NIT No.: NIFT/SHL/PO/2018-19/E02-LAN

Tender Document Fee Rs. 500/- + GST@18%

राष्ट्रीय फैशन टैक्नालॉजी संस्थान शिलांग

NATIONAL INSTITUTE OF FASHION TECHNOLOGY, SHILLONG
(A Statutory Body governed by the NIFT Act 2006 &
set up by Ministry of Textiles, Govt. of India)

TENDER
For
“SETTING UP OF NETWORK INFRASTRUCTURE (LAN & WiFi) IN NIFT SHILLONG PERMANENT CAMPUS”

Tender No.: NIFT/SHL/PO/2018-19/E02-LAN

DATE OF PUBLICATION OF TENDER NOTIFICATION	8th June 2018 (Friday)
OPENING DATE FOR ONLINE SUBMISSION OF TENDER	8th June 2018 (Friday)
PREBID MEETING	14th June 2018 (Thursday)
CLOSING DATE FOR ONLINE SUBMISSION OF TENDER	27th June 2018 (Wednesday) upto 2 PM
DATE AND TIME OF OPENING OF TECHNICAL BIDS	28th June 2018 (Thursday) at 11:00 AM
DATE AND TIME OF OPENING OF FINANCIAL BIDS	Will be notified to the technically qualified bidders only

Note:

1. The Terms and Conditions in the Tender document may be read thoroughly before submission along with all enclosures

2. The tender document contains **31** pages and bidders are requested to sign on all the pages. The Technical bid and the Financial bid should be sealed by the tenderer in two separate envelopes duly super scribed as “Technical Bid” and “Financial Bid” respectively for “Tender for Setting up of Network Infrastructure (LAN & WiFi)-NIFT in NIFT Shillong Permanent Campus: NIFT/SHL/PO/2018-19/E02-LAN” and addressed to:

The Purchase Officer, National Institute of Fashion Technology,
NIFT Shillong Campus, (Old NEIGRIHMS Campus),
'C' Block, Pasteur Hills, Lawmali,
Shillong - 793 001, Meghalaya

The Tender Fee along with EMD Demand Draft should be put in the Technical bid envelope.

INDEX

Sl. No	Particulars	Page No
1	Notice Inviting Tender	1
2	Introduction	3
3	Tender Notice	3
4	Submission of Bids	4
5	General Terms and Conditions	4
6	Annexure – I	7
7	Annexure – II Technical Bid	8
8	Scope of Work	9
9	Minimum Desired Specification for Active Items	11
10	Minimum Desired Specification for Passive Items	21
11	Annexure – III (Declaration by the Tenderer)	27
12	Annexure – IV (Financial Bid)	28

NIT No.: NIFT/SHL/PO/2018-19/E02-LAN

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 National Institute of Fashion Technology (NIFT) was set up by the Ministry of Textiles, Government of India in 1986 which has been accorded statutory status under the Act of Parliament in 2006 (NIFT Act 2006) for the promotion and development of education and research in field of Fashion Technology. NIFT provides fashion business education across the country through its network of 16 centers. It provides Four years under graduate (UG) program in design and technology, two years post graduate (PG) program in Design, Fashion Management & Fashion Technology and short duration education program to address the specialized needs of professional and students in the field of Fashion. NIFT has its head office at New Delhi with its campuses located at Bengaluru, Bhopal, Bhubaneswar, Chennai, Gandhinagar, Hyderabad, Jodhpur, Kangra, Kannur, Kolkata, Mumbai, New Delhi, Patna, Raibareli, Shillong and Srinagar.
NIFT Shillong Permanent Campus is located at Mawdiang diang, Umsawli – 793018. NIFT Shillong Resource Centre offers access to a rich repository of books as well as electronic resources comprising e-books, e-journals, online databases and services, and intellectual assets produced by the students and faculty of NIFT.

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 Shillong invites online tender under "Two Bids System" for "Setting up of Network Infrastructure (LAN & WiFi) in NIFT Shillong Permanent Campus" from the eligible reputed Firms/Agencies.

The hard copy of the tender along with fees (DDs for EMD, Tender Cost), necessary/relevant documents should be placed in a sealed envelope super scribed with "Tender for Setting up of Network Infrastructure (LAN & WiFi)-NIFT in NIFT Shillong Permanent Campus: NIFT/SHL/PO/2018-19/E02-LAN" and shall be addressed and sent to the Purchase Officer, National Institute of Fashion Technology, National Institute of Fashion Technology, NIFT Shillong Campus, (Old NEIGRIHMS Campus), 'C' Block, Pasteur Hills, Lawmali, Shillong - 793 001, Meghalaya or dropped in the Tender Box kept at the said address on or before 12th June 2018 (Tuesday) before 2:00 PM in the following manner.

i. Description of Services: "Setting up of Network Infrastructure (LAN & WiFi) in NIFT Shillong Permanent Campus Mawdiangdiang, Umsawli – 793018"

ii. Commencing date of Tender Notice: 8th June 2018

iii. Closing date & time for submission of Bids: 27th June 2018 upto 02:00 PM

iv. Date & time of opening of Bids :
Technical bid: 28th June 2018 at 11:00 AM (in presence of the tenderers or their authorized representatives.)
Financial bid: Will be notified to the technically qualified bidders only

v. Bid validity upto: 60 days from the date of opening of Financial bid

vi. Correspondence Address: The Purchase Officer, National Institute of Fashion Technology, NIFT Shillong Campus, (Old NEIGRIHMS Campus),'C' Block, Pasteur Hills, Lawmali, Shillong - 793 001, Meghalaya

vii. EMD Amount: Rs 7,50,000/- (Rupees Seven Lac Fifty Thousand Only)
(In the form of DD/PO in favour of NIFT, Shillong payable at Shillong)
(Refundable to unsuccessful Bidders by NIFT after receiving the "letter of acceptance" of the Order from the Successful bidder.)

viii. Tender Cost: Rs 500/- + Rs 90/- (@ 18% GST) = Rs 590/-
(Rupees Five Hundred and Ninety Only and Non Refundable)
(In the form of DD/PO in favour of NIFT, Shillong payable at Shillong)

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 8th June 2018 (Friday) to 27th June 2018 (Wednesday) up to 2.00 P.M. Tender documents are also available for viewing on the "tenders" link of the NIFT website i.e. https://www.nift.ac.in/shillong/tenders

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

- Annual Registration Charges of Rs. 2000/- + Rs. 360/- (@18% GST) = Rs 2360/- (Two Thousand Three Hundred Sixty Only) non-refundable.
- Bid Processing Fee charges of Rs. 5,000/- + Rs. 900/- (@18% GST) = Rs. 5,900/- (Rupees Five Thousand Nine Hundred Only) non-refundable through Online/Net Banking 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 Shillong office on Telephone No. 0364-2591492/2590963 or email: purchase.shillong@nift.ac.in, National Institute of Fashion Technology, National Institute of Fashion Technology, NIFT Shillong Campus, (Old NEIGRIHMS Campus), 'C' Block, Pasteur Hills, Lawmali, Shillong - 793 001, Meghalaya

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

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. 590/- (Rupees Five Hundred & Ninety Only) (Non-Refundable) drawn in favour of NIFT Shillong payable at Shillong towards Tender Cost shall be attached with Technical Bid.
6. All tenderers are required to submit Earnest Money Deposit (EMD) of Rs.7,50,000/- (Rupees Seven Lakh Fifty Thousand Only)(refundable) in the form of Demand Draft (should be drawn beyond the date of notification of this NIT) in favour of NIFT Shillong payable at Shillong. 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 Shillong 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 three years (i.e F.Y. 2014-15, 2015-16 & 2016-17) 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 to be 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 Setting up of Network Infrastructure (LAN & WiFI) at NIFT Shillong Permanent Campus & submission of required performance security and acceptance of goods in good condition on the basis of certification by the concerned department of NIFT, Shillong. 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 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.

17. The Renovation and Up-Gradation of Network Infrastructure (LAN & WiFi) should be executed at NIFT Shillong Permanent Campus, Umsawli, Mawdiang diang, Shillong – 793 018 by the supplier at its own cost within 10 -12 weeks from the date of receiving of Work Order.

18. 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.

19. 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.

20. 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.

21. Late submission of bids will not be considered whatsoever.

22. Tender shall be accompanied by the relevant documents including the following:-
    - Current Trade License:
    - Aadhar Number of the Proprietor
    - A client list as per Sl.no.3, Annex-I
    - Total turnover of the company for last 3 years (supporting documents should be submitted)
    - Copy of PAN [in the name of firm/agency or proprietor]:
    - GST Registration Certificate:
    - Authorization Certificate of OEM:

23. The full & final payment shall be made after SITC [supply, installation, testing & commissioning] for the Setting up 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.

24. The successful bidder shall deposit the Security Deposit of 5% of the ordered value through DD/Bank Guarantee in favour of NIFT Shillong 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.

25. 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.

26. The supplier shall ensure that he himself or his authorized representative is available for proper handing over the supplies/consignments at NIFT Shillong Centre.
27. For the specification of goods refer Annexure 'IV'.
28. Delivery is required to be completed within 10 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.
29. Items / goods supplied and installed should be New and Unused.
30. If any malafide intention is observed by NIFT, the agency shall not be eligible to participate in any future tenders with NIFT.
31. The vendor should have the qualified engineers/staff to attend to After Sales Service at NIFT Shillong 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 Shillong 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, Shillong Campus/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, Shillong. 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. at NIFT Shillong Permanent Campus, Umsawli, Mawdiangdiang, Shillong – 793 018
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 (0364-2590240/963). However, NIFT will not entertain or clarify any such query during post bid.
41. In case of any dispute arising out of the present tender, only the courts at Shillong will have the exclusive Jurisdiction to adjudicate the dispute.(Advisable to have an arbitration clause for settlement of disputes).

Selection Criteria:

The work will be awarded to L1 vendor on overall basis of Setting up of Network Infrastructure (LAN & WiFi)-NIFT in NIFT Shillong Permanent Campus: NIFT/SHL/PO/2018-19/E02-LAN. The determination of lowest bidder will NOT be on individual rates of financial bids. Rather it will be on overall basis.

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:
   a) Current Trade License:
   b) Aadhar Number of the Proprietor
   c) A client list as per Sl.no.3, Annex-I
   d) Total turnover of the company for last 3 years (supporting documents should be submitted)
   e) Copy of PAN [in the name of firm/agency or proprietor]:
   f) GST Registration Certificate:
   g) Authorization Certificate of OEM:

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.

ANNEXURE – II

TECHNICAL BID
[SETTING UP OF NETWORK INFRASTRUCTURE (LAN & WiFi) IN NIFT SHILLONG PERMANENT CAMPUS]

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.590/- (Rupees Five Hundred & Ninety Only) favouring NIFT Shillong is enclosed as tender cost (if tender document is downloaded from website/not purchased).	
03	Whether Demand Draft of Rs.7,50,000/- (Rupees Seven Lakh Fifty Thousand Only) in favour of NIFT, SHILLONG 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 Aadhar Number Enclosed	
07	Whether copy of GST Registration Certificate enclosed	
08	Whether Copy of PAN enclosed	
09	Whether price quoted as per the required specification mentioned in the Annexure 'IV' and inclusive of all taxes & other charges with delivery upto NIFT, Shillong Permanent Campus	
10	Whether relevant document submitted showing Annual Turnover for the last three years [i.e. FY: 2014-2015; 2015-2016 & 2016 -17] 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]	
11	Whether Copy of Income Tax Return for the last 3 years submitted [Assessment year 2014 -15; 2015 -16 & 2016 - 17]	
12	Whether agreed to abide by all the terms & conditions of this tender	
13	Whether all DDs, Annexure-I, II & III duly filled, are enclosed with this Technical Bid and Annexure-IV, duly filled, with Financial Bid	

NIT No.: NIFT/SHL/PO/2018-19/E02-LAN

SCOPE OF WORK:SETTING UP OF NETWORK INFRASTRUCTURE (LAN & WiFi) IN NIFT SHILLONG PERMANENT CAMPUS:

A) Active Components:

SL	Item Type	Description	Qty./As Per Actual	UoM
1	Firewall/UTM	Throughout put 25 GBPS Gbps, Concurrent Session 4500000 No, New Session Per Second 180000 No, Integrated Interface "GE copper ", IPsec VPN Peers (Users) free, Local Storage 480 GB SSD with RAID, Expansion Slots 2 No, Total Value Subscription Plus includes Anti Malware, Anti Spam, Web and Application Filter, Intrusion Prevention System , 24x7 Support, hardware warranty and RMA fulfillment, IPv6 Ready, +3 years warranty support	2	No
2	Core Switch L3	24 Port x 10G SFP L3 Managed Switch with at least 2x (10G)SFP+ slots & 2 (two) nos. of SM 1G transceiver module loaded + 3 Years Warranty Support	2	No.
3	Access Switch – 48 Ports	48 Port x 1G 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	50	Nos.
4	Access Switch – 24 Ports	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	3	Nos.
5	Wireless Lan Controller	Wireless LAN Controller(WLC) with minimum 150+ AP support + 3 Years warranty	1	No.
6	AP License	Single AP adder License for WLC	134	Nos.
7	Wireless AP (CAP)	Dual-band 802.11ac Indoor Wireless Access Point with Mounting Bracket + 3 Years warranty	134	Nos.

B) Passive Components:

SL	Item Type	Description	Qty	UoM
1	SFP transceiver module	GLC-LH-SMD= (Single mode optical transceiver - 1000BaseLX) 1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	65	Nos
2	SFP-GE-T	SFP (mini-GBIC) transceiver module, GigE, 1000Base-T, RJ-45, up to 328 ft, for P/N: 10720-GE-FE-TX, 10720-GE-FE-TX= , 10720-GE-FE-TX-B, 10720-GE-FE-TX-B=	5	Nos
3	24 Port Rack Mount LIU	24 Port Rack Mount LIU loaded with Splice Tray and Cable spool & also fitted with 2-nos of 6 Port adapter plate loaded with SC (OM3) couplers per LIU	2	Nos
4	12 Port Rack Mount LIU	12 Port Rack Mount LIU loaded with Splice Tray and Cable spool & also fitted with 2-nos of 6 Port adapter plate loaded with SC (OM3) couplers per LIU	17	Nos
5	Optical Fiber Patch Chord SC - LC	SM. SC - LC Duplex, 9.2/125 micron SM Fiber (3mtr) : SC to LC Fiber Duplex patch cord (OM3) (3 Mtrs)	70	Nos
6	Optical Fiber Patch Chord SC - SC	Optical Fiber Patch Chord, SM. SC - SC Duplex, 9.2/125 micron SM Fiber (3mtr) : SC to SC Fiber Duplex patch cord (OM3) (3 Mtrs) in-lieu of Pigtail SC SM - 1.5 Mtr compatible with fusion or mechanical splices	100	Nos
7	Outdoor Armoured Cable (OFC)	12 core outdoor armoured cable – SM (OS2)	9300	Mtr
8	Rack 12U	19"12U Wall Mount rack with necessary accessories	28	Nos
9	Rack 42U	42U Rack with necessary accessories	4	Nos
10	Cable Manager	1U Horizontal wire manger (CAT6A)	32	Nos
11	Patch Panel 48 Ports	48 Port, Cat 6 Jack Panel (Loaded with UTP I/O)	24	Nos
12	Patch Panel 24 Ports	24 Port, Cat 6 Jack Panel (Loaded with UTP I/O)	10	Nos
13	Cat 6 Cable	CAT6 23AWG 4-Pair UTP Cable (305 mtr per box)	8	Nos
14	I/O Box	I/O Box (Single SMB)	125	Nos
15	Casing	Supply of ISI marked 32 mm Casing Caping (with 1 year warranty)	580	Mtr
16	PVC Conduit	Supply of 1" PVC Conduit Medium with necessary fixtures (with 1 year warranty)	220	Mtr
17	UTP Patch Cable	UTP Patch Cord-1 mtr (CAT 6)	521	Nos
18	UTP Patch Cable	UTP Patch Cord -3 mtr	521	Nos
19	Labels	Labels for Jackpanel/ face Plate/Patch Cords (set of 100)	11	Nos
20	RJ45 Connecter	RJ-45 Connector for Cat6 Cable crimping (Set of 100 per Box)	2	Box
21	HDPE Pipe	HDPE Pipe for Outdoor OFC laying	9300	Mtr.

Details Specification for setting up of Network Infrastructure (LAN & WiFi)

General Requirements:

a. **All active components including LAN & Wi-Fi should be from single OEM.**
b. **End of life for all active components should have minimum of 5 years and bidder should arrange an undertaking from OEM side in this regard along with next 5 years support commitment**
c. **OEM must have ISO 9001:2008, ISO 14001:2004 certified**
d. **Both UTP & Fiber components must be from the same OEM**

NIT No.: NIFT/SHL/PO/2018-19/E02-LAN

MINIMUM DESIRED TECHNICAL SPECIFICATIONS OF ACTIVE ITEMS

Firewall/UTM

Sl. No.	TECHNICAL SPECIFICAITONS AND STANDARDS FOR UNIFIED THREAT MANAGEMENT	Compliance (Yes/No/ Equivalent or Higher)	Remarks (if any)
1	Product or OEM should attain ISO 9001 certification as well as should attain ISO for its Support Services		
2	Proposed appliance should build in min hot swappable 450GB SSD with RAID as an internal storage with Hot Swap Redundant Power Supply& Hot swappable Fan Tray		
3	The Firewall should be ICSA Labs certified and NSS Lab recommended. OEM should be leader in Gartner UTM Magic Quadrant for last 5 years.		
4	Appliance Throughput		
4.1	Must have a 64-bit hardware platform		
4.2	Must be based on Multicore Parallel Processing Architecture with 24GB of RAM		
4.3	Firewall throughput (IMIX) of 22Gbps or better.		
4.4	Minimum 10Gbps of Antivirus Throughput		
4.5	Minimum 30,000,000 Concurrent sessions or better		
4.6	Minimum 16Gbps of IPS throughput or better		
4.7	Minimum 9000Mbps NGFW throughput or better		
4.8	Minimum 200,000 New Sessions/second or better		
4.9	Minimum 8000 Mbps of IPSec VPN throughput and 4000 Mbps of SSL VPN throughput		
5	**General Features**		
5.1	Identity based Firewall		
5.2	Intrusion Prevention System		
5.3	Gateway Anti-virus		
5.4	Gateway Anti-spam		
5.5	Web Content, Application Filtering and Web Application Firewall features		
5.6	Bandwidth Management		
5.7	Inbuilt-on Appliance Reporting for Compliance		
5.8	Network: OSPF, Round Robin load balance, RIPv2, BGP, equal & unequal cost load balance, High Availability, QoS, etc. Round Robin Balance, Server Load Balancing.		
5.9	Support for user authentication over SMS.		
5.10	Country Based Blocking, FQDN support and should support MIX mode deployment		
5.11	Support for ICAP and Link Aggregation		
5.12	Shall support DHCP Relay, NTP/SNTP, SNMP, Syslog		
5.13	User/IP/MAC binding functionality to map username & IP address & MAC address		
5.14	Network Interfaces: 8 x 10/100/1000BaseT Ports, and 2 x 10GbE SFP and expandable to additional 4 x 10GbE SFP+ with 2X 40G QSFP+ SFP future ready ports from day one.		
5.15	Shall support 802.1Q VLANs		
5.16	Shall support deployment in Active-Active HA mode and statefull failover with Multiple ISP Link Aggregation Support (minimum 4 nos.)		
5.17	Shall support source and destination NAT, NAT Traversal for Voice protocols.		
5.18	It shall support management through web based GUI and CLI by way of serial console, Telnet and SSH.		
6	Gateway Antivirus, Anti-Spyware, Anti Malware and Anti-Spam		

6.1	Ransomware Protection, Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area.		
6.2	The next generation firewall should support dual anti malware engine from day one		
7	Web and Application Filtering:		
7.1	URL, Keyword, File type block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL, block P2P application, anonymous proxies, Customized block on group basis. Minimum of 82 categories with more than 100 million URLS supported with more than 6000 application support.		
8	**Intrusion Prevention System (IPS):**		
8.1	Checkmark Certified. For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (6000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection		
8.2	Shall provide statefull firewall and protection against SQL Injections, Cross-site Scripting, Session Hijacking, URL Tampering, Cookie Poisoning etc.		
9	**Web Application Firewall (WAF):**		
9.1	Should have On appliance WAF with Positive Protection Module, Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Extensive Logging and reporting with subscription. If WAF is external Appliance should be quoted separately with 9000 Mbps throughput & 3 years subscription licenses.		
9.2	Web Application Firewall for at least 40 backend running servers.		
10	**VPN:**		
10.1	IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal, VPNC Certified.		
11	**Load Balance:**		
11.1	For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.		
12	Bandwidth Management:		
12.1	Application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Group, Firewall Rule, URL and Applications.		
13	**Monitoring and Reporting System:**		
13.1	Includes reports for Centralized management, Monitoring & Logging, Command line interface. Monitoring Gateways, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. IPS, Web filter, Antivirus, Anti-spam system reports. IP and User basis report, 45+ Compliance reports and 1000+ drilled down reports on the appliance.		
13.2	Shall support logging, viewing and reporting of all UTM services including firewall, IPS, Web & Application control, Anti-Virus & Anti-Spam etc.		
14	License for UTM (Unified Threat Management)		
14.1	Three Years for Gate Way Antivirus, spyware, Anti-Spam, content and application filtering, IPS, WAF and 24*7 supports License. License period will be counted after activation.		

24 Port L3 Core Switch

S/N	**Features**	**Compliance (Yes/No/Equivalent or Higher)**	**Remarks (if any)**
1	**General**		

1.1	The Switch should have minimum 24 x 10G SFP+ ports.		
1.2	The switch should have the option to support 8 x 10G SFP+ ports in future.		
1.3	Should have internal Redundant Power supply		
1.4	Support for Configuration and image rollback		
1.5	IPv4 & IPv6 Layer 3 forwarding in hardware		
1.6	Should have 4GB DRAM & 2GB Flash memory		
1.7	Switch OEM should be in the Gartner's/IDC Leaders quadrant for Wired and Wireless LAN Access Infrastructure		
2	**Performance**		
2.1	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.		
2.2	Should have 480Gbps Switching capacity & 200 Mpps forwarding rate		
2.3	Fully non-blocking backplane and wire-speed throughput with minimal latency		
2.4	MAC Address table : 30000		
2.5	Should support 24000 routes		
3	**Layer 3 feature**		
3.1	Basic IP unicast routing protocols (Static, RIPv1 and RIPv2) should be supported from day 1.		
3.2	Should have future support for advanced routing support including OSPF, IS-IS, BGP, policy based routing & Multicast routing		
4	**Layer 2 feature**		
4.1	IEEE 802.1Q VLAN encapsulation. At least 1000 VLANs should be supported. Support for 4000 VLAN IDs.		
4.2	Support for Voice VLAN which will simplify telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.		
4.3	Administration and troubleshooting.		
4.5	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.		
4.6	IEEE 802.1d, 802.1s, 802.1w, 802.3ad standard support from day-1		
4.7	Link Aggregation Protocol (LACP)		
4.8	Support for Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.		
4.9	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.		
4.1	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.		
4.1	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.		
5	**Network Security Features**		
5.1	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.		
5.2	IEEE 802.1x to allow dynamic, port-based security, providing user authentication.		
5.3	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.		
5.4	Support for SSHv2 and SNMPv3.		
5.5	Support for Network Admission Control, IP source Guard, MAC Limiting		

5.6	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.		
5.7	MAC address notification to allow administrators to be notified of users added to or removed from the network.		
5.8	Dynamic ARP Inspection or equivalent which can ensure user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.		
5.9	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.		
5.1	Port security to secure the access to an access or trunk port based on MAC address.		
5.1	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.		
5.1	Spanning tree feature to shut down Spanning Tree Protocol enabled interfaces when BPDU’s are received to avoid accidental topology loops.		
5.1	Security ACL entries – At least 1000.		
6	**Quality of Service (QoS) & Control**		
6.1	Standard 802.1p CoS and DSCP		
6.2	Control- and Data-plane QoS ACLs		
6.3	Eight egress queues per port to enable differentiated management of up to four traffic types across the stack.		
6.4	Support for congestion avoidance mechanism		
6.5	Strict priority queuing mechanisms		
6.6	There should not be any performance penalty for highly granular QoS functions.		
6.7	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.S		
6.8	Switch should support at least 1000 aggregate polices.		
7	**Management**		
7.1	Command Line Interface (CLI) support for configuration & troubleshooting purposes.		
7.2	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.		
7.3	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.		
7.4	FTP/ Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.		
7.5	Network Timing Protocol (NTP) based on RFC 1305 to provide an accurate and consistent timestamp to all intranet switches.		
7.6	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.		
7.7	RMON I and II standards		
7.8	SNMPv1, SNMPv2c, and SNMPv3		
8	**Certification**		
8.1	The switch should be common criteria EAL4 or NDPP certified.		

24 Port and 48 Port POE Access Switch

S/N	**Features**	**Compliance (Yes/No/ Equivalent or Higher)**	**Remarks (if any)**

1	**General Features**		
1.1	The switch should have minimum 24 x 10/100/1000 Base-T PoE/PoE+ Ports & 2 x 10G SFP+ slots for 24 Ports PoE Switch. The switch should have minimum 48 x 10/100/1000 Base-T PoE/PoE+ Ports & 2 x 10G SFP+ slots for 48 Ports PoE Switch		
1.2	Future support for Redundant Power supply		
1.3	Should have fan for proper cooling.		
2	**Performance**		
2.1	At least 88 Gbps (24 Port POE switch) / 200 Gbps (48 Port POE switch) switching bandwidth.		
2.3	Forwarding rate - At least 70 Mpps (24 Port POE switch) / 120 Mpps (48 Port POE switch)		
2.4	Configurable at least 16000 MAC addresses		
2.5	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.		
2.6	DRAM 512 MB and 128 MB Flash		
3	**Layer-2 Features**		
3.1	IEEE 802.1Q VLAN encapsulation. At least 1000 VLANs should be supported. Support for 4000 VLAN IDs.		
3.2	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.		
3.3	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.		
3.4	Spanning-tree Enhancements for fast convergence		
3.5	IEEE 802.1d, 802.1s, 802.1w, 802.3ad,		
3.6	Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.		
3.7	IGMPv3. Support for at least 1000 IGMP Groups. IGMP filtering.		
3.8	Link Aggregation Protocol (LACP)		
3.9	Support for UDLD (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.		
3.10	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.		
3.11	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.		
3.12	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.		
3.13	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.		
4	**Network Security Features**		
4.1	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.		
4.2	IEEE 802.1x to allow dynamic, port-based security, providing user authentication.		
4.3	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.		
4.4	SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.		

4.5	Bidirectional data support on the Mirrored port to allow the intrusion detection system (IDS) to take action when an intruder is detected.		
4.6	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.		
4.7	MAC address notification to allow administrators to be notified of users added to or removed from the network.		
4.8	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.		
4.9	Port security to secure the access to an access or trunk port based on MAC address.		
4.10	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.		
4.11	BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU's are received to avoid accidental topology loops.		
4.12	Should support 500 IPv4 ACL entries, 500 IPv6 ACL entries,		
5	**Quality of Service (QoS) & Multicast**		
5.1	Standard 802.1p CoS and DSCP		
5.2	Control- and Data-plane QoS ACLs, Cross-stack QoS		
5.3	Up to eight egress queues per port		
5.4	Strict priority queuing mechanisms		
5.5	There should not be any performance penalty for highly granular QoS functions.		
5.6	Committed information rate (CIR) function to provide bandwidth in increments of 8 Kbps		
5.7	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.		
5.8	Flow-based rate limiting and up to 200 aggregate or individual policers per port		
5.9	Shaped Round Robin (SRR) scheduling and Weighted Tail Drop (WTD) congestion avoidance.		
5.10	2000 IPv4 & IPv6 Unicast Routes		
5.11	1000 IPv4 Multicast Groups, 1000 IPv6 Multicast Groups		
6	**Management**		
6.1	Superior manageability Features		
6.2	Command Line Interface (CLI) support for configuration & troubleshooting purposes.		
6.3	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.		
6.4	Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.		
6.5	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.		
6.6	FTP/ Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.		
6.7	Network Timing Protocol (NTP) based on RFC 1305 to provide an accurate and consistent timestamp to all intranet switches.		
6.8	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.		
6.9	RMON I and II standards		
7	**Certification:**		
7.1	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)**	**Remarks (if any)**
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 support minimum 3000 concurrent devices.		
6	WLAN controller should support 134 Access points from day 1. It should be scalable to support up to 150 Access Points without any hardware change.		
7	Should be rack-mountable. Required accessories for rack mounting to be provided.		
8	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.		
9	WLC should support AP License Migration from one WLC to another		
10	Should support minimum 4000 VLANs		
11	WLAN controller should support 802.11ac wave 2		
12	the controller should have overall throughput of 4Gbps		
13	**Wireless Controller Features**		
14	Must support stateful switchover between active and standby controller in a sub second time frame.		
15	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients		
16	WLC should support guest-access functionality for IPv6 clients.		
17	Should support IEEE 802.1p priority tag.		
18	Should ensure WLAN reliability by proactively determining and adjusting to changing RF conditions.		
19	Should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments.		
20	Should support automatic radio channel adjustments for intelligent channel switching and real-time interference detection.		
21	Should support client load balancing to balance the number of clients across multiple APs to optimize AP and client throughput.		
22	Should support policy based forwarding to classify data traffic based on ACLs		
23	WLC should support PMIPv6 and EoGRE tunnels on northbound interface		
24	Should support flexible DFS to prevent additional 20/40 Mhz channels from going unused		
25	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.		
26	Should support minimum 500 WLANs		
27	Should support dynamic VLAN assignment		
28	Should support Hot Spot 2.0		
29	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.		
30	Should able to do dynamic channel bonding based on interference detected on particular channel.		

31	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.		
32	Must support RF Management with 40 MHz and 80 Mhz channels with 802.11n & 802.11ac		
33	Should provide visibility to Network airtime in order to set the airtime policy enforcement		
34	Must support dynamic Airtime allocation on per WLAN, per AP, Per AP group basis.		
35	Must be able to restrict the number of logins per user.		
36	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		
37	**Security**		
38	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.		
39	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.		
40	Should support port-based and SSID-based IEEE 802.1X authentication.		
41	Should support MAC authentication to provide simple authentication based on a user's MAC address.		
42	WLC should be able to exclude clients based on excessive/multiple authentication failure.		
43	Shall support AES or TKIP encryption to secure the data integrity of wireless traffic		
44	Shall support the ability to classify over 20 different types of interference with in 5 to 30 seconds.		
45	Shall able to provide an air quality index for ensuring the better performance		
46	Shall able to provide real time chart showing interference per access point on per radio and per-channel basis.		
47	Should support AP location-based user access to control the locations where a wireless user can access the network		
48	Should support Public Key Infrastructure (PKI) to control access		
49	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.		
50	WLC Shall support WIDS/WIPS, and spectral analysis from day 1.		
51	WLC should detect if someone connect a Rogue Access Point in network and able to take appropriate action to contain rogue Access point.		
52	In case of Access point connected in remote locations over WAN, containment should happen even if WAN is down.		
53	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		
54	WLC should detect if a user try to impersonate a management frame.		
55	WLC should detect and take appropriate containment action if a smartphone user using tethering to connect other device.		
56	WLC should detect and protect if a user try to spoof mac address of valid client or AP for unauthorized access/authentication.		
57	WLC should detect if a user trying to do internet sharing through a valid system to an unauthorized device.		
58	**Management & QoS**		
59	Should support SNMPv3, SSHv2 and SSL for secure management.		
60	Should support encrypted mechanism to securely upload/download software image to and from Wireless controller.		

61	Should provide visibility between a wired and wireless network using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and sFlow/equivalent.		
62	Should support AP Plug and Play (PnP) deployment with zero-configuration capability		
63	Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group		
64	Should support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation		
65	Should have a suitable serial console port.		
66	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS		
67	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.		
68	Should be able to do application visibility for application running behind HTTP proxy.		
69	Support profiling of wireless devices based on known protocols like http and dhcp to identify clients		
70	Should support visibility and control based on the type of applications		

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

S/N	Features	Compliance (Yes/No/ Equivalent or Higher)	Remarks (if any)
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 must have an two ethernet port for Link aggregation		
5	Access point should have console port		
6	**Must have atleast 3 dBi Antenna gain on each radios**		
7	**Must support 4x4:4 spatial streams for both 802.11ac and 802.11n client**		
8	Access point must support a minimum of 1.9 Gbps user throughput including both the radios		
9	Must support minimum of 22dbm of transmit power in both 2.4Ghz and 5Ghz radios. And should follow the WPC norms.		
10	Should support Multiuser MIMO (MU-MIMO)		
11	Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.		
12	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		
13	Must have -100 dB or better Receiver Sensitivity.		
14	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.		
15	Must support Management Frame Protection.		
16	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
17	Access Points must support Hardware-based encrypted user data and management traffic between controller and Access point for better security.		

18	Mesh support should support QoS for voice over wireless.		
19	Must be plenum-rated (UL2043).		
20	Must support 16 WLANs per AP for SSID deployment flexibility.		
21	Must continue serving clients when WAN link to controller is back up again, should not reboot before joining		
22	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.		
23	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.		
24	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.		
25	Must support Power over Ethernet, local power (DC Power), and power injectors.		
26	802.11e and WMM		
27	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level		
28	Must support QoS and Video Call Admission Control capabilities.		
29	Access Point should 802.11 DFS certified		

MINIMUM DESIRED TECHNICAL SPECIFICATIONS OF PASSIVE ITEMS

SM Fiber optic Cable

Feature	**Specification**	**Compliance (Yes/No/ Equivalent or Higher)**	**Remarks (if any)**
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	06/12/2024		
Cable Construction	BELLCORE GR 20 / IEC 794-1		
Nominal Diameter	9.5 - 10.5 mm		
Cable Sheath Thickness	Not less than 2mm		
Water blocking compound	Cable must have Water blocking compound		
Strength Member	Should have glass yarn strength member		
Cable outer jacket Specification	HDPE outer jacket. Cable must be direct buried		
Attenuation :			
@1310nm	< = 0.33 dB/Km		
@1550nm	< = 0.22 dB/Km		
@1380-1386nm	<=0.31 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		
	<18.5 ps/nm-km @1550 nm		
Fiber cable	ETL certified for Fiber channel compliance as per ANSI/TIA 568-C		
Tensile rating	1200N		
Maximum Crush resistance	3000N		
Operating Temperature	-20 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		
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 - 110 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	ANSI/TIA 568-C.3and ISO/IEC 11801		
	IEC 60794-1		
Complies	ANSI/TIA 568.C.0		
Approval	Intertek certified Fiber. Product OEM shall be member of global TIA committee.		
RoHS	RoHS Compliant		
Length of cable drum	(+/-) 4000 Mtrs		

06/12/24 Port SM Fiber Optic LIU

Feature	**Specification**	**Compliance (Yes/No/ Equivalent or Higher)**	**Remarks (if any)**
Fiber optic patch panel	19-inch, Rack Mount Fiber optic patch panel		
Height	1 U, 1.75 inches		
No. of fibers	06/12/24		
Material	Complete Aluminium Alloy / Steel housing, fully powder coated. 16 gauge material construction.		
	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 4		
Grounding	Earthing lugs, pre-loaded		
Cable Management rings	2 nos of cable management rings, pre-loaded		
No. of 6-port adapter plates	4 max or as per configuration required		
RoHS	RoHS Compliant		
Fiber Optic adapter plate	6-port, LC-Style, SM		
Attenuation	Max of 0.75 dB per mated pair		
Insertion Loss	< 0.3 dB max		
Durability (1000 Mattings)	< 0.2 dB max		
Material Ferrule	Zirconia (for SM)		
ROHS	RoHS Compliant		
Certification	ETL certified		
Compliant	EIA/TIA 568-C.0		
RoHS	RoHS verified.		
Product Features & Compliances	Zirconia or Phosphor Bronze Sleeve		
Compliant	As per ISO/IEC 11081		
RoHS	RoHS Compliant		
SM Pigtails - LC type	Should support multiple applications including CWDM.		
	Available in 0.9 mm cordage		
	Should support Pull proof connector design		

	Minimum Cable Retention Strength: 1.6mm; 11.24 lbs (50N)		
	Product Must have RoHS Compliant		
Insertion Loss	0.3 dB max		
Return Loss	> 45 dB		

SM Fiber Optic Patch Cord LC/UPC-LC/UPC Type

Feature	**Specification**	**Compliance (Yes/No/ Equivalent or Higher)**	**Remarks (if any)**
F.O. Patch Cords	**Patch Cord / SM patch cord LC/UPC - LC/UPC TYPE**		
Outside Diameter	(Duplex): 1.8mm x 3.6mm		
Minimum Cable Retention Strength	1.6mm: 11.24 lbs (50 N)		
Insertion Loss	Less than 0.3 dB for SM		
Return Loss	> 45dB		
Fiber Glass Technology	Patch Cords must be Clear Curve Fiber		
Micro bending coating	CPC coating		
RoHS	RoHS Compliant		
Approval	Shall be ETL certified for SM as per ANSI/TIA 568-C fiber channel requirement		

UTP Cable - Cat6

Feature	**Specification**	**Compliance (Yes/No/ Equivalent or Higher)**	**Remarks (if any)**
Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2			
Material:			
Conductors	23 AWG solid bare copper or better		
Insulation	Polyethylene		
Jacket	Sheath shall be LSZH as per IEC 60332-3-22 (Flame test), IEC 60754-2 (Acid gas emission) and IEC 61034-2 (Smoke density). Test reports against these standards must be submitted with bid for evaluation.		
Pair Separator	Cross-member fluted member		
Approvals	ETL certified for 4 connector channel performance as per ANSI/TIA 568-C.2 requirements of Category 6, tested upto 600 MHz. Report to be submitted with bid.		
	ETL verified to Cat 6		
Operating temperature	-20 Deg. C to +60 Deg. C		
Frequency tested up to	Upto 600 MHz		
Packing	Box of 305 meters		
Delay Skew	45ns 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 under 4 connector channel configuration	31.2 dB/100m at 250MHz		
	40.3 dB/100m at 400MHz		
	51.1 dB/100m at 600MHz		
Identification	Cable jacket shall feature unique tracking number for accessing factory test reports online at OEM website.		
Qualification	Product OEM must be member of global TIA committee.		

Information Outlet- Cat6

Feature	Specification	Compliance (Yes/No/ Equivalent or Higher)	Remarks (if any)
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 4 connector channel compliant		
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 Panel

Feature	Specification	Compliance (Yes/No/ Equivalent or Higher)	Remarks (if any)
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, " goldm94V-0 rated, Spring Contact: Phosphor bronze 50		
Jack contacts	Phosphorous bronze		
Panel	Black, powder coated steel		
Approvals	UL , ETL 4 connector channel compliant		
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)**	**Remarks (if any)**
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	LSZH as per IEC 60332-1		
Insulation	Polyethylene		
End point connector	Factory fitted RJ45 connector		
Approvals	UL / ETL		
Material	ROHS compliant		

Network Rack-12U/42U

Feature	**Specification**	**Compliance (Yes/No/ Equivalent or Higher)**	**Remarks (if any)**

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 1360 Kg in 42U rack and 113Kg in 12U rack.		
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 - 12U overall height : 533.4mm; Usable Height : 464.1mm 42U overall height : 2000mm; Usable Height : 1897.9mm		
	Width – It should be 600mm and 19” mounting should be there		
	12U Depth – It should be 500mm 42U Depth – It should be 1000mm		
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 5/15 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.		

(All above enclosures must be valid)

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

Place:

Annexure-III

[To be submitted by the tenderer on their company letter head along with the technical bid]

Declaration by the Tenderer

To,

The Purchase Officer,

National Institute of Fashion Technology,

NIFT Campus, Old NEIGRIHMS, Block-C,

Pasteur Hills, Lawmali, Polo,

Shillong-793001

Sub: Technical bid relating to setting up of network infrastructure at NIFT, Shillong Permanent Campus

Ref.: Your Notice e- Inviting Tender No…………………… dated ………….

Sir/ Madam,

This is to certify that

- 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.
- I/We also confirm my/our commitment to provide the services as enlisted in schedule of item with your Notice Inviting Tender under reference.
- 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.
- That I/We have not been blacklisted by any Central/ State Government organization for similar kind of activities in past or for future.
- That I/We have acquainted self with all the tasks required to be carried out, before making this offer.
- That I/We have the means to execute the scope of work as specified in the tender document
- That I/We hereby sign this undertaking as token of our acceptance of various conditions mentioned in tender document.

(Signature of Tenderer with seal)

Name:

Seal:

Address:

Phone No (O):

Date:

Annexure-IV

FINANCIAL BID

[SETTING UP OF NETWORK INFRASTRUCUTRE (LAN & WIFI) AT NIFT SHILLONG PERMANENT CAMPUS, UMSAWLI, MAWDIANGDIANG]

Name of the Tenderer:……………………………………………………………………………………………………..

Part A - BOQ FOR SETTING UP OF NETWORK INFRASTRUCTURE AT NIFT, SHILLONG PERMANENT CAMPUS

A) Active Components:

Particulars						Unit Rate (In Rs.)	GST (In Rs.)	Total Amount (including GST)(Rs.)
SL	Item Type	Make & Model	Description	Qty./As per Actual	UoM			
1	Firewall/UTM		Throughout put 25 GBPS Gbps, Concurrent Session 4500000 No, New Session Per Second 180000 No, Integrated Interface "GE copper ", IPsec VPN Peers (Users) free, Local Storage 480 GB SSD with RAID, Expansion Slots 2 No, Total Value Subscription Plus includes Anti Malware, Anti Spam, Web and Application Filter, Intrusion Prevention System , 24x7 Support, hardware warranty and RMA fulfillment, IPv6 Ready, +3 years warranty support	2	Nos.			
2	Access Switch – 24 Ports		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	3	Nos.			
	Access Switch – 48 Ports		48 Port x 1G 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	50	Nos.			
3	Core Switch L3		24 Port x 10G SFP L3 Managed Switch with at least 2x (10G)SFP+ slots & 2 (two) nos. of SM 1G transceiver module loaded + 3 Years Warranty Support	2	Nos.			

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

4	Wireless LAN Controller		Wireless LAN Controller(WLC) with minimum 150+ AP support + 3 Years warranty	1	Nos.			
5	AP License		Single AP adder License for WLC	134	Nos.			
6	Wireless AP (CAP)		Dual-band 802.11ac Indoor Wireless Access Point with Mounting Bracket + 3 Years warranty	134	Nos.			

Sub Total = A) Active Components: INR ______________________________

In Words Rupees: ____

B) Passive Components:

SL	Item Type	Make & Model	Description	Qty./As per Actual	UoM	Unit Rate (In Rs.)	GST (In Rs.)	Total Amount (including GST)(Rs.)
1	SFP transceiver module		GLC-LH-SMD= (Single mode optical transceiver - 1000BaseLX) 1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	65	Nos			
2	SFP-GE-T		SFP (mini-GBIC) transceiver module, GigE, 1000Base-T, RJ-45, up to 328 ft, for P/N: 10720-GE-FE-TX, 10720-GE-FE-TX= , 10720-GE-FE-TX-B, 10720-GE-FE-TX-B=	5	Nos			
3	24 Port Rack Mount LIU		24 Port Rack Mount LIU loaded with Splice Tray and Cable spool & also fitted with 2-nos of 6 Port adapter plate loaded with SC (OM3) couplers per LIU	2	Nos			
4	12 Port Rack Mount LIU		12 Port Rack Mount LIU loaded with Splice Tray and Cable spool & also fitted with 2-nos of 6 Port adapter plate loaded with SC (OM3) couplers per LIU	17	Nos			
5	Optical Fiber Patch Chord SC - LC		SM. SC - LC Duplex, 9.2/125 micron SM Fiber (3mtr) : SC to LC Fiber Duplex patch cord (OM3) (3 Mtrs)	70	Nos			
6	Optical Fiber Patch Chord SC		Optical Fiber Patch Chord, SM. SC - SC Duplex, 9.2/125 micron SM Fiber (3mtr) : SC to	100	Nos			

	- SC		SC Fiber Duplex patch cord (OM3) (3 Mtrs) in-lieu of Pigtail SC SM - 1.5 Mtr compatible with fusion or mechanical splices					
7	Outdoor Armoured Cable (OFC)		12 core outdoor armoured cable – SM (OS2)	9300	Mtr			
8	Rack 12U		19"12U Wall Mount rack with necessary accessories	28	Nos			
9	Rack 42U		42U Rack with necessary accessories	4	Nos			
10	Cable Manager		1U Horizontal wire manger (CAT6A)	32	Nos			
11	Patch Panel 48 Ports		48 Port, Cat 6 Jack Panel (Loaded with UTP I/O)	24	Nos.			
12	Patch Panel 24 Ports		24 Port, Cat 6 Jack Panel (Loaded with UTP I/O)	10	Nos			
13	Cat 6 Cable		CAT6 23AWG 4-Pair UTP Cable (305 mtr per box)	8	Nos			
14	I/O Box		I/O Box (Single SMB)	125	Nos			
15	Casing		Supply of ISI marked 32 mm Casing Caping (with 1 year warranty)	580	Mtr			
16	PVC Conduit		Supply of 1" PVC Conduit Medium with necessary fixtures (with 1 year warranty)	220	Mtr			
17	UTP Patch Cable		UTP Patch Cord - 1 mtr (CAT 6)	521	Nos			
18	UTP Patch Cable		UTP Patch Cord -3 mtr	521	Nos			
19	Labels		Labels for Jackpanel/ face Plate/Patch Cords (set of 100)	11	Nos			
20	RJ45 Connecter		RJ-45 Connector for Cat6 Cable crimping. (Set of 100 per Box)	2	Box			
21	HDPE Pipe		HDPE Pipe for Outdoor OFC laying	9300	Mtr.			

Sub Total = B) Passive Components: INR ______________________________________

In Words Rupees: ____

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

(Rupees in words ………Only)

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

NIT No.: NIFT/SHL/PO/2018-19/E02-LAN

#*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