NIT No.: e-08/2018(Pur-Kol)-Revised

Date: 23.02.2018

CORRIGENDUM / ADDENDUM

Tender No. e-08/2017 (Pur-Kol)

"RENOVATION AND UP-GRADATION OF NETWORK INFRASTRUCTURE (LAN & WiFi)"

Sl. No.	Existing Spec./Item/Particulars	Revised Spec./Item/Particulars
1	Sl. No. 56 under "24 port PoE Access Switch" Part-A, Main Campus: The switch should have minimum 24 x 10/100/1000 Base-T POE/POE+ Ports & 2 x 10G SFP+ slots. The switch should have 360W POE Budget	The switch should have minimum 24 x 10/100/1000 Base-T POE/POE+ Ports & 2 x 10G SFP+ slots populated with 1 x 1000 Base-LX SM Module. The switch should have 360W POE Budget
2	Sl. No. 110 under "24 port Non- PoE Access Switch" Part-A, Main Campus: The switch should have minimum 24 x 10/100/1000 Base-T Ports & 2 x 10G SFP+ slots.	The switch should have minimum 24 x 10/100/1000 Base-T Ports & 2 x 10G SFP+ slots populated with 1 x 1000 Base-LX SM Module.
3	Sl. No.2 (12 Access Switch – PoE) under Part B-BOQ FOR GIRL S' HOSTEL: No detail spec. mentioned in the tender document	Detail spec. incorporated as "12 port Layer 2 POE Switch"
4	FINANCIAL BID (Annexure-IV) Sl. No. 9 (Installation and Configuration) under Part-A of Service Components, Main Campus and Sl. No. 4 (Installation and Configuration) under Part-B, Girls' Hostel of Service Components: Installation and Configuration of Active devices, Testing and Documentation of entire project. 3 Years service support	Installation and Configuration of Active devices, Testing and Documentation of entire project with 3 Years' service support + Dismantling of existing old networking cables and equipment's

The above has been incorporated/modified as and where applicable in the tender document and a revised tender document has been uploaded. All the bidders are requested to follow the revised tender document only and quote accordingly and ignore the earlier tender document. Bid submitted based on the earlier tender document will be summarily rejected. Bid submitted based on the revised tender document will only be considered.

Sd/-
(Purchase Officer)

NIFT CAMPUS, Plot No. – 3B, Block-LA, Sector – III, Salt Lake,
Kolkata - 700098
Phone: 91-33-2335 7546, 2890, 8350 Fax No. 91-22-2335 5734
Web: www.nift.ac.in/kolkata

NIT No.: e-08/2018(Pur-Kol)-Revised

Tender Document Fee Rs. 500/-

राष्ट्रीय फैशन टैक्नालॉजी संस्थान कोलकाता केन्द्र

(वस्त्र मंत्रालय, भारत सरकार)

NATIONAL INSTITUTE OF FASHION TECHNOLOGY, KOLKATA
(A Statutory Body governed by the NIFT Act 2006 &
set up by Ministry of Textiles, Govt. of India)
(ISO 9000:2008 certified Institute)

TENDER
For

"RENOVATION AND UP-GRADATION OF NETWORK INFRASTRUCTURE (LAN & WiFi)"

Tender No.: e-08/2017(Pur-Kol)

OPENING DATE FOR ONLINE SUBMISSION OF TENDER	14/02/2018
CLOSING DATE FOR ONLINE SUBMISSION OF TENDER	09/03/2018 up to 2.00 pm.
Date and time of opening of tenders (Technical Bid)	09/03/2018 at 3.00 pm.

Opening Date and Time of Financial Bidding: will be notified to the short listed bidders only

PREAMBLE / INTRODUCTION

National Institute of Fashion Technology is a Statutory Body governed by the NIFT Act 2006 & set up by the Ministry of Textiles, Govt. of India

Note: 1. NIFT Donations are exempted u/s 80 (G) of Income Tax Act.
2. Being registered with DSIR, NIFT is entitled for Custom/Central Excise duty exemption.

(A) **TENDER NOTICE**

NIFT Kolkata invites online tender under two bid systems for "Renovation and Up-Gradation of Network Infrastructure (LAN & WiFi)" from the eligible reputed Firms/ Agencies.

The hard copy of the tender alongwith fees (DDs for EMD, Tender Cost), necessary/relevant documents should be placed in a sealed envelope superscribed with "Tender for Renovation and Up-Gradation of Network Infrastructure (LAN & WiFi)-NIFT: e-08/2018(Pur-Kol)" and shall be addressed and sent to the Purchase Officer, National Institute of Fashion Technology, Block-LA, Plot-3B, Sector-III, Salt Lake City, Kolkata- 700098 or dropped in the Tender Box kept at the said address on or before 09.03.2018 up to 2.00 pm in the following manner. Hard copy of Financial Bid/ Quotation need not be submitted.

(B) SUBMISSION OF BID

The interested firms should apply online and submit their bids along with scanned copies of all the relevant certificates, documents, etc. in support of their technical & price bids – all duly signed – on the https://nifttenders.eproc.in from 14.02.2018 to 09.03.2018 up to 2.00 P.M.
Tender documents are also available for viewing on the "tenders" link of the NIFT website i.e. https://nifttenders.eproc.in
Applications to this tender will be accepted only in the online mode through the website https://nifttenders.eproc.in. No other mode of application will be considered & accepted.
For applying online, the prospective bidder/Firm should get itself registered at https://nifttenders.eproc.in
• Registration Charges of Rs. 2000/- + (GST) = Rs-2360/- (Two thousand three hundred sixty only) non-refundable.
• Bid Processing Fee charges of Rs. 3200/- + Rs. 576/- (GST) =Rs. 3776/- (Three Thousand seven hundred seventy six only) non-refundable through online payments only.
The interested firms are advised to read carefully the entire tender document before submitting their tender and the tender documents not received online in prescribed format and/or are found incomplete in any respect shall be summarily rejected.
Any further clarifications can be sought from the NIFT office on Telephone No. 033- 23357546, NATIONAL INSTITUTE OF FASHION TECHNOLOGY, NIFT Campus, Block-LA, Plot-3B, Sector-III, Salt Lake City, Kolkata-700098.

For online procedure:
For More enquiries/For Helpdesk officers:- Mr.Sandeep Bhandari,
E-mail:- sandeep.bhandari@c1india.com
Phone No.:- 0124-4302033/36

Commencing date of Tender: 14.02.2018
Last date of Submission: 09.03.2018 up to 2.00 PM
Date of opening of Tender (Technical Bid): 09.03.2018 at 3.00 PM
Cost of Tender form: Rs 500/- (Non-refundable)
Earnest Money Deposit: Rs 1,20,000/- (Rupees One Lakh Twenty Thousand only) (refundable)
Security Deposit: 5% of the order value [refundable; to be submitted by the successful bidder only after receiving of the P.O.]

GENERAL TERMS & CONDITIONS:

1. Only online bids will be considered.

   In addition to on-line, the hardcopy of the Technical Bid (Annexure-I, II & III only) along with necessary fees through DD, and documents should be submitted within the specified date & time and at the said address. Annexure-IV (Financial Bid) to be submitted online only.

2. Please read the terms & conditions carefully before online submission/filling up the document. Incomplete tender documents will be summarily rejected.

3. Conditional or offline tender will not be accepted or the condition(s) may not be considered.

4. Tender(s) submitted beyond the scheduled last date & time due to whatever reason including postal delays and without the required fees, Annexure(s) & documents will not be considered.

5. A separate Demand Draft of Rs. 500/- (Rupees Five Hundred Only) (Non-Refundable) drawn in favour of NIFT Kolkata payable at Kolkata towards Tender Cost shall be attached with Technical Bid.

6. All tenderers are required to submit Earnest Money Deposit (EMD) of Rs.1,20,000/- (Rupees One Lakh Twenty Thousand Only)(refundable) in the form of Demand Draft (should be drawn beyond the date of notification of this NIT) in favour of NIFT Kolkata payable at Kolkata. No interest shall be paid on the said EMD and will be returned after finalization of the tender; however, the EMD of the successful bidder will remain with NIFT and will be forfeited in the following events:

   a. If information declared/document submitted found false/fake/forged
   b. If the selected/successful bidder does not accept the W.O., or, unable to supply the product
   c. If the bidder withdraws his bid/quote

7. The successful bidder shall deposit the Security Deposit of 5% of the ordered value through DD/Bank Guarantee in favour of NIFT Kolkata within two weeks from the date of receiving of Work Order. No interest will be paid on this deposit which will be refunded after two months on completion of warranty period of the delivered items and after adjusting dues, if any.
8. The minimum annual turnover of the tenderer for the last two years (i.e F.Y. 2014-15 & 2015-16) should not be less than Rs.10.00 Crore per year which should be substantiated by valid document(s), viz. IT Returns/Audit report, etc..
9. The Financial Bids of technically qualified bidders only will be opened.
10. Even after qualifying in technical bid, the financial bid may not be accepted if found not in order.
11. In case of L-1 is more than one, the selection criteria [viz. the past performance, experience, etc.] would be at the discretion of NIFT. The decision of NIFT, in this regard and for selection of successful bidder in such situation, will be final in all respect and will be binding on all the tenderers.
12. Lowest bid may not be the only criteria for selection and NIFT is not bound to issue work order to the agency being the 'L-1' bidder; weightage/ preference will also be given to the other factors, viz. previous experience, quality of service, number of client, yearly turnover, etc. to select the agency to award the work and the decision of NIFT in this regard and for selection of successful bidder will be final in all respect and will be binding on all the tenderers.
13. GST & other charges, if any, should be mentioned clearly; otherwise, the rates may be treated as all inclusive, or bid may not be considered.
14. The full and final payment for indigenous items shall be made after Renovation and Up-Gradation of Network Infrastructure (LAN & WiFI) at NIFT Kolkata & submission of required performance security and acceptance of goods in good condition on the basis of certification by the concerned department of NIFT, Kolkata. No payment will be made in advance. Deduction (TDS, etc.), if any and as applicable, will be made during payment.
15. The rates quoted should be in INR only.
16. The annual turnover of the tenderer during the last two years [FY: 2014-2015; 2015-2016] should not be less than Rs.10.00 Crore per year.
17. The bidder should be authorized dealer/partner/reseller etc. of the concerned OEM and submit the authorization certificate; however, tender specific authorization of the respective OEM may also be considered and tenderer should enclose a copy of the same with the Technical bid.
18. The Renovation and Up-Gradation of Network Infrastructure (LAN & WiFi) should be executed at NIFT Campus, Block-LA, Plot-3B, Sector-III, Salt Lake City, Kolkata – 700 098 by the supplier at its own cost within 10-12 weeks from the date of receiving of Work Order.
19. The schedule issued with the form of tender listing the details of item to be supplied must not be altered by the tenderer. Any modifications/ alterations of the schedule considered necessary by the tenderer, should be in a separate letter accompanying the tender.
20. The financial bid will be valid in the case of all the tenders for at least 3 months from the date of opening of the tender (Financial bid). In the case of the successful bidder, rates quoted will be valid for the entire period till the commissioning of the work.
21. The tender is liable to be rejected if complete information is not given there-in, or if the particulars and data (if any) asked for in the Schedule of the tender are not filled in correctly.
22. Late submission of tender will not be considered.

23. Tender shall be accompanied by the relevant documents including the following:-
    a) Current/valid trade license
    b) A client list as per sl.no.3, Annex-I
    c) Total turnover of the company for last 2 years (supporting documents should be submitted)
    d) Copy of GST of the company/firm
    e) Copy of PAN of the company/firm

24. The full & final payment shall be made after SITC [supply, installation, testing & commissioning] for the Renovation and Up-Gradation of Network Infrastructure (LAN & WiFI), submission of bill in triplicate and satisfactory report submitted by the concerned NIFT Official(s). TDS etc., if any, will be deducted during payment.

25. The successful bidder shall deposit the Security Deposit of 5% of the ordered value through DD/Bank Guarantee in favour of NIFT Kolkata within two weeks from the date of receiving of Work Order. No interest will be paid on this deposit which will be refunded after two months on completion of warranty period of the delivered items and after adjusting dues, if any.

26. As per NIFT policy, payments and receipts of Government and Semi Government Agencies would be rounded off to the next higher rupee and in other cases the rounding off will be to nearest i.e. paise 50 or above will be rounded off to the next higher rupee and paise less than 50 will be ignored.

27. The supplier shall ensure that he himself or his authorized representative is available for proper handing over the supplies/consignments at NIFT Kolkata Centre.

28. For the specification of goods refer Annexure 'IV'.

29. Delivery is required to be completed within 6-8 weeks from the date of receiving of supply order. In case of delay in supply, a penalty of 0.1% of the Order Value will be imposed per day beyond the stipulated period of supply.

30. Items / goods supplied and installed should be New and Unused.

31. The vendor should have the qualified engineers/ staff to attend to After Sales Service at NIFT Kolkata Centre where the machines are to be supplied and installed during the warranty period.

32. Tender of branded/ reputed make shall only be considered. Assembled or locally manufactured items shall not be entertained.

33. For any imported machine(s) the vendor/agent should have an authorization certificate from the Manufacturing Company and should enclose a copy of the same with the Technical bid.

34. The pre-inspection /post inspection of the machines may be undertaken by NIFT Kolkata and the machines shall be accepted only after the machines are certified 'OK' by the Inspecting Engineer/Body.

35. The installation of the equipment's / machineries with proper demonstration shall be the responsibility of the vendor and it should be certified as in working condition by the consignee after the installation.

36. Comprehensive warranty: The built-in warranty should be of at least of three year or as per OEM whichever is higher.

37. Support/Service and Scope of Work: After Installation & Commissioning, onsite Support & Service to be provided as and when required for any modification and configuring / up-gradation, shifting of Active and Passive components and changing of RJ45 during the warranty period [i.e. three year or as per OEM whichever is higher]. Call should be attended within 2-3 hours from the time of logging of call for uninterrupted service at NIFT, Kolkata Campus/Girls' Hostel failing which penalty will be imposed on the Security Deposit/Bank Guarantee and deduction will be made, either part or full, as may be decided by the Competent Authority of NIFT, Kolkata. Work should be executed under supervision of concerned NIFT officials and as per NIFT layout/Design.

38. For the said items, the Insurance Coverage, if any, shall be at the cost of the vendor & his responsibility shall be up to 'FOR Destination' i.e. NIFT Kolkata Centre.

39. Tenderer must sign along with company seal on each page of the tender document as a token of acceptance of tender conditions.

40. Any query/clarification with respect to the tender (T&Cs, etc.) may get cleared prior to submission of bid; concerned NIFT official(s) may be contacted in this regard in between 10.00 am to 5.00 pm on any working day with prior appointment (033-23357546). However, NIFT will not entertain or clarify any such query during post bid.

41. All disputes are subject to Kolkata Jurisdiction only.

NIFT reserves the right to accept or reject any or all the tenders in part or whole or may cancel the tender at its sole discretion without assigning any reason whatsoever and decision of NIFT in this regard shall be final and binding. No further correspondence in this regard will be entertained.

Annexure- I

(TENDERER TO FILL UP THIS PAGE)

1. a. Name of the tenderer / organization ……..

   b. Name of the proprietor/partner(s)……

   c. Date of Establishment: ……

   d. Please specify as to whether Tenderer is sole proprietor/ Partnership firm/ Private or Limited Company……..

2. a. Address (Office):

   b. Telephone No.:
   c. Mobile No.:
   d. Email Id.:

3. List of reputed clients:

Sl. No.	Client's Name	Contact Person	Contact number (with email-id, if any)	Remarks, if any
1				
2				
3				

4. Furnish copies of the following documents:
(i) Current Trade License:
(ii) Copy of PAN [in the name of firm/agency or proprietor]:
(iii) GST Registration Certificate:
(iv) Authorization Certificate of OEM:
(v) Document supporting yearly turnover

5. DD [enclosed] details:

1. DD no._____, dtd._____, amt._____, bank_____ [Tender Cost, if downloaded]

2. DD no._____, dtd._____, amt._____, bank_____ [EMD]

1. Tenderer should submit the entire set of tender papers duly signed while dropping the tender.
2. Additional paper(s) to furnish the above information may be used.

Signature of the tenderer with date & seal

ANNEXURE – II

TECHNICAL BID
[Renovation and Up-Gradation of Network Infrastructure (LAN & WiFi)]

Sl. No.	Particulars	Mention 'Yes' or 'No'
01	Whether 'Technical' & Financial bids submitted separately and the respective envelopes superscribed properly.	
02	Whether demand Draft of Rs.500/- (Rupees Five Hundred Only) favouring NIFT Kolkata is enclosed as tender cost (if tender document is downloaded from website/not purchased).	
03	Whether Demand Draft of Rs.1,20,000/- (Rupees One Lakh Twenty Thousand Only) in favour of NIFT, KOLKATA is enclosed as EMD with the Technical Bid submitted.	
04	Whether capable and agreed to submit 5% of the order value as Security Deposit, if purchase order is awarded.	
05	Whether Trade License for this kind of jobs enclosed	
06	Whether copy of GST Registration Certificate enclosed	
07	Whether Copy of PAN enclosed	
08	Whether price quoted as per the required specification mentioned in the Annexure 'IV' and inclusive of all taxes & other charges with delivery upto NIFT, Kolkata	
09	Whether relevant document submitted showing Annual Turnover for the last two years [i.e. FY: 2014-2015; 2015-2016] is not less than Rs.10.00 Crore per year [Please attach relevant documents (ITR, P&L, audited report from authorized Chartered Accountant, etc.) as a proof]	
10	Whether Copy of Income Tax Return for the last 2 years submitted [Assessment year 2013-14; 2014-15]	
11	Whether agreed to abide by all the terms & conditions of this tender	
12	Whether all DDs, Annexure-I, II & III duly filled, are enclosed with this Technical Bid and Annexure-IV, duly filled, with Financial Bid	

Part-A, MAIN CAMPUS- RENOVATION AND UP-GRADATION OF NETWORK INFRASTRUCTURE (LAN & WiFi)

Part A-BOQ FOR MAIN CAMPUS					
A) Active Components:					
SL	Item Type	Make & Model	Description	Qty./As per Actual	UoM
1	Core Switch		24 Port 10/100/1000Mbps L3 Managed Switch with at least 2x (10G)SFP+ slots & 2 (two) nos. of SM 1G transceiver module loaded + 3 Years Warranty Support	1	No.
2	Access Switch - PoE		24 Port 10/100/1000Mbps L2 Managed POE Switch with 2 x (10G) SFP+ slots loaded with at least 1 (one) no. of SM 1G transceiver module + 3 Years Warranty Support	10	Nos.
	Access Switch - NON-PoE		24 Port 10/100/1000Mbps L2 Managed Switch with 2 x (10G) SFP+ slots loaded with at least 1 (one) no. of SM 1G transceiver module + 3 Years Warranty Support	13	Nos.
3	Wireless Lan Controller		Wireless LAN Controller(WLC) with minimum 150+ AP support + 3 Years warranty	1	No.
4	AP License		Single AP adder License for WLC	33	Nos.

5	Indoor Access Point		Dual-band 802.11ac Indoor Wireless Access Point with Mounting Bracket + 3 Years warranty	32	Nos.
6	Outdoor Access Point		Dual-band 802.11ac Outdoor Wireless Access Point with Mounting Bracket + 3 Years warranty	1	Nos.

Passive Components:

SL	Item Type	Make & Model	Description	Qty	UoM
1	Optical Fiber Cabel		6 Core Single Mode Outdoor OFC	700	Mtr.
2	Fiber Patch Panel (LIU)		24 Port fully loaded SM with SC Adapter & SC SM Pigtails	2	Nos.
			12 Port fully loaded SM with SC Adapter & SC SM Pigtails	8	Nos.
3	Fiber Patch Cord		Single Mode SC-LC 2-Mtr. OFC Patch Cord	22	Nos.
4	UTP Cable		CAT6 23AWG 4-Pair UTP Cable	45	Boxes
5	Information Outlet		CAT6 I/O with Face Plate and SMB	420	Nos.
6	Patch Pannel		24 Port fully loaded CAT6 Patch Pannel	24	Nos.
7	UTP Patch Cord		1 Mtr. CAT6 UTP Patch Cord	480	Nos.
			2 Mtr. CAT6 UTP Patch Cord	430	Nos.
8	RJ45 Connecter		RJ-45 Connector for Cat6 Cable crimping.	1	Box
9	Network Rack		9U Wall Mount Rack with standard accessories.	7	Nos.
10	PVC Conduit		PVC Casing/Capping or PVC Pipe for laying of UTP Cable as per site requirement.	3500	Mtr.
11	HDPE Pipe		HDPE Pipe for Outdoor OFC laying	200	Mtr.

Details Specification of Renovation and Up-Gradation of Network Infrastructure (LAN & WiFi)

General Requirements:

a. All active components including LAN & Wi-Fi should be from single OEM.
b. OEM must have ISO 9001:2008, ISO 14001:2004 certified
c. Both UTP & Fiber components must be from the same OEM

MINIMUM DESIRED TECHNICAL SPECIFICATIONS OF ACTIVE ITEMS

24 Port L3 Core Switch

S/N	Features	Compliance (Yes/No/Equivalent or Higher)
	General	
1	The Switch should have minimum 24 x 10/100/1000 base-T Ports and 4 x 1G SFP ports populated with 2 x 1000 Base-LX modules.	
2	The switch should have the option to support 2x 10G SFP+ port with a module upgrade.	
3	Should have internal Redundant Power supply	
4	Support for Configuration and image rollback	
5	IPv4 & IPv6 Layer 3 forwarding in hardware	
6	Should have 4GB DRAM & 2GB Flash memory	
7	Switch OEM should be in the Gartner's/IDC Leaders quadrant for Wired and Wireless LAN Access Infrastructure	
	Performance	
8	Should have stacking facility with dedicated stacking port and support minimum total stacking bandwidth of 360 Gbps. Should support stacking of eight switches into a virtual switch.	
9	Should have 80Gbps Switching capacity & 40 Mpps forwarding rate	
10	Fully non-blocking backplane and wire-speed throughput with minimal latency	
11	MAC Address table : 30000	
12	Should support 24000 routes	
	Layer 3 feature	

13	Basic IP unicast routing protocols (static, RIPv1, and RIPv2) should be supported from day 1.	
14	Should have future support for advanced routing support including OSPF, IS-IS, BGP, policy based routing & Multicast routing	
	Layer 2 feature	
15	IEEE 802.1Q VLAN encapsulation. At least 1000 VLANs should be supported. Support for 4000 VLAN IDs.	
16	Support for Voice VLAN which will simplify telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.	
17	administration and troubleshooting.	
18	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.	
19	IEEE 802.1d, 802.1s, 802.1w, 802.3ad standard support from day-1	
20	Link Aggregation Protocol (LACP)	
21	Support for Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.	
22	The Switch should be able to discover the neighboring device giving the details about the platform, IP Address, Link connected through etc., thus helping in troubleshooting connectivity problems.	
23	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.	
24	Support for Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.	
	Network Security Features	
25	Support for mechanisms to improve the network's ability to automatically identify, prevent, and respond to security threats and also to enable the switches to collaborate with third-party solutions for security-policy compliance and enforcement before a host is permitted to access the network. Thus preventing the spread of Viruses & worms.	
26	IEEE 802.1x to allow dynamic, port-based security, providing user authentication.	
27	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.	
28	Support for SSHv2 and SNMPv3.	
29	Support for Network Admission Control, IP source Guard, MAC Limiting	
30	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
31	MAC address notification to allow administrators to be notified of users added to or removed from the network.	
32	Dynamic ARP Inspection or equivalent which can ensure user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	
33	DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addresses. This can be used to prevent attacks that attempt to poison the DHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.	
34	Port security to secure the access to an access or trunk port based on MAC address.	
35	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.	

36	Spanning tree feature to shut down Spanning Tree Protocol enabled interfaces when BPDU's are received to avoid accidental topology loops.	
37	Security ACL entries – At least 1000.	
	Quality of Service (QoS) & Control	
38	Standard 802.1p CoS and DSCP	
39	Control- and Data-plane QoS ACLs	
40	Eight egress queues per port to enable differentiated management of up to four traffic types across the stack.	
41	Support for congestion avoidance mechanism	
42	Strict priority queuing mechanisms	
43	There should not be any performance penalty for highly granular QoS functions.	
44	Future support for feature which will provide rate limiting based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.	
45	Switch should support at least 1000 aggregate polices.	
46	**Management**	
47	Command Line Interface (CLI) support for configuration & troubleshooting purposes.	
48	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.	
49	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.	
50	FTP/ Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.	
51	Network Timing Protocol (NTP) based on RFC 1305 to provide an accurate and consistent timestamp to all intranet switches.	
52	SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management.	
53	RMON I and II standards	
54	SNMPv1, SNMPv2c, and SNMPv3	
	Certification	
55	The switch should be common criteria EAL4 or NDPP certified.	

24 port PoE Access Switch

S/N	Specification	Compliance (Yes/No/Equivalent or Higher)
	General Features	
56	The switch should have minimum 24 x 10/100/1000 Base-T POE/POE+ Ports & 2 x 10G SFP+ slots populated with 1 x 1000 Base-LX SM Module. The switch should have 360W POE Budget	
57	Future support for Redundant Power supply	
58	Should have fan for proper cooling.	
	Performance	
59	At least 176 Gbps switching bandwidth	
60	Forwarding rate – At least 90 Mpps.	
61	Configurable at least 16000 MAC addresses	
62	The switch should support stacking with 80 Gbps Stacking bandwidth to stack upto 8 switches into a single virtual switch. Stacking is not required from day 1, but stacking should be supported on the proposed switch model.	

63	DRAM 512 MB and 128 MB Flash	
	Layer-2 Features	
64	IEEE 802.1Q VLAN encapsulation. At least 1000 VLANs should be supported. Support for 4000 VLAN IDs.	
65	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.	
66	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.	
67	Spanning-tree Enhancements for fast convergence	
68	IEEE 802.1d, 802.1s, 802.1w, 802.3ad, 802.3at, 802.3af	
69	Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.	
70	IGMPv3. Support for at least 1000 IGMP Groups. IGMP filtering.	
71	Link Aggregation Protocol (LACP)	
72	Support for UDLD (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.	
73	The Switch should be able to discover 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.	
74	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.	
75	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.	
76	Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.	
	Network Security Features	
77	Support for mechanisms to improve the network's ability to automatically identify, prevent, and respond to security threats and also to enable the switches to collaborate with third-party solutions for security-policy compliance and enforcement before a host is permitted to access the network. Thus preventing the spread of Viruses & worms.	
78	IEEE 802.1x to allow dynamic, port-based security, providing user authentication.	
79	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.	
80	SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.	
81	Bidirectional data support on the Mirrored port to allow the intrusion detection system (IDS) to take action when an intruder is detected.	
82	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
83	MAC address notification to allow administrators to be notified of users added to or removed from the network.	
84	DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addresses. This can be used to prevent attacks that attempt to poison the DHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.	
85	Port security to secure the access to an access or trunk port based on MAC address.	
86	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.	
87	BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU's are received to avoid accidental topology loops.	
88	Should support 500 IPv4 ACL entries, 500 IPv6 ACL entries,	
	Quality of Service (QoS) & Multicast	

89	Standard 802.1p CoS and DSCP	
90	Control- and Data-plane QoS ACLs, Cross-stack QoS	
91	Up to eight egress queues per port	
92	Strict priority queuing mechanisms	
93	There should not be any performance penalty for highly granular QoS functions.	
94	Committed information rate (CIR) function to provide bandwidth in increments of 8 Kbps	
95	Rate limiting should be provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.	
96	Flow-based rate limiting and up to 200 aggregate or individual policers per port	
97	Shaped Round Robin (SRR) scheduling and Weighted Tail Drop (WTD) congestion avoidance.	
98	2000 IPv4 & IPv6 Unicast Routes	
99	1000 IPv4 Multicast Groups, 1000 IPv6 Multicast Groups	
	Management	
100	Superior manageability Features	
101	Command Line Interface (CLI) support for configuration & troubleshooting purposes.	
102	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.	
103	Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.	
104	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.	
105	FTP/ Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.	
106	Network Timing Protocol (NTP) based on RFC 1305 to provide an accurate and consistent timestamp to all intranet switches.	
107	SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management.	
108	RMON I and II standards	
	Certification:	
109	The switch should be Common Criteria EAL4 or NDPP certified and IPv6 Ready Logo certified (The supporting URL and certification link need to be attached with the Bid)	

24 port Non-PoE Access Switch

S/N	Features	Compliance (Yes/No/Equivalent or Higher)
	General Features	
110	The switch should have minimum 24 x 10/100/1000 Base-T Ports & 2 x 10G SFP+ slots populated with 1 x 1000 Base-LX SM Module.	
111	Future support for Redundant Power supply	
112	Should have fan for proper cooling.	
	Performance	
113	At least 176 Gbps switching bandwidth	
114	Forwarding rate – At least 90 Mpps.	

115	Configurable at least 16000 MAC addresses	
116	The switch should support stacking with 80 Gbps Stacking bandwidth to stack upto 8 switches into a single virtual switch. Stacking is not required from day 1, but stacking should be supported on the proposed switch model.	
117	DRAM 512 MB and 128 MB Flash	
	Layer-2 Features	
118	IEEE 802.1Q VLAN encapsulation. At least 1000 VLANs should be supported. Support for 4000 VLAN IDs.	
119	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.	
120	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.	
121	Spanning-tree Enhancements for fast convergence	
122	IEEE 802.1d, 802.1s, 802.1w, 802.3ad,	
123	Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.	
124	IGMPv3. Support for at least 1000 IGMP Groups. IGMP filtering.	
125	Link Aggregation Protocol (LACP)	
126	Support for UDLD (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.	
127	The Switch should be able to discover 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.	
128	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.	
129	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.	
130	Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.	
	Network Security Features	
131	Support for mechanisms to improve the network's ability to automatically identify, prevent, and respond to security threats and also to enable the switches to collaborate with third-party solutions for security-policy compliance and enforcement before a host is permitted to access the network. Thus preventing the spread of Viruses & worms.	
132	IEEE 802.1x to allow dynamic, port-based security, providing user authentication.	
133	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.	
134	SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.	
135	Bidirectional data support on the Mirrored port to allow the intrusion detection system (IDS) to take action when an intruder is detected.	

136	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
137	MAC address notification to allow administrators to be notified of users added to or removed from the network.	
138	DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addresses. This can be used to prevent attacks that attempt to poison the DHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.	
139	Port security to secure the access to an access or trunk port based on MAC address.	
140	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.	
141	BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU's are received to avoid accidental topology loops.	
142	Should support 500 IPv4 ACL entries, 500 IPv6 ACL entries,	
	Quality of Service (QoS) & Multicast	
143	Standard 802.1p CoS and DSCP	
144	Control- and Data-plane QoS ACLs, Cross-stack QoS	
145	Up to eight egress queues per port	
146	Strict priority queuing mechanisms	
147	There should not be any performance penalty for highly granular QoS functions.	
148	Committed information rate (CIR) function to provide bandwidth in increments of 8 Kbps	
149	Rate limiting should be provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.	
150	Flow-based rate limiting and up to 200 aggregate or individual policers per port	
151	Shaped Round Robin (SRR) scheduling and Weighted Tail Drop (WTD) congestion avoidance.	
152	2000 IPv4 & IPv6 Unicast Routes	
153	1000 IPv4 Multicast Groups, 1000 IPv6 Multicast Groups	
	Management	
154	Superior manageability Features	
155	Command Line Interface (CLI) support for configuration & troubleshooting purposes.	
156	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.	
157	Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.	
158	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.	
159	FTP/ Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.	
160	Network Timing Protocol (NTP) based on RFC 1305 to provide an accurate and consistent timestamp to all intranet switches.	

161	SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management.	
162	RMON I and II standards	
	Certification:	
163	The switch should be Common Criteria EAL4 or NDPP certified and IPv6 Ready Logo certified (The supporting URL and certification link need to be attached with the Bid)	

Wireless Controller Specifications:-

S/N	Features	Compliance (Yes/No/Equivalent or Higher)
1	**Hardware Specifications**	
2	Must be compliant with IEEE CAPWAP or equivalent for controller-based WLANs.	
3	Should have at least 4 x 1G Baste-T ports.	
4	Should support both centralized as well as distributed traffic forwarding architecture with L3 roaming support from day 1. Should have IPv6 support from day one.	
5	Controller should have hot-swappable internal redundant power supplies.	
6	Controller should support minimum 3000 concurrent devices.	
7	WLAN controller should support 35 Access points from day 1. It should be scalable to support up to 150 Access Points without any hardware change.	
8	Should be rack-mountable. Required accessories for rack mounting to be provided.	
9	WLAN controller should provide Application visibility with both traffic forwarding mode i.e when traffic coming to controller and when traffic moving locally from Ap to connected access switch. Admin should have option to create policies to allow or deny access based on applications.	
10	WLC should support AP License Migration from one WLC to another	
11	**S**hould support minimum 4000 VLANs	
12	WLAN controller should support 802.11ac wave 2	
13	the controller should have overall throughput of 4Gbps	
14	**Wireless Controller Features**	
15	Must support stateful switchover between active and standby controller in a sub second time frame.	
16	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients	
17	WLC should support guest-access functionality for IPv6 clients.	
18	Should support IEEE 802.1p priority tag.	
19	Should ensure WLAN reliability by proactively determining and adjusting to changing RF conditions.	
20	Should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments.	
21	Should support automatic radio channel adjustments for intelligent channel switching and real-time interference detection.	
22	Should support client load balancing to balance the number of clients across multiple APs to optimize AP and client throughput.	
23	Should support policy based forwarding to classify data traffic based on ACLs	
24	WLC should support PMIPv6 and EoGRE tunnels on northbound interface	
25	Should support flexible DFS to prevent additional 20/40 Mhz channels from going unused	

26	Should support dynamic bandwidth selection among 20Mhz, 40 Mhz and 80Mhz channels, ensuring one access point on 20Mhz and another on 80 Mhz channel connected on the same controller at same WLAN group.	
27	Should support minimum 500 WLANs	
28	Should support dynamic VLAN assignment	
29	Should support Hot Spot 2.0	
30	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.	
31	Should able to do dynamic channel bonding based on interference detected on particular channel.	
32	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.	
33	Must support RF Management with 40 MHz and 80 Mhz channels with 802.11n & 802.11ac	
34	Should provide visibility to Network airtime in order to set the airtime policy enforcement	
35	Must support dynamic Airtime allocation on per WLAN, per AP, Per AP group basis.	
36	Must be able to restrict the number of logins per user.	
37	Proposed solution should have support for policy based automation for wired and wireless and the proposed wireless solution to be seamlessly integrated with software driven architecture which can provide network automation, assurance & security	
38	**Security**	
39	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.	
40	WLC should support web based authentication in different traffic forwarding modes i.e Central switching and Local switching when traffic move locally from AP to connected switch.	
41	Should support port-based and SSID-based IEEE 802.1X authentication.	
42	Should support MAC authentication to provide simple authentication based on a user's MAC address.	
43	WLC should be able to exclude clients based on excessive/multiple authentication failure.	
44	Shall support AES or TKIP encryption to secure the data integrity of wireless traffic	
45	Shall support the ability to classify over 20 different types of interference with in 5 to 30 seconds.	
46	Shall able to provide an air quality index for ensuring the better performance	
47	Shall able to provide real time chart showing interference per access point on per radio and per-channel basis.	
48	Should support AP location-based user access to control the locations where a wireless user can access the network	
49	Should support Public Key Infrastructure (PKI) to control access	
50	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.	
51	WLC Shall support WIDS/WIPS, and spectral analysis from day 1.	
52	WLC should detect if someone connect a Rogue Access Point in network and able to take appropriate action to contain rogue Access point.	
53	In case of Access point connected in remote locations over WAN, containment should happen even if WAN is down.	
54	WLC should detect and protect an Ad-hoc connection when a connected user forming a network with other system without an AP or try enabling bridging between two interface	
55	WLC should detect if a user try to impersonate a management frame.	
56	WLC should detect and take appropriate containment action if a smartphone user using tethering to connect other device.	
57	WLC should detect and protect if a user try to spoof mac address of valid client or AP for unauthorized access/authentication.	
58	WLC should detect if a user trying to do internet sharing through a valid system to an	

	unauthorized device.	
59	**Management & QoS**	
60	Should support SNMPv3, SSHv2 and SSL for secure management.	
61	Should support encrypted mechanism to securely upload/download software image to and from Wireless controller.	
62	Should provide visibility between a wired and wireless network using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and sFlow/equivalent.	
63	Should support AP Plug and Play (PnP) deployment with zero-configuration capability	
64	Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group	
65	Should support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation	
66	Should have a suitable serial console port.	
67	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS	
68	Controller should support deep packet inspection for all user traffic across Layer 4-7 network to analyses information about applications usage, peak network usage times for all access points from day one with different traffic forwarding modes i.e central switching with WLC and local switching when traffic move locally from AP to connected switch.	
69	Should be able to do application visibility for application running behind HTTP proxy.	
70	Support profiling of wireless devices based on known protocols like http and dhcp to identify clients	
71	Should support visibility and control based on the type of applications	

Indoor Wireless Access Point 802.11b/g/n/802.11ac

S/N	Features	Compliance (Yes/No/Equivalent or Higher)
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave 2.	
2	An access point must include a standard OEM provided Mounting brackets for mounting on Celling or Roof top.	
3	Access point must support spectrum intelligence across 20-, 40-, and 80-MHz-wide channels to combat performance problems due to wireless interference.	
4	Access point should have console port	
5	Must have 3dBi 2.4Ghz Antenna & 5 dBi 5.0Ghz Antenna	
6	Must support 3x3 spatial streams for both 802.11ac and 802.11n client	
7	Access point must support a minimum of 1.9 Gbps user throughput including both the radios	
8	Must support minimum of 22dbm of transmit power in both 2.4Ghz and 5Ghz radios. And should follow the WPC norms.	
9	Should support Multiuser MIMO (MU-MIMO)	
10	Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.	
11	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	
12	Must have -100 dB or better Receiver Sensitivity.	
13	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.	
14	Must support Management Frame Protection.	

15	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).	
16	Access Points must support Hardware-based encrypted user data and management traffic between controller and Access point for better security.	
17	Must support the ability to serve clients and monitor the RF environment concurrently.	
18	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.	
19	Should support mesh capabilities for temporary connectivity in areas where no Ethernet cabling.	
20	Mesh support should support QoS for voice over wireless.	
21	Must be plenum-rated (UL2043).	
22	Must support 16 WLANs per AP for SSID deployment flexibility.	
23	Must continue serving clients when WAN link to controller is back up again, should not reboot before joining	
24	The APs must support centralized wireless mode with the use of a controller, but the APs must also support operation in autonomous mode without the presence of any controller, when needed	
25	When operated in remote AP mode, the AP must not disconnect any clients when the connection to the controller fails or in the case the failed connection has been restored again.	
26	When operated in remote AP mode, the AP must be able to authenticate new users with local radius server directly at the AP itself in case of link failure to controller.	
27	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.	
28	Must support Power over Ethernet, local power (DC Power), and power injectors.	
29	802.11e and WMM	
30	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level	
31	Must support QoS and Video Call Admission Control capabilities.	
32	Access Point should 802.11 DFS certified	

Outdoor WIRELESS ACCESS POINT 802.11b/g/n/802.11ac

Sr. No.	Specification	Compliance (Yes/No/Equivalent or Higher)
1	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.	
2	AP should support dual band antenna ports.	
3	Must support a variety of antenna options. (Omni and directional)	
4	Must have -88 dB or better Receiver Sensitivity.	
5	Must support 2X2 multiple-input multiple-output (MIMO) with two spatial streams	
6	Must support 802.11ac, Wave 2 and backward compatible with 802.11n standards	
7	Must support data rates up to 1.3 Gbps on 5Ghz radio.	
8	Must support 80 MHz wide channels in 5 GHz.	
9	Must support WAP enforced load-balance between 2.4Ghz and 5Ghz band.	
10	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data	
11	Must support upto 28dbm or higher of transmit power	
12	Access point should 802.11ac, 802.11n and 802.11a/b/g Beamforming	
13	The Wireless Backhaul/Mesh shall operate in 5Ghz	

14	Support Encrypted and authenticated connectivity between all backhaul components	
15	Access point should have multiple wired uplink interfaces including 10/100/1000BASE-T Ethernet autosensing (RJ-45) and a build-in SFP port	
16	Wireless AP should support beamforming technology to improve downlink performance of all mobile devices, including one-, two-, and three-spatial-stream devices on 802.11ac without taking the inputs from client.	
17	Wireless AP Should able to detect and classify non-Wi-Fi wireless transmissions.	
18	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data.	
19	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	
20	Access point shall support powering from AC /DC/ UPOE.	
21	Access point shall support pole, wall and Cable strand mounting options.	
22	The equipment shall support up to 100 MPH sustained winds & 140 MPH wind gusts.	
23	The Access point shall be IP67 and NEMA rated	
24	The Access point shall support operating temperature of -40 to 65°C	
25	The Access point shall support Storage temperature of -50 to 70°C	
26	802.11e and WMM	
27	WiFi Alliance Certification for WMM and WMM power save	
28	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level	
29	Must support QoS and Video Call Admission Control capabilities.	
30	Must support the ability to serve clients and monitor the RF environment concurrently.	
31	Must support Spectrum analysis including @ 80 MHz	
32	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.	
33	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.	
34	Should have and option of configuring all the antennae port via software to run all on dual band or any single band configuration.	
35	Must support 16 WLANs per AP for BSSID deployment flexibility.	
36	Must support telnet and SSH login to APs directly for troubleshooting flexibility.	

MINIMUM DESIRED TECHNICAL SPECIFICATIONS OF PASSIVE ITEMS

SM Fiber optic Cable

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Cable Type	**Single Mode, OS2, Armored, Loose Tube – Unitube, CSTA, Jelly Filled**	
Fiber type	9/ 125, Telcordia's GR-20 and ITU-T 652.D Compliance, **OS2**	
No. of cores	6/12/24	
Cable Construction	BELLCORE GR 20 / IEC 794-1	
Nominal Diameter	Not less than 09mm	
Cable Sheath Thickness	Not less than 2mm	
Water blocking compound	Cable must have Water blocking compound	
Strength Member	Should have FRP strength member	

Cable outer jacket Specification	Must have Dielectric and Metallic Sheath Cable. Cable must be direct buried	
Attenuation :		
@1310nm	< = 0.33 dB/Km	
@1550nm	< = 0.19 dB/Km	
Coating / Cladding non-circularity	<= 12 microns	
Zero Dispersion Slope	<= 0.092 ps / sqnm-km	
Max (chromatic) dispersion	<5.3 ps/nm-km @1270-1340 nm <3.5 ps/nm-km @1285-1330 nm <185 ps/nm-km @1550 nm	
Fiber core	UL Listed	
Tensile rating	Not less than 1000N	
Maximum Crush resistance	Not less than 44N/mm	
Operating Temperature	-30 Degree C to +70 Degree C	
Storage Temperature	-40°C to + 75°C	
Micro bending coating	CPC coating	
Armor	Corrugated Steel tape Armor	
Color	Black	
Inner jacket	High density polyethylene	
Outer jacket	High density polyethylene, anti - termite, anti - rodent suitable for direct burial application.	
Coating	Polymer Coating over Corrugated Steel tape	
Secondary Buffer Material	Jelly filled Unitube.	
Min Bend	20 X Outer Diameter	
Weight	90 Kg/Km (Approx.)	
Test (Must pass)	IEC794-1-E1 , IEC794-1-E2 , IEC794-1-E3 , IEC794-1-E4 , EIA-455-104 , IEC794-1-E7 , IEC794-1-E10 , IEC794-1-F1 , IEC794-1-F3 and IEC794-1-F5	
Marking	Identification marking at regular intervals of 1 meter	
SM Fiber type	Silica glass	
Qualifies	EIA/TIA 568B and ISO/IEC 11801	
	ICEA-640	
	UL-94V-O	
Complies	ANSI/TIA 568.C.0	
Approval	UL Listed Fiber	
RoHS	RoHS Compliant	
Length of cable drum	(+/-) 4000 Mtrs	

12/24 Port SM Fiber Optic LIU

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Fiber optic patch panel	**19-inch, Rack Mount Fiber optic patch panel**	
Height	1 U, 1.75 inches	
No. of fibers	6/12/24	
Material	Complete Aluminium Alloy housing, fully powder coated	
	Splice tray and cable spools to be included from day one without any additional cost	
	Fully cushioned splice holder containing grooves for fixing splice protective sleeves	
No. of OSP Cables for termination	Minimum 2	
Grounding	2 Nos. of earthing lugs, pre-loaded	
Cable Management rings	Front and rear cable management rings, pre-loaded	
No. of 6-port adapter plates	4 max	
RoHS	RoHS Compliant	
Fiber Optic adapter plate	**6-port, SC-Style, SM**	
Attenuation	Max of 0.75 dB per mated pair	

Insertion Loss	< 0.3 dB max	
Durability (1000 Mattings)	< 0.2 dB max	
Operation Temp.	-40°C to 80°C	
Material Ferrule	Zirconia (for SM)	
ROHS	RoHS Compliant	
UL	UL Listed	
IEC	IEC-874	
Compliant	EIA/TIA 568-C.0	
ISO/IEC Certificate	ISO/IEC 11081	
RoHS	RoHS verified.	
Product Features & Compliances	Zirconia or Phosphor Bronze Sleeve	
Compliant	As per ISO/IEC 11081	
UL	UL Listed	
RoHS	RoHS Compliant	
Product Compliance	IEC-874	
SM Pigtails	Should support multiple applications including CWDM.	
	Available 1.6mm cordage making	
	Different color-coding for easy Identification.	
	Should support Pull proof connector design	
	Outside Diameter (Simplex): 1.6mm x 3.0mm	
	Outside Diameter (Duplex): 1.6mm x 3.0mm	
	Minimum Cable Retention Strength: 1.6mm; 11.24 lbs (50N)	
	Product Must have RoHS Compliant	
	CPC coating for superior micro bend and environmental performance	

SM Fiber Optic Patch Cord LC-SC TYPE.

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
F.O Patch Cords	**Patch Cord / SM patch cord LC-SC TYPE**	
Type	1.6mm or 3mm simplex or Duplex Zipcord.	
Outside Diameter	(Simplex): 1.6mm x 3.0mm (Duplex): 1.6mm x 3.3mm	
Minimum Cable Retention Strength	1.6mm: 11.24 lbs (50 N)	
Insertion Loss	Less than 0.3 dB for SM	
Fiber Glass Technology	Patch Cords must be Clear Curve Fiber	
Micro bending coating	CPC coating	
RoHS	RoHS Compliant	

UTP Cable - Cat6

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2		
Material:		
Conductors	23 AWG solid bare copper or better	
Insulation	Polyethylene	
Jacket	Sheath Fire retardant PVC Compound (FRPVC) Flame Rating : 60 deg. C As per UL 1685 CM/CMR	
Pair Separator	Cross-member fluted member	
Approvals	UL tested for TIA/EIA-568C.2	
	ETL verified to Cat 6	
	Zero Bit Error verified by ETL.	
Operating temperature	-20 Deg. C to +60 Deg. C	
Frequency tested up to	Minimum 600 MHz	

Packing	Box of 305 meters	
Delay Skew	35ns MAX.	
Impedance	100 Ohms + / - 6 ohms	
Performance characteristics to be provided along with bid	Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR	
Attenuation	22.8dB/100m at 250MHz	
	29.4dB/100m at 400MHz	
	39dB/100m at 600MHz	

Information Outlet- Cat6

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Type	**Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2**	
Durability		
Modular Jack	750 mating cycles	
Wire terminal	200 termination cycles	
Accessories	Strain relief and bend-limiting boot for cable	
	It should have a Dust cover to cover the keystone..	
Approval	UL	
Housing	Polyphenylene oxide, 94V-0 rated	
Wiring blocks	Polycarbonate, 94V-0 rated	
Jack contacts	Phosphorous bronze, plated with 1.27micro-meter thick gold	
Approvals	UL , ETL and 3P	
Performance Characteristics to be provided with bid	Attenuation, NEXT, PS NEXT, FEXT and Return Loss	
Material	Spring Contact: 50m" goldover 100m" nickel	
	ROHS compliant	
FacePlate	**1-port, White surface box**	
Material	ABS / UL 94 V-0	
No. of ports	One / two	
	High Impact Plastic Body ABS FR Grade 86 x 86 mm	
	Flush mountable or surface mountable with a back mount frame	

24Port Cat-6 UTP Patch Pannel

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Type	**24-port, Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2**	
Ports	24	
Port arrangement	Keystone type. Ports must be individually replaceable.	
Category	Category 6	
Circuit Identification Scheme	Icons on each of 24-ports	
Port Identification	9mm or 12mm Labels on each of 24-ports (to be included in supply)	
Height	1 U (1.75 inches)	
Durability		
Modular Jack	750 mating cycles	
Wire terminal (110 block)	200 termination cycles	
Accessories	Strain relief and bend limiting boot for cable	
Materials	ROHS compliant	
Housing	Polyphenylene oxide, 94V-0 rated	
Wiring blocks	Polycarbonate, 94V-0 rated, Spring Contact: Phosphor bronze 50" gold	
Jack contacts	Phosphorous bronze	

Panel	Black, powder coated steel	
Approvals	UL , ETL	
Termination Pattern	TIA / EIA 568 A and B;	
Performance Characteristics to be provided along with bid	Attenuation, NEXT, PS NEXT, FEXT and Return Loss	

UTP Patch Cord- Cat6

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Type	**Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2**	
Conductor	24-26 AWG **stranded** copper.	
Length	1 /2/3 meter	
Plug Protection	Matching colored snag-less, boot to maintain bend radius	
Warranty	25-year component warranty	
Category	Category 6 Plug	
Housing	Clear polycarbonate	
Terminals	Phosphor Bronze with gold plating , 50 micron'' gold over nickel	
Load bar	PBT polyester	
Jacket	PVC	
Insulation	Flame Retardant Polyethylene	
End point connector	Factory standard connector	
Approvals	UL, ETL	
Material	ROHS compliant	

Network Rack-9U

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Basic Structure	Cabinet should be as per DIN 41494 standards, Basic structure of CRCA Steel (CRCA Should be "IS 513 Gr D" standard) in a welded Rigid construction frame with top, bottom and side frame at least 1.2 mm thickness., It should be able to take load of 40 Kg	
Front Door	Front Glass toughened and tinted, with easy detachable hings. Glass Door with lock – should be easily removable type.	
Side Panel	Fixed Side Panel with top & bottom vented for easy air flow.	
Space	Height - 9U overall height : 475.1mm; Usable Height : 406.1mm	
	Width – It should be 600mmW and 19" mounting should be there	
	Depth – It should be 500mm	
Wall Mounting	Provision for easy wall mounting should be there with appropriate anchor fasteners	
Heat Management	Rack must be provided with one fan directly mounted on the roof top as an exhaust from the cabinet. Fan should be of AC 230V with flow volume of at least 90CFM	
Standard	Rack should conform to DIN41494 standard.	
Cable Management	Rack should be provided with cable management accessories.1U Cable manager	
Powder Coating Details	Thickness Powder Coating of 80 to 100 Microns with scratch resistance properties.	
	To avoid corrosion & rusting : Rack to be powder coated with Nano ceramic pre-treatment process using a zirconium coat,	

Power Management	Rack should have PDU, 19", 6 nos sockets of 5 Amp with Indicator, 5Amp fuse	
Manufacturers Details	1. Manufacturer should have ISO 18001: 2007; ISO 9001-2015 & 14001-2015 Certifications, Certificate needed to be submitted.	
	2. Process of Manufacturing of rack should have ROHS complied.	

Part B, GIRLS HOSTEL - RENOVATION AND UP-GRADATION OF NETWORK INFRASTRUCTURE (LAN & WiFi)

Part B-BOQ FOR GIRLS' HOSTEL

A) Active Components:

SL	Item Type	Make & Model	Description	Qty./As per Actual	UoM
1	24 Access Switch - PoE		24 Port 10/100/1000Mbps L2 Managed POE Switch with 2 x (10G)SFP+ slots + 3 Years Warranty Support	1	Nos.
2	12 Access Switch - PoE		12 Port 10/100/1000Mbps L2 Managed POE Switch with 2 x (10G)SFP+ slots + 3 Years Warranty Support	3	Nos.
3	Wireless Lan Controller		Wireless LAN Controller(WLC) with minimum 150+ AP support + 3 Years warranty	1	No.
4	AP License		Single AP adder License for WLC	34	Nos.
5	Indoor Access Point		Dual-band 802.11ac Indoor Wireless Access Point with Mounting Bracket + 3 Years warranty	33	Nos.
6	Outdoor Access Point		Dual-band 802.11ac Outdoor Wireless Access Point with Mounting Bracket + 3 Years warranty	1	Nos.

Passive Components:

SL	Item Type	Make & Model	Description	Qty	UoM
1	UTP Cable		CAT6 23AWG 4-Pair UTP Cable	2	Boxes
2	UTP Patch Cord		1 Mtr. CAT6 UTP Patch Cord	40	Nos.
3	RJ45 Connecter		RJ-45 Connector for Cat6 Cable crimping.	1	Box
4	PVC Conduit		PVC Casing/Caping or PVC Pipe for laying of UTP Cable as per site requirement.	200	Mtr.

General Requirements:

a. All active components including LAN & Wi-Fi should be from single OEM.
b. OEM must have ISO 9001:2008, ISO 14001:2004 certified.
c. Both UTP & Fiber components must be from the same OEM

MINIMUM DESIRED TECHNICAL SPECIFICATIONS OF ACTIVE ITEMS

24 port PoE Access Switch

S/N	Specification	Compliance (Yes/No/Equivalent or Higher)
	General Features	
1	The switch should have minimum 24 x 10/100/1000 Base-T POE/POE+ Ports & 2 x 10G SFP+ slots. The switch should have 360W POE Budget	

2	Future support for Redundant Power supply	
3	Should have fan for proper cooling.	
	Performance	
4	At least 176 Gbps switching bandwidth	
5	Forwarding rate – At least 90 Mpps.	
6	Configurable at least 16000 MAC addresses	
7	The switch should support stacking with 80 Gbps Stacking bandwidth to stack upto 8 switches into a single virtual switch. Stacking is not required from day 1, but stacking should be supported on the proposed switch model.	
8	DRAM 512 MB and 128 MB Flash	
	Layer-2 Features	
9	IEEE 802.1Q VLAN encapsulation. At least 1000 VLANs should be supported. Support for 4000 VLAN IDs.	
10	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.	
11	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.	
12	Spanning-tree Enhancements for fast convergence	
13	IEEE 802.1d, 802.1s, 802.1w, 802.3ad, 802.3at, 802.3af	
14	Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.	
15	IGMPv3. Support for at least 1000 IGMP Groups. IGMP filtering.	
16	Link Aggregation Protocol (LACP)	
17	Support for UDLD (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.	
18	The Switch should be able to discover 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.	
19	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.	
20	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.	
21	Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.	
	Network Security Features	
22	Support for mechanisms to improve the network's ability to automatically identify, prevent, and respond to security threats and also to enable the switches to collaborate with third-party solutions for security-policy compliance and enforcement before a host is permitted to access the network. Thus preventing the spread of Viruses & worms.	
23	IEEE 802.1x to allow dynamic, port-based security, providing user authentication.	
24	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.	
25	SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.	
26	Bidirectional data support on the Mirrored port to allow the intrusion detection system (IDS) to take action when an intruder is detected.	
27	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
28	MAC address notification to allow administrators to be notified of users added to or removed from the network.	

29	DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addresses. This can be used to prevent attacks that attempt to poison the DHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.	
30	Port security to secure the access to an access or trunk port based on MAC address.	
31	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.	
32	BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU's are received to avoid accidental topology loops.	
33	Should support 500 IPv4 ACL entries, 500 IPv6 ACL entries,	
	Quality of Service (QoS) & Multicast	
34	Standard 802.1p CoS and DSCP	
35	Control- and Data-plane QoS ACLs, Cross-stack QoS	
36	Up to eight egress queues per port	
37	Strict priority queuing mechanisms	
38	There should not be any performance penalty for highly granular QoS functions.	
39	Committed information rate (CIR) function to provide bandwidth in increments of 8 Kbps	
40	Rate limiting should be provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.	
41	Flow-based rate limiting and up to 200 aggregate or individual policers per port	
42	Shaped Round Robin (SRR) scheduling and Weighted Tail Drop (WTD) congestion avoidance.	
43	2000 IPv4 & IPv6 Unicast Routes	
44	1000 IPv4 Multicast Groups, 1000 IPv6 Multicast Groups	
	Management	
45	Superior manageability Features	
46	Command Line Interface (CLI) support for configuration & troubleshooting purposes.	
47	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.	
48	Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.	
49	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.	
50	FTP/ Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.	
51	Network Timing Protocol (NTP) based on RFC 1305 to provide an accurate and consistent timestamp to all intranet switches.	
52	SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management.	
53	RMON I and II standards	
	Certification:	
54	The switch should be Common Criteria EAL4 or NDPP certified and IPv6 Ready Logo certified (The supporting URL and certification link need to be attached with the Bid)	

12 Port Layer-2 POE Switch

S/N	Description	Compliance (Yes/No/Equivalent or Higher)
1	**General Features**	
2	The switch should have minimum 12 x 10/100/1000 Base-T POE/POE+ Ports, 2 x 10/100/1000 Base-T ports and 2 x 10G SFP+ ports. 240W POE Budget.	
3	At least 64 Gbps Forwarding bandwidth and 48 Mpps forwarding rate	
4	DRAM : 512MB & Flash : 128MB	
5	Configurable up to 8000 MAC addresses	
6	**Layer-2/3 Features**	
7	IEEE 802.1Q VLAN encapsulation. Upto 1000 VLANs should be supported. Support for 4000 VLAN IDs.	
8	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.	
9	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.	
10	Spanning-tree Enhancements for fast convergence	
11	IEEE 802.1d, 802.1s, 802.1w, 802.3ad, 802.3af, 802.3at	
12	Spanning-tree feature to prevent other edge switches becoming the root bridge.	
13	Link Aggregation Protocol (LACP)	
14	Support for Detection of Unidirectional Links (in case of fibre cut) and to disable them to avoid problems such as spanning-tree loops.	
15	The Switch should be able to discover the neighbouring device of the same vendor giving the details about the platform, IP Address, Link connected through etc., thus helping in troubleshooting connectivity problems.	
16	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.	
17	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.	
18	Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.	
19	Should support static routing & dynamic routings	
20	Future support for Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Policy-Based Routing (PBR), Multicast Routing, and Virtual Routing and Forwarding (VRF) Lite	
21	**Network security features**	
22	Support for mechanisms to improve the network's ability to automatically identify, prevent, and respond to security threats and also to enable the switches to collaborate with third-party solutions for security-policy compliance and enforcement before a host is permitted to access the network. Thus preventing the spread of Viruses & worms.	
23	IEEE 802.1x to allow dynamic, port-based security, providing user authentication. Support for 8MAC Authentication Bypass and web authentication.	
24	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.	
25	SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.	
26	Bidirectional data support on the Mirrored port to allow the intrusion detection system (IDS) to take action when an intruder is detected.	
27	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
28	Support for RFC 1492 - TACACS+, RFC 2463 - ICMP IPv6, RFC 2373 - IPv6 Aggregatable Addrs, RFC 2461 - IPv6 Neighbour Discovery and RFC 2462 - IPv6 Auto configuration	

29	MAC address notification to allow administrators to be notified of users added to or removed from the network.	
30	DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addresses. This can be used to prevent attacks that attempt to poison the DHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.	
31	Dynamic ARP Inspection or equivalent which can ensure user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	
32	IP source guard which can prevent a malicious user from spoofing or taking over another user's IP address	
33	Port security to secure the access to an access or trunk port based on MAC address.	
34	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.	
35	BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU's are received to avoid accidental topology loops.	
36	**Quality of Service (QoS) & Control**	
37	Standard 802.1p CoS and DSCP	
38	Control- and Data-plane QoS ACLs	
39	Four egress queues per port to enable differentiated management of up to four traffic types across the stack.	
40	Weighted tail drop (WTD) to provide congestion avoidance	
41	Strict priority queuing mechanisms	
42	There should not be any performance penalty for highly granular QoS functions.	
43	Rate limiting should be provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.	
44	**Management**	
45	Superior manageability Features	
46	Command Line Interface (CLI) support for configuration & troubleshooting purposes.	
47	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.	
48	Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.	
49	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.	
50	Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.	
51	Network Timing Protocol (RFC 1305) to provide an accurate and consistent timestamp to all intranet switches.	
52	SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management.	
53	RMON I and II standards	
54	**Certification**	
55	The switch should be Common Criteria EAL4 or NDPP certified.	

Wireless Controller Specifications:-

S/N	Features	Compliance (Yes/No/Equivalent or Higher)
1	**Hardware Specifications**	
2	Must be compliant with IEEE CAPWAP or equivalent for controller-based WLANs.	

3	Should have at least 4 x 1G Baste-T ports.	
4	Should support both centralized as well as distributed traffic forwarding architecture with L3 roaming support from day 1. Should have IPv6 support from day one.	
5	Controller should have hot-swappable internal redundant power supplies.	
6	Controller should support minimum 3000 concurrent devices.	
7	WLAN controller should support 35 Access points from day 1. It should be scalable to support upto 150 Access Points without any hardware change.	
8	Should be rack-mountable. Required accessories for rack mounting to be provided.	
9	WLAN controller should provide Application visibility with both traffic forwarding mode i.e when traffic coming to controller and when traffic moving locally from Ap to connected access switch. Admin should have option to create policies to allow or deny access based on applications.	
10	WLC should support AP License Migration from one WLC to another	
11	**S**hould support minimum 4000 VLANs	
12	WLAN controller should support 802.11ac wave 2	
13	the controller should have overall throughput of 4Gbps	
14	**Wireless Controller Features**	
15	Must support stateful switchover between active and standby controller in a sub second time frame.	
16	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients	
17	WLC should support guest-access functionality for IPv6 clients.	
18	Should support IEEE 802.1p priority tag.	
19	Should ensure WLAN reliability by proactively determining and adjusting to changing RF conditions.	
20	Should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments.	
21	Should support automatic radio channel adjustments for intelligent channel switching and real-time interference detection.	
22	Should support client load balancing to balance the number of clients across multiple APs to optimize AP and client throughput.	
23	Should support policy based forwarding to classify data traffic based on ACLs	
24	WLC should support PMIPv6 and EoGRE tunnels on northbound interface	
25	Should support flexible DFS to prevent additional 20/40 Mhz channels from going unused	
26	Should support dynamic bandwidth selection among 20Mhz, 40 Mhz and 80Mhz channels, ensuring one access point on 20Mhz and another on 80 Mhz channel connected on the same controller at same WLAN group.	
27	Should support minimum 500 WLANs	
28	Should support dynamic VLAN assignment	
29	Should support Hot Spot 2.0	
30	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.	
31	Should able to do dynamic channel bonding based on interference detected on particular channel.	
32	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.	
33	Must support RF Management with 40 MHz and 80 Mhz channels with 802.11n & 802.11ac	
34	Should provide visibility to Network airtime in order to set the airtime policy enforcement	
35	Must support dynamic Airtime allocation on per WLAN, per AP, Per AP group basis.	
36	Must be able to restrict the number of logins per user.	

37	Proposed solution should have support for policy based automation for wired and wireless and the proposed wireless solution to be seamlessly integrated with software driven architecture which can provide network automation, assurance & security	
38	**Security**	
39	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.	
40	WLC should support web based authentication in different traffic forwarding modes i.e Central switching and Local switching when traffic move locally from AP to connected switch.	
41	Should support port-based and SSID-based IEEE 802.1X authentication.	
42	Should support MAC authentication to provide simple authentication based on a user's MAC address.	
43	WLC should be able to exclude clients based on excessive/multiple authentication failure.	
44	Shall support AES or TKIP encryption to secure the data integrity of wireless traffic	
45	Shall support the ability to classify over 20 different types of interference with in 5 to 30 seconds.	
46	Shall able to provide an air quality index for ensuring the better performance	
47	Shall able to provide real time chart showing interference per access point on per radio and per-channel basis.	
48	Should support AP location-based user access to control the locations where a wireless user can access the network	
49	Should support Public Key Infrastructure (PKI) to control access	
50	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.	
51	WLC Shall support WIDS/WIPS, and spectral analysis from day 1.	
52	WLC should detect if someone connect a Rogue Access Point in network and able to take appropriate action to contain rogue Access point.	
53	In case of Access point connected in remote locations over WAN, containment should happen even if WAN is down.	
54	WLC should detect and protect an Ad-hoc connection when a connected user forming a network with other system without an AP or try enabling bridging between two interface	
55	WLC should detect if a user try to impersonate a management frame.	
56	WLC should detect and take appropriate containment action if a smartphone user using tethering to connect other device.	
57	WLC should detect and protect if a user try to spoof mac address of valid client or AP for unauthorized access/authentication.	
58	WLC should detect if a user trying to do internet sharing through a valid system to an unauthorized device.	
59	**Management & QoS**	
60	Should support SNMPv3, SSHv2 and SSL for secure management.	
61	Should support encrypted mechanism to securely upload/download software image to and from Wireless controller.	
62	Should provide visibility between a wired and wireless network using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and sFlow/equivalent.	
63	Should support AP Plug and Play (PnP) deployment with zero-configuration capability	
64	Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group	
65	Should support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation	
66	Should have a suitable serial console port.	
67	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS	

68	Controller should support deep packet inspection for all user traffic across Layer 4-7 network to analyses information about applications usage, peak network usage times for all access points from day one with different traffic forwarding modes i.e central switching with WLC and local switching when traffic move locally from AP to connected switch.	
69	Should be able to do application visibility for application running behind HTTP proxy.	
70	Support profiling of wireless devices based on known protocols like http and dhcp to identify clients	
71	Should support visibility and control based on the type of applications	

Indoor Wireless Access Point 802.11b/g/n/802.11ac

S/N	Features	Compliance (Yes/No/Equivalent or Higher)
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave 2.	
2	An access point must include a standard OEM provided Mounting brackets for mounting on Celling or Roof top.	
3	Access point must support spectrum intelligence across 20-, 40-, and 80-MHz-wide channels to combat performance problems due to wireless interference.	
4	Access point should have console port	
5	Must have 3dBi 2.4Ghz Antenna & 5 dBi 5.0Ghz Antenna	
6	Must support 3x3 spatial streams for both 802.11ac and 802.11n client	
7	Access point must support a minimum of 1.9 Gbps user throughput including both the radios	
8	Must support minimum of 22dbm of transmit power in both 2.4Ghz and 5Ghz radios. And should follow the WPC norms.	
9	Should support Multiuser MIMO (MU-MIMO)	
10	Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.	
11	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	
12	Must have -100 dB or better Receiver Sensitivity.	
13	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.	
14	Must support Management Frame Protection.	
15	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).	
16	Access Points must support Hardware-based encrypted user data and management traffic between controller and Access point for better security.	
17	Must support the ability to serve clients and monitor the RF environment concurrently.	
18	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.	
19	Should support mesh capabilities for temporary connectivity in areas where no Ethernet cabling.	
20	Mesh support should support QoS for voice over wireless.	
21	Must be plenum-rated (UL2043).	
22	Must support 16 WLANs per AP for SSID deployment flexibility.	
23	Must continue serving clients when WAN link to controller is back up again, should not reboot before joining	

24	The APs must support centralized wireless mode with the use of a controller, but the APs must also support operation in autonomous mode without the presence of any controller, when needed	
25	When operated in remote AP mode, the AP must not disconnect any clients when the connection to the controller fails or in the case the failed connection has been restored again.	
26	When operated in remote AP mode, the AP must be able to authenticate new users with local radius server directly at the AP itself in case of link failure to controller.	
27	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.	
28	Must support Power over Ethernet, local power (DC Power), and power injectors.	
29	802.11e and WMM	
30	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level	
31	Must support QoS and Video Call Admission Control capabilities.	
32	Access Point should 802.11 DFS certified	

Outdoor WIRELESS ACCESS POINT 802.11b/g/n/802.11ac

Sr. No.	Specification	Compliance (Yes/No/Equivalent or Higher)
1	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.	
2	AP should support dual band antenna ports.	
3	Must support a variety of antenna options. (Omni and directional)	
4	Must have -88 dB or better Receiver Sensitivity.	
5	Must support 2X2 multiple-input multiple-output (MIMO) with two spatial streams	
6	Must support 802.11ac, Wave 2 and backward compatible with 802.11n standards	
7	Must support data rates up to 1.3 Gbps on 5Ghz radio.	
8	Must support 80 MHz wide channels in 5 GHz.	
9	Must support WAP enforced load-balance between 2.4Ghz and 5Ghz band.	
10	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data	
11	Must support upto 28dbm or heigher of transmit power	
12	Accesspoint should 802.11ac, 802.11n and 802.11a/b/g Beamforming	
13	The Wireless Backhaul/Mesh shall operate in 5Ghz	
14	Support Encrypted and authenticated connectivity between all backhaul components	
15	Access point should have multiple wired uplink interfaces including 10/100/1000BASE-T Ethernet autosensing (RJ-45) and a build-in SFP port	
16	Wireless AP should support beamforming technology to improve downlink performance of all mobile devices, including one-, two-, and three-spatial-stream devices on 802.11ac without taking the inputs from client.	
17	Wireless AP Should able to detect and classify non-Wi-Fi wireless transmissions.	
18	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data.	
19	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	

20	Access point shall support powering from AC /DC/ UPOE.	
21	Access point shall support pole, wall and Cable strand mounting options.	
22	The equipment shall support up to 100 MPH sustained winds & 140 MPH wind gusts.	
23	The Access point shall be IP67 and NEMA rated	
24	The Access point shall support operating temperature of -40 to 65°C	
25	The Access point shall support Storage temperature of -50 to 70°C	
26	802.11e and WMM	
27	WiFi Alliance Certification for WMM and WMM power save	
28	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level	
29	Must support QoS and Video Call Admission Control capabilities.	
30	Must support the ability to serve clients and monitor the RF environment concurrently.	
31	Must support Spectrum analysis including @ 80 MHz	
32	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.	
33	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.	
34	Should have and option of configuring all the antennae port via software to run all on dual band or any single band configuration.	
35	Must support 16 WLANs per AP for BSSID deployment flexibility.	
36	Must support telnet and SSH login to APs directly for troubleshooting flexibility.	

MINIMUM DESIRED TECHNICAL SPECIFICATIONS OF PASSIVE ITEMS

UTP Cable - Cat6

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2		
Material:		
Conductors	23 AWG solid bare copper or better	
Insulation	Polyethylene	
Jacket	Sheath Fire retardant PVC Compound (FRPVC) Flame Rating : 60 deg. C As per UL 1685 CM/CMR	
Pair Separator	Cross-member fluted member	
Approvals	UL tested for TIA/EIA-568C.2	
	ETL verified to Cat 6	
	Zero Bit Error verified by ETL.	
Operating temperature	-20 Deg. C to +60 Deg. C	
Frequency tested up to	Minimum 600 MHz	
Packing	Box of 305 meters	
Delay Skew	35ns MAX.	
Impedance	100 Ohms + / - 6 ohms	
Performance characteristics to be provided along with bid	Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR	

Attenuation	22.8dB/100m at 250MHz	
	29.4dB/100m at 400MHz	
	39dB/100m at 600MHz	

UTP Patch Cord- Cat6

Feature	**Specification**	**Compliance (Yes/No/Equivalent or Higher)**
Type	**Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2**	
Conductor	24-26 AWG **stranded** copper.	
Length	1 /2/3 meter	
Plug Protection	Matching colored snag-less, boot to maintain bend radius	
Warranty	25-year component warranty	
Category	Category 6 Plug	
Housing	Clear polycarbonate	
Terminals	Phosphor Bronze with gold plating , 50 micron'' gold over nickel	
Load bar	PBT polyester	
Jacket	PVC	
Insulation	Flame Retardant Polyethylene	
End point connector	Factory standard connector	
Approvals	UL, ETL	
Material	ROHS compliant	

(All above enclosures must be valid)

Date: **Signature of the tenderer with date & seal**

Place:

Annexure-III

Declaration by the Tenderer

This is to certify that I/We, before signing this tender have read and fully understood all the terms and conditions contained herein and undertake myself/ourselves to abide by them.

I/We hereby undertake that the information provided with this tender are true and the tender is liable to rejection if the same is found to be false or the information is found to have been suppressed by me/us.

(Signature of Tenderer with seal)

Name:

Seal:

Address:

Phone No (O):

Date:

Annexure-IV

FINANCIAL BID

[RENOVATION AND UP-GRADATION OF NETWORK INFRASTRUCUTRE (LAN & WIFI)]

Name of the Tenderer:……

Part A-BOQ FOR MAIN CAMPUS FOR RENOVATION AND UP-GRADATION OF NETWORK INFRASTRUCTURE AT NIFT, KOLKATA

Particulars						Unit Rate (In Rs.)	GST (In Rs.)	Total Amount (including GST)(Rs.)
A) Active Components:								
SL	Item Type	Make & Model	Description	Qty./As per Actual	UoM			
1	Core Switch		24 Port 10/100/1000Mbps L3 Managed Switch with at least 2x (10G)SFP+ slots & 2 (two) nos. of SM 1G transceiver module loaded + 3 Years Warranty Support	1	No.			
2	Access Switch - PoE		24 Port 10/100/1000Mbps L2 Managed POE Switch with 2 x (10G) SFP+ slots loaded with at least 1 (one) no. of SM 1G transceiver module + 3 Years Warranty Support	10	Nos.			
	Access Switch - NON-PoE		24 Port 10/100/1000Mbps L2 Managed Switch with 2 x (10G) SFP+ slots loaded with at least 1 (one) no. of SM 1G transceiver module + 3 Years Warranty Support	13	Nos.			
3	Wireless Lan Controller		Wireless LAN Controller(WLC) with minimum 150+ AP support + 3 Years warranty	1	No.			
4	AP License		Single AP adder License for WLC	33	Nos.			
5	Indoor Access Point		Dual-band 802.11ac Indoor Wireless Access Point with Mounting Bracket + 3 Years warranty	32	Nos.			
6	Outdoor Access Point		Dual-band 802.11ac Outdoor Wireless Access Point with Mounting Bracket + 3 Years warranty	1	Nos.			

Passive Components:

SL	Item Type	Make & Model	Description	Qty	UoM			
1	Optical Fiber Cable		6 Core Single Mode Outdoor OFC	700	Mtr.			

Signature of Authorized person of the Firm/Agency with stamp/ seal

2	Fiber Patch Panel (LIU)		24 Port fully loaded SM with SC Adapter & SC SM Pigtails	2	Nos.			
			12 Port fully loaded SM with SC Adapter & SC SM Pigtails	8	Nos.			
3	Fiber Patch Cord		Single Mode SC-LC 2-Mtr. OFC Patch Cord	22	Nos.			
4	UTP Cable		CAT6 23AWG 4-Pair UTP Cable	45	Boxes			
5	Information Outlet		CAT6 I/O with Face Plate and SMB	420	Nos.			
6	Patch Pannel		24 Port fully loaded CAT6 Patch Pannel	24	Nos.			
7	UTP Patch Cord		1 Mtr. CAT6 UTP Patch Cord	480	Nos.			
			2 Mtr. CAT6 UTP Patch Cord	430	Nos.			
8	RJ45 Connecter		RJ-45 Connector for Cat6 Cable crimping.	1	Box			
9	Network Rack		9U Wall Mount Rack with standard accessories.	7	Nos.			
10	PVC Conduit		PVC Casing/Caping or PVC Pipe for laying of UTP Cable as per site requirement.	3500	Mtr.			
11	HDPE Pipe		HDPE Pipe for Outdoor OFC laying	200	Mtr.			

Service Components:

SL	Item Type	Description	Qty.	UoM			
1	UTP cable Laying	Laying of UTP Cable through the PVC conduit	13725	Mtr.			
2	OFC cable Laying	Laying of OFC Cable through the PVC conduit	700	Mtr.			
3	Soil Trenching & Refilling	Hard soil cutting & refilling	100	Mtr.			
4	Rack Fixing & Dressing	Fixing and dressing of Rack	10	Nos.			
5	Patch Panning Fixing	Patch Panel fixing & Punching	22	Nos.			
6	I/O Fixing	I/O Punching & fixing	420	Nos.			
7	RJ45 Crimping	RJ 45 connector crimping	35	Nos.			
8	Splicing	Splicing of each core of fiber cable	132	No			
9	Installing and Configuration	Installation and Configuration of Active devices, Testing and Documentation of entire project with 3 Years' service support + Dismantling of existing old networking cables and equipment's	1	Job			
				Sub Total of Part A			

Rupees in words_____

#1. GST to be mentioned specifically
#2. Other charges, if any, (delivery, installation, etc.) should mentioned clearly
#3. Bidder should quote for all the items as mentioned above; otherwise, the bid will liable to be canceled.
#4. Quantity may vary and payment will be made on actual

Signature of Authorized person of the
Firm/Agency with stamp/ seal

NIT No.: e-08/2018(Pur-Kol)-Revised

Part B-BOQ FOR GIRLS' HOSTEL FOR RENOVATION AND UP-GRADATION OF NETWORK INFRASTRUCTURE AT NIFT, KOLKATA

Particulars						Unit Rate (In Rs.)	GST (in Rs.)	Total Amount (including GST)(Rs.)
A) Active Components:								
SL	Item Type	Make & Model	Description	Qty./As per Actual	UoM			
1	24 Access Switch - PoE		24 Port 10/ 100/1000Mbps L2 Managed P OE Switch with 2 x (10G)SFP+ slots + 3 Years Warranty Support	1	Nos.			
2	12 Access Switch - PoE		12 Port 10/100/1000Mbps L2 Managed POE Switch with 2 x (10G)SFP+ slots + 3 Years Warranty Support	3	Nos.			
3	Wireless Lan Controller		Wireless LAN Controller(WLC) with minimum 150+ AP support + 3 Years warranty	1	No.			
4	AP License		Single AP adder License for WLC	34	Nos.			
5	Indoor Access Point		Dual-band 802.11ac Indoor Wireless Access Point with Mounting Bracket + 3 Years warranty	33	Nos.			
6	Outdoor Access Point		Dual-band 802.11ac Outdoor Wireless Access Point with Mounting Bracket + 3 Years warranty	1	Nos.			

Passive Components:

SL	Item Type	Make & Model	Description	Qty	UoM			
1	UTP Cable		CAT6 23AWG 4-Pair UTP Cable	2	Boxes			
2	UTP Patch Cord		1 Mtr. CAT6 UTP Patch Cord	40	Nos.			
3	RJ45 Connecter		RJ-45 Connector for Cat6 Cable crimping.	1	Box			
4	PVC Conduit		PVC Casing/Caping or PVC Pipe for laying of UTP Cable as per site requirement.	200	Mtr.			

Service Components:

SL	Item Type	Description	Qty	UoM			
1	UTP cbale Laying	Laying of UTP Cable through the PVC conduit	610	Mtr.			
2	Rack Fixing & Dressing	Fixing and dressing of Rack	4	Nos.			
3	RJ45 Crimping	RJ 45 connector crimping	66	Nos.			
4	Installing and Configuration	Installation and Configuration of Active devices, Testing and Documentation of entire project with 3 Years' service support + Dismantling of existing old networking cables and equipment's if required.	1	Job			

Signature of Authorized person of the Firm/Agency with stamp/ seal

	Sub Total of Part B			

Grand Total = Sub Total of Part A + Sub Total of Part B	(Amount in Rs.)
(Rupees.....Only)	

#1. GST to be mentioned specifically
#2. Other charges, if any, (delivery, installation, etc.) should mentioned clearly
#3. Bidder should quote for all the items as mentioned above; otherwise, the bid will liable to be canceled.
#4. Quantity may vary and payment will be made on actual

Date:_____
Place:_____

Signature of the tenderer with date & seal

Signature of Authorized person of the
Firm/Agency with stamp/ seal