inviting E-Tender**	
Name of work	PROCUREMENT & RATE CONTRACT FOR 1 YEAR OF WI-FI EQUIPMENT FOR STRENGTHENING WI-FI COVERAGE
E Service Fees+ Tender Doc. Fees	1000/- + 4,000/- =5,000/- (TO BE PAID ONLINE)
Earnest Money **Time Limit**	2% OF THE QUOTED RATE 21 DAYS
Tenders to be received till: 23.04.2018 till 02:30 P.M	
(1) THE TENDERS WILL BE RECEIVED ONLY THROUGH E-TENDERING FOR FURTHER DETAILS VISIT WEBSITE HTTPS://HARYANAEPROCUREMENT.GOV.IN.	

REGISTRAR

The Bidders can download the tender documents from the Portal: https://haryanaeprocurement.gov.in.

1) Earnest Money and Document Fee Deposit have to be deposited through Online Mode Only.
2) Willing Contractors shall have to pay the e- service fees of Rs.1000/- through Online mode
3) However, the details of the EMD, Tender document Fee & E–Service Fee are required to be filled/provided scan copies at the time of online Bid Preparation Stage the Bidders are required to keep the EMD, Tender document fee & E- Service fee details ready beforehand. The contractual Agencies can submit their tender documents as per the date mentioned below:

KEY DATES

Sr. No.	M.D.U. Rohtak Stage	Contractor Stage	Start Date & Time	End Date & Time
1		Tender Document Download and Bid Preparation & Submission	**31-03-2018**	**23.04.2018 till 02:30 P.M**
3		Submission of Tender Fees and online EMD Fees	**Error! Reference source not found.**	**23.04.2018 till 02:30 P.M**
5	Technical Opening/ Technical Evaluation Opening of Financial Bid		**23.04.2018 till 02:30 P.M**	

Important Note:-

1) The bidders shall have to complete Bid Preparation & Submission" stage on scheduled date & time as mentioned above. If any bidder failed to complete his/her aforesaid stage in the stipulated online time schedule for this stage, his/her bid status will be considered as "bids not submitted".
2) Bidder must confirm & check his/her bid status after completion of his/her all activities for e-bidding.
3) Bidder can rework on his/her bids even after completion of "Bid Preparation & submission stage" (Bidder Stage), subject to the condition that the rework must take place before the stipulated time frame of the Bidder Stage.

DETAIL NOTICE INVITING TENDER

e-Tender is invited for purchase of below mentioned items in single stage two cover system i.e. Request for Technical Bid (online Bid under PQQ/ Technical Envelope) and Request for Financial Bid (comprising of price bid Proposal under online available Commercial Envelope).

1. Detailed notice inviting tender/estimate drawing can be seen in the office of the undersigned during office hours.
2. Bidding documents available on website http://mdurohtak.haryanaeprocurement.gov.in
3. Newly enlisted contractors/societies/suppliers/manufactures should bring with them proof of their enlistment in appropriate class.
4. The bidders would submit bid through e-tendering only on the website i.e. http://haryanaeprocurement.gov.in

Under this process, the Pre-qualification/ Technical online bid Application as well as online Price Bid shall be invited at single stage under two covers i.e. PQQ/Technical & Commercial Envelope. Eligibility and qualification of the Applicant will be first examined based on the details submitted online under first cover (PQQ or Technical) with respect to eligibility and qualification criteria prescribed in this Tender document. The Price Bid under the second cover shall be opened for only those Applicants whose PQQ/ Technical Applications are responsive to eligibility and qualifications requirements as per Tender document.

1. The payment for Tender Document Fee and e-Service Fee shall be made by eligible bidders online directlythrough Debit Cards & Internet Banking Accounts and the payment for EMD can be made online directly throughRTGS/NEFT or OTC Please refer to 'Online Payment Guideline' available at the Single e-Procurement portal of GoH(Govt. of Haryana) and also mentioned under the Tender Document.

2. Intending bidders will be mandatorily required to online sign-up (create user account) on the website https://haryanaeprocurement.gov.in to be eligible to participate in the e-Tender. The firm will be required to make onlinepayment of 2% of the bid cost towards EMD fee in due course of time. The intended bidder fails to pay EMD fee under thestipulated time frame shall not be allow to submit his / her bids for the respective event / Tenders.

3. The interested bidders must remit the funds at least T+1 working day (Transaction day + One working Day) in advance and make payment via RTGS /NEFT or OTC to the beneficiary account numberspecified under the online generated challan. The intended bidder / Agency thereafter will be able to successfullyverify their payment online, and submit their bids on or before the expiry date & time of the respective events/Tendersat https://haryanaeprocurement.gov.in.

The interested bidders shall have to pay mandatorily e-Service fee (under document fee – Non-refundable) of Rs.1000/- (Rupee One Thousand Only) online by using the service of secure electronic gateway. The secure electronic payments gateway is an online interface between bidders & online payment authorization networks.

The Payment for document fee/ e-Service fee can be made by eligible bidders online directly through Debit Cards & Internet Banking.

The Bidders can submit their tender documents (Online) as per the dates mentioned at Page no 3 of Document: -

Important Note:

1. The Applicants/bidders have to complete 'Application / Bid Preparation & Submission' stage on scheduled time as mentioned above. If any Applicant / bidder failed to complete his / her aforesaid stage in the stipulated online time schedule for this stage, his / her Application/bid status will be considered as 'Applications / bids not submitted'.
2. Applicant/Bidder must confirm & check his/her Application/bid status after completion of his/her all activities for e-bidding.
3. Applicant/Bidder can rework on his/her bids even after completion of 'Application/Bid Preparation & submission stage' (Application/Bidder Stage), subject to the condition that the rework must take place during the stipulated time frame of the Applicant/Bidder Stage.
4. In the first instance, the online payment details of tender document fee + e-Service and EMD&PQQ/Technical Envelope shall be opened. Henceforth financial bid quoted against each of the item by the shortlisted bidder/ Agency wherever required shall be opened online in the presence of such bidders/ Agency who either themselves or through their representatives choose to be present. The bidder can submit online their bids as per the dates mentioned in the schedule/Key Dates above.

The bids shall be submitted online in two separate envelopes:

Envelope 1: Technical Bid

The bidders shall upload the required eligibility & technical documents online in the Technical Bid.

Envelope 2: Commercial Bid

The bidders shall quote the prices in price bid format under Commercial Bid.

CONDITIONS: -

1. DNIT& prequalification criteria can be seen on any working day during office hours in office of the undersigned.
2. Conditional tenders will not be entertained & are liable to be rejected.
3. In case the day of opening of tenders happens to be holiday, the tenders will be opened on the next working day. The time and place of receipt of tenders and other conditions will remain unchanged.
4. The undersigned reserve the right to reject any tender or all the tenders without assigning any reasons.
5. The societies shall produce an attested copy of the resolution of the Co-operative department for the issuance of tenders.
6. The tender without earnest money/bid security will not be opened.
7. The Jurisdiction of court will be at **Rohtak**.

8. The tender of the bidder who does not satisfy the qualification criteria in the bid documents are liable to be rejected summarily without assigning any reason and no claim whatsoever on this account will be considered.
9. The bid for the work shall remain open for acceptance during the bid validity period to be reckoned from the last date of 'Manual submission of BS. If any bidder/tenders withdraws his bid/tender before the said period or makes any modifications in the terms and conditions of the bid, the earnest money shall stand forfeited. Bids shall be valid for 120 days from the date of bid closing i.e. from last date of manual submission of EMD. In case the last day to accept the tender happens to be holiday, validity to accept tender will be the next working day.

For & on behalf of Registrar, MDU, Rohtak

P&S

M. D. University, Rohtak

INSTRUCTIONS TO BIDDER ON ELECTRONIC TENDERING SYSTEM

These conditions will over-rule the conditions stated in the tender documents, wherever relevant and applicable.

REGISTRATION OF BIDDERS ON E-PROCUREMENT PORTAL: -

All the bidders intending to participate in the tenders process online are required to get registered on the centralized e - Procurement Portal i.e. https://haryanaeprocurement.gov.in. Please visit the website for more details.

OBTAINING A DIGITAL CERTIFICATE:

1.1 The Bids submitted online should be encrypted and signed electronically with a Digital Certificate to establish the identity of the bidder bidding online. These Digital Certificates are issued by an Approved Certifying Authority, by the Controller of Certifying Authorities, Government of India.

1.2 A Digital Certificate is issued upon receipt of mandatory identity (i.e. Applicant's PAN Card) and Address proofs and verification form duly attested by the Bank Manager / Post Master / Gazetted Officer. Only upon the receipt of the required documents, a digital certificate can be issued. For more details, please visit the website – https://haryanaeprocurement.gov.in.

1.3 The bidders may obtain Class-II or III digital signature certificate from any Certifying Authority or Sub-Certifying Authority authorized by the Controller of Certifying Authorities or may obtain information and application format and documents required for the issue of digital certificate from:

M/s Nextenders (India) Pvt. Ltd.
O/o. DS&D Haryana,
SCO – 09, IInd Floor,
Sector – 16,
Panchkula – 134108
E-mail: chandigarh@nextenders.com
Help Desk: 1800-180-2097 (Toll Free Number)

1.4 The bidder must ensure that he/she comply by the online available important guidelines at the portal https://haryanaeprocurement.gov.in for Digital Signature Certificate (DSC) including the e-Token carrying DSCs.

1.5 Bid for a particular tender must be submitted online using the digital certificate (Encryption & Signing), which is used to encrypt and sign the data during the stage of bid preparation. In case, during the process of a particular tender, the user loses his digital certificate (due to virus attack, hardware problem, operating system or any other problem) he will not be able to submit the bid online. Hence, the users are advised **to keep a backup of the certificate** and also keep the copies at safe place under proper security (for its use in case of emergencies).

1.6 In case of online tendering, if the digital certificate issued to the authorized user of a firm is used for signing and submitting a bid, it will be considered equivalent to a no-objection certificate /power of attorney / lawful authorization to that User. The firm has to authorize a specific individual through an authorization certificate signed by all partners to use the digital certificate as

per Indian Information Technology Act 2000. Unless the certificates are revoked, it will be assumed to represent adequate authority of the user to bid on behalf of the firm in the department tenders as per Information Technology Act 2000.

1.7 The digital signature of this authorized user will be binding on the firm.

1.8 In case of any change in the authorization, it shall be the responsibility of management / partners of the firm to inform the certifying authority about the change and to obtain the digital signatures of the new person / user on behalf of the firm / company. The procedure for application of a digital certificate however will remain the same for the new user.

1.9 The same procedure holds true for the authorized users in a private/Public limited company. In this case, the authorization certificate will have to be signed by the directors of the company.

OPENING OF AN ELECTRONIC PAYMENT ACCOUNT:

For purchasing the tender documents online, bidders are required to pay the tender documents fees online using the electronic payments gateway service shall be integrated with the system very soon till then it will be submitted manually. For online payments guidelines, please refer to the Home page of the e-tendering Portal https://haryanaeprocurement.gov.in.

Pre-requisites for online *bidding*:

In order to operate on the electronic tender management system, a user's machine is required to be set up. A help file on system setup/Pre-requisite can be obtained from Nextenders (India) Pvt. Ltd. or downloaded from the home page of the website -https://haryanaeprocurement.gov.in.. The link for downloading required java applet & DC setup are also available on the Home page of the e-tendering Portal.

ONLINE VIEWING OF DETAILED NOTICE INVITING TENDERS:

The bidders can view the detailed N.I.T and the time schedule (Key Dates) for all the tenders floated through the single portal eProcurement system on the Home Page at https://haryanaeprocurement.gov.in.

DOWNLOAD OF TENDER DOCUMENTS:

The tender documents can be downloaded free of cost from the eProcurement portal https://haryanaeprocurement.gov.in

KEY DATES:

The bidders are strictly advised to follow dates and times as indicated in the online Notice Inviting Tenders. The date and time shall be binding on all bidders. All online activities are time tracked and the system enforces time locks that ensure that no activity or transaction can take place outside the start and end dates and the time of the stage as defined in the online Notice Inviting Tenders.

ONLINE PAYMENT OF TENDER DOCUMENT FEE, ESERVICE FEE ,EMD FEES & BID PREPARATION & SUBMISSION (PQQ/ TECHNICAL& COMMERCIAL/PRICE BID):

i) Online Payment of Tender Document Fee + e-Service fee**:**

The online payment for Tender document fee, eService Fee &EMD can be done using the secure electronic

payment gateway. The Payment for Tender Document Fee and eService Fee shall be made by bidders/ Vendors online directly through Debit Cards & Internet Banking Accounts and the Payment for EMD shall be made online directly through RTGS / NEFT& OTC. The secure electronic payments gateway is an online interface between contractors and Debit card / online payment authorization networks.

ii) PREPARATION & SUBMISSION of online APPLICATIONS/BIDS**:**

Detailed Tender documents may be downloaded from e-procurement website (https://haryanaeprocurement.gov.in) and tender mandatorily be submitted online.

Scan copy of Documents to be submitted/uploaded for Prequalification or Technical bid under online PQQ/ Technical Envelope: The required documents (refer to DNIT) shall be prepared and scanned in different file formats (in PDF /JPEG/MS WORD format such that file size is not exceed more than 10 MB) and uploaded during the on-line submission of PQQ or Technical Envelope.

FINANCIAL or Price Bid PROPOSAL shall be submitted mandatorily online under Commercial Envelope and original not to be submitted manually)

ASSISTANCE TO THE BIDDERS: -

In case of any query regarding process of e-tenders and for undertaking training purpose, the intended bidder can also avail the following and can contact service provider as per below:

Office Timings of Help-desk support for Single e Procurement Portal of Government of Haryana-Technical Support Assistance will be available over telephone Monday to Friday (09:00 am. to 5:30 pm) & Training workshop will be conducted on every 1st, 2nd Friday (from 3:30 pm upto 6:00 pm) and 4th Saturday (from 11:30 am upto 3:00 pm) of each month.

All queries would require to be registered at our official email-chandigarh@nextenders.com for on- time support (Only those queries which are sent through email along with appropriate screenshots or error description will be considered as registered with the Help-desk)

IMPORTANT NOTE: -

(a) Any intending bidder can contact the helpdesk on or before prior to 4 hours of the scheduled closing date & time of respective e-Auction/ Tender event.

(b) For queries pertaining to e-Payment of EMD, please contact the helpdesk at least 2 business days prior to the closing date & time of e-Auction/Tender event.

(c) Help-desk support will remain closed during lunch break i.e. from 1:30 PM up to 2:15 PM on each working day.

SCHEDULE FOR TRAINING:

Training workshop will be held on 1st, 2nd Friday (from 3:30 pm upto 6:00 pm) and 4th Saturday (from 11: 30 am upto 3:00 pm) of each month at following addresses:		
Nextenders (India) Pvt. Ltd Municipal Corporation Faridabad, Near B.K. Chowk, Opp. B.K.Hospital, NIT, **Faridabad** Contact no.	Nextenders (India) Pvt. Ltd. Public Health Division No. 2 Hisar, Model Town Opp. N.D Gupta Hospital, **Hisar**	Nextenders (India) Pvt. Ltd., NirmanSadan (PWDB&R), Plot No.- 01, Basement, Dakshin Marg, Sec- 33 A, **Chandigarh** -160020 **For Support- 1800-180-2097**,

Haryana eProcurement Help Desk Office will remain closed on Saturday (except 4thSaturday), Sunday and National Holidays

NOTE:-Bidders participating in online tenders shall check the validity of his/her Digital Signature Certificate before participating in the online Tenders at the portal https://haryanaeprocurement.gov.in.

For help manual please refer to the 'Home Page' of the e-Procurement website at https://haryanaeprocurement.gov.in, and click on the available link 'How to...?' to download the file.

GUIDELINE FOR ONLINE PAYMENTS IN E-TENDERING

Post registration, bidder shall proceed for bidding by using both his digital certificates (one each for encryption and signing). Bidder shall proceed to select the tender he is interested in. On the respective Department's page in the e-tendering portal, the Bidder would have following options to make payment for tender document &EMD:

i. Debit Card
ii. Net Banking
iii. RTGS/NEFT

OPERATIVE PROCEDURES FOR BIDDER PAYMENTS

A) DEBIT CARD

The procedure for paying through Debit Card will be as follows.

i. Bidder selects Debit Card option in e-Procurement portal.
ii. The e-Procurement portal displays the amount and the card charges to be paid by bidder. The portal also displays the total amount to be paid by the bidder.
iii. Bidder clicks on "Continue" button

iv. The e-Procurement portal takes the bidder to Debit Card payment gateway screen.

v. Bidder enters card credentials and confirms payment

vi. The gateway verifies the credentials and confirms with “successful” or “failure” message, which is confirmed back to eProcurement portal.

vii. The page is automatically routed back to e-Procurement portal

viii. The status of the payment is displayed as “successful” in e-Procurement portal. The e-Procurement portal also generates a receipt for all successful transactions. The bidder can take a print out of the same,

ix. The e-Procurement portal allows Bidder to process another payment attempt in case payments are not successful for previous attempt.

B) NET BANKING

The procedure for paying through Net Banking will be as follows.

i. Bidder selects Net Banking option in e-Procurement portal.

ii. The e-Procurement portal displays the amount to be paid by bidder.

iii. Bidder clicks on “Continue” button

iv. The e-Procurement portal takes the bidder to Net Banking payment gateway screen displaying list of Banks (v) Bidder chooses his / her Bank

v. The Net Banking gateway redirects Bidder to the Net Banking page of the selected Bank

vi. Bidder enters his account credentials and confirms payment

vii. The Bank verifies the credentials and confirms with “successful” or “failure” message to the Net Banking gateway which is confirmed back to e-Procurement portal.

viii. The page is automatically routed back to e-Procurement portal

ix. The status of the payment is displayed as “successful” in e-Procurement portal.

The e-Procurement portal also generates a receipt for all successful transactions. The bidder can take a print out of the same. (xi) The e-Procurement portal allows Bidder to process another payment attempt in case payments are not successful for previous attempt.

C) RTGS/ NEFT

The bidder shall have the option to make the EMD payment via RTGS/ NEFT. Using this module, bidder would be able to pay from their existing Bank account through RTGS/NEFT. This would offer a wide reach for more than 90,000 bank branches and would enable the bidder to make the payment from almost any bank branch across India.

I. Bidder shall log into the client e-procurement portal using user id and password as per existing process and selects the RTGS/NEFT payment option.

II. Upon doing so, the e-procurement portal shall generate a pre-filled challan. The challan will have all the details that is required by the bidder to make RTGS-NEFT payment. iii.

III. Each challan shall therefore include the following details that will be pre-populated:

- Beneficiary account no: (unique alphanumeric code for e-tendering)
- Beneficiary IFSC Code:
- Amount:
- Beneficiary bank branch:
- Beneficiary name:

iv. The Bidder shall be required to take a print of this challan and make the RTGS/NEFT on the basis of the details printed on the challan.

v. The bidder would remit the funds at least T + 1 day (Transaction + One day) in advance to the last day and make the payment via RTGS / NEFT to the beneficiary account number as mentioned in the challan.

vi. Post making the payment, the bidder would login to the e-Tendering portal and go to the payment page. On clicking the RTGS / NEFT mode of payment, there would be a link for real time validation. On clicking the same, system would do auto validation of the payment made.

D) OVER-THE-COUNTER (OTC)

This solution shall allow the bidder having account with ICICIBank, to make the payment from any CMS enabled Branch of ICICI Bank in India. Bidders can make the payment via cash (if amount is<= 49,999), ICICI Bank Cheque.

The procedure for paying through OTC mode is as follows:

i Bidder selects Over-the-Counter remittance option in e-Procurement portal.

ii The e-Procurement portal displays the amount to be paid. Bidder chooses the bank account no. for refund of the amount.

iii Bidder clicks on “Continue” button

iv The e-Procurement portal displays the details of payment. Bidders clicks on “print _challan” and prints the OTC challan.

v Bidder submits the OTC challan at the counter of any designated branch of ICICI Bank with

vi Cash / Demand Draft / ICICI Bank Cheque (Payment in cash is allowed uptoRs. 49,999/-)

vii ICICI Bank verifies the URN (format to be discussed and decided) and Amount with e-Procurement portal prior to accepting the payment

viii On successful verification from e-Procurement portal, ICICI Bank accepts the payment. In case of failure, ICICI Bank shall return back the OTC challan and payment to the Bidder.

ix ICICI Bank will commit the payment transaction (in case of successful verification from e-Procurement portal) and sends the Bank Transaction Number (I-Sure Reference Number) online against the URN and Amount.

x ICICI Bank will generate receipt for the payment transaction and issues the same to the Bidder.

xi The e-Procurement system updates the bank transaction number against the URN and Amount based on details sent by ICICI Bank online prior to generation of receipt.

xii The status of payment will be displayed as “verification successful” in e-Procurement portal, when the bidder clicks on verification option in the portal

xiii Bidder would be required to upload the scan copy of receipt as received from ICICI Bank as part of proof in Nex-tender portal before submitting the tender

IMPORTANT NOTES(DO'S/DON'T)

Sr no.	Scenario	Do's / Don'ts
1	**In the event of making Payment through NEFT/RTGS**	Do's • It is the bidder's responsibility to ensure that RTGS/NEFT payments are made to the exact details as mentioned in the challan which are: 1) Beneficiary account no: <client code> + <random number> 2) Beneficiary IFSC Code: As prescribed by ICICI Bank (this shall remain same across all tenders) • Amount: As mentioned on the challan. It is specific for every tender/transaction • Beneficiary bank branch: ICICI Bank Ltd, CMS • Beneficiary name: As per the challan • For every tender, details in the challan are different and specific to that tender only. Bidder should not make use of a challan for making payment for another tenders' EMD • It is advised that all the bidders make payment viaRTGS/NEFT at least one day in advance to the last day of tender submission as certain amount of time is required for settlement and various parties are involved. The payment may not be available for the bidder validation. In such cases bidder may not be able to submit the tender • Bidder has to make only single payment against a challan as per the amount mentioned on the challan. • Bidder must do the payment before tender validity gets expired **Don'ts** • Bidder should not enter erroneous details while filling the NEFT/RTGS form at their bank. The following possibilities may arise: 1) Incorrect IFSC code mentioned: - Transaction would be rejected and the amount would be refunded back in to the bidders account 2) Incorrect Beneficiary account number mentioned (<client code> + <random number>): - a) In case, the beneficiary account number mentioned is incorrect the transaction would be rejected and the bid would not be accepted. 3) Incorrect Amount mentioned: The amount would be rejected if the amount mentioned in while making the payment is incorrect. Such cases will be captured as unreconciled transactions and will be auto-refunded directly to bidder's account. In the event of any discrepancy, payment would not be considered and bidder would not be allowed to bid/ participate. • Bidder is not supposed to use challan generated in one tender for payment against another tender since details in the challan are unique to the tender and bidder combination. • Bidder must not make multiple or split payments against a particular challan. Any split payment received against the same challan will be refunded back to the bidder.

		• Bidder would not be entitled to claim that he is deprived of participating in the tender because his funds are blocked with the division on account of incorrect payment made by the bidder
2	**In the event of making Payment through OTC**	**Do's** It is the bidder's responsibility to ensure that OTC payments are made to the exact details as mentioned in the challan which are: Beneficiary account no: <client code> + <random number> Amount: As mentioned on the challan It is specific for every tender/transaction Beneficiary name: As per the challan Bidder has to make only single payment against a challan as per the amount mentioned on the challan Bidder must do the payment before tender validity gets expired Bidder needs to mandatorily upload the scan copy of the payment receipt issued by ICICI Bank, in Nextender Portal before submitting the Tender
		Don'ts • If the bidding amount is greater than Rs49,999, then • Bidder should not make payment in cash. In this case, • Bidder should pay via Demand Draft/ICICI Bank Cheque • It is bidder's responsibility to ensure that Demand draft should be valid and should not have discrepancies such as signature not found, stale DD, mutilated, material alteration, favouring third party etc., Inthe event of Demand Draft returned by bidder's Bank on account of such discrepancies, ICICI Bank shall ensure that such communication is sent to the Client within 3 days from the date of rejection by the Bidder's Bank • For every tender, details in the challan are different and specific to that tender only. Bidder should not make use of a challan for making payment for another tenders' EMD

COVERING LETTER:

Format of letter to be submitted with the Tender forProcurement & Rate Contract for 1 Year of Wi-Fi Equipment for strengthening Wi-Fi Coverage, **University Computer Centre**, M.D. University, Rohtak- 124001.

TO,

Deputy Registrar
Purchase & Supply Branch
MD University
Rohtak – 124001 (Haryana)

SUB:PROCUREMENT & RATE CONTRACT FOR 1 YEAR OF WI-FI EQUIPMENT FOR STRENGTHENING WI-FI COVERAGE TO UNIVERSITY COMPUTER CENTRE ROHTAK.

Dear Sir,

1. This is with reference to your TENDER notice dated …….. I have examined the TENDER document and understood its contents. I hereby submit e-tender for Procurement & Rate Contract for 1 Year of Wi-Fi Equipment for strengthening Wi-Fi Coverage, **University Computer Centre**, M.D.University, Rohtak- 124001,
2. The Bid is unconditional for the said Tender. This bid is valid for a period not less than 180 days.
3. It is acknowledged that the Authority will be relying on the information provided in the Tender and the documents accompanying such Tender for qualification of the bidders for the above subject items and we certify that all information provided in the Tender and in Annexures are true and correct; nothing has been misrepresented and omitted which renders such information misleading; and all documents accompanying the bid are true copies of their respective originals.
4. This statement is made for the express purpose of the above mentioned subject.
5. We shall make available to the Authority any additional information it may find necessary or require to supplement or authenticate the Qualification statement.
6. We acknowledge the right of the Authority to reject our bid without assigning any reason or otherwise and hereby relinquish, to the fullest extent permitted by applicable law, our right to challenge the same on any account whatsoever.
7. It is declared that:
   a) We have examined the Tender document and have no reservations to the Tender document.
   b) We have not directly or indirectly or through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice in respect of any Bid or request for proposal issued by or any Agreement entered into with the

      Authority or any other public sector enterprise or any Government, Central, State or local.

8. It is understood that the University may cancel the Bidding Process at any time without incurring any liability to the University and that you are neither bound to invite the applicants to Bid for the items nor to accept any bid that you may receive.
9. It is understood that the University can use any evaluation scheme/evaluation metrics/weightage or take the help of any consultant, as required in selecting the successful agency/agencies and we agree to abide by it.
10. It is certified that wehave not been convicted by aCourt of Law or indicted or adverse orderspassed by a regulatory authority which could cast a doubt on our ability to undertake the Services or which relates to a grave offence that outrages the moral sense of the community.
11. It is here by certified that the firm has not been debarred/blacklisted for any reason/period by any central/state Govt. department/University/PSU etc. if so particulars of the same may be furnished. Concealments of facts shall not only lead to cancellation of the order but may also warrant legal action.University may reject bids of firms which has been blacklisted at any time.
12. It is hereby affirmed that we are in compliance of/shall comply with the statutory requirements, as applicable.
13. We hereby irrevocably relinquish any right or remedy which we may have at any stage at law or howsoever otherwise arising to challenge or question any decision taken by the Authority in connection with the selection of bidders, selection of the Tenderer, or in connection with the selection/Bidding Process itself, in respect of the above mentioned items and the terms and implementation thereof.
14. We agree to undertake to abide by all the terms and conditions of the TENDER document.
15. We agree to undertake to be liable for all the obligations of the Tenderer under the Agreement. In witness thereof, we submit this application under and in accordance with the terms of the TENDER document.

Place:- …….

Date :……..

Yours faithfully,

(Signature, name and designation of the Tenderer/Authorized Signatory)

Official Seal

CHECK LIST FOR DOCUMENTS TO BE SUBMITTED ALONGWITH TECHNICAL BID

1. Processing Charge Rs. 4000/- through Demand Draft (Non-Refundable).
2. Bid document signed & stamped on each page.
3. A photocopy of the Authorization Certificate from OEMs.
4. Power of Attorney, as applicable, on company letter head.
5. Details of service support centers located in Delhi/NCR/Haryana.
6. EMD 2% of total Bid Amount.
7. Attested photocopies of Income **Tax and Sales Tax returns** for the last three Financial Years (2014-15, 2015-16, 2016-17).
8. Contact details of 5 customers, along with P.O. photocopy and/or installation report.
9. Financial Bid in separate sealed envelope.
10. A duly attested photo copy of the Firm Registration number and PAN Number.
11. Any other information that the bidder may like to submit in support of his capabilities and performance etc.

NOTE

1. In case of any queries on technical specifications, please refer the specifications mentioned in "Annexure A" only.
2. Delivery to be made at :

   UNIVERSITY COMPUTER CENTRE
   MD University
   Rohtak-124 001
   Haryana, India
3. VAT will be at concessional rates, as applicable to non-profit, own-use institutions.
4. Filled quotations may be personally submitted P&S Branch Rohtak or sent through Registered Post or Courier addressed to:

   UNIVERSITY COMPUTER CENTRE
   MD University
   Rohtak-124 001
   Haryana, India
5. The decision of acceptance of the quotation will lie with the competent authority of University, who does not bind himself to accept the lowest quotation and who reserves the right to himself to reject or accept any or all quotations received, without assigning any reason.
6. The quotations are liable to be rejected if any of the above conditions are not fulfilled or if the bid is not accompanied with EMD and Processing Charge.
7. Number of items may vary, as required.
8. The University reserves the right to split the order among more than one Tenderers.
9. Financial Bid of the Tenderers who qualify in the Technical Bid shall be opened in presence of the authorized designated representatives and Tenderers who wish to be present there. The date of Financial Bid opening will be informed to the shortlisted bidders subsequently.
10. The University will be at liberty to involve any expert or consultant in evaluating the bid for completing the entire bid process.

SUBMISSION OF TENDER

SEALING AND MARKING OF TENDER:

1. The TENDER must be complete in all aspects and should contain requisite certificates, informative literature etc.
2. This is a two part bid consisting of Technical Bid and Financial bid
3. The bid shall include:
   a. Forwarding letter by the Tenderer
   b. All required documents
   c. Tender processing charges (non-refundable)
   d. Interest free EMD (Earnest Money Deposit) in the form of Demand Draft in favour of Finance Officer MD University Rohtak, payable at Rohtak, from a Nationalized Bank to be submitted with Technical Bid.
   e. Technical Bid
   f. Financial Bid
4. TENDER should be addressed to: -

UNIVERSITY COMPUTER CENTRE
MD University
Rohtak-124
001 Haryana,
India

EXPENSES OF AGREEMENT:

All the expenses on the execution of the Agreement (if any) including cost of stamp or any other kind of expenditure incurred in the process of TENDER submission till final compliance shall be borne by the Tenderer.

DEADLINE FOR SUBMISSION OF BIDS:

TENDER must be received by the MD University Rohtak at the date, time and address specified in the TENDER notice/TENDER documents.

LATE BIDS:

Any TENDER received after the deadline specified for submission of TENDER shall be rejected without any further correspondence to the Tenderer.

TENDER OPENING

OPENING OF FINANCIAL BID:

Financial Bid (Tenders) of the Tenderers who qualify in the Technical Bid shall be opened in the presence of designated Authority and Tenderers who wish to be present there. The date of financial bid opening will be informed to the shortlisted bidders subsequently.

CLARIFICATION OF TENDER:

To assist in the examination, evaluation and comparison of Tender, University may at its discretion ask the Tenderers for a clarification on the Tender which is submitted by him. The request for clarification and the response shall be in writing.

University will be at liberty to involve any expert or consultant and use appropriate metrics and weightages in evaluating the bid for completing the entire bid process.

AWARD OF PURCHASE ORDER

Successful Tenderer shall be awarded the Purchase Order. If after accepting the Purchase Order, the agency fails to supply the items, EMD will be forfeited and the agency will be blacklisted, in addition to recourse to other penal measures. No grievance will be entertained in this regard.

6.1 University reserves the right to negotiate with eligible Tenderer before finalization of the Tender and/or contract.

6.2 University reserves the right at the time of award of Purchase Order to increase or decrease even obsolete the number of items without any change in terms and conditions.

6.3 The bidders must quote rates and other terms and conditions for all the equipment's/items failing which tender will be rejected. Total cost of the bid will be one of the important deciding factor while deciding the bid in favor or against any bidder.

NOTIFICATION OF AWARD

Prior to the expiration of the period of Tender validity, the University will inform the Tenderer appropriately that the Bid has been accepted and the Purchase Order has been awarded.

(Signature of Tenderer)

Official seal

The* Procurement & Rate Contract for 1 Year of Wi-Fi Equipment for strengthening Wi-Fi Coverage** *as per* ***Annexure 'A' *are required to be purchased for this University. You are requested to kindly quote your rates for the same. The terms & conditions for quoting/tendering the rates given in enclosed page may also be kept in view and signed. Your tender will interalia be subject to the following conditions: -*

1. The packing, forwarding, freight, insurance charges etc. may be quantified in terms of amount. These charges will not be payable against such vague statement as "packing, forwarding, freight and insurance charges etc. extra".
2. Charges not mentioned in the tender shall not be paid.
3. FOR shall be M.D. University, Rohtak or Offices situated at Outstations as the case may be. The rates quoted Ex-Godown can be rejected.
4. The offer/rates must be valid for a period of at least three months from the date of opening of tender.
5. The authorized bidder must have a minimum annual turnover of Rs. 10.00 crores failing which the bid will be rejected. Proof of turn over may be appended with the bid.
6. The current price list duly authenticated by the Principals with dated signature and seal along with literature/pamphlets may be supplied along with the offer.
7. The quantity may increase or decrease or obsoleted without any notice. The University shall communicate the increase or decrease within 90 days of acceptance of tender.
8. The University is situated within the Municipal Limits. As such, Octroi, if any, shall be payable. In case, the material is supplied through a Transport Company by road, the Transport Company's charges, labour charges and octroi charges shall be borne by the supplier. It may be mentioned specifically as to whether the material will be sent by rail or by road through a Transport Company.
9. The goods shall be supplied by the Supplier within the time limit specified in the supply order. The delivery period can be extended by the Director UCC with the approval of registrar only in exceptional cases on written request of the Supplier giving reasons/explaining circumstances due to which delivery period could not be adhered to. **In case, the material is not supplied within the delivery period, the supplier shall be liable to pay the University the compensation amount equivalent to 1% (one percent) of the cost of material per week or such other amount as the Registrar may decide till the supply remains incomplete, provided that the total amount of compensation shall not exceed 10% (ten percent) of the total amount of the cost of material supplied.** Appeal against these orders shall, however, lie with the Vice-Chancellor, M.D.University, Rohtak whose decision shall be final.
10. In case, the supplier/contractor fails to execute the supply order/contract on the rates, and terms and conditions as contained in the supply order within the stipulated period, they shall be liable to such action as blacklisting, debarring from having any business with this University,

forfeiture of earnest money/security, besides any other action as may be deemed proper by the University.

11. As a general policy, the University tries to make 100% payment within 15 days of the receipt of material subject to proper installation, wherever applicable, and satisfaction of the Inspection Committee. No advance payment or payment against documents negotiated through Bank shall be made. However, Advance payment may be made against security for imported items to avil Custom Duty Exemption.
12. The acceptance of the material shall be subject to satisfactory report of this Office's Inspection Committee/Technical Committee/Experts Committee.
13. The samples of the material, if necessary and possible, shall be supplied with the tender. The unapproved samples shall be collected on receipt of information failing which the same shall be dispatched by Goods Carrier on your risk with the condition of **"Freight to Pay"**. Samples **costing less than** Rs. 100.00 shall not be returned to the **quotes**. However, if the **quotes** wish to take the same back, it can be collected at their own cost within a period of one month, failing which the samples will be disposed off.
14. The bidder should possess minimum 3 Years' experience in direct supply, installation, testing and commissioning of similar equipment/Software's and support to the Govt./Public Sector/Reputed Institutions for a minimum of 2 orders. Proof of direct dealership details i.e. OEM authorization letter/dealership certificate for supply along with Prime Customers contact details and photocopies of Purchase Order and/or installation report, to whom the similar Products Have Been supplied by the Tenderers, is required to be submitted along with the Technical Bid.
15. The vendor will also provide complete technical and operational training with no cost and the virtual lab/class will be provided the vendor at no extra cost for R&D before and after the commencement of project for at least 2 persons one time.
16. All the features present in the devices should come with all required licences from day 1.
17. All the ports should carry valid licences for enabling or disabling. No port constraint should be put as a hidden cost on MDU.
18. All Core equipment's/switches should carry a warranty and support of 24x7 for 5 Years.
19. All layer 2 switches should be manageable via GUI preferably over http/https.
20. The acceptance of the tender shall rest with the undersigned who does not bind himself to accept the lowest tender and reserves the right to reject any or all items of tender without assigning any reason therefore. The undersigned also reserves the right to accept tender in part i.e. any item or any quantity and to reject it for the rest.
21. The University is registered with the Department of Scientific & Industrial Research, Ministry of Science & Technology, New Delhi in terms of Govt. Notification No. 10/97- Central Excise dated 1 March, 1997 and Notification No. 51/96-Customs dated 23.7.1996 vide Registration No. TU/V/RG-CDE(244)/2015 dated September, 1,2015 upto 31-08-2020. Thus the University is exempted from payment of Custom Duty, GST is applicableat concessional rate. The consignee

shall issue necessary certificates duly countersigned by the Registrar, M.D. University, Rohtak to avail of exemption.

22. It may be certified that you have not been debarred/ blacklisted for any reason/period by DGS&D, DS&D (Haryana) or any other Central/State Govt. Dept./University/PSU etc. If so, particulars of the same may be furnished. Concealment of facts shall not only lead to cancellation of the supply order, but may also warrant legal action.
23. In case, any other information/clarification is required, the undersigned may be contacted at Telephone No. 01262-393548 on any working day (Monday to Friday) during office hours (9 a.m. to 5.00 p.m.).
24. **Access point under any circumstances shall not work in absence of controller. Violation of which may lead to rejection of Bid.**
25. Approved make are CISCO, HPE/Aruba (present in leaders quadrant of Gartner Report for wired & wireless LAN access infrastructure) and Fortinet (existing Wi-Fi vendor).
26. The successful bidder has to deposit a Performance Guarantee equal to 5% of annual cost of Material, in the form of FDR/Bank Guarantee/TDR for the warranty period (5 years), in the name of Finance Officer MD University Rohtak. When Performance Guarantee/warranty is deposited, EMD will be returned subsequently.
27. The Financial Bid should be accompanied with an Earnest Money Deposit (EMD) of Rs. 2% of Bid Amount rounded to the nearest ten thousand through Online using E-tender Portal. EMD of unsuccessful bidder will be returned subsequently. No interest shall be paid on EMD.
28. The Firms registered with NSIC /NSME are exempted from Tender Fee and EMD, copy of the valid certificate must be uploaded with technical cover
29. After winning the order, if the vendor fails to deliver product and provides satisfactory Warranty, EMD will be forfeited and also the vendor will be blacklisted from participating in any future bid.
30. The Sub Committee reserves the right for negotiation thereafter if considered necessary.
31. No tender documents will be issued and rates are to be offered on Company's Letter Pad.
32. The rates should be quoted for required specifications. The technical specification of the equipment's required must accompany the tender. The decision of the University will be final with regard equipment's to be purchased.
33. The bidders must quote rates and other terms and conditions for all the equipment/items failing which tender will be rejected. Total cost of the bid will be one of the important deciding factor while deciding the bid in favour or against any bidder.
34. University reserves the right at the time of award of Work Order to increase or decrease or even delete the number of items without any change in terms and conditions.
35. The tender should be submitted only if the material is readily available in your stock or can be supplied within 45 days after the order is placed.

36. The dispute, if any, shall be subject to the jurisdiction of Courts at Rohtak. Any other jurisdiction mentioned in the tender or invoices of the manufacturers/distributors/ dealers/suppliers etc. shall be invalid and shall have no legal sanctity.
37. Terms and conditions should Invoice or other letters of the firm, if any, shall not be binding on the University, except those mentioned specifically on the supply order, and your acceptance of the order shall be construed as your agreement to all the terms and conditions contained in the order.
38. No Consortium BID is allowed.
39. The Bidder should be doing Business in India for this particular OEM for at least last 5 years.
40. The Bidder should be a company incorporated and registered in India Under the companies Act, 1956.
41. Bidder should be ISO 9001 Certified.

Signature _____

Name of the firm with seal/stamp _____ **M. D. University, Rohtak**

Affix Rubber Stamp of the firm

BOQ (CONSOLIDATED REQUIREMENT SHEET)

Proposed BoQ: as per specifications below		
S. No.	Description	**Required Qty**
1.	Wireless Controller	1
2.	Indoor Access points	150
3.	Outdoor Access Points	30
4.	Outdoor point-to-point wireless connection:	2
5.	POE Switches	20

Technical Compliance Envelope

ANNEXURE-A

WIRELESS CONTROLLER& AAA SERVER (ON CAMPUS OR CLOUD BASED) IF REQUIRED - WE HAVE FORTIGATE CONTROLLER FOR OTHER OEM IT WILL BE REQUIRED

Sr. No.	Specifications	Compliance	Vendor Remarks
A	**Hardware Specifications**		
A1	Must be compliant with IEEE CAPWAPor equivalent for controller-based WLANs.		
A2	Should have at least 2 x 10 Gigabit Ethernet interface.		
A3	Should support both centralized as well as distributed traffic forwarding architecture with L3 roaming support from day 1. Should have IPv6 ready from day one.		
A4	Controller should have hot-swappable redundant power supplies.		
A5	Controller should support Solid State Drive (SSD) based storage		
A6	Controller should be capable of supporting both 1G and 10 G SPFs on same Network I/O ports		
A7	Should support Software Defined Segmentation, reducing the ACL maintenance, complexity and overhead		
A8	Controller should support minimum 20,000 users per chassis		
A9	WLAN Controller should support minimum of 1500 Access points in a single chassis. If any OEM/Bidder can't provide WLAN controller to support 1500 AP in single RU form factor, multiple controllers must be proposed to meet the requirement from day one. Proposed controller should support N+N redundancy from day one		
A10	Shall support WIPS, and spectral analysis from day 1.		
A11	Should be rack-mountable. Required accessories for rack mounting to be provided.		
A12	WLC should support AVC functionality on local switching architecture		
A13	WLC should support AC Powering options		
A14	WLC should support AP License Migration from one WLC to another		
A15	**S**hould support minimum 4000 VLANs		
B	**Wireless Controller Features**		
B1	Must support stateful switchover between active and standby controller in a sub second time frame.		
B2	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients		

B3	WLC should support guest-access functionality for IPv6 clients.		
B4	Should support IEEE 802.1p priority tag.		
B5	Should ensure WLAN reliability by proactively determining and adjusting to changing RF conditions.		
B6	Should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments.		
B7	Should support automatic radio channel adjustments for intelligent channel switching and real-time interference detection.		
B8	Should support client load balancing to balance the number of clients across multiple APs to optimize AP and client throughput.		
B9	Should support policy based forwarding to classify data traffic based on ACLs		
B10	WLC should support PMIPv6/Equivallent and EoGRE/IPSEC tunnels on northboud interface		
B11	Should support flexible DFS to prevent additional 20/40 Mhz channels from going unused		
	Should support dynamic bandwidth selection among 20Mhz, 40 Mhz and 80Mhz channels, ensuring one access point on 20Mhz and another on 80 Mhz channel connected on the same controller at same WLAN group.		
B12	Should support minimum 500 WLANs		
B13	Should support dynamic VLAN assignment		
B14	Should support Hot Spot 2.0		
B15	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.		
B16	Should able to do dynamic channel bonding based on interference detected on particular channel.		
B17	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.		
B18	Must support RF Management with 40 MHz and 80 Mhz channels with 802.11n & 802.11ac		
B19	Should provide visibility to Network airtime in order to set the airtime policy enforcement		
B20	Must support dynamic Airtime allocation on per WLAN, per AP, Per AP group basis.		
B21	Must be able to restrict the number of logins per user.		
C	**Security**		

C1	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.		
C2	Should support port-based and SSID-based IEEE 802.1X authentication.		
C3	Should support MAC authentication to provide simple authentication based on a user's MAC address.		
C4	WLC Should support Rogue AP detection, clasification and standard WIPS signatures.		
C5	WLC should be able to exclude clients based on excessive/multiple authentication failure.		
C6	Shall support AES or TKIP encryption to secure the data integrity of wireless traffic		
C7	Shall support the ability to classify over 20 different types of interference		
C8	Shall able to provide an air quality index for ensuring the better performance		
C9	Shall able to provide real time chart showing interference per access point on per radio and per-channel basis.		
C10	Should support AP location-based user access to control the locations where a wireless user can access the network		
C11	Should support Public Key Infrastructure (PKI) to control access		
C12	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.		
C13	WLC Shall support WIDS/WIPS, and spectral analysis from day 1.		
C14	WLC should detect if someone connect a Rogue Acess Point in network and able to take appropriate action to contain rogue Acess point.		
C15	WLC should detect and protect an Ad-hoc connection when a connected user forming a network with other system without an AP or try enabling bridging between two interface		
C16	WLC should detect if a user try to impersonate a management frame.		
C17	WLC should detect and take appropriate containment action if a smartphone user using tethering to connect other device.		
C18	WLC should detect and protect if a user try to spoof mac address of valid client or AP for unauthorized acess/authentication.		
C19	WLC should detect if a user trying to do internet sharing through a valid system to an unauthorized device.		

D	**Management &QoS**		
D1	Should support SNMPv3, SSHv2 and SSL for secure management.		
D2	Should support encrypted mechanisum to securely upload/download software image to and from Wireless controller.		
D3	Should provide visibility between a wired and wireless network using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and sFlow/equivalent.		
D4	Should support AP Plug and Play (PnP) deployment with zero-configuration capability		
D5	Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group		
D6	Should support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation		
D7	Should have a suitable serial console port.		
D8	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS		
D9	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 in a central and local switching mode.		
D10	Should be able to do application visibility for application running behind HTTP proxy.		
D11	Support profiling of wireless devices based on known protocols like http and dhcp to identify clients		
D12	Should support visibility and control based on the type of applications		
E	**Guest Access Solution**		
E1	Integrated/ External Solution must provide Self registration based Guest access workflow for minimum 4000 users. Bidder must quote necessary compute for external solution.		
E2	Should support sponsored based Guest access workflow.		
E3	Should Support different custom branding of captive portal for Laptop and mobile.		
E4	Should support RADIUS authentication.		
E5	Should support integration with SMS gateway for OTP.		
	AAA Access Control		
	General Requirements		

1	Solution should integrate seamlessly with MDU's existing IT infrastructure comprising of routers, switches, various types of WAN links and computers, devices, printers, IP phones, Operating Systems etc.		
	Broad Requirement		
2	Solution should support a highly powerful and flexible attribute-based access control solution that combines authentication, authorization and accounting (AAA), NAC, BYOD, posture, profiling, guest management services and conditional elements on a single dedicated platform. This features should not be part of any Firewall/UTM functionality.		
3	It should allow to authenticate and authorize users and endpoints via wired, wireless and VPN with consistent policy throughout the enterprise and should support variety of authentication methods (802.1X, MAC auth, Web authetc).		
4	Solution support agent and dissolvable agent method for performing endpoint profiling, base-lining, health check and prevention		
	Capacity & Architecture Requirement		
5	The proposed solution should support minimum 5,000 devices from day one for AAA and Guest management and should be scalable to 7500 devices without requiring hardware upgrade for AAA and Guest Management. It also include complete Logging Features.		
	Functional Requirement		
6	Solution should Support EAP-FAST, PAP, MS-CHAPv1, MS-CHAPv2, EAP-GTC, EAP-TLS and PEAP-TLS Authentication Protocols		
7	Enable administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, greatly simplifying administration by providing consistency in managing all these services, when all services are enabled by licenses		
8	Solution should support the capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).		
9	Identity and access management. Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.		
10	Readymade Policies, ability for custom policy creation and enforcement		
11	Policy for Time Based Access		
12	Location Based Access		

13	Policy creation tools: • Pre-configured templates • Wizard based interface • LDAP browser for quick look-up of AD attributes • Policy simulation engine for testing policy integrity		
14	Should Support Visibility into user identities and device types		
15	Guest user self-enrollment		
16	Support for WPA2,WEP secure wireless and wired networks		
17	Workflow for user and device registration		
18	Access control lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs.		
	Role based administrative capabilities		
19	The solution Must be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform a. Built-in guest management and device/user onboarding b. Web based management interface with Dashboard c. Reporting and analysis with custom data filters d. Data repository for user, device, transaction information e. Rich policies using identity, device, health, or conditional elements f. Deployment and implementation tools.		
20	Solution must support Non 802.1x technology on assigned ports and 802.1x technology on open use ports		
21	Solution should support Mac Address Bypass (MAB) and can further utilize identity of the endpoint to apply the proper rules for access. Mac Address Bypass is typically used for devices which do not support 802.1x		
22	Solution should support the capability to get finer granularity while identifying devices on the network with Active Endpoint Scanning. This Feature will be required in future upgrades without adding additional Hardware.		
23	Solution should have capability to grant authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.		
24	Solution should support endpoint access to the network with the Endpoint Protection Service, which enables administrators to specify an endpoint and select an action - for example, move to a new VLAN, return to the original VLAN, or isolate the endpoint from the network entirely - all in a simple interface. This Feature will be required in future upgrades without adding additional Hardware.		

25	It should support Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type. This Feature will be required in future upgrades without adding additional Hardware.		
26	Verifies endpoint posture assessment for PCs connecting to the network. Works via either a persistent client-based agent or a temporal web agent to validate that an endpoint is conforming to a company's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc), and applications. Solution should support auto-remediation of PC clients as well as periodic reassessment to make sure the endpoint is not in violation of company policies. This Feature will be required in future upgrades without adding additional Hardware.		
27	Solution should classify a client machine, and should support client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles, if necessary. This Feature will be required in future upgrades without adding additional Hardware.		
28	Solution should have automatic switch vlan provisions for end device based on pre-defined rule		

29	Solution should support the following endpoint checks for compliance for windows endpoints: I. Check operating system/service packs/hotfixes II. Check process, registry, file & application III. check for Antivirus installation/Version/ Antivirus Definition Date IV. check for Antispyware installation/Version/ Antispyware Definition Date V. Check for windows update running & configuration VI. Solution should support following remediation options for windows endpoints: VII. File remediation to allow clients download the required file version for compliance VIII. link remediation to allow clients to click a URL to access a remediation page or resource IX. Antivirus remediation to update clients with up-to-date file definitions for compliance after remediation. X. Antispyware remediation to update clients with up-to-date file definitions for compliance after remediation. XI. Launch program remediation for NAC Agent to remediate clients by launching one or more applications for compliance. XII. Windows update remediation to ensure Automatic Updates configuration is turned on Windows clients per security policy **This Feature will be required in future upgrades without adding additional Hardware.**		
30	Solution should support automated remediation and integration with all major OEM Antivirus, patch update and O/S systems. This Feature will be required in future upgrades without adding additional Hardware.		
31	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets.		
32	Soltuion should support user authentication performed against identity, user credentials, role based access control, or attribute based authentication (location, time, etc.)		
33	Solution should allow only authenticated and managed devices to connect to organisation network		
34	Solution should support to Integrate with firewall, IPS, Router, Switch, Wireless Access Points, Active Directory, LDAP, MDM solutions etc of major OEMs		
35	Solution should support granular level policy enforment and provide information about users beyound that obtained in a login system		
36	Solution should detect network threats by itself or by integrating with other Security defences and should be prevented from spreading and notifications to be sent to end user and administrator concerning the network threat activity via e-mail and http notification		
37	Integration with Firewalls for unified access across the		

	network.		
38	Solution should have endpoint client capability to be installed in endpoints via Active Directory group policy		
39	Solution should allow NAC credentials to be stored within a trusted protection module or other secured storage mechanism		
40	Solution should support the following guest networking capabilities: a. automated provisioning of network login credentials b. network access to certain hours of the day c. secured profile control related to the application uses for guest users		
41	Solution should provision guests notification of their login credentials by: email, SMS etc		
42	Provides complete guest lifecycle management by empowering sponsors to on-board guests		
43	Delivers customizable self service portals as well as the ability to host custom web pages to ease device and guest on-boarding, automate endpoint secure access and service provisioning, and enhance the overall end-user experience inside business-defined workflows		
44	Solution should allow end users to interact with a self-service portal for device on-boarding, providing a registration vehicle for all types of devices as well as automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms.		
45	Solution should support the capability to determine whether users are accessing the network on an authorized, policy-compliant device.		
46	The portal used for Device registration (MY device Portal) should be customizable, allowing to customize portal theme by changing text, banners, background color, and images		
47	Should provide a Registered Endpoints Report which provides information about a list of endpoints that are registered through the device registration portal by a specific user for a selected period of time. The report should provide the following :•Logged in Date and Time •Portal User (who registered the device) •MAC Address •Identity Group •Endpoint Policy •Static Assignment •Static Group Assignment •Endpoint Policy ID •NMAP Subnet Scan ID •Device Registration Status		

48	Solution should have capability to look at various elements when classifying the type of login session through which users access the internal network, including the following: •Client machine operating system and version •Client machine browser type and version •Group to which the user belongs •Condition evaluation results (based on applied dictionary attributes)		
49	Should support full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Allows administrators to customize portals and policies based on specific needs of the enterprise		
50	Solution should support threat monitoring, containment, and remediation, extending beyond rogue detection and authentication		
51	Should support session termination with port shutdown option to block an infected host that sends a lot of traffic over the network. This Feature will be required in future upgrades without adding additional Hardware.		
52	Support for importing endpoints from LDAP server. Should allow to import MAC addresses and the associated profiles of endpoints securely from an LDAP server		
53	Should support multiple Admin Group Roles and responsibilities like HelpDesk Admin, Identity Admin, Monitoring Admin, Network Device Admin, Policy Admin, RBAC Admin, Super Admin and System Admin		
54	Must incorporate a complete set of tools for reporting (Audit trailing, customizable reporting and data export capabilities), analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together		
55	Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.		
	AAA, NAC, BYOD and Guest Management Solution		
56	Solution should support to generate real time and on demand reports		
57	Solution should be capable of Real-Time Monitoring, Management & event Collection		
58	Solution should support alert mechanisms like email, smsetc		
59	Solution should be able to monitor, audit and tie incidents to a specific user		

60	Solution should have various inbuilt and customized dashboards like solution health dashboards, concurrent users, logged in users etc		
61	Solution should provide detailed Event co-relation and analysis and also should integrate with other major SIEM tools		
62	The system should provide standard based external facing APIs to extend support and integration with external applications like SIEM, Firewall, IDS/IPS solutions etc		
63	Must be able to join multiple Active Directory domains to facilitate 802.1x PEAP authentication.		
64	Must be able to issue certificates using an inbuilt Certificate Authority		
65	Support the following enforcement methods: a. VLAN steering via RADIUS IETF attributes and VSAs b. VLAN steering and port bouncing via SNMP		
66	Encryption of traffic to the wireless and wired network using protocols for 802.1X such as EAP-TLS, EAP-PEAP or EAP-MSCHAP.		
67	Propose solution should integrate with proposed Firewall for contextual sharing.		
	Others		
68	**Bidder is required to quote all required software and hardware to support full functioning of the AAA/NAC/BYOD Solution and the management platform**		
69	**Bidder is required to quote all required licenses, software and hardware support for 5 years from the date of supply**		
70	**MDU requires the deployment design of the AAA/NAC to be created/approved by the proposed OEM directly**		
71	**A One Day training for operation & management of the proposed AAA/NAC device should be provided post successful deployment**		

OUTDOOR ACCESS POINTS

Sr. NO.	Specification	Compliance	Vendor Remarks
1	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.		
2	AP should support dual band antenna ports.		
3	Must support a variety of antenna options. (Omni and directional)		
4	Must have -88 dB or better Receiver Sensitivity.		
5	Must support 2x2 multiple-input multiple-output (MIMO) with two spatial streams		

6	Must support 802.11ac, Wave 2 and backword compatible with 802.11n standards		
7	Must support datarateupto 867 Mbps on 5Ghz radio.		
8	Must support 80 MHz wide channels in 5 GHz.		
9	Must support WAPenforced load-balance between 2.4Ghz and 5Ghz band.		
10	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data		
11	Must support upto 24dbm or heigher of transmit power		
12	Accesspoint should 802.11ac, 802.11n and 802.11a/b/g Beamforming		
13	The Wireless Backhaul/Mesh shall operate in 5Ghz		
14	Support Encrypted and authenticated connectivity between all backhaul components		
15	Access point should have multiple wired uplink interfaces including 10/100/1000BASE-T Ethernet autosensing (RJ-45) and a build-in SFP port		
16	Wireless AP should support beamforming technology to improve downlink performance of all mobile devices, including one-, two-, or three-spatial-stream devices on 802.11ac without taking the inputs from client.		
17	Wireless AP Should able to detect and classify non-Wi-Fi wireless transmissions.		
18	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data.		
19	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		
20	Access point shall support powering from AC /DC/ UPOE.		
21	Access point shall support pole, wall and Cable strand mounting options.		
22	The equipment shall support up to 100 MPH sustained winds & 120 MPH wind gusts.		
23	The Access point shall be IP67 rated		
24	The Access point shall support operating temperature of -20 to 65°C		
25	The Access point shall support Storage temperature of -20 to 70°C		
26	802.11e and WMM		
27	WiFi Alliance Certification for WMM and WMM power save		
28	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level		
29	Must support QoS and Video Call Admission Control capabilities.		

30	Must support the ability to serve clients and monitor the RF environment concurrently.		
31	Must support Spectrum analysis including @ 80 MHz		
32	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		
34	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.		
35	Should have and option of configuring all the antennae port via software to run all on dual band or any single band configuration.		
36	Must support 16 WLANs per AP for BSSID deployment flexibility.		
37	Must support telnet and SSH login to APs directly for troubleshooting flexibility.		

INDOOR ACCESS POINTS

Sr. No.	Specification	Compliance	Vendor Remarks
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave 2		
2	Access Point must provide Kensington lock option for theft protection.		
3	Must have internal / external antenna options.		
4	Mounting kit should be standard from OEM directly.		
5	The Access Point should have a capability to handle high density environment with more number of concurrent users by having more memory and CPU power		
6	Access point must support flexible Dynamic Frequesncy Selection across 20Mhz, 40Mhz, 80MHz and 160Mhz wide channels to combat performance problems due to wireless interference.		
7	Access point must have an additional USB port for future use.		
8	Access point should have 2x10/100/1000 Ethernet and serial/console port		
9	Must have atleast 3 dBi Antenna gain on both 2.4 Ghz and 5Ghz		
10	Must support 4X4 multiple-input multiple-output (MIMO) with three spatial streams		
11	Must support the physical rate of 1.73Gbps on 5GHz radios.		
12	Must support minimum of 22dbm of transmit power on both 2.4 Ghz& 5GHz Radio.		
13	The AP must be capable of optimizing the SNR exactly at the position where 802.11a/g/n/ac client is placed (beamforming) without requiring any support or feedback		

	from clients, hence it should work with all 802.11a/g/n/ac clients.		
14	Should have detecting and classifying non-Wi-Fi wireless transmissions while simultaneously serving network traffic		
15	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data.		
16	Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.		
17	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		
18	Must have -94 dB or better Receiver Sensitivity.		
19	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.		
20	Must support Management Frame Protection.		
21	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
22	Must operate as a sensor for wireless IPS		
23	Should support non-Wi-Fi detection for off-channel rogues and Containment for both radio while serving the client simaltaniously.		
24	Access Points must support a distributed encryption/decryption model.		
25	Access Points must support Hardware-based encrypted user data and management traffic between controller and Access point for better security.		
26	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		
27	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services.		
28	Mesh support should support QoS for voice over wireless.		
29	Must be plenum-rated (UL2043).		
30	Must support 16 WLANs per AP for SSID deployment flexibility.		
31	Must continue serving clients when WAN link to controller is back up again, should not reboot before joining		
32	The APs must support centralized wireless mode with the use of a controller		
33	When operated in remote AP mode, the AP must not disconnect any clients when the connection to the controller fails or in the case the failed connection has been restored again.		

34	Access point should able to do the spectrum scanning for Wi-Fi and non-WiFi interference for both on-channel and off-channel at all 20Mhz ,40Mhz, 80Mhz and 160Mhz channels		
35	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.		
36	Must support Power over Ethernet)/ power injectors.		
37	802.11e and WMM		
38	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level		
39	Must support QoS and Video Call Admission Control capabilities.		

OUTDOOR POINT-TO-POINT WIRELESS CONNECTION:

Sr. No.	Specifications	Compliance	Vendor Remarks
1	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.		
2	AP should support dual band antenna ports.		
3	Must support a variety of antenna options. (Omni and directional)		
4	Must have -88 dB or better Receiver Sensitivity.		
5	Must support 2x2 multiple-input multiple-output (MIMO) with two spatial streams		
6	Must support 802.11ac, Wave 2 and backword compatible with 802.11n standards		
7	Must support dataratesupto 867 Mbps on 5Ghz radio.		
8	Must support 80 MHz wide channels in 5 GHz.		
9	Must support WAPenforced load-balance between 2.4Ghz and 5Ghz band.		
10	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data		
11	Must support upto 24dbm or heigher of transmit power		
12	Accesspoint should 802.11ac, 802.11n and 802.11a/b/g Beamforming		
13	The Wireless Backhaul/Mesh shall operate in 5Ghz		
14	Support Encrypted and authenticated connectivity between all backhaul components		
15	Access point should have multiple wired uplink interfaces including 10/100/1000BASE-T Ethernet autosensing (RJ-45) and a build-in SFP port		

16	Wireless AP should support beamforming technology to improve downlink performance of all mobile devices, including one-, two-, or three-spatial-stream devices on 802.11ac without taking the inputs from client.		
17	Wireless AP Should able to detect and classify non-Wi-Fi wireless transmissions.		
18	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data.		
19	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		
20	Access point shall support powering from AC /DC/ UPOE.		
21	Access point shall support pole, wall and Cable strand mounting options.		
22	The equipment shall support up to 100 MPH sustained winds & 120 MPH wind gusts.		
23	The Access point shall be IP67 rated		
24	The Access point shall support operating temperature of -20 to 65°C		
25	The Access point shall support Storage temperature of -20 to 70°C		
26	802.11e and WMM		
27	WiFi Alliance Certification for WMM and WMM power save		
28	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level		
29	Must support QoS and Video Call Admission Control capabilities.		
30	Must support the ability to serve clients and monitor the RF environment concurrently.		
31	Must support Spectrum analysis including @ 80 MHz		
32	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		
34	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.		
35	Should have and option of configuring all the antennae port via software to run all on dual band or any single band configuration.		
36	Must support 16 WLANs per AP for BSSID deployment flexibility.		
37	Must support telnet and SSH login to APs directly for troubleshooting flexibility.		
38	The Access Points must be supplied with antennas and accessories for Point to point communication with 1 Km Range		

24 PORT POE EDGE 1G SWITCH

Sl. No	Specifications	Compliance (Yes/ No)	Vendor's Remarks
A	**General Features**		
1	The switch should support a minimum of 24 nos. 10/100/1000 Ethernet Ports		
2	The switch should support a minimum of 4 SFP Uplinks		
3	The switch should support 4x1G SFP modules		
4	The switch should support a total of 28 Ports		
5	The switch should support MTBF of 324280 hours		
B	**Performance and Scalability**		
1	The switch should support Forwarding bandwidth of 108 Gbps		
2	The switch should support Full-duplex Switching bandwidth of 216 Gbps		
3	The switch should support 64-Byte Packet Forwarding Rate of 71.4 Mpps		
4	The switch should support a Dual Core CPU		
5	The switch should support 128 MB of Flash memory		
6	The switch should support 512 MB of DRAM		
7	The switch should support 1023 VLANs		
8	The switch should support 4096 VLAN IDs		
9	The switch should support Jumbo frames of 9216 bytes		
10	The switch should support Maximum transmission unit (MTU) of 9198 bytes		
11	The switch should support 16000 Unicast MAC addresses		
C	**Dimension**		
1	The Switch should be 1RU		
2	The switch should support Operating temperature up to 5000 ft (1500 m) -5º to 45ºC		
3	The switch should support Operating relative humidity 10% to 95% noncondensing		
D	**Stacking**		
1	The switch should support Stacking		
2	Stacking should enable all switches to function as a single unit		
3	The switch should support an optional Stacking Port		
4	Stacking module should be Hot-swappable		
5	Stacking should support a minimum of 2 or more Switches		
6	Stacking should support a maximum of 8 Switches		
7	Stacking should support 80 Gbps of throughput		
8	Stacking should support single IP address management for the group of switches		
9	Stacking should support single configuration		

10	Stacking should support simplified switch upgrade		
11	Stacking should support automatic upgrade when the master switch receives a new software version		
12	Stacking should support stacking cable length of 3m		
13	Stacking should support QoS to be configured across the entire stack		
E	**PoE&PoE+**		
1	The switch should support PoE (IEEE 802.3af)		
2	The switch should support PoE+ (IEEE 802.3at)		
3	The switch should support flexible power allocation across all ports		
4	The switch should have 370W of Available PoE Power		
5	The switch should support 24 ports up to 15.4W		
6	The switch should support 12 ports up to 30W		
7	The switch should support Per port power consumption to specify maximum power setting on an individual port		
8	The switch should support Per port PoE power sensing to measure actual power being drawn		
9	The switch should support protocol to allow switch to negotiate a more granular power setting of IEEE classiffied devices		
10	The switch should support a PoEMIB to get visibility into power usage		
11	The switch should support a PoEMIB to set different power-level thresholds		
F	**Power Supply**		
1	The switch should support an auto-ranging power supply with input voltages between 100 and 240V AC		
2	The switch should support an External Redundant Power Supply		
G	**Standards**		
1	The switch should support IEEE 802.1D Spanning Tree Protocol		
2	The switch should support IEEE 802.1p		
3	The switch should support IEEE 802.1Q Trunking		
4	The switch should support IEEE 802.1s Multiple Spanning Tree (MSTP)		
5	The switch should support IEEE 802.1w Rapid Spanning Tree (RSTP)		
6	The switch should support IEEE 802.1x		
7	The switch should support IEEE 802.1ab (LLDP)		
8	The switch should support IEEE 802.3ad Link Aggregation Control Protocol (LACP)		
9	The switch should support IEEE 802.3af Power over Ethernet		
10	The switch should support IEEE 802.3af Power Classification		

11	The switch should support IEEE 802.3at Power over Ethernet +		
12	The switch should support IEEE 802.3ah (100BASE-X single/multimode fiber only)		
13	The switch should support IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports		
14	The switch should support IEEE 802.3 10BASE-T specification		
15	The switch should support IEEE 802.3u 100BASE-TX specification		
16	The switch should support IEEE 802.3ab 1000BASE-T specification		
17	The switch should support IEEE 802.3z 1000BASE-X specification		
18	The switch should support RMON I and II standards		
19	The switch should support SNMP v1, v2c, and v3		
H	**RFC compliance**		
1	The switch should support RFC 768 – UDP		
2	The switch should support RFC 783 – TFTP		
3	The switch should support RFC 791 – IP		
4	The switch should support RFC 792 – ICMP		
5	The switch should support RFC 793 – TCP		
6	The switch should support RFC 826 – ARP		
7	The switch should support RFC 854 – Telnet		
8	The switch should support RFC 951 - Bootstrap Protocol (BOOTP)		
9	The switch should support RFC 959 – FTP		
10	The switch should support RFC 1112 - IP Multicast and IGMP		
11	The switch should support RFC 1157 - SNMP v1		
12	The switch should support RFC 1166 - IP Addresses		
13	The switch should support RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery		
14	The switch should support RFC 1305 - NTP for accurate and consistent timestamp		
15	The switch should support RFC 1492 - TACACS+		
16	The switch should support RFC 1493 - Bridge MIB		
17	The switch should support RFC 1542 - BOOTP extensions		
18	The switch should support RFC 1643 - Ethernet Interface MIB		
19	The switch should support RFC 1757 - RMON (history, statistics, alarms, and events)		
20	The switch should support RFC 1901 - SNMP v2C		
21	The switch should support RFC 1902-1907 - SNMP v2		
22	The switch should support RFC 1981 - Maximum Transmission Unit (MTU) Path Discovery IPv6		
23	The switch should support FRC 2068 – HTTP		

24	The switch should support RFC 2131 – DHCP		
25	The switch should support RFC 2138 – RADIUS		
26	The switch should support RFC 2233 - IF MIB v3		
27	The switch should support RFC 2373 - IPv6 AggregatableAddrs		
28	The switch should support RFC 2460 - IPv6		
29	The switch should support RFC 2461 - IPv6 Neighbor Discovery		
30	The switch should support RFC 2462 - IPv6 Autoconfiguration		
31	The switch should support RFC 2463 - ICMP IPv6		
32	The switch should support RFC 2474 - Differentiated Services (DiffServ) Precedence		
33	The switch should support RFC 2597 - Assured Forwarding		
34	The switch should support RFC 2598 - Expedited Forwarding		
35	The switch should support RFC 2571 - SNMP Management		
36	The switch should support RFC 3046 - DHCP Relay Agent Information Option		
37	The switch should support RFC 3376 - IGMP v3		
38	The switch should support RFC 3580 - 802.1X RADIUS		
I	**Layer-2 Features**		
1	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors		
2	The switch should support IEEE 802.1Q VLAN encapsulation		
3	The switch should support Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically		
4	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence		
5	The switch should support UplinkFast&BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability		
6	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.		
7	The switch should support IGMP filtering		
8	The switch should support discovery of the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
9	The switch should support Per-port broadcaststorm control to prevent faulty end stations from degrading overall systems performance		
10	The switch should support Per-port multicast storm control to prevent faulty end stations from degrading overall systems performance		
11	The switch should support Per-port unicast storm control to prevent faulty end stations from degrading overall systems performance		

12	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN		
13	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth		
14	The switch should support Automatic media-dependent interface crossover (MDIX) to automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.		
15	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.		
16	The switch should support Local Proxy Address Resolution Protocol (ARP) working in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.		
17	The switch should support IGMP v1, v2 Snooping		
18	The switch should support IGMP v3 Snooping		
19	The switch should support IGMP v1, v2 Filtering		
20	The switch should support IGMP Snooping Timer		
21	The switch should support IGMP Throttling		
22	The switch should support IGMP Querier		
23	The switch should support Configurable IGMP Leave Timer		
24	The switch should support MVR (Multicast VLAN Registration)		
J	**L3 Features**		
1	The switch should support Inter-VLAN routing		
2	The switch should support IPv4 unicast Static Routing		
3	The switch should support 16 IPv4 Static routes		
K	**Smart Operations**		
1	The switch should support configuration of the Software image and switch configuration without user intervention		
2	The switch should support automatic configuration as devices connect to the switch port		
3	The switch should support diagnostic commands to debug issues		
4	The switch should support system health checks within the switch		
5	The switch should support Online Diagnostics		
L	**Quality of Service (QoS) & Control**		
1	The switch should support 8 egress queues per port to enable differentiated management		
2	The switch should support scheduling techniques for Qos		

3	The switch should support Weighted tail drop (WTD) to provide congestion avoidance		
4	The switch should support Standard 802.1p CoS field classification		
5	The switch should support Differentiated services code point (DSCP) field classification		
6	The switch should support Control- and Data-plane QoS ACLs		
7	The switch should support Strict priority queuing mechanisms		
8	The switch should support Rate Limiting function to guarantee bandwidth		
9	The switch should support rate limiting based on source and destination IP address		
10	The switch should support rate limiting based on source and destination MAC address		
11	The switch should support rate limiting based on Layer 4 TCP and UDP information		
12	The switch should support availability of up to 256 aggregate or individual polices per port.		
M	**Management**		
1	The switch should support Command Line Interface (CLI) support for configuration & troubleshooting purposes.		
2	The switch should support four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis		
3	The switch should support Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.		
4	The switch should support Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.		
5	The switch should support SNMP v1, v2c, and v3 of-band management.		
6	The switch should support Telnet interface support for comprehensive in-band managementof-band management.		
7	The switch should support CLI-based management console to provide detailed out-of-band management.		
8	The switch should support Serial Console Port		
9	The switch should support USB Console Port		
10	The switch should support SNMPv1, SNMPv2c, and SNMPv3		
N	**Miscellaneous**		
1	The switch should support greener practices		
2	The switch should support solutions that monitors and conserves energy with customized policies		
3	The switch should support reduction of greenhouse gas (GhG) emissions		
4	The switch should support an increase in energy cost savings		

5	The switch should support sustainable business behavior		
6	The switch should support Efficient switch operation		
7	The switch should support Intelligent power management		
8	The switch should support measuring of energy between itself and endpoints		
9	The switch should support control of energy between itself and endpoints		
10	The switch should support discovery of manageable devices for Energy measurement		
11	The switch should support monitoring of power consumption of endpoints		
12	The switch should support taking of action based on business rules to reduce power consumption		
O	**Network security features**		
1	The switch should support IEEE 802.1x to allow dynamic, port-based security, providing user authentication.		
2	The switch should support Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.		
3	The switch should support SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.		
4	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.		
5	The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.		
6	The switch should support Port security to secure the access to an access or trunk port based on MAC address.		
7	The switch should support Multilevel security on console access to prevent unauthorized users from altering the switch configuration.		
8	The switch should support Private VLAN		
P	**DHCP Features**		
1	The switch should support DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addressesDHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.		
2	The switch should support DHCP Interface Tracker (Option 82) feature to augment a host IP address request with the switch port ID.		
3	The switch should support DHCP Option 82 data Insertion		
4	The switch should support DHCP Option 82 Pass Through		
5	The switch should support DHCP Option 82 - Configurable Remote ID and Circuit ID		

6	The switch should support DHCP Snooping Statistics and SYSLOG		
Q	**IPv6 Features**		
1	The switch should be on the approved list of IPv6 Ready Logo phase II - Host		
2	The switch should support IPv6 unicast Static Routing		
3	The switch should support 16 IPv6 Static routes		
4	The switch should support IPv6 MLDv1 & v2 Snooping		
5	The switch should support IPv6 Host support for IPv6 Addressing		
6	The switch should support IPv6 Host support for IPv6 Option processing		
7	The switch should support IPv6 Host support for IPv6 Fragmentation		
8	The switch should support IPv6 Host support for IPv6 ICMPv6		
9	The switch should support IPv6 Host support for IPv6 TCP/UDP over IPv6		
10	The switch should support IPv6 Host support for IPv6 Ping		
11	The switch should support IPv6 Host support for IPv6 Traceroute		
12	The switch should support IPv6 Host support for IPv6 VTY		
13	The switch should support IPv6 Host support for IPv6 SSH		
14	The switch should support IPv6 Host support for IPv6 TFTP,		
15	The switch should support IPv6 Host support for IPv6 SNMP for IPv6 objects		
16	The switch should support IPv6 Port Access Control Lists		
17	The switch should support IPv6 Router Access Control Lists		
18	The switch should support HTTP, HTTP(s) over IPv6		
19	The switch should support SNMP over IPv6		
20	The switch should support SysLog over IPv6		
21	The switch should support IPv6 Stateless Auto Config		
22	The switch should support DHCP based Auto Config (Auto Install) and Image download		
23	The switch should support IPv6 QoS		
24	The switch should support RFC4292/RFC4293 MIBs for IPv6 traffic		
25	The switch should support SCP/SSH over IPv6		
26	The switch should support Radius over IPv6		
27	The switch should support TACACS+ over IPv6		
28	The switch should support NTPv4 over IPv6		
29	The switch should support IPv6 First-Hop Security		
30	The switch should support IPv6 First Hop Security: RA Guard		
31	The switch should support IPv6 First Hop Security: DHCPv6 Guard		

32	The switch should support IPv6 First Hop Security: IPv6 Binding Integrity Guard		

TECHNICAL ENVELOPE

List of Technical Documents:

Sr. No.	**Description**	**Bidders Response (Yes/No)**	**Remarks**
1.	ISO 9001 and ISO 27001 Certified Copies		
2.	Registration proof of incorporation in companies act		
3.	Copy of PAN Card		
4.	Copy of latest Income Tax Return (last Three years) i.e. 2013-14, 2014-15, 2015-16		
5.	Prime Customers Details as per Page no 26, Point no 19		
6.	Online Receipts of Payment		
7.	Declaration of validity of rates as per Page 19, Point no 8.		
8.	OEM Authorization Letter/ MAF's		
9.	Product Brochures/technical Compliances Sheet as per Annexure A(Only Color Print out may be submitted)		
10.	Certificate of not Debarred/blacklisted as page no 21 point no 22		
11.	Proof of Turnover for last 3 years		

NOTE:

All the Technical Documents should be uploaded on the e-tender portal. The non-submission/poor management of documents may lead to disqualification as well.

FINANCIAL ENVELOPE

Sr.No	Name of Item	Qty	Product Model No / Remarks(If Any)	Unit Rate with 1 Year Warranty without tax	Unit Rate with 1 Year Warranty with tax	**Total Rate** (Qty X Unit Rate with 1 Year Warranty with tax)	Unit Rate for (2nd+3rd) Year Warranty without tax	Unit Rate for (2nd+3rd) Year Warranty with tax	Unit Rate for (4th+5th) Year Warranty and without tax	Unit Rate for (4th+5th) Year Warranty and with tax
1	Wi-Fi Controller& AAA Server	1								
2	Outdoor Access Points	50								
3	Indoor Access Point	200								
4	Outdoor point-to-point wireless connection:With External Antenna	2								
5	24 Port PoE Edge 1G Switch	20								

All the Financial Documents should be uploaded on the e-tender portal. The non-submission/poor management of documents may lead to disqualification as well.