CENTRAL UNIVERSITY OF KASHMIR
Transit Campus Sonwar Srinagar 190004

TENDER NOTICE
FOR THE SUPPLY, INSTALLATION & COMMISSIONING OF LOCAL AREA NETWORKING

Quotations under two-bid-system are invited from suppliers/firms for supply and installation of LAN and other allied items at different campuses of the University. The last date for receiving sealed tender documents by post/hand is **05th December, 2014 latest by 4 p.m** to be opened **at 3 p.m** on 09th December, 2014. Interested parties can obtain the tender document from the office of the University at Sonwar, Srinagar, J&K on payment of non-refundable amount of Rs. 1000/- through DD of any nationalized bank drawn in favour of Central University of Kashmir payable at Srinagar or can download from the University website **www.cukashmir.ac.in**.

Sd/-
Registrar

Date: 14.11.2014 0194-2468354.2468357
Cukmr/Pur/F.No.413/14/ 34

Cost of the tender Document:
Rs. 1000/-
(Rupees One Thousand only)

CENTRAL UNIVERSITY OF KASHMIR

Transit Campus: Sonwar, Near GB Pant Hospital, Srinagar – 190 004 (J&K)
Phone: 0194-2468354, 2468357, Website www.cukashmir.ac.in

Tender No.: CUKmr/Estt-IT/F.No.221/13/

Dated: 14.11.2014

1. Name of the Firm/Supplier/Vendor: ……...…..……...…..……
……..……..

2. Address with telephone No. :…… …… …… ……..…… …… …
……

3. Earnest Money Deposit (EMD)

(to be deposited along with the tender document)

a) Bank Draft No……...….

b) Date…….……

c) for Rs…….…….

d) Drawn on ……...

4. Cost of Tender Document:

(to be deposited in case of downloaded tender document)

a) Bank Draft No……...….

b) Date……

c) for Rs……..

d) Drawn on ……

Central University of Kashmir

TENDER NOTICE
FOR THE SUPPLY, INSTALLATION & COMMISSIONING OF LOCAL AREA NETWORKING

LAST DATE & TIME FOR SUBMISSION OF TENDER ***05th December, 2014 by 4 p.m.***

DATE, TIME & VENUE FOR OPENING OF BIDS: ***09th of December 2014(3 p.m.)***
At COMMITTEE ROOM, CENTRAL UNIVERSITY OF KASHMIR, SONWAR, SRINAGAR – 190 004 (J&K)

General Terms & Conditions

Sealed tenders under two-bid-system are invited from reputed manufactures or their authorized suppliers having proper after sale service set up at Srinagar (J&K) for THE SUPPLY, INSTALLATION & COMMISSIONING OF LOCAL AREA NETWORKING as per specification given in the financial bid. Tender Document can be had from the Transit Campus of the University on payment of Rs 1000/- or can be downloaded from the University website: www.cukashmir.ac.in. The downloaded form should be accompanied by a DD of Rs 1000/- as cost of Tender Document. Part 1 of the bid (Technical Bid) comprises of bidders profile in the prescribed format, EMD, application fee with regard to the eligibility of the bidder as set out in this NIT. Part 2 comprises of financial Bid in the prescribed format. Both parts should be sealed separately and submitted in a single covering envelope superscripted "THE SUPPLY, INSTALLATION & COMMISSIONING OF LOCAL AREA NETWORKING" on or before 05.12.2014 (04:00 pm). The bids will be opened on 09.12.2014 at 03:00 pm at the Transit Campus Sonwar. Bidders or their authorized representatives who wish to attend tender opening, may do so.

SCOPE OF WORK

As a part of IT infrastructure build up, **Central University of Kashmir** desires to set up Campus wide LAN & WiFi Networking, IP Surveillance & IP Telephony infrastructure along with related IT services using state of the art networking equipment, Access points, Controller, IP Camera, IP Telephony, AAA, NMS Overall Solution, UTP cabling system at multiple Campus of **Central University of Kashmir, Srinagar.**

The following summarizes the scope of work.

1. To Implement LAN Networking in **Central University of Kashmir** Campus.
2. To Supply, install and commission Wireless Controller, Switches, IP Camera, IP Phones with NVR & Analytics, AAA, NMS, AP's and all active components as per specifications.
3. To supply, install and commission Intra building UTP CAT6 structured cabling / Point to Multi Point RF Network for as per BOQ across the multiple campuses.
4. Detailed Solution in Annexure's to be implemented.

SALE OF TENDER DOCUMENT

1. The interested bidders may obtain the tender document from the University office at Transit Campus, Sonwar, Near GB Pant Hospital, Srinagar, J&K on all working days against the payment of non-refundable amount of Rs. 1000/- through DD of any nationalized bank drawn in favour of Central University of Kashmir payable at Srinagar (J&K). The tender document can also be downloaded from the University Website: www.cukashmir.ac.in. The cost of tender document (Rs. 1000) is to be attached with the Technical Bid in the form of a DD along with the downloaded form. This DD should be submitted separately and not merged with the EMD.

EMD

1. The Technical Bid should be accompanied with EMD of Rs. 3,00,000/- in shape of Demand Draft drawn on any nationalized bank favoring Central University of Kashmir payable at Srinagar (CDRs will not be

accepted). The EMD of the unsuccessful bidders will be returned after the selection of the successful bidder and that of the successful bidder after the submission of Performance Security to the extent of 10% of Purchase order value. The offers without EMD shall be summarily rejected.

2. All the DD's of the nationalized banks are to be drawn in favour of Central University of Kashmir payable at Srinagar (J&K) issued after the date of tender notification.

ELIGIBLE BIDDERS

1. The bidder/OEM must have supplied LAN Active & Passive components for Rs. 2 Crore Single Order or Rs. 1 Crore Two Orders or Rs.50 lakhs 4 orders of similar specifications as mentioned in this NIT in last three years. Bidder/OEM is required to submit E-Mail ID(s) & Phone Numbers of the Purchase Order issuing authorities for verification by CUK.
2. Bidder must have service presence in Srinagar either direct or indirect through partner and in case of service requirement; the downtime will be 4 hours. An undertaking to this effect must be enclosed in the technical bid.
3. Bidders must be either Original Equipment Manufacturer (OEM) or authorized dealer of the OEM. Traders are not eligible to participate in the tender. The authorization letter, in case of the authorized dealer, issued by each manufacturer (OEM) should be attached along with the tender.
4. The bidder/OEM should have Turnover of at least 5 Crores each year for last three financial years.
5. The bid must include latest ITR Certificate.
6. ISO certification is mandatory for all bidders.
7. The bidder must submit site survey report duly signed by the concerned authority from the University.
8. OEM should be a Profit making Entity for at least last 3 years/12 Quarters.
9. OEM should be listed in latest Gartner's Leader's quadrant for both Unified Communications as well as Corporate Telephony
10. OEM should be listed in latest Gartner's Leaders quadrant for both Wired and Wireless LAN Access Infrastructure.

(Note: Failure to meet above requirements shall disqualify the bidder from participation in bidding. Claim of bidder on account of above must be substantiated by suitable documentary evidence).

SUBMISSION OF BIDS

1. The bids should be addressed to the REGISTRAR, Central University of Kashmir, Sonwar, Srinagar – 190004 (J&K) within the dates and time as specified above by hand or by post. PLEASE NOTE THAT THE UNIVERSITY IS NOT RESPONSIBLE FOR ANY POSTAL LOSSES/DELAYS. IN CASE OF BIDS SENT BY POST AND BEING RECEIVED AFTER 4.00 p.m. ON 05th December, 2014 THE UNIVERSITY SHALL REJECT THE SAME AND IN CASE OF ANY DISPUTE IN THE TIMING OF RECEIPT, THE DECISION OF THE UNIVERSITY SHALL BE FINAL.
2. The Bidder is expected to examine all instructions, terms & condition as specified in the bidding documents. Failure to furnish all information required by the bidding documents or submission of a bid not substantially responsive to the bidding documents in every respect will be at the Bidder's risk and may result in rejection of the bid.
3. At any time prior to the deadline for submission of bids, the University may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder/s, modify the bidding documents by amendment.
4. **Late Bids:** Any bid received by the University after the deadline for submission of bids prescribed by the University, will be rejected/returned unopened to the Bidder.
5. Quotations received after due date, improperly sealed, or with incomplete marking or with overwriting/corrections in the quotation document are liable to be rejected.
6. No bid will be allowed to be modified subsequent to the deadline for submission of bids.
7. No bid will be allowed to be withdrawn in the interval between the deadline for submission of bids and the expiration of the period of bid validity specified by the Bidder on the bid form. Withdrawal of a bid during this interval may result in the Bidder's forfeiture of his bid security.
8. The bid will be opened on 09th December, 2014 at 03:00 pm in presence of bidders or their authorized representatives. The representative should bring the authorization letter from their vendor for attending the tender opening. However, the presence of the bidders or their representatives is not mandatory.

9. In the event of the date specified for bid receipt and opening being declared as a closed holiday for University's office, the due date for submission of bids and opening of bids will be the following working day at the time fixed above.

EVALUATION OF BIDS (Two Bid System)

1. The evaluation of bids shall be a two stage process. In Stage–1, Technical bid (Part-I) shall be opened and only those bidders shall qualify for stage–2 of bidding, whose technical bid meets the requirements set by the University as eligibility mentioned in the foregoing clauses and the specifications in this NIT as per *Annexure-I*. Financial Bid of only those bidders shall be opened whose Technical Bid is declared accepted by the University.
2. In stage–2, Financial Bids (Part-2) of the qualified bidders as per *Annexure-II* shall be opened and on the basis of the comparative statement, the contract shall be awarded to the L1.
3. The University's evaluation of a financial bid will be based on the landing cost at the site taking in to account all the taxes, duties, transportation and assembling charges etc.
4. No Bidder shall contact the University on any matter relating to its bid, from the time of the bid opening to the time the Contract is awarded. If the bidder wishes to bring additional information to the notice of the University, it should do so in writing.
5. Any effort by a Bidder to influence the University, in its decisions on bid evaluation, bid comparison or contract award may result in rejection of bid.
6. Failure of the successful bidder to comply with the requirements of the University shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event the University may make the award to the next lowest evaluated bidder or call for new bids.
10. Bids that are not opened and read out at bid opening shall not be considered further for evaluation, irrespective of the circumstances.
11. During evaluation of bids, the University may, at its discretion, ask the Bidder for a clarification of its bid. The request for clarification and the response shall be in writing and no change in prices or substance of the bid shall be sought, offered or permitted.
12. Period of Validity of Bids: Bids shall remain valid for a minimum 90 days after the date of bid opening prescribed by the University. A bid valid for a shorter period shall be rejected by the University as non-responsive.
13. In exceptional circumstances, the University may solicit the Bidder's consent to an extension of the period of validity. The request and the responses there to, shall be made in writing. The bid security provided shall also be suitably extended. A Bidder may refuse the request without forfeiting his bid security. A Bidder granting the request will not be required nor permitted to modify its bid.
14. The successful Tenderer shall have to deposit (**10%**) of total payable-amount as Security Deposit in the form of DD in favour of Central University of Kashmir as Performance Security for warranty period of two years. The performance security shall be returned to the supplier after 60 days beyond the date of completion of all contractual obligations of the supplier including the warranty obligations of two years. In case of unsatisfactory service provided by the bidder, the Performance Security shall be forfeited.
15. The bid security (EMD) may be forfeited:
    (a) If a Bidder withdraws its bid during the period of bid validity;
    (b) If at any stage it is proven that the information given by the bidder is incorrect;
    (c) In case of a successful Bidder, if the Bidder fails:
        (i) to sign the Contract
        (ii) to furnish Performance Security
        (iii) to execute the supply within stipulated time.
16. Bidders must also quote charges for extended warranty of 03 years (beyond mandatory warranty of 02 years) in the technical bid. However, University reserves its rights not to utilize the services under this head.
17. Documents such as operation manuals, user manuals and network diagrams and other relevant materials shall be provided by the Tenderer along with equipment, free of cost.
18. The bidder should confirm that there are no hidden costs. Any items found necessary to make structure functional will be provided by the bidder without extra cost.

Payment Terms and Conditions

1. Prices shall be quoted in Indian Rupees only.
2. The amount to be quoted both in figures and in words, in case of a discrepancy the amount quoted in words will be taken as final.
3. The supply, transportation, installation & commissioning etc, of all equipment/s will be on the risk of the firm till the acceptance by the University.
4. The site of installation shall be in and around the Srinagar city. However, the exact location shall be communicated to the selected bidder at the time of placing the Purchase Order/s.
5. The quoted rates should be final and should include taxes, levies, freight, insurance, forwarding, installation, transportation etc. and shall be **FOR Central University of Kashmir** Any extra amount over and above the quoted rates will not be entertained.
6. The supply and installation of equipments and other accessories should be made strictly in accordance with the specifications given in the Technical Bid. The warrantee period takes effect from the date of satisfactory installation. The Tenderer shall be liable to make good the loss (free of cost) by replacing/repairing the equipment or other accessories found defective during the minimum warranty period of two years.
7. **Payment terms:** All the payment will be made in Indian rupees. Payment (50%) shall be made by the University after successful delivery of material subject to inspection of the material by a Committee specially constituted for the same and its subsequent acceptance by the University, further (30%) payment shall be released after successful installation & testing of the item/s and Balance 20% of Payment will be released after furnishing of performance security equal to 10% of total payable amount as DD or Bank Guarantee favoring Central University of Kashmir. The performance security shall be returned to the supplier after 60 days beyond the date of completion of all contractual obligations of the supplier including the warranty obligations of two years. However, in case of unsatisfactory service during the warranty period, the Performance Security will be forfeited. The decision of declaring the service unsatisfactory will be the discretion of the University and shall prevail on all other judgments made thereto.
8. The amount payable to the supplier against supplies shall be subject to the TDS/GST etc, as may be applicable, if any.
9. The actual quantity to be purchased can be increased or decreased by the Competent Authority of the University at the time of the placement of purchase orders in favour of successful bidder. The purchase orders in favour of successful bidders may also be issued in a phase wise manner depending upon the requirement of the University.
10. Submission of bid under this NIT shall mean that the bidder has accepted all the terms and conditions laid down in the tender document.
11. The University may at any time, by written order given to the supplier, make changes within general scope of the Contract in any one or more of the following:
    (a) Drawings, designs, or specifications, where Goods to be furnished under the Contract are to be specifically manufactured for the University;
    (b) The method of shipping or packing;
    (c) The place of delivery; and/or
    (d) The Services to be provided by the Supplier
12. The supply of LAN Active & Passive components has to be made within a period of 45 days from the date of the issue of Purchase Order by the University. In case firm fails to supply within the stipulated time, the University may impose the penalty as decided by the University Committee.
13. All the supplies made under this tender notice will be inspected by a Committee specially constituted for the purpose and in case the Committee is of the opinion that the supplies are not of the required specifications, the supplies shall be rejected and responsibility of lifting back the supplies will devolve upon the supplier. Besides, in such event the EMD shall stand forfeited and the extra cost incurred in arranging the supply from the alternative sources shall also be recovered from the defaulting supplier apart from initiating the proceedings for blacklisting.
14. Item offered in the tender can be re-ordered at the same rate, under same terms & conditions within a period of twelve months from the tender opening date.

15. All the items supplied through this tender shall be covered by a comprehensive warranty of Two years. During the period of warranty, no charges will be paid by the University on any kind of service or repairment carried by the supplier. **However, for some instruments/equipments, the warranty has been mentioned against each. In such cases, warranty mentioned against the instruments/equipments shall be applicable.**
16. The selected firm will be required to enter into an Agreement with the University by submitting an Instrument of Agreement on non-judicial stamp paper/s of Rs. 100/. Necessary clauses mentioned in this NIT shall be incorporated in the said agreement. In addition an undertaking to comply with all rules, regulations, Laws and Byelaws enforced by Local and `Central Govt. and Central University of Kashmir in whose premises the work has to be done must be incorporated in the said agreement.
17. The University reserves the right to accept/reject a part/whole or all tenders without assigning any reason or cancel or withdraw the tender notice.
18. Once the bidder submits the tender, it would be presumed that the bidder has understood and accepted all the terms and conditions given in NIT. No inquiry, verbal or written, shall be entertained in respect of acceptance/rejection of the tender.
19. The University reserves the right to relax any condition enumerated or arising out of this Tender notice, without assigning any reason/s thereof.
20. The University reserves the right to place the order for limited number of items or to out-rightly cancel the tender without assigning any reason/s thereof.
21. If the supply, installation and commissioning of the systems are not effected before the specified period from the date of purchase order, the University shall have the authority to cancel the order or to take any such action which will be deemed fit in the circumstances.

STANDARD TERMS AND CONDITIONS OF TENDER

1. The Tender should be neatly typed. The rates should be quoted in words and figures without any over writing/ erasure. Any over writing/ erasure will render the Tender of the particular item invalid. The tenderer should attest all corrections by affixing his signatures and each page of the tender should be signed by the tenderer.
2. The rates quoted should be per unit and should include charges for packing and delivery and should be as per Financial Bid format mentioned on **Annexure-II**. However, the Sales tax, wherever applicable should be shown separately at the prevailing rate. If it is decided to ask for excise duty or any other levy as extra, the same must be specifically stated. In the absence of such a stipulation, it will be presumed that the prices include all such charges and no claim for the same will be entertained. This University is not liable to pay any other charges over the above the rates quoted.
3. In case of any manufacturing defects in the equipment, it should be replaced immediately.
4. Local suppliers must possess a counter guarantee of service in case of imported equipments from Parent Company (OEM).
5. Successful Tenderer will have the responsibility for arranging training to the designated employees of the University for Smooth handling and proper functioning of supplied equipments through specified number of training sessions.
6. The University shall not be responsible if the consignment incurs any demurrage.
7. The University reserves the right to make any changes in the Technical Specification, Bill of Quantity of this Tender.
8. Bidders are not allowed to sub-contract in any manner and Consortium Bids are not acceptable. However, if Bidder and OEM wish to appoint local partner for the sake of providing services and support or the Facility Management Services to the University specific to this tender only, the University may evaluate the local presence of partner and shall agree to have their services either directly or indirectly through the Bidder.
9. The issue of this Tender document does not imply that the University is bound to select a Bidder and Central University of Kashmir reserves the right to reject all or any of the Bidders without assigning any reason whatsoever.
10. The University reserves the right to cancel this Tender anytime without assigning any reason thereof.
11. The Bidder should abide by the terms and conditions specified in the Tender document. Conditional offers are not acceptable.
12. At any time before the deadline for submission of Tender, The University may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the Tender Document by amending, modifying and / or supplementing the same. All changes shall be posted on website www.cukashmir.ac.in and prospective Bidders are required to go through the same before submission of

Tender. All such amendments shall be binding on them without any further act or deed on the University part. In the event of any amendment, The University reserves the right to extend the deadline for the submission of the Tender, in order to allow prospective Bidders reasonable time in which to take the amendment into account while preparing their Tender.

13. The compatibility of all the networking components is the essence of this tender for efficient working of the network, hence bidders shall essentially quote all active components of one make only and also passive components of one make only. **Any deviations in this matter will subject to disqualification.**
14. All information in the Tender/Bid shall be in English. Information in any other language should be accompanied by its translation in English. Failure to comply with this may disqualify the Bidder.
15. Validity of the quoted offer should cover the period of the completion of project. Offers without such validity shall be rejected.
16. The vendor must give a point-by-point compliance to the Technical Specifications of the quoted products as per **Annexure I** of the Tender/Bid Documents and enclose with the technical bid.
17. Each page of the Tender/Bid document should be signed & stamped by the Bidder as a token of acceptance to terms and conditions mentioned.
18. Bidders should quote for all accessories which are either part of an item or are necessary for proper functioning of that item. Thus, for accessories of individual items **the University** shall not pay anything separately and if the functioning of any item is not proper or does not function at all, The University shall have the full right to deduct complete payment of that item(s).
19. After assigning of the contract by the University, it shall be the responsibility of the contractor to make an inventory of all the materials upon its arrival at the customer's location and notify the customer of any missing components.
20. The contractor shall be responsible for safe custody of the items handed over to him by the University any loss or wastage shall have to be made good by the contractor at their own cost.
21. If the contractor commits any violation of the above terms, the University shall claim such damages as it may deem fit and the decision of the University in this regard shall be final and binding.
22. All Passive Cabling work whether it is UTP, Patch Panels, and Racks Patch Cords etc. should be done neatly and with proper tagging. It must be very professional and aesthetic. Entire cabling should be structured.
23. All work shall be done in a thorough and conscientious manner according to EIA/TIA guidelines and industry standards, and shall be subject to inspection and acceptance.
24. The contractor shall be certain that all the installation work areas are secure and made safe in accordance with Health and Safety regulations.
25. All legal disputes, arising if any, would be settled under jurisdiction of J & K (Srinagar) court.

SPECIAL CONDITIONS OF THE TENDER/BID

1. The bidder must clearly mention the **make, model & enclose relevant datasheet/brochures along with requisite certificates of the products** as per the Technical specifications as mentioned in Annexure.
2. In the event of the goods not being in accordance with the specification or the conditions of the contract or failure by the bidder to perform services as outlined in the Tender/Bid document, **The University** reserves the right to cancel the contract at any stage.
3. A detailed Project plan is to be provided by bidder for material delivery and execution. Material delivery has to be done in 4 to 6 weeks from the release of PO and complete installation has to be done in 14 weeks from the date of release of PO.
4. **Bidder has to quote all the active components of switching, WiFi and telephony of the same make or as per Tender Specifications. Similarly, bidder has to quote all the passive components of the same make or as per Tender Specifications.**

DELIVERY SCHEDULE

5. The delivery and installation of all the ordered items shall be completed within 12 to 14 weeks from the date of placement of order by the University. In case firm fails to supply within the stipulated time, the University may impose 0.5% of the cost of the pending supply for every week as penalty and the amount so collected will be deducted from the bill to the maximum of 10% beyond which the order will remain cancelled and Bid Security/Earnest Money deposited will be forfeited. Besides, the extra cost incurred in arranging the supply from the alternative sources shall also be recovered from the defaulting supplier. However, if the University authorities are convinced that the delay was because of any unavoidable condition they can consider such delays in supplies/installation/completion of project for condonation.

WARRANTY / GUARANTEE

6. The system supplied or installed shall be guaranteed by the contractor for a minimum period of **Two Years** with regards to quality of material, workmanship, performance, efficiency, installation, etc. Defects developed in the system within guarantee period, shall be rectified by the contractor at his own expense promptly.

VARIATIONS IN QUANTITY

7. The quantity mentioned in the Tender/Bid is only indicative one. The University reserves the right to increase/ decrease/ remove any/all quantities while placing the order. Switches, Cables/Jack Panels, Connectors, Racks, PVC channel, Fiber patch cords, Cat 6 patch cords, UTP Cable Box's, all passive components will be on actual basis.
8. During the Site Survey, the successful Bidder may suggest additional equipment which **the University** may have left by oversight or which the Contractor considers essential in Project Implementation, The same may be submitted with the BOM after site Inspection. However the total cost of such equipment may not exceed **25 %** of the complete passive Tender/Bid value, and the price justification for the same shall be submitted by the Bidder, if the item is not a part of the Tender/Bid documents.
9. Any work not covered under this contract, but which is essentially required for the completion of job (to the satisfaction of the University) shall be carried out by the Contractor as extra item with prior approval of the University for which payment shall be made separately at the rates decided by the University**.**
10. In case of any dispute, the same shall be resolved initially by mutual discussion between the parties with in a period of 60 days failing which appropriate courts at Srinagar will have the jurisdiction to adjudicate upon the matter.

Sd/-

REGISTRAR

Central University of Kashmir

No.: CUKmr/Estt-IT/F.No.221/13

Date: 14.11.2014

BIDDER'S PROFILE

(PART –I)

Passport size Photograph of the Tenderer/authorized signatory holding power of attorney

1. Name of the bidder ……..……

2. Name of the authorized signatory (whose photograph is affixed)
Mr/Ms/Mrs……

3. Permanent address of the firm/Supplier……

……..……

Tel. No. (with STD Code) (O) ……..… (Fax) …..…….

(R) …….. (Mobile) ……..

4. Registration & incorporation particulars of the firm.

4.1 Proprietorship

4.2 Partnership

4.3 Private Limited

4.4 Public Limited

(Please attach attested copies of documents of registration/incorporation of your firm with the competent authority as required by business law).

5. Name proprietor/partners/directors ……..…….

……

6. Bidders bank, its address and his current account number
……..…….

……

7. Permanent Account Number, Income Tax Circle……..…….…..

8. TIN……

I/We hereby declare that the information furnished above is true and correct. At any stage if the above information is found incorrect, University may cancel my/our empanelment.

Name and sign of the authorized person
of the firm along with seal

Place:

Date:

Annexure-I (Technical)

CHECK LIST

To ensure that your offer submitted to Central University of Kashmir is complete in all respects, please go through the following checklist & tick mark for the enclosures attached with your offer:

SR. NO.	DESCRIPTION	ATTACHED	NOT ATTACHED
1	Details of Technical Staff as on FORM I		
2	General Information about Bidder as in FORM II		
3	Passive Work Specification as on FORM III		
4	UTM / Firewall Specification and Compliance as on FORM IV		
5	Point to Multi Point Access Point Specifications as on FORM V		
6	Point to Multi Point Subscriber Module Specifications as on FORM VI		
7	Indoor AP 802.11ac Specifications as on FORM VII		
8	Outdoor AP Compliance as on FORM VIII		
9	AAA with Guest Life Cycle as on FORM IX		
10	NMS - Converged Management Infrastructure as on FORM X		
11	Core Switch Specifications as on FORM XI		
12	Wireless LAN Controller as on FORM XII		
13	Access Switches as on FORM XIII		
14	IP Indoor / Outdoor Camera Specifications as on FORM XIV		
15	Voice Gateway Specifications as on form XV		
16	IP EPABX Specifications as on FORM XVI		
17	IP Video Phone Specifications as on Form XVII		
18	IP Phone Specifications as on XVIII		
19	TECHNICAL SPECIFICATIONS FOR INTEGRATED RACK as on XIX		
20	TECHNICAL SPECIFICATIONS FOR COMMUNICATION TOWER as on FORM XX		
21	Professional Video Management Software as on FORM XXI		
22	Overall Solution as on FORM XXII		
23	Overall Location Wise BOQ as on form XXIII		

Annexure-I

FORM I

Details of Technical staff available with the company for execution of work

(Information to be attached with the Offer)

Sr. No.	Name	Qualification	Additional Certification, if any	Total Experience, no. of years	Remarks
1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23.					

- If necessary, separate sheet may be used to submit the information.

Annexure-I

FORM II

General information about the bidder

1.	**Name Of The Bidder**	
2	**Postal Address**	
3	**Telephone/Fax no**	
4	**E-mail address & URL**	
5	**Type of Company** Attach Proof of Company Registration along with a copy of the Partnership Deed/ Article of Association and Memorandum of Understanding	
6	**Name and designation of the representative** of the Bidder to whom all references shall be made to expedite technical co-ordination.	
7	**Amount and reference of the EMD**	
8	**Financial capacity of the company/ firm.** (Attach copies of I.T. Returns and Balance Sheets for last 3 years)	
9	**Name and address of the Indian/Foreign collaborator(s) if any**.	
11	**PAN/TAN Number** (A copy should be enclosed)	

Annexure-I

FORM III

Passive Work Specification

REFERENCE STANDARDS

The following ANSI/TIA/EIA Standards.

1) This Technical Specification and Associated Drawings
2) ANSI/TIA/EIA/568-C.1, Commercial Building Telecommunications Cabling Standard – 2009
3) ANSI/TIA/EIA 568-C.3, Optical Fiber Cabling Components Standard
4) ANSI/TIA/EIA-569-B, Commercial Building Standard for Telecommunications Pathways and Spaces
5) ANSI/TIA/EIA-606-A, Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
6) ANSI/J-STD-607-A, Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications
7) Building Industries Consulting Services International (BICSI) Telecommunications Distribution Methods Manual (TDMM)
8) ANSI/TIA-942, Telecommunications Infrastructure Standard for Data Centers

The Contractor is responsible to determine and adhere to the most recent edition of these standards when developing their responses in accordance with non-commercial building meant for education

- **OEM should have direct presence in India more than at-least 10 years (Supporting documents required)**
- **OEM should have stood at no. 1 position at least once in structured cabling market from last 10 years.(Please provide supporting documents)**
- **OEM should have members participating in International Standard Bodies like EIA/TIA, ISO/IEC**
- **OEM should be a member of Telecommunications Industry Association (TIA) Information and**
- **Communications Technology (ICT)**
- **All material should be from one OEM make only**

Technical Specification for UTP Cabling System

Sr No.	Details	Specification	Compliance (Yes/No)	Deviation
1	**Type**	Unshielded twisted pair cabling system, Certificate by Intertek (ETL) for the 4-Connectors channel testing to the Cat 6 Cabling system as per the ANSI/TIA 568 C.2 & as well as the ISO 11801 standards up to 550 MHz or more		
2	**Networks Supported**	10 / 100/1000 Ethernet, 155 Mbps ATM, 1000 Mbps IEEE 802.3ab Ethernet, and proposed Cat 6 Gigabit Ethernet		
3	**TIA / EIA 568 C.2**	ETL Verified / UL Listed		
4	**Warranty**	25 year systems warranty; Warranty to cover Bandwidth of the specified and installed cabling system, and the installation costs		
5	**Performance characteristics to be provided along with bid**	(a) Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR for 4-connector channel		
		(b) Should perform to CAT6 with short channel		
		(c) 4-Connectors channel testing to the Cat 6 Cabling system as per the ANSI/TIA 568 C.2 & as well as the ISO 11801 standards up to 500 MHz or more		
		(d) CAT6 cabling system should be tested and verified by the Independent third party laboratories for Zero BER (Bit Error Rate) testing at the data transmission speed of 1 Gbit/s.		

UTP CABLE, Cat 6

Sr No.	Details	Specification	Compliance (Yes/No)	Deviation
1	**Type**	Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2 & ISO/IEC 11801		
2	**Conductors**	23 AWG solid bare copper		
3	**Insulation**	Polyethylene		
4	**Jacket**	Flame Retardant PVC		
	Pair Separator	Cross-member **(+)** fluted Spine/isolator for uniform separation for all pairs.		
5	**Approvals**	(a) UL Listed / UL Verified		
		(b) ETL verified to TIA / EIA Cat 6		
6	**Operating temperature**	-20 Deg. C to +60 Deg. C		
7	**Frequency tested up to**	600 MHz		
8	**Packing**	Box of 305 meters		
9	**Bend Radius**	4 * Cable Diameter		
10	**UL/NEC Ratings**	NEC 800 CMR Rated or IEC 60332-1 and UL 1666		
11	**Performance characteristics to be provided along with bid**	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR		
12	**ROHS Compliance**	ROHS Complaint		

Cat 6, UTP JACKS

Sr No.	Details	Specification	Compliance (Yes/No)	Deviation
1	**Type**	PCB based, Unshielded Twisted Pair, Category 6, TIA /EIA 568-C.2 and ISO/IEC 11801		
2	**Modular Jack**	750 mating cycles		
3	**Wire terminal**	200 termination cycles		
4	**Accessories**	Integrated bend-limiting strain-relief unit for cable entry or other mechanism to reduce the strain and bends at cable entry		
		Integrated hinged dust cover		
		Support cable pair termination process on the jacks at 45, 90 or 180 degree angle.		
		Bidder should have a mechanism to maintain the quality of the termination ir-respective of the skill level of the termination staff.		
5	**Housing**	Polyphenylene oxide, 94V-0 rated.		
6	**110 Blocks**	polycarbonate, 94V-0 rated		
7	**Jack contacts**	Beryllium copper, plated with 1.27 mm [.000050] thick gold in localized area and 3.81 mm [.000150] minimum thick tin-lead in solder area over 1.27 mm [.000050] minimum thick nickel under plate		
8	**Wiring blocks**	Polycarbonate, 94V-0 rated		
9	**Approvals**	(a) UL Listed / CSA Approved		
		(b) ETL verified to TIA / EIA Cat 6		
10	**Performance Characteristics to be provided with bid**	Attenuation, NEXT, PS NEXT, FEXT and Return Loss		
11	**ROHS Compliance**	ROHS compliant		

UTP Jack Unloaded Panels, Cat 6

Sr No.	Details	Specification	Compliance (Yes/No)	Deviation
1	**Type**	24port, 1U, Unloaded Modular, PCB based, Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2 and ISO/IEC 11801		
2	**Ports**	24/48		
3	**Port arrangement**	Configured as 6 Port Module with individually replaceable CAT-6 Jacks		
4	**Circuit Identification**	Front of each module shall be capable of accepting labels		
5	**Port Identification**	Labels on each of 48-ports (to be included in supply		
6	**Modular Jack**	750 mating cycles		
7	**Wire terminal**	200 termination cycles		
8	**Accessories**	Integrated bend-limiting strain-relief unit for cable entry or other mechanism to reduce the strain and bends at cable entry		
9	**Material Housing**	Polyphenylene oxide, 94V-0 rated		
	Wiring blocks	Polycarbonate, 94V-0 rated		
	Jack contacts	Beryllium copper, plated with 1.27 mm [.000050] thick gold in localized area and 3.81 mm [.000150] minimum thick tin-lead in solder area over 1.27 mm [.000050] minimum thick nickel under plate		
	Panel	Black, powder coated steel		
10	**Approvals**	UL listed / ETL Verified		
11	**Termination Pattern**	TIA / EIA 568 A and B;		
12	**ROHS Compliant**	ROHS/ELV Compliant		

WORKSTATION / EQUIPMENT PATCH CORDS

Sr No.	Details	Specification	Compliance (Yes/No)	Deviation
1	**Type**	Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2 & ISO/IEC 11801		
2	**Conductor**	24 AWG 7 / 32, stranded copper conductors 100 Ohm		
3	**Length**	4 feet, 7 feet, 10 feet		
4	**Plug Protection**	Transparent/clear/anti snag Slim boot		
5	**Warranty**	25-year component		
6	**Jacket**	CM Rated		
7	**ROHS Compliance**	ROHS/ELV Complaint		

FACEPLATE

Sr No.	Details	Specification	Compliance (Yes/No)	Deviation
1	**Type**	**Single Gang, US style, 2.5 x 4 inches**		
2	**Material**	ABS / UL94 V-0		
3	**No. of ports**	Two/Four/Six		
4	**Holder, Jack**	ABS UL 94V-0		
5	**Cover Label**	Acrylic UL94V-0		
6	**ROHS Compliance**	ROHS/ELV Complaint		

Warranty

Central University of Kashmir seeks warranty for the installed cable plant from the OEM equipment supplier. Bidder shall ensure that the OEM norms for supply, installation, testing and documentation as specified by the OEM supplier shall be adhered to, provided those are in line with TIA / EIA standards and Owner requirement specifications. The warranty shall be provided by the OEM vendor to Central University of Kashmir and shall be administered in India. The duration of the warranty shall be for a minimum of 25 years on structured cabling.

Annexure-I

FORM IV

UTM / Firewall Specification and Compliance

S.No.	Specifications	Compliance (Yes/No)	Deviation
1	**Appliance Throughput**		
1.1	Firewall throughput of 30Gbps.		
1.2	Minimum 5Gbps of Antivirus Throughput		
1.3	Minimum 7,500,000 Concurrent sessions		
1.4	Minimum 12Gbps of IPS throughput		
1.5	Minimum 3.5Gbps firewall throughput with IPS, Content Filtering and Anti-Virus features enabled.		
1.6	Minimum 250,000 New Sessions/second		
1.7	Minimum 4.5Gbps of IPsec VPN throughput and 1Gbps of SSL VPN throughput		
1.8	Minimum of 4000 IPsec Site to Site tunnel support and 1000 SSL VPN user support. License for the same should be included in the BOM.		
1.9	10x 10/100/1000 interfaces supporting Hardware Bypass expandable to 16.		
1.10	Minimum of 6x1GE SFP ports with a support to upgrade to 4 x10GE SFP in same box if required in future.		
2	**General Features**		
2.1	Should be appliance based and rack mountable		
2.2	Should have redundant power supply. Added box to be quoted separately in HA in case of lack of Redundant Power Supply.		
2.3	Identity based Firewall		
2.4	Intrusion Prevention System		
2.5	Gateway Anti-virus		
2.6	Inbound and Outbound Gateway Anti-spam		
2.7	Web Content & Application Filtering		
2.8	Web Application Firewall		
2.9	Bandwidth Management		
2.10	Inbuilt-on Appliance Reporting		
2.11	Network: OSPF, Round Robin load balance, RIPv2, BGP, equal & unequal cost load balance, High Availability, QoS, etc. Round Robin Balance, Server Load Balancing.		
2.12	Support for user authentication over SMS.		
2.13	Country Based Blocking, FQDN support and should support MIX mode deployment		
2.14	4 Eye Authentication feature for data integrity.		
3	**Gateway Antivirus, Anti-Spyware and Anti-Spam**		

3.1	Checkmark Certified. Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area.		
4	**Web and Application Filtering:**		
4.1	Checkmark Certified.URL, Keyword, File type block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL, block P2P application, anonymous proxies, Customized block on group basis. Minimum of 82 categories with more than 42 million URLS supported. 2000+ application support categorized into Characteristics, Technology, Category and Risk Level.		
5	**Security Features**		
5.1	Intrusion Prevention System (IPS): Checkmark Certified. For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (3000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection		
6	**Web Application Firewall (WAF):**		
6.1	Should provide minimum of 1.3 Gbps of WAF throughput.		
6.2	Should have on appliance WAF with Positive Protection Module, Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Extensive Logging and reporting. If external, then has to be quoted separately.		
7	**VPN:**		
7.1	IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal, should be VPNC Certified.		
8	**Load Balance:**		
8.1	For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Support for Active-Active / Active-Passive Deployment. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.		
9	**Bandwidth Management:**		
9.1	Application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Group, Firewall Rule, URL and Applications.		
10	**Monitoring and Reporting System:**		
10.1	External hardware reporting solution supporting at least 1000 events per second with minimum of 8 HDD configured in RAID 5		
10.2	Minimum of 4GBE ports, 1 Console and a USB interface		

10.3	Should provide more than 1200 drilled down reports, Compliance Reports - HIPPA, SOX, FISMA, GLBA, PCI, User and Group based Reports - Web, Email, IM, FTP, Application, Internet Usage Reports - Data Transfer, Surfing Time, Security Reports - Firewall, Attacks, Spam, Virus, Blocked Attempts, Remote Access Reports - VPN, SSL VPN, Search Engine Reports - Google, Yahoo, Bing, Wikipedia, Rediff, eBay, Trend & Search Reports, Multi-format reports - tabular, graphical, Exportable formats - PDF, Excel, Email Alerts/automated Report Scheduling		
10.4	Supported Network and Security Devices- Custom/Proprietary devices including UTMs- Proxy Firewalls, Access Gateway, Smart Wireless Router, Web Server, Endpoint Security Solution, Syslog-compatible devices		
11	**License for UTM (Unified Threat Management)**		
11.1	Five Years round the clock support for Gate Way Antivirus, spyware, Anti-Spam, WAF, content and application filtering. IPS, reporting and Monitoring hardware, support and Upgrades.		
11.2	License period will be counted after activation.		
12	**Support and Warranty**		
12.1	Standard warranty and Support should be mentioned (Minimum Warranty and Support should be three years). There should be minimum Service Assurance and Subscription for three years from the date of Installation and commissioning.		
12.2	Should have ISO 20000:2011 Certified support.		
12.3	Appliance should have EAL4+ Certification and ICSA certification for Firewall.		

Annexure-I

FORM V

Point to Multi Point Access Point Specifications

SPECTRUM	SPECIFICATIONS	Compliance (Yes / No)
General Features	System should be able to deliver more than 110 mbps throughput across 20 Mhz channel	
	To ensure flexibility in design it should be possible to have multiple radios on the center location. The operation of radio should ensure that co-location of the same radio is possible on a single mast of up to 4 radios with simultaneous throughput of 500 Mbps (aggregate) or better with 20 Mhz channel width	
	All System should be able to operate in LOS ,nLOS and NLOS environment to ensure complete flexibility in choosing deployment locations.	
	System should support at least 512 subcarrier to support Non Line of Sight	
	System must support on board synchronization GPS to avoid interference	
	System must provide two level of Synchronization auto redundancy to ensure smooth operation of system	
	System should have inbuilt surge protection mechanism of minimum 1 Joule	
CHANNEL SPACING	Should be configurable on 2.5 MHz increments, selectable to 50 KHz.	
FREQUENCY RANGE	ISM Bands	
CHANNEL WIDTH	5 MHz, 10 MHz or 20 MHz	
INTERFACE		
MAC (MEDIA ACCESS CONTROL) LAYER	System should have Scheduled access to avoid the collision rather than CSMA technology	
PHYSICAL LAYER	2x2 MIMO OFDM, System must have the support for 2 X 2 MIMO-B technology to increase throughput	
ETHERNET INTERFACE	10/100/BaseT, half/full duplex, rate auto negotiated (802.3 compliant)	
PROTOCOLS USED	1IPv4, UDP, TCP, IP, ICMP, Telnet, SNMP, HTTP, FTP	
NETWORK MANAGEMENT	HTTP, Telnet, FTP, SNMP v2c	
VLAN	802.1ad (DVLAN Q-inQ), 802.1Q with 802.1p priority, dynamic port VID	
PERFORMANCE	Should support upto 150 subscriber per sector	
	System must support minimum 238 virtual circuit for remote module usage	
	System should support Auto Transmit power control for CPE to avoid unnecessary interference	
	Spectral efficiency should be at least 6.25 bps/hz for access.	
	Device should be capable of being configured for uplink/ downlink split data ratio in any percentage combination.	
ARQ	YES	
MODULATION LEVELS (ADAPTIVE)	**SIGNAL TO NOISE REQUIRED (SNR, in dB)**	
1X	10	

2X	10	
4X	17	
6X	24	
8X	32	
RECEIVE SENSITIVITY (PER CHAIN, IN dB)	**2.4GHz / 5 GHz**	
	8X	
@ 5MHZ CHANNEL	-66 / -64	
@ 10MHZ CHANNEL	-66 / -62	
@ 20MHZ CHANNEL	-66 / -60	
MAXIMUM DEPLOYMENT RANGE	UP TO 40 MILES	
LATENCY	3 - 5 ms, TYPICAL	
GPS SYNCHRONIZATION	YES, VIA AUTOSYNC (CMM3, CMM4, uGPS, iGPS)	
QUALITY OF SERVICE	DIFFSERVE QoS	
LINK BUDGET		
ANTENNA BEAM WIDTH	5 GHz - 60° OR 90° SECTORS (DUAL POLARITY, H + V)	
	2.4 GHz - 60° SECTOR (DUAL SLANT)	
ANTENNA GAIN	9 dBi H+V, INTEGRATED PATCH (5 GHz)	
	8 dBi DUAL SLANT, INTEGRATED PATCH (2.4 GHz)	
TRANSMIT POWER RANGE	-30 TO +22 dBm (COMBINED, TO EIRP LIMIT BY REGION) (1 dB INTERVAL)	
MAXIMUM TRANSMIT POWER	22 dBm COMBINED	
PHYSICAL		
ANTENNA CONNECTION	50 ohm, N-TYPE	
SURGE SUPPRESSION	IEC 61000-4-2 (ESD) 15kV (AIR), 8kV (contact)	
	IEC 61000-4-4 (EFT) 40A (5/50ns)	
	IEC 61000-4-5 (LIGHTNING) 100A (8/20mS)	
MEAN TIME BETWEEN FAILURE	> 40 YEARS	
ENVIRONMENTAL	IP67, IP66	
TEMPERATURE	-40°C TO +55°C (-40°F TO +131°F), 0-95% NON-CONDESNSING	
WIND SURVIVAL	190 km/hour (118 mi/hour)	
SECURITY	Should support encryption 56-bit DES, FIPS-197 128-bit AES	
CERTIFICATIONS	Should be FCC ID & CE Certified	

Annexure-I

FORM VI

Point to Multi Point Subscriber Module Specifications

SPECTRUM	SPECIFICATIONS	Compliance (Yes / No)
General Features	System must be software 20 mbps throughput.It must be software upgradable to 50 mbps	
	All System should be able to operate in LOS ,nLOS and NLOS environment to ensure complete flexibility in choosing deployment locations.	
	System should support at least 512 subcarrier to support Non Line of Sight	
	All the SM should be able to support auto firmware upgrade from AP	
CHANNEL SPACING	Should be configurable on 2.5 MHz increments, selectable to 50 KHz.	
FREQUENCY RANGE	ISM Bands.	
CHANNEL WIDTH	5 MHz, 10 MHz or 20 MHz	
INTERFACE		
MAC (MEDIA ACCESS CONTROL) LAYER	System must have the support for 2 X 2 MIMO-B technology to increase throughput	
	System design approach should be taken to carry small Radio data packet to ensure negligible impact of interference on performance	
PHYSICAL LAYER	2x2 MIMO OFDM	
ETHERNET INTERFACE	10/100/BaseT, half/full duplex, rate auto negotiated (802.3 compliant)	
PROTOCOLS USED	1IPv4, UDP, TCP, IP, ICMP, Telnet, SNMP, HTTP, FTP	
NETWORK MANAGEMENT	HTTP, Telnet, FTP, SNMP v2c	
VLAN	802.1ad (DVLAN Q-inQ), 802.1Q with 802.1p priority, dynamic port VID	
PERFORMANCE	Should support ARQ	
	System should support Auto Transmit power control for CPE to avoid unnecessary interference	
	System should have the support of carrier to noise ratio as low as 7 dB	
MODULATION LEVELS (ADAPTIVE)	**SIGNAL TO NOISE REQUIRED (SNR, in dB)**	
1X	10	
2X	10	
4X	17	
6X	24	
8X	32	
RECEIVE SENSITIVITY (PER CHAIN, IN dB)	**2.4GHz / 5 GHz**	
	8X	
@ 5MHZ CHANNEL	-68 / -69	

@ 10MHZ CHANNEL	-65 / -64	
@ 20MHZ CHANNEL	-66 / -62	
MAXIMUM DEPLOYMENT RANGE	UP TO 40 MILES	
LATENCY	3 - 5 ms, TYPICAL	
GPS SYNCHRONIZATION	YES, VIA AUTOSYNC (CMM3, CMM4, uGPS, iGPS)	
QUALITY OF SERVICE	DIFFSERVE QoS	
LINK BUDGET		
ANTENNA BEAM WIDTH	55° AZIMUTH, 55° ELEVATION (BOTH POLARIZATIONS)	
ANTENNA GAIN	9 dBi H+V, INTEGRATED PATCH (5 GHz)	
	8 dBi DUAL SLANT, INTEGRATED PATCH (2.4 GHz)	
TRANSMIT POWER RANGE	-30 TO +22 dBm (COMBINED, TO EIRP LIMIT BY REGION) (1 dB INTERVAL).	
MAXIMUM TRANSMIT POWER	22 dBm COMBINED OFDM	
REFLECTOR GAIN	+14 dBi FOR 5 GHz, +12 dBi FOR 2.4 GHz	
CLIP GAIN	+8 dBi	
PHYSICAL		
ANTENNA CONNECTION	INTEGRATED PATCH ANTENNA, CONNECTORIZED VERSIONS AVAILABLE	
SURGE SUPPRESSION	IEC 61000-4-2 (ESD) 15kV (AIR), 8kV (contact)	
	IEC 61000-4-4 (EFT) 40A (5/50ns)	
	IEC 61000-4-5 (LIGHTNING) 100A (8/20mS)	
MEAN TIME BETWEEN FAILURE	> 40 YEARS	
ENVIRONMENTAL	IP55	
TEMPERATURE	-40°C TO +55°C (-40°F TO +131°F), 0-95% NON-CONDESNSING	
WIND SURVIVAL	190 km/hour (118 mi/hour)	
INPUT VOLTAGE	20 TO 32 V	
SECURITY	Should support encryption 56-bit DES, FIPS-197 128-bit AES	
CERTIFICATIONS	Should be FCC ID & CE Certified	

Annexure-I

FORM VII

Indoor AP 802.11ac Specifications

Feature	Specifications	Compliance (Yes/No)	Deviation
Hardware:	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave 1.		

	Must have a robust design for durability, without visible vents		
	Mounting kit should be standard from OEM directly.		
	Must have atleast 512 MB DRAM and 64 MB flash		
	Must have atleast 4 dBi gain on both radios		
802.11ac	Must support 3x4 multiple-input multiple-output (MIMO) with three spatial streams		
	Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios.		
	Must support 802.11ac Wave 1 on the integrated 5-GHz radio		
	Must support datarates upto 450Mbps and 1.3 Gbps on 802.11ac.		
	Must support upto 23dbm of transmit power in both 2.4Ghz and 5Ghz radios.		
RF	The Wireless AP should have the technology to improve downlink performance to all mobile devices including one-, two-, and three spatial stream devices on 802.11n and 802.11ac. The technology should work without requiring feedback from clients and should work with all existing 802.11 clients.		
	Should support detecting and classifying non-Wi-Fi wireless transmissions while simultaneously serving network traffic		
	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.		
	Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.		
	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		
	Should support spectrum analysis and security scanning using a dedicated hardware separate from the radio serving the clients with 80MHz channel support		
	Should be able to detect atleast 20 sources of non 802.11 interference within 30 seconds		
	Must have -100 dB or better Receiver Sensitivity.		
Roaming	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.		
Security	Must support Management Frame Protection.		
	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
	Must operate as a sensor for wireless IPS		
	Should support non-Wi-Fi detection for off-channel rogues and Containment for both radio		
Encryption	Access Points must support a distributed encryption/decryption model.		
	Access Points must support Hardware-based DTLS encryption on CAPWAP Standard		
Monitoring	Must support the ability to serve clients and monitor the RF environment concurrently.		
	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		
Flexibility:	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services.		
	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling		
	Mesh support should support QoS for voice over wireless.		
	Must be plenum-rated (UL2043).		
	Must support 16 WLANs per AP for SSID deployment flexibility.		
	Must continue serving clients when WAN link to controller is back up again, should not reboot before joining		
	Must support Controller-based and standalone(autonomous)		

	deployments		
	Should support Local authentication at the AP level in case of WAN outage		
Operational:	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.		
Power:	Must support Power over Ethernet, local power(DC Power), and power injectors.		
	Must operate at 3x3 or higher with 802.3af PoE is the source of power		
Quality of Service:	802.11e and WMM		
	Must support Reliable Multicast Video to maintain video quality		
	Must support QoS and Video Call Admission Control capabilities.		
	Access Point should 802.11 DFS certified		

Annexure-I

FORM VIII

Outdoor AP Compliance

Outdoor AP with 802.11n or ac			
Features	**Specifications**	**Compliance (Yes\No)**	**Deviation**
Hardware	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.		
	It should be an outdoor rugged Hardware AP, and not the indoor AP with casing.		
	Must include dual band antennas to support both the 2.4GHz and 5GHz operations simultaneously from single antenna.		
	Option to attach Single band, Dual band antennas directly on Access Point		
	Access Points must be configurable via software to support dual-band OR single-band antennas.		
	Access Points must support signal rejection for 3G/LTE/WiMAX in co-Located environment.		
802.11n/802.11 ac	Must support 2X2 multiple-input multiple-output (MIMO) with two spatial streams in case of 802.11n. Must support 3X3:3 or 4X4:3 or 3X4:4 multiple-input multiple-output (MIMO) with three/four spatial streams in case of 802.11ac respectively .		
	Must support simultaneous 802.11 n or 802.11 ac on both the 2.4 GHz and 5 GHz radios.		
	Must support data rates up to 300Mbps on 802.11 n and if incase 802.11 ac then higher data rates.		
	Must support 40 MHz wide channels in 5 GHz in case of 802.11n. Must Support 40 and 80 Mhz incase of 802.11 ac		
	Must support up to 27dbm of transmit power in both 2.4 GHz and 5 GHz radios.		
	Should support controller based and autonomous operations.		
	Must support 802.11 dynamic frequency selection (DFS)		
MESH & RF Specifications	Access Point should support Wireless Backhaul, point-to-point, point-to-multipoint bridging		
	Support Encrypted and authenticated connectivity between all backhaul components		
	Mesh Nodes shall provide a 'wired' interface for connection to local area networks or backhaul of local clients.		
	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		
Environment and Electrical Specifications	Access point shall support powering from AC Adapter, DC and POE (802.3at+).		
	Access point shall support pole, wall, and roof mounting options.		
	Geographic orientation flexibility - tilt angle for pole, wall, and roof mounting units		
	The Access point shall be IP67 rated for dust and water ingress		
	The Access point shall wind gusts up to 165 mph		
	The Access point shall be rated for operation over an ambient temperature range of -30° to 65°C (-22° to 149°F)		

Annexure-I

FORM IX

AAA with Guest Life Cycle

Specifications	Compliance (Yes/No)	Deviation
The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA) and guest management services on a single platform.		
It should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise		
Provides complete guest lifecycle management by empowering sponsors to on-board guests		
Solution should be scalable enough to support 250,000 endpoints in the network when it is required.		
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		
Solution should support comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint		
Solution should support Addresses vulnerabilities on user machines through periodic evaluation and remediation to help proactively mitigate network threats such as viruses, worms, and spyware		
Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention		
Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations		
Allows you to get finer granularity while identifying devices on your network with Active Endpoint Scanning		
Augments network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of what is on your network		
Manages 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		
Utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA).		
Supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS).		
Offers a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols, profiling identity, or other external attribute sources. Attributes can also be created dynamically and saved for later use		
Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.		
Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets.		
It should allow 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.		

The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.		
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.		
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.		
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.		
Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.		
Enables 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.		
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.		
Should be available as a physical or virtual appliance.		
Should support consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed		
Employs advanced enforcement capabilities including security group access (SGA) through the use of security group tags (SGTs) and security group access control lists (SGACLs)		
Solution should have capability to determine whether users are accessing the network on an authorized, policy-compliant device.		
Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.		
Solution should have capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).		
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.		
Solution should support Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance		
Solution should have capability which allows users to add a device on a portal (My Devices Portal), where the device goes through a registration process for network access. Should allow users to mark as lost any device that you have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device. Should have capability to reinstate a blacklisted device to its previous status in the My Devices Portal, and regain network access without having to register the device again in the My Devices Portal. Should also support removing any device in the enterprise network temporarily, then register the device for network access again later.		
The portal used for Device registration (MY device Portal) should be customizable, allowing to customize portal theme by changing text, banners, background colour, and images		

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 details •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		
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)		
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		
Solution should support automatic provisioning of NAC agents		
Solution should support periodic reassessment for clients that are already successfully postured for compliance.		
Solution should support the following endpoint checks for compliance for windows endpoints:		
Check operating system/service packs/hotfixes		
Check process, registry, file & application		
check for Antivirus installation/Version/ Antivirus Definition Date		
check for Antispyware installation/Version/ Antispyware Definition Date		
Check for windows update running & configuration		
Solution should support following remediation options for windows endpoints:		
File remediation to allow clients download the required file version for compliance		
link remediation to allow clients to click a URL to access a remediation page or resource		
Antivirus remediation to update clients with up-to-date file definitions for compliance after remediation.		
Antispyware remediation to update clients with up-to-date file definitions for compliance after remediation.		
launch program remediation for NAC Agent to remediate clients by launching one or more applications for compliance.		
Windows update remediation to ensure Automatic Updates configuration is turned on Windows clients per security policy		
Solution should integrate with the following MDM vendors		
Airwatch, Inc.		
Good Technology		
MobileIron, Inc.		
Zenprise, Inc.		
SAP Afaria		
Fiberlink MaaS		
Solution should support configuring MDM policy based on the following attributes		
Device Register Status, Device Compliant Status, Disk Encryption Status, Pin Lock Status, Jail Broken Status, Serial Number, Manufacturer, IMEI, OsVersion & phone number		
Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database.		

Should support native supplicant profiles to enable users to bring their own devices into the network. When the user logs in, based on the profile that you associate with that user's authorization requirements, solution should provide the necessary supplicant provisioning wizard needed to set up the user's personal device to access the network. This should be supported over Microsoft windows, Apple Mac and iOS and Android devices.		
Should support an endpoint identity group which is used to group all the identified endpoints on your network according to their profiles. Solution should create the following four identity groups in the system: Registered Devices, Blacklist, Profiled, and Unknown.		
When endpoints are discovered on the network, they can be profiled dynamically based on the configured endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.		
Should support using a simple filter that you can use to filter endpoints. The quick filter filters endpoints based on field descriptions, such as the endpoint profile, MAC address, and the static status that is assigned to endpoints when they are created in the Endpoints page.		
Should support an advanced filter that you can preset for use later and retrieve, along with the filtering results, The advanced filter filters endpoints based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.		
Should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma.		
Support for importing endpoints from LDAP server. Should allow to import MAC addresses and the associated profiles of endpoints securely from an LDAP server. Should support an LDAP server to import endpoints and the associated profiles, by using either the default port 389, or securely over SSL, by using the default port 636.		
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		
Should support Role-based access policies which are access control policies which allow you to restrict the network access privileges for any user or group. Role-based access policies are defined when you configure specific access control policies and permissions. These admin access policies allow you to customize the amount and type of access on a per-user or per-group basis using specified role-based access permission settings that apply to a group or an individual user.		
Should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases: •Internal Users •Internal Endpoints •Active Directory •LDAP •RSA •RADIUS Token Servers •Certificate Authentication Profiles		

Should Support the following Authentication Protocols •Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) and Protected Extensible Authentication Protocol (PEAP)—support for user and machine authentication and change password against Active Directory using EAP-FAST and PEAP with an inner method of Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) and Extensible Authentication Protocol-Generic Token Card (EAP-GTC). •Password Authentication Protocol (PAP)—support for authenticating against Active Directory using PAP and also allows you to change Active Directory user passwords. •Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)—support for user and machine authentication against Active Directory using MS-CHAPv1. •MS-CHAPv2—support for user and machine authentication against Active Directory using EAP-MSCHAPv2. •EAP-GTC—support for user and machine authentication against Active Directory using EAP-GTC. •Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)—Should use the certificate retrieval option to support user and machine authentication against Active Directory using EAP-TLS. •Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)—support for user and machine authentication against Active Directory using PEAP-TLS. •LEAP—support for user authentication against Active Directory using LEAP.		
Must be able to differentiate policy based on device type + authentication		
Should have Ability to authenticate at least one phone and multiple users on the same switch port without interrupting service		
Solution should support 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		
Solution must support Non 802.1x technology on assigned ports and 802.1x technology on open use ports		
Solution must allow users access to the network in a worst case scenario in case of AAA server outages or any other reasons like WAN failure.		
Should support authenticating Machines and users connected to the same port on the switch in a single authentication flow		
Should support authenticating IP phones and users connected behind IP phones on the same physical port.		
Solution support the profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors: * Profiling using MAC OUIs * Profiling using DHCP information * Profiling using RADIUS information * Profiling using HTTP information * Profiling using DNS information * Profiling using NetFlow information * Profiling using SPAN/Mirrored traffic		
Should be able to classify endpoints based on information like DHCP, CDP, and LLDP attributes using IOS sensor capabilities enabled on switches		
Should support Microsoft Windows 2012 Active Directory.		
Solution should support troubleshooting authentication issues by triggering session reauthentication to follow up with an attempt to reauthenticate again.		
Should support session termination with port shutdown option to block an infected host that sends a lot of traffic over the network.		

Annexure-I

FORM X

NMS - Converged Management Infrastructure

Specifications	Compliance (Yes/No)	Deviation
The network management platform shall provide a single integrated solution for comprehensive lifecycle management of the wired/wireless access, campus, and branch networks, and rich visibility into end-user connectivity and application performance assurance issues.		
The platform shall support as many as fifteen thousand devices through virtual or physical appliances.		
The platform shall deliver application-level visibility through the normalization and correlation of rich performance instrumentation data to help ensure application delivery and an optimal end-user experience.		
The management utility shall help enable regulatory compliance analysis and reporting against PCI DSS standards.		
The platform shall accelerate the rollout of new services and provides secure access and management of mobile devices.		
The management utility shall have deep integration with the secure access mechanism like 802.1x authentication, posture and profiling to provide visibility across security and policy-related problems, presenting a complete view of client access issues with a clear path to solving them.		
The utility shall simplify and automate many of the day-to-day tasks associated with maintaining and managing the end-to-end network infrastructure from a single pane of glass thereby reducing the need for multiple tools, and lowering operating expenses and training costs.		
The platform would deliver all of the existing wireless capabilities for RF management, user access visibility, reporting, and troubleshooting along with wired lifecycle functions such as discovery, inventory, configuration and image management, automated deployment, compliance reporting, integrated best practices, and reporting.		
The platform shall be based on lifecycle processes that would align with the product functionality clearly describing the phases like design, deploy, operate, report and administer.		
The design functionality shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the-box implementation automating the work required to use OEM validated designs and best practices.		
The management infrastructure shall provide continuous compliance and auditing capabilities to help IT organizations monitor and assess their network and device configuration for out-of-policy configuration, discrepancies, and security and risk vulnerabilities.		
The platform shall offer unified alarm displays with detailed forensics provide actionable information and the ability to automatically open service requests with the OEM's Technical Assistance Center		
The platform should have flexible virtual machine and physical appliance solution that would provide cost-effective, easy-to-install options for small to global enterprise-class networks.		
The management utility shall have Role-based access control provides flexibility to segment the network into one or more virtual domains controlled by a single Infrastructure platform. These Virtual domains shall help deploy both large, multisite networks and managed services.		
The management platform shall support the following device types like integrated services routers, aggregation services routers, access switches, distribution switches, Ethernet Core switches, server farm switches, network analysis modules, wide area applications service modules, Fiber channel & Storage switches, Wireless access points, Mobility Services Engine and Wireless LAN Controllers.		

Annexure-I

FORM XI

Core Switch Specifications

Core Switch Specification	Compliance (Yes/No)	Deviation
Switch should have 48 1/10G ports SFP+ & should support 12 number 40G QSFP ports		
Should support Openflow & should be SDN ready		
Hot-swappable, redundant power supplies and fan trays increase availability.		
Support for both front-to-back and back-to-front airflow configurations.		
Support native 40 Gigabit Ethernet QSFP+ transceiver on existing OM3 MMF with LC connectors (without any breakout cables of 4x10G)		
Layer 2 Features		
4096 VLANs		
960 GBPS backplane		
Should support 95,000 MAC addresses		
Spanning Tree Protocol		
IEEE 802.1w Rapid Spanning Tree (Rapid PVST+)		
IEEE 802.1s Multiple Spanning Tree (MST)		
VLAN Trunk Protocol (VTP) Versions 1 and 2 (v1 and v2): Transparent mode		
MAC addresses: Static		
Unicast and multicast		
IEEE 802.3x Flow Control		
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
User-configurable interface maximum transmission unit (MTU) and jumbo frames		
Automatic medium-dependent-interface crossover (auto-MDIX)		
Unidirectional Link Detection (UDLD)		
Should support Layer 3 Features :		
IPv4		
Static routes		
BGP, EIGRP, OSPFv2, and Intermediate System to Intermediate System (ISIS)		
VRF-Lite and VRF route leaking		
HSRPv1 and v2		
Virtual Router Redundancy Protocol (VRRP)		
Bidirectional Forwarding Detection (BFD)		
Dynamic Host Configuration Protocol (DHCP) relay		
IPv6		
Static routes		
BGP and OSPFv3		
VRF-Lite and VRF route leaking		
HSRPv6		
VRRPv3		
DHCP relay		
Multicast Features		
IGMPv1, v2, and v3		
IGMP snooping		
Protocol-Independent Multicast (PIM) sparse mode (PIM-SM) and Any Source Multicast (ASM)		

Multicast Source Discovery Protocol (MSDP)		
Availability Features support		
Stateless process restart		
Comprehensive Monitoring Features		
Minimum, complete, bypass, on-demand, and health checks		
Onboard fault logging (OBFL)		
Embedded Event Manager (EEM): Scheduler, monitor, and event manager		
Integrated packet capture and analysis with Wireshark		
Default SSD for logging and data capture		
SPAN		
Source and destination on switch		
ERSPAN		
Ingress ACL filtering		
Security Features		
Ingress and egress ACLs using Layer 2, 3, and 4 fields		
Extended ACLs, MAC addresses, port ACL (PACL), VLAN ACL (VACL), and routed ACL (RACL)		
Flexible ACL carving		
ACL counters		
Storm control		
Broadcast, multicast, and unknown unicast		
User-configurable Control-Plane Policing (CoPP)		
Authentication, authorization, and accounting (AAA)		
Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Microsoft MS-CHAP, and MS-CHAPv2		
Capability to disable role-based access control (RBAC) and use AAA server authentication		
RBAC integration to replace privilege levels		
Logging		
Test parameters		
VRF context support		
LDAP support		
RADIUS		
RBAC		
TACACS+		
Interface Types		
Layer 2 switch port		
Access and trunk (VLAN list and native VLAN tagged and untagged)		
Layer 3 routed		
Loopback interface		
Switched virtual interface (SVI)		
Port Channel		
Static mode		
IEEE 802.3ad LACP		
QoS Features		
Up to 4 queues per port		
Modular QoS command-line interface (CLI; MQC)		
ACL-based classification		

Queuing		
Marking and classification		
Differentiated services code point (DSCP) on switch		
Class of service (CoS)		
Policing		
Ingress		
Explicit congestion notification (ECN)		
Weighted Random Early Detection (WRED)		
Priority flow control (PFC) with support for up to 3 PFC classes		
Device Management Features		
Power on auto provisioning		
Configuration rollback		
FTP, SFTP, and TFTP client		
Network Time Protocol (NTP)		
Remote monitor (RMON)		
Simple Network Management Protocol (SNMP) v1, v2, and v3		
Syslog		
Virtual terminal (vty)		
XML (Netconf)		
Secure Shell (SSH) v2 (client and server)		
Telnet (client and server)		
USB port		
100/1000-Gbps management port		
RS-232 serial console port		
Supported in plug-in for OpenStack		
Standards Compliance		
IEEE 802.1D Bridging and Spanning Tree		
IEEE 802.1p QoS/CoS		
IEEE 802.1Q VLAN Tagging		
IEEE 802.1w Rapid Spanning Tree		
IEEE 802.1s Multiple Spanning Tree Protocol		
IEEE 802.1AB Link Layer Discovery Protocol		
IEEE 802.3ad Link Aggregation with LACP		
IEEE 802.3x Flow Control		
IEEE 802.3ab 1000BASE-T		
IEEE 802.3z Gigabit Ethernet		
IEEE 802.3ae 10 Gigabit Ethernet		
IEEE 802.3ba 40 Gigabit Ethernet		
RFC 2460 IPv6		
RFC 2461 Neighbor Discovery for IPv6		
RFC 2462 IPv6 Stateless Address Auto configuration		
RFC 2463 ICMPv6		

Annexure-I

FORM XII

Wireless LAN Controller

WLAN Controller should be based on the following key requirements:		Compliance (Yes/No)	Deviation
Hardware and Standards	1. Must be compliant with IEEE CAPWAP for controller-based WLANs.		
	2. WLAN Controller should support upto 1000 Access Points in a single 1 RU chassis.		
	3. WLAN controller must have atleast 2 x 1 G and 2 x 10Gbps of uplink interfaces.		
	4. WLAN Controller must support atleast 4K VLANs		
	5. Should support a mechanism to detect connectivity issues with both fiber and copper cabling. Ensures that a partially failed link is shut down on both sides, to avoid L2/L3 protocol convergence issues		
Compatibility	6. Must not require a separate controller for Wireless Intrusion Prevention Access Points.		
High Availability	7. Must support both 1+1 and N+1 redundancy models. The controllers will be implemented in HA mode. When the primary controller fails and secondary controller comes up, the clients connected at point in time and all applications running on the clients should not disconnect. Controllers must work in Active-Active mode.		
	8. Must have feature for stateful failover of Access Points		
	9. Must support redundant power supplies and redundant Fan		
RF Management	10. Must support an ability to dynamically adjust channel and power settings based on the RF environment.		
	11. Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference		
	12. The controller should be capable of dynamic Channel allocation to AP. The controller should have the capability to monitor interference created by different Hospital/Other RF equipments and respond by allocating least or non-interfering channel to the AP's automatically. No manual intervention should be required.		
	13. The controller should support 802.11ac with all its versions, 802.11 a/b/g/n with all versions.		
	14. Must have Automatic 802.11 interference detection, identification, classification, and mitigation. Classification should support a dynamically updatable signature library		
	15. Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.		
IPv6 features	16. WLC Should support configuring interface with IPv6 address		
	17. WLC should support L2 and L3 roaming of IPv6 clients		
	18. WLC should support First hop security features in IPv6 network like Router Advertisement guard, DHCPv6 guard.		
	19. WLC should support IPv6 Access List in hardware to provide line-rate performance		
Performance	20. Controller performance must remain the same if encryption is		

	on or off for wireless SSIDs.		
	21. Max throughput without DTLS should be 50 Gbps		
	22. AP per Radio resource management group should support 2000 numbers.		
	23. No of Rouge client detection should be more than 4500 at any given point of time.		
	24. Minimum clients supported per controller should be more than 12000.		
	25. Controller should support battery conservation on mobile devices.		
	26.		
	27. Should support ability to adjust Delivery Traffic Indicator Message (DTIM) to improve performance for latency sensitive applications.		
Security	28. Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS),RFC 4347		
	29. Should support Management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure.		
	30. The Controller should support a capability to shun / block WLAN client in collaboration with wired IPS on detecting malicious client traffic.		
	31. Controller should have rogue AP detection, classification and automatic containment feature		
	32. Should support VLAN-based, Port-based and Time-based ACLs		
	33. Should support Storm control features to prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces		
	34. Should support secure mechanism with MD5 for automatic configurations of VLANS or equivalent protocol to reduce administrative burden of configuring VLANs on multiple switches in turn eliminating the configuration errors & troubleshooting in secure manner		
	35. Controller should support all known wireless attacks.		
	36. Should offer 100% visibility into infrastructure attack with Hybrid AP's.		
	37. The controller or external overlay solution should be capable of wireless intrusion detection & prevention .The WLAN should be able to detect Rogue AP and take corrective action to prevent the rogue AP. The system should detect and prevent an organization's wireless client connecting to rogue AP and also prevent an outside client trying to connect to organizational WLAN.		
	38. The controller and overlay solution should detect & prevent an Ad-hoc connection (i.e. clients forming a network amongst themselves without an AP) as well as windows bridge (client that is associated to AP is also connected to wired network and enabled bridging between two interfaces)		

	39. Controller should have device profiling capabilities based on protocols like http, dhcp and more to identify the devices on the network.		
	40. Should be able to detect all known attacks.		
	41. Should support Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination		
Guest Wireless	42. Must support internal web authentication.		
	43. Must support a method of authentication for users based on Certificate, radius, tacacs. There should be a captive portal		
Functionality	44. Must support rate limiting per user		
	45. Must support user load balancing across Access Points.		
	46. Controller must provide Mesh capability for Mesh supported AP.		
	47. Must be SDN(Software Defined Networking) ready to make access networks more flexible for business.		
Monitoring	48. Must be able to dedicate some APs to monitor-only for Intrusion Prevention Services.		
	49. Must support functionality like wireshark to capture and analyse traffic for wireless network		
QOS:	50. Must support 802.11e WMM		
	51. Should have Voice and Video Call Admission and Stream prioritization for preferential QOS		
	52. Controller should have Deep Packet Inspection for Layer 4-7 traffic for user for all traffic across the network to analyses information about applications usage		
	53. To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.		
	54. controller should support Voice and Video streaming and Video Conferencing without any delay over Wireless Network.		
Spectrum Analysis	55. In addition to serving clients, controller should perform spectrum analysis to detect and classify sources of interferences. System should provide fast Fourier transform displays and spectrograms for real-time troubleshooting and visualization. Bidder can quote add on component to achieve this functionality.		
	56. Controller should detection and classification of non 802.11 based interferences and should perform spectrum analysis and serve client using same radio. If there is any License required for it, then the cost of same should be incorporated in solution.		
	57. System should provide details on Wi-Fi and NON-Wi-Fi active interfering devices and channels affected by those devices.		
Mobility	58. Controller should support an architecture where we can split Mobility agent and Mobility Controller between Switch and Controller.		
	59. Controller should support reliable fast roaming standards 802.11k and 802.11r		
	60. Controller should support efficient roaming decisions with AP assisted hand-offs		
	61. Controller should support seamless roaming for clients.		

Annexure-I

FORM XIII

Access Switches

Feature	Specifications	Compliance (Yes/No)	Deviation
General Features	The switch should support a minimum of 24 nos. 10/100/1000 Ethernet Ports		
	The switch should support a minimum of 4 SFP Uplinks		
	The switch should support 4x1G SFP modules		
	The switch should support a total of 28 Ports		
Performance and Scalability	The switch should support Forwarding bandwidth of 108 Gbps		
	The switch should support Full-duplex Switching bandwidth of 216 Gbps		
	The switch should support 64-Byte Packet Forwarding Rate of 71.4 Mpps		
	The switch should support 128 MB of Flash memory		
	The switch should support 512 MB of DRAM		
	The switch should support 1023 VLANs		
	The switch should support 4096 VLAN IDs		
	The switch should support Jumbo frames of 9216 bytes		
	The switch should support Maximum transmission unit (MTU) of 9198 bytes		
	The switch should support 16000 Unicast MAC addresses		
Dimension	The Switch should be 1RU		
	The switch should support Operating temperature up to 5000 ft (1500 m) -5º to 45ºC		
	The switch should support Operating relative humidity 10% to 95% noncondensing		
Stacking	The switch should support Stacking		
	Stacking should enable all switches to function as a single unit		
	The switch should support an optional Stacking Port		
	Stacking module should be Hot-swappable		
	Stacking should support a minimum of 2 or more Switches		
	Stacking should support a maximum of 8 Switches		
	Stacking should support 80 Gbps of throughput		
	Stacking should support single IP address management for the group of switches		
	Stacking should support single configuration		
	Stacking should support simplified switch upgrade		
	Stacking should support automatic upgrade when the master switch receives a new software version		
	Stacking should support stacking cable length of 3m		
	Stacking should support QoS to be configured across the entire stack		
PoE & PoE+	The switch should support PoE (IEEE 802.3af)		
	The switch should support PoE+ (IEEE 802.3at)		
	The switch should support flexible power allocation across all ports		
	The switch should have 370W of Available PoE Power		
	The switch should support 24 ports up to 15.4W		
	The switch should support 12 ports up to 30W		
	The switch should support Per port power consumption to specify maximum power setting on an individual port		
	The switch should support Per port PoE power sensing to measure actual power being drawn		

	The switch should support protocol to allow switch to negotiate a more granular power setting of IEEE classiffied devices		
	The switch should support a PoE MIB to get visibility into power usage		
	The switch should support a PoE MIB to set different power-level thresholds		
Power Supply	The switch should support an auto-ranging power supply with input voltages between 100 and 240V AC		
	The switch should support an External Redundant Power Supply		
Standards	The switch should support IEEE 802.1D Spanning Tree Protocol		
	The switch should support IEEE 802.1p		
	The switch should support IEEE 802.1Q Trunking		
	The switch should support IEEE 802.1s Multiple Spanning Tree (MSTP)		
	The switch should support IEEE 802.1w Rapid Spanning Tree (RSTP)		
	The switch should support IEEE 802.1x		
	The switch should support IEEE 802.1ab (LLDP)		
	The switch should support IEEE 802.3ad Link Aggregation Control Protocol (LACP)		
	The switch should support IEEE 802.3af Power over Ethernet		
	The switch should support IEEE 802.3af Power Classification		
	The switch should support IEEE 802.3at Power over Ethernet +		
	The switch should support IEEE 802.3ah (100BASE-X single/multimode fiber only)		
	The switch should support IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports		
	The switch should support IEEE 802.3 10BASE-T specification		
	The switch should support IEEE 802.3u 100BASE-TX specification		
	The switch should support IEEE 802.3ab 1000BASE-T specification		
	The switch should support IEEE 802.3z 1000BASE-X specification		
	The switch should support RMON I and II standards		
	The switch should support SNMP v1, v2c, and v3		
RFC compliance	The switch should support RFC 768 - UDP		
	The switch should support RFC 783 - TFTP		
	The switch should support RFC 791 - IP		
	The switch should support RFC 792 - ICMP		
	The switch should support RFC 793 - TCP		
	The switch should support RFC 826 - ARP		
	The switch should support RFC 854 - Telnet		
	The switch should support RFC 951 - Bootstrap Protocol (BOOTP)		
	The switch should support RFC 959 - FTP		
	The switch should support RFC 1112 - IP Multicast and IGMP		
	The switch should support RFC 1157 - SNMP v1		
	The switch should support RFC 1166 - IP Addresses		
	The switch should support RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery		
	The switch should support RFC 1305 - NTP for accurate and consistent timestamp		
	The switch should support RFC 1492 - TACACS+		
	The switch should support RFC 1493 - Bridge MIB		
	The switch should support RFC 1542 - BOOTP extensions		
	The switch should support RFC 1643 - Ethernet Interface MIB		
	The switch should support RFC 1757 - RMON (history, statistics, alarms, and events)		
	The switch should support RFC 1901 - SNMP v2C		
	The switch should support RFC 1902-1907 - SNMP v2		
	The switch should support RFC 1981 - Maximum Transmission Unit (MTU) Path Discovery IPv6		

	The switch should support FRC 2068 - HTTP		
	The switch should support RFC 2131 - DHCP		
	The switch should support RFC 2138 - RADIUS		
	The switch should support RFC 2233 - IF MIB v3		
	The switch should support RFC 2373 - IPv6 Aggregatable Addrs		
	The switch should support RFC 2460 - IPv6		
	The switch should support RFC 2461 - IPv6 Neighbor Discovery		
	The switch should support RFC 2462 - IPv6 Autoconfiguration		
	The switch should support RFC 2463 - ICMP IPv6		
	The switch should support RFC 2474 - Differentiated Services (DiffServ) Precedence		
	The switch should support RFC 2597 - Assured Forwarding		
	The switch should support RFC 2598 - Expedited Forwarding		
	The switch should support RFC 2571 - SNMP Management		
	The switch should support RFC 3046 - DHCP Relay Agent Information Option		
	The switch should support RFC 3376 - IGMP v3		
	The switch should support RFC 3580 - 802.1X RADIUS		
Layer-2 Features	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors		
	The switch should support IEEE 802.1Q VLAN encapsulation		
	The switch should support Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically		
	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence		
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability		
	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.		
	The switch should support IGMP filtering		
	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.		
	The switch should support Per-port broadcaststorm control to prevent faulty end stations from degrading overall systems performance		
	The switch should support Per-port multicast storm control to prevent faulty end stations from degrading overall systems performance		
	The switch should support Per-port unicast storm control to prevent faulty end stations from degrading overall systems performance		
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN		
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth		
	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.		
	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.		
	The switch should support Local Proxy Address Resolution Protocol (ARP) working in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.		
	The switch should support IGMP v1, v2 Snooping		
	The switch should support IGMP v3 Snooping		

	The switch should support IGMP v1, v2 Filtering		
	The switch should support IGMP Snooping Timer		
	The switch should support IGMP Throttling		
	The switch should support IGMP Querier		
	The switch should support Configurable IGMP Leave Timer		
	The switch should support MVR (Multicast VLAN Registration)		
L3 Features	The switch should support Inter-VLAN routing		
	The switch should support IPv4 unicast Static Routing		
	The switch should support 16 IPv4 Static routes		
Smart Operations	The switch should support configuration of the Software image and switch configuration without user intervention		
	The switch should support automatic configuration as devices connect to the switch port		
	The switch should support diagnostic commands to debug issues		
	The switch should support system health checks within the switch		
	The switch should support Online Diagnostics		
Quality of Service (QoS) & Control	The switch should support 4 egress queues per port to enable differentiated management		
	The switch should support scheduling techniques for Qos		
	The switch should support Weighted tail drop (WTD) to provide congestion avoidance		
	The switch should support Standard 802.1p CoS field classification		
	The switch should support Differentiated services code point (DSCP) field classification		
	The switch should support Control- and Data-plane QoS ACLs		
	The switch should support Strict priority queuing mechanisms		
	The switch should support Rate Limitting function to guarantee bandwidth		
	The switch should support rate limiting based on source and destination IP address		
	The switch should support rate limiting based on source and destination MAC address		
	The switch should support rate limiting based on Layer 4 TCP and UDP information		
	The switch should support availability of up to 256 aggregate or individual polices per port.		
Management	The switch should support Command Line Interface (CLI) support for configuration & troubleshooting purposes.		
	The switch should support four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis		
	The switch should support Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.		
	The switch should support Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.		
	The switch should support SNMP v1, v2c, and v3 of-band management.		
	The switch should support Telnet interface support for comprehensive in-band managementof-band management.		
	The switch should support CLI-based management console to provide detailed out-of-band management.		
	The switch should support Serial Console Port		
	The switch should support USB Console Port		
	The switch should support SNMPv1, SNMPv2c, and SNMPv3		
Miscellaneous	The switch should support greener practices		
	The switch should support solutions that monitors and conserves energy with customized policies		

	The switch should support reduction of greenhouse gas (GhG) emissions		
	The switch should support an increase in energy cost savings		
	The switch should support sustainable business behavior		
	The switch should support Efficient switch operation		
	The switch should support Intelligent power management		
	The switch should support measuring of energy between itself and endpoints		
	The switch should support control of energy between itself and endpoints		
	The switch should support discovery of manageable devices for Energy measurement		
	The switch should support support monitoring of power consumption of endpoints		
	The switch should support taking of action based on business rules to reduce power consumption		
Network security features	The switch should support IEEE 802.1x to allow dynamic, port-based security, providing user authentication.		
	The switch should support Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.		
	The switch should support SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.		
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.		
	The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.		
	The switch should support Port security to secure the access to an access or trunk port based on MAC address.		
	The switch should support Multilevel security on console access to prevent unauthorized users from altering the switch configuration.		
	The switch should support Private VLAN		
DHCP Features	The switch should support DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addresses DHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.		
	The switch should support DHCP Interface Tracker (Option 82) feature to augment a host IP address request with the switch port ID.		
	The switch should support DHCP Option 82 data Insertion		
	The switch should support DHCP Option 82 Pass Through		
	The switch should support DHCP Option 82 - Configurable Remote ID and Circuit ID		
	The switch should support DHCP Snooping Statistics and SYSLOG		
IPv6 Features	The switch should be on the approved list of IPv6 Ready Logo phase II - Host		
	The switch should support IPv6 unicast Static Routing		
	The switch should support 16 IPv6 Static routes		
	The switch should support IPv6 MLDv1 & v2 Snooping		
	The switch should support IPv6 Host support for IPv6 Addressing		
	The switch should support IPv6 Host support for IPv6 Option processing		
	The switch should support IPv6 Host support for IPv6 Fragmentation		
	The switch should support IPv6 Host support for IPv6 ICMPv6		
	The switch should support IPv6 Host support for IPv6 TCP/UDP over IPv6		
	The switch should support IPv6 Host support for IPv6 Ping		

	The switch should support IPv6 Host support for IPv6 Traceroute		
	The switch should support IPv6 Host support for IPv6 VTY		
	The switch should support IPv6 Host support for IPv6 SSH		
	The switch should support IPv6 Host support for IPv6 TFTP,		
	The switch should support IPv6 Host support for IPv6 SNMP for IPv6 objects		
	The switch should support IPv6 Port Access Control Lists		
	The switch should support IPv6 Router Access Control Lists		
	The switch should support HTTP, HTTP(s) over IPv6		
	The switch should support SNMP over IPv6		
	The switch should support SysLog over IPv6		
	The switch should support IPv6 Stateless Auto Config		
	The switch should support DHCP based Auto Config (Auto Install) and Image download		
	The switch should support IPv6 QoS		
	The switch should support RFC4292/RFC4293 MIBs for IPv6 traffic		
	The switch should support SCP/SSH over IPv6		
	The switch should support Radius over IPv6		
	The switch should support TACACS+ over IPv6		
	The switch should support NTPv4 over IPv6		
	The switch should support IPv6 First-Hop Security		
	The switch should support IPv6 First Hop Security: RA Guard		
	The switch should support IPv6 First Hop Security: DHCPv6 Guard		
	The switch should support IPv6 First Hop Security: IPv6 Binding Integrity Guard		

Annexure-I

FORM XIV

IP Indoor / Outdoor Camera Specifications

Feature	Specifications	Compliance (Yes/No)	Deviation
Lens options	L12 (180° x 160°)		
Sensitivity	Colour sensor: 0.25 lux at 1/60 s, 0.013 lux at 1 s B/W sensor: 0.05 lux at 1/60 s, 0.0025 lux at 1 s		
Image sensors	1/2.5" CMOS, 5 megapixels, progressive scan		
Max. image size	Colour: 2048 x 1536 (QXGA), B/W: 2048 x 1536 (QXGA)		
Image formats	Freely selectable image format (160 x 120 up to 2048 x 1536/color); PTZ views: Surround (Quad), fisheye full image, normal, panorama, double panorama, panorama focus (3 views)		
Max. frame rate, M-JPEG (live/ recording)	VGA: 30 fps, MEGA/HD: 10 fps, QXGA 4 fps		
Max. video rate MxPEG live/recording/sound)	VGA: 30 fps, MEGA/HD: 30 fps, QXGA: 20 fps		
Image compression	MxPEG, M-JPEG, JPEG, H.264 (SIP video only)		
Internal DVR	MicroSD Slot (recording inside the camera, up to 64 GB; 4-GB card preinstalled)		
External storage	Directly on NAS and computer/ server without additional recording software		
Software	Video Management Software, Control Center Software, App for iOS devices iOS 5.0 and higher		
Image processing	Backlight compensation, Automatic White Balance, Image Distortion Correction (including Panorama Image Correction), Motion Detection.		
Virtual PTZ (vPTZ)	Digital Pan/ Tilt/ Zoom, continuous 8x Zoom, full image recording in the background		
Alarm/events	Triggering of events by integrated multiple-window Motion Detection, Temperature Sensor, notification over email, FTP, IP telephony (VoIP, SIP), Visual/ Acoustic Alarm, Pre- and Post-Alarm Images		
Audio	Lip-synchronous Audio, Intercom, Audio recording (optional).		
Interfaces	Ethernet 10/100, IPv4 / IPv6, Mini USB, Audio (IO); RS232		
Video telephony	VoIP/SIP, intercom, remote controlling with key code, event notification		
Security	User / Group management, HTTPS/SSL, IP address filter, IEEE 802.1x, intrusion detection, digital image signature		
Certifications	EMC (EN50121-4, EN55022, EN55024, EN61000-6-2, FCC part15B, AS/NZS3548)		
Power supply	Power over Ethernet (PoE in accordance with		

	IEEE802.3af): PoE class		
Operating conditions	IP65 (DIN EN 60529), -30° to +60°C (-22° to +140°F)		

Annexure-I
FORM XV

Voice Gateway Specifications

1. Should be chassis based & modular architecture for scalability and should be a single box configuration for ease of management.
2. Should support at least 4 interface slots to accommodate the current requirement as well as for the future expansion. The router should have 1 Service module slot and 1 ISM slot.
3. Should have support for hardware based IPSEC VPN (3DES/AES) Encryption card. Should have complete IPSEC VPN, Firewall, IPS features & future support for SSL VPN features.

4.Interfaces Required

Specifications	Compliance (Yes/No)	Deviation
2 x 10/100/1000 Base T interface.		
Should support e&m interface		
1 port Multiflex Trunk Voice/WAN Interface card - T1/E1		
1 Card to host Analog Lines		

5.Performance

Specifications	Compliance (Yes/No)	Deviation
Should support high performance traffic forwarding with concurrent features like Security, Voice enabled		
Should support variety of interfaces like V.35 Sync Serial (2 Mbps), Async Serial, E1 G.703, Ch-E1 for remote office aggregation		
GE as per IEEE 802.3z and 802.3ab, FE as per IEEE 802.3u, Chassis support for PoE as per IEEE 802.3af ISDN BRI, PRI		
Support for 802.11a/b/g Wireless Cards for Wireless LAN or Wireless Bridging functionality.		
Should have support for high density Voice interfaces like E &M, Voice E1 for connecting Analog phones & integration to PBX / PSTN.		
Should support performance enhancement through hardware based encryption / compression module.		
Should support at least 25 Mbps Throughput		
Should have USB 2.0 ports for storing OS images & secure token.		
Should have capabilities to support high volume internal storage up to 1TB to support various services as and when needed.		

7. High Availability

Specifications	Compliance (Yes/No)	Deviation
Should support redundant connection to LAN		
Should support Non-Stop forwarding for fast re-convergence of routing protocols		
Should support boot options like booting from TFTP server, Network node		
Should support multiple storage of multiple images and configurations		
Should support link aggregation using LACP as per IEEE 802.3ad		
Should support VRRP or equivalent		

8. Protocol Support

Specifications	Compliance (Yes/No)	Deviation
Should support Routing protocols like RIP ver1 (RFC1058)&2 (RFC 1722 and 1723), OSPF ver2 (RFC2328), OSPF on demand (RFC1793), BGP4 (RFC1771), IS-IS (RFC1195).		
Multicast routing protocols support : IGMPv1,v2 (RFC 2236), PIM-SM (RFC2362) and PIM-DM, DVMRP, M-BGP		
Should have IPv6 features: DHCPv6, IPv6 QoS, IPv6 Multicast support, Bi-Directional PIM, Multicast VPN, PIM SSM (Source Specific Multicast), IPv6 PIMv2 Sparse Mode, IPv6 PIMv2 Source-Specific Multicast,		
Should have RIPng and OSPFv3 for IPv6.		
Should have MPLS Features: MPLS VPN, MPLS (mVPN (Multicast VPN), VRF-Aware Services (NAT, FW, IPsec…), Carrier Supporting Carrier (CsC), DiffServ Tunnel Modes, MPLS TE, DiffServ-Aware TE, Inter-AS VPNs).		
Support for TCP Acceleration mechanisms to enhance the TCP performance over the WAN links. The TCP Acceleration mechanisms should be supported over end-to-end encrypted tunnels.		
Support for Circuit Emulation over IP to carry PBX traffic or legacy protocols in their native form.		

8. Voice Media Features

Specifications	Compliance (Yes/No)	Deviation
Shall support Voice capabilities. Should be able to act as IP PBX for		
ü Voice pass-through		
ü Codec support for G.711 and G.729		
ü Should support H.323, SIP, MGCP		
Should support Voice call processing of IP Phones in the event of WAN link failure to central location housing Central call processing Engine		
Should support bandwidth optimization features like Voice Activity Detection, Silence Suppression, Echo cancellation		

9. QOS Features

Specifications	Compliance (Yes/No)	Deviation
Shall support the following		
Classification and Marking: Policy based routing, IP Precedence, DSCP, MPLS exp bits		
Congestion Management: WRED, Priority queuing, Class based weighted fair queuing		
Traffic Conditioning: Committed Access Rate/Rate limiting		
Signalling: RSVP		
Link efficiency mechanisms: cRTP, LFI, MLPPP		
Per VLAN QoS. Time Based Shaping and Policing for QoS		
Shall support Classifiers for Intelligent Application Identification		

Annexure-I

FORM XVI

IP EPABX Specifications

Specifications	Compliance (Yes/No)
Voice Network	
The IP telephony system should be a converged communication System with ability to run TDM and IP on the same platform using same software load based on server and Gateway architecture. The system should be capable of supporting Analogue and IP Telephones. The single IP EPABX system should be provisioned to support up to 1000 stations (any mix/percentage of Analog/IP) to achieve the future capacity. All the users to be managed in a single database, which is managed centrally, no multiple databases. CLI facility for all users should be provisioned from day 1.	
The system should be based on server gateway architecture with **external** appliance server running on Linux OS. No card based processor systems should be quoted.	
The voice network architecture and call control functionality should be based on SIP.	
The Communication Server/Call Server would be deployed in a active-active configuration over the distributed IP infrastructure (LAN/WAN). The call control system should be fully redundant solution with NO single point of failure & should provide 1:1 redundancy. Both the servers should do call processing all the time and act as backup in case of the failure of one server.	
The system to have distributed architecture and the centralized control for all the IP PBX entities in the network. It should be possible to have centralized applications like voice mail, UC for the network users.	
The communication feature server and gateway should support IP V6 from day 1 so as to be future proof.	
It is required to provide Survivable Call Control functionality so that the survivable system at the remote location shall provide fall back call control service in case the remote site looses all connectivity to the main Call Control system placed at HQ datacenter. It is expected that the survivability call control system will provide a minimal set of essential telephony features to the end-users that could be a subset of the feature that are available from the main call control system.	
It should be possible for the IP phone to be connected on the same line, which is connected to the computer i.e. Single wire to desk.	
Call control server/ appliance should be Intel based hardware with necessary configuration to support the desired expandability. No proprietary hardware is acceptable.	
The system software version offered should be the latest release as on the date of supply of EPABX as available globally.	
The offered solution must provide a standard based mechanism for QoS implementation.	
System should allow direct registration / profile creation of SIP endpoints onto it and perform all functions of Proxy/ Registrar / Redirect etc	
In progress PSTN Calls at each of the locations should not be interrupted in the event of any WAN link failure or a call control server failure.	
Quality of Services (QoS) would be configured to administer the call and ensure voice traffic get priority over normal traffic.	
The System should support Call Admission Control to configure number of calls that can be active between locations —intercluster and intracluster.	
Should support LDAP integration for directory synchronization & user authentication.	
Support for call-processing and call-control.	
Should support signaling standards/Protocols – SIP, MGCP, H.323, Q.Sig.	
Voice CODEC support - G.711, G.729, G.729ab, g.722, ILBC	
Video codecs: H.261, H.263, H.264, and Wideband Video Codec	
Video telephony support (H.323, and SIP)	
Support for configuration database (contains system and device configuration information, including dial plan)	

Having inbuilt administration web based administration. No additional thick client for administration on the Admin PC. Should also support HTTPS for management.	
Should support 6 party adhoc conferencing.	
IP Phone Address Book Synchronizer—allows users to synchronize Microsoft Outlook or Outlook Express address books with Personal Address Book.	
Should provide Single Number Reach (Simultaneous Ring on IP phone and user defined alternate phone) for all the IP phone users.	
System Management & monitoring	
The System should have GUI support web based management console	
System should provide management tool to monitor system performance, device status, device discovery and CTI applications.	
Should provide alert notifications for troubleshooting performance	
It should support secure HTTPS & TCP to troubleshoot system problems.	
Generate various alerts in the form of e-mails, for objects when values go over/below pre-configured threshold levels.	
Should monitor the system in real-time on a set of preconfigured parameters.	
It should be possible to configure the sample interval rate for the applicable performance monitoring.	
The management platforms must provide different levels for accessing the system based on the role being played by the user who is accessing the system. The administrator should have the highest authority.	
Should provide a daily summary report of key monitoring parameters like Call Activity (No of calls attempts and completed), Device status (Number of registered phones / gateways / trunks per server), server status (load on server resources), alert status etc.	
Security	
The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS.	
The password and Access Control must Include the following:	
Passwords to prevent the possibility of an aggressor to easily read or deduce system or account access password.	
Password aging with Configurable time periods.	
System should support MLPP feature.	
Proposed system should support SRTP for media encryption and signaling encryption by TLS.	
Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory.	
The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server.	
End user / system Features required:	
Extension mobility	
Message-waiting indicator (MWI)	
Hunt groups	
Dial-plan partitioning	
The system should support at least **13** digit numbering scheme.	
Distributed call processing	
Hotline and private line automated ringdown (PLAR)	
Interface to H.323 gatekeeper for scalability, CAC, and redundancy	
Multi-Level Precedence and Preemption (MLPP)	
Q.SIG (International Organization for Standardization [ISO])	
Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool.	
Secure Sockets Layer (SSL) for directory	
Phone Security: TFTP files (configuration and firmware loads) are signed with the self-signed certificate of the TFTP server. The CallServer system admin will be able to disable http and telnet on the IP phones	

SIP trunk (RFC 3261) and line side (RFC 3261-based services)	
SIP trunk Call Admission Control (SIP CAC)	
Vendor should support basic SIP Trunking without need for any additional license or cost	
Time-of-day, day-of-week, and day-of-year routing and restrictions	
The proposed system should support automatic route selection (ARS) and least Cost routing (LCR) features to route the calls based on priorities related to user profile, tariff, and network availability, along the most cost-effective path. This service will be transparent for users and irrespective of the physical carrier connection.	
Distinctive Ringing. The system should provide audibly different station ringing patterns to distinguish between internal and external calls	
User Features	
Abbreviated Dial	
Callback busy, no reply to station	
Call park and pickup	
Call status per line (state, duration, number)	
Calling Line Identification (CLID)	
Calling party name identification (CNID)	
Direct inward dial (DID)	
Direct outward dial (DOD)	
Directory dial from phone—corporate, personal	
Directories—missed, placed, received calls list stored on selected IP phones	
Distinctive ring (on net vs. off net)	
Shared Line support	
Message waiting indication (Visual and Audio)	
Multiple line appearances per phone	
Music-on-hold	
Station volume controls (audio, ringer)	
Transfer	
Video (SIP and H.323)	
Boss-secretary feature support	
On-hook dialing	
Call waiting	
Call Conference.	
The System should be capable to integrate with Microsoft Exchange for Voice Mail Integration.	
Presence Services for IP phone users:	
The bidders should provide a "presence" application for all IP Phones users, so that they can see the availability status of his contacts in their buddy list.	
The common supported status for this application should be available, busy, idle, away etc.	
Should provide network based presence. This means that the user should be able to see the communication channel on which the other user is available; like chat, phone, video, email etc. If the remote user has not logged on to the presence client, primary user should be able to contact the person through phone, email etc.	
Should support the users to see other user's IP phone's on/off hook states	
The instant messaging application should support manual setting of user status to: Available, Away, Do Not Disturb (DND), Logged Off etc.	
Should support management of contact list, IM history, and personal settings.	
Shall provide support for open protocols like XMPP.	
It should support federation with other IM and Presence Applications/Server using open standard protocols	
Presence based desktop application shall allow escalation of Instant Message to Audio call and further to Video call	

Should support management of contact list, IM history, and personal settings from Presence based desktop application	
Presence based desktop application shall support logging of Instant Messages for compliance purpose if any.	
Should provide SSH and HTTPS access to management platform for enhanced security.	
Should support click to call, click to Video and click to conference features.	
Video Telephony Features and Support:	
The call control system should provide integrated video telephony features to the users so that user with IP Phone / Soft phone and video telephony end point should be able to place video calls with the same user model as audio calls.	
The users should be able to transfer video calls as audio calls	
It should be possible to have multiparty video call through the conferencing system.	
Call-Server should provide a common control agent for signaling, configuration, and serviceability for voice or video end points.	
Call control system should handle CODEC and video capabilities of the endpoints, bandwidth negotiation to determine if video/audio call can take place.	

Annexure-I

FORM XVII

IP Video Phone Specifications

Specifications	Compliance (Yes/No)
The IP Video phone should meet the following requirements –	
Phone should be of the same OEM as the IP-PBX/Call Control	
Have high-resolution 640 x 480 pixel backlit display with 5" or higher LCD Screen with integrated video Camera.	
Have Intuitive user interface and keypad for quick access to all IP phone and video services	
Have an integrated 2-port 10/100/1000 Ethernet switch.	
Support Bluetooth 2.0 or above and RJ-9 interface for headsets.	
Should have 3 or more line keys.	
Should have 4 or more programmable feature keys.	
SIP support for signaling.	
Audio Codec Support: G.711, G.729.	
Video Codec Support: using H.264 upto 30 fps.	
It support XML based applications for productivity enhancement.	
Full-duplex speakerphone with high-definition voice support for handset, headset and speaker	

Annexure-I

FORM XVIII

IP Phone Specifications

Specifications	Compliance (Yes/No)
Phone should be of the same OEM as the IP-PBX/Call Control	
The phone should be a SIP based	
Should have atleast 3.5” Display Size with resolution of 390 x 160 or better	
Should have full duplex speaker phone and dedicated headset port with RJ-9 interface.	
It should support G.711, G.729a/b audio compression codecs.	
Should provide the directory services to the user by displaying the missed, received and dialed call details including the caller ID and calling time.	
Should have 2 or more programmable line keys.	
Should have 4 or more programmable soft keys.	
Should support IEEE 802.3af POE, and external AC power adapter option.	
The phone should have two 10/100 BASE-T Ethernet ports, one for the LAN connection and the other for connecting to PC/laptop.	
The phone should support QoS mechanism through 802.1p/q.	
The phone should support XML based services and applications.	
Should support 7 adjustable ring tones.	

Annexure-I
FORM XIX

TECHNICAL SPECIFICATIONS FOR INTEGRATED RACK

ITEM	Specification	Compliance (Yes/No)
Integrated Cabinet with following :		
Rack	Two 42 U Racks for Information Technology Devices with integrated active cooling and hot air Exhaust with redundant UPS in the cabinet	
Features	Racks should be easy to install, remove and use	
Structure	Racks should be modular, flexible and easy to expand with Fire detection	
Capacity	6 KW or higher	
Active Cooling	2 Nos of Precision Air conditioner with variable scroll compressor 19inch rack mountable design fits only in 6U height . Both the units should be integrated and mounted Active Cooling with 5 star rating to control the heat density	
UPS	Rack Mounted Redundant 2 x 6 KVA UPS with minimum back up time of 60 minutes. Batteries would be kept externally.	
User Space	62 U or higher	
Monitoring and Sensor	Temperature, Humidity, Door Switch Sensor and Water Leak Sensor	
Power Distribution	AC power catered by redundant UPS on power strip with proper indicator and Earth Bus Bar on standard Rack PDU	
Monitoring	Integrated Monitoring and Control from remote	
Alerts & Notification	Event Alerts, SNMP, email notification	
Dimension (HxDxW) in mm	2100 x 1000 x 1600 or higher	
Remote Monitoring	24x7 remote monitoring from Central NOC for the installed integrated rack	
Warranty and Support	Minimum Comprehensive warranty and support for 3 years for components	

Annexure-I

FORM XX

TECHNICAL SPECIFICATIONS FOR COMMUNICATION TOWER

S.No	Specifications	Compliance (Yes/No)
1	Self supporting Latticed Tower with each section of 3 mtrs should be optimally designed for various parameters like height, wind speeds (140Kmph to 200Kmph), terrain, space available for site built-up, speed of erection etc.	
2	Tower should be designed to withstand various combinations of loading consisting of antenna loading, wind loading, seismic loading and self load of the structure in accordance to the relevant Indian Standards & Safety Factors.	
3	Various types of RF & MW Antenna can be easily mounted on these towers. Safety and ease of climbing for the maintenance team are the prime factors considered for the towers.	
4	Towers should be provisioned with adequate working space at working platform levels if required	
5	Should have provision for climbing ladder with safety hoops, Cable Ladder & Lightening Protection System.	
6	The material should be mild steel or high tensile steel.	
7	Entire structure should be hot dipped galvanized to provide weather protection against rusting.	
8	Depending on the placement, towers or poles are broadly categorized into two types –	
8.1	Ground Based (30m to 110m)	
8.2	Roof Top (3m to 30m).	

Annexure-I

FORM XXI

Professional Video Management Software

S.No	Specifications	Compliance (Yes/No)
1	VMS should be have user-friendly interface and camera display, convenient video search, practical alarm handling, automatic camera integration, video storage on file servers and a useful configuration and update assistant	
2	VMS should have Unlimited number of users and cameras, unlimited licenses and have the capability to run without third-party software	
3	Should have Individual user interface, adaptable to each individual user	
	Should have Central management and monitoring of several VMS locations from a central VMS location.	
4	Should have convenient layout editor for integrating real building plans	
5	Should have Integration of conventional network and analog cameras as well	
6	Should support export recordings as AVI and Quick time video with sound	
7	VMS should automatically discover cameras and storage in the network and configures all cameras at the push of a button.	
8	VMS should support the decentralized recording technology of the cameras. with higher performance, should have capability to bridge network failures without losing any of the recording data.	
9	VMS should support hybrid IP cameras and even Analog, motor-controlled PTZ cameras that can be integrated with VMS, displayed live and remotely controlled via a virtual or real joystick. The recorded videos of these third-party cameras can also be evaluated and exported to the VMS.	
8.1	Should have Time-Controlled Event Search using the chronological display of all event recordings of one camera. The search results should be displayed in a time line and preview of the selected event. The image settings should be immediately optimized and the event can be directly exported to VMS.	
8.2	Should support Filtering Events, Convenient Playback Functions, Printing of Event Images, Exporting of Recorded Video, Automatic Distortion Correction, Recorded video sequences can be analyzed later using Virtual PTZ.	
	Evaluation of recordings	
	Use of individually configurable search profiles (e.g. based on time, cameras, events). Scheduled display of event frequency for fast finding of events. Analysis of recorded video files for movements in the desired area. Replay of the recordings corresponding to the actual time sequence and Reference time-based evaluation.	
	Security	
	User management with group access Rights – Group/user management including limitation of specific work areas.	
	Failure detection of individual cameras/storage systems – Including notification by phone call, E-mail, network message.	
	Falsification safety – By signature of the recorded files; data integrity can be checked at the time of export.	
	Activity log – All activities of the users are recored and can be traced; filter functions for fast access to desired information.	
	Time synchronization – Uniform system time through support of internal/external time servers.	

Annexure-I

FORM XXII

Overall Solution

General Solution Overview and Key Deliverables

This is a converged solution in which multiple devices will be used. The solution needs to be implemented in a way that user will be authenticated by AAA in collaboration with Microsoft Active Directory. The NAC will control entire Guest profiling. The bidder need to study the solution comprehensively and will be providing Software only for AD, NMS, AV, and Video Monitoring which will be implemented on Oracle Blade Chassis that will be provided by University. Bidder needs to create the Entire end to end Network with DHCP, DNS, Active Directory, WiFi Network with high level of Security as per overall Solution specification. Bidder need to visit University and check the Blade Configuration before bidding in order to ascertain incase upgrade is required so that the same can be included in the bid. Successful bidder need to ensure that all three campuses (Nowgam, Magarmal Bagh and Sonawar should be primary connected on BNSL WAN (Connectivity provided by University in collaboration with BNSL) and Secondary Link on Radio with >100 Mbps of throughput. The Network should be implemented in such a way that there should be a hassle free Network with full utilization of NKN that will be based at Nowgam. The Bandwidth needs to be shared from Nowgam to Sonawar and Magarmal Bagh. The IP EPABX will be centrally implemented and accessed from anywhere in the Network. Selected vendor needs to migrate from existing EPABX. The IP Phone app should have capability to be installed on Smart Phone for accessibility to IP EPABX while the user is in campus. Bidder needs to ensure Virus and Broadcast free Network with quarterly Network Audit and preventive Maintenance. Replacement of any equipment should be Next Business day. The Bidder needs to quote with Comprehensive three years onsite warranty with two Resident Engineers 8*5 hours Support in the University from Monday to Saturday.

Detailed Solution Overview and Key Deliverables

Requirements	Description	Compliance (Yes/No)	Deviation
Logging and Reports	The Proposed solution then should allow user to access the internet/Intranet services and maintain a log of such users by storing User name, Mac Address/ IP Address/ Time of access etc. The system should give Comprehensive reports in a graphical format for decision making.		
Connectivity	SI will ensure a secure Wi-Fi connectivity and internet access through user Login ID and password to all the subscribers with central authentication mechanism.		
NMS	The SI will deploy NMS and integrate it with Existing wired network devices and proposed Wireless network devices. Any required software on Server to be provided by bidder.		
Documentation	Complete documentation and Project report should be submitted with all Network diagrams in a PPT and word Format.. All diagrams should be well marked with each and every component and easily understandable. Vendor to share the detailed HLD and LLD for the proposed solution post qualification of Tender in 15 days time.		
UAT Plan	The SI shall be responsible for Preparation and submission of detailed UAT plans/ schedules/ procedures/ formats.		

UAT	UAT of each Wi-Fi network shall include the following tests which are essential requirement under the project : - i. Footprint Test. ii. SSID Test. iii. IEEE 802.11 b/g/n/ac: The Wi-Fi network should support IEEE 802.11 b/g/n/ac standards. iv. Security: The compliance of security/ access mechanism as proposed. v. Logs: The compliance of authentication, access, usage and other required logs as proposed. vi. Performance Test: A file download test from any HTTP/ FTP server using FTP would be done.		
Reliability	Beamforming to fortify RF connections – AP's must increase reliability of the AP/client link		
	Satisfactorily handling all the issues related to connectivity, performance and security.		
	Appliances have ability to be clustered in any combination via local and remote network connections providing unlimited scale, redundancy, and access load balancing through external load balancer.		
	Solution platform must have support for deployable in with N+1 redundancy model.		
	Must support several deployment modes including centralized, distributed, or mixed.		
User Density	The different locations in the campus will be categorized into three categories based on the density of concurrent user devices for designing of the system architecture. i) High density locations: 30-70 user devices/ 100 square meters ii) Medium density locations: 10-30 user devices/ 100 square meters iii) Low density locations: < 10 user's devices/ 100 square meters		
Consistency	Consistent policy across wired, wireless, and VPN for managed and BYOD assets, revealing who and what are on the network		
Device Management	Should support Mobile device and mobile application management (MDM/MAM) integration for greater visibility and control		
Self Service	User-specific services, with self-service onboarding, guest handling, and location-based services		
Life Cycle Management	Lifecycle management that simplifies and automates infrastructure management tasks		
Proactive Alerts	Wireless AP, Controller, AAA, NMS, Switches should be remotely monitored by the SI or their local partner for all the devices that are procured as a part of this Tender. Direct access 24 hours a day, 365 days a year to specialized engineers in the Technical Assistance Center. Whenever a problem affects our setup or systems, TAC team from SI/Local Partner / OEM must have full access and do the real time analysis as applicable and inform customer about the issues.Relevant hardware, software, security alerts, and field notices should be available in a portal format accessible to the designated IT SPOC's of Central University of Kashmir with a secured login to help Preempt service disruptions and notification of important information about the products in the network.		
Hardware Replacement	Advance hardware replacement to be made available Next-business-day		

Reporting	Reporting - Reports identify which products have been moved, added, or changed in your installed base between two analysis/collection points in time, as well as changes to product alerts. Product Alert Reports should be available to show alerts between two analysis/collection points in period of time, such as from the last 30 days		
Asset Management	The SI/ Local Partner needs to ensure that their tools does give Assets information of installed assets in every 30 days.		
Expiry Coverage	SI /Local Partner / OEM TAC tools should generate reports that show Central University of Kashmir contract expiry dates, helping us to plan our budget accordingly. The minimum Contract for all products supplied by SI / OEM in this RFP for advance diagnostics support needs to be 3 years from the time of signing the contract with SI		
Wi-Fi Coverage	Wi-Fi network access should be available throughout the campus inside the buildings as well as in outdoor locations to all the staff, students and visitors of the university based on well-defined access policy. It is also mandatory to ensure that coverage is there but with appropriate throughput not less than 20 mbps per user depending upon the environmental conditions.		
General Terms and Conditions	Vendor to ensure that all indoor Access points need to be 802.11 ac		
	Bidder to ensure that supplied Access points should support end user standard i.e 802.11a/b/g/n.		
	Bidder to ensure that quoted 11ac AP is field upgradable to 2nd generation 11ac standard when it becomes available in market; Latest Access Point must be provided to Central University of Kashmir.		
	The System should support seam-less roaming within the connected campuses for users with mobile devices such as smart phones and tablets.		
	The network should support the user devices with 2.4 GHz as well as 5 GHz frequency band at the same time.		
	It should be possible to manage the Wi-Fi network from a central location though the wireless management system. The management system should preferably support unified wired and wireless network management, and BYOD (Bring your own device) solution. Vendor should be able to manage Wired and Wireless from a Centralized Solution		
	It should be possible to configure and deploy access points (Apes) remotely through controller		
	System should support multiple VLANS to support users with different privileges. Instead of one single large vlan(Broadcast domain),System must be able to have multiple small vlans will be grouped to map with single SSID without any external device.		
	Every concurrent user should effectively get at least 20 Mbps bandwidth. The end user needs to ensure to be in a diameter of any AP on which it is latched to achieve the same till 30 feet of distance from AP.		
	Time-of-day availability of SSID		

	Must support AP enforced load-balance between 2.4Ghz and 5Ghz band. Incase end points are coming fro 802.11 a/b/g/ac/n, then they should get load balanced way of bandwidth.		
	The Architecture of the system should support scalability to support future expansions – subsequent project phases and increased user density.		
	The system architecture should ensure that interference of Apes is avoided.		
	The system should provide radio resource management. Compliance to 802.11k and 802.11r is preferred whenever these standards are finalized.		
Authentication	The entire Wi-Fi network should be fully secure. In particular.		
	Multiple authentication mechanisms should be implemented. The user will be authenticated by AD and AAA.		
	Every user should get access to only those services for which they are authorized.		
	Support for Role-based access rights		
	Data communication between devices should take place in encrypted form to ensure end-to-end security of user information/ data.		
	Support in-line security standards WPA, WPA2		
	Secure Guest Portal should be implemented from day 1.		
	System must have Role based access e.g student should not able to execute telnet and ping, however on same SSID IT team will be able to execute telnet and ping. Similarly other policies also. This should also include Location based access.		
QOS	System should provide QoS features given below		
	Traffic Prioritization for different application requirements		
	Support Type of Service marking and 802.11p priority tagging.		
	Support Wi-Fi Multi Media (WMM) based on 802.11e standard		
	Ability to limit per-user bandwidth rate.		
	Self-healing should be available from day 1.		
	Support per user, per device, and per application/TCPport Prioritization		
	Dynamic load balancing from day 1.		
	Adaptive RF management from day 1.		
	Support advanced multicast features with multicast rate optimization, multi channel use and IGMP snooping		
	The physical security measures such as Enclosures for AP's with locks should be provided		
Facility Management	Bidder will arrange for atleast 2onsite Engineers, for the period of 3 year from the date of acceptance and for additional two years if University decides to enter into comprehensive AMC, to look after the facility management services related to Wi-Fi facility. These services include		

	The delivery for all equipment's should be done in 45 days after the release of PO.		
	The entire project needs to be completed in 2 Months from supply of equipment.		
	Providing connectivity to user devices as per Wi-Fi access policy		
	Passive Work		
	Bidder to ensure that there must be Professional workmanship done for any Passive work.		
	Every Cable needs to have a Tag from both ends so as to Identify the Cable and its purpose		
	Bidder to ensure that in 3 years onsite Maintenance Contract all change Managements will be Free of any Cost.		
	Bidder to ensure that all persons onsite must have hands on Wireless Experience. Persons with BE/B Tech/BIT/Bsc IT/MCA/M.Tech/Msc IT will be preferred.		
DAM on 802.11 ac	**Denser amplitude modulation** – 128/256-QAM supported AP's on 802.11ac.		
MIMO	Multi-user MIMO – AP's should support simultaneous transmissions to multiple clients and maximizes RF band utilization. 3*3:3 streams is required. 4*4:3/4*4:4 streams will be preferred.		
Security	Wi-Fi access points (APs) must be configured to use cryptographic keys or other methods to ensure that only authenticated users can use the Wi-Fi service.		
	The Wi-Fi network should be secure and conform to the industry standard security requirement. SI shall deploy policies at various levels (i.e. on firewall, IDS/IPS, antivirus etc.) to prevent any attack/ intrusion in the Wi-Fi network.		
	In case of misuse of the Wi-Fi network, the SI shall be liable for legal proceedings / penalties as per the Law/ Act in force and as applicable		
	There should be an encrypted tunnel between AP to Controller.		
	Must Support Certificate Authority based authentication. In case Central University of Kashmir wants that SI should implement it from day 1.		
	Meet all Security features as mentioned in Controller and AAA and Security Specifications		
Certifications	For all the quoted AP's the bidder should provide WPC license copy as per DOT, Govt Of India Regulation. Must have all necessary Health regulation certifications and to be shared with Central University of Kashmir.		
Maintenance	The SI shall provide preventive maintenance services for all the equipment at least once in every quarter. The preventive maintenance shall include - a) Check for any loose contacts in the cables & connections. b) Cleaning and removal of dust and dirt from the interior and exterior of the equipment etc.		

	The maintenance services involves comprehensive maintenance of all component covered under the contract, including repairing, replacement of parts, modules, sub-modules, assemblies, sub-assemblies, spares part, updating, security alerts and patch uploading etc. to make the system operational.		
	Provide comprehensive onsite warranty and maintenance with spare parts, system software/ firmware/ signature updates, patches etc. for all the IT infrastructure supplied and installed under this project and to maintain the required SLA for a period of 3 years from the date of commissioning.1.		
	Providing connectivity to user devices as per Wi-Fi access policy		
Passive Work	Meet all specification as mentioned in Passive specifications.		
	Bidder to ensure that there must be Professional workmanship done for any Passive work.		
	Every Cable needs to have a Tag from both ends so as to Identify the Cable and its purpose		
NMS	As per NMS specification		
IP EPABX	As per IP EPABX specification		
IP Camera	As per IP Camera specification		
Antivirus Server	Bidder to install, implement and common Antivirus Server		
Active Directory	Bidders have to install & configure AD Server and integrate with AAA. Bidder will be responsible for configurations required for End Point Devices.		
Video Monitoring	Bidders have to install & configure VMS software and ensure that it can be used to connect any numbers of cameras without purchasing any licences. VMS should have the capability for Analytics required by University from time to time. Bidder should provide necessary training to University Officials for VMS & Analytics operation and administration.		

Annexure-I
FORM XXIII
Overall Location Wise BOQ

S.No.	Central University of Kashmir	No. Floors	Proposed NKN Connectivity From	Data Nodes	Indoor AP	Outdoor AP	UTM / Firewall Appliance	AD SERVER (Win DataCenter Server	AV Server Software	AAA Server Appliance based	IP EPABX (HA)	Voice Gateway	IP Video Phone	IP Phone	NMS	IP Camera - Indoor	IP Camera - Outdoor	Video Management Software	NAS	Core Switch	24 Port PoE Switch	Point to Multi Point RF Radio with Sectoral	Point to Point RF Radio	Mast 10 mtr	Datacentre Smart Rack	Rack 12 U	UTP Cable	PVC Conduit 1"	PVC Flexible1"	Unloaded 24 Ports Jack Panel	CAT 6 Information Outlet	Surface Mount Box / FP - Single Port	CAT 6 UTP 1 Mtr Patch Cord
1	**SONAWAR CAMPUS**	4	BSNL/Nowgam										3	20							5		1	1									
	1st Floor			30	2											1	1										680	225	20	5	34	30	34
	2nd Floor			30	2											1											660	220	20		33	30	33
	3rd Floor			30	2											1											660	220	20		33	30	33
2	**MAGARMAL BAGH CAMPUS**	3	Nowgam											5							1		1	1									
	G-Floor				2											1	1										30	20	5	1	4	6	4
	1st Floor				2											1											50	40	10		3		3
	2nd Floor				2											1											80	65	15		3		3
3	**NOWGAON CAMPUS**	4	BSNL				1	1	1	1	1	1	2	45	1			1	1	1	6	1		1	1	1							
	G-				7											2											100	50	10	3	9		9

	Floor																															
	1st Floor				7	2										2											200	100	10		11		11
	2nd Floor				7											2											100	50	10		9		9
	3rd Floor				5											2											100	50	10		7		7
4	**BROWSING CENTRE**		Nowgam	70												1					3					1	1420	710	20	3	71	70	71
5	**BOYS HOSTEL**		Nowgam		10																1		1	1		1	200	150	20	1	10	10	10
6	**GIRLS HOSTEL**		Nowgam		10																1		1	1		1	200	150	20	1	10	10	10
TOTAL				**160**	**58**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**5**	**70**	**1**	**15**	**2**	**1**	**1**	**1**	**17**	**1**	**4**	**5**	**1**	**4**	**4480**	**2050**	**190**	**14**	**237**	**186**	**237**

Annexure-II
FORM I
FINANCIAL BID
ACTIVE COMPONENTS

S.No	Description	UoM	Qty	Unit Rate	Amount in INR	Tax - %	Tax Amount	Total Amount in INR.
1	Indoor Wireless Access Point 802.11ac with mounting kit and accessories.	Nos.	58					
2	Outdoor Wireless Access Point 802.11n with mounting kit and accessories.	Nos.	2					
3	WLAN Controller should support up to 1000 Access points	Nos.	2					
4	Core Switch with 48 1/10G ports SFP+ & should support 12 number 40G QSFP ports for future scalability	Nos.	1					
5	1000 Base T SFP Module for Core Switch	Nos.	24					
6	Access Switch with 24 10/100/1000BASE-T PoE with 4 1 G SFP Uplink Ports.	Nos.	17					
7	UTM / Firewall with 5 Year Support & Reporting Software	Nos.	1					
8	AAA Server (Hardware Appliance) with advanced policy control for up to 1000 unique endpoints scalable upto 250000 end points.	Nos.	1					
9	MS Windows Server Data Center 2012 Single OLP (Academic Software)	Nos.	1					
10	MS Windows 2012 Client Access License Dvc CAL Academic OLP Licenses	Nos.	300					
11	NMS for alerting, management and reporting with (Software Only)	Nos.	1					
12	IP EPABX system should be provisioned to support up to 1000 stations (any mix/percentage of Analog/IP) to achieve the future capacity	Nos.	1					
13	VoIP Gateway should support at least 4 interface slots to accommodate the current requirement as well as for the future expansion	Nos.	1					
14	IP Video Phone (As per specifications).	Nos.	5					
15	IP Phone (As per specifications).	Nos.	70					
16	McAfee Endpoint Protection Suite LICENSE: Per Node. DELIVERABLE: Download. PRODUCT CONTENT: VirusScan Enterprise, VirusScan Command Line, VirusScan Enterprise for Linux, SiteAdvisor Enterprise with Web Filtering, Endpoint Protection for MAC, Device Control, Desktop Firewall, McAfee Security for Email Servers with Anti-Spam, RealTime for ePO. Management system should included: ePolicy Orchestrator. **End Point Protection should have license subscription for 3 Yrs**	Nos.	300					
17	5 Mega Pixel High-Resolution Integrated 4 GB DVR IP Indoor Camera with Video Management Software	Nos.	15					
18	5 Mega Pixel High-Resolution Weatherproof Integrated 4 GB DVR IP Outdoor Camera with Video Management Software	Nos.	2					
19	Video Management Software with unlimited license (As per specifications)	Nos.	1					
20	NAS Dual Core 2.4 Ghz/4 GB DDR-III/ + 6 bay Open for future expansion /USB 3.0/USB 2.0/Dual Giga LAN /10 G optional /2 U RACK /RAIL KIT with 3 TB Enterprise Class HDD X 6 Nos.	Nos.	1					
21	Point to Multi Point RF Radio with 90° Sectorial Antenae, Reflector and accessories	Nos.	4					
22	Point to Point RF Radio for connectivity with PMP Radio and including all accessories	Nos.	4					
TOTAL ACTIVE COST								-

Annexure-II
FORM II
FINANCIAL BID
PASSIVE COMPONENT

S.No	Passive Components	UOM	Qty	Unit Rate (in Rs.)	Amount	Tax %	Tax Amount	Total Amount
1	Datacentre Integrated Smart Rack (As per specifications)	Nos.	1					
2	19 " 12 U Network Rack 2 Fans with Fan Tray, 1 x Cable Manager, 1 x 6 Socket PDU, 1 x H/w Packet of 10 and should be complete with all accessories.	Nos.	4					
3	CAT 6 UTP Cable - roll of 305 mtrs. - *BLUE Color*	Nos.	15					
4	Unloaded 24 Ports Modular Jack Panel	Nos.	14					
5	CAT 6 Information Outlet - *BLUE Color*	Nos.	397					
6	Surface Mount Box - Single Port	Nos.	186					
7	CAT 6 UTP Patch Cord 4 feet - *BLUE Color*	Nos.	237					
8	1-inch PVC Conduit Pipe with accessories (AKG)	Mtrs.	2050					
9	1-inch PVC Flexible pipe including all accessories (Reputed Brand)	Mtrs.	190					
10	Mast / Tower Self Supporting (As per specifications)	Mtrs.	50					
TOTAL PASSIVE COST - B								

Annexure-II
FORM III
FINANCIAL BID
INSTALLATION & SERVICE COMPONENT

S.No	Service Components	Qty	UOM	Unit Rate* (in Rs.)	Total Amount (in Rs.)	Service Tax- 12.36%	Total Amount (in Rs.) Including ST
1	Installation of Access Points (Indoor)	58	Nos.				
2	Installation of Access Points (Outdoor)	2	Nos.				
3	Installation & Configuration of Wireless LAN Controller Switch	2	Nos.				
4	Installation & Configuration of AAA Server & integration.with Guest Life Cycle	1	Nos.				
5	Installation & Configuration of Access Switch	17	Nos.				
6	Installation & Configuration of Core Switch	1	Nos.				
7	Installation & Configuration of UTM / Firewall	1	Nos.				
8	Installation & Configuration of AD Server	1	Nos.				
9	Installation & Configuration of AV on End Points	300	Nos.				
10	Installation & Configuration of EPO Server	1	Nos.				
11	Installation & Configuration of DHCP Server	1	Nos.				
12	Installation & Configuration of DNS Server	1	Nos.				
13	Installation & Configuration of IP EPABX Server	1	Nos.				
14	Installation & Configuration of IP Phones	75	Nos.				
15	Installation & Configuration of IP Camera	17	Nos.				
16	Installation & Configuration of Video Monitoring & Management Software	1	Nos.				
17	Installation & Configuration of RF Point to Multi Point Base APs	4	Nos.				
18	Installation & Configuration of RF Point to Point Subscriber Modules	4	Nos.				
19	Installation & Configuration of Datacentre Rack	1	Nos.				
20	Laying of UTP Cable	4480	Mtrs.				
21	Laying of PVC Conduit / Flexible pipe.	2050	Mtrs.				
22	Installation of 24 ports Jack panel	14	Nos.				
23	Installation of Information Oultlet	397	Nos.				
24	Termination of Information Outlet	397	Nos.				

25	Installation of Surface Mount Box	186	Nos.				
26	Fixing of cable manager, Switch, LIU, Jack Panel, Patch Cords, etc.	4	Nos.				
27	Installation of 12 U Rack	4	Nos.				
28	Installation of Mast / Communication Tower	50	Mtrs.				
29	Installation and dressing of patch cords on Jack Panel/Cable Manager/Switch	237	Nos.				
30	Labeling of Jack Panels with Printed labels	14	Nos.				
31	Labeling of patch cords with Printed Labels	237	Nos.				
32	Pentascanning Testing of Data Nodes	237	Nos.				
33	Certification of Site for Performance Warranty of 25 Years.	237	Nos.				
34	Complete Documentation w.r.t. network layout, cable structure, with count of Active, Passive Components with segregated list of each component for each network site implemented / operational as directed by CUK.	1	Nos.				
35	Project Management Charges	1	Nos.				
36	Per Resident Engineer per Year Cost	3	Yr				
TOTAL INSTALLATION COST - (C)							
Total Amount (Active(A)+Passive(B)+Service(C)) =							-

Amount in words: _____

Name and signature of the authorized person of the firm along with seal

Place:

Date: